ISSN: 2174 - 503 X
DL: M - 28040 - 2011
URL: www.matgazine.tk

MATGAZINE
REVISTA DE MATEMÁTICAS

Número 3, Junio 2012

Asociación cultural **Lewis Carroll**
Aula S-202, Facultad de Ciencias Matemáticas,
Universidad Complutense de Madrid (UCM)
Ciudad Universitaria, Plaza de las Ciencias 3, 28040, Madrid

Cómo publicar en Matgazine

Matgazine es una revista gestionada por alumnos, lo que se publique en ella debe ser entendido por los mismos. Esto no quiere decir que todos los alumnos tengan que entender el artículo, sino que el tema tratado lo pueda seguir un alumno universitario que tenga suficiente interés y asignaturas básicas cursadas.

En segundo lugar debes mandar el artículo en formato .tex siguiendo la plantilla y la guía de estilo que podrás encontrar en nuestra página web `www.matgazine.tk`.

En **Matgazine** tenemos distintas secciones, ¡elige en cuál quieres participar!

- **Artículos**: es la sección principal de la revista. Aquí entran los trabajos de investigación o divulgación realizados por alumnos. En esta sección permitimos que haya, a lo sumo, un artículo de divulgación escrito por un profesor de matemáticas. Estos artículos deberán ser rigurosos y estar documentados con la bibliografía oportuna.

- **Problemas y soluciones**: en esta sección se publican los problemas y las soluciones propuestos. Pedimos que los problemas propuestos vayan acompañados de la solución y que sean originales o poco conocidos suficientemente documentados.

- **Curiosidades**: si quieres escribir algo no demasiado complejo pero que tenga un interés especial ésta es tu sección. Debe tener un nivel de dificultad suficientemente bajo, pues para cosas más complejas está la sección de artículos. Tendrá un marcado carácter divulgativo.

- **Pasatiempos**: aquí puedes mandarnos pasatiempos de todo tipo que tengan que ver con las matemáticas. Pueden ser originales o no, pero si no lo son deberán tener el permiso del autor.

- **Biblioteca**: si has leído algún libro de matemáticas que te haya gustado ésta es la sección para hacer la reseña.

Índice

Editoriales

Una vez más, un número de **Matgazine** cruza la geografía española, y con éste van 4.

En el último año hemos conseguido unas cuantas cosas. La primera es que parece que por fin nuestra situación económica se ha estabilizado, gracias al apoyo que hemos recibido de DECIDE Soluciones[1], que ha ofrecido su ayuda sin pedir nada a cambio. De paso, como sabéis, nuestra revista ha llegado ya a seis ciudades de España, y procuraremos que llegue a muchas más. Aprovechamos para animar a quien pueda leer esto y en cuya facultad no se distribuya **Matgazine** a ponerse en contacto con nosotros para colaborar en la difusión del proyecto.

Y ya que estamos hablando de colaborar, queremos invitar a todo estudiante de matemáticas a que nos ayude a superar el próximo reto que se nos presenta: el de sobrevivir con éxito al paso de una generación. Todo tiene que llegar a su fin, y afortunadamente, nosotros acabamos nuestras carreras y alguien tiene que ocupar nuestros puestos y escribir más artículos. Aunque ya hemos conseguido que alguna gente de los primeros cursos de la carrera se anime a colaborar, desde aquí te invitamos a que contactes con nosotros si tienes ganas de ayudar con cualquier cosa. Necesitamos de todo: si tienes una idea para un artículo (o simplemente ganas, nosotros te podemos dar ideas), una curiosidad, alguien a quien entrevistar, una caricatura, energía para buscar erratas... Todo es útil y muy necesario si esta revista ha de llegar a los 1729 números[2].

Los estudiantes de la Complutense ya no tenéis excusa para no responder a esta invitación: todo parece indicar que el curso de introducción a LaTeX que hemos organizado ha sido un éxito: ambas clases llenas y los que vinisteis no os habéis quejado. Además, hemos organizado un ciclo de conferencias de lógica, con las charlas de Ignacio Sols, Pepe Ruiz, Paco López y Javier Fresán, a los que agradecemos que se prestaran a hablarnos sobre el tema. Pero sobre todo, queremos agradecer a Pedro Ángel, que organizó las conferencias prácticamente él solo (según él, con ayuda de Ignacio Sols y Vicente Muñoz), con su habitual energía y entusiasmo, que sospechamos que fueron los únicos artífices de que esta revista empezara a rodar. Esperemos que, con él en el extranjero, nos quede algo de su energía para que esto siga funcionando.

[1] `www.decidesoluciones.es`

[2] $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

Tengo que contar otro gran éxito para **Matgazine**: conseguir una entrevista con el profesor Efim Zelmanov, que tenéis entre las manos.

Con la marcha de Pedro Ángel he quedado yo, Moisés Herradón, como director de **Matgazine**. Sobre esto, quiero decir que procuraré hacer todo lo que esté en mi mano para que no perdamos este tirón con el que hemos empezado y mantengamos este nivel de actividad, sobre todo consiguiendo que llegue nueva gente a trabajar con nosotros. Y ya que empiezo, voy a pedir perdón porque este número llegue un mes tarde: para el próximo habrá mejor organización.

El director
Moisés Herradon Cueto
`moises_herradon@yahoo.es`

Editorial del director saliente, Pedro Ángel Castillejo

Como dice Moisés, todo tiene que llegar a su fin. Y éste es mi caso como director de la revista. Hace ya año y medio decidimos comenzar este proyecto, cuyo objetivo inicial era el de fomentar el trabajo de los estudiantes de matemáticas. La verdad es que no sólo se ha cumplido este objetivo, sino que además se ha conseguido una colaboración de la que todos podemos estar orgullosos. Frente a la competitividad que recorre nuestros tiempos, **Matgazine** se ha convertido en un oasis de cooperación y compañerismo que está permitiendo ir más allá de lo que cualquiera de los que fundamos la revista habríamos podido imaginar.

Esta marcha supondrá la prueba definitiva para la revista: este tipo de proyectos suelen personalizarse, suelen recaer en un pequeño grupo de personas que son las que acaban tirando del carro, pero la renovación parcial del consejo editorial nos permitirá saber si hemos hecho bien el trabajo, pues si **Matgazine** sigue adelante habremos probado que las ganas de hacer una revista de matemáticas por estudiantes no respondía a la voluntad de unos pocos, sino que realmente quieren y están dispuestos a trabajar por una auténtica revista de matemáticas.

En lo personal esta revista me ha permitido conocer a muchísima gente trabajadora. Nunca pensé que iba a encontrar tanta gente tan dispuesta a colaborar, desde compañeros que se dedican a buscar erratas a compañeros que nos ayudan a difundir y vender la revista, pasando por los autores de los artículos o la gente que nos hace recomendaciones para tratar de mejorar nuestra revista. Al fin y al cabo, nuestra revista es su revista. Es tu revista.

Por ello siento una mezcla de alegría y tristeza al dejar la dirección de **Matgazine**: alegría porque la revista seguirá, y porque por fin podré dejar de lado las cuestiones de gestión y administrativas para dedicarme a escribir cosillas, que era la idea inicial; tristeza porque probablemente echaré de menos las estupendas experiencias que he tenido con mis compañeros, ahora amigos, gestionando y administrando la revista. Pero en el fondo esta tristeza es un síntoma de que el trabajo ha dado sus frutos, por lo que si hay un sentimiento que pueda describir mi estado de ánimo es el de satisfacción. Satisfacción y tranquilidad, porque sé que la revista queda en buenísimas manos: no sólo el consejo editorial es excepcional, sino que el director entrante, Moisés Herradón, además de ser un grandísimo matemático, compañero y amigo, es capaz de encabezar este proyecto con humildad, dedicación y, como pronto veremos, buenísimos resultados. Gracias por mantener viva la ilusión de **Matgazine**.

Sólo espero que los valores que considero que han guiado a la revista en todo momento sigan estando presentes, no sólo en **Matgazine**, sino en todas las personas que hayáis leído la revista. Estos valores de cooperación, compañerismo, solidaridad, altruismo y colaboración deben siempre ir orientados hacia el conocimiento: debemos ir hacia él, cuidarlo y defenderlo de aquellos que pretenden hacer negocio con él. El conocimiento es un fin, no un medio. Y los fines, los resultados, no hay que dejarlos estar, sino que hay que llegar a ellos:

> "Pues la cosa no se agota en sus *fines*, sino en el proceso de su *ejecución*, ni el *resultado* es el todo *efectivo*, sino que lo es conjuntamente con su devenir; la meta, tomada para sí, es lo universal sin vida, igual que la tendencia es el mero afán que todavía carece de su realidad efectiva, y el resultado desnudo es el cadáver que la tendencia deja tras de sí." (Hegel, Fenomenología del espíritu, p. 59).

Por ello os animo a todos a que no os conforméis con la revista en vuestras manos como si fuese un mero resultado, como si de un punto y final se tratase, y que participéis en el proceso de ejecución de esta revista. No os arrepentiréis. Yo no me arrepiento.

Gracias. De todo corazón, gracias.

El director (saliente)
Pedro Ángel Castillejo
pedroangelcastillejo@gmail.com

Joaquín Hernández es catedrático en el IES San Juan Bautista, profesor asociado en la facultad de matemáticas de la Universidad Complutense y miembro del comité organizador de cada concurso matemático de secundaria que se organiza en la Comunidad de Madrid. Pero sobre todo, es una de las personas con más compromiso, dedicación, talento y sobre todo energía y ganas por la enseñanza que hemos conocido. Quizás los que lo conocemos estaríamos estudiando matemáticas aunque no lo hubiéramos conocido, pero desde luego no lo haríamos con la mitad de ilusión con la que lo hacemos ahora. Desde Matgazine queremos darte las gracias por todo y todos los ánimos del mundo para que estés en septiembre de nuevo al pie del cañón.

Actualidad y Novedades

Sección a cargo de

Irene de Parada Muñoz

Una aplicación experimental del algoritmo cuántico

Investigadores de la empresa canadiense Systems D-Wave han realizado cálculos con 84 qubits (bits cuánticos) en un ordenador cuántico experimental, dando cierto rigor a la viabilidad de los verdaderos ordenadores cuánticos, que podrían superar ampliamente las capacidades de todos los basados en la tecnología tradicional.

Estos equipos se diferencian en que pueden utilizar los fenómenos de la mecánica cuántica para realizar operaciones sobre datos, en lugar de las simples transacciones binarias. Así, mientras que los bits de los ordenadores actuales toman los valores 0 y 1, la física cuántica permite a partículas, como un átomo, un electrón o un fotón, estar en dos sitios a la vez, lo que quiere decir que pueden representar el 0 y el 1 al mismo tiempo, permitiendo hacer cálculos mucho más complejos y con mucha mayor rapidez.

En la investigación se trabajó para resolver los números de Ramsey, $R(m, 2)$, donde $m = 4$, 5, 6, 7 y 8. El problema de Ramsey generaliza el principio del palomar (si tenemos n nidos y $kn + 1$ palomas, entonces al menos $k + 1$ de ellas duermen en el mismo nido). La particularización del teorema de Ramsey que se ha pretendido resolver es la siguiente: dados unos enteros p y q, encontrar el mínimo entero $r = R(p, q)$ tal que para cualquier coloración con dos colores (por ejemplo, azul y rojo) de las aristas del grafo K_r (el grafo K_n tiene n vértices y todas las aristas posibles) haya contenido un subgrafo K_p cuyas aristas estén todas coloreadas de rojo o bien un subgrafo K_q con todas sus aristas azules. Un ejemplo de este problema es: en cualquier reunión de 6 personas, o bien 3 de ellas se conocen entre sí, o bien 3 de ellas no se conocen entre sí, es decir, $R(3, 3) \leq 6$. Como esto no ocurre necesariamente con 5 personas, $R(3, 3) = 6$.

