TEMat

vol. 2 — julio 2018

divulgación de trabajos de estudiantes de matemáticas

e-ISSN 2530-9633

SF	56 %
MV	41 %
HF	29 %
GU	22 %
GV	19 %

Asociación Nacional de Estudiantes de Matemáticas

TEMat

divulgación de trabajos de estudiantes de matemáticas

volumen 2
julio de 2018

https://temat.es/volumen/2018/
https://anemat.com/

Una iniciativa de la
Asociación Nacional de Estudiantes de Matemáticas

Información editorial

Publica

Asociación Nacional de Estudiantes de Matemáticas
Plaza de las Ciencias, 3
Despacho 525, Facultad de Matemáticas
Universidad Complutense de Madrid
28040 – Madrid

temat@temat.es
publicaciones@anemat.com
contacto@anemat.com

Diseño de portada: Roberto Berná Larrosa, rbernalarrosa@gmail.com

TEMat, divulgación de trabajos de estudiantes de matemáticas – volumen 2 – julio de 2018
e-ISSN: 2530-9633
https://temat.es/

Sobre TEMat

TEMat es una revista de divulgación de trabajos de estudiantes de matemáticas publicada sin ánimo de lucro por la Asociación Nacional de Estudiantes de Matemáticas. Se busca publicar trabajos divulgativos de matemáticas, escritos principalmente (pero no exclusivamente) por estudiantes, de todo tipo: breves reseñas, introducciones a temas de investigación complejos, o artículos explicando las bases e incluso algún pequeño resultado de trabajos desarrollados por estudiantes.

TEMat persigue el doble objetivo de dar visibilidad a la calidad y diversidad de los trabajos realizados por estudiantes de matemáticas en los centros españoles a la vez que permite a los estudiantes publicar sus primeros artículos, familiarizándose así con el proceso de redacción, revisión y corrección que va asociado a la actividad investigadora.

Se contemplan para su publicación artículos escritos en castellano de todas las áreas de las matemáticas, incluyendo álgebra, análisis, ciencias de la computación, combinatoria, educación matemática, estadística, geometría, teoría de números y cualquier otra área de las matemáticas (puras y aplicadas), así como aplicaciones científicas o tecnológicas en las que las matemáticas jueguen un papel central.

La publicación en línea de este volumen de *TEMat* ha sido posible gracias al Ministerio de Educación, Cultura y Deporte a través de la convocatoria de 2017 de Subvenciones a Asociaciones Juveniles y a Federaciones y Confederaciones de Estudiantes Universitarios.

Revisiones externas

En este volumen han colaborado realizando revisiones externas:

Enric Cosme Llópez
Alba Delgado Calvache
Daniel Eceizabarrena
Ander Lamaison Vidarte
Manuel Mellado Cuerno
Erik Sarrión Pedralva
María Soria Carro

Índice general

Carta del presidente de la ANEM

Un año después del primer volumen de *TEMat*, desde la Asociación Nacional de Estudiantes de Matemáticas seguimos trabajando para apoyar iniciativas que doten de más recursos a los estudiantes de matemáticas de toda España. Dentro de esta estrategia, no podemos obviar la importancia de *TEMat*, revista pionera a nivel internacional que sigue creciendo.

Con la publicación de este segundo volumen reafirmamos nuestra voluntad de defender la ciencia abierta y apostar por los estudiantes que comienzan a caminar hacia una carrera de investigación, con todos los sacrificios que supone debido a la situación actual de precariedad que vive la ciencia española. Creemos firmemente que la educación y la investigación son bases indispensables para el funcionamiento y el progreso de una sociedad moderna, y que las matemáticas, disciplina en la que España ya pelea por encima de su peso, son la base fundamental para el desarrollo de un ecosistema científico de primer nivel.

No podría finalizar sin dar las gracias a todo el comité editorial por su dedicación y entusiasmo, así como a los autores de los artículos y a los revisores. Sin vosotros, este maravilloso proyecto nunca hubiera visto la luz. Esperamos que, los que no lo hayáis hecho ya, os apuntéis a enviar vuestros artículos a *TEMat* o a revisar los de vuestros compañeros de estudios.

Guillem García Subies,
presidente de la ANEM.

Madrid, julio de 2018.

TEMat

Los sorteos que utilizan las primeras letras de los apellidos como criterio de selección son injustos

Ramiro Martínez Pinilla
Graduado en Matemáticas (UPC)
Estudiante del Master in Advanced Mathematics and Mathematical Engineering (UPC)
ramiro.martinez@estudiant.upc.edu

Resumen: Este estudio pretende cuantificar las diferencias de probabilidad que se producen al seleccionar un grupo de personas mediante un sorteo en el que se obtiene una pareja de letras al azar y se asignan las plazas por orden alfabético de los apellidos. La distribución de las primeras letras de los apellidos no es uniforme en la población, por lo que este sistema no garantiza que todos los participantes tengan la misma probabilidad de ser seleccionados. Este es un hecho conocido, pero hasta el momento no se habían calculado estas probabilidades y estos sorteos se siguen utilizando.

Para calcular cada probabilidad de ser elegido realizaremos simulaciones de este tipo de sorteos. Analizaremos el margen de error de los resultados y comprobaremos que, efectivamente, se dan estas diferencias y las desigualdades que se producen son significativas.

Finalmente se propone una alternativa justa en la que todos los solicitantes tienen la misma probabilidad de ser seleccionados.

Abstract: This paper tries to quantify the inequalities that are produced when you select a group of people by means of a draw in which a pair of letters is obtained at random and the posts are assigned in alphabetical order. The distribution of the firsts letters of surnames is nonuniform, hence this scheme does not guarantee that all participants have the same probability of being selected. This is a well-known fact but, as far as we know, those probabilities have not been computed and this kind of draw is still being used.

To compute each probability of being selected we simulate many draws of this kind. We analyze the error of the results and we check that those differences arise and the inequalities are significant.

Finally, we propose an alternative fair scheme in which all participants have the same probability of being selected.

Palabras clave: probabilidad, estadística, simulación, intervalos de confianza, sorteos, apellidos.

MSC2010: 62P25.

Recibido: 12 de febrero de 2017.
Aceptado: 23 de octubre de 2017.

Agradecimientos: Agradezco a la ANEM por la creación de esta revista y especialmente a los revisores, que me ayudaron a mejorar notablemente el artículo y me animaron a ampliarlo a partir de su versión inicial.

Referencia: Martínez Pinilla, Ramiro. «Los sorteos que utilizan las primeras letras de los apellidos como criterio de selección son injustos». En: *TEMat*, 2 (2018), págs. 1-13. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p1/.

1. Introducción

En este estudio analizaremos un tipo de sorteo en el que, de una lista de N aspirantes, se pretende asignar una plaza a n de ellos, con $n \leq N$. En los sorteos que estudiamos se ordenan alfabéticamente sus apellidos y se obtiene al azar una pareja de letras. A partir de la posición en la lista marcada por estas dos letras se comienzan a adjudicar las plazas por orden alfabético, teniendo en cuenta que si se llega a la ZZ se continúa por la AA.

Estos sorteos tienen una serie de problemas. Aunque la elección de la pareja de letras sea uniformemente aleatoria, la distribución de las primeras letras de los apellidos en la población no es homogénea, y tampoco lo será en un grupo concreto de solicitantes. Esto hace que, dada una lista, si realizamos el sorteo, no todos tengan la misma probabilidad de obtener plaza, y el sorteo sea manifiestamente injusto.

Observación 1. Durante todo el artículo trataremos con diferentes espacios de probabilidad. Cuando se escogen las dos letras se hace de forma equiprobable, pues se eligen uniformemente al azar, pero esto no se traduce en que la distribución de las plazas sea también equiprobable, pues se trata de un espacio de probabilidad distinto. En el resultado final del sorteo, al escoger n de los N candidatos el término *equiprobable* podría interpretarse como que cada subconjunto de n elementos del conjunto N tenga la misma probabilidad de ser escogido. Sin embargo, no es necesaria una condición tan fuerte, pues es suficiente con que cada candidato individualmente tenga una probabilidad de n/N de ser escogido, pero no necesitamos que sean eventos independientes. Es por ello que nos fijaremos en esta última condición: todo candidato ha de tener la misma probabilidad de ser elegido al participar en un sorteo en el que el resto de candidatos se escogen uniformemente al azar del resto de la población. Esto es lo que denominaremos de forma abreviada como sorteo *justo*, pues es lo que realmente esperaríamos de este tipo de sorteos. ◂

La distribución de los apellidos en la muestra de solicitantes reflejará la distribución de los apellidos dentro de la población, no siendo tampoco homogénea. En un sorteo justo la distribución de las plazas debería reflejar la de los apellidos dentro de dicha población. Lo importante es que cualquier solicitante tenga la misma probabilidad de ser admitido, independientemente de las iniciales de su apellido.

Sin embargo, una persona cuyo apellido comience por una letra posterior a una muy frecuente tendrá una menor probabilidad de obtener plaza que otra cuya inicial siga a letras menos frecuentes. Simplificando el sorteo con una sola letra podemos ver fácilmente un ejemplo. Alguien cuyo apellido comience por A obtendrá plaza si en el sorteo se extrae la letra A. Pero, como las letras W, X, Y, Z son muy poco frecuentes en castellano, es improbable que haya algún otro solicitante cuyo apellido empiece por alguna de ellas. Por eso, si la escogida por el sorteo es W, X, Y o Z, la persona con apellido que comienza por A tiene también bastante probabilidad de obtener la plaza. Por otra parte alguien cuyo apellido comience por la letra N obtendrá plaza cuando sea esta letra la que salga del sorteo, pero tiene pocas posibilidades de obtenerla si el resultado es una letra anterior, puesto que la probabilidad de que alguno de los otros solicitantes tenga un apellido que comience por M es elevada. Este mismo razonamiento es igual de válido cuando se consideran dos letras en vez de una, pues lo único que se hace es aumentar el número de variables. Este es un hecho conocido y se ha publicado en blogs [4], artículos especializados [6] y en la prensa generalista [8] desde hace décadas.

Un caso extremo sucedería si a un sorteo de una única plaza se presentaran dos personas con apellidos diferentes pero que comenzaran por las mismas dos primeras letras. Aquella con el apellido anterior por orden alfabético siempre precederá a la otra en el resultado del sorteo, y esta segunda persona nunca podrá obtener plaza independientemente de las letras seleccionadas.

A pesar de ello, este sistema de selección en el que se utilizan las primeras letras de los apellidos para asignar plazas está muy extendido y se utiliza, entre otros, en la admisión del alumnado en los centros docentes de algunas comunidades autónomas [1, 3]. Es importante, por tanto, ir un paso más allá y comprobar si se trata de una mera curiosidad teórica o si en casos reales estas desigualdades son significativas y realmente se está discriminando a una parte de la población.

Para cuantificar las posibles diferencias no es suficiente con analizar una muestra concreta, como se ha hecho en el artículo de la revista de matemáticas *SUMA* [6] y en el artículo del diario *El País* [4]. Por ello, en este trabajo, para calcular la probabilidad de obtener plaza con un apellido concreto, programaremos

la simulación de un número suficientemente grande de sorteos utilizando datos de la población española. De esta forma, empleando herramientas estadísticas, conseguiremos cuantificar estas diferencias.

Es necesario hacer esto porque no podemos descartar *a priori* el caso de que, aunque en cada ejemplo concreto el sorteo sea injusto, globalmente estos desequilibrios puedan compensarse y la esperanza para cada inicial del apellido sea la misma. Podría ser que con una lista de solicitantes concreta un apellido que comience por XY se vea perjudicado, mientras que otra lista le beneficie, y la esperanza podría ser la de un resultado justo. En ocasiones, quienes plantean este tipo de sorteos interpretan que, como es aleatorio, unas veces perjudicará y otras veces beneficiará y se acabará compensando, confundiendo aleatorio con uniformemente aleatorio. Descartaremos esta posibilidad pues, fijados N y n, veremos que hay parejas de iniciales con una probabilidad de obtener plaza significativamente menor que otras.

También habría que tener en cuenta la posibilidad de que la dependencia respecto a los parámetros N y n fuera caótica, y pequeñas variaciones en ellos dieran lugar a distribuciones de probabilidad completamente distintas, en las que de nuevo unas parejas de iniciales fueran perjudicadas en unos casos y beneficiadas en otros. Calcular sistemáticamente los porcentajes de probabilidad concretos para cada caso nos permitirá comprobar que esto no es lo que sucede, y que las desigualdades generalmente persisten para diferentes valores de n y N.

Analizaremos en último lugar la dependencia geográfica de los resultados, pensando sobre todo en las comunidades con dos lenguas oficiales, repitiendo los experimentos tomando como población únicamente las comunidades autónomas de Castilla y León y del País Vasco para así identificar si existen grandes diferencias entre ellas. Veremos que, aunque en casos específicos los resultados son diferentes, en líneas generales obtendremos probabilidades similares.

Para finalizar, propondremos un método justo en el que todos los participantes tengan la misma probabilidad de ser escogidos independientemente de su apellido, teniendo en cuenta que sea sencillo de realizar y publicar, discutiendo las posibles dificultades técnicas a la hora de implementarlo.

2. Método

Consideraremos como población todos los habitantes de España a fecha de 1 de enero de 2016 [1]. Para la realización de este trabajo se han solicitado las primeras letras de los apellidos de la población al Instituto Nacional de Estadística [2] [2]. Ordenamos alfabéticamente estos apellidos para obtener una lista de 46 524 505 habitantes.

Fijado un número de plazas n y un número de solicitantes $N \geq n$, queremos calcular cuál es la probabilidad $p_{\mathtt{XY}}$ de que un solicitante cuyo apellido comience por las letras XY obtenga una plaza, siendo XY la pareja de letras que queramos estudiar en cada momento. Modelamos cada sorteo como una variable aleatoria de Bernoulli X que toma valor 1 si obtiene plaza y 0 en caso contrario. Idealmente, en un sorteo justo $p_{\mathtt{XY}} = n/N$ independientemente de XY.

Para obtener una muestra aleatoria simple de estas variables aleatorias programamos un *script* (algoritmo 1) en C++ que simule sorteos como los que estamos estudiando.

Queremos calcular la probabilidad de que, si una persona cuyas iniciales comienzan por XY se presenta al sorteo, obtenga plaza. Para ello, el *script* selecciona una persona control cuyo apellido comience por XY, simula todo el sorteo y anota si el candidato control ha obtenido o no plaza en el sorteo.

Utilizaremos la notación habitual en la que $variable \xleftarrow{\$} \{conjunto\}$ significa que se asigna a la variable *variable* un elemento de forma uniformemente aleatoria de entre los del conjunto $\{conjunto\}$. Cuando simplemente utilicemos el símbolo $\leftarrow$ se trata de una asignación determinista.

Hemos de tener en cuenta que, como los solicitantes siempre se ordenan alfabéticamente, no todos aquellos cuyo apellido comience por XY tienen la misma probabilidad de obtener la plaza. En el caso de

[1] En las simulaciones se han excluido los apellidos con caracteres especiales (*ñ, ç, '*) o de una sola letra, para facilitar el tratamiento informático.

[2] El INE es la fuente del dato primario, el grado de exactitud o fiabilidad de la información derivada por elaboración propia del autor es de la exclusiva responsabilidad de este.

Algoritmo 1 (Sorteo estudiando a un sujeto XY, con N solicitantes y n plazas).

subrutina SORTEO
▷ Elegimos a un candidato control cuyo apellido empiece por las letras que queremos estudiar
sujeto control $\xleftarrow{\$}$ {*población con apellidos que comienzan por* XY}
{*candidatos*} $\leftarrow$ *sujeto control*
▷ Elegimos al resto de candidatos uniformemente al azar entre el resto de la población
para $i \leftarrow 2, \ldots, N$ **hacer**
aux $\xleftarrow{\$}$ {*población*} $\setminus$ {*candidatos*}
{*candidatos*} $\leftarrow$ {*candidatos*} $\cup$ *aux*
fin para
▷ Escogemos uniformemente al azar una pareja de letras
letras $\xleftarrow{\$}$ {*parejas de letras*}
▷ Encontramos la posición que determinan en la lista y asignamos las plazas
encuentra la posición de la lista {*candidatos*} que señala *letras*
asigna plaza a los n primeros candidatos a partir de esta posición
▷ Comprobamos si el sujeto control ha recibido plaza
si *sujeto control* ha recibido plaza, **entonces**
$X \leftarrow 1$
en caso contrario
$X \leftarrow 0$
fin si
fin subrutina

que coincidan en el mismo sorteo dos personas con apellidos diferentes que comiencen por las mismas dos primeras letras, aquella cuyo apellido sea anterior por orden alfabético siempre obtendrá su plaza antes que la otra, independientemente del resultado del sorteo, como ya hemos mencionado previamente. Por lo tanto, hemos de precisar que llamamos p_{XY} al promedio de las probabilidades de obtener una plaza de cada una de las personas cuyo apellido comienza por XY. En consecuencia, elegiremos el solicitante control aleatoriamente entre todas las personas cuyo apellido comience por XY.

La pareja de letras que se obtenga del sorteo no determina directamente si una persona cuyo apellido comienza por XY obtendrá o no plaza. Esto dependerá también de los apellidos del resto de personas que hayan solicitado esa misma plaza. Por ello completamos la lista con otros $N-1$ solicitantes elegidos completamente al azar de la lista que contiene a toda la población. Podría haber más solicitantes cuyo apellido comience también con XY, pero nos aseguramos de que todos ellos sean distintos entre sí y del primero.

Por último, elegimos aleatoriamente un par de letras y anotamos si el individuo inicial ha obtenido una de las n plazas ($X = 1$) o no ($X = 0$). Repetimos este experimento m veces para tener una muestra aleatoria simple $X_1, \ldots, X_m$ de tamaño m.

Con esta muestra aleatoria simple, nuestro estimador de p_{XY} será $\widehat{p_{\mathrm{XY}}} = \frac{\sum_{i=1}^{m} X_i}{m}$. Si m es suficientemente grande, gracias al teorema central del límite (teorema 1) podemos considerar que

$$\widehat{p_{\mathrm{XY}}} \sim N\left(p_{\mathrm{XY}}, \sqrt{\frac{p_{\mathrm{XY}}(1-p_{\mathrm{XY}})}{m}}\right).$$

Teorema 1 (teorema central del límite [7]). *Si las variables independientes idénticamente distribuidas X_i tienen todas la misma distribución y media μ y desviación típica $\sigma \neq 0$ finitas, entonces la variable*

$$Y_m = \frac{X_1 + \cdots + X_m - m\mu}{\sigma\sqrt{m}}$$

es asintóticamente normal $N(0,1)$, es decir, la función de distribución $F_m(z)$ de Y_m verifica para todo z la relación

$$\lim_{m\to\infty} F_m(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} \mathrm{e}^{-x^2/2}\,\mathrm{d}x.$$

En nuestro caso, la media es p_{XY} y la desviación típica de las variables de Bernoulli es $\sqrt{p_{XY}(1-p_{XY})}$. Sustituyendo en la fórmula obtenemos

$$N(0,1) \sim \frac{X_1 + \cdots + X_m - m p_{XY}}{\sqrt{p_{XY}(1-p_{XY})}\sqrt{m}} = \frac{\frac{\sum_{i=1}^m X_i}{m} - p_{XY}}{\sqrt{\frac{p_{XY}(1-p_{XY})}{m}}}$$

$$N\left(p_{XY}, \sqrt{\frac{p_{XY}(1-p_{XY})}{m}}\right) \sim \frac{\sum_{i=1}^m X_i}{m} = \widehat{p_{XY}}.$$

Queremos que el estimador $\widehat{p_{XY}}$ nos permita asegurar, con un alto nivel de confianza, que el valor real se encontrará en un cierto entorno del valor del estimador. Para ello tendremos que tomar un valor suficientemente grande de m.

Elegimos como entorno $\left[\widehat{p_{XY}} - 0{,}005, \widehat{p_{XY}} + 0{,}005\right]$ y como nivel de confianza, un 99 %. Es decir, queremos asegurar que con una probabilidad de un 99 % el valor real de la probabilidad p_{XY} satisface que

$$p_{XY} \in \left[\widehat{p_{XY}} - 0{,}005, \widehat{p_{XY}} + 0{,}005\right]. \tag{1}$$

Modificamos la expresión (1) para normalizar el estimador y obtenemos

$$\frac{-0{,}005}{\sqrt{\frac{p_{XY}(1-p_{XY})}{m}}} \leq \frac{\widehat{p_{XY}} - p_{XY}}{\sqrt{\frac{p_{XY}(1-p_{XY})}{m}}} \leq \frac{0{,}005}{\sqrt{\frac{p_{XY}(1-p_{XY})}{m}}}. \tag{2}$$

Ahora $\frac{\widehat{p_{XY}} - p_{XY}}{\sqrt{\frac{p_{XY}(1-p_{XY})}{m}}} \sim N(0,1)$, y queremos que el intervalo definido por (2) abarque al menos un 99 % de probabilidad. Consultamos los cuantiles de la normal y obtenemos que ha de contener al intervalo $[-2{,}575829, 2{,}575829]$.

Para una m concreta, la longitud del intervalo (2) dependerá del valor de p_{XY} y será mínima con $p_{XY} = 0{,}5$. Sustituimos p_{XY} por 0,5 para calcular m, pues así garantizamos que en cualquier otro caso con esa m tenemos una confianza superior al 99 %. De esta manera tenemos que para $m \geq 66\,349$ obtendremos una estimación de p_{XY} con la que, efectivamente, podremos asegurar que el valor real se encontrará en el intervalo (1), con un 99 % de confianza.

Este proceso se ha de realizar para cada pareja de letras XY y para todos los pares (n, N) que queramos estudiar. Escogeremos diferentes valores de N que sean representativos de las posibles situaciones reales en las que se utilizan este tipo de sorteos.

3. Resultados

Para obtener las figuras 1 a 3 se ha calculado, para cada letra, la media ponderada de las probabilidades obtenidas para las parejas que comienzan por esa letra. Se ha tenido en cuenta el peso específico en la población de cada pareja de letras entre las que comienzan por la misma inicial.

La figura 1 corresponde al caso $n = 10$ y $N = 20$. En un sorteo justo esperaríamos que cada solicitante tuviera una probabilidad de un 50 % de obtener plaza. Observamos, sin embargo, que existen diferencias significativas entre las probabilidades de las distintas iniciales, que llegan a superar 15 puntos porcentuales.

Si analizamos el caso $n = 20$ y $N = 40$ en la figura 2, la probabilidad deseada es de nuevo un 50 %, pero el resultado experimental sigue sin ser el de un sorteo justo. Observamos que la distribución es muy similar a la del caso anterior, aunque no coincide exactamente.

Completamos este primer análisis con el caso $n = 10$ y $N = 40$ (figura 3). Podemos apreciar que las diferencias relativas entre las iniciales beneficiadas y las perjudicadas se han incrementado respecto a las figuras 1 y 2, en las que había una misma proporción *plazas*/*solicitantes*, que no se mantiene en esta figura. En este caso hay letras que tienen el doble de probabilidad que otras.

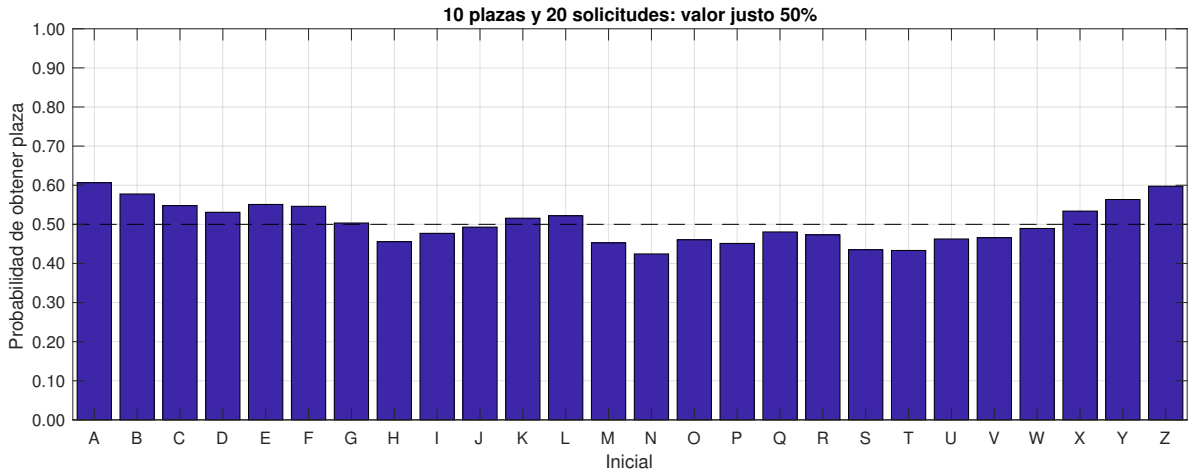

Figura 1: Probabilidad para cada inicial ($n = 10, N = 20$).

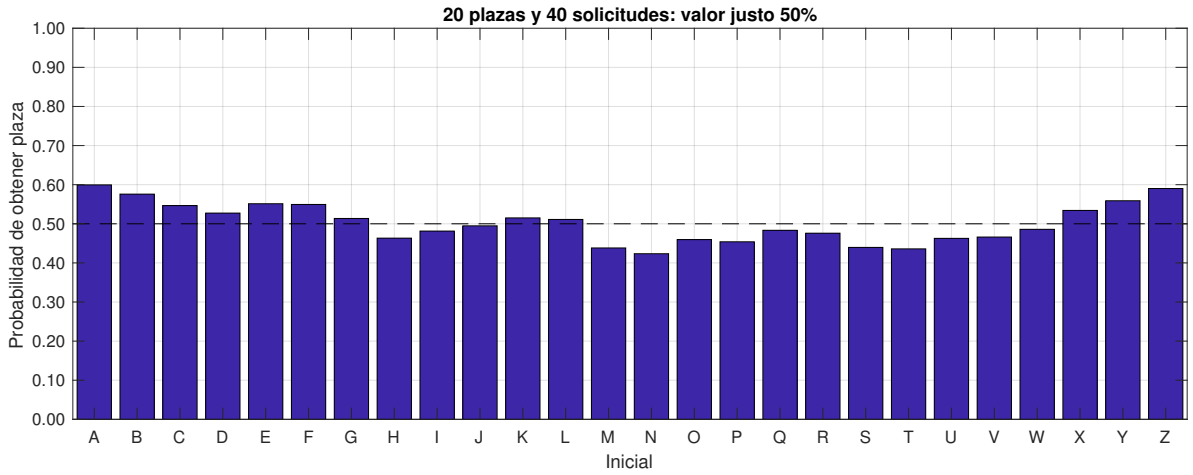

Figura 2: Probabilidad para cada inicial ($n = 20, N = 40$).

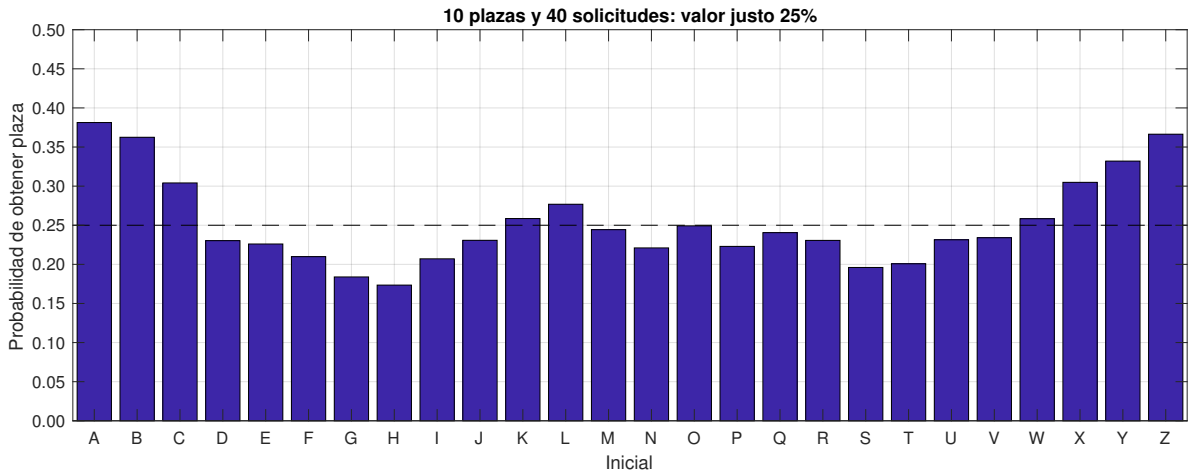

Figura 3: Probabilidad para cada inicial ($n = 10, N = 40$).

Las figuras 1 a 3 muestran que este sistema, basado en las iniciales de los apellidos, da lugar a unas probabilidades no uniformes, con las que no todos los apellidos tienen las misma probabilidad de obtener una plaza.

En las figuras 4 y 5 representamos la probabilidad de obtener plaza para los apellidos que comienzan por AL, CI, HE, KE y MU. Hemos seleccionado estas cinco parejas de iniciales porque representan los diferentes comportamientos que se pueden dar.

Estudiamos distintos casos dejando el número de plazas fijo y observamos el comportamiento de la probabilidad, a medida que incrementamos el número de solicitantes.

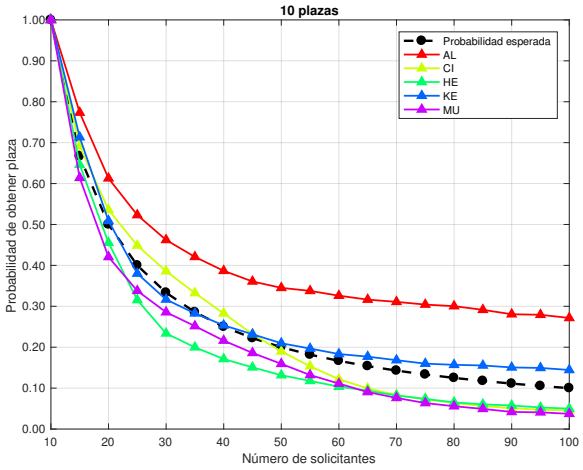

Figura 4: Diez plazas

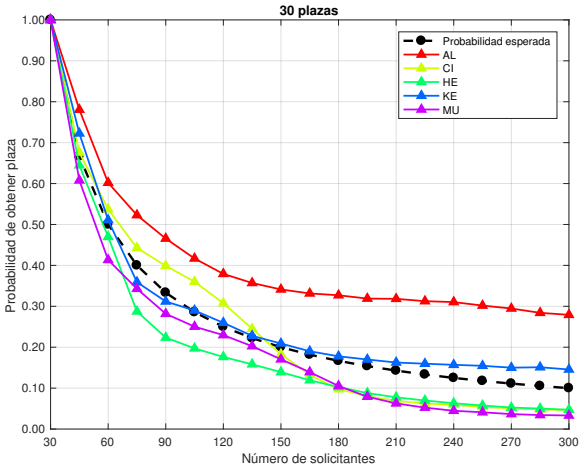

Figura 5: Treinta plazas

En el caso $n = 10$ (figura 4), aquellos cuyo apellido comience por AL se verán claramente beneficiados, con cualquier número de solicitantes. Aquellos cuyo apellido comience por HE o MU siempre se verán perjudicados por este tipo de sorteo. En algunos casos, como los apellidos que comienzan por KE, la probabilidad real se aproxima bastante bien a la teórica para los primeros valores del número de solicitantes N, mientras que, a medida que aumentan los solicitantes, resultan beneficiados con una probabilidad superior a la deseada. Por último, es también interesante el ejemplo de los apellidos que comienzan por CI, pues se ven beneficiados con un número bajo de solicitantes mientras que a partir de 50 solicitantes su probabilidad de obtener una plaza cae por debajo de lo esperado en un sorteo justo.

En la figura 5 hemos representado el caso $n = 30$. Observamos que el comportamiento es cualitativamente muy similar al de la figura anterior, aunque con mayores fluctuaciones, por ejemplo, en los apellidos que comienzan por CI.

Los cuadros 1 y 2 reflejan la probabilidad de obtener una plaza de aquellos cuyo apellido comience por las parejas de iniciales más beneficiadas y perjudicadas en cada caso, en el primer cuadro cuando se adjudican 10 plazas y en la segunda cuando se adjudican 20.

Cuadro 1: Parejas de iniciales con menor y mayor probabilidad de obtener una plaza ($n = 10$).

N	15	20	25	30	35	40	45	50	55	60	65	70
prob. teórica	67 %	50 %	40 %	33 %	29 %	25 %	22 %	20 %	18 %	17 %	15 %	14 %
iniciales mín.	SE	MV	HG	HG	GV	GV	GW	HG	DK	DJ	DJ	MV
probabilidad	56 %	41 %	31 %	23 %	19 %	17 %	15 %	13 %	11 %	9 %	8 %	7 %
iniciales máx.	AJ	AE	AI	AI	AK	AJ	AI	AK	AK	AK	AK	AK
probabilidad	78 %	62 %	53 %	47 %	43 %	40 %	37 %	35 %	34 %	33 %	32 %	32 %

Finalmente, en la figura 6 dejamos fijo el número de plazas ($n = 10$) y variamos de nuevo el número de solicitantes. Para cada número de solicitantes y cada valor de la probabilidad, el color blanco significa que

Cuadro 2: Parejas de iniciales con menor y mayor probabilidad de obtener una plaza ($n = 20$).

N	30	40	50	60	70	80	90	100	110	120	130	140
prob. teórica	67 %	50 %	40 %	33 %	29 %	25 %	22 %	20 %	18 %	17 %	15 %	14 %
iniciales mín.	SF	MV	HF	GV	GV	GV	DJ	DJ	DJ	DJ	NB	MV
probabilidad	56 %	41 %	29 %	22 %	19 %	17 %	15 %	12 %	10 %	9 %	8 %	6 %
iniciales máx.	AK	AK	AK	AA	AI	ZZ	AJ	AJ	AK	AK	AK	AK
probabilidad	79 %	62 %	53 %	48 %	43 %	39 %	37 %	35 %	34 %	33 %	33 %	32 %

en un sorteo con esas condiciones nadie tiene esa probabilidad de obtener plaza. El color negro significa que toda la población tiene esa probabilidad (es lo que sucede con 10 solicitantes: toda la población tiene probabilidad 1). Finalmente, los colores intermedios representan, en escala logarítmica, la fracción de la población que tiene esa probabilidad de obtener una plaza. En este caso se ha representado con línea discontinua verde la probabilidad deseada.

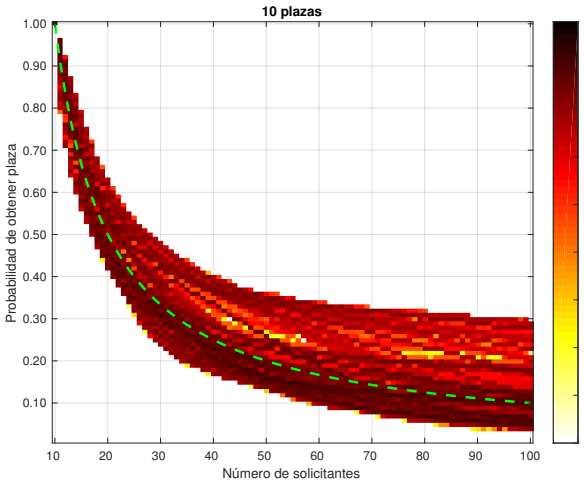

Figura 6: Diez plazas

3.1. Análisis de los resultados

Únicamente hemos mostrado una serie de ejemplos en las figuras y los cuadros, pero estos son suficientes para extraer las conclusiones que buscábamos.

Podemos concluir, en primer lugar, que, fijados el número de plazas y el de solicitantes, el sorteo no es justo, pues la probabilidad de obtener una plaza no es la misma para todos los solicitantes, sino que depende de su apellido. Además, como se puede ver en los cuadros 1 y 2, así como en las figuras 4 y 5, estas desigualdades no son anecdóticas, sino que las diferencias entre los beneficiados y los perjudicados son muy significativas.

En el caso $n = 10$ vemos que, cuando el número de solicitantes es 15, ya hay apellidos con 22 puntos porcentuales más de probabilidad de obtener una plaza que otros y, si el número de solicitantes es 30, hay personas cuya probabilidad de obtener plaza es el doble que la de otras.

Lo mismo sucede si el número de plazas ofertadas es 20, pues con 30 solicitantes una persona cuyo apellido comience por AK tiene 23 puntos porcentuales más de probabilidad de obtener una plaza que otra cuyo apellido comience por SF. Si el número de solicitantes es superior a 60, vuelve a haber apellidos con más del doble de probabilidad de obtener una plaza que otros. La existencia de estos casos tan desiguales es suficiente para replantearse el uso de este tipo de sorteos.

Es interesante comprobar que estas desigualdades no son un caso particular, sino que se mantienen para diferentes valores de n y N. Es lo que podemos observar en el comportamiento suave de las figuras 4 y 5 y en las similitudes entre ellas. Notamos también que, cuando la proporción entre plazas y solicitudes es la misma, los resultados obtenidos para cada pareja de letras son muy similares, con algunas fluctuaciones. Esta apreciación se pone de manifiesto tanto en las figuras 1 y 2 como en las figuras 4 y 5.

Aunque por cuestiones de espacio no hemos podido incluir el resto de iniciales ni más valores para n y N, hemos estudiado otros casos y en todos ellos se observan comportamientos similares a los descritos. Hemos estudiado el comportamiento global de la población en la figura 6 y lo que se observa concuerda con lo descrito anteriormente. En un sorteo justo toda la población debería tener la probabilidad deseada y, sin embargo, vemos cómo hay una franja de probabilidades por encima y por debajo que no es anecdótica. Esto significa que hay personas que (por su apellido) siempre se ven perjudicadas en este tipo de sorteos, independientemente del número de plazas y de solicitantes.

3.2. Dependencia geográfica de los resultados

Hasta ahora hemos analizado la dependencia respecto al número de plazas y de solicitantes, pero para conocer la probabilidad real en un caso concreto también habría que tener en cuenta la población que se considera a la hora de obtener los datos de las frecuencias de los diferentes apellidos.

Unos apellidos son más comunes en unas regiones que en otras, y tiene interés por sí mismo el analizar cómo repercute esto en este tipo de sorteos. Como ejemplo, repetiremos el mismo experimento tomando como poblaciones los habitantes de Castilla y León y el País Vasco respectivamente.

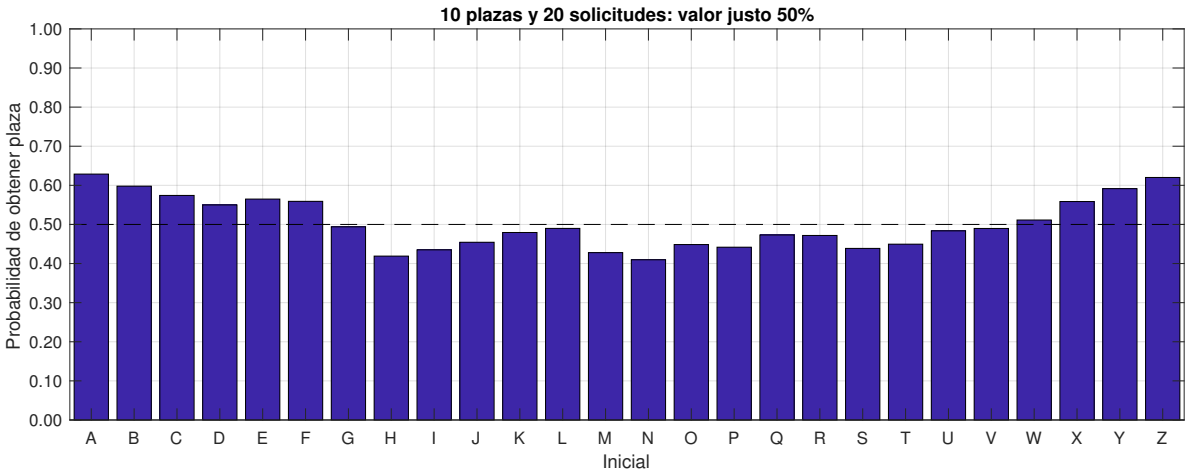

Figura 7: Probabilidad para cada inicial ($n = 10$, $N = 20$, Castilla y León).

En las figuras 7 y 8 representamos la probabilidad de obtener una plaza en un sorteo con 10 plazas y 20 solicitantes con un apellido que comience por cada una de las letras del abecedario, obtenida tras calcular la probabilidad para cada pareja de letras y luego ponderar su peso, tal como hemos hecho anteriormente en la figura 1.