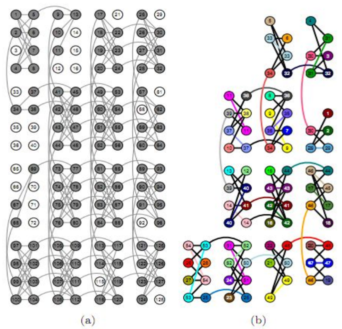


Figura 1: Izquierda: Diseño de qubits y acopladores. Derecha: R(8, 2) sumergido con la conectividad de los qubits.

¿Cómo rompe una ola?

El moderno y ya prestigioso Clay Mathematics Institute (CMI) de Massachussets es una fundación sin fines de lucro, dedicada a promocionar el conocimiento matemático y que otorga premios e incentivos para matemáticos prometedores. Dicho instituto estableció en mayo de 2000 los siete problemas del Milenio, cuya resolución está premiada con un millón de dólares.

Uno de estos siete problemas (hasta el momento sólo se ha resuelto la conjetura de Poincaré) son las Ecuaciones de Navier-Stokes, formuladas en el siglo XIX, y que se refieren a la dinámica de fluidos. Estas ecuaciones, muy complejas, son esenciales hoy en día en simulaciones de clima y en ingeniería aeronáutica. Pero estas ecuaciones no explican cómo se comportará un fluido a lo largo del tiempo bajo ciertas condiciones.

Un equipo integrado por cuatro matemáticos españoles y un estadounidense ha resuelto un aspecto concreto del problema: han descrito matemáticamente cómo se produce la ruptura de una ola, abriendo vías para acercarse al problema del Milenio.

Lo que el trabajo ahora publicado demuestra es que, en las ecuaciones que hoy en día se usan para describir el movimiento de los fluidos, puede formarse lo que los matemáticos llaman una singularidad; es lo que ocurre, por ejemplo, cuando se forma un tornado, rompe una ola, o cuando un fluido se vuelve turbulento. El fenómeno se traduce en que una de las variables que describen ese fluido, como su presión, su velocidad, etc, cambia de forma explosiva y alcanza un valor infinito.

El problema planteado por el CMI preguntaba que si, bajo determinadas condiciones, un fluido, que no está en contacto con ninguna otra sustancia (algo que no se da en la realidad), empieza a moverse de forma suave y laminar, a lo largo del tiempo el movimiento seguirá siendo regular, sin cambios bruscos (singularidades).

Los autores del trabajo han demostrando que no seguirá siendo regular, que habrá singularidades, pero en distintas condiciones: su fluido (el agua) sí está en contacto con otra sustancia (el aire), y además no se considera la viscosidad. Sin embargo, se trata de la primera vez que se logra demostrar que las singularidades existen en tales ecuaciones, a pesar de que son ya muy antiguas. De ahí la relevancia del resultado obtenido.

Centenario del nacimiento de Alan Turing

En este aniversario queremos recordar al matemático, lógico, criptógrafo y teórico de la computación Alan Turing. Considerado el precursor de la informática moderna, reformuló los resultados de Gödel sobre los límites de la demostrabilidad mediante la hoy conocida como Máquina de Turing. Probó que ésta era capaz de implementar cualquier problema matemático que pudiera representarse mediante un algoritmo y demostró existían funciones que no se pueden calcular mediante tal máquina (el paradigma irresoluble es el Problema de Parada, que establece si dada una Máquina de Turing, ésta produce un resultado o, por el contrario, se queda calculando indefinidamente).

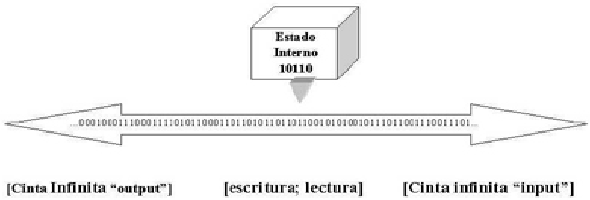


Figura 2: Ejemplo de Máquina de Turing

Durante la Segunda Guerra Mundial trabajó para el servicio de inteligencia británico en Bletchley Park, donde se encontraban los hombres encargados de romper los códigos secretos alemanes y japoneses. Para la ruptura de códigos de la máquina Enigma alemana, Turing construyó una máquina de cálculo a la que llamo Bomba. Tras la guerra, dedicó sus esfuerzos a construir el primer computador digital (al igual que John Von Neumann en un proyecto distinto).

Los últimos artículos de Turing se centran en la vigente cuestión de la inteligencia artificial, donde encontramos, por ejemplo, su test para determinar si una máquina es inteligente (lo será si una persona no puede discernir mediante preguntas si se está comunicando a través de un terminal con una persona o con un ordenador).

Pero su carrera se encontró con un final inesperado. En 1952 unos ladrones asaltaron la casa en la que vivía en Manchester y en la investigación policial Turing señaló que sospechaba que su pareja estaba involucrada. Esta declaración de su homosexualidad (que él no consideraba algo que ocultar) le llevó a un juicio en el que fue declarado culpable y en el que se le dio a elegir entre la cárcel o ser tratado con inyecciones de estrógenos, opción por la que se decantó y por la que padeció importantes consecuencias físicas. Tras dos años durante los que se dedicó a la biología matemática (concretamente a la morfogénesis centrándose en el estudio de repetición de patrones regulares en los sistemas biológicos) se suicidaba comiendo una manzana envenenada con cianuro.

Centenario de la muerte de Poincaré

Jules Henri Poincaré (1854-1912) es considerado como uno de los grandes genios y como el último universalista, capaz de entender y contribuir en todos los ámbitos de las Matemáticas. Y es que sus aportaciones pertenecen campos tan diversos como: ecuaciones diferenciales, teoría general de funciones, cuestiones de álgebra, aritmética, teoría de grupos, topología, mecánica celeste, mecánica de fluidos, geodesia, física matemática, filosofía de las ciencias, enseñanza y divulgación. En el ámbito de la Física matemática desarrolló conceptos básicos de la Teoría de la Relatividad especial por lo que se le considera unos de los cofundadores, junto con Einstein y con Lorentz; en el área de las Matemáticas cabe destacar tres campos que han constituido auténticos programas de investigación para los matemáticos del siglo XX.

En primer lugar, es el creador de las funciones automorfas de una variable compleja (llamadas por él fuchsianas) y sus estudios revelaron la existencia de funciones hasta ahora desconocidas (como las zeta-fuchsianas) que además, como él mismo demostró, podían ser utilizadas para resolver ecuaciones diferenciales lineales de segundo orden con coeficientes algebraicos.

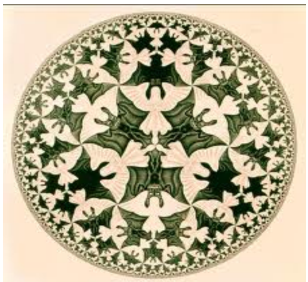


Figura 3: Disco de Poincaré.

En segundo lugar, sobresale su trabajo en mecánica celeste. Con el problema de los tres cuerpos ganó una competición matemática organizada por Oscar II, rey de Suecia y Noruega. Con la memoria a punto de ser publicada se halló un error cuya subsanación condujo a Poincaré a nuevos descubrimientos que hoy se consideran los comienzos de la teoría del Caos.

Finalmente, Poincaré también crea la topología algebraica y en ese ámbito establece su famosa conjetura: *Toda variedad cerrada simplemente conexa de dimensión 3 es homeomorfa a la 3-esfera*. Éste es el único resuelto (por Grigori Perelman) de los siete problemas del milenio.

Premio Abel 2012.

El matemático húngaro **Endre Szemerédi** ha sido galardonado a los 71 años con el premio Abel 2012 (considerado el "Nobel" de las Matemáticas) por la Norwegian Academy of Science and Letters por *"sus contribuciones fundamentales en matemática discreta y en teoría de las ciencias de la computación, así como en reconocimiento del profundo y duradero impacto de estas contribuciones a la teoría aditiva de números y la teoría ergódica"*.

Figura 4: Endre Szemerédi.

Su resultado más importante es el conocido como teorema de Szemerédi (1977): Si la densidad de un conjunto infinito de enteros es positiva, entonces contiene progresiones aritméticas arbitrariamente largas. También hay que destacar sus aportaciones a la teoría combinatoria aplicada a grafos y algoritmos, en especial el Lema de Regularidad, que afirma que en un gran grafo que pueda ser particionado en más o menos partes iguales, las conexiones entre las partes son esencialmente pseudoaleatorias.

Szemerédi, recuerdan los responsables del Premio Abel, comenzó tarde su carrera como matemático, tras cursar estudios de medicina durante un año y trabajar en una fábrica. Pero se pasó a las matemáticas y su extraordinario talento fue descubierto, cuando era un joven estudiante en Budapest, por su mentor Paul Erdős. Muchos resultados de sus más de 200 artículos publicados han abierto líneas de investigación para el futuro y han puesto los cimientos de nuevas direcciones de las matemáticas. El galardón, dotado con 800.000 euros, fue entregado el 22 de mayo en una ceremonia en Oslo.

XIII Encuentro Nacional de Estudiantes de Matemáticas

Entre el 23 y el 29 de julio se celebrará la decimotercera edición del ENEM en Murcia, que se convertirá en lugar para la formación, debate y contacto de estudiantes de Matemáticas de toda España. En la programación se incluyen conferencias y workshops, en los que se pretende dar una formación especializada y breve sobre temas de actualidad; además de excursiones y visitas culturales por la región. Esta iniciativa surgió en el año 2000 con el objetivo de consolidar ideas comunes, crear una red de enlaces entre los estudiantes y un foro de debate para dar cabida a los temas que les afectasen comúnmente y poner en marcha ideas y soluciones. El programa y todos los detalles se pueden consultar en la página web: `www.um.es/13enem`. Aunque oficialmente el plazo de inscripción ha terminado, si tienes muchas ganas de ir, infórmate.

$\int$Ú$\sum\alpha$Tε!

Concurso del Teorema de Pitágoras

La Escuela de Pensamiento Matemático Miguel de Guzmán ha organizado un concurso que pretende recoger 366 de demostraciones diferentes del teorema, una por día del año 2012, pretendiendo emular al matemático Loomis, que recopiló más de 350 demostraciones clasificadas en: geométricas, que se realizan en base a la comparación de áreas; algebraicas, desarrolladas a partir de la relación entre los lados y los segmentos del triángulo; dinámicas, que apelan a las propiedades de fuerza; y cuaterniónicas, que surgen con el uso de vectores. Si se alcanzan las 366 válidas y diferentes, la más elegante y original será premiada con 1500 €. Más información en
`http://www.escuelapensamientomatematico.org/`

Concurso de Microrrelatos Científicos

El II Certamen de Microrrelatos Científicos Feelsynapsis 5'-3' está organizado por la Red Social para la divulgación científica Feelsynapsis en colaboración con Fisher Scientific `www.feelsynapsis.com`). El objeto de este certamen se centra en descubrir el talento literario, despertar la creatividad y fomentar la divulgación científica de todas aquellas personas interesadas en las ciencias, tecnología, innovación, arte y cultura. El plazo de admisión de microrrelatos finaliza el 2 de septiembre.

Concurso de Primavera de Matemáticas

El pasado sábado 21 de abril de 2012 en la Facultad de Matemáticas de la UCM se celebró la decimosexta edición del Concurso de Primavera, que reunió a más de 3000 estudiantes de la Comunidad de Madrid. Nervios y ganas de disfrutar con las matemáticas llenaron pasillos y aulas durante toda la mañana; niños, adolescentes, familiares, profesores y voluntarios con una pasión común: el gusto por esta disciplina.

Los alumnos, entre los 10 y los 18 años y divididos en cuatro niveles, demostraron su ingenio enfrentándose a 25 problemas con múltiple opción de respuesta, como por ejemplo: *Si p, q y M son números positivos y $q < 100$, el número obtenido al crecer M el $p\,\%$ y, posteriormente, bajar el resultado en el $q\,\%$, es mayor que M si y sólo si:*

A) $p > q$ B) $p > \frac{q}{100-q}$ C) $p > \frac{q}{1-q}$ D) $p > \frac{100q}{100+q}$ E) $p > \frac{100q}{100-q}$

El miércoles 25 de abril tuvo lugar la entrega de premios, presidida por José Carrillo (rector de la UCM), Javier Montero (decano de la Facultad), Gustavo Martínez (Subdirector General de Formación del Profesorado de la Comunidad de Madrid) y María Gaspar y Mercedes Sánchez en representación del comité organizador del concurso. Desde aquí queremos agradecer y felicitar a organizadores, participantes, voluntarios y, por supuesto, ganadores, entre los que se encuentra el colaborador de **Matgazine** Jaime Mendizábal.

Figura 5: Foto de familia del XVI Concurso de Primavera.

Olimpiada Iberoamericana

La decimocuarta Olimpiada Iberoamericana de Matemática Universitaria se celebró el 11 de noviembre de 2011. En ella estudiantes de toda Iberoamérica se enfrentaron (participando cada uno desde su propia universidad) durante 5 horas a 7 problemas. Destacaron el oro de Gabriel Fürstenheim (UCM), las platas de Iván Geffner (UPC) y Moisés Herradón (UCM) y los bronces de Adrián Rodrigo (UZ), Carlos Pastor (UV), Arnau Messegué (UPC) y Adrián Franco (UZ). ¡Enhorabuena!

Premio Wolf de Matemáticas 2012

El Premio Wolf ha sido entregado anualmente desde 1978 a científicos y artistas vivos en seis campos: Agricultura, Química, Matemáticas, Medicina, Física y Artes. Consiste en un diploma y 100 000$ y es considerado uno de los premios más importantes en cada una de las áreas. En Matemáticas, puede considerarse el premio más importante después de la Medalla Fields y el Premio Abel; entre los galardonados se encuentran André Weil, Andrey Kolmogorov, Paul Erdős, John Milnor, Andrew Wiles , Vladimir Arnold y Stephen Smale. En su edición de 2012 ha sido otorgado a los matemáticos Luis Caffarelli y Michael Aschbacher.

El argentino Caffarelli ha sido galardonado por su trabajo sobre ecuaciones en derivadas parciales y el estadounidense Aschbacher por sus aportaciones a la demostración del teorema de clasificación de grupos finitos simples.

El teorema de clasificación de grupos finitos simples afirma que todo grupo finito simple es isomorfo a uno de los siguientes grupos:

- Un grupo cíclico cuyo orden es un número primo.
- Un grupo alternado de grado mayor o igual que 5.
- Un grupo de Lie simple, incluyendo: los grupos de Lie clásicos,los grupos de Chevalley y los grupos de Steinberg (con los grupos Tits también incluidos).
- Uno de los 26 grupos esporádicos (el mayor de los cuales tiene 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000 elementos, por lo que es conocido como “El monstruo”).

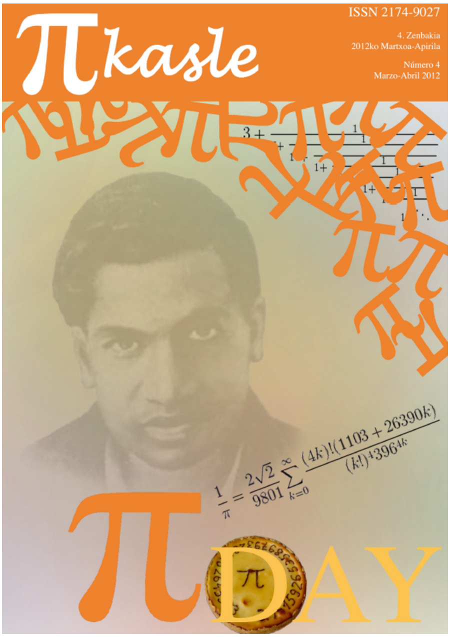
La demostración de este teorema (también conocido como el enorme teorema) es la más larga de la historia de las matemáticas: ocupa aproximadamente 15 000 páginas y son más de 100 las personas que han realizado contribuciones entre 1955 y 2004.

Cuarto número de la revista Pikasle

Os informamos de está disponible en internet[1] el cuarto número de la revista Pikasle, una revista en el mismo espíritu que ésta, hecha por estudiantes de matemáticas de la Universidad del País Vasco.

Pikasle, de π e ikasle, estudiante, es una revista de matemáticas dirigida a todos los públicos editada en dos idiomas. Cuenta con una sección de noticias matemáticas, otra de artículos de historia de las matemáticas y de otras ciencias y una sección de problemas, por cuyas soluciones ofrecen premios consistentes en chicles y libros de divulgación.

Los cuatro números están disponibles para descargar. En este último número, nos hablan del día de Pi y de la causa de Tim Gowers contra Elsevier, nos traen una entrevista a Maider Mateos sobre su trabajo como matemática en la investigación sanitaria, nos cuentan cómo ha ido el año de Galois y el ciclo de conferencias Un Paseo por la Geometría y nos narran la vida de Emmy Noether, además de su habitual concurso de problemas. Os dejamos la portada para que os pique el gusanillo:



[1] www.pikasle.tk

Ciclo de conferencias sobre lógica

El pasado mes de abril tuvo lugar el ciclo de conferencias sobre lógica organizado por **Matgazine**. Con estas conferencias pretendíamos acercar la lógica a los estudiantes de Madrid (de la UAM y de la UCM), en particular los sorprendentes resultados de Gödel en los años 30 del siglo pasado, cuando los lógicos estaban tratando de fundamentar las matemáticas en un conjunto de axiomas consistente. A continuación repasamos el contenido de las conferencias:

Ignacio Sols. ¿Qué le llevó a Gödel a investigar la fundamentación lógica de las matemáticas? Contexto de las matemáticas de su tiempo.

El catedrático del departamento de Álgebra de la facultad de matemáticas de la UCM fue el encargado de abrir el ciclo de conferencias. Tras unas pinceladas sobre la necesidad de fundamentar las matemáticas en la lógica, nos comentó los axiomas de la teoría de conjuntos y las nociones de lógica necesarias para formular los teoremas de incompletitud de Gödel.

Pepe Ruiz. Demostración de los teoremas de Gödel.

En esta conferencia Pepe Ruiz, fiel seguidor de **Matgazine**, nos comentó el teorema de completitud de Gödel, que afirma que las verdades de la lógica de primer orden son demostrables. Después nos comentó la independencia de la hipótesis del continuo respecto de los axiomas de la teoría de conjuntos de Zermelo y Fraenkel. Comentados estos teoremas, el profesor Pepe Ruiz se dispuso a probar los teoremas de incompletitud de Gödel, aunque sólo le dio tiempo a esbozar de forma precisa la demostración del primer teorema.

Paco López. ¿Podemos formular los teoremas de incompletitud de Gödel en otros términos? Computabilidad y test de parada de Turing.

El catedrático del área de Lenguajes y Sistemas Informáticos Paco López nos habló sobre computabilidad: nos definió función computable, estuvo analizando propiedades de estas funciones y nos probó que no existe ningún algoritmo que te diga si un algoritmo y unas entradas dadas van a ejecutarse en tiempo finito. Más aún, en la segunda parte de la charla, nos demostró el sorprendente teorema de Rice, que viene a decir que ninguna propiedad interesante de los algoritmos es computable.

Javier Fresán. ¿Hay vida más allá de Gödel? Relación entre los teoremas de Gödel y las ecuaciones diofánticas.

Como broche final al ciclo de conferencias tuvimos el placer de contar con otro fiel seguidor de **Matgazine**, Javier Fresán, quien está haciendo el doctorado en París. Nos contó cómo han aparecido a lo largo del s. XX distintos problemas indecidibles. Por ejemplo, nos comentó por qué la clasificación de las 4-variedades compactas es un indecidible: resulta que es un problema indecidible sobre grupos saber si dos grupos finitamente presentados[2] son isomorfos. Esto tiene graves consecuencias para la decibilidad de la clasificación de 4-variedades, pues para todo grupo finitamente presentado existe una 4-variedad que lo tiene por grupo fundamental. Después estuvo analizando el décimo problema de Hilbert, que se pregunta si existe un algoritmo que determine si hay o no soluciones enteras en una ecuación diofántica polinómica. La solución es negativa, como demostró Matiyasevich en los años 70. La prueba se basa en que los conjuntos diofánticos (esto es, aquellos definidos como los enteros que son solución de una ecuación diofántica[3]) son los mismos que los conjuntos recursivamente enumerables (que son aquellos conjuntos para los que existe un algoritmo que te va dando todos los elementos del conjunto). Si un número pertenece a un conjunto recursivamente enumerable, tenemos un algoritmo que para en tiempo finito diciéndote que está en él, pero si un número no está en el conjunto no lo podremos saber con este algoritmo. Por lo visto en la anterior conferencia, no todos los conjuntos recursivamente enumerables son computables (pues el conjunto de Turing está ahí), por lo que los conjuntos diofánticos tampoco lo son, dando así respuesta negativa al 10° problema de Hilbert.

[2]Un grupo finitamente presentado es un grupo que se puede definir a partir de un número finito de generadores y de relaciones entre ellos.

[3]En el número 0 de **Matgazine** vimos que existen polinomios cuyas únicas soluciones son los primos, por lo que los primos forman un conjunto diofántico.

La quema de libros

Dicen que el destino de un hombre, a veces, pasa por tener a su disposición una buena biblioteca.

(Anónimo)

En este breve obituario queremos rendir homenaje a las bibliotecas quemadas. Aquellas que desaparecieron junto con papiros, palimpsestos, códices, incunables. . . de vaya usted a saber qué o quién. Atroces bibliocidios de nuestra Historia en penumbra. Trepanaciones a la memoria, al saber, al futuro. Hechos impúdicos y deleznables que no podemos más que denunciar. Hechos que siguen ocurriendo. Mayores que las bibliotecas de Alejandría y Constantinopla juntas, casi borgianas en su infinita medida acaban de agonizar otras, quemadas hasta la última letra. Es por esto, y debido a la filosofía editorial de nuestra revista, que no podemos sino rendir homenaje a *gigapedia* o *library*, entre tantas recientemente fallecidas a manos de las cesáreas editoriales, que con su yugo nos suprimen. Que con su yugo nos exprimen. Y en relación a esto último hemos de romper nuestra lanza en favor de la causa iniciada por Timothy Gowers

`http://thecostofknowledge.com`

No ofrecemos más información pues sabemos que seréis capaces de emplear la red para informaros sobre éstos y otros temas relacionados. Mientras tanto *la Biblioteca*, que era cobijo de ejemplares raros, fuera de imprenta, perdidos, notas de cursos mimeografiadas. . . extingue su fuego.

Descanse en paz. Tus hijos te extrañan.

Entrevista

Sección a cargo de

Eva Elduque y Adrián Toledano

Efim Zelmanov es profesor de la Universidad de California en San Diego, nacido en Jabárovsk, Rusia. Obtuvo la medalla Fields en 1994 por su solución afirmativa al problema restringido de Burnside. El pasado noviembre visitó Zaragoza con motivo de la VI International Conference on Non Associative Algebra and its Applications, celebrada en honor a Santos González, y pudimos hacerle algunas preguntas para **Matgazine**.