Observamos que existen diferencias entre ambas gráficas y también respecto al caso estatal, con iniciales que en un caso se ven perjudicadas y en otro beneficiadas y viceversa. Comprobamos también lo que venimos recalcando en todo este estudio, y es que existen diferencias significativas entre unas iniciales y otras. Observamos que las diferencias entre comunidades son menores que las diferencias que existen entre unas letras y otras, y que en general se mantiene la forma cualitativa de las gráficas.

Recalcamos que, aunque únicamente mostremos el caso $n = 10, N = 20$, las mismas conclusiones se deducen del resto de casos, salvo alguna excepción anecdótica. Por ejemplo, al disminuir la proporción entre plazas y solicitudes tanto a nivel estatal como en Castilla y León, aquellos cuyo apellido comienza por B van perdiendo poco a poco su ventaja respecto a otros apellidos, pero incluso con una proporción

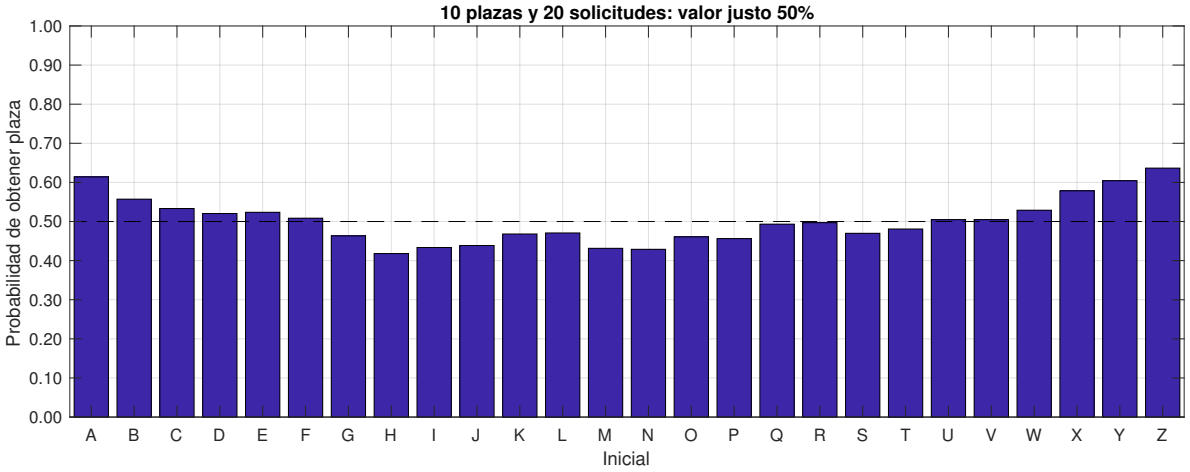

Figura 8: Probabilidad para cada inicial ($n = 10$, $N = 20$, País Vasco).

de solicitudes respecto a las plazas de 10 a 1 todavía siguen siendo beneficiados. Esta caída es mucho más rápida en el País Vasco, donde con una proporción de 6 a 1 los apellidos que comienzan por B ya pasan a verse perjudicados.

Este tipo de diferencias pueden observarse mejor en las figuras 9 y 10, en las que analizamos la evolución de parejas de letras concretas en un sorteo con 10 plazas cuando incrementamos el número de solicitudes.

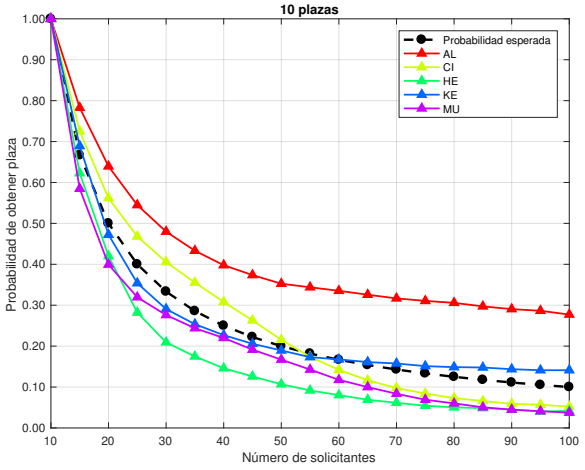

Figura 9: Diez plazas (Castilla y León).

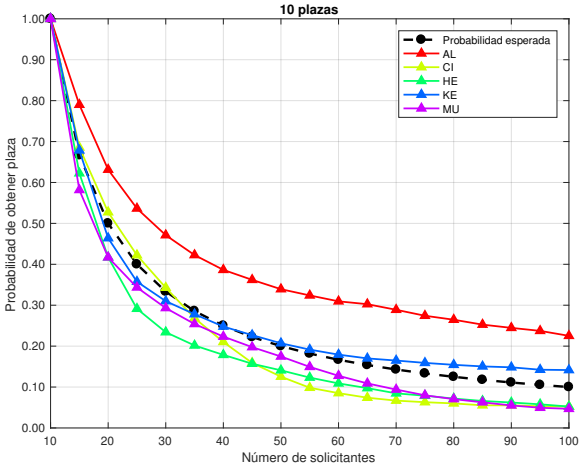

Figura 10: Diez plazas (País Vasco).

Las cinco parejas de letras escogidas a nivel estatal representan bastante bien lo que sucede al comparar diferentes regiones. Vemos que, a grandes rasgos, los resultados son similares, pero existen algunas particularidades específicas. Los apellidos que comienzan por CI se ven ampliamente beneficiados en Castilla y León cuando hay pocos solicitantes; no obstante, esta ventaja es menor y casi inexistente en el País Vasco, donde a su vez la desventaja de los apellidos que comienzan por HE es menos pronunciada. Esto es lo que veríamos comparando el resto de parejas de letras, la mayoría siguen la misma tendencia que a nivel estatal pero con algunas diferencias locales.

Análogamente a la figura 6, representamos la distribución de la población en las diferentes probabilidades en las figuras figuras 11 y 12. Vemos que el resultado es similar en ambas, con diferencias ligeramente más pequeñas en el País Vasco.

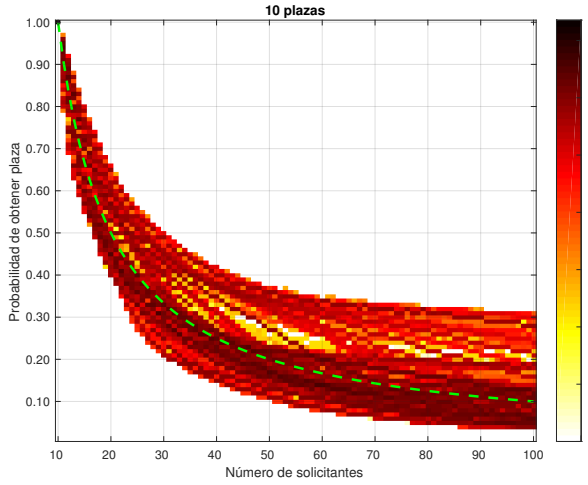

Figura 11: Diez plazas (Castilla y León).

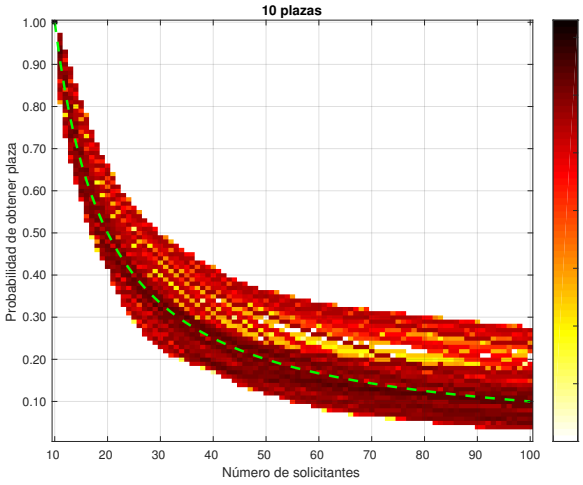

Figura 12: Diez plazas (País Vasco).

El método de sorteo es injusto independientemente de la región, y no se esperan mayores diferencias en otras comunidades autónomas a las ya estudiadas.

4. Propuesta alternativa de sorteo

Nuestro objetivo es encontrar una forma de seleccionar n candidatos de un conjunto de N con la que cada uno de ellos individualmente tenga una probabilidad de n/N de ser escogido.

Para ello lo más natural sería ordenar a los candidatos (por ejemplo, por orden alfabético) y escoger uniformemente al azar un entero $m \xleftarrow{\$} [1, N]$. Entonces asignaríamos plazas a los candidatos $m, m+1, \ldots, m+(n-1) \mod N$. Es inmediato comprobar que para cualquier candidato la probabilidad de obtener plaza es exactamente n/N.

Esto nos lleva a preguntarnos por qué no se utiliza directamente este método en lugar del actual. Una de las razones esgrimidas por la administración es que el sorteo ha de ser justo pero también fácil de publicar y de ser reutilizado en múltiples casos. Según su argumento, una pareja de letras `XY` publicada en el boletín oficial de la comunidad autónoma les sirve para asignar plazas en diferentes centros, mientras que con el método natural sería necesario realizar un sorteo específico para cada centro, dada la dependencia con N, que será diferente en cada caso.

Se trata de un argumento falaz, porque es posible diseñar un sistema que sea a la vez sencillo de auditar y que otorgue la misma probabilidad de obtener plaza a todos los solicitantes. Si pensamos desde el punto de vista de una implementación informática, requeriríamos un generador de números pseudoaleatorios que tome como entrada una N y produzca como salida un entero módulo N de forma uniformemente aleatoria. Lo único que sería necesario publicar en el boletín oficial de la comunidad autónoma sería la descripción del generador utilizado y una semilla (el estado interno del generador, que una vez especificado lo transforma en una función determinista).

Habitualmente, un generador de números pseudoaleatorios produce como salida un entero en un intervalo $[1, RAND\_MAX]$ (dependiendo de la implementación, el intervalo puede comenzar en el 0, pero se trata de casos equivalentes). Si escogemos uniformemente un entero de ese intervalo y nos quedamos con él, módulo N, esto no garantiza que la distribución sea equiprobable. Si $RAND\_MAX$ no es un múltiplo de N lo podemos escribir como $RAND\_MAX = cN + r$, con $c = \lfloor RAND\_MAX/N \rfloor$ y $r = RAND\_MAX - N\lfloor RAND\_MAX/N \rfloor$. Los enteros $m \in [1, r]$ tendrán una probabilidad $(c+1)/(RAND\_MAX)$, mientras que los enteros $m \in [r+1, N]$ tendrán únicamente una probabilidad $c/(RAND\_MAX)$.

Si $RAND\_MAX$ es suficientemente grande podemos hacer este error tan pequeño como queramos. Si no es suficiente tolerar pequeños errores sino que queremos que exactamente todo el mundo tenga la misma probabilidad, entonces la estrategia más común sería forzar que $RAND\_MAX$ fuera un múltiplo de N.

Habitualmente esto se consigue ejecutando el generador de números pseudoaletorios y aceptando la salida únicamente si pertenece a un intervalo que sí sea múltiplo de N, por ejemplo $[1, cN]$. Esto nos lleva a descartar las salidas $m \in [cN + 1, RAND\_MAX]$. Si rechazamos la salida, volvemos a ejecutar el generador hasta obtener un número en $[1, cN]$, lo que garantiza que al hacer módulo N todos los resultados tengan la misma probabilidad. Se trata de un compromiso entre el error que estamos dispuestos a asumir y el número de ejecuciones del generador que podamos utilizar (la probabilidad de que en la i-ésima ejecución no hayamos obtenido una salida válida decae exponencialmente en i).

Nos encontramos ahora con que estos descartes que nos vemos obligados a realizar para obtener una salida realmente equiprobable dependen nuevamente de N. Una primera aproximación sería forzar que el *RAND_MAX* efectivo después de hacer los rechazos sea ahora un múltiplo del mínimo común múltiplo entre $1, 2, \ldots, N\_MAX$, donde N_MAX sea una cota al número máximo de solicitantes que esperamos. De esta forma, al hacer módulo por cualquier natural menor que N_MAX tendríamos una distribución equiprobable. Esto no es implementable, puesto que la sucesión de mcm $(1, 2, 3, ..., n)$ crece demasiado rápido como para que sea práctico utilizarlos, tal como se puede comprobar en *La Enciclopedia On-Line de las Secuencias de Números Enteros* (OEIS, por sus siglas en inglés) [5].

La solución más sencilla sería, entonces, publicar únicamente la semilla que se va a utilizar con el generador de números pseudoaleatorios y, en cada caso, realizar el número de ejecuciones necesarias, tal como se ha explicado, para obtener un entero uniformemente distribuido en $[1, N]$. Como la semilla se ha fijado desde un primer momento, el número de rechazos necesarios es determinista y sigue siendo posible auditar el sorteo.

Esta es una posible implementación de un sorteo que cumpla las condiciones explicitadas en la observación 1, pero podría implementarse de otra forma, siempre que respetara esas condiciones y no acabase discriminando a parte de la población.

5. Conclusiones

Al plantear y mantener este sorteo como criterio de desempate, da la impresión de que los legisladores supusieron que el hecho de que el sorteo sea aleatorio implica que todos los participantes han de tener la misma probabilidad de obtener una plaza. Sin embargo, este estudio demuestra que este no es el caso. Solo con tener unas nociones básicas sobre probabilidad podemos aplicarlas para detectar una situación injusta, en la que, sin pretenderlo, se está discriminando a una parte de la población.

Ante situaciones como esta se pone de manifiesto que, aunque el conjunto de la población no va a tener que utilizar habitualmente contenidos matemáticos de un nivel avanzado, sí que es imprescindible haber adquirido la competencia matemática necesaria para entender problemas como el que aquí se plantea. Por ejemplo, para la mayoría de la población no es necesario conocer los pormenores del teorema central del límite, pero sí tener suficientemente claro el concepto de probabilidad, para no llegar a la conclusión errónea de que el sorteo es justo a partir del hecho de que todas las parejas de letras tienen la misma probabilidad.

Una de las razones por las que posiblemente este tipo de sorteos se mantienen, a pesar de ser injustos, podría ser la dificultad para calcular analíticamente cada una de las probabilidades, debido a la gran cantidad de variables a considerar. Como el resultado depende de la población concreta, del número de plazas y del número de solicitudes, no hay una fórmula sencilla que exprese las probabilidades para poder evidenciar ante las administraciones que el procedimiento es manifiestamente injusto. Sin embargo, aunque no sea fácil obtener una solución analítica al problema, cualquier ordenador personal tiene capacidad para realizar todos los cálculos necesarios, y la estadística nos proporciona las herramientas para asegurar qué nivel de fiabilidad tienen los resultados obtenidos. De esta forma, combinando matemáticas, estadística y la potencia de cálculo de un ordenador, podemos no solo afirmar que este tipo de sorteos discriminan a una parte de la población, sino también cuantificar las diferencias que se producen.

Referencias

[1] Gobierno del Principado de Asturias. «RESOLUCIÓN de 19 de febrero de 2014, de la Consejería de Educación, Cultura y Deporte, por la que se aprueba el procedimiento de admisión del alumnado en centros docentes no universitarios públicos y privados concertados del Principado de Asturias». En: *Boletín Oficial del Principado de Asturias* 46 (25 de feb. de 2014), págs. 1-19. issn: 1579-4180. url: https://sede.asturias.es/bopa/2014/02/25/2014-03363.pdf.

[2] Instituto Nacional de Estadística. *Estadística del Padrón Continuo a fecha 01/01/2016*. 2016.

[3] Junta de Castilla y León. «RESOLUCIÓN de 15 de enero de 2016, de la Dirección General de Política Educativa Escolar, por la que se concreta la gestión del proceso de admisión del alumnado en los centros docentes de Castilla y León para cursar en 2016-2017 enseñanzas sostenidas con fondos públicos de segundo ciclo de Educación Infantil, Educación Primaria, Educación Secundaria Obligatoria o Bachillerato». En: *Boletín Oficial de Castilla y León* 16 (26 de ene. de 2016), págs. 4962-4981. issn: 1989-8959. url: http://bocyl.jcyl.es/html/2016/01/26/html/BOCYL-D-26012016-13.do.

[4] Murcia, Joseángel. «¿Por qué el sorteo por letra es el más injusto?» En: *Verne* (2016). url: http://verne.elpais.com/verne/2015/12/21/articulo/1450708343_196121.html.

[5] OEIS Foundation Inc. *A003418. Least common multiple (or LCM) of {1, 2, ..., n} for n >= 1, a(0) = 1*. En: *The On-Line Encyclopedia of Integer Sequences*. url: http://oeis.org/A003418.

[6] Pérez Porcel, José Antonio. «¿Son justos los sorteos de tribunales basados en las letras de los apellidos?» En: *SUMA, revista para la enseñanza y el aprendizaje de las matemáticas* 50 (nov. de 2005), págs. 65-68. url: http://revistasuma.es/revistas/50-noviembre-2005/son-justos-los-sorteos-de.html.

[7] Ríos, Sixto. *Métodos Estadísticos*. Ediciones del Castillo, 1977. isbn: 978-84-219-0154-0.

[8] Simón, Federico y González Olaya, Vicente. «El teatro de la Zarzuela reconoce que el sorteo para adjudicar los abonos de la ópera es injusto». En: *El País* (1 de dic. de 1993). url: http://elpais.com/diario/1993/12/01/madrid/754748666_850215.html.

TEMat

El duodécimo problema de Hilbert para cuerpos cuadráticos imaginarios

Daniel Gil Muñoz[a]
Universitat Politècnica de Catalunya (UPC)
daniel_gilmu@hotmail.com

Resumen: En este artículo se presentan los conceptos y herramientas más básicas para presentar una demostración debida a Deuring de la resolución del caso cuadrático-imaginario del duodécimo problema de Hilbert, que consiste en calcular explícitamente la extensión abeliana maximal de un cuerpo cuadrático imaginario.

Presentamos el teorema de Kronecker-Weber para resolver el caso ciclotómico. Mediante la introducción de la teoría de cuerpos de clases, utilizamos la misma idea del caso ciclotómico para reducir el caso cuadrático-imaginario a describir explícitamente todos los cuerpos de clases radiales del cuerpo cuadrático imaginario. Introducimos la teoría de curvas elípticas con multiplicación compleja para resolver esta nueva formulación del problema y vemos un ejemplo de cálculo.

Abstract: In this article we present the main notions and basic tools to solve the imaginary-quadratic case of Hilbert's 12th problem. This problem consists in computing explicitly the maximal abelian extension of an imaginary quadratic field.

We present Kronecker-Weber's theorem to solve the cyclotomic case. Next, we introduce class field theory and we use it to adapt the idea of the cyclotomic case in order to reduce the imaginary-quadratic case to describe explicitely all Ray class fields of the imaginary quadratic field. We introduce the theory of elliptic curves with complex multiplication to solve this new formulation and we see an example of computation.

Palabras clave: cuerpo cuadrático imaginario, curva elíptica, multiplicación compleja, cuerpo de clases radiales, extensión abeliana maximal, j-invariante.

MSC2010: 11G45, 14K22.

Recibido: 18 de noviembre de 2017.
Aceptado: 3 de febrero de 2018.

Agradecimientos: El contenido de este artículo es un resumen de mi Trabajo Final de Máster para el Máster de Matemática Avanzada de la Universidad de Barcelona. Quiero agradecer a mi tutor del trabajo, Xavier Guitart Morales, por la propuesta del tema así como su dedicación e interés en la tutorización del trabajo, además de todas sus explicaciones y esfuerzo por enseñarme y hacerme comprender esta teoría.

Referencia: Gil Muñoz, Daniel. «El duodécimo problema de Hilbert para cuerpos cuadráticos imaginarios». En: *TEMat*, 2 (2018), págs. 15-30. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p15/.

[a] El autor estaba afiliado a la Universidad de Barcelona (UB) cuando realizó este trabajo.

1. Introducción

En 1900, Hilbert propuso veintitrés problemas de diferentes áreas de las matemáticas que no habían sido resueltos hasta ese momento y que influirían de manera notable en el desarrollo de las matemáticas del siglo xx. La mayoría de ellos fueron resueltos posteriormente, mientras que algunos continúan hoy sin resolver (véase el libro de Schappacher [10]). En este artículo vamos a ver uno de los problemas del segundo grupo, que es el número doce: el duodécimo problema de Hilbert, también conocido como *Jugendtraum* de Kronecker (sueño de juventud de Kronecker en alemán). Para más información histórica del problema, consúltense el libro de Vladut [13] y las notas de Breiding y Samart [1].

El enunciado del duodécimo problema de Hilbert es el siguiente:

Problema 1 (Duodécimo problema de Hilbert). Sea K un cuerpo numérico. Determinar explícitamente los elementos de un sistema de generadores de la extensión abeliana maximal K^{ab} de K. ◂

Lo primero que vamos a hacer es entender este enunciado. Para ello, vamos a dar algunas pinceladas de la teoría de Galois (si el lector la conoce, se puede saltar esta parte; si, por el contrario, desea conocerla con mayor profundidad de lo aquí mostrado, puede consultar el capítulo V del libro de Hungerford [4] o las notas de Milne [8]).

Sean K y L dos cuerpos de forma que $K \subset L$. Decimos entonces que L es una extensión de K o que L/K es una **extensión de cuerpos**. Nótese que L se puede ver como un espacio vectorial con escalares en K en el que la operación externa es el producto en L. Este espacio se llama el K-espacio vectorial L, y una base de dicho espacio se llama K-base de L. La extensión L/K es finita si el K-espacio vectorial L tiene dimensión finita.

Definición 1. Un **cuerpo numérico** es una extensión finita de $\mathbb{Q}$. ◂

Por ejemplo, el conjunto

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

es un cuerpo numérico: se puede comprobar que tiene estructura de cuerpo y claramente contiene a todos los números racionales. Además $\{1, \sqrt{2}\}$ es una base del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}(\sqrt{2})$, por lo que tal espacio tiene dimensión 2.

El concepto de cuerpo numérico es fundamental en esta teoría. Presentaremos todo lo que necesitamos saber sobre ellos. Sin embargo, el lector interesado en conocer más información puede consultar el capítulo 2 del libro de Marcus [7].

En este ejemplo, la notación $\mathbb{Q}(\sqrt{2})$ significa que se trata del menor subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{Q}$ y $\sqrt{2}$ para la inclusión de conjuntos. Es decir, si L es otro subcuerpo de $\mathbb{C}$ tal que $\mathbb{Q} \subset L$ y $\sqrt{2} \in L$, entonces $\mathbb{Q}(\sqrt{2}) \subset L$.

Más generalmente, si K es un subcuerpo de $\mathbb{C}$ y $x \in \mathbb{C}$, $K(x)$ denota el menor subcuerpo de $\mathbb{C}$ que contiene a K y a x. Esta notación se extiende de manera natural a un subconjunto $S \subset \mathbb{C}$: $K(S)$ es el menor subcuerpo de $\mathbb{C}$ que contiene a K y a S. El conjunto S se llama **sistema de generadores** de la extensión L/K. Partiendo de un sistema de generadores de L/K, podemos obtener una K-base de L.

Definición 2. Sea L/K una extensión de cuerpos. Se define el **grupo de Galois** de L/K como el grupo

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(\alpha) = \alpha \text{ para todo } \alpha \in K\}$$

con la composición de aplicaciones, donde $\mathrm{Aut}(L)$ es el grupo de automorfismos de cuerpos de L. ◂

El grupo de Galois es un objeto fundamental desde el punto de vista de la teoría de Galois. Este grupo se puede describir de una manera más fácil cuando la extensión es de Galois. La definición de extensión de Galois no la vamos a necesitar en este artículo. Todo lo que vamos a necesitar saber de estas extensiones es que nos permiten definir el concepto de extensión abeliana.

Definición 3. Una extensión de cuerpos L/K se dice **abeliana** si es de Galois y $\mathrm{Gal}(L/K)$ es abeliano. ◂

Definición 4. Sea K un subcuerpo de $\mathbb{C}$. Una extensión abeliana L de K se dice **maximal** si para toda extensión abeliana M de K tal que $L \subset M$ se tiene que $L = M$. ◂

La extensión abeliana maximal de un tal subcuerpo K siempre existe, y es única salvo isomorfismo que fije los elementos de K. Así, el duodécimo problema de Hilbert nos propone, dado un cuerpo numérico K, hallar un sistema de generadores de la extensión abeliana maximal de K. Preguntamos además por la forma explícita de tales generadores, es decir, queremos expresarlos en términos de objetos matemáticos conocidos.

Como ya hemos mencionado, el caso general del duodécimo problema de Hilbert permanece sin resolver a día de hoy. Sin embargo, está completamente resuelto para tres casos particulares de K:

1. Cuando K es el propio cuerpo $\mathbb{Q}$ de los números racionales.
2. Cuando K es un cuerpo cuadrático imaginario (es decir, de la forma $K = \mathbb{Q}(\sqrt{-n})$, con n un entero positivo).
3. Cuando K es un cuerpo de multiplicación compleja.

El tercer caso es más complicado y no lo vamos a tratar en este artículo (una demostración se puede encontrar en el artículo de Wei [14]). El objetivo fundamental es probar el segundo caso, es decir, el caso cuadrático-imaginario. Primero veremos la solución para el caso 1 (también conocido como caso ciclotómico; en la siguiente sección veremos por qué) y esto nos permitirá plasmar algunas de las ideas que utilizaremos en el caso 2. Para entender la resolución de este segundo caso, utilizaremos la teoría de cuerpos de clases y la teoría de curvas elípticas con multiplicación compleja.

2. El caso ciclotómico

En esta sección vamos a resolver el duodécimo problema de Hilbert para el primer caso de los listados anteriormente. En este caso, el problema es el siguiente:

Problema 2. Determinar explícitamente un sistema de generadores de la extensión abeliana maximal $\mathbb{Q}^{\mathrm{ab}}$ de $\mathbb{Q}$. ◂

La resolución de este problema pasa por el estudio de las extensiones ciclotómicas de $\mathbb{Q}$ (de ahí que este problema sea nombrado como el caso ciclotómico del duodécimo problema de Hilbert).

Sea $m \in \mathbb{Z}_{>0}$. El conjunto de las raíces complejas m-ésimas de la unidad (es decir, las raíces del polinomio $X^m - 1$ en $\mathbb{C}$) es

$$\{e^{\frac{2\pi i k}{m}} \mid k \in \{0, \dots, m-1\}\}.$$

Si consideramos el producto de números complejos, este conjunto tiene estructura de grupo cíclico (es decir, está generado por un solo elemento). Cualquier generador de dicho grupo es llamado **raíz m-ésima primitiva de la unidad**. Usando teoría de grupos básica (véase el libro de Hungerford [4, capítulo I, teorema 3.6]), se puede ver fácilmente que el conjunto de tales raíces es

$$\{e^{\frac{2\pi i k}{m}} \mid k \in \{0, \dots, m-1\},\ \mathrm{mcd}(k, m) = 1\},$$

donde $\mathrm{mcd}(k, m)$ denota el máximo común divisor de k y m.

Definición 5. Sea $m \in \mathbb{Z}_{>0}$. La m-ésima extensión ciclotómica de $\mathbb{Q}$ se define como

$$K = \mathbb{Q}(e^{\frac{2\pi i}{m}}).$$ ◂

Como primer apunte, una extensión ciclotómica K de $\mathbb{Q}$ es un cuerpo numérico. En efecto, es un cuerpo que, por definición, contiene a $\mathbb{Q}$, y el conjunto de las raíces m-ésimas primitivas de la unidad es una base de K como $\mathbb{Q}$-espacio vectorial (esto se puede deducir, por ejemplo, del libro de Marcus [7, teorema 3]).

Cualquier extensión ciclotómica de $\mathbb{Q}$ es de Galois (véase la proposición 5.8 de Milne [8]). Otra propiedad que tiene la extensión ciclotómica m-ésima es que se puede expresar como $K = \mathbb{Q}(\xi)$, donde ξ es *cualquier* raíz m-ésima primitiva de la unidad. Esto hace que la aplicación

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \\ \overline{k} & \longmapsto & \xi \mapsto \xi^k \end{array}$$

sea un isomorfismo de grupos, donde $(\mathbb{Z}/m\mathbb{Z})^*$ denota al grupo de los enteros módulos m invertibles para el producto (es decir, los de la forma $\overline{k}$ con $k \in \mathbb{Z}$ coprimo con m). Esta aplicación se llama **aplicación de Artin** de la extensión ciclotómica. Así, como el grupo $(\mathbb{Z}/m\mathbb{Z})^*$ es claramente abeliano y es isomorfo al grupo de Galois de $\mathbb{Q}(\xi)/\mathbb{Q}$, concluimos que $\mathbb{Q}(\xi)$ es una extensión abeliana de $\mathbb{Q}$.

Así, hemos probado que cualquier extensión ciclotómica de $\mathbb{Q}$ es una extensión abeliana de $\mathbb{Q}$. De hecho, se tiene un resultado mucho más potente:

Teorema 1 (teorema de Kronecker-Weber). *Cualquier extensión abeliana y finita de $\mathbb{Q}$ está contenida en una extensión ciclotómica.*

Este resultado es muy conocido en teoría de números y se puede probar usando teoría de cuerpos de clases, que introduciremos en la siguiente sección, aunque no veremos la demostración. El lector puede consultar una demostración usando este enfoque en el libro de Cox [2, teorema 8.8]. También es posible probarlo usando técnicas de teoría algebraica de números [7, capítulo 4, ejercicios 29-36].

El teorema de Kronecker-Weber nos permite resolver el duodécimo problema de Hilbert para el caso que tratamos. Para entender cómo, debemos introducir un concepto más de teoría de Galois. Dados dos subcuerpos K y F de $\mathbb{C}$, en general su unión $K \cup F$ *no* es un cuerpo. Pero no hay ningún problema en considerar el menor subcuerpo de $\mathbb{C}$ (de nuevo para la inclusión) que contiene a ambos. Este cuerpo se llama la **composición** de K y F, y se denota por $K \vee F$. De manera completamente análoga se define la composición de una cantidad arbitraria de subcuerpos de $\mathbb{C}$. Claramente, si $F \subset K$, $K \vee F = K$.

La clave en el problema que nos compete es que la composición de extensiones abelianas de un mismo cuerpo es de nuevo abeliana (pues hay un monomorfismo de grupos del grupo de Galois de la composición en el producto directo de los grupos de Galois de cada extensión). Por tanto, la extensión abeliana maximal de $\mathbb{Q}$ se puede escribir como la composición de *todas* las extensiones abelianas de $\mathbb{Q}$. En particular, esto prueba que la extensión abeliana maximal de $\mathbb{Q}$ existe y es única salvo $\mathbb{Q}$-isomorfismo, y el mismo razonamiento sirve si sustituimos $\mathbb{Q}$ por cualquier subcuerpo K de $\mathbb{C}$.

Ahora bien, la composición de cuerpos, tal y como la hemos definido, es claramente conmutativa y asociativa. Usando el teorema de Kronecker-Weber y que las extensiones ciclotómicas son abelianas, podemos reordenar los cuerpos de la expresión de $\mathbb{Q}^{\text{ab}}$ de forma que agrupemos los que están contenidos en la misma extensión ciclotómica. Así, $\mathbb{Q}^{\text{ab}}$ es de hecho la composición de todas las extensiones ciclotómicas de $\mathbb{Q}$, es decir,

$$\mathbb{Q}^{\text{ab}} = \vee_{m \in \mathbb{Z}_{>0}} \mathbb{Q}(\xi_m),$$

donde ξ_m es una raíz m-ésima de la unidad.

Queda, pues, determinar el menor cuerpo que contiene a todas las extensiones ciclotómicas de $\mathbb{Q}$. Lo único que tenemos que hacer es reunir los generadores de todas ellas. Es decir,

$$\mathbb{Q}^{\text{ab}} = \mathbb{Q}(\mu),$$

donde μ es el conjunto de *todas* las raíces de la unidad. Este conjunto es, por tanto, un sistema de generadores de $\mathbb{Q}^{\text{ab}}/\mathbb{Q}$. Esto resuelve el primer caso.

3. Teoría de cuerpos de clases

Para resolver el caso cuadrático-imaginario del duodécimo problema de Hilbert, la teoría de cuerpos de clases será una herramienta crucial. En esta sección veremos la formulación clásica de esta teoría, que se encarga del estudio del grupo de Galois de las extensiones abelianas de un cuerpo numérico K fijado usando la *aritmética de K* (más adelante veremos qué significa esto último). Como los contenidos expuestos a continuación son de un elevado nivel técnico, no los vamos a presentar minuciosamente en este artículo, sino que daremos algunas pinceladas para facilitar su comprensión. Para conocer los detalles se recomienda al lector consultar el libro de Cox [2, capítulo 2, sección 8].

Antes de empezar, necesitamos dos conceptos básicos en teoría algebraica de números.

Definición 6. Un **entero algebraico** es cualquier raíz de un polinomio mónico con coeficientes enteros. ◂

Definición 7. Sea K un cuerpo numérico. Se define el **anillo numérico** $\mathcal{O}_K$ asociado a K como el conjunto de los enteros algebraicos de dicho cuerpo numérico. ◂

El anillo numérico de un cuerpo numérico K, como su propio nombre indica, tiene estructura de anillo. Más aún, se trata de un dominio de integridad (un anillo conmutativo y unitario sin divisores de cero), por lo que podemos considerar su cuerpo de fracciones. Resulta que K es isomorfo al cuerpo de fracciones de su anillo numérico $\mathcal{O}_K$, por lo que no puede haber dos cuerpos numéricos que tengan el mismo anillo numérico asociado.

También necesitaremos el concepto de ideal fraccionario del anillo de enteros.

Definición 8. Sea K un cuerpo numérico. Se define un **ideal fraccionario** de $\mathcal{O}_K$ como un subconjunto $\mathfrak{a} \subset K$ de la forma

$$\mathfrak{a} = \alpha\, I,$$

donde $\alpha \in K$ e I es un ideal de $\mathcal{O}_K$. ◂

El nombre de ideal fraccionario se debe a que K es isomorfo al cuerpo de fracciones de $\mathcal{O}_K$. Con esta definición, cuando a un ideal de $\mathcal{O}_K$ le multiplicamos un elemento de su cuerpo de fracciones, que es K, obtenemos un ideal fraccionario. De hecho, esta definición se puede hacer más general tomando cualquier dominio de integridad y su cuerpo de fracciones.

Un apunte importante es que es que el conjunto I_K de los ideales fraccionarios tiene estructura de grupo cuando consideramos el producto natural $(\alpha\, I)\,(\beta\, J) = (\alpha\ \beta)\,(I\, J)$ de ideales fraccionarios.

La teoría de cuerpos de clases se puede formular para un cuerpo numérico K general, pero nosotros tomaremos un cuerpo cuadrático imaginario. El motivo es que es todo lo que necesitamos para resolver el segundo caso del duodécimo problema de Hilbert, y la teoría además en este caso presenta algunas simplificaciones. Por tanto, de aquí en adelante *K siempre denotará un cuerpo cuadrático imaginario.*

El primer concepto que vamos a introducir es el de subgrupo de congruencia para un ideal $\mathfrak{m}$ de $\mathcal{O}_K$ fijado.

Antes de esto, definimos el conjunto $I_K(\mathfrak{m})$ como el conjunto de los ideales fraccionarios de $\mathcal{O}_K$ coprimos con $\mathfrak{m}$. No vamos a ver la definición rigurosa, pero la idea es que tanto ideales fraccionarios como ideales tienen factorización única como productos de ideales primos de $\mathcal{O}_K$, y son coprimos si no comparten ideales primos en sus factorizaciones (como en el caso de los números enteros coprimos). Tiene estructura de grupo, pues se trata de un subgrupo de I_K.

Un ideal fraccionario $\mathfrak{a} = \alpha\, I$ es **principal** si I es un ideal principal de $\mathcal{O}_K$, es decir, generado por un solo elemento, digamos $I = \langle\beta\rangle$. En tal caso, $\mathfrak{a}$ está generado por $\alpha\ \beta$ como $\mathbb{O}_K$-módulo, es decir, $\mathfrak{a} = \langle\alpha\ \beta\rangle$. Así, dentro de $I_K(\mathfrak{m})$, definimos el grupo $P_{K,1}(\mathfrak{m})$ de los ideales fraccionarios principales $\langle\alpha\rangle$ coprimos con $\mathfrak{m}$ tales que $\alpha - 1 \in \mathfrak{m}$.

Definición 9. Sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$. Se dice que un subgrupo G del grupo I_K de los ideales fraccionarios de $\mathcal{O}_K$ es un **subgrupo de congruencia** para $\mathfrak{m}$ si $P_{K,1}(\mathfrak{m}) \subset G \subset I_K(\mathfrak{m})$. ◂

El siguiente concepto que vamos a introducir es el de símbolo de Artin, pero no lo haremos de manera rigurosa, sino que daremos una idea.

Sea L una extensión abeliana de K. Sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$ divisible por todos los primos de K que ramifican en L. Esta condición se necesita para que la definición de símbolo de Artin que haremos en breves momentos sea correcta, pero no necesitamos saber qué significa. El lector puede encontrar la definición de ramificación en el libro de Marcus [7, capítulo 3, página 71].

Sea $\mathfrak{a} \in I_K(\mathfrak{m})$. El **símbolo de Artin** de L/K sobre $\mathfrak{a}$, denotado por $\left(\frac{L/K}{\mathfrak{a}}\right)$, es un elemento del grupo de Galois $\mathrm{Gal}(L/K)$ de forma que la aplicación

$$\begin{array}{rccc} \Phi_{\mathfrak{m}}\colon & I_K(\mathfrak{m}) & \longrightarrow & \mathrm{Gal}(L/K) \\ & \mathfrak{a} & \longmapsto & \left(\frac{L/K}{\mathfrak{a}}\right) \end{array}$$

sea, en cierto sentido, una generalización de la aplicación de Artin que vimos en el caso ciclotómico. Esta aplicación $\Phi_{\mathfrak{m}}$ se llama **aplicación de Artin** de L/K para $\mathfrak{m}$.

Con los conceptos introducidos hasta ahora, estamos preparados para ver el resultado clave de la teoría de cuerpos de clases.

Teorema 2 (teorema de existencia). *Sea $\mathfrak{m}$ un ideal de O_K y sea G un subgrupo de congruencia para $\mathfrak{m}$. Entonces existe una única extensión abeliana L de K tal que:*

1. *$\mathfrak{m}$ es divisible por todos los primos de K que ramifican en L.*
2. *$G = \mathrm{Ker}(\Phi_{\mathfrak{m}})$, donde $\Phi_{\mathfrak{m}}$ es la aplicación de Artin de L/K para $\mathfrak{m}$.*

La demostración de este teorema está fuera del alcance de este artículo y puede consultarse en el libro de Janusz [5, capítulo v, teorema 9.16]. Nuevamente, el resultado 1 del teorema anterior es una condición necesaria para que la aplicación de Artin $\Phi_{\mathfrak{m}}$ de la extensión L/K para $\mathfrak{m}$ esté bien definida. El resultado 2 nos permite, usando otro resultado llamado teorema de reciprocidad de Artin (Cox [2, teorema 8.5]), establecer un isomorfismo de grupos entre $\mathrm{Gal}(L/K)$ y el grupo cociente $I_K(\mathfrak{m})/\mathrm{Ker}(\Phi_{\mathfrak{m}})$. Esto ilustra la idea de la teoría de cuerpos de clases: hemos logrado determinar la estructura del grupo de Galois de extensiones abelianas de K usando los grupos de ideales fraccionarios de O_K (lo que hemos llamado anteriormente como *aritmética de K*).

Pero más que los resultados 1 y 2 del teorema anterior, lo que nos interesa en este artículo es que, fijados un ideal de O_K y un subgrupo de congruencia para este ideal, existe una única extensión abeliana L de K cuyo grupo de Galois podemos describir en términos del ideal y el subgrupo de congruencia. Esto nos va a permitir introducir un concepto fundamental para nuestros propósitos.

Definición 10. Sea $\mathfrak{m}$ un ideal de O_K. Se define el **cuerpo de clases radiales** de K para $\mathfrak{m}$, denotado por $K_{\mathfrak{m}}$, como la extensión abeliana dada por el teorema anterior cuando tomamos el ideal $\mathfrak{m}$ y el subgrupo de congruencia $G = P_{K,1}(\mathfrak{m})$. ◂

Además, nos va a interesar un caso concreto del cuerpo de clases radiales de K.