Matgazine: En primer lugar, queremos darle las gracias por contestar a algunas preguntas de **Matgazine**, la revista de matemáticas de los estudiantes.

Efim Zelmanov: El placer es mío.

MZ: ¿Cuándo empezó a interesarse por las matemáticas?

EZ: Quizás cuando estaba en quinto de primaria, es decir, cuando tenía doce años y tuve la suerte de tener una profesora muy buena en el colegio. No puedo decir que ella era, como matemática, genial en algún área de las matemáticas, pero era muy entusiasta, generosa, alentadora... Empecé a disfrutar de las matemáticas a partir de ese año y desde entonces supe que probablemente intentaría ser matemático.

MZ: Se licenció en Novosibirsk (Rusia). ¿Qué le llevó hasta la Universidad de Wisconsin-Madison en el 90?

EZ: El Telón de Acero cayó en 1989, y entonces... Bueno, la primera vez que fui a Occidente fue a Zaragoza. Conocí a Santos [González] y Chelo [Martínez][1] en una conferencia, y me invitaron. En 1989 ya fue posible. Así que les visité y recibí una gran impresión. No puedo explicarlo, era como llegar a otro planeta. Ese mismo año fui también a Estados Unidos y di charlas en quince universidades, y en Madison, Georgia Benkart y Marshall Osborn me preguntaron si me gustaría ir a dar clases allí. Así que comencé el proceso y en 1992 fui finalmente a enseñar a la Universidad de Wisconsin-Madison.

MZ: ¿Qué diferencias encuentra entre el sistema educativo ruso y el americano o el europeo?

EZ: ¿A nivel universitario? Bueno, las universidades rusas son buenas, especialmente la de Moscú y la de San Petersburgo. Novosibirsk era quizás

[1] Santos González y Chelo Martínez son catedráticos de Álgebra en la Universidad de Oviedo.

la tercera del país. Aún con todo, las universidades americanas son mejores porque son internacionales, muy abiertas... y bueno, me gusta estar allí. Las universidades son muy importantes en Estados Unidos. Son el análogo a los monasterios en la Edad Media, una fuente de orgullo para toda la sociedad. ¿Que cuál es la diferencia? Bueno, después de todo, la mayoría de los matemáticos rusos están ahora en Occidente, en universidades americanas.

MZ: ¿Conoce el sistema universitario español? ¿Qué recomendaría para mejorarlo?


Prof. Efim Zelmanov

EZ: Sí, un poco. Pienso que la organización de las universidades españolas y americanas es muy diferente. De alguna manera, las universidades americanas se dirigen como los equipos de fútbol españoles. Si te fijas en el Barcelona, o en el Real Madrid, ves que tienen jugadores de todo el mundo. Cuando nosotros tenemos una plaza, cuando queremos contratar a alguien, no buscamos sólo en Estados Unidos. Por eso en nuestro departamento hay gente de Francia, China, Suecia, Reino Unido, Rusia... es muy internacional. Observa cómo funcionan los equipos de fútbol españoles, las universidades americanas funcionan igual. Por eso los equipos de fútbol españoles son los mejores del mundo. Las universidades americanas no tienen tanto dinero, pero hay un poco de competición entre ellas y entre departamentos, y en EE. UU., tienen que atraer a gente nueva. Por ejemplo, si un equipo quiere fichar un jugador tiene que pensar con qué lo puede atraer. Quizá un salario más alto, o quizá otra cosa. Así que en las universidades americanas hacen lo mismo. Si no, ¿por qué se iba a mover la gente?

MZ: España es campeona del mundo de fútbol, pero no tenemos a ningún medalla Fields entre nuestros matemáticos. ¿Qué recomendaría para que la investigación española pudiese obtener ese plus de excelencia?

EZ: Las universidades deberían tener más autonomía y más libertad para tomar sus propias decisiones. En general, también pienso que las universidades americanas reciben más dinero que las universidades españolas en total y puede que tengan mucha más libertad. Si nosotros pensamos que necesitamos algún especialista en algún área, y por ejemplo, hay algunos especialistas en Oxford, Gran Bretaña, entonces vamos a empezar a pensar qué podemos hacer para atraerles.

MZ: Hay un gran número de matemáticos rusos realmente importantes. En su opinión, ¿cuál es la razón por la que su nación destaca en esta materia?

EZ: Había dos razones para el éxito en matemáticas en la Unión Soviética. La primera es que el gobierno fomentaba mucho la investigación en matemáticas, porque era importante para el ejército. Y la segunda es que había una tradición muy fuerte de matemáticas y física teórica, y como en matemáticas no necesitamos laboratorios, podían hacerlo. Además, ser un profesor de universidad de matemáticas o de física en la Unión Soviética era extremadamente prestigioso. También estaba muy bien pagado, relativamente, claro. Así que los mejores y los más brillantes querían ser matemáticos, físicos... En América los mejores y los más brillantes frecuentemente quieren ir a Wall Street, o ser abogados, médicos... Pero por supuesto que hay gente interesada en matemáticas, así que se vuelven matemáticos.

MZ: ¿Sigue siendo así en Rusia?

EZ: No, ahora ha cambiado todo. El gobierno no está interesado ya en la ciencia, está interesado en el petróleo y el fútbol. Cuando la frontera se abrió toda esa generación se fue y eso supuso un varapalo enorme para las matemáticas rusas.

MZ: ¿Qué opina del tratamiento de los medios a Grigori Perelman? ¿Cómo cree que debemos interpretar los matemáticos su reacción ante la prensa después de que se le otorgase la medalla Fields y el Clay Institute Award?

EZ: Perelman es una persona muy especial. Probablemente necesitas ser así de especial para resolver los problemas que ha resuelto. No quería la atención de los medios, honestamente. Ha llevado su timidez al extremo. No era un juego ni nada por el estilo, él no quería todo eso. Supongo que se convirtió en una especie de celebridad. También porque es la imagen clásica de un matemático: un poco loco, aislado del mundo... Pero ahora, gente que nunca había oído hablar de la medalla Fields sabe lo que es gracias a Perelman.

MZ: ¿Puede comentarnos la matemática en la que se basa su solución al problema restringido de Burnside y resumirla un poco?

EZ: Es un problema de teoría de grupos, y pregunta qué es lo que hace que un grupo sea finito. Por ejemplo, en el caso en que todo elemento tiene orden finito. Como pasa a menudo en teoría de grupos, la solución vino de fuera de la teoría de grupos. Mi trabajo involucraba más álgebras de Lie, álgebras de Jordan... eso es muy típico en teoría de grupos. Un buen problema algebraico, y en general un buen problema matemático, es muy difícil de diseccionar. La demostración de Perelman de la conjetura de geometrización de Thurston, que implica la conjetura de Poincaré, usaba métodos de EDPs, de Análisis... Estoy seguro de que Poincaré, cuando se preguntó esto, no pensaba en todos estos métodos. Es bastante típico que un problema de algún área se resuelva mediante técnicas y resultados de otra área. Usé todo lo que sabía en el momento.

MZ: ¿Hacia dónde cree que va a evolucionar la investigación en Álgebra?

EZ: La única cosa que puedo decir estando seguro es que nadie puede predecir esto. Hubo varios intentos de predecir cómo iban a ir las matemáticas y ninguno de ellos tuvo éxito. Siempre pensamos que nuestro tema va a ir de una manera y luego va de otra. Hay algunos problemas de hace mucho tiempo. Puede que se afronten, pero a dónde nos llevará eso, nadie lo sabe. Por ejemplo, uno de los proyectos más grandes del siglo XX fue la clasificación de todos los grupos finitos simples. Ese proyecto está terminado, pero la solución tiene más de 10 000 páginas. Espero que haya nuevas ideas que hagan ver todo ese tema desde una perspectiva nueva. La conjetura jacobiana no ha sido resuelta... y aparecerán nuevos problemas. Conjeturas que ni siquiera vemos. El Álgebra siempre ha sido un servicio para otras áreas, porque estudiaba abstractamente estructuras que aparecían en matemáticas. Puede que aparezcan nuevas estructuras.

MZ: Usted se dedica al álgebra no asociativa, un campo muy abstracto de las matemáticas, que no obstante tiene su aplicación en el mundo real, como la teoría de códigos y la criptografía. ¿Cómo debemos entender la relación entre la matemática teórica y la utilidad de las mismas?

EZ: Se podría hablar durante mucho tiempo de este tema. Todo ha cambiado recientemente. Las matemáticas desempeñaron un papel muy importante en la Segunda Guerra Mundial. En particular, los avances en criptografía fueron muy importantes. Después de la Segunda Guerra Mundial se reconoció que las matemáticas eran muy importantes, muy útiles, y se les dedicó dinero. Al empezar la década de los setenta nuevos retos crearon nuevas matemáticas. Por ejemplo, cada vez que miras tu cuenta de correo electrónico o sacas dinero de un cajero automático usas matemáticas no triviales. Antes, si un general quería mandar un mensaje cifrado a algún oficial, tenían que tener un código secreto que los dos conocieran. Ahora hay cientos de millones de usuarios en internet. No sería práctico para todos ellos intercambiar códigos con los proveedores. Sabemos que las contraseñas y los códigos tienen que ser cambiados todo el tiempo, lo que supone un nuevo problema. Ese problema se afrontó usando Álgebra, teoría de números... áreas que antes eran consideradas muy puras. Ahora la organización que más especialistas en Álgebra y teoría de números contrata es la Agencia de Seguridad Nacional de Estados Unidos. Sobre cómo han cambiado las cosas... Évariste Galois inventó los cuerpos finitos. En esa época era abstracción pura y dura. Cuando yo era estudiante nos decían que sólo algebristas decadentes y especialistas en teoría de números podían estar interesados en objetos tan abstractos e inútiles. Ahora son los instrumentos más importantes en cualquier comunicación porque un ordenador no entiende nada infinito. No puedes ser capaz de explicarle a un ordenador lo que son los números reales. Sólo cuerpos finitos. Así que se volvieron algo práctico y aplicable. Creo que, en general, no hay matemáticas puras y matemáticas aplicadas. Hay matemáticas buenas y matemáticas malas y hay aplicaciones de las matemáticas.

MZ: En julio de 2011 el gobierno de David Cameron decidió dejar de financiar becas de investigación en otras áreas de matemáticas que no fueran Estadística y Probabilidad Aplicada. Tim Gowers, Michael Atiyah, Michael Berry, Simon Donaldson, Marcus du Sautoy y más matemáticos escribieron una carta mostrando su rechazo[2]. ¿Qué opina al respecto?

EZ: Los políticos necesitan tener buenos asesores en temas de ciencia y escuchar sus consejos. No sé cómo funciona el sistema en Reino Unido. Aparentemente no pudieron demostrar la calidad de su asesoramiento científico. Las matemáticas en Reino Unido siempre han sido muy fuertes. Hay mucha tradición que viene desde Newton y en vez de mantenerla mostraron su falta de entendimiento.

MZ: ¿Y aparte de las matemáticas? ¿A qué dedica el tiempo libre un medalla Fields?

EZ: Viajo mucho. Me gusta hablar con amigos. Muchos de ellos son también matemáticos, pero son cosas que pasan. No, pero generalmente creo que hay vida fuera de las matemáticas y que los no-matemáticos son también seres humanos [risas]. En mi tiempo libre leo libros, visito nuevos lugares y entonces no tengo mucho tiempo libre. Bueno, tengo una nieta...

MZ: ¿Tiene algún consejo para los lectores de **Matgazine**?

EZ: Mi consejo para cualquier estudiante es ser mentalmente muy independiente. Que intenten entender ellos mismos qué quieren en su profesión, en sus estudios. Si lo entienden pueden descubrir que hay muchas posibilidades. Que no pasen toda su vida matemática en la misma facultad, que intenten ver otras universidades.