Definición 11. Se define el **cuerpo de clases de Hilbert** de K, denotado por H, como el cuerpo de clases radiales de K para el ideal $\mathfrak{m} = O_K$. ◂

La importancia del cuerpo de clases radiales de un cuerpo cuadrático imaginario radica en que juega el papel de las extensiones ciclotómicas en el caso ciclotómico. En efecto, los cuerpos de clases radiales de K son por definición extensiones abelianas de K, y se tiene además el siguiente resultado:

Teorema 3. *Dada una extensión abeliana L de K, existe algún ideal $\mathfrak{m}$ de O_K tal que $L \subset K_{\mathfrak{m}}$.*

Utilizando el mismo razonamiento que en el caso ciclotómico, obtenemos lo siguiente:

Corolario 4. *Sea K un cuerpo cuadrático imaginario. Entonces,*

$$K^{\mathrm{ab}} = \vee_{\mathfrak{m} \triangleleft O_K} K_{\mathfrak{m}}.$$

Y, por tanto, si calculamos un sistema de generadores de $K_{\mathfrak{m}}/K$ para cada ideal $\mathfrak{m}$ de O_K, la unión de todos ellos será un sistema de generadores de K^{ab}. Hemos, pues, *reformulado el problema*: queremos describir explícitamente un sistema de generadores de cada cuerpo de clases radiales $K_{\mathfrak{m}}$ de K.

4. Curvas elípticas y multiplicación compleja

Sin perder de vista nuestro objetivo, que es describir explícitamente todos los cuerpos de clases radiales $K_{\mathfrak{m}}$ de un cuerpo cuadrático imaginario K, hacemos una pausa para introducir la teoría de curvas elípticas y multiplicación compleja. En la introducción comentamos que queremos describir los generadores que vamos a obtener en términos de objetos matemáticos conocidos. Estos objetos se encuadran en la teoría que vamos a introducir en esta sección. La principal referencia utilizada es el libro de Silverman [11].

4.1. Curvas elípticas: definición y propiedades

Una curva elíptica es un caso particular de lo que llamamos curva algebraica plana. La definición de curva algebraica plana es algo elaborada y no la vamos a ver (para una definición rigurosa, véanse los capítulos 1 y 2 del citado libro de Silverman [11]). Se trata, esencialmente, de una abstracción de la idea intuitiva que tenemos de curva en el plano afín $\mathbb{A}^2(\mathbb{R})$, que corresponde al conjunto de puntos de $\mathbb{R}^2$ que pertenecen a dicha curva. La idea es sustituir el cuerpo $\mathbb{R}$ por un cuerpo F. Así, los puntos de una curva algebraica C están en el espacio afín $\mathbb{A}^2(F)$ (tienen sus coordenadas en F) y vendrán dados por una ecuación de la forma

$$C\colon\ g(x,y)=0,$$

donde pedimos que $g \in F[x,y]$ sea un polinomio. Esta ecuación se llama **ecuación afín de la curva** C. Pero debemos, además, admitir que una curva pueda tener (o no) por punto cualquiera de los puntos de la *recta del infinito* del espacio proyectivo $\mathbb{P}^2(\mathbb{R})$. Para poder definir esto, debemos expresar los puntos de la curva con coordenadas proyectivas (u homogéneas), es decir, como elementos de $\mathbb{P}^2(\mathbb{R})$. Esto lo podemos hacer mediante una ecuación

$$C\colon\ G(x_0,x_1,x_2)=0,$$

donde $G \in F[x_0,x_1,x_2]$ es un polinomio homogéneo. Esta ecuación se llama **ecuación proyectiva de la curva** C.

Así, una curva algebraica es esencialmente el conjunto de puntos dados por una ecuación afín o proyectiva. Para pasar de la afín a la proyectiva, hacemos $G(x_0,x_1,x_2) = g(\frac{x_0}{x_1},\frac{x_2}{x_1})$. Este proceso se conoce como *proyectivización*. Por el contrario, para pasar de la proyectiva a la afín, hacemos $g(x,y) = G(x,1,y)$. Este proceso se conoce como *deshomogeneización*.

Definición 12. Sea F un cuerpo con característica distinta de 2 y 3. Una **curva elíptica** E definida sobre F es una curva algebraica con ecuación afín

$$E\colon\ y^2 = 4\,x^3 - g_2\,x - g_3,$$

donde $g_2, g_3 \in F$ y $g_2^3 - 27\,g_3^2 \neq 0$. ◂

El conjunto de puntos de una curva elíptica definida sobre F, denotado por $E(F)$, viene dado por los puntos afines (x,y) con coordenadas en F y un punto en la recta del infinito, con coordenadas homogéneas $[0,1,0]$, que denotamos por ∞ (en adelante llamado **punto del infinito**). El motivo es que si proyectivizamos la ecuación de la curva veremos que el punto del infinito la satisface.

Está bastante claro que una curva elíptica no viene dada por una única ecuación, pues podemos hacer cambios de variables que transformen la ecuación de la definición anterior en otra ecuación de la forma $g(x,y)=0$ con $g \in F[x,y]$. Pero una curva elíptica sí que tiene una única ecuación en la forma de la que aparece en la definición 12, que se llama **ecuación de Weierstrass** de la curva elíptica.

A continuación introducimos el concepto de j-invariante de una curva elíptica, que es un objeto que va a ser fundamental en nuestros propósitos.

Definición 13. Sea E una curva elíptica definida sobre F con ecuación de Weierstrass

$$E\colon\ y^2 = 4\,x^3 - g_2\,x - g_3.$$

Se define el j**-invariante** de E como el número

$$j(E) = 1728\,\frac{g_2^3}{g_2^3 - 27\,g_3^2}.$$ ◂

Nótese que $j(E)$ está bien definido porque, por definición de curva elíptica, $g_2^3 - 27\,g_3^2 \neq 0$.

Sea E una curva elíptica definida sobre un cuerpo F. Podemos definir una operación binaria sobre el conjunto de puntos $E(F)$ de la curva E que lo dota de **estructura de grupo abeliano**. El elemento neutro

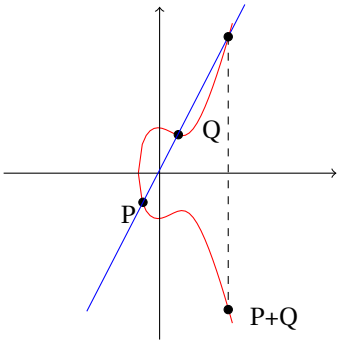

Figura 1: Suma de puntos en una curva elíptica.

de $E(F)$ es el punto del infinito. Para ver como se suman dos puntos, vamos a considerar el caso en que nuestra curva elíptica tiene coeficientes reales. Entonces podemos representarla gráficamente, como en la figura 1.

Para sumar dos puntos P y Q, seguimos el procedimiento indicado en la figura: trazamos la recta que pase por los puntos P y Q, que cortará a la curva elíptica en un tercer punto, y $P+Q$ es el simétrico de este punto respecto del eje horizontal.

Si utilizamos coordenadas afines, podemos calcular las coordenadas de $P+Q$ en función de las coordenadas de P y Q. Estas expresiones son las que utilizamos para definir la suma de puntos de una curva elíptica definida sobre un cuerpo arbitrario (véase el libro de Silverman [11, capítulo 3, sección 2]). Podemos deducir también gráficamente que el opuesto de un punto P de E es el simétrico de P respecto del eje horizontal, y que la suma es conmutativa. Por supuesto, esto no es una demostración general porque no todas las curvas elípticas tienen una representación como la de la figura 1.

4.2. Curvas elípticas con multiplicación compleja

En esta sección vamos a establecer qué significa que una curva elíptica definida sobre el cuerpo $\mathbb{C}$ de los números complejos tenga multiplicación compleja. Esta familia de curvas tienen algunas buenas propiedades que aprovecharemos para llevar a cabo la construcción explícita que buscamos.

Empezaremos esta sección introduciendo el concepto de isogenia. Sean E y E' curvas elípticas definidas sobre un mismo cuerpo F. Un **morfismo de curvas elípticas** $\phi\colon E \longrightarrow E'$ es, esencialmente, una aplicación entre los conjuntos de puntos $\phi\colon E(F) \longrightarrow E'(F)$ tales que, para cada $(x,y) \in E(F)$, las coordenadas de $\phi(x,y)$ vienen dadas por funciones racionales de x e y (o sea, sumas, restas, multiplicaciones y divisiones de x e y). Esto solo sirve como idea y no como definición rigurosa porque tiene algunos problemas técnicos (se puede ver una definición rigurosa y más general en el libro de Silverman [11, pág. 12]). Habitualmente la notación para estos morfismos será $\phi\colon E \longrightarrow E'$, y estaremos entendiendo que hay una aplicación bien definida entre los conjuntos de puntos de E y E'. Una isogenia es un caso particular de morfismo de curvas elípticas.

Definición 14. Sean E y E' curvas elípticas definidas sobre un mismo cuerpo F. Una **isogenia** de E a E' es un morfismo de curvas elípticas $\phi\colon E \longrightarrow E'$ que manda el punto del infinito de E al punto del infinito de E'. ◂

Por ejemplo, si E es una curva elíptica, el morfismo $\phi\colon E \longrightarrow E$ que manda cada punto a sí mismo es una isogenia, porque en particular manda el punto del infinito a sí mismo.

Veamos un ejemplo más interesante. Sea E una curva elíptica definida sobre un cuerpo F de característica 0 y sea $m \in \mathbb{Z}$. Recordemos que $E(F)$ tiene estructura de grupo, por lo que dado $P \in E(F)$, podemos sumar P consigo mismo un número arbitrario de veces. Así, tenemos definido un morfismo de curvas elípticas dado por

$$[m]\colon E(F) \longrightarrow E(F)$$

de forma que, para $P \in E(F)$, $[m](P)$ es la suma de P m veces si m es positivo o la suma de P $-m$ veces si m es negativo. Si $m = 0$, parece lógico convenir que *la suma de P* 0 *veces* es el neutro del grupo, o sea ∞. Por definición de elemento neutro, $[m]$ es una isogenia. La llamaremos **multiplicación por** m.

Definición 15. Sea E una curva elíptica. Se define el anillo de endomorfismos de E como el conjunto

$$\mathrm{End}(E) = \{\phi \colon E \longrightarrow E \mid \phi \text{ es isogenia}\}. \qquad \blacktriangleleft$$

El anillo de endomorfismos de una curva elíptica tiene, en efecto, estructura de anillo con las operaciones

$$(\phi + \psi)(P) \coloneqq \phi(P) + \psi(P),$$
$$(\phi\,\psi)(P) \coloneqq \phi \circ \psi(P).$$

Por ejemplo, los morfimos *multiplicación por m* son endomorfismos de una curva elíptica E.

Definición 16. Sea E una curva elíptica definida sobre $\mathbb{C}$. Decimos que E tiene **multiplicación compleja** si $\mathrm{End}(E)$ tiene más elementos aparte de los morfismos *multiplicación por m*. $\blacktriangleleft$

Para curvas elípticas definidas sobre otros cuerpos no hemos definido qué significa que una curva elíptica tenga multiplicación compleja. Por tanto, cada vez que digamos que una curva elíptica tiene multiplicación compleja obviaremos que está definida sobre $\mathbb{C}$ (o un subcuerpo de $\mathbb{C}$).

Teorema 5. *Sea E una curva elíptica con multiplicación compleja. Entonces, el anillo* $\mathrm{End}(E)$ *de endomorfismos de E es isomorfo a un orden en un cuerpo cuadrático imaginario.*

Un orden en un cuerpo numérico es un subanillo de ese cuerpo numérico que generaliza la noción de anillo numérico. El anillo numérico de un cuerpo numérico es un orden y, además, es el maximal (para la inclusión). Así, si E es una curva elíptica con multiplicación compleja, puede suceder que $\mathrm{End}(E) \cong \mathcal{O}_K$. En tal caso, diremos que E **tiene multiplicación compleja por** $\mathcal{O}_K$. Este tipo de curvas tienen propiedades adicionales y son las que utilizaremos para resolver el caso cuadrático-imaginario.

Sea E una curva elíptica con multiplicación compleja por $\mathcal{O}_K$. Sabemos entonces que $\mathrm{End}(E)$ y $\mathcal{O}_K$ son anillos isomorfos. Resulta que podemos tomar un isomorfismo de anillos

$$[\cdot] \colon \mathcal{O}_K \longrightarrow \mathrm{End}(E)$$

de forma que la imagen de cada número entero $m \in \mathbb{Z}$ (que pertenece a $\mathcal{O}_K$) es el endomorfismo $[m]$ *multiplicación por m*. Se tiene, por tanto, que el isomorfismo $[\cdot]$ generaliza la asignación que acabamos de describir a todo el anillo $\mathcal{O}_K$. Es decir, cada elemento $\alpha \in \mathcal{O}_K$ tiene asociado un endomorfismo $[\alpha]$ de E que se puede ver como la generalización de los morfismos *multiplicación por m*. La aplicación $[\cdot]$ se llama **identificación normalizada** de E.

El grupo de puntos de una curva elíptica en general tiene parte de torsión no trivial. Así, dado $m \in \mathbb{Z}$, podemos considerar el grupo de m-torsión de E,

$$E[m] = \{P \in E(\mathbb{C}) \mid [m](P) = \infty\},$$

que es un subgrupo de $E(\mathbb{C})$. Utilizando la identificación normalizada de E, podemos generalizar esto a un ideal $\mathfrak{m}$ de $\mathcal{O}_K$ cualquiera.

Definición 17. Sea E una curva elíptica con multiplicación compleja por $\mathcal{O}_K$ y sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$. Se define el **grupo de** $\mathfrak{m}$**-torsión** de E como

$$E[\mathfrak{m}] = \{P \in E(\mathbb{C}) \mid [\alpha](P) = \infty \text{ para todo } \alpha \in \mathfrak{m}\}. \qquad \blacktriangleleft$$

Esto será importante para entender la construcción explícita que queremos llevar a cabo.

5. El caso cuadrático imaginario

Con todas las herramientas introducidas, estamos preparados para entender la respuesta al duodécimo problema de Hilbert para el caso cuadrático imaginario. La referencia utilizada en esta sección es el libro de Silverman [12, capítulo II, secciones 1-5]. En este caso el problema es el siguiente:

Problema 3. Sea K un cuerpo cuadrático imaginario. Determinar explícitamente los generadores de la extensión abeliana maximal K^{ab} de K. ◂

Lo que haremos es encontrar primero un sistema de generadores del cuerpo de clases de Hilbert H de K, y utilizaremos este resultado para encontrar un sistema de generadores del cuerpo de clases radiales $K_{\mathfrak{m}}$ de K para cualquier ideal $\mathfrak{m}$. Esto lo haremos usando la teoría de curvas elípticas introducida en la sección anterior.

Primero de todo, vamos a introducir el concepto de isomorfismo para curvas elípticas definidas sobre $\mathbb{C}$.

Definición 18. Un **isomorfismo de curvas elípticas** definidas sobre $\mathbb{C}$ es una isogenia $\phi\colon E \longrightarrow E'$ entre curvas elípticas definidas sobre $\mathbb{C}$ que es biyectiva y cuya inversa es también una isogenia. En tal caso, decimos que E y E' son isomorfas (o $\mathbb{C}$-isomorfas). ◂

Consideremos ahora el conjunto de todas las curvas elípticas con multiplicación compleja por $\mathcal{O}_K$. Definamos sobre este conjunto la relación binaria

$$E \cong E' \iff E \text{ y } E' \text{ son isomorfas.}$$

Esta relación es de equivalencia y divide al conjunto anteriormente mencionado en clases de equivalencia, de modo que las curvas elípticas de cada clase son $\mathbb{C}$-isomorfas entre sí y no lo son con las de ninguna otra clase. Denotamos la clase de equivalencia de una curva elíptica E con multiplicación compleja por $\mathcal{O}_K$ como $[E]$. El conjunto cociente, o sea, el conjunto de todas estas clases, se denota por $\mathcal{ELL}(\mathcal{O}_K)$. Se tiene el siguiente resultado:

Teorema 6. *$\mathcal{ELL}(\mathcal{O}_K)$ es finito.*

La demostración utiliza técnicas de teoría algebraica de números que no hemos visto en este artículo. Lo que se hace es establecer una aplicación biyectiva con el grupo de clases de ideales de $\mathcal{O}_K$, que es finito (véase el libro de Silverman [12, capítulo II, proposición 1.2]).

Se tiene además que el j-invariante es un invariante de la relación de isomorfía de curvas elípticas definidas sobre $\mathbb{C}$. Es decir:

Proposición 7. *Sean E y E' curvas elípticas definidas sobre $\mathbb{C}$. Entonces, E y E' son isomorfas si y solo si $j(E) = j(E')$.*

Lo que este resultado nos dice es que si tomamos una clase $[E] \in \mathcal{ELL}(\mathcal{O}_K)$ de curvas elípticas, entonces todas las curvas elípticas de dicha clase tienen el mismo j-invariante $j(E)$. Además, este valor es distinto de todos los demás j-invariantes de las curvas elípticas de otras clases de $\mathcal{ELL}(\mathcal{O}_K)$.

Combinando los dos resultados anteriores, obtenemos lo siguiente:

Corolario 8. *El conjunto $\{j(E) \mid E \in \mathcal{ELL}(\mathcal{O}_K)\}$ es finito.*

Por tanto, si tomamos $j(E)$ y hacemos variar E por el conjunto de las curvas elípticas con multiplicación compleja por $\mathcal{O}_K$, obtenemos un número finito de valores. Pero, además, se tiene el siguiente resultado.

Proposición 9. *Sean E y E' curvas elípticas con multiplicación compleja por $\mathcal{O}_K$. Entonces $j(E)$ y $j(E')$ son conjugados (es decir, raíces del mismo polinomio irreducible sobre K). Además, si fijamos E, todos los conjugados de $j(E)$ se obtienen de esta forma.*

Dicho de otra forma, obtenemos todos los conjugados de $j(E)$, que son un número finito por el corolario 8. Además, todos ellos pertenecen a $K(j(E))$, pues la extensión $K(j(E))/K$ es de Galois (véase la demostración del teorema 4.3 del capítulo II del libro de Silverman [12]). Pero en realidad podemos decir mucho más.

Teorema 10. *Sea K un cuerpo cuadrático imaginario y sea E una curva elíptica con multiplicación compleja por O_K. Entonces, el cuerpo de clases de Hilbert de K es*

$$H = K(j(E)).$$

En el lenguaje de teoría de Galois, H es el cuerpo de descomposición del polinomio mínimo (o irreducible) de $j(E)$ sobre K.

Vamos a entender la última frase del enunciado. Si L/K es una extensión de cuerpos y $f \in K[X]$ es un polinomio, decimos que L es cuerpo de descomposición de f sobre K si $L = K(S)$, donde S es el conjunto de las raíces de f en L. Así, la última frase del enunciado anterior dice que H se obtiene de adjuntar a K todas las raíces en H del polinomio irreducible de $j(E)$ sobre K. Esto será importante en los ejemplos de cálculo.

Este resultado nos da, pues, un sistema de generadores de H/K. Para demostrarlo hace falta una serie de resultados que utilizan conceptos de los que no hemos hablado aquí y con unas demostraciones muy técnicas, así que omitiremos esta parte. La demostración se puede encontrar en la referencia de Silverman [12, capítulo II, teorema 4.3].

Recuérdese que queremos encontrar un sistema de generadores de $K_{\mathfrak{m}}/K$ para cualquier ideal $\mathfrak{m}$ de O_K. El resultado que resuelve esta cuestión, y el más importante de este artículo, es el siguiente.

Teorema 11 (teorema principal). *Sea K un cuerpo cuadrático imaginario y sea $\mathfrak{m}$ un ideal de O_K. El cuerpo de clases radiales de K para $\mathfrak{m}$ es*

$$K_{\mathfrak{m}} = K(j(E), x(E[\mathfrak{m}])),$$

donde E es una curva elíptica con multiplicación compleja por O_K y definida sobre H, y x es, esencialmente, la función primera coordenada.

La función primera coordenada es aquella que envía un punto (x, y) de la curva elíptica E a su primera coordenada x. Decimos *esencialmente* porque hay un par de casos en los que la función primera coordenada no funciona. Cuando $j(E) = 0$, hay que sustituirla por la función $(x, y) \longmapsto x^3$, y cuando $j(E) = 1728$, hay que sustituirla por $(x, y) \longmapsto x^2$. Combinando el teorema principal con el corolario 4 obtenemos la solución al problema 3.

Corolario 12. *Sea K un cuerpo cuadrático imaginario. Entonces,*

$$K^{\mathrm{ab}} = K(j(E), x(E_{\mathrm{tors}})),$$

donde E es una curva elíptica con multiplicación compleja por O_K y definida sobre H, y x es, esencialmente, la función primera coordenada.

Esto resuelve completamente el caso cuadrático-imaginario del duodécimo problema de Hilbert. La demostración del teorema 11 es también muy técnica y requiere de otros resultados que no vamos a presentar aquí (el lector la puede consultar en la referencia de Silverman [12, capítulo II, teorema 5.6]).

Una posible pregunta es, ¿para qué nos sirve el teorema 10? Si lo que queríamos era saber una expresión explícita de $K_{\mathfrak{m}}$ para cada ideal $\mathfrak{m}$ de O_K, podríamos haberla enunciado sin decir que $K(j(E))$ es el cuerpo de clases de Hilbert de K. Lo que sucede es que este hecho es teóricamente crucial para la demostración del teorema principal. Sin ir más lejos, el saber que $H = K(j(E))$ nos asegura que toda clase de curvas elípticas $[E] \in \mathcal{ELL}(O_K)$ tiene algún representante definido sobre H. Por tanto, existe alguna curva elíptica definida sobre O_K y definida sobre H, que es la que nos sirve para el teorema principal.

6. Ejemplos de cálculo

Ya sabemos, para cada cuerpo cuadrático imaginario K, la expresión explícita de K^{ab}. Pero, si nos dan un cuerpo cuadrático imaginario concreto, ¿cómo calcularíamos K^{ab}? En esta sección vamos a tratar de responder a esta pregunta siguiendo el capítulo 7 del artículo de Kedlaya [6].

6.1. Cuerpo de clases de Hilbert

No tan rápido, primero vamos a tratar de calcular el cuerpo de clases de Hilbert H de K. Por el teorema 10, $H = K(j(E))$, con $E \in \mathcal{ELL}(\mathcal{O}_K)$ definida sobre H. Podemos hallar cómo son todos los elementos de $\mathcal{O}_K$, pero en principio no parece fácil hallar una curva elíptica con multiplicación compleja por $\mathcal{O}_K$ y calcular su j-invariante.

Aún si hubiésemos conseguido calcular una tal curva E y su j-invariante $j(E)$, probablemente lo tendríamos como una expresión decimal aproximada. Pero esto es algebraicamente insuficiente. De poco nos serviría saber, por ejemplo, que $j(E) \approx 1{,}0003$, pues no tendríamos información de la estructura de $K(j(E))$ (más allá de que está generada por $j(E)$). Lo que nos interesa es saber el polinomio irreducible de $j(E)$, pues esto nos permite conocer todos sus conjugados y poder describir algebraicamente $K(j(E))$.

Pero lo que hacemos realmente en la práctica es al revés: calculamos todos los conjugados de $j(E)$ y, una vez sabiendo esto, podemos calcular el polinomio irreducible de $j(E)$ como

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i),$$

donde $\alpha_1, \ldots, \alpha_n$ son los conjugados de $j(E)$. Así, si calculamos f, por el teorema 10, H es el cuerpo de descomposición de f sobre K y habremos acabado.

Calculemos, pues, el polinomio f. Por la proposición 9, los conjugados de $j(E)$ son los elementos del conjunto

$$\{j(E) \mid [E] \in \mathcal{ELL}(\mathcal{O}_K)\}.$$

Así, tenemos que

$$f(X) = \prod_{[E] \in \mathcal{ELL}(\mathcal{O}_K)} (X - j(E)).$$

Por tanto, ahora la pregunta que cabe hacerse es, ¿cómo calculamos $j(E)$ para cada curva elíptica E con multiplicación compleja por $\mathcal{O}_K$? En este punto, introducimos una nueva herramienta que vamos a necesitar: el grupo de clases de ideales de $\mathcal{O}_K$. La idea es la siguiente: definimos en el conjunto de todos los ideales de $\mathcal{O}_K$ la relación

$$I \sim J \iff \text{existe } \alpha \in K \text{ tal que } I = \alpha J.$$

Esta relación es de equivalencia y las clases de equivalencia son las clases de homotecias de ideales de $\mathcal{O}_K$ (es decir, las clases de múltiplos por elementos de K). A la clase de un ideal $\mathfrak{a}$ de $\mathcal{O}_K$ la denotaremos por $\overline{\mathfrak{a}}$.

Definición 19. Se define el **grupo de clases de ideales** de $\mathcal{O}_K$, y se denota por $C(\mathcal{O}_K)$, como el conjunto cociente para la relación de equivalencia anterior. ◂

El grupo de clases de ideales, como su propio nombre indica, tiene estructura de grupo con la operación $\overline{I}\,\overline{J} := \overline{IJ}$. El neutro es la clase del ideal trivial $\mathcal{O}_K$ (también llamada clase trivial), que de hecho es la clase de todos los ideales principales de $\mathcal{O}_K$.

Y, ¿para qué queremos el grupo de clases de ideales? Resulta que *hay una correspondencia biunívoca* entre el grupo de clases de ideales $C(\mathcal{O}_K)$ y el conjunto de clases $\mathcal{ELL}(\mathcal{O}_K)$. Más concretamente:

Proposición 13. *Hay una aplicación biyectiva*

$$\begin{array}{ccc} C(\mathcal{O}_K) & \longrightarrow & \mathcal{ELL}(\mathcal{O}_K) \\ \overline{\mathfrak{a}} & \longmapsto & [E_{\mathfrak{a}}]. \end{array}$$

La demostración se deduce del teorema 10.14 y el ejercicio 14.2 del libro de Cox [2]. Esto nos permite hacer la siguiente definición:

Definición 20. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Definimos el j-invariante de $\mathfrak{a}$ como

$$j(\mathfrak{a}) := j(E_{\mathfrak{a}}).$$ ◂

En otras palabras, el j-invariante de un ideal de O_K es el j-invariante de la clase de curvas elípticas $[E_{\mathfrak{a}}]$ que corresponde a su clase de ideales $\overline{\mathfrak{a}}$. Nótese que esta definición no depende de representantes por la proposición 7.

Combinando la proposición 13 y la definición 20, tenemos que hay una aplicación biyectiva

$$\begin{array}{ccc} C(O_K) & \longrightarrow & j(\mathcal{ELL}(O_K)) \\ \overline{\mathfrak{a}} & \longmapsto & j(E_{\mathfrak{a}}). \end{array}$$

Por tanto, el polinomio f que queríamos calcular se puede escribir como

$$f(X) = \prod_{\overline{\mathfrak{a}} \in C(O_K)} (X - j(\mathfrak{a})).$$

Hemos **trasladado el problema** de calcular las clases de curvas elípticas de $\mathcal{ELL}(O_K)$ a calcular las clases de ideales de $C(O_K)$. Y esto último lo podemos hacer utilizando Sage [9].

Así, el procedimiento a seguir es el siguiente:

1. Calculamos un sistema de representantes de $C(O_K)$ (el conjunto que forman un representante de cada clase).
2. Calculamos el j-invariante de cada ideal del sistema anterior.
3. Calculamos $f(X) = \prod_{\overline{\mathfrak{a}} \in C(O_K)} (X - j(\mathfrak{a}))$.

Veámoslo con un ejemplo concreto. Calculemos el cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-15})$. En Sage ponemos la instrucción

```
K=QuadraticField(-15).
```

Para calcular el grupo de clases de ideales, ponemos la instrucción

```
C=K.class_group().
```

Entonces, C será una lista cuyos elementos son representantes de distintas clases de ideales de $C(O_K)$, justo como queríamos. Así, las instrucciones

```
C[0],
```

```
C[1]
```

tendrán *outputs*

```
Trivial principal fractional ideal class,
```

```
Fractional ideal class (2, 1/2*a - 1/2).
```

El grupo de clases de ideales tiene, pues, dos elementos: la clase trivial y la clase $\overline{\langle 2, \frac{\sqrt{-15}-1}{2} \rangle}$.

Ahora toca calcular los j-invariantes. Por supuesto, Sage nos devolverá valores aproximados de los mismos. En realidad, el j-invariante induce una función analítica, que es la que está implementada en Sage bajo el nombre de *elliptic_j*. En general, se tiene que $j(\langle a, b \rangle) = j(\frac{b}{a})$. Así que para calcular el j-invariante de un ideal en Sage lo que haremos será *dividir el segundo generador por el primero*.

Aquí hacemos un inciso. En general, cuando estemos trabajando con el cuerpo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-n})$, existen dos posibilidades:

- $n \equiv 1, 2 \pmod 4$, en cuyo caso un representante de la clase trivial es $\langle 1, \sqrt{-n}\rangle$.
- $n \equiv 3 \pmod 4$, en cuyo caso un representante de la clase trivial es $\langle 2, 1 + \sqrt{-n}\rangle$.

En nuestro caso se tiene que $15 \equiv 3 \pmod 4$ y, por tanto, estamos en la segunda situación. Así, un representante de la clase trivial es $\mathfrak{a}_1 = \langle 2, 1 + \sqrt{-15}\rangle$. Por tanto, el valor de su j-invariante vendrá dado por la siguiente instrucción:

```
elliptic_j((1+sqrt(-15))/2).
```

Para la otra clase, un representante suyo es $\mathfrak{a}_2 = \langle 2, \frac{\sqrt{-15}-1}{2}\rangle$, y ponemos la instrucción

```
elliptic_j((sqrt(-15)-1)/4).
```

Observando los *outputs*, obtenemos que

$$j(\mathfrak{a}_1) \approx -191657{,}832862547 + 1{,}34213412519219 \cdot 10^{-10}\,\mathrm{i},$$
$$j(\mathfrak{a}_2) \approx 632{,}832862547208 + 1{,}06394370576499 \cdot 10^{-13}\,\mathrm{i}.$$

Por último, calculamos el polinomio $(X - j(\mathfrak{a}_1))(X - j(\mathfrak{a}_2))$. Si llamamos $j1 = j(\mathfrak{a}_1)$ y $j2 = j(\mathfrak{a}_2)$, poniendo como *input*

```
(X-j1)*(X-j2)
```

obtenemos el *output*

```
24 x^2 + (191025.000000000 - 1.34319806889795e-10*I) x
                - 1.21287375000000e8 + 6.45433435433001e-8*I.
```

Aquí podemos usar que el polinomio que buscamos *tiene coeficientes enteros* [12, capítulo II, teorema 6.1], de forma que los coeficientes que obtendremos los podemos aproximar a los números enteros más cercanos. Así, obtenemos que el cuerpo de clases de Hilbert de K es el cuerpo de descomposición de

$$f(x) = x^2 + 191025\,x + 121287375$$

sobre K.

6.2. Cálculo del cuerpo de clases radiales

En virtud del corolario 4, K^{ab} es la composición de todos los cuerpos de clases radiales $K_{\mathfrak{m}}$. En esta sección vamos a ver cómo calcular los cuerpos de clases radiales $K_{N\,O_K}$, donde N es un entero positivo (en realidad, esto es suficiente para poder calcular K^{ab}, pues todos los cuerpos de clases radiales de K están contenidos en alguno de la forma $K_{N\,O_K}$).

Según el teorema 11,

$$K_{N\,O_K} = K(j(E), x(E[N])),$$

donde E es una curva elíptica definida sobre H y con multiplicación compleja por O_K.

Recuérdese que $K(j(E))$ es el cuerpo de clases de Hilbert de K, que ya sabemos calcular. Por tanto, todo lo que tenemos que hacer es añadir al cuerpo de clases de Hilbert las primeras coordenadas de los puntos de N-torsión de E. El cálculo de puntos de torsión de una curva elíptica en general es complicado, pero para este caso podemos utilizar una herramienta adicional: los **polinomios de división** asociados a una curva elíptica. Se trata de una familia de polinomios $\{D_N\}_{N\in\mathbb{Z}_{>0}}$ con coeficientes en el cuerpo de definición de la curva elíptica elegida (véase el ejercicio 3.7 del libro de Silverman [11]). En nuestro caso, el interés de estos polinomios reside en el siguiente resultado.

Teorema 14. *Sea $E \in \mathcal{ELL}(\mathcal{O}_K)$ definida sobre H. Las raíces del N-ésimo polinomio de división D_N de E son las primeras coordenadas de los puntos de $E[N]$.*

Se deduce, por tanto, que $K_{N\,\mathcal{O}_K}$ es el cuerpo de descomposición de D_N sobre H.

El procedimiento a seguir en este caso es:

1. Calcular el polinomio f que define el cuerpo de clases de Hilbert utilizando el procedimiento anterior.
2. Tomar una raíz α de f y calcular una curva elíptica E tal que $j(E) = \alpha$.
3. Calcular el N-ésimo polinomio de división asociado a E.

Trabajemos nuevamente sobre el ejemplo de $K = \mathbb{Q}(\sqrt{-15})$. Vamos a calcular $K_{3\,\mathcal{O}_K}$. Partimos de que tenemos el polinomio f que define el cuerpo de clases de Hilbert de K y que hemos calculado en el ejemplo anterior.

Con la instrucción

```
H.<z> = K.extension(f)
```

estamos definiendo $H = K(z)$, donde z tiene polinomio irreducible f (o sea, H es el cuerpo de clases de Hilbert de K). Expresaremos todos los elementos de H en función de z. A continuación, con la instrucción

```
alpha=f.roots(H)[0][0]
```

definimos `alpha` como una raíz del polinomio f en H; concretamente, la primera de la lista de tales raíces, que tiene el valor de $\alpha = -z + 191025$. Después ponemos la instrucción

```
E=EllipticCurve_from_j(alpha),
```

mediante la cual definimos E como la curva elíptica con ecuación afín

$$y^2 = x^3 + (-578259\,z - 110825787600)\,x + 74550012768\,z + 14288092368961950,$$

cuyo j-invariante es α. Por último, calculamos el tercer polinomio de división asociado a E mediante la instrucción

```
E.division_polynomial(3),
```

que es

$$\begin{aligned} D_3(x) = {} & 3\,x^4 + (-3469554\,z - 664954725600)\,x^2 \\ & + (894600153216\,z + 171457108427543400)\,x \\ & - 64296415660328775\,z - 12322911690611116662375. \end{aligned}$$

Por tanto, $K_{3\,\mathcal{O}_K}$ es el cuerpo de descomposición de D_3 sobre H.

Estamos preparados para responder a la pregunta que nos hicimos al principio de la sección. Para calcular K^{ab}, calcularíamos para cada $N \in \mathbb{Z}_{>0}$ el cuerpo de clases radiales $K_{N\,\mathcal{O}_K}$ mediante el proceso que acabamos de presentar. Si adjuntamos a K las raíces de todos estos polinomios, obtenemos K^{ab}.

Como último comentario, esta manera de proceder justifica también la importancia de calcular el cuerpo de clases de Hilbert de un cuerpo cuadrático imaginario. En la práctica, se puede ver como un paso previo al cálculo de los cuerpos de clases radiales de ese cuerpo cuadrático imaginario.

Referencias

[1] Breiding, Paul y Samart, Detchat. «Kronecker's Jugendtraum». En: (2012). URL: http://www.math.psu.edu/papikian/BreidingSamart.pdf.

[2] Cox, David A. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics. John Wiley & Sons, Inc., 1997. https://doi.org/10.1002/9781118400722.

[3] Gil Muñoz, Daniel. *Explicit class field theory via elliptic curves*. Trabajo final de máster. Universitat de Barcelona, 2017. URL: https://hdl.handle.net/2445/121135.

[4] Hungerford, Thomas W. *Algebra*. 1.ª ed. Graduate Texts in Mathematics 73. Springer-Verlag, 1980. https://doi.org/10.1007/978-1-4612-6101-8.

[5] Janusz, Gerald J. *Algebraic number fields*. Pure and applied mathematics a series of monographs and textbooks 55. Academic Press, 1973. https://doi.org/10.1090/gsm/007.

[6] Kedlaya, Kiran S. *Complex Multiplication and Explicit Class Field Theory*. Tesis doct. Harvard University, 1996. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.49.3926.

[7] Marcus, Daniel A. *Number fields*. Universitext. Springer-Verlag, 1977. https://doi.org/10.1007/978-1-4684-9356-6.

[8] Milne, James S. *Fields and Galois Theory*. (v4.53). 2017. URL: http://www.jmilne.org/math/CourseNotes/ft.html.

[9] The Sage Developers. *SageMath, the Sage Mathematics Software System*. https://doi.org/10.5281/zenodo.593563.

[10] Schappacher, Norbert. «On the history of Hilbert's twelfth problem: a comedy of errors». En: *Matériaux pour l'histoire des mathématiques au XXe siècle - Actes du colloque à la mémoire de Jean Dieudonné*. Séminaires et Congrès 3. Société Mathématique de France, 1998, págs. 243-273.

[11] Silverman, Joseph H. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. Springer-Verlag, 1986. https://doi.org/10.1007/978-0-387-09494-6.

[12] Silverman, Joseph H. *Advanced Topics in the Arithmetic of Elliptic Curves*. 1.ª ed. Graduate Texts in Mathematics 151. Springer-Verlag New York, 1994. https://doi.org/10.1007/978-1-4612-0851-8.

[13] Vladut, Serge G. *Kronecker's Jugendtraum and Modular Functions*. Gordon y Breach Publishers, 1995. ISBN: 978-2-88124-754-5.

[14] Wei, Wafa. «Moduli Fields of CM-Motives Applied to Hilbert's 12th Problem». 1994. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.57.5573.

TEMat

Puntos en figuras convexas: el caso del hexágono regular

Manuel Mellado Cuerno
Universidad Autónoma de Madrid (UAM)
manuel.mellado@estudiante.uam.es

Resumen: Para una figura plana, acotada y con borde F se define el número o función de Soifer de F, $S(F)$, como el mínimo entero m tal que dados m puntos cualesquiera de F al menos tres de ellos forman un triángulo de área menor o igual que un cuarto del área de F.

Cuando F es convexa, la función $S(F)$ solo puede tomar los valores 5 o 6. En este artículo se demuestra que $4 \leq S(F) \leq 6$. Las limitaciones de espacio nos impiden incluir la demostración de que $S(F) \neq 4$, que el lector puede ver en las referencias citadas. Como aportación original, se prueba que si H es un hexágono regular, $S(H) = 5$.

Abstract: For any figure F in a plane, bounded and including its border, we define the Soifer's function or Soifer's number of F, $S(F)$, as the minimum integer m such that given any m points of F at least three of them form a triangle with area less than or equal to a quarter of the area of F.

When F is convex, $S(F)$ can take only the values 5 or 6. In this article, we prove that $4 \leq S(F) \leq 6$. The proof that $S(F) \neq 4$ is omitted for brevity, but can be found in the references. As an original result, we prove that $S(H) = 5$ when H is a regular hexagon.

Palabras clave: figuras convexas, geometría descriptiva, triángulos.

MSC2010: 52A10, 97G80.

Recibido: 1 de agosto de 2017.
Aceptado: 13 de febrero de 2018.

Agradecimientos: Quería agradecer todo su trabajo, dedicación y apoyo al profesor Eugenio Hernández, sin el cual la idea de este artículo no habría salido a la luz. Gracias por su paciencia y ganas de ir a más cuando quedarse en lo cercano era lo fácil. Gracias Inés.

Referencia: Mellado Cuerno, Manuel. «Puntos en figuras convexas: el caso del hexágono regular». En: *TEMat*, 2 (2018), págs. 31-44. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p31/.

1. Introducción

En esta sección introduciremos los conceptos necesarios para entender este artículo y expondremos una herramienta básica que se usará a lo largo de todo el trabajo.

Notación. Entendemos por figura plana y acotada F una región del plano limitada por una curva cerrada y continua. Consideramos el borde como dicha curva cerrada.

Para una figura plana y acotada F, denotamos por $|F|$ su área. Todas las figuras en este trabajo incluirán su borde.

Una figura plana F es **convexa** si, dados dos puntos cualesquiera de F, el segmento que los une está incluido en F. ◂

Definición 1. Dada una figura plana y acotada F, el **número de Soifer** de F, $S(F)$, es el mínimo entero m tal que dados m puntos cualesquiera de F al menos tres de ellos forman un triángulo de área menor o igual que $|F|/4$. ◂

Lema 1. *$S(F)$ existe para cualquier figura plana y acotada F.*

Demostración. Como F es acotada existe un cuadrado L que contiene a toda la figura. Podemos dividir L en m rectángulos, cada uno de ellos de área menor o igual que $|F|/4$.

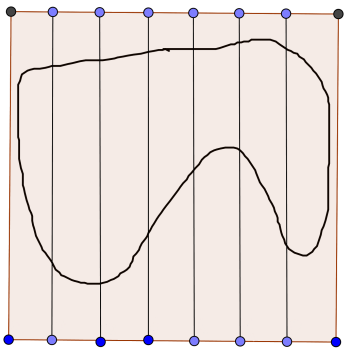

Figura 1: Figura plana y acotada dividida en m rectángulos.

Dados $2m+1$ puntos de F, por el principio del palomar, uno de los rectángulos contendrá al menos tres puntos. El área del triángulo formado por estos tres puntos es menor o igual que $|F|/4$. Por lo tanto, sabemos que hay un número de puntos $2m+1$ que cumplen lo requerido. Usando que todo subconjunto no vacío de números naturales contiene un elemento minimal, podemos asegurar que existe un entero positivo n_1 que nos da el mínimo de $S(F)$. ■

El siguiente lema se usa con bastante frecuencia en las demostraciones que vamos a presentar, por lo que hemos creído conveniente ponerlo al inicio y lo presentamos a continuación:

Lema 2. *El área máxima de un triángulo contenido en un paralelogramo de área $|P|$ es $|P|/2$.*

Demostración. Sea T un triángulo cualquiera ABC contenido en P (por ejemplo, como en el paralelogramo 1 de la figura 2). Trazamos una recta paralela a AB por el vértice del paralelogramo más alejado de este segmento (C' en el paralelogramo 2 de la figura 2). El triángulo T' de vértices ABC' satisface que $|T'| \geq |T|$ por tener mayor o igual altura que el triángulo T y la misma base. Siguiendo este proceso con el resto de lados del triángulo T' se obtienen los triángulos T'' (como en el paralelogramo 3 de la figura 2) y T''' (como en el paralelogramo 4 de la figura 2) tales que $|T'''| \geq |T''| \geq |T'| \geq |T|$. El triángulo T''' tiene como vértices tres de los vértices del paralelogramo y satisface $|T'''| = \frac{|P|}{2}$. Por tanto, $|T| \leq \frac{|P|}{2}$. ■

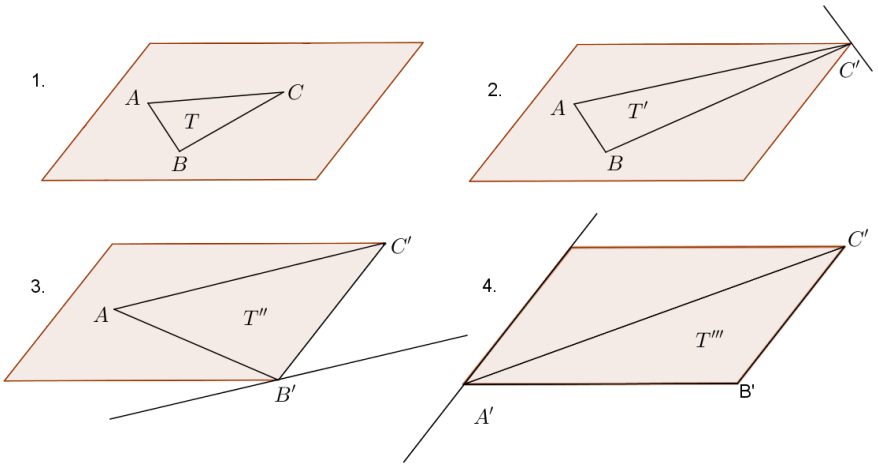

Figura 2: Proceso por el cual se obtiene el triángulo de mayor área de un paralelogramo.

Veamos un ejemplo de lo útil que es este lema:

Proposición 3. *Para un paralelogramo P se tiene que*

$$S(P) = 5.$$

Demostración. Si tomamos los cuatro vértices del paralelogramo, tres cualesquiera de ellos forman un triángulo de área $\frac{|P|}{2} > \frac{|P|}{4}$. Por tanto, $S(P) > 4$.

Para probar que $S(P) = 5$, tomemos los puntos medios de dos lados paralelos del paralelogramo y tracemos el segmento que los une. Ahora tenemos dos mitades de área $|P|/2$ cada una.

Por el principio del palomar, tres de los cinco puntos van a ir a parar a una de las dos mitades y, por el lema 2, el triángulo que formen esos tres puntos tendrá área menor o igual que $|P|/4$. ■

En la sección 2 se muestra que si T es un triángulo, $S(T) = 5$. La sección 3 se dedica a probar que $S(F) \leq 6$ para cualquier figura plana, acotada y convexa. En la sección 4 se demuestra que $S(F) \geq 4$. En la sección 5 se prueba que $S(F) = 6$ para un pentágono regular. Como aportación original, se prueba en la sección 6 que $S(H) = 5$ para un hexágono regular. Para finalizar, se enuncia un problema abierto en esta área.

2. El caso del triángulo

Proposición 4. *Para un triángulo T se tiene que*

$$S(T) > 4.$$

Demostración. Es suficiente ver que los tres vértices del triángulo y el centro de masas (la intersección de las medianas) cumplen lo que buscamos.

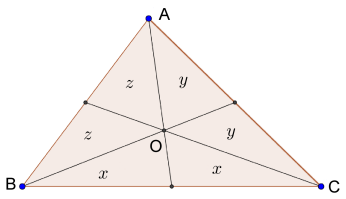

Figura 3: Triángulo dividido por sus tres medianas.

Consideremos los seis triángulos formados al trazar las tres medianas del triángulo ABC. De estos, los triángulos marcados con la misma letra en la figura 3 tienen igual área por tener base de igual longitud y la misma altura. Denotaremos el área de cada triángulo con el mismo nombre que este. Como cada mediana divide un lado del triángulo en dos mitades iguales, tenemos las siguientes identidades:

$$x + x + y = y + z + z \Rightarrow z = x,$$
$$z + z + x = x + y + y \Rightarrow y = z,$$
$$x + x + z = z + y + y \Rightarrow y = x.$$

Por tanto, $x = y = z = \frac{|T|}{6}$. Entonces, el área del menor triángulo formado por tres de los cuatro puntos es $\frac{|T|}{3} > \frac{|T|}{4}$. ■

Proposición 5. *Para un triángulo T se tiene que*

$$S(T) = 5.$$

Demostración. Vamos a hacer una demostración por reducción al absurdo. En primer lugar, sin pérdida de generalidad, tomaremos $|T| = 1$. Supongamos que todo triángulo de los diez posibles que se pueden formar con los cinco puntos ($\binom{5}{3}$ triángulos) tuviera área mayor que $1/4$. Veamos dónde habría que colocar esos cinco puntos.

Se divide el triángulo en cuatro triángulos iguales uniendo los puntos medios de los lados del triángulo original, como se muestra en la parte a) de la figura 4:

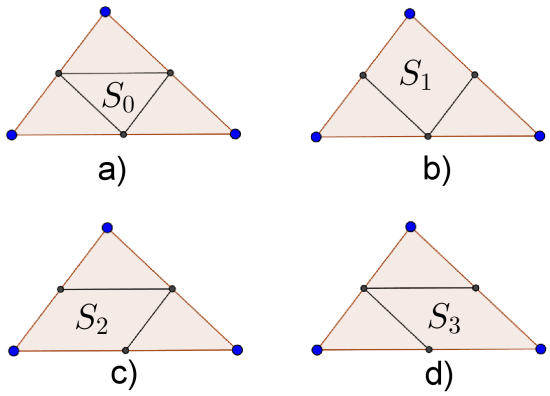

Figura 4: División del triángulo en las porciones S_0, S_1, S_2 y S_3.

Denotemos por S_0 el triángulo central en esta partición y por S_1, S_2 y S_3 los paralelogramos que se muestran en las figuras 4b), 4c) y 4d) formados por la unión de S_0 y uno de los otros tres triángulos considerados en la figura 4a). Denotaremos por $m(S_i)$ al número de puntos contenidos en la sección S_i. Se tiene que

$$m(S_1) \leq 2,$$
$$m(S_2) \leq 2,$$
$$m(S_3) \leq 2,$$

ya que si $m(S_i) \geq 3$ para algún $i \in \{1, 2, 3\}$ entonces, por el lema 2, el paralelogramo S_i contendrá un triángulo formado por tres puntos con área menor o igual que $1/4$.

Supongamos que cogemos los triángulos b), c) y d) de la figura 4 y los superponemos a la figura a) de tal modo que las cuatro figuras coincidan. Los paralelogramos S_1, S_2 y S_3 cubren una vez por completo el triángulo original y el triángulo S_0 lo cubren dos veces más. Esto nos lleva a

$$m(S_1) + m(S_2) + m(S_3) = 5 + 2m(S_0) \Longrightarrow 2 + 2 + 2 \geq 5 + 2m(S_0) \Longrightarrow m(S_0) \leq \frac{1}{2}.$$

Como $m(S_i) \in \mathbb{Z}$, entonces

$$m(S_0) = 0.$$

Por tanto, sabemos que los puntos estarán repartidos en los triángulos exteriores siguiendo el patrón $2-2-1$. Sin pérdida de generalidad, podemos suponer que el triángulo de arriba es el que contiene un solo punto.

Hagamos una partición del triángulo inicial en dieciséis triángulos iguales entre sí uniendo los puntos medios de los lados de los cuatro triángulos en los que hemos dividido la figura original. Marquemos el triángulo S_0 en negro, como se muestra en la figura 5, para indicar que ningún punto va a caer ahí.

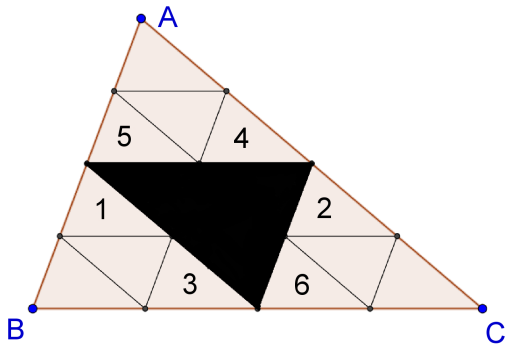

Figura 5: Triángulo dividido en 16 triángulos iguales.

Etiquetaremos los triángulos como en la figura 5 y denotaremos por i_1 el número de puntos contenidos en el triángulo 1. Del mismo modo definimos $i_2, \ldots, i_6$ (véase la figura 5).

Dividamos el triángulo en las tres regiones (roja, morada y verde) de la figura 6. Como hay un punto en el triángulo superior, los otros cuatro puntos deben estar en los paralelogramos morado y verde.

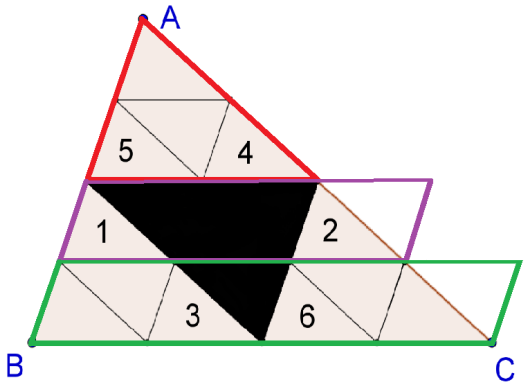

Figura 6: Triángulo dividido en las regiones roja, morada y verde.

Si hubiera tres puntos en la región central, como está contenida en un paralelogramo de área $\frac{6}{16} = \frac{3}{8} < \frac{1}{2}$ (figura 6), por el lema 2 tendríamos un triángulo de área menor que $\frac{1}{4}$.

Igualmente, como la región inferior está contenida en un paralelogramo de área $\frac{8}{16} = \frac{1}{2}$, si hubiera tres puntos en esta región, por el lema 2, formarían un triángulo de área menor o igual que $\frac{1}{4}$.

Por tanto, la región central contendrá dos puntos y la región inferior los otros dos. Como en S_0 no hay puntos, los dos puntos de la región de en medio estarán en los triángulos 1 y 2. Así pues,

$$i_1 + i_2 = 2.$$

Tomando las distintas rotaciones del triángulo y haciendo la misma partición para cada una de las distintas bases, por el mismo razonamiento llegamos a que

$$i_3 + i_4 \geq 1,$$

$$i_5 + i_6 \geq 1.$$

Ahora definimos las siguientes sumas:

$$\begin{array}{lll} \Sigma_1 = i_1 + i_5 + i_4; & \Sigma_3 = i_2 + i_4 + i_5; & \Sigma_5 = i_3 + i_6 + i_1; \\ \Sigma_2 = i_1 + i_5 + i_3; & \Sigma_4 = i_2 + i_4 + i_6; & \Sigma_6 = i_3 + i_6 + i_2. \end{array}$$

Se tiene que

$$\sum_{i=1}^{6} \Sigma_i = 3(i_1 + i_2 + i_3 + i_4 + i_5 + i_6) \geq 3(2 + 1 + 1) = 12. \tag{1}$$

Por otro lado, vamos a probar que para todo $i \in \{1, \ldots, 6\}$ tenemos que $\Sigma_i \leq 2$. En efecto, si se diera que $\Sigma_i > 2$ para algún $i \in \{1, \ldots, 6\}$, entonces tendríamos un paralelogramo de área $1/2$ que contendría tres puntos (en el caso de Σ_3, el paralelogramo $DEFG$ de la figura 7).

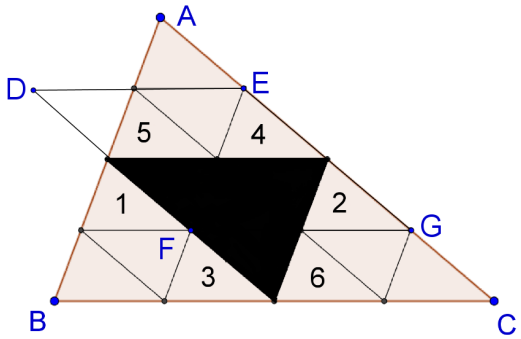

Figura 7: Paralelogramo $DEFG$ de área $\frac{1}{2}$.

Como este paralelogramo tiene área $1/2$, por el lema 2 tendríamos un triángulo de área menor o igual que $1/4$.

De la desigualdad (1) y el hecho anteriormente probado de que $\Sigma_i \leq 2$ para todo i se deduce que $\Sigma_i = 2$ para todo $i \in \{1, \ldots, 6\}$.

La igualdad $\Sigma_1 = \Sigma_2$ implica que $i_3 = i_4$. Por otro lado teníamos que $i_3 + i_4 \geq 1$ y, como i_3 e i_4 son números enteros, obtenemos que

$$i_3 + i_4 \geq 2.$$

Por el mismo razonamiento obtenemos que

$$i_5 + i_6 \geq 2.$$

Debido a que $i_1 + i_2 = 2$ y a las dos desigualdades anteriores obtenemos que

$$\sum_{j=1}^{6} i_j \geq 6.$$

Como habíamos partido de un triángulo con cinco puntos, se obtiene una contradicción. ■

3. Cota superior para $S(F)$

Para poder demostrar que 6 es una cota superior de $S(F)$ necesitamos el siguiente lema.

Lema 6. *Para una figura acotada F y un punto P cualquiera de la figura, existe una recta que pasa por P y divide a la figura en dos partes de igual área.*

Demostración. Trazamos dos rectas que pasen por P y que formen entre sí un ángulo α como en la figura 8. Mantendremos fija una de ellas y rotaremos la otra haciendo variar el ángulo α.

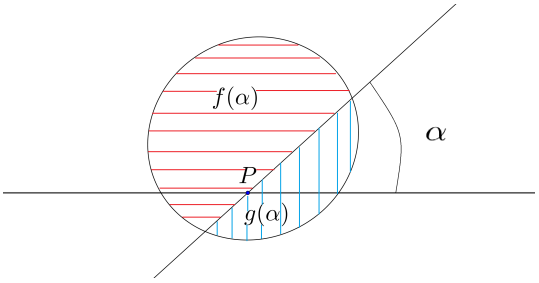

Figura 8: Una figura y dos rectas concurrentes en P.

Sean $f(\alpha)$ y $g(\alpha)$ las áreas de F en cada uno de los semiespacios determinados por la recta que no está fija. Como f y g son continuas y $f(0) - g(0) = -(f(\pi) - g(\pi))$, por el teorema de los valores intermedios, existe un valor de α, digamos α_0, tal que $f(\alpha_0) = g(\alpha_0)$. Esto prueba que por el punto P pasa una recta L que divide a la figura F en dos partes de igual área. ■

Proposición 7. *Para toda figura F acotada y convexa con borde se tiene que*

$$S(F) \leq 6.$$

Demostración. Supongamos que tenemos los seis puntos $v_1, \ldots, v_6$ en la figura F. Por el lema 6, a través del punto v_1 podemos trazar una línea que divida la figura en dos porciones de igual área. Sean estas porciones F_1 y F_2.

Por el principio del palomar, una de las dos porciones contendrá al menos tres de los cinco puntos restantes. Supongamos, sin pérdida de generalidad, que F_1 contiene v_2, v_3, v_4.

Por el lema 6, a través de v_1 podemos trazar una línea que divida F_1 en dos porciones de igual área. Sean estas porciones F_{11} y F_{12}. Por el principio del palomar, al menos una de las dos porciones restantes va a contener dos de los tres puntos. Sin pérdida de generalidad, supongamos que F_{11} contiene a v_2 y v_3.

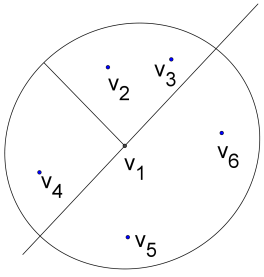

Figura 9: Figura convexa y acotada con seis puntos y dividida dos veces en partes iguales.

La porción F_{11} tiene área $|F_{11}| = |F|/4$. Por tanto,

$$|v_1 v_2 v_3| \leq \frac{|F|}{4}.$$

■

4. Cota inferior para $S(F)$

Vamos a probar que $S(F) \geq 4$ para toda figura F convexa, acotada y con borde. Para la demostración necesitaremos la siguiente definición:

Definición 2. Sea F una figura convexa y p un punto del borde de F. Una **recta soporte** de F por p es una recta que pasa por p y deja la totalidad de la figura F en uno de los dos semiplanos en los que la recta divide al plano. ◂

Observación 1. La recta soporte puede no ser única. ◂

Es momento de pasar a buscar esa cota inferior.

Proposición 8. *Para toda figura F convexa, acotada y con borde se tiene que*

$$S(F) \geq 4.$$

Demostración. Todo lo que hace falta probar es que $S(F) \neq 3$, es decir, que existen tres puntos M, N y P en la figura F tales que

$$|MNP| > \frac{1}{4}|F|.$$

Por el lema 6, sabemos que hay una recta L que divide F en dos partes de igual área. Sean M y N los puntos de intersección de la recta L con el borde de la figura F. Ahora vamos a dibujar tres rectas soporte: una que pasa por M y dos paralelas al segmento $\overline{MN}$.

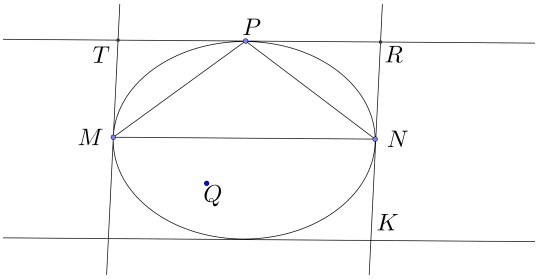

Figura 10: Rectas soporte de una figura.

Trazamos una recta por N paralela a la recta de soporte de M que al cortar con las dos rectas paralelas al segmento $\overline{MN}$ nos dará los puntos R y K. El segmento $\overline{KR}$ no tiene por qué pertenecer a una recta soporte. Observemos que, como la figura F es convexa, el segmento $\overline{RK}$ no contendrá puntos del interior de F por encima y por debajo del segmento $\overline{MN}$. Sin pérdida de generalidad, supongamos que el segmento $\overline{RK}$ solo contiene a puntos de F (interior y borde) por debajo de $\overline{MN}$ o que no contiene a ningún punto distinto de N.

Sea P un punto de la figura y de la recta soporte que está por encima de $\overline{MN}$. Probaremos que M, N y P son los tres puntos buscados. Sea T el punto de intersección de esta recta soporte con la recta soporte de F que pasa por M. Como exactamente la mitad del área de la figura F está completamente contenida en el paralelogramo $MTRN$, obtenemos que

$$|MNP| = \frac{1}{2}|MTRN| \geq \frac{1}{4}|F|.$$

Queremos probar la desigualdad estricta y solo hemos obtenido «≥». La igualdad solo se obtiene cuando la mitad de la figura F coincide exactamente con el paralelogramo $MTRN$. En ese caso, podemos tomar los puntos T, R y cualquier punto Q de la figura F que se encuentre por debajo de MN. Entonces

$$|TRQ| > \frac{1}{4}|F|. \qquad \blacksquare$$

En el libro de Soifer [4, sección 8.5] se prueba la siguiente proposición. Debido a su extensión hemos decidido omitir su demostración.

Proposición 9. *Para toda figura F convexa, acotada y con borde se tiene que*

$$S(F) \neq 4.$$

Por tanto, se tiene que

$$S(F) \geq 5.$$

5. Pentágono regular

Proposición 10. *Para un pentágono regular F se tiene que*

$$S(F) = 6.$$

Demostración. Como $S(F) \leq 6$ por la proposición 7, tenemos que ver que $S(F) > 5$, es decir, que podemos encontrar un conjunto de cinco puntos tales que los diez triángulos ($\binom{5}{3}$ triángulos) formados por tres de ellos tengan área mayor que $\frac{1}{4}|F|$.

Los cinco vértices de F nos dan el conjunto buscado. Sea S el triángulo formado por dos lados contiguos y una diagonal, que está formado por tres de los cinco puntos (ver la figura 11). El triángulo S es isósceles con ángulos de 108 y 36 grados y base (lado desigual) de longitud $\phi \cdot L$, donde L es la longitud del lado del pentágono inicial y $\phi = \frac{1+\sqrt{5}}{2}$ es el número áureo. Supongamos, sin pérdida de generalidad, que el lado del pentágono vale 1. La razón entre áreas será la misma que la de cualquier pentágono con longitud de lado L.

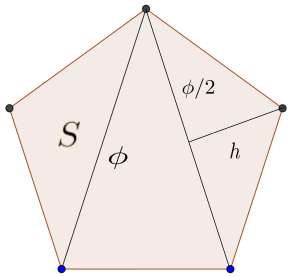

Figura 11: Pentágono regular dividido en los tres triángulos isósceles que se obtienen de trazar las diagonales por un vértice.

Como el ángulo menor de S mide 36 grados y el lado del pentágono mide 1, tenemos que $h = \sin 36$, siendo h la altura del triángulo S. Por tanto,

$$|S| = \frac{(1+\sqrt{5})\sin 36}{4} = 0,4755\ldots$$

Por otro lado, si dividimos el pentágono en cinco triángulos iguales, con vértice común en el centro del mismo, obtenemos cinco triángulos isósceles cuyo ángulo mayor mide 72 grados. Usando esta información y que el lado del pentágono mide 1, obtenemos que el valor de la apotema es $a = \frac{1}{2\tan 36}$. Entonces

$$|F| = \frac{5}{4\tan 36} = 1,7204\ldots$$

Por tanto,

$$\frac{|S|}{|F|} = \frac{(1+\sqrt{5})\sin 36}{4} : \frac{5\cos 36}{4\sin 36} = 0,2763\ldots > \frac{1}{4}.$$

Por último, el área del otro tipo de triángulo T que se podría formar en el pentágono uniendo tres de los cinco puntos escogidos sería

$$|T| = |F| - 2|S| = 0,7694\ldots$$

Entonces,

$$\frac{|T|}{|F|} = 0,4472\ldots > \frac{1}{4}.$$ ■

6. El hexágono regular

Uno de los problemas que propone Alexander Soifer en su libro [4, Problema 8.6.5] es hallar el valor de la función $S(F)$ cuando F es un hexágono regular. En la realización del trabajo de Mellado Cuerno [3] se dio con la solución de este problema.

Proposición 11. *Sea H un hexágono regular. Entonces,*

$$S(H) = 5.$$

Demostración. Supongamos que $|H| = 1$. Trabajaremos con el mallado del hexágono regular que se muestra en la figura 12:

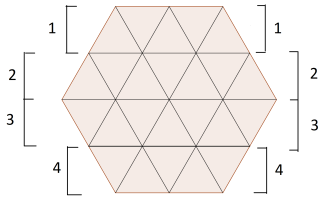

Figura 12: Mallado del hexágono regular y los cuatro trapecios que se obtienen con él.

Este mallado consta de veinticuatro triángulos equiláteros de área $1/24$ y se construye tomando el punto medio de cada lado del hexágono y trazando dos segmentos paralelos a los lados contiguos más las diagonales del hexágono. Con esta división hemos conseguido cuatro trapecios isósceles, dos formados por cinco triángulos cada uno (numerados con el 1 y el 4 en la figura 12) y otros dos formados por siete triángulos cada uno (numerados con el 2 y el 3 en la figura 12). A partir de este punto, siempre que nos refiramos a los trapecios en la demostración hablaremos de estos que acabamos de definir y usaremos la notación de la figura 12. Tomemos cinco puntos en el hexágono. Por el principio del palomar, al menos uno de los trapecios va a tener dos puntos. Vamos a dividir la demostración en varios casos.

Caso 1 Supongamos que al menos tres puntos van a parar a un mismo trapecio.

En este caso ya tendríamos el triángulo buscado aplicando el lema 2. Si tres de estos puntos estuvieran en un trapecio como el 1 o el 4 de la figura 12, estarían incluidos en los paralelogramos de color morado y rojo (figura 13), que tienen área $1/2$. Si los tres puntos estuvieran en uno de los trapecios numerados con 2 y 3 en la figura 12, estarían incluidos en los paralelogramos azul y verde (figura 13), que tienen área menor que $1/2$:

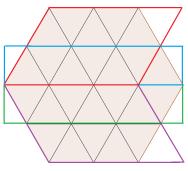

Figura 13: Paralelogramos de área menor o igual a $\frac{1}{2}$ para resolver el caso 1.

Tenemos que estudiar los casos en los que hay como máximo dos puntos en cada uno de los trapecios.

Caso 2 Supongamos que el trapecio inferior contiene dos puntos y el trapecio contiguo, uno.

Volveremos a servirnos del lema 2 para resolver este caso.

Sea donde sea que coloquemos el punto solitario, los tres puntos estarán en un paralelogramo de área $1/2$ (rojo o verde en la figura 14) y, por tanto, tendremos nuestro triángulo deseado de área menor o igual que $1/4$:

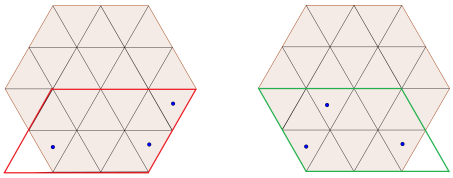

Figura 14: Paralelogramos de área $\frac{1}{2}$ para resolver el caso 2

De este caso también derivamos la situación de que cada uno de estos dos trapecios tenga dos puntos.

Caso 3 Supongamos que el trapecio inferior tiene un punto y el contiguo dos.

Sea arbitrario el triángulo donde coloquemos el punto inferior. Si los otros dos puntos estuvieran o bien en el paralelogramo rojo o en el verde de la figura 15, como ambos son de área $1/2$, por el lema 2 se obtendría un triángulo de área menor o igual que $1/4$.

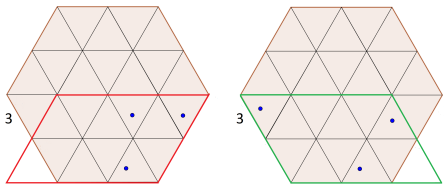

Figura 15: Paralelogramos de área $\frac{1}{2}$ para resolver el caso 3

Por tanto tenemos que considerar el caso en que haya un punto en cada uno de los triángulos extremos del trapecio 3. Con esta colocación de los tres puntos no podemos asegurar que vayan a formar un triángulo de área menor o igual que $1/4$; necesitamos que entre un cuarto punto en juego. Vamos a volver a separarlo en tres casos.

3.1. Supongamos que hubiera un punto en el trapecio 2 de la figura 16, que es contiguo al que ya tiene dos puntos. Si el punto está en un triángulo contenido en los paralelogramos rojo o verde de la figura 16, se tendría un triángulo de área menor o igual a $1/4$, debido al lema 2:

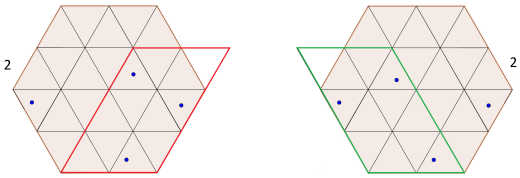

Figura 16: Paralelogramos de área $\frac{1}{2}$ para resolver el caso 3.1.

Quedaría por estudiar la posibilidad de que el punto se sitúe en el triángulo central del trapecio 2 de la figura 16.

El punto restante debería estar en el trapecio superior. Sea donde sea que lo coloquemos podremos trazar un paralelogramo de área $1/2$ y aplicar el lema 2:

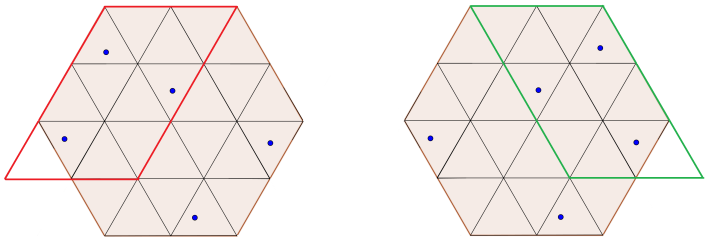

Figura 17: Paralelogramos de área $\frac{1}{2}$ para resolver el caso 3.1.

3.2. Supongamos que en el trapecio 2 de la figura 16 estuvieran los dos puntos restantes. Por el razonamiento del caso anterior, los dos puntos tendrían que estar en el triángulo central de ese trapecio. Es fácil encontrar un paralelogramo de área menor o igual que $1/2$ que contenga tres puntos (figura 18) y por el lema 2, los tres puntos formarán un triángulo de área menor o igual que $1/4$.

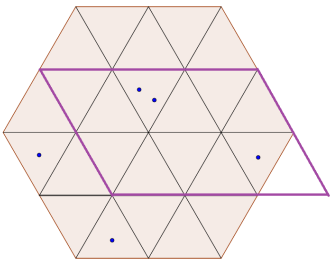

Figura 18: Paralelogramo de área $\frac{1}{2}$ para resolver el caso 3.2.

3.3. Supongamos que colocamos los dos puntos restantes en el trapecio superior. Si uno de los dos puntos no está en un triángulo de los extremos, aplicamos el lema 2 a los paralelogramos rojo o verde de la figura 19 y obtenemos de nuevo un triángulo de área menor o igual que $1/4$.

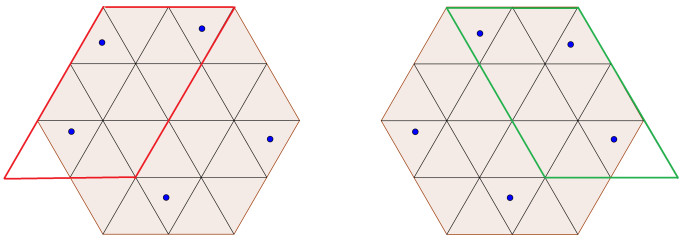

Figura 19: Paralelogramos de área $\frac{1}{2}$ para resolver el caso 3.3.

Colocando cada uno de los dos puntos en sendos triángulos de los extremos del trapecio superior encontramos los paralelogramos que se muestran en la figura 20 de área $1/2$ y podemos volver a aplicar el lema 2 para obtener el triángulo deseado.

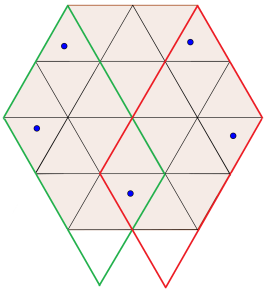

Figura 20: Paralelogramos de área $\frac{1}{2}$ para resolver el caso 3.3.

El resto de combinaciones posibles se derivan de uno de los casos que acabamos de discutir gracias a la simetría del hexágono regular.

Con esto acaba la demostración y vemos que

$$S(H) = 5.$$ ■

7. Clasificación de figuras convexas con borde

Debido a las proposiciones 7 y 9, la función $S(F)$ solo puede tomar dos valores:

$$S(F) = 5 \text{ o } S(F) = 6.$$

Se cree que la excepción es $S(F) = 6$. Ante la dificultad de encontrar las figuras que cumplieran este caso, en 1990 Alexander Soifer lanzó un reto matemático. Ofrecía cincuenta dólares a la persona que diera la clasificación de las figuras F tales que $S(F) = 6$. El propio Soifer conjeturó lo siguiente:

Conjetura 12. *Las figuras F acotadas y convexas tales que $S(F) = 6$ son aquellas cuyo borde se obtiene como transformación afín del borde de un pentágono regular y queda comprendido entre dos pentágonos regulares concéntricos, como se puede observar en la figura 21.*

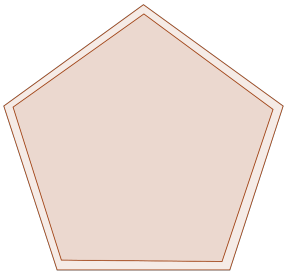

Figura 21: Pentágonos regulares concéntricos.

El matemático ruso Karabash probó en 2007 con dos artículos [1, 2], el primero publicado en 2007 y el segundo en 2008, que la conjetura de Alexander Soifer era falsa.

Actualmente, la cuantía del reto ha ascendido a cien dólares y prima la conjetura que el propio Karabash dio:

Conjetura 13. *Es imposible dar una clasificación de las figuras F tales que $S(F) = 6$.*

Referencias

[1] Karabash, Dmytro. «On The Soifer Fifty Dollar Problem, Part I: Construction». En: *Geombinatorics* 17.2 (2007), págs. 68-77.

[2] Karabash, Dmytro. «On The Soifer Fifty Dollar Problem, Part II: The Existence of the Counterexample to the Conjecture». En: *Geombinatorics* 17.3 (2008), págs. 124-128.

[3] Mellado Cuerno, Manuel. *¿Cómo cortar un triángulo?: Problemas de geometría descriptiva en el plano*. Trabajo de fin de grado. Universidad Autónoma de Madrid, 2017.

[4] Soifer, Alexander. *How Does One Cut a Triangle?* Nueva York: Springer-Verlag, 2009. https://doi.org/10.1007/978-0-387-74652-4.

TEMat

El sistema de axiomas de ZFC

Víctor González López
Universidad de Murcia
victorgl94@gmail.com

Resumen: En este artículo realizamos una introducción al sistema de axiomas de Zermelo-Fraenkel, complementado con el axioma de elección, base de la teoría de conjuntos. Para ello, comenzaremos exponiendo los axiomas del sistema de Zermelo-Fraenkel, para después introducir el axioma de elección. Hablaremos de la presencia de este en las matemáticas, así como de dos versiones suyas. Finalmente, hablaremos del debate de la consistencia y de una posible alternativa al axioma de elección. Es importante resaltar que no haremos un uso estricto de la lógica de primer orden, ya que nuestro objetivo es presentar y motivar los axiomas, y no hacer un estudio minucioso de ellos en términos lógicos.

Abstract: In this article, we introduce the sistem of axioms of Zermelo-Fraenkel, complemented with the axiom of choice, base of set theory. In order to achieve this, we begin by presenting the axioms of Zermelo-Fraenkel and, after that, the axiom of choice. We talk about the presence of the axiom of choice in mathematics, as well as about a couple of versions of it. Finally, we talk about the debate of consistency and about a possible alternative to the axiom of choice. It is important to emphasise that we do not use first order logic, given that our main purpose is to present and motivate the axioms, and not to make a thorough study of them in logical terms.

Palabras clave: axiomática, conjuntos, axioma de elección, Zermelo-Fraenkel.

MSC2010: 03E25, 03E30.

Recibido: 24 de julio de 2017.
Aceptado: 13 de octubre de 2017.

Agradecimientos: Me gustaría agradecer al profesor Antonio Avilés López de la Universidad de Murcia su trabajo y dedicación a la hora de dirigir tanto mi trabajo fin de Grado como de Máster, ya que este trabajo está basado en un capítulo de mi trabajo fin de Grado.

Y, por supuesto, a mis padres y a mi hermano.

Referencia: González López, Víctor. «El sistema de axiomas de ZFC». En: *TEMat*, 2 (2018), págs. 45-52. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p45/.

1. Introducción

A finales del siglo XIX, David Hilbert, afamado matemático alemán, afirmaba que la manera adecuada de desarrollar cualquier teoría científica de manera rigurosa era a partir de una axiomatización. Entre estas teorías estaba la teoría de conjuntos, rama de las matemáticas que estudia las «colecciones bien definidas, llamadas **conjuntos**, de objetos a los que llamamos miembros o **elementos**» [4], que a su vez son conjuntos. La teoría de conjuntos sirve como fundamento de las matemáticas, ya que a partir de ella se pueden desarrollar formalmente las demás teorías matemáticas y sus diferentes estructuras.

En principio, dados dos conjuntos x e y, lo único que podemos decir sobre ellos es si son iguales, lo cual denotaríamos por $x = y$, o si uno pertenece a otro, lo cual denotaríamos por $x \in y$. Estas afirmaciones pueden ser verdaderas o falsas. Sin embargo, estas dos relaciones que podemos establecer entre dos conjuntos han de satisfacer una serie de axiomas, es decir, unos principios fundamentales e indemostrables, que asumimos ciertos, sobre los que se construye la teoría.

Una vez asumido este sistema de axiomas, el objetivo de la teoría de conjuntos es determinar qué afirmaciones sobre los conjuntos son verdaderas (pueden demostrarse siguiendo unos razonamientos lógicos), cuáles son falsas (su negación es verdadera) y cuáles son indecidibles (ni ellas ni sus negaciones se pueden deducir de los axiomas).

En este trabajo vamos a comenzar enunciando los axiomas de Zermelo-Fraenkel, para los cuales la principal referencia son los apuntes de Avilés López [3][1]. Posteriormente, estableceremos el axioma de elección, el cual, unido a los axiomas de Zermelo-Fraenkel, constituye el sistema de axiomas más utilizado. Asimismo, comentaremos la dualidad de la presencia del axioma de elección en las matemáticas. Finalizaremos el artículo hablando del concepto de consistencia de un sistema de axiomas, así como de una posible alternativa al axioma de elección.

2. Los axiomas de ZF

En 1904, Ernst Zermelo, matemático y lógico alemán, formuló el axioma de elección para probar que todo conjunto puede ser bien ordenado. Zermelo recibió muchas críticas por ello y célebres colegas como Borel, Baire y Lebesgue se opusieron al axioma, ya que este establece la existencia de un cierto conjunto sin dar una definición explícita del mismo, algo inasumible por muchos en aquel momento[2].

Cuatro años más tarde, en 1908, con el fin de proteger su demostración, Zermelo publicó la primera axiomatización de la teoría de conjuntos, donde los axiomas que postuló eran principios consonantes con su prueba, entre los que se encontraba el axioma de elección. Lejos de alejar la controversia sobre su prueba, lo que ocurrió es que la propia axiomatización fue cuestionada.

Fue en 1930 cuando Zermelo publicó una nueva axiomatización en la que se modificó la anterior y se incluyeron las sugerencias hechas por Fraenkel unos años antes. Este sistema es muy parecido al usado hoy en día y se conoce como Zermelo-Fraenkel (ZF). Comenzamos ahora a enunciar los axiomas que lo componen:

Axioma 1 (ZF1: axioma de extensionalidad). *Dos conjuntos son iguales si y solo si tienen los mismos elementos.*

Este axioma es muy importante porque nos proporciona la unicidad de los conjuntos.

Axioma 2 (ZF2: axioma del conjunto vacío). *Existe un conjunto que no tiene elementos. Lo denotaremos por* $\varnothing$.

Para entender la necesidad de varios de los siguientes axiomas de ZF es necesario hablar de la paradoja más famosa de la teoría de conjuntos: la **paradoja de Russell**. Podría parecer lógico introducir el siguiente axioma en el sistema ZF:

[1] Dado que estos apuntes son privados, recomendamos al lector consultar el libro de Goldrei [9], donde se exponen los axiomas de ZF con gran claridad.