[2] Carta que se puede ver en `http://www.dpmms.cam.ac.uk/~bt219/pm22.pdf`

Artículos

Sección a cargo de

Víctor Arnaiz Solórzano

El problema de Burnside

Moisés Herradón Cueto

Resumen

En consonancia con la entrevista a Efim Zelmanov, repasamos la historia del problema de Burnside, parte del cual fue resuelto a principios de los 90 por Zelmanov, valiéndole la medalla Fields en el Congreso Internacional de Matemáticas en Zúrich en 1994. Además, construimos un contraejemplo dado por el primer grupo de Grigorchuk: un 2*-grupo infinito finitamente generado.*

§1. La historia del problema

Una de las primeras cosas que se aprenden en un curso de teoría de grupos es la posibilidad de estudiar un grupo a través de sus generadores: un conjunto de elementos del grupo de forma que con productos suyos y de sus inversos podemos obtener todo el grupo. De esta forma, D_4, el grupo de simetrías de un cuadrado, está generado por un giro de 90°, llamémoslo ρ; y una simetría axial, a la que llamaremos σ. Es fácil comprobar que $D_4 = \{1, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ (usaremos 1 para la identidad del grupo a lo largo de todo el artículo) y que por tanto está generado por ρ y σ, como decíamos.

Con esta herramienta, uno aprende que una forma práctica (esto es relativo) de describir un grupo es a través de sus generadores y una serie de relaciones que verifican estos generadores, del tipo $x_1x_2\ldots x_n = 1$, siendo x_i generadores del grupo o sus inversos. Para hacer esto en el caso de D_4, podemos usar que ρ tiene orden 4 (pues recordemos que es un giro de 90°), y σ tiene orden 2 por ser una reflexión. Esto no determina el grupo, pues nadie nos dice que $\rho\sigma = \sigma\rho$, y de hecho es mentira, pero sí podemos establecer otra relación, que es $\rho\sigma = \sigma\rho^{-1}$, y ésta junto con las otras dos sí que determinan D_4, algo que se puede comprobar tras trastear un poco con los productos de ρ y σ y estas tres relaciones. De forma abreviada, se suele escribir $D_4 = \langle \rho, \sigma | \rho^4 = \sigma^2 = \sigma\rho\sigma\rho = 1\rangle$. En general es verdad que se puede dar un grupo a partir de un sistema de generadores y un conjunto de relaciones entre ellos (ninguno de los dos conjuntos necesariamente finito), y que un grupo dado de esta forma está en efecto bien definido[1]. A esta forma de dar el grupo se la conoce como una presentación.

Lo primero que uno piensa es que un grupo dado por una presentación es una forma muy cómoda de "conocer" un grupo, donde todos entendemos qué queremos decir por conocer: nos gustaría saber características del tipo del orden del grupo, sus subgrupos, sus clases de conjugación, una tabla de multiplicar... Por desgracia, no es así (¿qué grupo es $G = \langle a, b | a^{-1}ba = b^2, b^{-1}ab = a^2\rangle$?). De hecho, ni siquiera es fácil (ni siquiera tiene por qué ser computable) saber si a partir de las relaciones, dos palabras escritas con los generadores y sus inversos son el mismo elemento del grupo.

Así pues, William Burnside en 1902 planteó una pregunta bastante natural, relacionada con si podemos saber que un grupo es finito a partir de las relaciones más sencillas que se le ocurren a uno: las del tipo $a^n = 1$. La pregunta es

Problema 1 (Problema de Burnside). *¿Un grupo finitamente generado y en el que cada elemento tiene orden finito es necesariamente finito?*

Nada más leer el problema, parece que si cada generador tiene orden finito y hay un número finito de ellos, hay sólo un número finito de productos distintos de ellos y además debería ser fácil de acotar su número, pero esto no es verdad: nada garantiza que dos elementos del grupo conmuten, y por tanto elementos como $a^5b^4c, abab^2a^3cb, a^4cab^4 \ldots$ pueden en principio ser distintos, dando un abanico importante de elementos distintos, quizás infinito. En su artículo [1], Burnside además propone otro problema relacionado con este:

Problema 2 (Problema general de Burnside). *¿Un grupo finitamente generado y con exponente finito es necesariamente finito? (El exponente es el mínimo n para el que todo elemento del grupo tiene orden divisor de n)*

Nótese que estamos exigiendo más al grupo esta vez: antes, todos los elementos podrían tener orden finito, pero podía ser arbitrariamente grande. Ahora, podemos plantearnos la pregunta fijando un número de generadores m y un exponente para el grupo n, y buscar si puede existir un grupo infinito así generado. Fijados n y m, uno puede reducir el problema al estudio de un solo grupo: el grupo más grande que está generado por m elementos y de exponente n, que se conoce como el grupo libre de Burnside, $B(m, n)$. Este grupo se puede construir de la siguiente forma: tómese el grupo libre de rango

[1] Esto se puede hacer considerando el grupo que tiene los mismos generadores que el grupo original y ninguna relación, al que se conoce como grupo libre, y comprobando que el grupo que se busca es isomorfo a un cociente del grupo libre.

m (el grupo de todas las palabras formadas con m letras y sus inversas, véase [2]), y considérese el subgrupo normal generado por las palabras que son de la forma x^n, donde x es una palabra arbitraria. El cociente del grupo libre por este subgrupo es $B(m, n)$, o lo que es lo mismo, $B(m, n) = \langle a_1, a_2, \ldots, a_m | X^n = 1$ para todas las palabras X en los generadores$\rangle$. El problema general de Burnside consiste entonces en decidir cuándo es $B(m, n)$ finito.

Para valores de los parámetros pequeños, es fácil calcular el grupo $B(m, n)$: si $m = 1$, el grupo es cíclico y es isomorfo a $\mathbb{Z}_n$. Si $n = 2$, es un ejercicio probar que el grupo ha de ser conmutativo, y por tanto $B(m, n)$ queda isomorfo (aplicando la conocida clasificación de los grupos abelianos finitamente generados) a $\mathbb{Z}_2^m$. Burnside probó estos dos resultados en su artículo de 1902, junto con otros dos, más interesantes: $B(m, 3)$ es finito y de orden como mucho 3^{2m-1} y $B(2, 4)$ tiene orden como mucho 2^{12}. Hasta hoy, se ha probado que $B(m, 4)$ es finito (Sanov, [10]) y que $B(m, 6)$ también lo es (Marshall Hall Jr,[11]). Hasta la fecha, no se sabe si $B(2, 5)$ es o no finito.

A primera vista del problema, parece muy difícil que pueda tener respuesta negativa: ¿si un grupo es tal que todos sus elementos tienen orden finito y está finitamente generado, no debería tener "pocos" elementos distintos? Y la intuición no engaña del todo: en caso de existir un contraejemplo, muy rápidamente probaron que sería difícil de hallar: Burnside en 1905 [3] y Schur en 1911 [4] probaban respectivamente que el problema de Burnside y el problema general de Burnside tienen respuesta afirmativa para grupos de matrices complejas de dimensión finita. Esto significa que en caso de existir un contraejemplo, no tendremos la suerte de que se pueda expresar como subgrupo de matrices, lo cual es común en los grupos "habituales".

No obstante, la respuesta a ambos problemas es no: en 1964, Golod y Shafarevich encontraron familias de p-grupos (grupos en los que todo elemento tiene orden p^n para algún n, con un primo fijo p) finitamente generados e infinitos [8]. Poco después, en 1968, Novikov y Adian demostraron usando palabras en grupos libres que para todo $n \geq 4381$ impar, $B(m, n)$ es infinito, dando respuesta negativa al problema general de Burnside. Después mejorarían la cota hasta 665, y explicarían su construcción combinatoria del grupo $B(m, n)$, que les sirvió que probar varias propiedades además de su infinitud: todos los subgrupos finitos o conmutativos de $B(m, n)$ son cíclicos y $B(2, n)$ contiene un subgrupo isomorfo a $B(3, n)$. Después, se ha conseguido rebajar la cota y dar otras para exponentes pares, algunas pruebas usando las técnicas de Novikov y Adian. La mejor cota obtenida es $n \geq 13$, obtenida en 1992 por Sergei Ivanov.

Existe una tercera pregunta relacionada con el problema de Burnside.

Sea o no $B(m,n)$ infinito, si tuviera sólo una cantidad finita de subgrupos normales de índice finito se podrían intersecar todos y darían un subgrupo que también tendría índice finito. Si existe este menor subgrupo de índice finito, al cocientar por él, el grupo cociente, $B_0(m,n)$, sería el grupo finito generado por m elementos y de exponente n más grande posible. Nótese que si $B(m,n)$ es finito, es trivial que $B_0(m,n)$ existe y de hecho $B_0(m,n) = B(m,n)$. Pero si $B(m,n)$ es infinito, como de hecho ocurre para casi todos los casos, en principio no hay garantía de que el grupo finito más grande tenga que existir, en cuyo caso el grupo obtenido al intersecar todos los subgrupos de índice finito podría tener índice infinito.

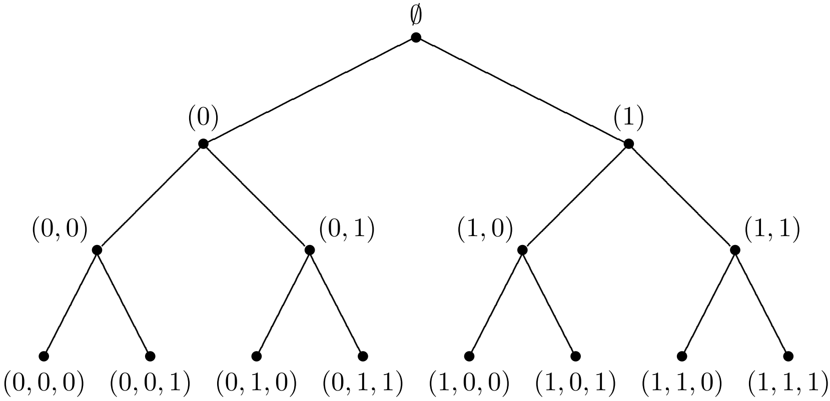
Problema 3 (Problema restringido de Burnside)**.** *Dados n y m, ¿hay una cantidad finita de grupos finitos generados por m elementos y de exponente n?*

El lector atento a la entrevista del presente número sabrá que Efim Zelmanov recibió la medalla Fields en 1994 por la respuesta afirmativa al problema Lo hizo demostrando que es cierto para potencias de primos, pues Hall y Higman habían probado que el teorema es cierto para $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ si lo es para cada factor $p_i^{\alpha_i}$ y si además eran ciertas algunas propiedades de los grupos simples finitos, que resultaron ser ciertas tras su clasificación completa en los años 80. El lector interesado encontrará las ideas de la prueba en [6].

Pasamos ahora a construir un contraejemplo para el problema general de Burnside: el primer grupo de Grigorchuk. Su construcción se puede encontrar en [5] y en [9].

§2. Un 2-grupo infinito finitamente generado

Empezamos considerando un grafo infinito: el árbol binario con raíz, T_2. Este es un grafo en el que se parte de un vértice, la raíz, del que salen dos aristas a dos vértices. De cada uno de éstos, salen dos aristas que terminan en 4 vértices, y así sucesivamente, construyendo niveles de forma que el nivel k tiene 2^k vértices (empezamos a numerar por el 0). Este grafo se puede ver como el conjunto de sucesiones finitas de ceros y unos, junto con la cadena vacía. Encontrar un cero o un uno nos indica entonces si debemos ir a la izquierda o a la derecha en este modelo. Dos sucesiones se conectan por una arista si y sólo si la diferencia de sus longitudes es 1, y si además la grande es la pequeña con un número al final. Así, $\emptyset$ y (0) ó $(0,1,1,0)$ y $(0,1,1,0,0)$ estarían conectadas, mientras que (0) y $(0,1,1,0,0)$ no lo estarían. Construido así, el nivel k está formado por las sucesiones de longitud k.