[2] Las referencias históricas utilizadas a lo largo del trabajo han sido extraídas del libro de Moore [16].

Axioma A. *Dada una propiedad $P(t)$, existe un conjunto x cuyos elementos son precisamente los conjuntos t que cumplen la propiedad.*

Sin embargo, este axioma lleva a contradicciones ya que, si consideramos la propiedad $t \notin t$, el axioma A nos dice que existe el conjunto $x = \{t : t \notin t\}$. Si ahora nos preguntamos si $x \in x$, tenemos dos opciones:

1. Si $x \in x$, x no puede ser elemento de sí mismo, por lo que $x \notin x$.
2. Si $x \notin x$, x es elemento de sí mismo, por lo que $x \in x$.

Así pues, $x \in x \iff x \notin x$. Esto es absurdo, por lo que nos vemos obligados a descartar este axioma. La explicación intuitiva reside en que un conjunto debe existir después de sus elementos. Así pues, no tiene sentido preguntarse si $x \in x$ antes de que exista. Esto conlleva la inclusión de otra serie de axiomas que lo sustituyan y eviten contradicciones. En concreto, estos son ZF3-ZF7:

Axioma 3 (ZF3: axioma de separación). *Dados un conjunto C y una propiedad $P(t)$ que los elementos t de C pueden cumplir o no, existe el conjunto $x = \{t \in C : P(t)\}$.*

Este axioma es diferente a nuestro axioma A puesto que, así como en el axioma A se asume la existencia del conjunto x de manera incondicional, en el axioma de separación está supeditada a la existencia previa del conjunto C. Esta diferencia conlleva que si consideramos de nuevo la propiedad $t \notin t$, la cual nos llevaba a contradicción con el axioma A, en este caso no lo hace, ya que tendríamos el conjunto $x = \{t \in C : t \notin t\}$, el cual veremos que es el propio C.

Axioma 4 (ZF4: axioma de pares). *Dados dos conjuntos x, y, existe el conjunto formado únicamente por x e y, al que denotaremos por $\{x, y\}$.*

Nota 1. En el caso en el que x e y sean iguales, denotaremos a $\{x, y\} = \{x, x\}$ por $\{x\}$. ◂

Este axioma nos permite definir los pares ordenados $(a, b) \coloneqq \{\{a\}, \{a, b\}\}$. A partir de estos definimos el producto cartesiano de dos conjuntos x, y como

$$x \times y \coloneqq \{(a, b) : a \in x \text{ y } b \in y\}.$$

Axioma 5 (ZF5: axioma de la unión). *Dado un conjunto x, existe la unión*

$$\bigcup x \coloneqq \{t : \exists\, y \in x : t \in y\}.$$

Lo que nos dice este axioma es que, dado un conjunto x, podemos encontrar un conjunto cuyos elementos son los elementos de los elementos de x.

Una vez que hemos enunciado ZF4 y ZF5, estamos en condiciones de definir la unión y la intersección de dos conjuntos. En efecto, dados a, b conjuntos, definimos $a \cup b \coloneqq \bigcup\{a, b\}$. Esta definición está justificada porque $x \in \bigcup\{a, b\} \iff \exists\, y \in \{a, b\}$ tal que $x \in y$. Basta notar ahora que los únicos elementos de $\{a, b\}$ son a y b. Así, $x \in \bigcup\{a, b\} \iff (x \in a) \vee (x \in b)$. Tener definida la unión de dos conjuntos nos da pie a definir la intersección de la siguiente manera (ver [9], p. 85): $a \cap b \coloneqq \{x \in a \cup b : (x \in a) \wedge (x \in b)\}$ (nótese el uso del axioma de separación).

Definición 1. Dados dos conjuntos x, y, diremos que y está **contenido** en x o y es un **subconjunto** de x si para todo $z \in y$, se cumple que $z \in x$. En tal caso, escribiremos $y \subseteq x$. ◂

Axioma 6 (ZF6: axioma de las partes). *Dado un conjunto x, existe el conjunto $\mathcal{P}(x) \coloneqq \{y : y \subseteq x\}$.*

Así pues, el conjunto $\mathcal{P}(x)$, al que llamaremos «**partes de *x***», está formado por los subconjuntos de x.

Axioma 7 (ZF7: axioma de reemplazamiento). *Si x es un conjunto y $F(t)$ una función que permite asignar a cada elemento $t \in x$ un conjunto $F(t)$, entonces existe el conjunto $\{F(t) : t \in x\}$.*

El axioma del conjunto vacío nos garantiza la existencia de al menos un conjunto. Sin embargo, no garantiza la existencia de conjuntos infinitos. Veamos un ejemplo: tomamos el conjunto $\varnothing$ y, usando ZF4, construimos $\{\varnothing\}$. Llamaremos 1 a la unión de $\varnothing$ y $\{\varnothing\}$. Así, $1 = \varnothing \cup \{\varnothing\}$. Está claro que $1 = \{\varnothing\}$. Del mismo modo, definimos $2 \coloneqq 1 \cup \{1\} = \{\varnothing, 1\}$. De manera general, dado el conjunto n, definimos el «sucesor de

n» como $\boldsymbol{s(n) := n \cup \{n\} = \{\varnothing, \ldots, n\}}$. Denotaremos $s(n)$ como $\boldsymbol{n+1}$. De esta forma podemos definir los números naturales. No obstante, no tenemos garantizada la existencia del conjunto que los contenga a todos ellos, es decir, $\mathbb{N}$. Esto es precisamente lo que nos proporciona el siguiente axioma, ya que afirma la existencia de un conjunto infinito.

Axioma 8 (ZF8: axioma del infinito). *Existe un conjunto x tal que*

- $\varnothing \in x$.
- $\forall\, n : n \in x \Rightarrow s(n) \in x$.

Nota 2. La intersección de los conjuntos x que satisfacen el axioma del infinito también es un conjunto que lo satisface. Esto nos permite definir $\mathbb{N}$ como el menor conjunto que cumple ZF8. ◂

Lema 1. *ZF4 puede ser deducido a partir de ZF1, ZF3, ZF6 y ZF7.*

Demostración. En efecto, dados x e y conjuntos, consideramos el conjunto $\{y \in x : y \neq y\}$ (por ZF3). Este conjunto es el vacío $\varnothing$. Aplicamos ahora ZF6 y obtenemos $\mathcal{P}(\varnothing) = \{\varnothing\} = 1$. De nuevo, por ZF6, $\mathcal{P}(1) = \{\varnothing, 1\} = 2$. Así, ya tenemos un conjunto con dos elementos. Definimos ahora una función de la siguiente manera:

$$\begin{array}{ccc} \varnothing & \mapsto & x. \\ 1 & \mapsto & y. \end{array}$$

Basta usar ahora ZF7 y tenemos que existe el conjunto $\{F(t) : t \in 2\} = \{x, y\}$. ■

A pesar de que ZF4 se pueda deducir de otros axiomas, se incluye por motivos didácticos, ya que permite clarificar la comprensión de los axiomas.

Axioma 9 (ZF9: axioma de regularidad). *Para cualquier conjunto no vacío x existe $y \in x$ tal que $x \cap y = \varnothing$.*

A priori, este axioma no parece intuitivo. Uno puede pensar en un conjunto muy importante, como es, por ejemplo, $\mathbb{N}$, el conjunto de los números naturales, y rápidamente llega a la conclusión de que es imposible que exista algún natural cuya intersección con $\mathbb{N}$ sea vacía, porque ¿qué sentido tiene que un número natural sea disjunto con $\mathbb{N}$? Esta aparente contradicción en realidad no es tal; está inducida por la manera de pensar en los números naturales. Lo que ocurre es que cuando trabajamos a diario con los números naturales, tratamos a estos como eso, números. Sin embargo, como hemos visto antes, estos son conjuntos, y su definición hace que no exista contradicción alguna.

Por otro lado, cabe destacar que el axioma de regularidad nos permite deducir que no existen conjuntos que se contengan a sí mismos:

Proposición 2 ([9, pág. 95]). *Ningún conjunto puede ser elemento de sí mismo.*

Demostración. Sea x un conjunto. Por el axioma de pares (ZF4), existe el conjunto $\{x\}$. Por el axioma de regularidad (ZF9), existe un elemento de $\{x\}$ que es disjunto con $\{x\}$. Ahora bien, como el único elemento de $\{x\}$ es x, $x \cap \{x\} = \varnothing$, lo que implica que el único elemento de $\{x\}$, x, no está en el otro conjunto de la intersección, x, es decir, $x \notin x$. ■

De aquí deducimos que el conjunto $x = \{t \in C : t \notin t\}$, considerado tras el axioma de separación, es, en efecto, el propio C. Del mismo modo, si consideramos el conjunto $x = \{t \in C : t \in t\}$, tenemos que no tiene ningún elemento. Así pues, el axioma del conjunto vacío (ZF2) se puede deducir de los demás axiomas, pero, al igual que el axioma de pares, se incluye por motivos didácticos.

3. El axioma de elección (AC)

Pasamos ahora a hablar del axioma de elección, al que denotaremos AC por sus siglas en inglés, un axioma clave en la teoría de conjuntos. En la primera axiomatización de esta, también llevada a cabo por Zermelo, en 1908, este aparecía dentro de los axiomas que postuló. Sin embargo, en el sistema ZF, formulado en 1930, fue excluido debido a las diferencias existentes entre el resto de axiomas y él.

Definición 2 ([11, pág. 47]). Si S es una familia de conjuntos no vacíos, una función de elección para S es una función $f: S \to \bigcup S$ tal que

$$f(X) \in X \quad \forall\, X \in S.$$ ◂

Axioma 10 (Axioma de elección (AC)). *Toda familia de conjuntos no vacíos tiene una función de elección.*

Nota 3. Dado que el producto cartesiano de una familia de conjuntos $\{X_i : i \in I\}$ se define como $\prod_{i\in I} X_i = \{f: I \to \bigcup\{X_i : i \in I\} : f(i) \in X_i \ \forall\ i \in I\}$ (ver [15], pág. 158), tenemos que el axioma de elección es equivalente a que, dada una familia de conjuntos no vacíos, su producto cartesiano sea no vacío. ◂

Sin embargo, cuando hablamos de una familia finita de conjuntos no vacíos, la existencia de una función de elección es consecuencia de ZF:

Proposición 3. *Sea S una familia finita de conjuntos no vacíos. Entonces, S tiene una función de elección.*

Como hemos comentado anteriormente, el axioma de elección fue formulado por Zermelo en 1904 cuando buscaba una prueba de que todo conjunto puede ser bien ordenado. Fue rechazado de manera tajante por aquellos matemáticos que identificaban la existencia de un objeto matemático con su construcción mediante una regla, puesto que el AC postula la existencia de un conjunto sin dar definición alguna de este. Por otro lado, a partir de él se obtienen resultados como la paradoja de Banach-Tarski y la existencia de conjuntos no medibles Lebesgue. Sin embargo, hoy en día es aceptado por la mayoría de los matemáticos y es necesario a la hora de obtener resultados en álgebra, análisis o topología.

3.1. Dualidad de AC

Otra característica del axioma de elección es que posee un carácter dual: su presencia en las matemáticas se ve claramente dividida en dos papeles. En primer lugar, hay resultados para los cuales AC es necesario tal y como se acaba de enunciar:

Teorema 4 (Lema de Zorn [14, págs. 161-162]). *Si $(P, <)$ es un conjunto parcialmente ordenado tal que todo subconjunto suyo totalmente ordenado tiene una cota superior, entonces P tiene un elemento maximal.*

Ahora bien, también se cumple el recíproco, lo cual deriva en lo siguiente:

Teorema 5 ([14, pág. 162]). *El lema de Zorn es equivalente al axioma de elección.*

Es gracias al lema de Zorn que podemos obtener resultados tan importantes en las matemáticas, cuyas pruebas pueden consultarse en el libro de Jech [12], como son los siguientes:

- Todo espacio vectorial tiene un base.
- Teorema de Hahn-Banach.
- Teorema de Tichonoff sobre compactos.
- Todo cuerpo tiene una única clausura algebraica.

Así mismo, de la existencia de una función de elección para una familia arbitraria de conjuntos no vacíos se derivan los resultados contraintuitivos de los que hemos hablado:

Teorema 6 ([5, págs. 109-110]). *Existen conjuntos no medibles Lebesgue en $\mathbb{R}$.*

Teorema 7 (Paradoja de Banach-Tarski [9, pág. 116]). *Sea S la bola unidad en $\mathbb{R}^3$. S puede ser particionada en un número finito de subconjuntos tales que, movidos mediante traslaciones y rotaciones, producen dos bolas unidad.*

Así como el axioma de elección se usa para probar ciertos resultados muy importantes, como son los anteriores, existe otro tipo de resultados, pertenecientes sobre todo al análisis real y a la teoría de la medida, para los cuales es suficiente una versión más débil de él:

Axioma 11 (Axioma numerable de elección (CAC)). *Toda familia numerable de conjuntos no vacíos tiene una función de elección.*

Antes de que Zermelo enunciara el axioma de elección, este ya había sido usado en diversas pruebas de manera implícita en su versión numerable, debido a que en su versión numerable es más complicada la identificación de su uso. A modo de ejemplo, vamos a demostrar un resultado muy conocido para el que se dio este tipo de situación.

Teorema 8 ([17, pág. 163]). *Sea $f : \mathbb{R} \to \mathbb{R}$ una aplicación. Entonces, f es continua si y solo si es continua por sucesiones, es decir, si y solo si para toda sucesión $(x_n)_{n\in\mathbb{N}}$ tal que $x_n \to x$ se cumple que $f(x_n) \to f(x)$.*

En concreto, el CAC es necesario para probar que la continuidad por sucesiones implica la continuidad:

Proposición 9. *Sea $f : \mathbb{R} \to \mathbb{R}$ continua por sucesiones. Entonces, f es continua.*

Demostración. Supongamos que f no es continua en a. Por tanto, existe un $\epsilon > 0$ tal que para todo $\delta > 0$ existe $x \in B(a, \delta)$ tal que $f(x) \notin B(f(a), \epsilon)$. En particular, para todo $n \in \mathbb{N}$ podemos elegir $x_n \in (a-\frac{1}{n}, a+\frac{1}{n})$ tal que $f(x_n) \notin B(f(a), \epsilon)$. Hemos construido una sucesión que converge a a cuya imagen no converge a $f(a)$. Esto es una contradicción, por lo que f es continua en a. ■

Notemos que el axioma numerable de elección está siendo usado en el momento en el que se dice «podemos elegir x_n tal que...», puesto que tenemos la familia numerable de conjuntos no vacíos $\mathcal{F}_n = \{x : x \in (a - \frac{1}{n}, a + \frac{1}{n}) \text{ y } f(x) \notin B(f(a), \epsilon)\}$, la cual posee una función de elección que nos permite elegir x_n con la propiedad deseada.

Otro resultado muy conocido en el que también es necesario el uso del CAC es el siguiente:

Proposición 10 ([16, pág. 9]). *La unión numerable de conjuntos numerables es numerable.*

3.2. Dos versiones del AC

En la sección anterior hemos enunciado el axioma numerable de elección (CAC) y hemos dicho que este es consecuencia del axioma de elección (AC). En esta sección vamos a probar este resultado, pero, previamente, pasaremos por otro axioma más fuerte que el CAC, llamado principio de elecciones dependientes (DC), necesario para definir sucesiones de manera inductiva.

Definición 3 ([11, pág. 10]). Dados dos conjuntos A, B, una relacion binaria R entre A y B es un subconjunto del producto cartesiano $A \times B$. Así, si $(a, b) \in R$, diremos que aRb. ◂

Axioma 12 (Principio de elecciones dependientes (DC)). *Sea R una relación binaria en un conjunto no vacío A. Si para todo $a \in A$ existe $b \in A$ tal que bRa, entonces existe una sucesión $(a_n)_{n\in\mathbb{N}}$ de elementos de A tal que $a_{n+1}Ra_n$ para todo $n \in \mathbb{N}$.*

Proposición 11 ([11, Ejercicio 5.7]). *El principio de elecciones dependientes implica el axioma numerable de elección.*

Demostración. Sea $S = \{A_n : n \in \mathbb{N}\}$ una familia numerable de conjuntos no vacíos. Sea

$$A = \{\text{funciones de elección para algún } S_n\},$$

donde $S_n = \{A_i : i \leq n\}$ para todo $n \in \mathbb{N}$. Consideramos también la relación binaria $\supsetneq$.

Sea ahora $f \in A$ (existe porque estamos en el caso finito). ¿Existe $g \in A$ tal que $g \supsetneq f$?[3]

Como $f \in A$, f es una función de elección en un cierto S_{n_0}. Por otro lado, como S es una familia de subconjuntos no vacíos, existe $x \in A_{n_0+1}$. Definimos ahora g de la siguiente manera:

$$\begin{array}{rccc} g: & S_{n_0+1} & \to & \bigcup S_{n_0+1} \\ & A_1 & \mapsto & f(A_1), \\ & A_2 & \mapsto & f(A_2), \\ & \vdots & \vdots & \vdots \\ & A_{n_0} & \mapsto & f(A_{n_0}), \\ & A_{n_0+1} & \mapsto & x. \end{array}$$

[3] Cuando decimos que una función contiene otra nos estamos refiriendo a que una es una extensión de la otra.

Así, tenemos una función de elección g tal que $g \supseteq f$. Ahora, por hipótesis, existe una sucesión $(f_n)_{n\in\mathbb{N}}$ con $f_n \subseteq f_{n+1}$ para todo n en $\mathbb{N}$. Sea ahora

$$\begin{array}{rccc} F: & S & \to & \bigcup S \\ & A_n & \mapsto & f_n(A_n). \end{array}$$

F es una función de elección porque, para todo $n \in \mathbb{N}$, se tiene que f_n es una función de elección de S_m, para cierto $m \geq n$. ∎

Proposición 12 ([17, pág. 243]). *El axioma de elección implica el principio de elecciones dependientes.*

Demostración. Sea R una relación binaria en un conjunto no vacío A. Supongamos que para todo $a \in A$ existe $b \in A$ tal que bRa. Veamos que existe una sucesión $(a_n)_{n\in\mathbb{N}}$ de elementos de A tal que $a_{n+1}Ra_n$ para cada $n \in \mathbb{N}$.

Consideramos ahora, para todo $x \in A$, el conjunto

$$R(x) = \{y \in A : yRx\}.$$

Tenemos, pues, una familia de conjuntos $T := (R(x))_{x\in A}$ no vacíos. Ahora, por hipótesis, existe

$$\begin{array}{rccc} F: & T & \to & \bigcup T \\ & R(x) & \mapsto & F(R(x)) \in R(x). \end{array}$$

Esto nos permite construir la función

$$\begin{array}{rccccc} f: & A & \to & T & \to & \bigcup T \\ & x & \mapsto & R(x) & \mapsto & F(R(x)) \in R(x). \end{array}$$

Sea ahora, para todo $x \in A$, la sucesión $(a_n)_{n\in\mathbb{N}} = (f^n(x))_{n\in\mathbb{N}}$. Gracias a que F es una función de elección se cumple que, para todo $n \in \mathbb{N}$, $f^{n+1}(x) = f(f^n(x)) \in R(f^n(x))$, por lo que $f^{n+1}(x)Rf^n(x)$. ∎

4. Consistencia

Ahora bien, una de las características que ha de tener un sistema de axiomas es la consistencia, es decir, que a partir de ellos no se pueda deducir ninguna contradicción. Existía una creencia de que el sistema de axiomas de Zermelo-Fraenkel era consistente y durante varios años se intentó probar. Sin embargo, entre 1930 y 1936 Gödel probó que la consistencia de ZF no puede ser deducida dentro del propio ZF (para consultar las obras de Gödel, véanse sus *Obras completas* [8]), sino que para ello es necesario un sistema de axiomas más general en el que *a priori* es más complicado tener consistencia:

Teorema 13 ([6, pág. 45]). *Bajo ZF, es imposible demostrar que ZF sea consistente.*

Este resultado arrojó un jarro de agua fría sobre aquellos que creían que sería posible encontrar un sistema de axiomas consistente que permitiera desarrollar todas las matemáticas dentro de él.

Otro problema seguía abierto, y era la consistencia relativa del axioma de elección respecto a ZF. En 1924 se publicó la paradoja de Banach-Tarski, que junto con el hecho de que existieran conjuntos no medibles Lebesgue en la recta real (debido esto último a Vitali) hizo pensar que el axioma de elección había de conducir a alguna contradicción, por lo que los que no creían en él sostenían que el sistema de axiomas ZFC era inconsistente. Sin embargo, de nuevo Gödel, en 1935, durante una visita al Instituto de Estudios Avanzados de Princeton, comunicó a Von Neumann que había demostrado que si ZF es consistente, ZFC es consistente, es decir, la consistencia relativa del AC respecto a ZF. Este resultado cerró el debate existente en torno al axioma de elección durante varias décadas, dándole la razón a Zermelo, el primero que abogó por él:

Teorema 14 ([6, pág. 99]). *Si ZF es consistente, entonces ZFC es consistente.*

El primero de estos resultados supuso un fracaso para la comunidad matemática porque limita el debate de la consistencia de ZF al empirismo. El segundo de ellos cerró el debate abierto sobre el axioma de elección. Muchos matemáticos seguían creyendo que este axioma llevaría a contradicciones. Sin embargo, la consistencia de ZFC es equivalente a la de ZF. Y la consistencia de ZF, pese a no poderse probar, es aceptada. Así pues, la de ZFC habría de serlo también.

5. Consideraciones finales

A lo largo de estas páginas hemos expuesto el sistema de axiomas más común de las matemáticas, el de ZF, y hemos hablado del axioma más famoso, el de elección. Del mismo modo, hemos visto que este último, pese a dar lugar a determinados resultados contraintuitivos, como la existencia de conjuntos no medibles Lebesgue en $\mathbb{R}$ y la paradoja de Banach-Tarski, es comúnmente aceptado por la comunidad matemática, algo que se ve respaldado por los resultados relativos a la consistencia que acabamos de enunciar.

Finalmente, cabe resaltar que existen alternativas al axioma de elección, como el axioma de determinación, incompatible con este y bajo el cual todo conjunto de números reales es medible Lebesgue[4].

Referencias

[1] Adams, Colin y Franzosa, Robert. *Introduction to Topology: Pure and Applied*. Prentice Hall, 2007. isbn: 978-0-13-184869-6.

[2] Alías Linares, Luis. *Apuntes de Topología de Superficies*. Universidad de Murcia. 2014.

[3] Avilés López, Antonio. *Apuntes de axiomática*. Universidad de Murcia. 2015.

[4] Bagaria, Joan. «Set Theory». En: *The Stanford Encyclopedia of Philosophy*. Ed. por Zalta, Edward N. Summer 2017. Metaphysics Research Lab, Stanford University, 2017. url: https://plato.stanford.edu/archives/sum2017/entries/set-theory/.

[5] Berberian, Sterling K. *Fundamentals of Real Analysis*. Universitext. Springer-Verlag, 1999. https://doi.org/10.1007/978-1-4612-0549-4.

[6] Cohen, Paul Joseph. *Set Theory and the Continuum Hypothesis*. The Benjamin/Cummings Publishing Company, 1966.

[7] Fernández Laguna, Víctor. *Teoría básica de conjuntos*. Base Universitaria. ANAYA, 2003. isbn: 978-84-667-2614-6.

[8] Gödel, Kurt. *Obras completas*. first. Alianza ensayo. Edición de Jesús Mosterín. Alianza Editorial, 2006. isbn: 978-84-206-4773-9.

[9] Goldrei, Derek. *Classic Set Theory For Guided Independent Study*. Champman & Hall, 1996. isbn: 978-0-412-60610-6.

[10] González López, Víctor. *El Axioma de Determinación*. Universidad de Murcia. Jun. de 2016. url: http://www.um.es/web/matematicas/tfg-axioma-determinacion-gonzalez-lopez-2016.

[11] Jech, Thomas. *Set Theory*. Springer Monographs in Mathematics. Springer-Verlag, 2003. https://doi.org/10.1007/3-540-44761-X.

[12] Jech, Thomas. *The Axiom of Choice*. Dover Publications, 2008. isbn: 978-0-486-46624-8.

[13] Kechris, Alexander. *Classical Descriptive Set Theory*. Vol. 256. Graduate Texts in Mathematics. Springer-Verlag, 1995. https://doi.org/10.1007/978-1-4612-4190-4.

[14] Levy, Azriel. *Basic Set Theory*. Perspectives in Mathematical Logic. Springer-Verlag, 1979. isbn: 978-0-387-08417-6.

[15] López Camino, Rafael. *Topología*. Editorial Universidad de Granada, 2014. isbn: 978-84-338-5676-0.

[16] Moore, Gregory H. *Zermelo's Axiom of Choice: Its Origins, Development, and Influence*. Studies in the History of Mathematics and Physical Sciences. Springer-Verlag, 1982. https://doi.org/10.1007/978-1-4613-9478-5.

[17] Potter, Michael. *Set Theory and Its Philosophy*. Oxford University Press, 2004. isbn: 978-0-19-927041-5.

[18] Royden, Halsey L. *Real Analysis*. Macmillan Publishing Company, 1988. isbn: 978-0-02-404151-7.

[19] Stewart, Ian y Tall, David. *The Foundations of Mathematics*. Oxford University Press, 1977. isbn: 978-0-19-853165-4.

[4] Para consultar una prueba de esto véanse el trabajo de González López [10] o el libro de Jech [11].

TEMat

Dominación *sparse* y el teorema A_2

Israel P. Rivera-Ríos
Universidad del País Vasco / Euskal Herriko Unibertsitatea
BCAM - Basque Center for Applied Mathematics
petnapet@gmail.com

Resumen: El objetivo de este trabajo no es otro que presentar, a modo introductorio, un resultado de dominación *sparse* puntual para operadores de Calderón-Zygmund. Este resultado se encuadra dentro de una teoría más amplia que se ha desarrollado, y, de hecho, aún sigue desarrollándose, en los últimos años: la teoría de dominación *sparse*, cuya filosofía consiste en controlar operadores clásicos en análisis armónico por operadores diádicos más sencillos de manejar a la hora de obtener desigualdades con pesos.

Abstract: The purpose of this paper is to introduce a pointwise sparse domination result for Calderón-Zygmund operators. This result can be regarded in a wider framework that has blossomed in the last years, the so-called sparse domination theory, that consists in dominating classic operators in harmonic analysis by dyadic operators that are easier to handle to obtain weighted estimates.

Palabras clave: pesos A_p, operador maximal de Hardy-Littlewood, operadores de Calderón-Zygmund, análisis diádico, operadores *sparse*.

MSC2010: 42B20, 42B25.

Recibido: 30 de noviembre de 2017.
Aceptado: 13 de febrero de 2018.

Agradecimientos: Querría expresar mi agradecimiento a mi director de tesis, Carlos Pérez Moreno, por su continuo estímulo en mi labor investigadora y por aquella escuela Santaló que organizó en el año 2014, que incluyó un curso del profesor A. Lerner sobre dominación *sparse*, el cual me hizo comenzar a interesarme en dicho tema. También me gustaría dar las gracias a Javier Martínez Perales y a los revisores por sus observaciones y sugerencias.

Referencia: Rivera-Ríos, Israel P. «Dominación *sparse* y el teorema A_2». En: *TEMat*, 2 (2018), págs. 53-65. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p53/.

1. Introducción. Desigualdades con pesos y el operador maximal de Hardy-Littlewood

El objetivo fundamental de este trabajo es presentar un caso particular de dominación *sparse*, el de los operadores de Calderón-Zygmund. En los últimos años este tipo de resultados han tenido un rol fundamental en la teoría de pesos, dentro de la cual han permitido obtener nuevos resultados y simplificar las pruebas de resultados ya conocidos. Para el lector que no esté familiarizado con el tema, las líneas anteriores deben resultar algo incomprensibles. Vamos, por tanto, a empezar desde el principio.

Recordamos que dada una función $f \in L^1_{\text{loc}}(\mathbb{R}^n)$, es decir, una función cuya integral es integrable Lebesgue en cualquier conjunto acotado medible, el operador maximal de Hardy-Littlewood se define como

$$Mf(x) = \sup_{Q \ni x} \frac{1}{|Q|} \int_Q |f(y)| \, \mathrm{d}y, \qquad x \in \mathbb{R}^n,$$

donde el supremo se toma sobre todos los Q a los que pertenece x. En lo que sigue, denotaremos por x_j a la j-ésima componente de $x \in \mathbb{R}^n$; cada Q será un cubo de $\mathbb{R}^n$, es decir, $Q = [a_1, a_1 + l(Q)] \times \cdots \times [a_n, a_n + l(Q)]$ donde $l(Q) > 0$ es el lado del cubo, y $|E|$ denotará la medida de Lebesgue en $\mathbb{R}^n$ del conjunto medible $E \subset \mathbb{R}^n$.

Es bien conocido que el operador maximal es acotado en $L^p(\mathbb{R}^n)$ o que es de tipo fuerte (p, p) para $1 < p < \infty$, es decir, que

$$\|Mf\|_{L^p(\mathbb{R}^n)} \leq c_n p' \|f\|_{L^p(\mathbb{R}^n)},$$

donde $\|g\|_{L^p(\mathbb{R}^n)} = \left(\int_{\mathbb{R}^n} |g(x)|^p \, \mathrm{d}x \right)^{\frac{1}{p}}$, $c_n > 0$ es una constante dimensional independiente de f y p' es el exponente conjugado de p, que se define como $p' = \frac{p}{p-1}$. En el caso $p = 1$ no es difícil ver que M no es acotado en L^1. Para ver esto en el caso $n = 1$, basta tomar $f = \chi_{[0,1]}$, es decir, la función que vale 1 en el intervalo $[0, 1]$ y 0 en los demás puntos. Pese a no ser de tipo fuerte $(1, 1)$, el operador maximal aún satisface una desigualdad de tipo débil $(1, 1)$, es decir,

$$\|Mf\|_{L^{1,\infty}(\mathbb{R}^n)} \leq c_n \|f\|_{L^1(\mathbb{R}^n)},$$

donde $\|g\|_{L^{1,\infty}(\mathbb{R}^n)} = \sup_{t>0} t \, |\{x \in \mathbb{R}^n : |g(x)| > t\}|$. Este último resultado puede encontrarse en las referencias clásicas [9, 15, 16].

Notación. En lo que sigue, y en el espíritu de las estimaciones que acabamos de presentar para el operador maximal, denotaremos por c a las constantes de acotación independientes de f. Los subíndices, si aparecen, denotarán la dependencia de los correspondientes parámetros. Por ejemplo, si c solo depende de la dimensión, denotaremos por c_n a la constante en cuestión. Si dependiese también de p, escribiríamos $c_{n,p}$. También nos tomaremos la libertad de omitir la mención a $\mathbb{R}^n$ al referirnos a $L^p(\mathbb{R}^n)$, escribiendo únicamente L^p. Procederemos de forma análoga con $L^{1,\infty}(\mathbb{R}^n)$. ◂

En los años 70, motivado por la idea de obtener resultados para cierto tipo de problemas de convergencia de series de ortogonales, Muckenhoupt [32] caracterizó la acotación en L^p con pesos del operador maximal de Hardy-Littlewood.

Definición 1. Llamaremos **peso** a toda función no negativa localmente integrable. ◂

La caracterización de Muckenhoupt fue la siguiente. Para $1 < p < \infty$ estableció que, dado un peso w,

$$\|Mf\|_{L^p(w)} \leq c_{p,n,w} \|f\|_{L^p(w)}, \tag{1}$$

donde $\|g\|_{L^p(w)} = \left(\int_{\mathbb{R}^n} |g(x)|^p w(x) \, \mathrm{d}x \right)^{\frac{1}{p}}$, si y solo si $w \in A_p$, es decir, si la constante A_p de w, definida como

$$[w]_{A_p} = \sup_{Q \subset \mathbb{R}^n} \frac{1}{|Q|} \int_Q w(x) \, \mathrm{d}x \left(\frac{1}{|Q|} \int_Q w(x)^{\frac{1}{1-p}} \, \mathrm{d}x \right)^{p-1},$$

es finita. En el caso $p = 1$, la desigualdad

$$\|Mf\|_{L^{1,\infty}(w)} \leq c_{n,w}\|f\|_{L^1(w)}, \tag{2}$$

donde $\|g\|_{L^{1,\infty}(w)} = \sup_{t>0} t\, w(\{x \in \mathbb{R}^n : |g(x)| > t\})$ con $w(E) = \int_E w(x)\,\mathrm{d}x$, se verifica si y solo si $w \in A_1$, es decir, si existe $\kappa > 0$ tal que

$$Mw(x) \leq \kappa w(x) \qquad \text{c.t.p. } x \in \mathbb{R}^n. \tag{3}$$

Llamaremos constante A_1 de w, $[w]_{A_1}$, al menor de los $\kappa > 0$ tales que (3) se verifica.

Recordamos que, por el teorema de diferenciación de Lebesgue, para toda función localmente integrable se tiene que $|f(x)| \leq Mf(x)$ en casi todo punto $x \in \mathbb{R}^n$. Teniendo esto en cuenta, lo que la condición A_1 nos dice es que, si $w \in A_1$, entonces w es «tan grande» como Mw, ya que

$$w(x) \leq Mw(x) \leq [w]_{A_1} w(x) \qquad \text{c.t.p. } x \in \mathbb{R}^n.$$

Observación 1. Llegado este punto, conviene notar que (1) y (2) contienen como caso particular a las desigualdades sin peso sin más que tomar $w = 1$. ◂

2. Operadores de Calderón-Zygmund

Desde los resultados de Muckenhoupt, multitud de autores han dedicado trabajos al estudio de desigualdades con pesos A_p y variantes de los mismos para diversos operadores. Una de las clases de operadores que ha recibido mayor atención es la de los operadores singulares. Empezamos presentando primero algunos ejemplos. Dada una función f «lo suficientemente buena» (por ejemplo, infinitamente diferenciable y con soporte compacto), definimos su **transformada de Hilbert** como

$$Hf(x) = \lim_{\varepsilon \to 0^+} \int_{|x-y|>\varepsilon} \frac{f(y)}{x-y}\,\mathrm{d}y, \qquad x \in \mathbb{R}. \tag{4}$$

Observamos que $\frac{1}{x}$ no es localmente integrable; sin embargo, tiene cierta propiedad de «cancelación», ya que $\int_{-R}^{R} \frac{1}{x}\,\mathrm{d}x = 0$ para todo $R > 0$. Asumiendo f «suficientemente buena», este hecho permite dotar de sentido la definición en (4) (ver cualquiera de los libros clásicos [9, 15, 16]). Hunt, Muckenhoupt y Wheeden [17] demostraron que la transformada de Hilbert satisface las siguientes propiedades:

1. Si $w \in A_p$, con $1 < p < \infty$, entonces,

   $$\|Hf\|_{L^p(w)} \leq c_{n,p,w}\|f\|_{L^p(w)}. \tag{5}$$

   Más aún, el recíproco también es cierto, es decir, si se verifica (5), entonces $w \in A_p$.

2. Si $w \in A_1$, entonces,

   $$\|Hf\|_{L^{1,\infty}(w)} \leq c_{n,w}\|f\|_{L^1(w)}. \tag{6}$$

Existen análogos n-dimensionales para la transformada de Hilbert, las transformadas de Riesz, que se definen de la siguiente forma: para cada f «suficientemente buena» definimos la **transformada de Riesz** j-ésima, $j = 1, 2, \ldots, n$, como

$$R_j f(x) = \lim_{\varepsilon \to 0} \int_{|x-y|>\varepsilon} \frac{x_j - y_j}{|x-y|^{n+1}} f(y)\,\mathrm{d}y, \qquad x \in \mathbb{R}^n.$$

Estos operadores también satisfacen (5) y (6). En este caso, es nuevamente la cancelación de $\frac{x_j - y_j}{|x-y|^{n+1}}$ lo que permite darle sentido a la definción para funciones «buenas» [9, 15, 16]. Estos operadores son casos particulares de una clase más general, la de los operadores de Calderón-Zygmund.

Definición 2. Decimos que un operador lineal T es un **operador de Calderón-Zygmund** si existe $C_{T,2} > 0$ tal que

$$\|Tf\|_{L^2} \leq C_{T,2}\|f\|_{L^2}$$

y, además, existe una función $K\colon \mathbb{R}^n \times \mathbb{R}^n \setminus \{(x,x) : x \in \mathbb{R}^n\} \to \mathbb{R}$, es decir, una función localmente integrable fuera de la diagonal, tal que para toda función f infinitamente diferenciable y con soporte compacto, es decir, nula salvo en un conjunto compacto, tenemos que si x no está en el soporte de f, entonces

$$Tf(x) = \int_{\mathbb{R}^n} K(x,y)f(y)\,\mathrm{d}y, \qquad x \in \mathbb{R}^n.$$

Adicionalmente, K deberá satisfacer las siguientes propiedades:

1. Condición de tamaño:
$$|K(x,y)| \leq \frac{C_K}{|x-y|^n}, \qquad x \neq y.$$

2. Condición de regularidad: si $2|x-x'| \leq |x-y|$, entonces
$$|K(x,y) - K(x',y)| + |K(y,x) - K(y,x')| \leq \omega\left(\frac{|x-x'|}{|x-y|}\right)\frac{1}{|x-y|^n},$$
donde ω es un módulo de continuidad, es decir, $\omega : [0,1) \to [0,\infty)$ es una función con $\omega(0) = 0$, continua, creciente y subaditiva (esto es, tal que $\omega(a+b) \leq \omega(a) + \omega(b)$ con $a, b \in [0,1)$). Supondremos también que ω satisface la condición de Dini, es decir, que
$$\|\omega\|_{\mathrm{Dini}} = \int_0^1 \omega(t)\frac{\mathrm{d}t}{t} < \infty. \qquad \blacktriangleleft$$

Nuevamente, esta clase de operadores satisface las estimaciones (5) y (6), resultado debido en el caso fuerte a Coifman y Fefferman [3]. Además, como apuntábamos antes, tanto la transformada de Hilbert como las transformadas de Riesz encajan dentro de esta definición sin más que elegir $K(x,y) = \frac{1}{x-y}$, en el caso de la transformada de Hilbert, o $K(x,y) = \frac{x_j - y_j}{|x-y|^{n+1}}$, en el caso de las transformadas de Riesz.

3. Estimaciones cuantitativas

Hasta ahora, en todas las estimaciones con pesos que hemos visto aparecía una constante con una dependencia en el peso indeterminada. Esencialmente en la última década ha surgido un gran interés por las llamadas estimaciones cuantitativas, es decir, estimaciones en las que se establece de forma cuantitativa la dependencia de la constante A_p del peso. Los primeros resultados que se dieron en esta dirección se remontan a inicios de los años 90 y se deben a Buckley [2], que en su tesis estableció la siguiente estimación para el operador maximal de Hardy-Littlewood: si $w \in A_p$ y $1 < p < \infty$, entonces

$$\|Mf\|_{L^p(w)} \leq c_{n,p}[w]_{A_p}^{\frac{1}{p-1}}\|f\|_{L^p(w)}$$

y el exponente es el mejor posible en el sentido de que, al reemplazarlo por otro más pequeño, la desigualdad falla. En el caso $p = 1$, el resultado se sigue de la desigualdad de Fefferman-Stein [13]. Dado un peso cualquiera w, se tiene que

$$\|Mf\|_{L^{1,\infty}(w)} \leq c_n\|f\|_{L^1(Mw)},$$

de lo cual se sigue, teniendo en cuenta la definición de peso A_1, que

$$\|Mf\|_{L^{1,\infty}(w)} \leq c_n[w]_{A_1}\|f\|_{L^1(w)}.$$

Buckley también estableció una estimación para operadores singulares, pero no era la mejor posible. En cualquier caso, sus resultados no recibieron inicialmente demasiada atención. En 2001, Astala, Iwaniec y Saksman [1] redujeron la posibilidad de obtener una automejora de la integrabilidad de las derivadas de

la ecuación de Beltrami a probar la dependencia lineal en la constante A_2 de la transformada de Beurling. En otras palabras, si B es la transformada de Beurling, las soluciones de la ecuación de Beltrami tendrían la citada automejora en caso de verificarse la siguiente estimación:

$$\|Bf\|_{L^2(w)} \leq c_{n,2,B}[w]_{A_2}\|f\|_{L^2(w)}, \qquad w \in A_2. \tag{7}$$

Petermichl y Volberg [36] demostraron que, efectivamente, (7) se verifica. No mucho después, Petermichl obtuvo resultados análogos para la transformada de Hilbert y las de Riesz [34, 35], que, combinados con un resultado de extrapolación [8], permitían obtener la siguiente estimación:

$$\|Tf\|_{L^p(w)} \leq c_{n,p,T}[w]_{A_p}^{\max\left\{1,\frac{1}{p-1}\right\}}\|f\|_{L^p(w)}, \qquad w \in A_p, \tag{8}$$

donde T es la transformada de Hilbert o cualquiera de las transformadas de Riesz. Observamos que dicho exponente es además el mejor posible, resultado debido a Buckley [2].

Teniendo en cuenta que los operadores que hemos mencionado más arriba tenían dependencia lineal en la constante A_2, la pregunta natural, que fue conocida como conjetura A_2, era si dicha dependencia se verificaba también para todo operador de Calderón-Zygmund T, es decir, si

$$\|Tf\|_{L^2(w)} \leq c_{n,2,T}[w]_{A_2}\|f\|_{L^2(w)}, \qquad w \in A_2. \tag{9}$$

Un buen número de autores se interesó por este problema, aportando respuestas parciales o nuevas vías para atacar el problema. Sin embargo, fue Hytönen el que consiguió convertir en teorema la conjetura A_2, en un trabajo que acabó siendo publicado en *Annals of Mathematics* [18].

4. Dominación *sparse*

Alrededor de la conjetura (ya teorema) A_2 y bajo la influencia de la misma, un buen número de autores ha dedicado parte de su labor en los últimos años a abordar la cuestión de establecer distintos tipos de desigualdades cuantitativas para diversos operadores. Esto ha llevado, entre otras cosas, a un aumento del nivel de comprensión de la teoría y al desarrollo de una depurada forma de estudiar los distintos operadores reemplazándolos por objetos diádicos más manejables, en el contexto de lo que ha venido a denominarse teoría de dominación *sparse*. Para presentar el marco en el que se desarrolla dicha teoría empezaremos tomando prestadas de Lerner y Nazarov [26] algunas definiciones fundamentales.

Dado un cubo Q de $\mathbb{R}^n$ es posible construir una red de cubos diádicos de Q de la siguiente forma.

1. Definimos a la familia $\mathcal{D}_0(Q)$ como $\mathcal{D}_0(Q) = \{Q\}$.
2. La familia $\mathcal{D}_1(Q)$ es la constituida por los 2^n subcubos que se obtienen al dividir a Q en 2^n cubos iguales.
3. Inductivamente, dado $k \in \mathbb{N}$, $\mathcal{D}_{k+1}(Q)$ es la familia constituida por los $2^{(k+1)n}$ subcubos obtenidos al dividir a cada $P \in \mathcal{D}_k(Q)$ en 2^n subcubos iguales. Si $R \in \mathcal{D}_{k+1}(Q)$ está contenido en $P \in \mathcal{D}_k(Q)$ diremos que R es hijo de P y también que P es el padre de R.

Llamaremos red diádica de Q o asociada a Q a la familia

$$\mathcal{D}(Q) = \bigcup_{k=0}^{\infty} \mathcal{D}_k(Q).$$

Una propiedad interesante de $\mathcal{D}(Q)$ es que, si $P, Q \in \mathcal{D}(Q)$, entonces necesariamente $P \cap Q \in \{P, Q, \emptyset\}$. Podemos visualizar la construcción de las generaciones 0, 1 y 2 en la figura 1.

Apoyándonos en la definición anterior vamos a presentar la definición de retículo diádico, que será el ambiente natural para definir el concepto de familia *sparse*, clave para construir los llamados operadores *sparse*.

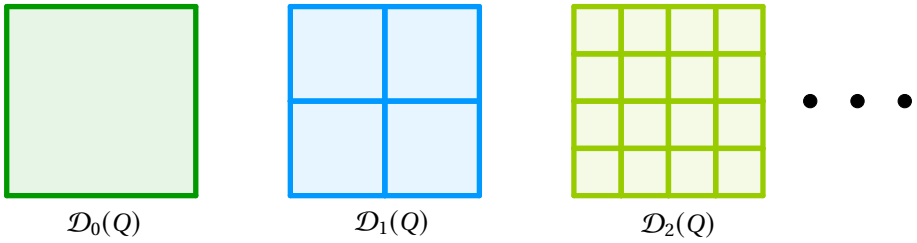

Figura 1: Generaciones 0, 1 y 2 para un cubo Q.

Definición 3. Decimos que una familia $\mathcal{D}$ de cubos de $\mathbb{R}^n$ es un **retículo diádico** si verifica las siguientes propiedades:

1. Si $Q \in \mathcal{D}$ entonces todos sus descendientes diádicos están en $\mathcal{D}$. En otras palabras: si $Q \in \mathcal{D}$, entonces $\mathcal{D}(Q) \subset \mathcal{D}$.
2. Si $P, Q \in \mathcal{D}$, existe un ancestro común a ambos, es decir, existe $R \in \mathcal{D}$ tal que $P, Q \in \mathcal{D}(R)$.
3. Para todo conjunto compacto $K \subset \mathbb{R}^n$ existe $Q \in \mathcal{D}$ tal que $K \subset Q$. ◂

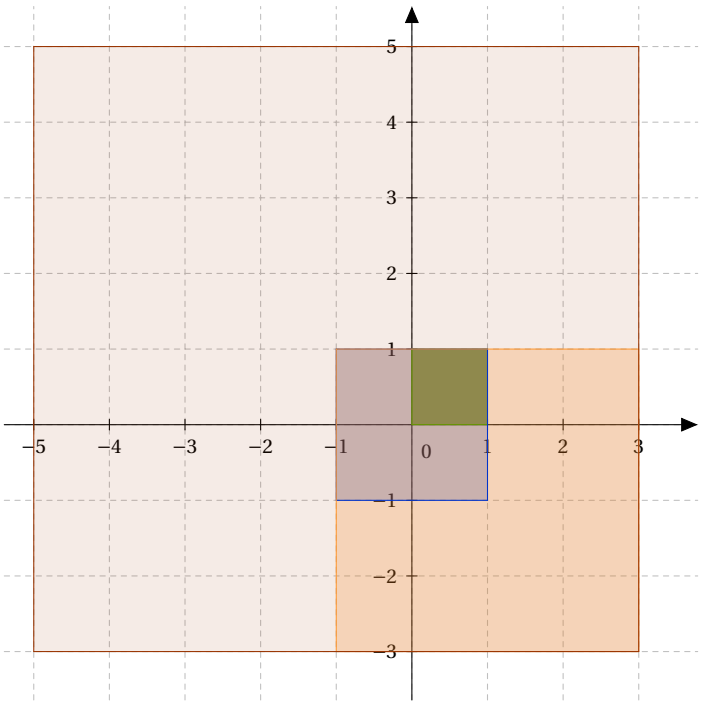

Figura 2: Sucesión de cubos en $\mathbb{R}^2$ adecuada para construir un retículo diádico.

Observación 2. Un método para construir un retículo diádico es el siguiente. Partiendo de un cubo Q_0, consideramos una sucesión de cubos $\{Q_j\}_{j=0}^{\infty}$ de manera que para cada $j > 0$ se tiene que Q_j tiene un vértice común con Q_{j-1} y $l(Q_j) = 2l(Q_{j-1})$ y, adicionalmente, $\mathbb{R}^n = \bigcup_{j=0}^{\infty} Q_j$ (ver figura 2). Para dicha sucesión es sencillo ver que

$$\mathcal{D} = \bigcup_{j=0}^{\infty} \mathcal{D}(Q_j)$$

es un retículo diádico. ◂

Llegados a este punto estamos en disposición de presentar la definición de familia *sparse* (que en castellano vendría a traducirse como familia dispersa).

Definición 4. Sea $\mathcal{D}$ un retículo diádico. Sea $\eta \in (0,1)$. Decimos que una familia $\mathcal{S} \subset \mathcal{D}$ es ***η-sparse*** si

1. Para cada $Q \in \mathcal{S}$ existe un subconjunto medible $E_Q \subset Q$ tal que
$$\eta|Q| \leq |E_Q|.$$
2. Los conjuntos E_Q son disjuntos dos a dos. ◂

Un primer ejemplo de familia *sparse* es la familia de intervalos $\{I_k\}_{k=0}^{\infty}$ con $I_k = [0, 2^{-k}]$. En este caso basta con tomar $E_k = I_k \setminus I_{k+1}$.

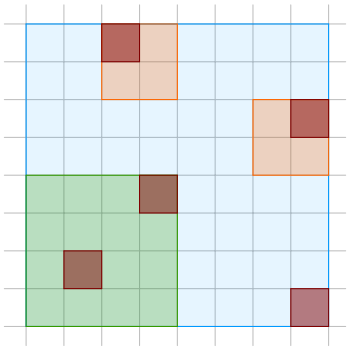

Figura 3: Ejemplo de familia $\frac{1}{2}$-*sparse*.

En la figura 3 podemos ver otro ejemplo de familia $\frac{1}{2}$-*sparse*. Para comprobar esto basta con tomar $E_Q = Q \setminus \cup_{P \in \mathcal{S}: P \subsetneq Q} P$ o simplemente un subconjunto de medida $\frac{1}{2}|Q|$ en el caso en que el cubo Q no tenga ningún subcubo.

En el siguiente teorema presentamos, por fin, uno de los resultados paradigmáticos dentro de lo que se conoce como teoría de dominación *sparse*, la dominación *sparse* puntual para operadores de Calderón-Zygmund.

Teorema 1. *Sea T un operador de Calderón-Zygmund. Sea $\varepsilon \in (0,1)$. Para cada función f integrable con soporte compacto, existen 3^n retículos diádicos $\mathcal{D}_j$ y 3^n familias $\frac{1-\varepsilon}{3^n}$-*sparse $\mathcal{S}_j \subset \mathcal{D}_j$ *tales que*

$$|Tf(x)| \leq \frac{c_n c_T}{\varepsilon} \sum_{j=1}^{3^n} A_{\mathcal{S}_j}|f|(x) \qquad \text{c.t.p. } x \in \mathbb{R}^n,$$

donde

$$A_{\mathcal{S}} f(x) = \sum_{Q \in \mathcal{S}} \frac{1}{|Q|} \int_Q f(y)\,\mathrm{d}y\, \chi_Q(x), \qquad x \in \mathbb{R}^n,$$

siendo $A_{\mathcal{S}}$ el operador al que conocemos como operador sparse *y $c_T = C_{T,2} + C_K + \|\omega\|_{Dini}$ (ver definición 2).*

Observación 3. Puede parecer un problema el hecho de que las familias *sparse* elegidas dependan de f; sin embargo, a efectos prácticos, dicha circunstancia no restringe la aplicabilidad del resultado, dado que, como veremos algo más adelante, este tipo de dominación se utilizará para obtener estimaciones independientes de la familia *sparse*.

Por otra parte, otra observación interesante [33] es que, fijado un cubo de una familia *sparse*, el conjunto de puntos de dicho cubo que están contenidos en una cantidad infinita de cubos de la familia tiene medida cero. Esta propiedad hace posible que los operadores *sparse* estén bien definidos para funciones integrables. ◂

El teorema 1 fue obtenido de forma independiente por Conde-Alonso y Rey [5] y Lerner y Nazarov [26] para operadores de Calderón-Zygmund con módulo de continuidad satisfaciendo una condición algo menos general que la condición de Dini en la definición 2. Más tarde, Lacey [21] extendió el resultado a operadores

satisfaciendo la condición de Dini. A este trabajo de Lacey le siguió otro de Hytönen, Roncal y Tapiola [20] en el que se obtenía la versión cuantitativa con la constante c_T que hemos presentado aquí. Finalmente, Lerner [23] obtuvo una prueba sumamente elegante de dicho resultado cuantitativo, basada en el control de un operador de tipo maximal asociado a T. Dicha técnica ha sido aplicada exitosamente en otros contextos, como el matricial [33], el de los conmutadores [30] o incluso en sentido de dominación «bilineal» a integrales singulares «*rough*» [24] (ver el artículo de Conde-Alonso, Culiuc, Di Plinio y Ou [4] para la prueba original de dicho resultado y la sección 6 para algunos detalles adicionales) o a los conmutadores de las mismas [37]. De cara a introducirse al análisis diádico y a la teoría de dominación *sparse*, recomendamos al lector la lectura del estudio de Lerner y Nazarov [26] y las notas de Hytönen [19].

De alguna manera, los resultados de dominación *sparse* pueden considerarse como una actualización del principio de Calderón-Zygmund. Dicho principio afirmaba que «para cada operador singular debería existir un operador maximal adecuado que lo controlase en algún sentido». Por ejemplo, si T es un operador de Calderón-Zygmund, Coifman y Fefferman [3] establecieron, esencialmente, que, si $w \in A_q$ para algún $q \geq 1$, entonces

$$\|Tf\|_{L^p(w)} \leq c_{n,T,p,w} \|Mf\|_{L^p(w)}, \qquad 0 < p < \infty.$$

A la vista del teorema 1, la actualización de este principio podría enunciarse del siguiente modo: «para cada operador singular existe un operador *sparse* adecuado que controla a dicho operador en algún sentido».

5. Una prueba simple del teorema A_2

Para ilustrar el uso de las técnicas de dominación *sparse* vamos a presentar una prueba del teorema A_2. Para dicho fin necesitaremos un resultado previo que tomamos prestado de Lerner y Nazarov [26, theorem 15.1].

Teorema 2. *Sean $\mathcal{D}$ un retículo diádico y w un peso. Definimos el operador maximal $M_w^{\mathcal{D}}$ como*

$$M_w^{\mathcal{D}} f(x) = \sup_{Q \in \mathcal{D} \,:\, Q \ni x} \frac{1}{w(Q)} \int_Q |f(y)| w(y)\, \mathrm{d}y.$$

Entonces:

1. *Si $1 < p < \infty$,*
$$\|M_w^{\mathcal{D}} f\|_{L^p(w)} \leq p' \|f\|_{L^p(w)}.$$
2. *Si $p = 1$,*
$$\|M_w^{\mathcal{D}} f\|_{L^{1,\infty}} \leq \|f\|_{L^1(w)}.$$

El resultado que acabamos de presentar nos dice, básicamente, que el operador maximal diádico con respecto a cierto peso, que en nuestro caso va a ser un peso A_2, es acotado en L^p con constante independiente del peso.

Otro ingrediente fundamental de la prueba será la expresión de la norma por dualidad. En el caso particular $p = 2$, si $g \in L^2(w)$, entonces,

$$\|g\|_{L^2(w)} = \sup_{\|h\|_{L^2(w)}=1} \left| \int_{\mathbb{R}^n} g(x) h(x) w(x)\, \mathrm{d}x \right|.$$

Con estos resultados a nuestra disposición ya podemos probar el teorema A_2. Empezamos observando que, en virtud del teorema 1,

$$\|Tf\|_{L^2(w)} \leq c_n c_T \sum_{j=1}^{3^n} \|A_{\mathcal{S}_j}(|f|)\|_{L^2(w)}.$$

Por tanto, basta con establecer la estimación para operadores *sparse*. Recogemos dicha estimación en el siguiente lema.

Lema 3. *Sean $\mathcal{S}$ una familia η-*sparse *y $w \in A_2$. Entonces,*

$$\|A_{\mathcal{S}} f\|_{L^2(w)} \leq \frac{4}{\eta}[w]_{A_2}\|f\|_{L^2(w)}.$$

Demostración. Expresando la norma por dualidad tenemos que

$$\|A_{\mathcal{S}} f\|_{L^2(w)} = \sup_{\|h\|_{L^2(w)}=1} \left| \int_{\mathbb{R}^n} A_{\mathcal{S}} f(x) h(x) w(x)\, \mathrm{d}x \right|, \tag{10}$$

de manera que basta con acotar $\left| \int_{\mathbb{R}^n} A_{\mathcal{S}} f(x) h(x) w(x)\, \mathrm{d}x \right|$. Observamos que

$$\left| \int_{\mathbb{R}^n} A_{\mathcal{S}} f(x) h(x)\, \mathrm{d}x \right| \leq \int_{\mathbb{R}^n} A_{\mathcal{S}}(|f|)(x)|h(x)| w(x)\, \mathrm{d}x,$$

lo cual nos permite asumir que $f, h \geq 0$. Hecha esta reducción y llamando $\sigma = w^{-1}$, procedemos como sigue:

$$\begin{aligned}
\int_{\mathbb{R}^n} A_{\mathcal{S}} f(x) h(x) w(x)\, \mathrm{d}x &= \sum_{Q\in\mathcal{S}} \left(\frac{1}{|Q|} \int_Q f(y)\, \mathrm{d}y \right) \left(\int_Q h(y) w(y)\, \mathrm{d}y \right) \\
&\leq \sum_{Q\in\mathcal{S}} \left(\frac{1}{\sigma(Q)} \int_Q \frac{f(y)}{\sigma(y)} \sigma(y)\, \mathrm{d}y \right) \left(\frac{1}{w(Q)} \int_Q h(y) w(y)\, \mathrm{d}y \right) \frac{w(Q)\sigma(Q)}{|Q|} \\
&\leq \sup_Q \left\{ \frac{w(Q)\sigma(Q)}{|Q|^2} \right\} \sum_{Q\in\mathcal{S}} \left(\frac{1}{\sigma(Q)} \int_Q \frac{f(y)}{\sigma(y)} \sigma(y)\, \mathrm{d}y \right) \left(\frac{1}{w(Q)} \int_Q h(y) w(y)\, \mathrm{d}y \right) |Q|.
\end{aligned}$$

Observamos que el supremo que aparece en el último paso no es otra cosa que la constante A_2, de manera que bastará con obtener una estimación de la suma independiente de dicha constante. Por la definición del operador maximal diádico respecto a un peso, está claro que

$$\left(\frac{1}{\sigma(Q)} \int_Q \frac{f(y)}{\sigma(y)} \sigma(y)\, \mathrm{d}y \right) \leq \inf_{z\in Q} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(z)$$

y también que

$$\left(\frac{1}{w(Q)} \int_Q h(y) w(y)\, \mathrm{d}y \right) \leq \inf_{z\in Q} M_w^{\mathcal{D}}(h)(z).$$

Por otra parte, como $\mathcal{S}$ es η-*sparse*, sabemos que para cada $Q \in \mathcal{S}$ existe un subconjunto $E_Q \subseteq Q$ tal que dichos conjuntos E_Q son disjuntos dos a dos y, además, $|Q| \leq \frac{1}{\eta}|E_Q|$. Teniendo todo esto en cuenta,

$$\begin{aligned}
&[w]_{A_2} \sum_{Q\in\mathcal{S}} \left(\frac{1}{\sigma(Q)} \int_Q \frac{f(y)}{\sigma(y)} \sigma(y)\, \mathrm{d}y \right) \left(\frac{1}{w(Q)} \int_Q h(y) w(y)\, \mathrm{d}y \right) |Q| \\
&\leq [w]_{A_2} \frac{1}{\eta} \sum_{Q\in\mathcal{S}} \left(\inf_{z\in Q} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(z) \right) \left(\inf_{z\in Q} M_w^{\mathcal{D}}(h)(z) \right) |E_Q| \\
&\leq [w]_{A_2} \frac{1}{\eta} \sum_{Q\in\mathcal{S}} \int_{E_Q} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(x) M_w^{\mathcal{D}}(h)(x)\, \mathrm{d}x.
\end{aligned}$$

En este punto hacemos uso de una propiedad clave de los conjuntos E_Q, el hecho de que son disjuntos dos a dos. Dicha propiedad nos permite continuar de la siguiente forma:

$$\begin{aligned}
&\frac{1}{\eta}[w]_{A_2} \sum_{Q\in\mathcal{S}} \int_{E_Q} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(x) M_w^{\mathcal{D}}(h)(x)\, \mathrm{d}x = \frac{1}{\eta}[w]_{A_2} \int_{\cup_{Q\in\mathcal{S}} E_Q} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(x) M_w^{\mathcal{D}}(h)(x)\, \mathrm{d}x \\
&\leq \frac{1}{\eta}[w]_{A_2} \int_{\mathbb{R}^n} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(x) M_w^{\mathcal{D}}(h)(x)\, \mathrm{d}x = \frac{1}{\eta}[w]_{A_2} \int_{\mathbb{R}^n} M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right)(x) M_w^{\mathcal{D}}(h)(x) w(x)^{\frac{1}{2}} \sigma(x)^{\frac{1}{2}}\, \mathrm{d}x \\
&\leq \frac{1}{\eta}[w]_{A_2} \left\| M_\sigma^{\mathcal{D}} \left(\frac{f}{\sigma} \right) \right\|_{L^2(\sigma)} \|M_w^{\mathcal{D}}(h)\|_{L^2(w)} \leq \frac{4}{\eta}[w]_{A_2} \left\| \frac{f}{\sigma} \right\|_{L^2(\sigma)} \|h\|_{L^2(w)} = \frac{4}{\eta}[w]_{A_2} \|f\|_{L^2(w)} \|h\|_{L^2(w)},
\end{aligned}$$

donde la última desigualdad es consecuencia directa del teorema 2 y la última identidad se sigue de que $\left(\frac{|f|}{\sigma}\right)^2 \sigma = |f|^2 w$. En resumen, hemos probado que

$$\left| \int_{\mathbb{R}^n} A_{\mathcal{S}} f(x) h(x) w(x)\, \mathrm{d}x \right| \leq \frac{4}{\eta} [w]_{A_2} \|f\|_{L^2(w)} \|h\|_{L^2(w)},$$

de manera que, tomando supremo cuando $\|h\|_{L^2(w)} = 1$ y teniendo en cuenta (10), obtenemos la estimación deseada. ∎

Observación 4. Contrariamente a lo que podría parecer, la estimación establecida en el lema 3 es anterior a la prueba del teorema A_2 y se debe a Cruz-Uribe, Martell y Pérez [6]. En dicho trabajo, los autores reducían la conjetura A_2 para operadores singulares con cierta regularidad a operadores *sparse*. Fue sin embargo Lerner [22] el primero en conectar la dominación *sparse* con los operadores de Calderón-Zygmund, obteniendo así una nueva prueba del teorema A_2. El resultado de dominación *sparse* que obtuvo fue un resultado en norma, que en el caso particular que nos ocupa se enuncia como sigue:

$$\|Tf\|_{L^2(w)} \leq c \sup \|A_{\mathcal{S}} f\|_{L^2(w)},$$

donde el supremo se toma sobre todas las familias *sparse* $\mathcal{S}$ contenidas en todos los retículos diádicos posibles. Este resultado es el precursor de la dominación *sparse* que presentamos en la sección 4 y probablemente el desencadenante que llevó al desarrollo de dicha teoría. ◂

6. Más resultados basados en la dominación *sparse*

Sea $\Omega \in L^\infty(\mathbb{S}^{n-1})$, donde $\mathbb{S}^{n-1}$ es la esfera $n-1$ dimensional. Por ejemplo, $\mathbb{S}^1$ es la circunferencia en $\mathbb{R}^2$ y $\mathbb{S}^2$ es la esfera (hueca) en $\mathbb{R}^3$. Asumamos adicionalmente que $\int_{\mathbb{S}^{n-1}} \Omega(\theta)\, \mathrm{d}\theta = 0$. Bajo estas hipótesis, para f «suficientemente buena», el operador T_Ω definido como

$$T_\Omega f(x) = \lim_{\varepsilon \to 0^+} \int_{|x-y|>\varepsilon} \frac{\Omega\left(\frac{x-y}{|x-y|}\right)}{|x-y|^n} f(y)\, \mathrm{d}y$$

tiene sentido [9, 15]. Las transformadas de Riesz y de Hilbert son casos particulares de esta clase de operadores. T_Ω satisface las mismas propiedades de acotación que los operadores de Calderón-Zygmund. Es de tipo fuerte (p,p) (tanto para el caso sin pesos [9] como para el caso con pesos [10]) y de tipo débil $(1,1)$ (tanto para el caso sin pesos [38] como para el caso con pesos [11, 12]). No obstante, este tipo de operador es más difícil de tratar que los operadores de Calderón-Zygmund, ya que, a diferencia de lo que ocurre con estos últimos, $K(x,y) = \frac{\Omega\left(\frac{x-y}{|x-y|}\right)}{|x-y|^n}$ no satisface ninguna condición de regularidad. Es por esto que en inglés se denomina a estos operadores como «*rough*».

Conde-Alonso, Culiuc, Di Plinio y Ou [4] obtuvieron una dominación *sparse* en el sentido bilineal (ver el trabajo de Lerner [24] para una prueba alternativa). El resultado es el siguiente: para cada $1 < r < \infty$, dadas f con soporte compacto e integrable y g «suficientemente buena», existen 3^n retículos diádicos $\mathcal{D}_j$ y 3^n familias *sparse* $\mathcal{S}_j \subset \mathcal{D}_j$ tales que

$$\left| \int_{\mathbb{R}^n} T_\Omega(f)(x) g(x)\, \mathrm{d}x \right| \leq c_n \|\Omega\|_{L^\infty(\mathbb{S}^{n-1})} r' \sum_{j=1}^{3^n} \sum_{Q \in \mathcal{S}_j} \left(\frac{1}{|Q|} \int_Q |f(x)|\, \mathrm{d}x \right) \left(\frac{1}{|Q|} \int_Q |g(x)|^r\, \mathrm{d}x \right)^{\frac{1}{r}} |Q|.$$

En la práctica, este tipo de resultado permite recuperar la gran mayoría de los resultados que se pueden obtener utilizando la dominación puntual, ya que muchos de ellos (como, por ejemplo, el teorema A_2 cuya prueba vimos en la sección anterior) se basan en el uso de la norma por dualidad. Sin embargo, la presencia del promedio L^r y de r' en la estimación la hacen más «imprecisa» que el análogo para operadores de Calderón-Zygmund que se sigue trivialmente del teorema 1:

$$\left| \int_{\mathbb{R}^n} Tf(x) g(x)\, \mathrm{d}x \right| \leq c_n c_T \sum_{j=1}^{3^n} \sum_{Q \in \mathcal{S}_j} \left(\frac{1}{|Q|} \int_Q |f(x)|\, \mathrm{d}x \right) \left(\frac{1}{|Q|} \int_Q |g(x)|\, \mathrm{d}x \right) |Q|.$$

En el siguiente teorema presentamos una serie de estimaciones que, en algunos casos, admiten nuevas pruebas utilizando resultados de dominación *sparse*, mientras que, en otros casos, están completamente basados en dichas técnicas. Además, contrastaremos los casos de los operadores de Calderón-Zygmund y los operadores T_Ω que acabamos de presentar. Como veremos a continuación, la mencionada «imprecisión» de la dominación *sparse* disponible para estos últimos repercute en algunos de los resultados que se pueden obtener utilizándola como ingrediente.

Teorema 4. *Sea $\Omega \in L^\infty(\mathbb{S}^{n-1})$ tal que $\int_{\mathbb{S}^{n-1}} \Omega(\theta)\,\mathrm{d}\theta = 0$. Sea T un operador de Calderón-Zygmund. Entonces:*

1. *Si $1 < p < \infty$ y $w \in A_p$, entonces*

$$\|T_\Omega f\|_{L^p(w)} \leq c_{n,p}\|\Omega\|_{L^\infty(\mathbb{S}^{n-1})}[w]_{A_p}^{p'}\|f\|_{L^p(w)}.$$

2. *Si $1 \leq q < p < \infty$ y $w \in A_q$, entonces*

$$\|Tf\|_{L^p(w)} \leq c_{n,T,p,q}[w]_{A_q}\|f\|_{L^p(w)} \quad y$$
$$\|T_\Omega f\|_{L^p(w)} \leq c_{n,p,q}\|\Omega\|_{L^\infty(\mathbb{S}^{n-1})}[w]_{A_q}\|f\|_{L^p(w)}.$$

3. *Si $1 \leq p < \infty$ y $w \in A_q$ para cualquier $1 < q < \infty$, entonces*

$$\|Tf\|_{L^p(w)} \leq c_{n,T,p,q}[w]_{A_q}\|Mf\|_{L^p(w)} \quad y$$
$$\|T_\Omega f\|_{L^p(w)} \leq c_{n,p,q}\|\Omega\|_{L^\infty(\mathbb{S}^{n-1})}[w]_{A_q}^2\|Mf\|_{L^p(w)}.$$

4. *Para $p = 1$, si $w \in A_1$, entonces*

$$\|Tf\|_{L^{1,\infty}(w)} \leq c_{n,T}[w]_{A_1}\log(e + [w]_{A_1})\|f\|_{L^1(w)} \quad y$$
$$\|T_\Omega f\|_{L^{1,\infty}(w)} \leq c_{n,p,q}\|\Omega\|_{L^\infty(\mathbb{S}^{n-1})}[w]_{A_1}^2\log(e + [w]_{A_1})\|f\|_{L^1(w)}$$

   y en el caso de T, además, la dependencia es la mejor posible.

En el caso T_Ω, todas las estimaciones del teorema que acabamos de enunciar fueron obtenidas por Li, Pérez, Rivera-Ríos y Roncal [31]. La estimación en el apartado 1 es la mejor hasta la fecha, si bien hay ciertos indicios (por ejemplo, los resultados de Lerner [25]) de que, en el caso $p = 2$, la dependencia debería ser lineal en lugar de cuadrática. En el caso de los operadores de Calderón-Zygmund, las estimacionenes de los apartados 2 y 3 pueden obtenerse empleando esencialmente la misma prueba que presentan Li *et al.* [31], aunque son anteriores a dicho trabajo. Finalmente, en cuanto al apartado 4, en el caso de los operadores de Calderón-Zygmund la estimación superior fue obtenida por Lerner, Ombrosi y Pérez [28, 29]. Domingo-Salazar, Lacey y Rey [7] presentaron una prueba basada en la dominación *sparse* (ver también el artículo de Frey y Nieraeth [14]). El hecho de que la dependencia en la constante A_1 es la mejor posible es un resultado muy reciente debido a Lerner, Nazarov y Ombrosi [27]. En el caso de los operadores *rough* la desigualdad en el apartado 4 fue obtenida por Li *et al.* [31]. Finalmente, cabe reseñar que, en el caso de los apartados 3 y 4, Li *et al.* [31] conjeturan que la dependencia de la correspondiente constante A_p es la misma que la que se verifica para los operadores de Calderón-Zygmund.

Referencias

[1] Astala, Kari; Iwaniec, Tadeusz y Saksman, Eero. «Beltrami operators in the plane». En: *Duke Mathematical Journal* 107.1 (2001), págs. 27-56. issn: 0012-7094. https://doi.org/10.1215/S0012-7094-01-10713-8.

[2] Buckley, Stephen M. *Harmonic analysis on weighted spaces*. Tesis doct. The University of Chicago, 1990.

[3] Coifman, Ralph R. y Fefferman, Charles. «Weighted norm inequalities for maximal functions and singular integrals». En: *Studia Mathematica* 51 (1974), págs. 241-250. issn: 0039-3223. https://doi.org/10.4064/sm-51-3-241-250.

[4] Conde-Alonso, José M.; Culiuc, Amalia; Di Plinio, Francesco y Ou, Yumeng. «A sparse domination principle for rough singular integrals». En: *Analysis & PDE* 10.5 (2017), págs. 1255-1284. issn: 2157-5045. https://doi.org/10.2140/apde.2017.10.1255.

[5] Conde-Alonso, José M. y Rey, Guillermo. «A pointwise estimate for positive dyadic shifts and some applications». En: *Mathematische Annalen* 365.3-4 (2016), págs. 1111-1135. issn: 0025-5831. url: 10.1007/s00208-015-1320-y.

[6] Cruz-Uribe, David; Martell, José M. y Pérez, Carlos. «Sharp weighted estimates for classical operators». En: *Advances in Mathematics* 229.1 (2012), págs. 408-441. issn: 0001-8708. url: 10.1016/j.aim.2011.08.013.

[7] Domingo-Salazar, Carlos; Lacey, Michael y Rey, Guillermo. «Borderline weak-type estimates for singular integrals and square functions». En: *Bulletin of the London Mathematical Society* 48.1 (2016), págs. 63-73. issn: 0024-6093. https://doi.org/10.1112/blms/bdv090.

[8] Dragičević, Oliver; Grafakos, Loukas; Pereyra, M. Cristina y Petermichl, Stefanie. «Extrapolation and sharp norm estimates for classical operators on weighted Lebesgue spaces». En: *Publicacions Matemàtiques* 49.1 (2005), págs. 73-91. issn: 0214-1493. https://doi.org/10.5565/PUBLMAT_49105_03.

[9] Duoandikoetxea, Javier. *Fourier analysis*. Trad. del original de 1995 en castellano por Cruz-Uribe, David. Vol. 29. Graduate Studies in Mathematics. American Mathematical Society, 2001, págs. xviii+222. isbn: 978-0-8218-2172-5.

[10] Duoandikoetxea, Javier y Rubio de Francia, José L. «Maximal and singular integral operators via Fourier transform estimates». En: *Inventiones Mathematicae* 84.3 (1986), págs. 541-561. issn: 0020-9910. https://doi.org/10.1007/BF01388746.

[11] Fan, Dashan y Sato, Shuichi. «Weak type (1, 1) estimates for Marcinkiewicz integrals with rough kernels». En: *The Tohoku Mathematical Journal. Second Series* 53.2 (2001), págs. 265-284. issn: 0040-8735. https://doi.org/10.2748/tmj/1178207481.

[12] Fan, Dashan y Sato, Shuichi. «Weighted weak type (1, 1) estimates for singular integrals and Littlewood-Paley functions». En: *Studia Mathematica* 163.2 (2004), págs. 119-136. issn: 0039-3223. https://doi.org/10.4064/sm163-2-2.

[13] Fefferman, Charles y Stein, Elias M. «Some maximal inequalities». En: *American Journal of Mathematics* 93 (1971), págs. 107-115. issn: 0002-9327. https://doi.org/10.2307/2373450.

[14] Frey, Dorothy y Nieraeth, Bas. «Weak and strong type $A_1 - A_\infty$ estimates for sparsely dominated operators». En: *Journal of Geometric Analysis* (2018). issn: 1559-002X. https://doi.org/10.1007/s12220-018-9989-2.

[15] García-Cuerva, José y Rubio de Francia, José L. *Weighted norm inequalities and related topics*. Vol. 116. North-Holland Mathematics Studies. Notas de Matemática 104. North-Holland Publishing Co., 1985, págs. x+604. isbn: 978-0-444-87804-5.

[16] Grafakos, Loukas. *Classical Fourier analysis*. 3.ª ed. Vol. 249. Graduate Texts in Mathematics. Springer, 2014, págs. xviii+638. https://doi.org/10.1007/978-1-4939-1194-3.

[17] Hunt, Richard; Muckenhoupt, Benjamin y Wheeden, Richard. «Weighted norm inequalities for the conjugate function and Hilbert transform». En: *Transactions of the American Mathematical Society* 176 (1973), págs. 227-251. issn: 0002-9947. https://doi.org/10.2307/1996205.

[18] Hytönen, Tuomas P. «The sharp weighted bound for general Calderón-Zygmund operators». En: *Annals of Mathematics. Second Series* 175.3 (2012), págs. 1473-1506. issn: 0003-486X. https://doi.org/10.4007/annals.2012.175.3.9.

[19] Hytönen, Tuomas P. *Dyadic analysis and weights*. Apuntes de un curso en la Universidad de Helsinki. 2017. url: https://wiki.helsinki.fi/download/attachments/213996485/dyadic.pdf.

[20] Hytönen, Tuomas P.; Roncal, Luz y Tapiola, Olli. «Quantitative weighted estimates for rough homogeneous singular integrals». En: *Israel Journal of Mathematics* 218.1 (2017), págs. 133-164. issn: 0021-2172. url: 10.1007/s11856-017-1462-6.

[21] Lacey, Michael T. «An elementary proof of the A_2 bound». En: *Israel Journal of Mathematics* 217.1 (2017), págs. 181-195. issn: 0021-2172. url: 10.1007/s11856-017-1442-x.

[22] Lerner, Andrei K. «A simple proof of the A_2 conjecture». En: *International Mathematics Research Notices. IMRN* 14 (2013), págs. 3159-3170. issn: 1073-7928. url: 10.1093/imrn/rns145.

[23] Lerner, Andrei K. «On pointwise estimates involving sparse operators». En: *New York Journal of Mathematics* 22 (2016), págs. 341-349. issn: 1076-9803. url: http://nyjm.albany.edu/j/2016/22_341.html.

[24] Lerner, Andrei K. «A weak type estimate for rough singular integrals». En: *ArXiv e-prints* (mayo de 2017). arXiv: 1705.07397 [math.CA].

[25] Lerner, Andrei K. «A note on weighted bounds for rough singular integrals». En: *Comptes Rendus Mathematique* 356.1 (2018). https://doi.org/10.1016/j.crma.2017.11.016.

[26] Lerner, Andrei K. y Nazarov, Fedor. «Intuitive dyadic calculus: the basics». En: *Expositiones Mathematicae* (2018). https://doi.org/10.1016/j.exmath.2018.01.001.

[27] Lerner, Andrei K.; Nazarov, Fedor y Ombrosi, Sheldy. «On the sharp upper bound related to the weak Muckenhoupt-Wheeden conjecture». En: *ArXiv e-prints* (oct. de 2017). arXiv: 1710.07700 [math.CA].

[28] Lerner, Andrei K.; Ombrosi, Sheldy y Pérez, Carlos. «Sharp A_1 bounds for Calderón-Zygmund operators and the relationship with a problem of Muckenhoupt and Wheeden». En: *International Mathematics Research Notices. IMRN* 6 (2008). issn: 1073-7928. https://doi.org/10.1093/imrn/rnm161.

[29] Lerner, Andrei K.; Ombrosi, Sheldy y Pérez, Carlos. «A_1 bounds for Calderón-Zygmund operators related to a problem of Muckenhoupt and Wheeden». En: *Mathematical Research Letters* 16.1 (2009), págs. 149-156. issn: 1073-2780. https://doi.org/10.4310/MRL.2009.v16.n1.a14.

[30] Lerner, Andrei K.; Ombrosi, Sheldy y Rivera-Ríos, Israel P. «On pointwise and weighted estimates for commutators of Calderón-Zygmund operators». En: *Advances in Mathematics* 319 (2017), págs. 153-181. issn: 0001-8708. https://doi.org/10.1016/j.aim.2017.08.022.

[31] Li, Kangwei; Pérez, Carlos; Rivera-Ríos, Israel P. y Roncal, Luz. «Weighted norm inequalities for rough singular integral operators». En: *ArXiv e-prints* (ene. de 2017). arXiv: 1701.05170 [math.CA].

[32] Muckenhoupt, Benjamin. «Weighted norm inequalities for the Hardy maximal function». En: *Transactions of the American Mathematical Society* 165 (1972), págs. 207-226. issn: 0002-9947. https://doi.org/10.2307/1995882.

[33] Nazarov, Fedor; Petermichl, Stefanie; Treil, Sergei y Volberg, Alexander. «Convex body domination and weighted estimates with matrix weights». En: *Advances in Mathematics* 318 (2017), págs. 279-306. issn: 0001-8708. https://doi.org/10.1016/j.aim.2017.08.001.

[34] Petermichl, Stefanie. «The sharp bound for the Hilbert transform on weighted Lebesgue spaces in terms of the classical A_p characteristic». En: *American Journal of Mathematics* 129.5 (2007), págs. 1355-1375. issn: 0002-9327. https://doi.org/10.1353/ajm.2007.0036.

[35] Petermichl, Stefanie. «The sharp weighted bound for the Riesz transforms». En: *Proceedings of the American Mathematical Society* 136.4 (2008), págs. 1237-1249. issn: 0002-9939. https://doi.org/10.1090/S0002-9939-07-08934-4.

[36] Petermichl, Stefanie y Volberg, Alexander. «Heating of the Ahlfors-Beurling operator: weakly quasiregular maps on the plane are quasiregular». En: *Duke Mathematical Journal* 112.2 (2002), págs. 281-305. issn: 0012-7094. https://doi.org/10.1215/S0012-9074-02-11223-X.

[37] Rivera-Ríos, Israel P. «Improved $A_1 - A_\infty$ and related estimates for commutators of rough singular integrals». En: *ArXiv e-prints* (mayo de 2017). arXiv: 1705.09981 [math.CA].

[38] Seeger, Andreas. «Singular integral operators with rough convolution kernels». En: *Journal of the American Mathematical Society* 9.1 (1996), págs. 95-105. issn: 0894-0347. https://doi.org/10.1090/S0894-0347-96-00185-3.