Los primeros niveles de T_2.

Ahora, consideramos del árbol su grupo de automorfismos: G. Como se puede adivinar, un isomorfismo de un grafo en otro es una biyección del conjunto de los vértices de uno en los del otro de forma que dos vértices están conectados por una arista si y sólo si sus imágenes lo están, y un automorfismo es un isomorfismo de un grafo en sí mismo. Se comprueba que el conjunto de automorfismos de un grafo es un grupo con la composición. Fijémonos en qué debe cumplir un automorfismo de T_2. Observamos que un automorfismo debe preservar el número de aristas que salen de cada vértice (el grado del vértice), y en nuestro árbol T_2 todos los vértices tienen grado 3 salvo la raíz que tiene grado 2. Por tanto, la raíz debe quedar fija por cualquier automorfismo. Además, la imagen de un camino por un isomorfismo es otro camino, de la misma longitud. Por tanto, la distancia de cada vértice a la raíz debe permanecer igual: como los vértices del nivel k están a distancia k de la raíz, concluimos que cada nivel permanece invariante por un automorfismo. Así pues, un automorfismo φ del árbol induce una permutación en cada nivel.

Vamos a fijarnos en un detalle importante. Si consideramos un vértice cualquiera, $x = (a_1, \ldots, a_n)$, podemos considerar el subgrafo formado por las sucesiones que empiezan por $(a_1, \ldots, a_n)$. Este grafo es isomorfo al original, y existe un isomorfismo canónico, que consiste en concatenar x con cada vértice. Este isomorfismo es

$$\varphi_x : T_2 \longrightarrow \varphi_x(T_2)$$

$$\varphi_x(b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$$

Consideremos ahora el subgrupo de G que deja fijos todos los vértices hasta el nivel k incluido. Cada automorfimo de este grupo, al que llamaremos $St_G(k)$

(de estabilizador en G del nivel k), induce isomorfismos en los 2^k subgrafos que parten de los vértices de este nivel. Entonces, podemos ver cada elemento f de $St_G(k)$ como 2^k automorfismos donde cada uno determina el automorfismo que induce f en el subgrafo que empieza en un vértice x_i, con $i = 1, 2, 3, \ldots 2^k$. Este automorfismo inducido por f es $\varphi_{x_i}^{-1} \circ f \circ \varphi_{x_i}$. Además, como f determina los 2^k autorfismos y viceversa, tenemos que la aplicación

$$\begin{array}{rcl} \psi : St_G(k) & \longrightarrow & G \times G \times \ldots \times G \\ f & \longrightarrow & (f_1, f_2, \ldots, f_{2^k}), \text{ donde } f_i = \varphi_{x_i}^{-1} \circ f \circ \varphi_{x_i} \end{array}$$

es biyectiva y como además es un homomorfismo de grupos, es un isomorfismo. De aquí en adelante, cuando tengamos un automorfismo de G, lo identificaremos con su imagen por ψ y simplemente escribiremos $f = (f_1, f_2)$, en el caso de que $k = 1$, por ejemplo.

Este grupo G no es el que nos interesa, pero vamos ahora a describir un subgrupo suyo, que será nuestro contraejemplo para el problema de Burnside.

Consideramos 4 automorfismos de T_2, a los que vamos a llamar a, b, c, d. A continuación describimos cuáles son estos automorfismos. Para $i \in \{0, 1\}$, definimos $\bar{i}$ como $1 - i$.

Definimos $a : T_2 \to T_2$ como el automorfismo que lleva $(i_1, i_2, \ldots, i_n)$ a $(\overline{i_1}, i_2, \ldots, i_n)$. En el dibujo del grafo, lo que hace este automorfismo es intercambiar el subárbol de la izquierda con el de la derecha. Está claro que $a^2 = 1$, donde 1 denota la identidad de T_2.

Ahora, vamos a definir los otros tres automorfismos, de forma recursiva. Esto es, definimos lo que hacen en el nivel k a partir de cómo actúan en el nivel $k-1$. Además, el nivel 1 queda fijo. Así pues, definimos $b := (a, c),\ c := (a, d),\ d := (1, b)$. Recordamos que íbamos a identificar los elementos de G que fijaran el primer nivel con los pares de elementos que actúan sobre los dos subárboles. Así pues, queremos decir que la acción de b sobre T_2 es actuar como a en el subárbol que empieza por $(0, \ldots)$ y actuar como c en el subárbol que empieza por $(1, \ldots)$. Aunque lo parezca, esta definición no es circular. Para ello, vamos a ver con un ejemplo cómo actúa c sobre un elemento de T_2, por ejemplo, $(1, 1, 0, 0, 1)$.

$$c(1, 1, 0, 0, 1) = (1, d(1, 0, 0, 1))$$

Veamos por qué esto es así: el primer término de la imagen de $(1, 1, 0, 1, 1)$ ha de ser 1, porque $b, c, d \in St_G(1)$. Ahora, ¿qué pasa con el segundo término? Como $c = (a, d)$, sobre el subgrafo que empieza por 0, la acción de c es la de a, y sobre el que empieza por 1, su acción es la de d. Como $(1, 1, 0, 1, 1)$ está en el segundo subgrafo (pues empieza por 1) hemos de encontrar $d(1,0,1,1)$. Proseguimos todo el tiempo de igual forma: si la transformación que tenemos que encontrar es a, cambiamos el primer término y terminamos. Si es una de las otras 3, no alteramos el primer término, y según si es un 1 o un 0, vemos qué transformación hay que aplicar y se la aplicamos al resto de la sucesión. Así:

$$c(1,1,0,0,1) = (1, d(1,0,0,1)) = (1,1,b(0,0,1)) = (1,1,0,a(0,1)) = (1,1,0,1,1)$$

Análogamente podríamos hacer para los demás automorfismos:

$$a(1,1,0,0,1) = (0,1,0,0,1)$$

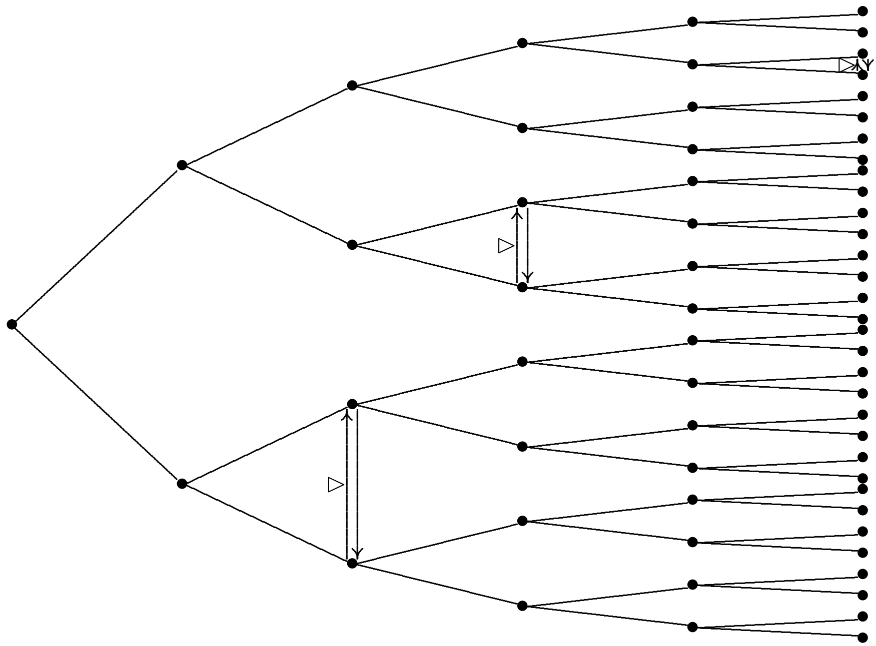
$$b(1,1,0,0,1) = (1, c(1,0,0,1)) = (1,1,d(0,0,1)) = (1,1,0,1(0,1)) = (1,1,0,0,1)$$

(Nótese que estamos usando 1 indistintamente para el elemento de las sucesiones y la identidad)

$$d(1,1,0,0,1) = (1, b(1,0,0,1)) = (1,1,c(0,0,1)) = (1,1,0,a(0,1)) = (1,1,0,1,1)$$

Vemos que b, c y d sí están bien definidos, pues la acción de los tres sobre una cadena de longitud k sólo depende de su acción de los tres sobre una cadena de longitud $k-1$ (y están bien definidos sobre las palabras de longitud 1). Sobre el grafo, vemos que la acción de b, c y d consiste en tomar ciertos árboles de la derecha y dar la vuelta a dos de cada tres (ver el dibujo). También podemos entender a, b, c y d como los estados de una máquina que va leyendo una secuencia de unos y ceros y ejecuta órdenes del tipo “Si está en el estado b y encuentra 1, pasa al estado c, dejando el número igual y pasa al siguiente número”.

Teniendo a, b, c, d, definimos el grupo Γ como $\Gamma = \langle a, b, c, d \rangle$; el subgrupo de G generado por estos cuatro automorfismos. Nuestro objetivo es probar que es infinito y que es un 2-grupo, esto es, que el orden de cada elemento es una potencia de 2. Primero, vamos a ver que $b^2 = c^2 = d^2 = 1$, y vamos a hacerlo por inducción sobre la longitud de las sucesiones de T_2. Para la palabra vacía, la acción es la identidad. Ahora, supongamos que b^2, c^2 y d^2 dejan fijas las sucesiones de longitud hasta $k-1$. Dada una sucesión $x = (x_1, \ldots, x_k)$, $b^2(x) = b(b(x_1, \ldots, x_k)) = b(x_1, g(x_2, \ldots, x_k)) = (x_1, g^2(x_2, \ldots, x_k))$, donde $g = a$ si $x_1 = 0$ y $g = c$ si $x_1 = 1$. En cualquier caso, $g^2 = 1$: para a lo hemos probado y para c es la hipótesis de inducción, pues la sucesión que queda tiene longitud uno menos, y por tanto $b^2(x) = (x_1, 1(x_2, \ldots, x_k)) = x$.



La acción de b sobre los primeros niveles de T_2 (dibujado con la dirección 1 arriba y 0 abajo). Las flechas indican qué partes del árbol se intercambian. Nótese que aparece una flecha en dos de cada tres niveles, que hemos marcado para que se vea mejor.

La prueba es análoga para c y d. Además, usando la misma técnica se prueba que $bc = cb = d,\ cd = dc = b,\ bd = db = c$ (de hecho sólo hace falta probar dos igualdades bien elegidas y las demás se deducen), de donde se sigue que $\langle b, c, d\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Vamos a ver ahora cómo actúan sobre T_2 aba, aca y ada. Cada uno de ellos actuando sobre (0) y (1) los dejan fijos, pues a los intercambia y b, c y d los dejan fijos. Como a actúa dos veces, al final quedan fijos. Así pues, sabemos que cada uno es de la forma (f, g) para ciertos $f, g \in G$. ¿Cuáles son f y g? Veamos la acción de aba sobre $x = (0, x_2, \ldots, x_n)$ y sobre $y = (1, y_2, \ldots, y_n)$:

$$aba(x) = ab(1, x_2, \ldots, x_n) = a(1, c(x_2, \ldots, x_n)) = (0, c(x_2, \ldots, x_n))$$

y

$$aba(y) = ab(0, y_2, \ldots, y_n) = a(0, a(y_2, \ldots, y_n)) = (1, a(y_2, \ldots, y_n))$$

Entonces, concluimos que $aba = (c, a)$. De igual forma, $aca = (d, a)$ y $ada = (b, 1)$. Con toda esta información, ya podemos hacernos una idea de cuáles son los elementos de $\Gamma = \langle a, b, c, d\rangle$. Por definición, son todos los productos finitos de $a, b, c, d, a^{-1}, b^{-1}, c^{-1}, d^{-1}$, pero sabemos que los cuatro generadores tienen orden 2. Por tanto, $x = x^{-1}$ para $x = a, b, c, d$, y podemos quedarnos sólo con los productos de a, b, c, d. Además, podemos usar que b, c y d conmutan entre sí y que el producto de dos de ellos es el tercero. Entonces, si en un producto encontramos dos elementos de b, c, d seguidos, podemos sustituirlo por el tercero, y si encontramos un elemento dos veces, lo podemos eliminar porque su cuadrado es la identidad. Así pues, tenemos que Γ está formado por todos los productos finitos de (o palabras formadas con) a, b, c, d en los que no aparece una letra dos veces seguidas ni aparecen juntas cualesquiera dos de b, c, d. Es decir, los elementos de Γ son de la forma $[a]x_1ax_2 \dots x_m[a]$, donde $x_i \in \{b, c, d\}$ salvo quizá eliminar alguna o ambas de las a que están entre corchetes. En lo sucesivo, hablaremos indistintamente de productos de a, b, c, d o de palabras formadas con a, b, c, d.