TEMat

Aplicación en combinatoria de las representaciones de grupos

Gonzalo Cao Labora
Universitat Politècnica de Catalunya (UPC)
gonzalocaolabora@yahoo.es

Resumen: El objetivo de este artículo es presentar una aplicación del álgebra en la combinatoria. Trataremos la teoría algebraica de representaciones de grupos, que se utiliza en multitud de áreas de las matemáticas (geometría diferencial, análisis armónico, teoría de números…) o incluso en física teórica. Nosotros la utilizaremos en la combinatoria, asociando conceptos algebraicos con conceptos combinatorios. Esto permite probar resultados combinatorios a través de los resultados algebraicos correspondientes. En particular, usaremos la teoría presentada para probar una igualdad combinatoria.

Al igual que en muchas otras partes del álgebra, nos interesará descomponer los objetos (en este caso representaciones) en sus componentes irreducibles. Tendremos el típico resultado de existencia y unicidad y presentaremos herramientas para el cálculo práctico de una descomposición. Por último, construiremos las representaciones irreducibles del grupo simétrico $\mathcal{S}_n$, que están ligadas a objetos combinatorios.

Abstract: The main goal of this article is to introduce an algebraic application in combinatorics. We will deal with the algebraic group representation theory, used over many branches of mathematics (differential geometry, harmonic analysis, number theory...) or even theoretical physics. We will use it in the context of combinatorics, linking algebraic concepts with combinatorial concepts. This allows to prove some combinatorics results through their algebraic analogues. Specifically, we will use this theory to prove a combinatorial equality.

As in other parts of algebra, it is interesting to decompose the objects (representations) into their irreducible components. We will prove typical results about existence and uniqueness and we will present some tools to decompose representations. Finally, we will construct the irreducible representations of the symmetric group $\mathcal{S}_n$, which are closely related to combinatorial objects.

Palabras clave: representaciones de grupos, grupo simétrico, combinatoria algebraica, tablas de Young, particiones, módulos de Specht.

MSC2010: 05E10, 20C30.

Recibido: 23 de febrero de 2018.
Aceptado: 5 de julio de 2018.

Referencia: Cao Labora, Gonzalo. «Aplicación en combinatoria de las representaciones de grupos». En: *TEMat*, 2 (2018), págs. 67-83. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p67/.

1. Introducción

Un problema clásico de la combinatoria es el problema de las particiones. Una partición es una descomposición de un número natural, n, en sumas de números naturales. Por ejemplo, $2+1+1$ es una posible partición de 4, aunque la forma usual de denotarla sería $(2,1,1)$. El problema consiste en contar de cuántas maneras es posible realizar estas particiones, es decir, cuántas particiones tiene el número n. En el caso de $n=3$, lo podemos descomponer como $(1,1,1)$, como $(2,1)$, o como (3) (descomponerlo en un único sumando también es válido). A la cantidad de particiones la llamamos $p(n)$, de forma que, por ejemplo, $p(3)=3$. Es importante fijarse en que el orden no importa a la hora de hacer particiones. Como $(2,1)$ es la misma partición que $(1,2)$, las podemos ordenar siempre en orden decreciente, que será lo que haremos.

Frobenius [2] en el año 1900 demostró que las particiones están asociadas a unas representaciones (que introduciremos más adelante). Alfred Young [7-17] estudió estas representaciones durante la primera mitad del siglo xx, y se dio cuenta de la importancia de introducir diagramas para codificar las particiones. Un diagrama de Young es una colección de n recuadros, donde en cada fila ponemos la cantidad correspondiente a uno de los números de la partición. Estas filas han de estar ordenadas por tamaño y alineadas a la izquierda. Podemos ver todos los posibles diagramas de Young para $n=3$ en la figura 1.

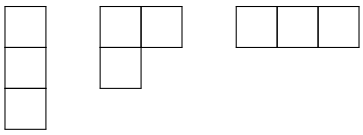

Figura 1: Diagramas de Young para $n=3$. Se corresponden con las particiones $(1,1,1)$, $(2,1)$ y (3), respectivamente.

Otros objetos interesantes en combinatoria son las permutaciones. Al conjunto de permutaciones de n elementos se lo llama **grupo simétrico** y se denota por $\mathcal{S}_n$. Las permutaciones descomponen de forma única en ciclos disjuntos, lo que permite denotarlas a través de ellos. Por ejemplo, la permutación $(123)(46) \in \mathcal{S}_6$ envía el 1 al 2, el 2 al 3 y el 3 al 1. El 4 lo envía al 6 y viceversa, y el 5 lo deja fijo. Una operación interesante entre permutaciones es la conjugación. Dos permutaciones σ y τ se dicen conjugadas si existe $\gamma \in \mathcal{S}_n$ tal que $\gamma^{-1} \circ \sigma \circ \gamma = \tau$. Equivalentemente, $\sigma \circ \gamma = \gamma \circ \tau$. Ser conjugados es una relación de equivalencia, y las clases de equivalencia se denominan clases de conjugación.

Este concepto hace de puente entre particiones y permutaciones. Hay tantas particiones de n como clases de conjugación de $\mathcal{S}_n$ (corolario 11). De hecho, a cada permutación le podemos asociar una partición mirando los tamaños de sus ciclos disjuntos. Por ejemplo, una partición de $\mathcal{S}_3$ que tenga un 2-ciclo y un 1-ciclo (punto fijo) tiene asociada la partición $(2,1)$ de $n=3$. Evidentemente, permutaciones diferentes pueden tener la misma partición asociada. Lo que ocurre es que tienen la misma partición asociada si y solo si son conjugadas. Por lo tanto, las clases de conjugación de $\mathcal{S}_n$ van asociadas de forma natural a las particiones, y en consecuencia, van asociadas también a los diagramas de Young.

Esta relación entre permutaciones y diagramas de Young es la que hace realmente importantes los diagramas de Young. En realidad, estos diagramas ya habían sido introducidos previamente por Ferrers en 1871. La novedad que introdujo Young es la posibilidad rellenarlos con los números del 1 al n (sin repetirlos). Esta idea permite que las permutaciones puedan actuar sobre los diagramas, permutando los números del diagrama. A estos diagramas de Young rellenos con números los llamamos tablas de Young. Si, además, las filas y columnas están ordenadas (de menor a mayor), decimos que son tablas estándar de Young. Por ejemplo, hay 4 tablas estándar de Young para $n=3$, como se ve en la figura 2. También podemos dejar que las permutaciones actúen sobre las tablas; por ejemplo, cuando (23) actúa sobre la primera tabla de la figura 2, obtenemos la segunda tabla.

Ahora podemos hacer la siguiente observación. De las tres particiones que hay para $n=3$, una tiene dos tablas estándar; otra, una, y la otra, una. Y ocurre que si sumamos los cuadrados de estos números, $2^2+1^2+1^2=6=3!$, obtenemos la cantidad de elementos de $\mathcal{S}_n$, que es $n!$. Podemos hacer lo mismo para otros valores de n. Para $n=4$ se obtienen cinco particiones, con dos, tres, tres, una y una tablas estándar, y

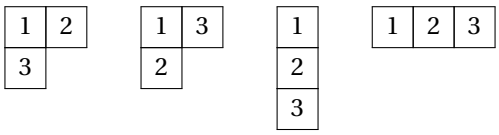

Figura 2: Tablas estándar de Young para $n = 3$. Para la partición $(2,1)$ hay dos posibles tablas estándar, mientras para las particiones $(1,1,1)$ y (3) solo hay una tabla estándar posible.

vuelve a ocurrir que $2^2 + 3^2 + 3^2 + 1^2 + 1^2 = 24 = 4!$. Con $n = 5$ obtenemos siete particiones con seis, cinco, cinco, cuatro, cuatro, una y una tablas estándar, y tenemos que $6^2 + 5^2 + 5^2 + 4^2 + 4^2 + 1^2 + 1^2 = 120 = 5!$.

La teoría de representaciones aplicada al grupo simétrico nos permitirá probar esta igualdad (corolario 19). Tras introducir las representaciones, utilizaremos sus caracteres para probar que $|\mathcal{S}_n| = \sum n_i^2$. Los n_i, que son la cantidad de tablas estándar, coincidirán con las dimensiones de unas representaciones, cada una asociada a una partición (o diagrama de Young). La construcción explícita de estas representaciones nos permitirá ver que las dimensiones n_i se corresponden a la cantidad de tablas estándar.

2. Representaciones lineales de grupos

Un grupo consiste en un conjunto G con una operación $\cdot$ tal que dados dos elementos $a, b \in G$, nos devuelve $a \cdot b \in G$. Esta operación ha de ser asociativa, tener elemento neutro y todo elemento ha de tener inverso. Por ejemplo, las permutaciones con la composición son un grupo, que es el grupo simétrico. Otro ejemplo es el conjunto de matrices invertibles $n \times n$ sobre $\mathbb{C}$, que es un grupo con el producto de matrices. Este grupo se denota por $\mathrm{GL}_n(\mathbb{C})$, y también se puede pensar como aplicaciones lineales invertibles de V en sí mismo (donde V es un $\mathbb{C}$-espacio vectorial de dimensión n). La idea de una representación del grupo G consiste en trasladar la estructura de G a este grupo concreto: $\mathrm{GL}_n(\mathbb{C})$. Si utilizamos lenguaje de aplicaciones en lugar de lenguaje matricial, el grupo se denotará por $\mathrm{GL}(V)$. Hablaremos de matrices o aplicaciones lineales indistintamente, según sea conveniente. En particular, omitiremos el $\circ$ de la composición, ya que desde el punto de vista matricial es simplemente un producto.

Definición 1. Una **representación** de un grupo G en un espacio vectorial V consiste en una aplicación $\rho\colon G \to \mathrm{GL}(V)$ tal que

$$\rho_{ab} = \rho_a \rho_b \qquad \forall\, a, b \in G.$$ ◂

Como vemos, la matriz asociada al elemento ab es el producto de la de a con la de b. En lenguaje de aplicaciones, la aplicación lineal de ab es la de b compuesta con la de a. En un contexto general de teoría de grupos, este tipo de aplicaciones entre grupos se denomina **homomorfismo de grupos** (la particularidad de este caso es que el espacio de llegada es $\mathrm{GL}(V)$). Aunque esta definición es totalmente general, nosotros consideraremos grupos G finitos y espacios vectoriales V de dimensión finita y sobre $\mathbb{C}$.

Observación 1. Tomando $b = 1$ en la definición vemos que $\rho_1 = \mathrm{Id}$, puesto que $\rho_a = \rho_a \rho_1$. Tomando $b = a^{-1}$ vemos que $\rho_{a^{-1}} = \rho_a^{-1}$, puesto que $\mathrm{Id} = \rho_1 = \rho_a \rho_{a^{-1}}$. ◂

En todo grupo finito ocurre que existe algún valor k tal que $a^k = 1$ (de hecho, $k = |G|$ lo cumple). Como consecuencia, ρ_a compuesta k veces consigo misma será la identidad. Los ejemplos más sencillos de este tipo de aplicaciones tienen un fuerte significado geométrico. Las simetrías, por ejemplo, lo cumplen para $k = 2$. Movimientos directos, como rotaciones de $360°/k$, también lo cumplen. Nuestras representaciones serán colecciones de aplicaciones de este tipo (una por cada $a \in G$).

Ejemplo 1. Sea V un espacio vectorial y sea G un grupo. Si a cada $a \in G$ le asociamos la identidad, tenemos una representación $\rho_a = \mathrm{Id}$. En el caso de que V sea de dimensión 1 la llamaremos representación **trivial**. ◂

Ejemplo 2. Consideremos las permutaciones de tres elementos, $\mathcal{S}_3$. Hay seis de ellas: la identidad, tres trasposiciones y dos 3-ciclos. Podemos representar este grupo en el plano $\mathbb{R}^2$, como vemos en la figura 3.

Los dos 3-ciclos son (123) y (132) y van asociados a rotaciones de 120° y −120°. Las trasposiciones (12), (13) y (23) son simetrías; por ejemplo, la (12) es la que intercambia los puntos 1 y 2. Aunque el dibujo está en $\mathbb{R}^2$, esto también es una representación sobre $\mathbb{C}^2$, porque las matrices 2×2 reales que nos dan los automorfismos son también matrices 2×2 complejas. A esta representación sobre $\mathbb{C}^2$ se la denomina representación **estándar**. Esta representación viene dada en forma matricial de la siguiente manera:

$$\rho_{id}=\begin{pmatrix}1&0\\0&1\end{pmatrix} \qquad \rho_{(123)}=\begin{pmatrix}-1/2&\sqrt{3}/2\\-\sqrt{3}/2&-1/2\end{pmatrix} \qquad \rho_{(132)}=\begin{pmatrix}-1/2&-\sqrt{3}/2\\\sqrt{3}/2&-1/2\end{pmatrix}$$
$$\rho_{(23)}=\begin{pmatrix}-1&0\\0&1\end{pmatrix} \qquad \rho_{(12)}=\begin{pmatrix}1/2&\sqrt{3}/2\\\sqrt{3}/2&-1/2\end{pmatrix} \qquad \rho_{(13)}=\begin{pmatrix}1/2&-\sqrt{3}/2\\-\sqrt{3}/2&-1/2\end{pmatrix}$$ ◂

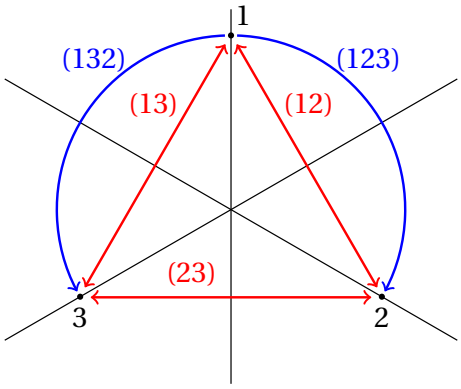

Figura 3: Representación esquemática de los automorfismos de la representación estándar de $\mathcal{S}_3$ sobre $\mathbb{R}^2$. En rojo, simetrías (corresponden a trasposiciones) y en azul, rotaciones (corresponden a 3-ciclos). Ver ejemplo 2.

Ejemplo 3. Tomemos el grupo simétrico $G=\mathcal{S}_n$ y sea $a\in\mathcal{S}_n$ una permutación. Como las permutaciones descomponen en ciclos y los ciclos en trasposiciones, la podemos descomponer en trasposiciones (no de forma única). Si a descompone en una cantidad par de trasposiciones decimos que a es par y que tiene signo $\varepsilon(a)=1$. Si, por el contrario, descompone en una cantidad impar de trasposiciones, a será impar y su signo será $\varepsilon(a)=-1$. Aunque la descomposición no es única, la paridad de la cantidad de trasposiciones es siempre la misma, de forma que el signo está bien definido. Además, el signo es multiplicativo, es decir, $\varepsilon(a)\varepsilon(b)=\varepsilon(ab)$. De todo esto se deduce que $\rho_a=\varepsilon(a)\mathrm{Id}$ es una representación, para cualquier espacio vectorial V. En el caso de $\dim(V)=1$ la llamamos representación **alternada**. ◂

Ejemplo 4. Consideremos un $\mathbb{C}$-espacio vectorial V de dimensión igual a $|G|$. Indexemos los vectores de la base con elementos de G, es decir $\mathcal{B}=\{e_a\}_{a\in G}$. La representación **regular** de G asocia a cada $b\in G$ el automorfismo definido por

$$\rho_b(e_a)=e_{ba}.$$

Como hemos definido ρ_b sobre la base $\mathcal{B}$, queda completamente definida. Esta representación será de especial importancia, porque guarda toda la información de G como grupo. ◂

Cuando trabajamos con matrices de aplicaciones lineales, suele ser interesante diagonalizarlas, es decir, encontrar una matriz semejante en forma diagonal. Esto lo hacemos a través de los autovectores, que definen rectas invariantes de la aplicación. En el caso de representaciones, tendríamos que diagonalizar simultáneamente todas las matrices ρ_a con $a\in G$. Esto es más complicado, y, en general, no será posible. Aún así, podemos seguir estudiando subespacios invariantes (que no sean necesariamente rectas), y también podemos descomponer ρ a través de sus subespacios invariantes. Para realizar la descomposición queremos que, si W es un subespacio invariante, exista otro subespacio suplementario W^c, también invariante, que nos permita descomponer ρ entre W y W^c. Ahora formalizaremos esta idea.

Definición 2. Decimos que $W\subset V$ es un subespacio **invariante** de ρ si $\rho_a(W)=W$, para todo $a\in G$. Esto es decir que W es subespacio invariante de cada ρ_a como automorfismo. ◂

Definición 3. Decimos que una representación es **irreducible** si no existe ningún subespacio $W \subset V$ invariante que no sea trivial (es decir, $W \neq V$, $W \neq \{0\}$). ◂

Definición 4. Dadas dos representaciones $\rho\colon G \to \mathrm{GL}(V_1)$, $\eta\colon G \to \mathrm{GL}(V_2)$, definimos su **suma directa** $\rho \oplus \eta\colon G \to \mathrm{GL}(V_1 \oplus V_2)$ como la nueva representación

$$(\rho \oplus \eta)_a(u+v) = \rho_a(u) + \eta_a(v) \qquad \forall\, u \in V_1, v \in V_2.$$ ◂

Teorema 1 (Maschke). *Toda representación $\rho\colon G \to \mathrm{GL}(V)$ se puede descomponer como*

$$\rho = \rho^{(1)} \oplus \rho^{(2)} \oplus \cdots \oplus \rho^{(k)},$$

donde todas las $\rho^{(i)}$ son representaciones irreducibles.

Demostración. Si ρ no es irreducible, existe algún $W \subset V$ invariante. Escojámoslo lo más pequeño posible, es decir, que no tenga ningún subespacio invariante dentro. Como W es invariante, $\rho_{|W}$ es una representación de W (restringimos cada ρ_a al subespacio W) y, como W es lo más pequeño posible, es irreducible. Ahora buscamos un subespacio invariante suplementario W^c para escribir $\rho = \rho_{|W} \oplus \rho_{|W^c}$. Nos basta con que W^c sea invariante porque, aunque no sea irreducible, podremos aplicarle el mismo razonamiento sucesivamente, hasta obtener solo subespacios irreducibles.

Hemos reducido la demostración a hallar un subespacio W^c, suplementario a W e invariante. Desde una intuición geométrica, nos gustaría coger una especie de W ortogonal, pero no hemos definido ningún producto escalar. Asumamos un producto escalar $\langle\cdot,\cdot\rangle$ y cojamos $W^c = W^\perp$, que es el conjunto de vectores v tales que $\langle v, u\rangle = 0$ para todo $u \in W$. Sea $v \in W^\perp$. Si tuviéramos que $\langle \rho_a(v), \rho_a(u)\rangle = \langle v, u\rangle$ habríamos acabado, porque eso es 0 para todo $u \in W$ y, como $\rho_a(u) \in W = \rho_a(W)$ por ser W invariante, se tendría que $\rho_a(v) \in W^\perp$. La existencia de un producto escalar con $\langle \rho_a(v), \rho_a(u)\rangle = \langle v, u\rangle$ nos la garantiza el lema 2 que presentamos a continuación. ■

Lema 2. *Sea ρ una representación en un espacio vectorial V. Existe un producto escalar $\langle\cdot,\cdot\rangle$ de V tal que*

$$\langle \rho_a(v), \rho_a(u)\rangle = \langle v, u\rangle \qquad \forall\, a \in G, \forall\, u, v \in V.$$

Demostración. En primer lugar consideremos un producto escalar cualquiera $[\cdot,\cdot]$ (producto respecto de una base cualquiera). Definimos a partir de él un nuevo producto

$$\langle v, u\rangle = \frac{1}{|G|}\sum_{b\in G}[\rho_b(v), \rho_b(u)],$$

es decir, hacemos la media de $[\rho_b(v), \rho_b(u)]$ haciendo que b varíe sobre G. Este nuevo producto cumple la propiedad deseada porque para todo $c \in G$ tenemos que

$$\langle \rho_c(v), \rho_c(u)\rangle = \frac{1}{|G|}\sum_{b\in G}[\rho_{bc}(v), \rho_{bc}(u)] = \frac{1}{|G|}\sum_{a\in G}[\rho_a(v), \rho_a(u)] = \langle v, u\rangle,$$

donde hemos definido $a = bc$. Como b recorre todo G y c es fijo, $a = bc$ variará por todo G. Además, el hecho de que $\langle\cdot,\cdot\rangle$ sea un producto escalar (bilineal, definido positivo y hermítico) se deriva directamente de que $[\cdot,\cdot]$ lo sea. ■

Ejemplo 5. Consideremos $V = \mathbb{C}^3$ con una base $\mathcal{B} = \{e_1, e_2, e_3\}$ y el grupo simétrico $G = \mathcal{S}_3$. Sea ρ_a el automorfismo que lleva e_1 a $e_{a(1)}$, lleva e_2 a $e_{a(2)}$ y lleva también e_3 a $e_{a(3)}$. Dichas ρ forman una representación, que puede parecer la regular, pero no lo es (la regular sería de dimensión $|\mathcal{S}_3| = 6$). Podemos ver esta representación esquemáticamente en la figura 4 (viendo únicamente la parte real, es decir, el corte en $\mathbb{R}^3$). Hay dos subespacios invariantes: la recta $\langle(1,1,1)\rangle$ y el plano perpendicular $x_1 + x_2 + x_3 = 0$. La representación restringida a la recta $\langle(1,1,1)\rangle$ es la trivial del ejemplo 1. La representación restringida al plano $x_1 + x_2 + x_3 = 0$ es la representación estándar que introdujimos en el ejemplo 2. ◂

Ejercicio 6. Se puede ver que la representación regular del ejemplo 4 para el grupo simétrico $\mathcal{S}_n$ contiene tanto a la representación trivial como a la representación alternada (de los ejemplos 1 y 3). ◂

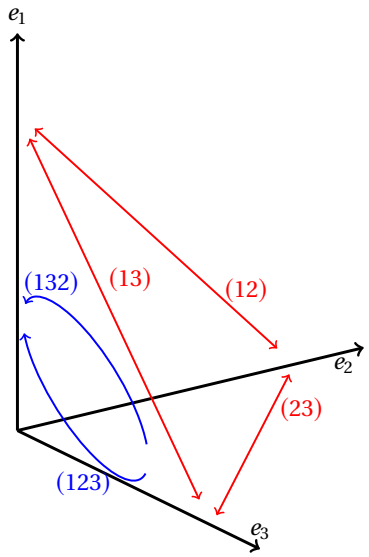

Figura 4: Dibujo esquemático de automorfismos de una representación sobre $\mathbb{R}^3$. En rojo, simetrías (corresponden a trasposiciones) y en azul, rotaciones (corresponden a 3-ciclos) .

Ejemplo 7. Es importante ver que la descomposición dada en el teorema 1 no es necesariamente única. Cojamos una representación de dimensión $n > 1$, donde $\rho_a = \mathrm{Id}$. Cualquier recta es invariante, por lo que hay infinitas posibilidades para descomponer en n rectas invariantes. Más adelante veremos que lo que sí son únicas son las representaciones que obtenemos en estos subespacios. Por ejemplo, aquí obtenemos siempre n representaciones triviales, independientemente de las rectas escogidas. ◂

Aunque se desvíe de nuestro objetivo, vale la pena comentar que hemos utilizado de forma fundamental la finitud de G para promediar y obtener nuestro producto en el lema 2. Esto permite descomponer ρ como suma de irreducibles, y este resultado no lo tendremos en casos más generales (G infinito). No obstante, si tenemos una integral razonable desde el punto de vista de G, podemos tomar promedios con integrales y todo funciona exactamente igual. Para ello es necesario exigir otras propiedades como, por ejemplo, que G sea un grupo topológico localmente compacto. Para más detalles se puede consultar el libro de Kowalski [4], en concreto, la primera parte del teorema 5.2.11.

3. El lema de Schur

Pensando en forma matricial, el teorema 1 dice que, en una cierta base, todas las matrices ρ_a están descompuestas en bloques. Estos bloques vienen definidos por los subespacios invariantes. Por tanto, lo lógico será estudiar la representación en esta base, donde podemos limitarnos a estudiar cada una de las representaciones irreducibles que componen ρ. Para ello, pasaremos por estudiar sus relaciones.

La relación natural entre dos representaciones ρ y η es una aplicación lineal g tal que $\rho_a g = g\eta_a$ para todo $a \in G$. A dicha g la llamaremos morfismo de ρ a η. En el caso de que g sea biyectiva, será un isomorfismo de ρ a η, y recuperamos el concepto de que ρ y η sean equivalentes (isomorfas). En el lenguaje de teoría de categorías esta g no es más que una transformación natural entre ρ y η, vistos como funtores de G a $\mathrm{Vec}_{\mathbb{C}}$. Existe un resultado muy importante sobre estos morfismos de representaciones.

Teorema 3 (Lema de Schur, [6]). *Sean $\rho\colon G \to \mathrm{GL}(V_1), \eta\colon G \to \mathrm{GL}(V_2)$ dos representaciones irreducibles. Entonces tenemos que:*

- *Si g es morfismo de ρ a η, o bien g es isomorfismo o bien $g \equiv 0$.*
- *Si h es morfismo de ρ a ρ (endomorfismo de ρ), entonces es una homotecia $h = c \cdot \mathrm{Id}$.*

Demostración. Empecemos por el primer apartado. Al ser g morfismo, $\rho_a g = g\eta_a$, lo cual implica que $\ker(g)$ e $\mathrm{Im}(g)$ son subespacios invariantes de η_a y ρ_a, respectivamente. Pero como ρ y η son irreducibles, sus subespacios invariantes son $\{0\}$ o el total. Si el núcleo es 0 y la imagen es el total, estamos ante un isomorfismo (y, por tanto, ρ y η serían equivalentes). En cualquier otro caso la aplicación es nula.

Situémonos ahora en la segunda parte, donde h es endomorfismo de ρ. Observemos que si h cumple que $h\rho_a = \rho_a h$, entonces $\hat{h} = h - c \cdot \mathrm{Id}$ también cumple que $\hat{h}\rho_a = \rho_a \hat{h}$. Como estamos en $\mathbb{C}$, siempre podemos escoger c para que $\hat{h}$ tenga un autovalor nulo (tomando c un autovalor de h). Pero entonces $\hat{h}$ no es isomorfismo y, por la primera parte, $\hat{h} = 0$. Es decir, $h = c \cdot \mathrm{Id}$, como queríamos. ■

Ejemplo 8. Consideremos una representación ρ no irreducible en V y sea h la proyección ortogonal (según el producto escalar del lema 2) sobre uno de los subespacios invariantes W. Descomponiendo un v cualquiera entre W y $W^\perp$ y teniendo en cuenta que $W^\perp$ también es invariante, tenemos que

$$h(\rho_a(v)) = h(\rho_a(w + w^\perp)) = h(\rho_a(w)) + h(\rho_a(w^\perp)) = \rho_a(w) + 0 = \rho_a(h(v)).$$

De esta forma, h es un endomorfismo de ρ y, como no es $c \cdot \mathrm{Id}$, no cumple el teorema 3. Esto ocurre porque ρ no es irreducible; de hecho, esto prueba que ρ es irreducible si y solo si cumple la segunda parte del teorema 3. ◂

Observación 2. Sean ρ y η las representaciones del teorema 3 (representaciones irreducibles cualesquiera) y sea $g\colon V_1 \to V_2$ una aplicación lineal cualquiera. Si consideramos $\hat{g}$ definida por

$$\hat{g} = \sum_{a \in G} \eta_a^{-1} g \rho_a,$$

se cumple que $\hat{g}$ está bajo las hipótesis del teorema 3. Es decir, $\eta_b^{-1}\hat{g}\rho_b = \hat{g}$ para todo $b \in G$. ◂

Esto nos da mucha información, porque escogiendo una g cualquiera, tendremos que $\hat{g}$ será 0 si ρ y η no son equivalentes. Por otro lado, si $\rho = \eta$, tendremos que $\hat{g}$ será una homotecia. Escribiendo esto en forma matricial podemos concluir información sobre las trazas de las matrices ρ_a y η_a. El desarrollo formal es algo pesado pero no especialmente difícil. El lector interesado puede intentarlo por su cuenta o consultar el libro de Serre [6].

Proposición 4. *Si ρ y η son dos representaciones irreducibles no equivalentes de G, entonces*

$$\sum_{a \in G} \overline{\mathrm{Tr}(\eta_a)}\,\mathrm{Tr}(\rho_a) = 0.$$

Proposición 5. *Si ρ es una representación irreducible de G, entonces*

$$\sum_{a \in G} \overline{\mathrm{Tr}(\rho_a)}\,\mathrm{Tr}(\rho_a) = |G|.$$

4. Caracteres

Las proposiciones 4 y 5 indican un sentido de ortonormalidad entre las funciones $\mathrm{Tr}(\rho_a)$ (siendo a el argumento). Para seguir este camino, definimos estas funciones y el producto adecuado.

Definición 5. Dada una representación $\rho\colon G \to \mathrm{GL}(V)$, su carácter será la función $\phi\colon G \to \mathbb{C}$ dada por $\phi(a) = \mathrm{Tr}(\rho_a)$. ◂

Definición 6. Dadas dos funciones $\phi, \psi\colon G \to \mathbb{C}$, definimos su producto escalar como

$$(\phi|\psi) = \frac{1}{|G|} \sum_{a \in G} \overline{\phi(a)}\psi(a).$$ ◂

Observación 3. Las proposiciones 4 y 5 hacen que los caracteres de representaciones irreducibles sean ortonormales respecto del producto que acabamos de definir. ◂

Al ser los caracteres ortogonales, una pregunta natural es qué subespacio vectorial generan (pues serán base ortogonal de este subespacio). Por el hecho de ser trazas de representaciones cumplirán $\phi(aba^{-1}) = \phi(b)$, ya que $\mathrm{Tr}(\rho_a\rho_b\rho_a^{-1}) = \mathrm{Tr}(\rho_b)$ al ser la traza un invariante en álgebra lineal. Como ya comentamos en la introducción, al elemento aba^{-1} se lo llama conjugado de b. Vemos que dos elementos conjugados de G tienen la misma imagen por ϕ.

Definición 7. La **clase de conjugación** de un elemento $b \in G$ son todos los elementos de G de la forma aba^{-1}. Una función $\phi\colon G \to \mathbb{C}$ que cumple que

$$\phi(aba^{-1}) = \phi(b) \quad \forall\, a, b \in G$$

se denomina **función de clase**. Es decir, una función de clase será aquella que sea constante sobre cada clase de conjugación. En particular, los caracteres son funciones de clase. ◂

Ejemplo 9. Consideremos la representación regular $\rho\colon G \to \mathrm{GL}(V)$ del ejemplo 4. Su carácter $\phi(a) = \mathrm{Tr}(\rho_a)$ será 0 para $a \neq 1$ (ya que cada vector de la base e_b lo envía a uno diferente e_{ab}). Por el contrario, para $a = 1$ tenemos que $\phi(1) = |G|$ (ya que deja fija toda la base). Por tanto, $\phi(a) = |G|\delta_1(a)$, donde δ_1 es una función que vale 1 en el elemento neutro de G y 0 en el resto de elementos. ◂

Ejemplo 10. Tomemos $G = \mathcal{S}_3$. Tiene 3 clases de conjugación: la identidad, las trasposiciones y los 3-ciclos. En el cuadro 1 podemos ver los valores que toma el carácter en cada clase de conjugación. Lo hemos hecho para la representación trivial (ejemplo 1), la representación alternada (ejemplo 3) y para la representación estándar (ejemplo 2). El cálculo de ϕ para la trivial y alternada es trivial y para la estándar lo podemos hacer tomando trazas en las matrices del ejemplo 2. Observamos que ϕ es constante sobre cada clase de conjugación. Además, como todas son irreducibles, los caracteres han de ser ortonormales, y así es. ◂

Cuadro 1: Caracteres de las representaciones irreducibles de $\mathcal{S}_3$.

Representación	id	(12)	(13)	(23)	(123)	(132)
Trivial	1	1	1	1	1	1
Alternada	1	−1	−1	−1	1	1
Estándar	2	0	0	0	−1	−1

Teorema 6. *Las funciones de clase forman un espacio vectorial. Los caracteres de las representaciones irreducibles de un grupo G sobre $\mathbb{C}$ forman una base ortonormal del espacio de funciones de clase.*

Demostración. Es trivial que las funciones de clase son un espacio vectorial con la suma de funciones y el producto por escalar. Ya hemos visto que los caracteres de representaciones irreducibles son ortonormales, y falta ver que generan todo el espacio de funciones de clase. Supongamos que generan el espacio $W \subset V$ dentro del espacio V de funciones de clase. Queremos probar que $W = V$, y para ello veremos que $W^\perp = \{0\}$. Sean $\phi^{(i)}$ los caracteres de representaciones irreducibles y sea ψ ortogonal a todas ellas. Veamos que $\psi = 0$. Para eso, utilizaremos la representación regular del ejemplo 4. Sea ρ la representación regular. Por el teorema 1, ρ descompone en las representaciones irreducibles $\rho^{(j)}$, de caracteres $\phi^{(j)}$ (puede haberlas repetidas). Por hipótesis, $(\psi|\phi^{(j)}) = 0$. Consideremos la función

$$f^{(j)}(x) = \sum_{a\in G} \overline{\psi(a)}\rho_a^{(j)}(x).$$

Por un lado, tenemos que $\mathrm{Tr}(f^{(j)}) = (\psi|\phi^{(j)}) = 0$. Por otro lado, $f^{(j)}$ es un morfismo de la representación irreducible $\rho^{(j)}$, ya que

$$\rho_b^{(j)} f^{(j)} \rho_b^{(j)^{-1}} = \sum_{a\in G} \overline{\psi(a)}\rho^{(j)}_{bab^{-1}} = \sum_{c\in G} \overline{\psi(b^{-1}cb)}\rho_c^{(j)} = \sum_{c\in G} \overline{\psi(c)}\rho_c^{(j)} = f^{(j)},$$

donde hemos tomado $c = bab^{-1}$ y usado que ϕ es función de clase. Como $\rho^{(j)}$ es irreducible, el teorema 3 afirma que $f^{(j)} = k \cdot \mathrm{Id}$, pero como $\mathrm{Tr}(f^{(j)}) = 0$, necesariamente $f^{(j)} = 0$. Ahora bien, si definimos f para la representación regular como

$$f(x) = \sum_{a\in G} \overline{\psi(a)}\rho_a(x),$$

está claro que f es suma de las $f^{(j)}$ (ya que ρ es suma de las $\rho^{(j)}$). Como todas las $f^{(j)}$ son nulas, $f \equiv 0$. En particular,

$$0 = f(e_1) = \sum_{a\in G} \overline{\psi(a)}\rho_a(e_1) = \sum_{a\in G} \overline{\psi(a)}e_a.$$

Como los e_a son una base, cada coeficiente conjugado es $\overline{\psi(a)} = 0$ y, por tanto, $\psi \equiv 0$. Como cualquier función de clase ψ ortogonal a las $\phi^{(j)}$ es nula, las $\phi^{(j)}$ generan todo el espacio de funciones de clase. ■

Corolario 7. *La representación regular contiene todas las representaciones irreducibles.*

El corolario se deriva directamente de la demostración del teorema, porque solo hemos usado las representaciones irreducibles contenidas en la regular.

Corolario 8. *Sean $\rho^{(i)}$ las representaciones irreducibles, sea η una representación cualquiera, y sea $\eta = n_1\rho^{(1)} \oplus \ldots \oplus n_k\rho^{(k)}$ su descomposición por el teorema 1 (donde n_i significa que cada $\rho^{(i)}$ aparece n_i veces). Estos n_i se pueden calcular mediante $n_i = (\varphi|\phi^{(i)})$, donde φ es el carácter de η. Además, esto implica la unicidad de la descomposición del teorema 1, salvo isomorfismo.*

Demostración. Para ver que $n_i = (\varphi|\phi^{(i)})$, simplemente ejecutamos el producto y usamos ortonormalidad:

$$(\varphi|\phi^{(i)}) = (n_1\phi^{(1)} + \ldots + n_k\phi^{(k)}|\phi^{(i)}) = n_1(\phi^{(1)}|\phi^{(i)}) + \ldots + n_k(\phi^{(k)}|\phi^{(i)}) = n_i.$$

Esto es válido para cualquier descomposición de η. Por tanto, todas las descomposiciones consisten en repetir n_i representaciones equivalentes a $\rho^{(i)}$. Es decir, la única descomposición de η es $n_1\rho^{(1)}\oplus\ldots\oplus n_k\rho^{(k)}$, salvo isomorfismo. ■

Corolario 9. *Hay tantas representaciones irreducibles de G como clases de conjugación.*

Demostración. De hecho, si V es el espacio de funciones de clase, tenemos que

$$\#\text{ representaciones irreducibles de G} = \dim(V) = \#\text{ clases de conjugación de G.}$$

La primera igualdad se deduce de que las $\phi^{(i)}$ son una base de V, y hay tantas como representaciones irreducibles. La segunda igualdad proviene de que los elementos de V son exactamente las funciones que son constantes sobre cada clase de conjugación. De esa manera, una posible base de V son las funciones que valen 1 en una clase de conjugación y 0 en el resto. Evidentemente, hay tantas funciones de ese tipo como clases de conjugación. ■

Corolario 10. *Supongamos que cada $\rho^{(i)}$ aparece n_i veces en la representación regular ρ. Entonces tenemos la fórmula*

$$|G| = \sum_{i=1}^{k} n_i^2.$$

Demostración. Sea ϕ el carácter de ρ. Calculemos $(\phi|\phi)$ de dos maneras. Tenemos que

$$(\phi|\phi) = (n_1\phi^{(1)} + \ldots + n_k\phi^{(k)}|n_1\phi^{(1)} + \ldots + n_k\phi^{(k)}) = \sum_{i=1}^{k} n_i^2.$$

Pero por otro lado, al ser ρ la representación regular, tenemos que $\mathrm{Tr}(\rho_a) = \delta_1|G|$ (ejemplo 9). De ahí deducimos que

$$(\phi|\phi) = \frac{1}{|G|}\sum_{a\in G}\overline{\mathrm{Tr}(\rho_a)}\,\mathrm{Tr}(\rho_a) = \frac{1}{|G|}\sum_{a\in G}\delta_1|G|^2 = \frac{1}{|G|}|G|^2 = |G|.$$

Como ambos resultados de $(\phi|\phi)$ han de ser iguales, tenemos la fórmula deseada. ■

Ejemplo 11. Continuemos el ejemplo 10. Teníamos tres representaciones irreducibles de $\mathcal{S}_3$ (la trivial, la alternada y la estándar). Por el corolario 9 sabemos que estas tres ya son todas (ya que hay tres clases de conjugación de $\mathcal{S}_3$: la identidad, la de trasposiciones y la de 3-ciclos). Tenemos sus caracteres $\phi^{(i)}$ en el cuadro 1 y, por otro lado, tenemos el carácter $\phi = |\mathcal{S}_3|\delta_1$ de la representación regular (ejemplo 9).