Vamos a pasar a probar el primer resultado interesante para nuestro objetivo (si definimos un grupo por sus generadores, no es interesante el hecho de que sea finitamente generado): demostraremos que Γ es infinito. Para ello, vamos a hacer uso del isomorfismo ψ que definimos entre $St_G(1)$ y $G \times G$ y que venimos usando desde entonces (sólo vamos a usar el que corresponde al primer nivel, así que no lo llamaremos ψ_1). Vamos a probar las propiedades que nos interesan de su restricción a $St_\Gamma(1)$, es decir, a los automorfismos de Γ que dejan fijo el primer nivel.

Proposición 1. El homomorfismo

$$\psi|_\Gamma = (\psi_0, \psi_1) : St_\Gamma(1) \longrightarrow \Gamma \times \Gamma$$

1. Está bien definido. Esto es, su imagen cae dentro de $\Gamma \times \Gamma$
2. Es inyectivo
3. Cumple que al proyectar sobre cada coordenada (es decir, al tomar para $i = 0, 1$ $\pi_i : \Gamma \times \Gamma \longrightarrow \Gamma$ dado por $\pi_i = (x_1, x_2) = x_i$), las dos componentes $\psi_0 = \pi_0 \circ \psi|_\Gamma$ y $\psi_1 = \pi_1 \circ \psi|_\Gamma$, son ambas suprayectivas.

Demostración. 1. Primero, está claro que es un homomorfismo (considerando que su imagen está en $G \times G$) pues es restricción de un homomorfismo a un subgrupo. Por ser homomorfismo, sabemos que su imagen estará generada por la imagen de los generadores de $St_\Gamma(1)$. Ahora bien, sabemos cómo son todas las palabras de Γ, y es fácil saber cuáles dejan fijo el primer nivel de T_2: como a intercambia sus dos vértices y el resto de generadores los dejan fijos, son las palabras que tienen el elemento a un número par de veces, que podemos escribir como una posibilidad de entre $ax_1 \dots ax_{2m}$, $ax_1 \dots ax_{2m-1}a$, $x_1a \dots ax_{2m-1}$, ó $x_1a \dots x_{2m}a$ (con $x_i \in \{b, c, d\}$). En el primer caso, podemos agrupar estos elementos convenientemente para obtener $(ax_1a)(x_2)(ax_3a) \dots (ax_{2m-1}a)(x_{2m})$ y en el resto podemos agrupar de forma parecida, donde lo fundamental es que los productos estén formados por concatenación de los términos b, c, d, aba, aca, ada. Esto es lo mismo que decir que $\{b, c, d, aba, aca, ada\}$ generan $St_\Gamma(1)$. Aplicando ψ a los generadores obtenemos (como ya sabemos) $(a, c), (a, d), (1, b), (c, a), (d, a), (b, 1)$, es decir, elementos de $\Gamma \times \Gamma$, con lo que queda probado que su imagen está incluida donde deseamos.

2. La inyectividad se sigue de que ψ sin restringir es inyectiva.

3. Vamos a usar los generadores de nuevo, esta vez de Γ. Basta ver que, por ejemplo para ψ_0, su imagen contiene a todos los generadores de Γ: como $\psi_0(St_\Gamma(1))$ es un grupo, habría de ser todo Γ. Pero es fácil ver que su imagen contiene a a, b, c, d, pues $\psi(b) = (a, c)$, $\psi(ada) = (b, 1)$, $\psi(aba) = (c, a)$, $\psi(aca) = (d, a)$, y por tanto, aplicando la proyección sobre la primera coordenada, $\psi_0(b) = a$, $\psi_0(ada) = b$, $\psi_0(aba) = c$, $\psi_0(aca) = d$, que es lo que queríamos, y de forma análoga para ψ_1.

□

Por tanto, concluimos lo que queríamos:

Proposición 2. Γ es infinito

Se sigue de que hay una aplicación de un subconjunto propio suyo , $St_\Gamma(1)$, sobreyectiva sobre todo él, por ejemplo ψ_0. El subconjunto es propio porque por ejemplo $a \notin St_\Gamma(1)$.

Usando lo que sabemos de aba, aca y ada, veamos cómo son los subgrupos de Γ $\langle a, b\rangle$, $\langle a, c\rangle$ y $\langle a, d\rangle$. De hecho, vamos a probar que son isomorfos a grupos diedrales D_n. Recordamos que el grupo diedral D_n se puede definir como el grupo de isometrías de un $n-$ágono regular, y se suele dar la presentación $D_n = \langle r, s | r^2 = s^n = rsrs = 1\rangle$, en la que r es una reflexión y s un giro de ángulo $\frac{2\pi}{n}$. Nosotros vamos a tomar como generadores dos reflexiones, lo que nos da la presentación (es fácil de probar) $D_n = \langle x, y | x^2 = y^2 = (xy)^n = 1\rangle$. Esta es la presentación que vamos a usar para probar nuestro resultado.

Proposición 3. $\langle a, b\rangle \cong D_{16}$, $\langle a, c\rangle \cong D_8$ y $\langle a, d\rangle \cong D_4$

Demostración. Vamos a usar las presentaciones que hemos dicho. Por tanto, lo que tenemos que probar es al menos que $a^2 = b^2 = c^2 = d^2 = (ab)^{16} = (ac)^8 = (ad)^4 = 1$, agrupando todas las relaciones que necesitamos. Con esto probado, tendríamos que esas relaciones están entre las que cumplen a, b, c y d , lo que nos daría que existen homomorfismos suprayectivos de D_4, D_8 y D_{16} en $\langle a, d\rangle$, $\langle a, c\rangle$ y $\langle a, b\rangle$, respectivamente (que se construyen llevando los generadores en los generadores). Para probar que son también inyectivos, nos basta ver que los cardinales de los subgrupos de la derecha son suficientemente grandes. Ya hemos demostrado las 4 primeras relaciones, así que vamos con las tres últimas (recuérdese que en todo grupo es verdad que el orden de fg y el orden de gf son iguales).

$$(ad)^4 = (ada)d(ada)d = (b, 1)(1, b)(b, 1)(1, b) = (b^2, b^2) = (1, 1) = 1$$

$$(ac)^8 = ((aca)c)^4 = ((d, a)(a, d))^4 = (da, ad)^4 = ((da)^4, (ad)^4) = 1$$

$$(ab)^{16} = ((aba)b)^8 = ((c, a)(a, c))^8 = (ca, ac)^8 = ((ca)^8, (ac)^8) = 1$$

Además, de aquí se deduce que los órdenes de ad, ac y ab son exactamente 4, 8 y 16 y no son menores. Además se tiene que a no es una potencia de ad, ac o ab, pues por los órdenes debería ser $(ad)^2$, $(ac)^4$ o $(ab)^8$ y se puede ver que no lo es. Por tanto, juntando las potencias de ad, ac y ab con a, obtenemos respectivamente 5, 9 y 17 elementos distintos de cada grupo. Como el orden debe ser un divisor de 8, 16 y 32, es el orden que queremos y los grupos son en efecto isomorfos a los diedrales. □

Proposición 4. Γ es un 2-grupo. Esto es, para todo $g \in \Gamma$, existe $m \in \mathbb{N}$ tal que $g^{2^m} = 1$

Demostración. Ya sabemos que todo elemento de Γ se puede escribir como una palabra en a, b, c, d de la forma que hemos explicado antes. Vamos a probar el resultado para estas palabras por inducción sobre l, donde l es la longitud de las palabras. Para $l = 0$, sólo tenemos la identidad, por lo que no hay nada que probar, y para $l = 1$ tenemos a, b, c, d, que ya sabemos que tienen orden 2. Para $l = 2$, hemos probado que ab tiene orden 16, ac tiene orden 8 y ad tiene orden 4, y por tanto el resultado es verdad. Ahora supongamos el resultado cierto para todo $l' < l$ y sea g una palabra de las que ya hemos explicado de longitud $l \geq 3$. Distinguimos dos casos según la paridad de l.

- Si $l = 2m + 1$, entonces g es o bien de la forma $ax_1ax_2 \dots x_ma$ o de la forma $x_1ax_2 \dots x_{m+1}$. En el primer caso, la palabra es conjugada a $a(ax_1ax_2 \dots x_ma)a^{-1} = x_1ax_2 \dots x_m$, que tiene longitud $l - 2$ y el mismo orden, por ser conjugada suya: se sigue la proposición por la hipótesis de inducción. En el segundo caso, conjugando por x_1, se obtiene una palabra de la forma $ax_2 \dots x_{m+1}x_1 = ax_2 \dots y_1$ para algún $y \in \{1, b, c, d\}$. De igual manera, es conjugada a una palabra de longitud como mucho $l-1$ y tenemos el mismo resultado.

- Si $l = 2m$, entonces, conjugando por a, podemos suponer que g es de la forma $ax_1ax_2 \dots x_m$. Supongamos que m es par, esto es, $m = 2k$. Podemos agrupar para obtener que $g = (ax_1a)(x_2)(ax_3a)\dots(x_m)$. Entonces, aplicando el isomorfismo de $St_\Gamma(1)$ en $\Gamma \times \Gamma$,

  $$g = (y_1, a)(a, y_2) \dots (a, y_{2k}) = (y_1ay_3 \dots y_{2k-1}a, ay_2ay_4 \dots ay_{2k}) = (\alpha, \beta)$$

  Por simplificar la notación, estamos escribiendo a donde quizás puede aparecer la identidad, por venir de $\psi(d)$. Esto no nos va a afectar, como se puede ver, pues lo que nos interesa es reducir el caso a palabras más cortas. Observamos que las dos palabras α, β tienen longitud $m < l$, y por tanto sabemos que tienen orden potencia de 2 por la hipótesis de inducción. Entonces, el orden de (α, β) será su mínimo común múltiplo y tenemos lo que queremos.