El corolario 8 nos permite decir que la representación regular descompone como $\rho = n_1\rho^{(1)} \oplus n_2\rho^{(2)} \oplus n_3\rho^{(3)}$, donde cada n_i viene dado por $(\phi|\phi^{(i)})$. Usando que $\phi = |\mathcal{S}_3|\delta_1$ y recordando que δ_1 es nula salvo para el neutro de $\mathcal{S}_3$ obtenemos

$$n_i = (\phi|\phi^{(i)}) = \frac{1}{|\mathcal{S}_3|}\sum_{a\in\mathcal{S}_3} |G|\overline{\delta_1(a)}\phi^{(i)}(a) = \phi^{(i)}(id).$$

Mirando los resultados $\phi^{(i)}(id)$ en el cuadro 1 vemos que tanto la representación trivial como la alternada tienen $n_1 = n_2 = 1$, mientras que la estándar tiene $n_3 = 2$. Por un lado comprobamos el corolario 7, porque se cumple que todo $n_i > 0$, estando cualquier representación dentro de la regular al menos una vez. Por otro lado, comprobamos también el corolario 10, ya que $n_1^2 + n_2^2 + n_3^2 = 1 + 1 + 4 = 6 = |\mathcal{S}_3|$. ◂

Ejemplo 12. En el ejemplo 5 tenemos una representación tridimensional tal que ρ_a envía e_i a $e_{a(i)}$. Claramente, su carácter φ valdrá 3 en la identidad (deja fija la base), 1 en las trasposiciones (deja un elemento de la base fijo) y 0 en los 3-ciclos (no dejan ninguno fijo). Esto permite descomponerla usando la ecuación $n_i = (\varphi|\phi^{(i)})$ del corolario 8. En concreto, siendo i la identidad, t una transposición y c un ciclo, tenemos que

$$\begin{aligned}
n_1 &= \frac{1}{6}\left(\overline{\varphi(i)}\phi^{(1)}(i) + 3\overline{\varphi(t)}\phi^{(1)}(t) + 2\overline{\varphi(c)}\phi^{(1)}(c)\right) = \frac{3\cdot 1 + 3\cdot 1\cdot 1 + 2\cdot 0\cdot 1}{6} = 1,\\
n_2 &= \frac{1}{6}\left(\overline{\varphi(i)}\phi^{(2)}(i) + 3\overline{\varphi(t)}\phi^{(2)}(t) + 2\overline{\varphi(c)}\phi^{(2)}(c)\right) = \frac{3\cdot 1 + 3\cdot 1\cdot (-1) + 2\cdot 0\cdot 1}{6} = 0,\\
n_3 &= \frac{1}{6}\left(\overline{\varphi(i)}\phi^{(3)}(i) + 3\overline{\varphi(t)}\phi^{(3)}(t) + 2\overline{\varphi(c)}\phi^{(3)}(c)\right) = \frac{3\cdot 2 + 3\cdot 1\cdot 0 + 2\cdot 0\cdot \frac{-1}{2}}{6} = 1.
\end{aligned}$$

Como ya habíamos visto en el ejemplo 5, esta representación descompone en la trivial ($n_1 = 1$) y la estándar ($n_3 = 1$) sin contener ninguna representación alternada ($n_2 = 0$). ◂

5. El caso del grupo simétrico

Como ya comentamos en la introducción, las clases de conjugación de $\mathcal{S}_n$ están asociadas con las particiones de n, de forma que hay $p(n)$ clases de conjugación de $\mathcal{S}_n$. Recordemos que a la permutación $a \in \mathcal{S}_n$ le podíamos asociar la partición de n que consiste en los tamaños de los ciclos disjuntos en los que descompone a.

Ejercicio 13. Probar que dos permutaciones $a, b \in \mathcal{S}_n$ son conjugadas si y solo si sus ciclos son de los mismos tamaños. ◂

Corolario 11. *Del ejercicio anterior deducimos que hay $p(n)$ clases de conjugación de $\mathcal{S}_n$.*

Demostración. Por el ejercicio anterior, hay tantas clases de conjugación como posibles permutaciones de $\mathcal{S}_n$ con tamaños de sus ciclos diferentes. Como la suma de tamaños de los ciclos es n, hay exactamente $p(n)$ posibilidades para escoger estos tamaños. ■

De esta manera, cada partición corresponderá a una única clase de conjugación de $\mathcal{S}_n$ y viceversa. Por ejemplo, la clase de conjugación de los c-ciclos va a asociada a la partición $(c, 1, 1, \ldots, 1)$. Cada clase de conjugación corresponde a una única representación irreducible por el corolario 9. Uniendo ambas cosas, sabemos que habrá una representación irreducible por cada partición de n, y nuestro objetivo será construirla. Sea λ una partición de n. Lo primero que necesitamos es un espacio vectorial, y este espacio nos lo darán las tablas de Young, de las que hablamos en la introducción. Recordemos que una tabla de Young consiste en un diagrama de recuadros rellenos con los números del 1 al n. La forma del diagrama codifica una partición de n.

También nos será útil considerar tablas donde no nos importe el orden de números en las filas, a las que llamaremos tabloides. Podemos ver estos tabloides como un conjunto cociente de las tablas respecto a una relación de equivalencia $\sim$. La relación $\sim$ vendría definida por $T \sim S$ si y solo si las filas de T son las mismas que las de S, con la posibilidad de que cada fila esté reordenada. Al tabloide que se obtiene de la tabla T lo denotamos por $\{T\}$, y es la clase de equivalencia de T respecto a $\sim$.

Definición 8. Denotaremos por V^λ al $\mathbb{C}$-espacio vectorial libre generado por los tabloides. Es decir, tomaremos $\mathbb{C}^m$, donde m es la cantidad de tabloides, y denotaremos por $\{T_i\}$ a los elementos de la base, donde $\{T_i\}$ puede ser cualquier λ-tabloide (tabloide con la forma de la partición λ). ◂

Definición 9. Tenemos una representación de $\mathcal{S}_n$ en cada V^λ, simplemente dejando que cada $a \in \mathcal{S}_n$ actúe en cada tabloide, permutando los números de su interior. Dicha representación la denotaremos por ρ (aunque depende de λ) y viene dada por

$$\rho_a(c_1\{T_1\} + \ldots + c_k\{T_k\}) = c_1\rho_a\{T_1\} + \ldots + c_k\rho_a\{T_k\},$$

donde $\rho_a\{T_i\}$ consiste simplemente en dejar que a permute los números del 1 al n que hay en la tabla T_i. Esto es lo mismo que decir que permute los elementos del tabloide $\{T_i\}$ correspondiente. ◂

Ejemplo 14. Consideremos $n = 3$ y $\lambda = (2,1)$. Tenemos tres tabloides de Young, que podemos ver en la figura 5 (en los tabloides se omiten las lineas verticales, indicando así que no hay orden por filas). Por tanto $V = \mathbb{C}^3$. Observemos que $\rho_{(23)}\{T_1\} = \{T_1\}$, por lo que existen permutaciones no triviales que fijan un tabloide. También tendríamos, por ejemplo, que $\rho_{(123)}\{T_1\} = \{T_2\}$, o también que $\rho_{(13)}\{T_1\} = \{T_3\}$. Si comprobamos cómo actúa cada ρ_a sobre cada $\{T_i\}$ veremos que esta representación es exactamente igual a la del ejemplo 5 (llamando T_i a lo que antes era e_i). ◂

$$\{T_1\} = \begin{array}{|cc|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array} \qquad \{T_2\} = \begin{array}{|cc|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array} \qquad \{T_3\} = \begin{array}{|cc|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}$$

Figura 5: Tabloides de Young de forma $\lambda = (2,1)$.

Ejemplo 15. Consideremos n cualquiera y $\lambda = (n)$. Como todos los números están en la misma fila, hay un único tabloide de Young y toda ρ_a lo deja fijo, de forma que la representación es la trivial unidimensional. ◂

Ejemplo 16. Consideremos n cualquiera y $\lambda = (1,1,\ldots,1)$. Como las filas son de un elemento, los tabloides son lo mismo que las tablas, y tenemos $n!$ tabloides. Asociemos a cada tabloide $\{T_a\}$ la permutación $a \in \mathcal{S}_n$ que toma como $a(i)$ el número de la fila i-ésima de T_a. De esta forma, si $\{T_a\}$ tiene asociada $a \in \mathcal{S}_n$, ocurre que $\rho_b\{T_a\}$ tiene asociada ba. Por lo tanto, esta representación es la regular, utilizando $\{T_a\}$ como elementos de la base, en vez de e_a. ◂

Ejercicio 17. Para $n = 3$ hay tres posibles particiones: $(1,1,1)$, $(2,1)$ y (3). Aplicando los ejemplos 14, 15 y 16 a $n = 3$, vemos que solo $\lambda = (3)$ nos da una representación irreducible, que es la trivial. Se puede probar esto en general, es decir, que solo $\lambda = (n)$ da representaciones irreducibles. Para ello puede ser útil considerar el carácter φ de la representación y ver cómo se traduce la irreducibilidad en términos de φ. ◂

Pese a no ser irreducibles, nuestras representaciones son útiles, porque contienen la representación irreducible asociada a λ que buscamos. Por ejemplo, la partición $\lambda = (1,1,1)$ nos da la representación regular, que, aunque no es irreducible, contiene a la representación alternada, que sí es irreducible. De la misma manera, la partición $\lambda = (2,1)$ nos da la representación del ejemplo 5, que contiene a la representación estándar, que es irreducible. La idea general será construir un subespacio $W^\lambda \subset V^\lambda$ que sea invariante, y de manera que ρ restringida a W^λ sí sea irreducible.

Si el espacio W^λ ha de ser invariante, al aplicarle ρ_a a cualquier elemento de W^λ hemos de permanecer en W^λ. Una manera de aprovechar esto es considerar combinaciones lineales de las ρ_a. Para ello utilizaremos el concepto de signo de permutación introducido en el ejemplo 3. Recordando que el signo es multiplicativo y que $\varepsilon(a) = \pm 1$, se deducen fácilmente otras propiedades, como que $\varepsilon(a) = \varepsilon(a^{-1})$, o también que $\varepsilon(bab^{-1}) = \varepsilon(a)$.

Definición 10. Sea $H \subset \mathcal{S}_n$ un subgrupo de $\mathcal{S}_n$. Definiremos la función $f_H \colon V^\lambda \to V^\lambda$, para una partición λ y un subgrupo H, como

$$f_H\{T\} = \sum_{a \in H} \varepsilon(a)\rho_a\{T\}.$$ ◂

Observación 4. Si tenemos un subespacio $U^\lambda \subset V^\lambda$ invariante de ρ, entonces U^λ es subespacio invariante de f_H. Esto ocurre porque U^λ es subespacio invariante de cada ρ_a y f_H es combinación lineal de las ρ_a. ◂

Proposición 12. *Si observamos como actúa ρ sobre f_H, tenemos que para todo $b \in \mathcal{S}_n$*

$$\rho_b(f_H\{T\}) = f_{bHb^{-1}}(\rho_b\{T\}).$$

En el caso particular de $b \in H$, f_H es endomorfismo de ρ y, además,

$$\rho_b(f_H\{T\}) = f_H(\rho_b\{T\}) = \varepsilon(b) f_H\{T\}.$$

Demostración. Para la primera parte, realizamos el cálculo usando que el signo es multiplicativo:

$$\rho_b(f_H\{T\}) = \sum_{a\in H} \varepsilon(a)\rho_{ba}\{T\} = \sum_{a\in H} \varepsilon(bab^{-1})\rho_{bab^{-1}}(\rho_b\{T\}) = \sum_{c\in bHb^{-1}} \varepsilon(c)\rho_c(\rho_b\{T\}) = f_{bHb^{-1}}(\rho_b\{T\}).$$

Para la segunda parte, observemos que si $b \in H$, tenemos que $bHb^{-1} = H$. Continuando el cálculo,

$$\rho_b(f_H\{T\}) = f_H(\rho_b\{T\}) = \sum_{a\in H} \varepsilon(a)\rho_{ab}\{T\} = \varepsilon(b) \sum_{ab\in H} \varepsilon(ab)\rho_{ab}\{T\} = \varepsilon(b) f_H\{T\}. \qquad \blacksquare$$

Vale la pena comentar que, aunque $f_{\mathcal{S}_n}$ sea endomorfismo de ρ (pues siempre ocurre que $b \in \mathcal{S}_n$), el teorema 3 no es aplicable, porque ρ no tiene por qué ser irreducible.

Observación 5. Fijémonos en la última igualdad de la segunda parte de la proposición. En el caso de $b \in H$ con $\varepsilon(b) = -1$, tenemos que $f_H(\rho_b\{T\}) = -f_H\{T\}$. Pero además existen ciertos $b \in \mathcal{S}_n$ para los que $\rho_b\{T\} = \{T\}$, concretamente, los que solo permutan filas de T. Haciendo esta suposición extra, tenemos que $f_H\{T\} = f_H(\rho_b\{T\}) = -f_H\{T\}$ y, por tanto, $f_H\{T\} = 0$. Estos b de $\mathcal{S}_n$ que permutan filas de T son un subgrupo de $\mathcal{S}_n$, que denotaremos por $F(T)$. A su versión análoga por columnas la denotamos por $C(T)$. Y, como acabamos de ver, si existe $b \in F(T) \cap H$ con $\varepsilon(b) = -1$, entonces $f_H\{T\} = 0$. ◂

Ahora la idea consiste en utilizar la primera parte de la proposición 12 para construirnos un subespacio invariante. Efectivamente, si nos cogemos el espacio generado por imágenes de f_{H_i} siendo $\{H_i\}$ una familia de subgrupos tal que $bH_jb^{-1} \in \{H_i\}$ para cualesquiera j y $a \in \mathcal{S}_n$, entonces el subespacio $\langle \mathrm{Im}(f_{H_i})\rangle$ será invariante (por la proposición). La idea clave es tomar un H_T por cada tabloide y conseguir que la imagen de f_{H_T} sea unidimensional (lo más pequeño posible no trivial). Para ello nos interesa que $f_{H_T}\{T\} \neq 0$ y, por tanto, no querremos que $H_T \cap F(T)$ contenga permutaciones impares (por el ejemplo anterior). Pero, por otro lado, nos interesa H_T lo más grande posible porque así la imagen de f_{H_T} será más pequeña (es trivial ver que si $H' \subset H$, la imagen de f_H está contenida en la de $f_{H'}$). Un H maximal (en cierto sentido) que no comparte trasposiciones con $F(T)$ es $H = C(T)$, que es el que tomaremos.

Ejercicio 18. Probar que $C(T)$ es un subgrupo maximal en el siguiente sentido. Cualquier subgrupo H que no comparta permutaciones impares con $F(T)$ contiene, a lo sumo, las mismas trasposiciones que $C(T)$. Puede ser útil probarlo primero solo para un H que no comparta permutaciones impares con $F(T)$ y aplicar luego el teorema de Cauchy sobre la existencia de elementos de orden primo. ◂

Vale la pena comentar que, aunque H puede ser más grande que $C(T)$, al contener las mismas trasposiciones que $C(T)$, se cumple que $\dim(\mathrm{Im}(f_H)) = \dim(\mathrm{Im}(f_{C(T)}))$. Esto puede verse de la definición de f usando que $[H : C(T)]$ es impar o como corolario de la proposición 13 que enunciamos a continuación.

Proposición 13. *La aplicación $f_{C(T)}$ proyecta todo V^λ sobre una única recta, generada por $f_{C(T)}\{T\}$.*

Demostración. Gracias a la elección de $H = C(T)$, tenemos que $f_{C(T)}\{T\} \neq 0$. Para verlo basta con desarrollar el sumatorio que define f_H y observar que todos los $\rho_a\{T\}$ que aparecen son tabloides diferentes (luego no pueden cancelarse). Ahora sea $\{S\}$ un tabloide cualquiera y veamos que $f_{C(T)}\{S\}$ es un múltiplo de $f_{C(T)}\{T\}$. En el caso de que existan trasposiciones en $F(S) \cap C(T)$, la observación 5 nos dice que $f_{C(T)}\{S\} = 0$ y, por tanto, es múltiplo de $f_{C(T)}\{T\}$. Falta el caso de que no existan trasposiciones en $F(S) \cap C(T)$, para el que necesitaremos el lema 14, que presentamos a continuación. ■

Lema 14. *Sean T y S dos tablas de Young de forma λ. Supongamos que no existen i, j diferentes que estén en la misma fila de S y misma columna de T (es decir, $\nexists (ij) \in F(S) \cap C(T)$). Entonces existen $a \in F(S)$ y $b \in C(T)$ tales que $\rho_b(T) = \rho_a(S)$.*

Demostración. Consideremos los λ_1 números diferentes que están en la primera fila de S. Por hipótesis, están en las λ_1 columnas diferentes de T (ya que no puede haber dos en la misma columna de T). Por lo tanto, existe una permutación $b_1 \in C(T)$ que lleva estos λ_1 números a la primera fila de T. Observamos que $\rho_{b_1}(T)$ y S tienen los mismos números en su primera fila (aunque estén ordenados diferente). Podríamos seguir este razonamiento con la segunda fila de S y obtener $b_2 \in C(T)$ tal que $\rho_{b_2 b_1}(T)$ y S tengan los mismos números en las dos primeras filas. Procediendo sucesivamente, tenemos $b = b_r \dots b_2 b_1 \in C(T)$ tal que $\rho_b(T)$ y S tienen los mismos números en sus filas. Por lo tanto, como solo se diferencian en el orden de sus filas, existe $a \in F(S)$ tal que $\rho_b(T) = \rho_a(S)$. ∎

Este lema permite concluir la demostración de la proposición 13. Considerando los tabloides generados por T y S tenemos que $\rho_b\{T\} = \rho_a\{S\} = \{S\}$ ya que $a \in F(S)$. Por lo tanto, $f_{C(T)}\{S\} = f_{C(T)}\rho_b\{T\} = \varepsilon(b) f_{C(T)}\{T\}$ utilizando la proposición 12.

Definición 11. Definimos el **politabloide** generado por T como $e_T = f_{C(T)}\{T\}$. Al subespacio generado por todos los politabloides e_T se lo llama **subespacio de Specht** y lo denotaremos por W^λ. ◂

Observación 6. Los politabloides son no nulos (en la demostración de la proposición 13 ya explicamos que $f_{C(T)}\{T\} \neq 0$). Pero, además, $f_{C(T)}$ es no idénticamente nula sobre el espacio de Specht porque

$$f_{C(T)}(e_T) = f_{C(T)}^2\{T\} = \sum_{a,b \in C(T)} \varepsilon(ab)\rho_{ab}\{T\} = |C(T)| \sum_{c \in C(T)} \varepsilon(c)\rho_c\{T\} = |C(T)| e_T \neq 0. \quad \blacktriangleleft$$

Ejemplo 19. Sea $n = 3$ y sea $\lambda = (2,1)$. Consideremos las tablas T_1, T_2 y T_3 de la figura 6. Consideremos $f_{C(T_1)}$, que viene definido por $f_{C(T_1)}(u) = u - \rho_{(13)}(u)$ para cualquier $u \in V^\lambda$. Podemos observar cómo $f_{C(T_1)}\{T_2\} = -f_{C(T_1)}\{T_1\} \neq 0$, ya que estamos en el caso en el que $F(T_2)$ y $C(T_1)$ no comparten trasposiciones. Por otro lado, $f_{C(T_1)}\{T_3\} = 0$, ya que la trasposición (13) está tanto en $C(T_1)$ como en $F(T_3)$. ◂

$$T_1 = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} \qquad T_2 = \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array} \qquad T_3 = \begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 \\ \cline{1-1}\end{array}$$

$$e_{T_1} = \begin{array}{\overline{cc}}\overline{1\ 2} \\ 3 \end{array} - \begin{array}{\overline{cc}}\overline{2\ 3} \\ 1 \end{array} \qquad e_{T_2} = \begin{array}{\overline{cc}}\overline{2\ 3} \\ 1 \end{array} - \begin{array}{\overline{cc}}\overline{1\ 3} \\ 2 \end{array} \qquad e_{T_3} = \begin{array}{\overline{cc}}\overline{1\ 3} \\ 2 \end{array} - \begin{array}{\overline{cc}}\overline{1\ 2} \\ 3 \end{array}$$

Figura 6: Algunas tablas de Young para $n = 3$ con sus respectivos politabloides.

Ejemplo 20. Continuando con la figura 6, podemos ver los politabloides e_{T_1}, e_{T_2} y e_{T_3}. Por supuesto, existirían otros tres más (ya que hay seis tablas), pero se puede comprobar que son estos tres cambiados de signo. Por lo tanto, estos tres ya generan todo W^λ. Además, podemos ver cómo $e_{T_1} + e_{T_2} + e_{T_3} = 0$, de manera que no son linealmente independientes. Tenemos, por tanto, $\dim(W^\lambda) = 2$. De hecho, la representación sobre W^λ será isomorfa a la estándar. Para verlo, hemos de pensar en los politabloides e_{T_1}, e_{T_2} y e_{T_3} dentro de la figura 3. Se puede comprobar que ρ actúa sobre los e_{T_i} igual que lo hace en la figura 3 sobre los puntos resultantes de girar 30° los puntos 1, 2 y 3. Otra forma más metódica de comprobar que esta representación es isomorfa a la estándar es calcular su carácter y utilizar el corolario 9. ◂

Ejemplo 21. Sea $n = 3$ y sea $\lambda = (1,1,1)$. En este caso $C(T) = \mathcal{S}_3 = C(S)$ para cualquier tabla T, por lo que $e_S = f_{C(S)}\{S\} = f_{C(T)}\{S\} \in \langle e_T \rangle$, por la proposición 13, y todos los politabloides están en la misma recta. Es decir, $\dim(W^\lambda) = 1$. De hecho, usando la segunda parte de la proposición 12, tenemos que $\rho_b(e_T) = \rho_b(f_{S_n}\{T\}) = \varepsilon(b) f_{S_n}\{T\} = \varepsilon(b) e_T$. Por lo tanto, estamos ante la representación alternada. ◂

Como ya vemos de los ejemplos, aunque los e_{T_i} no son una base (no son independientes), sí que generan un W^λ sobre el cual ρ es irreducible. Las proposiciones 12 y 13 serán las herramientas principales para probarlo. Solo nos falta un pequeño lema sobre el comportamiento de $C(\rho_a(T))$. La demostración se puede intentar como ejercicio. También se puede consultar la demostración en la bibliografía [1, 5].

Lema 15. *Sean T una tabla y $a \in \mathcal{S}_n$. Entonces se cumple que $C(\rho_a(T)) = aC(T)a^{-1}$.*

Teorema 16. *El subespacio de Specht W^λ es un subespacio invariante de ρ. Además, al restringir ρ a W^λ obtenemos una representación irreducible.*

Demostración. En primer lugar veamos que W^λ es invariante. Basta con ver que $\rho_a(e_T) \in W^\lambda$, porque los politabloides son generadores de W^λ. En efecto,

$$\rho_a(e_T) = \rho_a(f_{C(T)}\{T\}) = f_{aC(T)a^{-1}}(\rho_a\{T\}) = f_{C(\rho_a(T))}(\rho_a\{T\}) = e_{\rho_a(T)} \in W^\lambda,$$

donde hemos utilizado la primera parte de la proposición 12 y el lema 15.

Veamos ahora que ρ es irreducible sobre W^λ. Usando el teorema 1 descomponemos $W^\lambda = U_1 \oplus \ldots \oplus U_r$. Sea T un tabloide cualquiera; como $\ker(f_{C(T)}) \neq W^\lambda$ (observación 6), existe algún U_i que no está estrictamente contenido en $\ker(f_{C(T)})$. Sea $u \in U_i$ tal que $f_{C(T)}(u) \neq 0$. Por la proposición 13, tenemos que $\mathrm{Im}(f_{C(T)}) = \langle e_T \rangle$ y por la observación 4 tenemos que $f_{C(T)}(u) \in U_i$. De todo ello concluimos que $e_T \in U_i$. Ahora sea S otra tabla cualquiera, y sea $a \in \mathcal{S}_n$ la permutación tal que $\rho_a(T) = S$. Como U_i es invariante, $\rho_a(e_T) \in U_i$, pero, como hemos visto arriba, $\rho_a(e_T) = e_{\rho_a(T)} = e_S$. Por lo tanto, $e_S \in U_i$ para cualquier tabla S, siendo $U_i = W^\lambda$ el único subespacio invariante. ∎

Teorema 17. *Las representaciones ρ^λ restringidas a los subespacios W^λ son todas las representaciones irreducibles del grupo simétrico $\mathcal{S}_n$.*

Demostración. El corolario 9 unido al hecho de que $\mathcal{S}_n$ tiene $p(n)$ clases de conjugación nos dice que $\mathcal{S}_n$ tiene $p(n)$ representaciones irreducibles. Nosotros hemos construido $p(n)$ representaciones irreducibles, las ρ sobre W^λ, para cada partición λ. Faltaría ver que todas ellas son no equivalentes entre sí. La demostración puede enfocarse como la del teorema 16, pero en este caso viendo que $f_{C(S)} \equiv 0$ sobre V^λ cuando S no proviene de la partición λ. Cuando S era una λ-tabla, teníamos que $\mathrm{Im}(f_{C(S)}) = \langle e_S \rangle$; ahora tendremos que $\mathrm{Im}(f_{C(S)}) = \{0\}$. La prueba de este paso puede consultarse en la bibliografía [3, 5]. ∎

Teorema 18. *Una posible base para este espacio de politabloides consiste en tomar solo los politabloides generados por tablas estándar.*

Recordemos que una tabla es estándar si sus filas y columnas están en orden creciente.

Corolario 19. *Para cada λ partición de n, sea n_λ la cantidad de tablas estándar. Entonces, del corolario 10 se deduce que $n! = \sum n_\lambda^2$, ya que los n_λ son también las dimensiones de las representaciones irreducibles.*

La demostración del teorema 18 no la haremos y se puede encontrar en la bibliografía [3, 5]. La idea básica consiste en introducir una relación de orden en los tabloides según lo arriba o abajo que están los números. Para comparar $\{T\}$ y $\{S\}$ miramos el número más grande que esté en filas diferentes en ambos, llamémosle i. Si i está más arriba en $\{T\}$ que en $\{S\}$, decimos que $\{T\} < \{S\}$; en caso contrario, $\{S\} < \{T\}$. Esta relación de orden tiene la propiedad de que $\rho_a\{T\} \leq \{T\}$ para tablas estándar. Usando esta propiedad es fácil ver que los politabloides generados por tablas estándar son independientes. Lo que es más difícil es ver que generan todo W^λ. Una posible manera de probarlo es introducir un algoritmo que expresa los politabloides no estándar en función de los estándar: el *straightening algorithm*. Esta es la vía seguida en el artículo de McNamara [5]. Otra manera consiste en probar primero el corolario 19 mediante argumentos combinatorios y deducir, por cálculo de dimensiones, que los politabloides estándar son base de W^λ. Esta vía alternativa se encuentra en el libro de Fulton [3].

Ejemplo 22. En el ejemplo 20 ya vimos que para $\lambda = (2,1)$ obtenemos un W^λ de dimensión 2, con una posible base $\{e_{T_1}, e_{T_2}\}$. Pero si nos fijamos en la figura 6, las tablas T_1 y T_2 son exactamente las dos únicas tablas estándar para $\lambda = (2,1)$. Por lo tanto, vemos que se cumple el teorema 18. ◂

Ejemplo 23. Tanto para $\lambda = (3)$ como para $\lambda = (1,1,1)$ tenemos una única tabla estándar, siendo $n_{(3)} = n_{(1,1,1)} = 1$. Para $\lambda = (2,1)$ tenemos dos tablas estándar, de forma que $n_{(2,1)} = 2$. Podemos comprobar cómo

$$\sum_\lambda n_\lambda^2 = 1^2 + 1^2 + 2^2 = 6 = 3!.$$

Esto no es más que la igualdad combinatoria que habíamos presentado en la introducción. ◂

Ejemplo 24. En los ejemplos de este artículo hemos descrito las tres representaciones irreducibles de $\mathcal{S}_3$: la trivial, la alternada y la estándar. Todas ellas están dentro de la regular y, además, cada una está tantas veces como su dimensión (corolario 8). La trivial y la alternada son de dimensión 1 y la estándar es de dimensión 2. Por tanto, podemos visualizar la parte real de la representación regular (en $\mathbb{R}^6$) visualizando sus tres representaciones irreducibles (para el caso de la estándar, repetida). Podemos ver esto en la figura 7. ◂

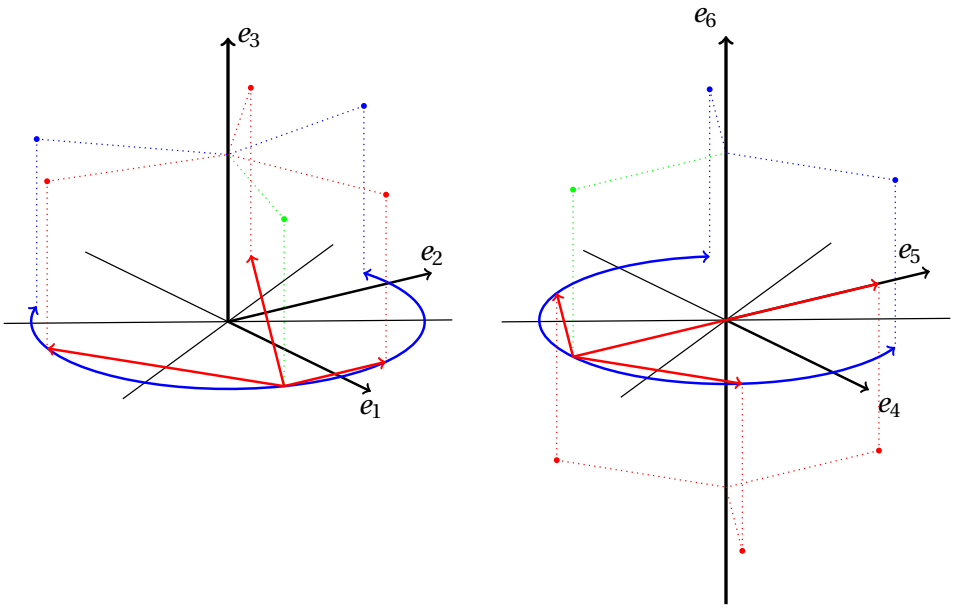

Figura 7: Dibujo esquemático de la representación regular de $\mathcal{S}_3$. En la recta $\langle e_3 \rangle$ tenemos la representación trivial y en la recta $\langle e_6 \rangle$ tenemos la alternada. En los planos $\langle e_1, e_2 \rangle$ y $\langle e_4, e_5 \rangle$ tenemos la representación estándar. En verde, un punto genérico de $\mathbb{R}^6 \subset \mathbb{C}^6$. En azul, sus imágenes por los 3-ciclos, y en rojo, sus imágenes por las trasposiciones.

Referencias

[1] Choi, Je-Ok. «The Representations of the Symmetric Group». 25 de ago. de 2010. URL: http://www.math.uchicago.edu/~may/VIGRE/VIGRE2010/REUPapers/Choi.pdf.

[2] Frobenius, Ferdinand Georg. *Über die Charaktere der symmetrischen Gruppe*. Königliche Akademie der Wissenschaften, 1900. https://doi.org/10.3931/e-rara-18862.

[3] Fulton, William. *Young Tableaux: With Applications to Representation Theory and Geometry*. London Mathematical Society Student Texts. Cambridge: Cambridge University Press, 1996. https://doi.org/10.1017/CBO9780511626241.

[4] Kowalski, Emmanuel. *Representation Theory*. ETH Zürich. 17 de feb. de 2017. URL: https://people.math.ethz.ch/~kowalski/representation-theory.pdf.

[5] McNamara, Redmond. «Irreducible Representations of the Symmetric Group». Ago. de 2013. URL: http://math.uchicago.edu/~may/REU2013/REUPapers/McNamara.pdf.

[6] Serre, Jean-Pierre. *Linear representations of finite groups*. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977, págs. x+170. https://doi.org/10.1007/978-1-4684-9458-7.

[7] Young, Alfred. «On Quantitative Substitutional Analysis». En: *Proceedings of the London Mathematical Society* 33 (1901), págs. 97-146. ISSN: 0024-6115. https://doi.org/10.1112/plms/s1-33.1.97.

[8] Young, Alfred. «On Quantitative Substitutional Analysis (Second Paper)». En: *Proceedings of the London Mathematical Society* 34 (1902), págs. 361-397. ISSN: 0024-6115. https://doi.org/10.1112/plms/s1-34.1.361.

[9] Young, Alfred. «On Quantitative Substitutional Analysis». En: *The Journal of the London Mathematical Society* 3.1 (1928), págs. 14-19. https://doi.org/10.1112/jlms/s1-3.1.14.

[10] Young, Alfred. «On Quantitative Substitutional Analysis (Third Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 28.4 (1928), págs. 255-292. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-28.1.255.

[11] Young, Alfred. «On Quantitative Substitutional Analysis (Fourth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 31.4 (1930), págs. 253-272. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-31.1.253.

[12] Young, Alfred. «On Quantitative Substitutional Analysis (Fifth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 31.4 (1930), págs. 273-288. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-31.1.273.

[13] Young, Alfred. «Corrigenda. On Quantitative Substitutional Analysis». En: *Proceedings of the London Mathematical Society. Second Series* 31.7 (1930), pág. 556. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-31.1.556-t.

[14] Young, Alfred. «On Quantitative Substitutional Analysis (Sixth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 34.3 (1932), págs. 196-230. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-34.1.196.

[15] Young, Alfred. «On Quantitative Substitutional Analysis (Seventh Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 36 (1934), págs. 304-368. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-36.1.304.

[16] Young, Alfred. «On Quantitative Substitutional Analysis (Eighth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 37.1 (1934), págs. 441-495. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-37.1.441.

[17] Young, Alfred. «On quantitative substitutional analysis (Ninth Paper)». En: *Proceedings of the London Mathematical Society. Second Series* 54 (1952), págs. 219-253. ISSN: 0024-6115. https://doi.org/10.1112/plms/s2-54.3.219.

A. Anexo: resolución de ejercicios

Solución del ejercicio 6. Para ver que la representación regular de $\mathcal{S}_n$ contiene la representación trivial, lo natural es considerar la recta $\langle(1,1,\dots,1)\rangle = V_1$. Parametricemos los puntos de $x \in V_1$ con el número complejo c, donde $x = (c,c,\dots,c)$. Si ρ es la representación regular, $\rho_a(x)$ será el resultado de permutar las coordenadas de x según a. Pero, como todas son iguales, obtendremos $(c,c,\dots,c)$, independientemente de la permutación $a \in \mathcal{S}_n$. Por tanto, V_1 es subespacio invariante, y ρ_a restringida a V_1 es la identidad. Es decir, la representación regular restringida a V_1 es la trivial.

Para ver que ρ contiene la representación alternada, recordemos que en la representación regular las coordenadas van indexadas por permutaciones $\{a_i\} = \mathcal{S}_n$. Consideremos la recta $\langle(\varepsilon(a_1),\varepsilon(a_2),\dots,\varepsilon(a_{n!}))\rangle = V_2$. Si consideramos $x = (c\varepsilon(a_1),c\varepsilon(a_2),\dots,c\varepsilon(a_{n!})) \in V_2$, tenemos que $\rho_b(x)$ será el resultado de permutar las coordenadas de x por $b \in \mathcal{S}_n$. De esta forma, la coordenada a_i irá a parar a la coordenada ba_i. Por tanto, el valor de la coordenada i-ésima de $\rho_b(x)$ será $\varepsilon(b^{-1}a_i) = \varepsilon(b)\varepsilon(a_i)$. De ahí se deduce $\rho_b(x) = \varepsilon(b)x$, para todo $x \in V_2$, por lo que V_2 es subespacio invariante, y la representación regular restringida a V_2 es la alternada. ∎

Solución del ejercicio 13. Queremos ver que dos permutaciones de $\mathcal{S}_n$ son conjugadas si y solo si sus ciclos son del mismo tamaño. Consideremos $a, b \in \mathcal{S}_n$ conjugadas, es decir, $ca = bc$, con $c \in \mathcal{S}_n$. Esto quiere decir que si a envía i a $a(i)$, b enviará $c(i)$ a $c(a(i))$. Es decir, b hace exactamente lo mismo que a pero sobre la imagen de c.

En particular, si tenemos el ciclo $(i, a(i), a^2(i), \dots, a^k(i))$ en a, tenemos el ciclo

$$(c(i), bc(i), b^2c(i), \dots, b^kc(i)) = (c(i), ca(i), ca^2(i), \dots, ca^k(i))$$

en b, de la misma longitud, y como c es una biyección, los ciclos de a y b son de los mismos tamaños. Recíprocamente, si los ciclos son de los mismos tamaños, podemos construir c que envíe cada ciclo de a a un ciclo de b del mismo tamaño y, además, preservando el orden dentro del ciclo. De esa manera, si $a(i)$ es el siguiente número a i en un ciclo de a, $c(a(i))$ será el siguiente número a $c(i)$ en un ciclo de b. Es decir, $bc(i) = ca(i)$, y como esto es para todo i, entonces, $bc = ca$, siendo a y b conjugados. ■

Solución del ejercicio 17. Supongamos que una partición $\lambda = (n_1, n_2, \dots, n_k)$ nos da una representación ρ irreducible sobre V^λ. Consideremos su carácter φ. Ya sabemos que si ρ es irreducible, entonces $(\varphi|\varphi) = 1$, pero el recíproco también es cierto (trivial por el corolario 8, por ejemplo). Ahora tratemos de calcular $(\varphi|\varphi)$ explícitamente. Para calcular φ, tomamos la base de los tabloides y vemos que

$$\varphi(a) = \mathrm{Tr}(\rho_a) = \#\{\lambda - \text{tabloides que fijan a}\} = m_a,$$

donde hemos definido m_a como la cantidad de tabloides que fija a. Esta igualdad es más fácil de entender en forma matricial: ρ_a es una matriz llena de ceros excepto en las entradas $(\{T\}, \{S\})$ tales que $\rho_a\{T\} = \{S\}$, donde la matriz tiene entrada uno. Por lo tanto, la traza es la cantidad de unos en la diagonal, es decir, la cantidad de tabloides tales que $\rho_a\{T\} = \{T\}$. Si ahora calculamos $(\varphi|\varphi)$ y aplicamos la desigualdad de medias cuadrática-aritmética,

$$(\varphi|\varphi) = \frac{\sum_a m_a^2}{|\mathcal{S}_n|} \geq \left(\frac{\sum_a m_a}{|\mathcal{S}_n|}\right)^2.$$

La suma de los m_a es fácil de computar utilizando la típica técnica combinatoria de doble conteo: en vez de sumar para a la cantidad de tablas fijas por a, sumaremos para $\{T\}$ la cantidad de permutaciones que fijan $\{T\}$. Esta cantidad es trivialmente $n_1!n_2!\dots n_k!$ (podemos permutar cada fila como queramos). Esa cantidad se suele denotar como $\lambda! = n_1!\dots n_k!$. Tenemos que

$$\sum_{a\in\mathcal{S}_n} m_a = \sum_{\{T\}} \lambda! = \#\{\lambda - \text{tabloides}\}\lambda! = \#\{\lambda - \text{tablas}\} = n!.$$

Esto viene de que la cantidad de tablas es la cantidad de tabloides por la cantidad de maneras de ordenar las filas (que es $\lambda!$). Por otro lado, es obvio que hay $n!$ tablas porque hay $n!$ maneras de colocar los n números en la tabla. Ahora ya hemos acabado porque

$$(\varphi|\varphi) \geq \left(\frac{\sum_a m_a}{|\mathcal{S}_n|}\right)^2 = \left(\frac{n!}{n!}\right)^2 = 1,$$

de lo que se deduce que, si ρ es irreducible, estamos en el caso de igualdad de la desigualdad de medias. Dicho caso se alcanza cuando todos los m_a son iguales; en particular, serán iguales a $m_1 = \#\{\text{tabloides}\}$, ya que $\rho_1 = \mathrm{Id}$ fija todos los tabloides. Luego cualquier ρ_a fija todos los tabloides. Esto implica que los tabloides solo tienen una fila, porque si hubiera dos filas (es decir, $\lambda \neq (n)$), para cualquier tabloide $\{T\}$ podríamos escoger como a una trasposición entre un número de la primera fila y uno de la segunda. Claramente, dicho ρ_a no fijaría $\{T\}$ y estaríamos ante una contradicción. ■

Solución del ejercicio 18. En primer lugar, supongamos un H con más trasposiciones que $C(T)$ pero que no comparte ninguna con $F(T)$. Sea (ij) una trasposición de $H - C(T)$. Es obvio que (ij) no está ni en $C(T)$ ni en $F(T)$ y, por tanto, i y j no comparten ni fila ni columna en T. Sin pérdida de generalidad supongamos que la fila de i es previa a la de j; entonces, existe una casilla en la tabla que tiene la columna de i y la fila de j. Supongamos dicha casilla ocupada por el número k. Tenemos que $(ik) \in C(T) \subset H$, luego $(ik)(ij)(ik) \in H$ ya que todos los elementos del producto están en H. No obstante, $(ik)(ij)(ik) = (jk) \in F(T)$, y esto contradice que H y $F(T)$ no compartan trasposiciones.

Ahora extrapolemos el resultado a permutaciones impares cualesquiera. Si $F(T)$ y H comparten permutaciones impares, entonces $F(T) \cap H$ no es subgrupo del grupo alternado $\mathcal{A}_n$. De esta manera, $[F(T) \cap H : F(T) \cap H \cap \mathcal{A}_n]$ es un divisor de $[\mathcal{S}_n : \mathcal{A}_n] = 2$ que no es 1. Por lo tanto, es 2 y tenemos que $|F(T) \cap H|$ es par. Aplicando el teorema de Cauchy para la existencia de elementos primos para $p = 2$ tenemos que existe alguna trasposición en $F(T) \cap H$, lo cual contradice el resultado previo. ■

TEMat, volumen 2. Julio de 2018.
e-ISSN: 2530-9633