  Si $m = 2k+1$, nos interesa hacer lo mismo que en el caso anterior, pero no podemos porque a aparece un número impar de veces. Para arreglarlo, consideramos g^2. Tenemos que $g^2 = ax_1ax_2 \dots ax_max_1 \dots ax_m = (ax_1a)(x_2)\dots(ax_ma)(x_1)\dots(ax_{m-1}a)(x_m)$, y con el isomorfismo sale

  $$g^2 = (y_1, a)(a, y_2) \dots (y_{2k+1}, a)(a, y_1) \dots (a, y_{2k+1}) =$$
  $$= (y_1ay_3 \dots y_{2k+1}ay_2 \dots y_{2k}a, ay_2ay_4 \dots y_{2k-1}ay_{2k+1}) = (\alpha, \beta)$$

  Ambas palabras salen con longitud como mucho $2m = l$ (algunas veces puede aparecer d de nuevo y ser $\psi_i(d)$ la identidad para algún i). Ahora, tenemos que distinguir tres casos, que no distan mucho de las demostraciones del orden de ab, ac, ad con ligeros cambios para una palabra más larga:

  d) Existe algún j tal que $x_j = d$. En este caso, al escribir x_j y ax_ja como elementos de $\Gamma \times \Gamma$, o lo que es lo mismo, al aplicar ψ, obtenemos $(1, b)$ y $(b, 1)$ respectivamente. Por tanto, en ambas palabras α, β aparece un 1, y se podrán reducir las palabras para obtener dos de longitud como mucho $l-2$. Entonces, podemos aplicar la hipótesis de inducción y concluir que tienen orden potencia de dos, y por tanto (α, β) tiene orden el mínimo común múltiplo de ambos órdenes, es decir, el mayor de los dos (pues uno divide a otro al ser potencias de dos).

c) Existe algún j tal que $x_j = c$. Ahora, repitiendo el proceso para x_j y ax_ja, obtenemos $x_j = (a, d)$ y $ax_ja = (d, a)$. Tenemos pues, que α, β son dos palabras de longitud como mucho l, que cumplen las hipótesis de *d*) al contener la letra d. Aplicando a estas el resultado de *d*), tenemos que tienen orden potencias de dos, y se sigue el resultado.

b) Existe algún j tal que $x_j = b$. El lector atento no tendrá dificultad en concluir que a las palabras α, β se les puede aplicar las hipótesis de *c*).

Esto agota todos los casos, y por tanto el teorema está probado.

□

Tenemos, pues, al fin lo que deseábamos:

Teorema 1. Γ está finitamente generado, es un 2-grupo y es infinito. Por tanto, el problema de Burnside tiene respuesta negativa.

No puedo terminar el artículo sin agradecer a Juan Ramón Delgado su ayuda con la búsqueda de información sobre el problema de Burnside ni sin hacer publicidad del curso de LaTeX organizado por **Matgazine**, en el que he aprendido a dibujar grafos.

Referencias

[1] Burnside, William: *On an unsettled question in the theory of discontinuous groups.*
Quart.J.Math. 33 (1902), 230-238

[2] Fürstenheim, Gabriel: *La paradoja de Banach-Tarski.*
Matgazine 1 (2011), 30 disponible en `matgazine.tk`

[3] Burnside, William: *On criteria for the finiteness of the order of a group of linear substitutions*
Proc.London Math. Soc. (2) 3 (1905), 435-440

[4] Schur, Issai: *Über Gruppen periodischer substitutionen*
Sitzungsber. Preuss. Akad. Wiss. (1911), 619-627

[5] Hudec, Drew A.: *On the Burnside Problem*
University of Chicago VIGRE REU 2006
http://www.math.uchicago.edu/~may/VIGRE/VIGRE2006/PAPERS/Hudec.pdf

[6] Paranjape Kapil H.: *The work of Efim Zelmanov (Fields Medal 1994)*
http://www.imsc.res.in/~kapil/papers/zelm.pdf

[7] S I Adian: *The Burnside problems and identities in groups*
Springer-Verlag (1979)

[8] Golod,E D: *On nil algebras and finitely residual groups*
Izv. Akad. Nauk SSSR. Ser. Mat. 1975, (1964), 273-276 (En ruso)

[9] de la Harpe, Pierre: *Topics on geometric group theory*
The University of Chicago Press, (2000)

[10] Sanov, I.N.: *Solution of Burnside's problem for $n = 4$*
Leningrad State University Annals (Uchenyi Zapiski) Math. Ser. 10 (1940),166-170 (En ruso)

[11] Hall, Marshall: *Solution of the Burnside problem for exponent 6*
Illinois J. of Math. 2 (1958), 764-786

Moisés Herradón Cueto
Estudiante de la Universidad Complutense de Madrid
moises_ herradon@yahoo.es

Las Medallas Fields

Víctor Arnaiz Solórzano

§1. Introducción

CONGREGATI EX TOTO ORBE MATHEMATICI
OB SCRIPTA INSIGNA TRIBUERE
(Reunidos los matemáticos de todo el
mundo para premiar las obras maestras).
Reverso de la medalla Fields.

A menudo, la Medalla Fields es considerada "el Premio Nobel en Matemáticas". Sin duda, ambos premios gozan del máximo prestigio en las disciplinas donde se conceden y, al fin y al cabo, las Fields suplen de alguna forma la carencia del Nobel en matemáticas (quizás junto con el premio Abel). Pero tanto las características como la historia de las Medallas Fields son independientes y particularmente interesantes. En este artículo ahondaremos un poco en dichos aspectos, además de insinuar la línea que sus portadores han trazado en el mundo matemático desde la creación del premio en 1936.

En primer lugar, no tiene sentido hablar de las Medallas Fields fuera de su medio natural, a saber, los Congresos Internacionales de Matemáticos (ICM). Para una amplia y agradable lectura al respecto, véase [1].

Figura 1: La medalla Fields

El primer ICM tuvo lugar en Zúrich en 1897, tras un congreso previo de similar caráter que se celebró en 1893 en Chicago. Los ICM's nacieron con el objetivo primordial de fomentar la cooperación internacional en matemáticas. Los siguientes Congresos Internacionales tuvieron lugar sucesivamente en Francia (1900), Alemania (1904), Italia (1908) e Inglaterra (1912) y en todos ellos se mantuvo este ambiente de cooperación. Pero la Primera Guerra

Mundial quebró la secuencia de congresos y destruyó en gran medida los lazos de colaboración establecidos. Los países vencedores expulsaron a las naciones centrales de los organismos internacionales. En particular, a sus matemáticos se les prohibió la asistencia a los Congresos Internacionales, una represalia culminada por la designación de Estrasburgo, la capital de la disputada Alsacia, recién recuperada por Francia, como sede del siguiente congreso, en 1920.

En este congreso se creó la Unión Matemática Internacional (IMU), organismo que sería el encargado de organizar los ICM's desde entonces, con periodicidad cuatrienial.

John Charles Fields, el presidente del Comité Organizador del siguiente ICM, que se celebró en Toronto en 1924, se enfrentó a la nada fácil tarea de aliviar las tensiones y rivalidades imperantes, así como el creciente clima de crispación. A la fuerte disputa en Europa se había sumado la renuncia de los estadounidenses a celebrar el ICM de 1924 en Nueva York, ciudad que había sido designada por la IMU en el congreso anterior, como muestra de rechazo hacia el recién creado organismo.

El dedicado esfuerzo organizativo y diplomático de Fields no logró que se levantara el veto a las naciones centrales, pero inició el camino de la normalización. Fields propuso al final del congreso de 1924 la creación de unos premios "de un carácter tan internacional e impersonal como fuera posible". Fields, al proponer la creación de los premios, insistió en que no tuvieran ninguna adscripción nacional, personal o institucional, pero irónicamente, cuando la IMU aprobó la creación de los premios durante el ICM de Zúrich de 1932, aceptando la donación de Fields (que falleció unos meses antes) para financiarlos, se hicieron universalmente conocidos como Medallas Fields, aunque su denominación oficial sea Medallas Internacionales para Descubrimientos Sobresalientes en Matemáticas.

Figura 2: John C. Fields.

§2. La Medalla Fields, un premio al porvenir

"Todos los límites, particularmente
los nacionales, son contrarios a la naturaleza
de las Matemáticas [...] *para las Matemáticas,*
todo el mundo cultural es un único país".
David Hilbert,
durante el ICM de Bolonia, 1928 [3].

Fields, en el ICM de 1924, propuso el establecimiento de un fondo para la concesión de dos medallas de oro en los sucesivos Congresos. Dada la multiplicidad de ramas de las matemáticas, y teniendo en cuenta el hecho de que el intervalo entre congresos es de cuatro años, consideró que debían concederse al menos dos medallas. Los premios estarían abiertos a todo el mundo y serían concedidos por un comité internacional. Desde el ICM de Moscú, en 1966, se pueden conceder entre dos y, muy preferiblemente, cuatro medallas. El motivo es que el mayor número de áreas posible dentro de las matemáticas queden representadas con los galardones.

Fields también señaló que "aunque la concesión del premio debe basarse en trabajo ya realizado, debe al mismo tiempo servir para animar futuros logros de los galardonados y como estímulo para el esfuerzo renovado de otros". Este es el origen de la tradición, pues no es una norma escrita, de premiar sólo a menores de cuarenta años.

El ICM de Zúrich en 1932 aceptó el legado de Fields, y, de acuerdo a los planes de éste, nombró al comité presidido por Constantin Carathéodory que, en el ICM de Oslo en 1936, otorgó las dos primeras Fields a Lars Valerian Ahlfors y Jesse Douglas. Desde entonces, se han concedido un total de 52 medallas:

Año	**Nombre**	**País**	**Centro de estudios**
1936	Lars Ahlfors	Finlandia	U. de Harvard
1936	Jesse Douglas	Estados Unidos	M.I.T.
1950	Laurent Schwartz	Francia	U. de Nancy
1950	Atle Selberg	Noruega	I.E.A. de Princeton
1954	Kunihiko Kodaira	Japón	U. de Princeton
1954	Jean-Pierre Serre	Francia	U. de París
1958	Klaus F. Roth	Reino Unido	U. de Londres
1958	René Thom	Francia	U. de Estrasburgo
1962	Lars V. Hörmander	Suecia	U. de Estocolmo
1962	John W. Milnor	Estados Unidos	U. de Princeton
1966	Michael F. Atiyah	Reino Unido	U. de Oxford

1966	Paul J. Cohen	Estados Unidos	U. de Stanford
1966	A. Grothendieck	Francia	U. de París
1966	Stephen Smale	Estados Unidos	U. de Berkeley
1970	Alan Baker	Reino Unido	U. de Cambridge
1970	Heisuke Hironaka	Japón	U. de Harvard
1970	Sergéi Nóvikov	Unión Soviética	U. de Moscú
1970	John G. Thompson	Estados Unidos	U. de Cambridge
1974	Enrico Bombieri	Italia	U. de Pisa
1974	David B. Mumford	Reino Unido	U. de Harvard
1978	Pierre R. Deligne	Bélgica	I.H.E.S.
1978	Charles L. Fefferman	Estados Unidos	U. de Princeton
1978	Grigori Margulis	Unión Soviética	U. de Moscú
1978	Daniel G. Quillen	Estados Unidos	M.I.T.
1982	Alain Connes	Francia	I.H.E.S.
1982	William P. Thurston	Estados Unidos	U. de Princeton
1982	Shing-Tung Yau	China	I.E.A. de Princeton
1986	Simon Donaldson	Reino Unido	U. de Oxford
1986	Gerd Faltings	Alemania	U. de Princeton
1986	Michael Freedman	Estados Unidos	U. de San Diego
1990	Vladimir Drinfeld	Unión Soviética	I. de Física Kharkov
1990	Vaughan Jones	Nueva Zelanda	U. de Berkeley
1990	Shigefumi Mori	Japón	U. de Kyoto
1990	Edward Witten	Estados Unidos	I.E.A. de Princeton
1994	Pierre-Louis Lions	Francia	U. de París-Dauphine
1994	Jean C. Yoccoz	Francia	U. de París-Sud
1994	Jean Bourgain	Bélgica	I.E.A. de Princeton
1994	Efim Zelmanov	Rusia	U. de Wisconsin
1998	Richard E. Borcherds	Sudáfrica	U. de Cambridge
1998	W. Timothy Gowers	Reino Unido	U. de Cambridge
1998	Maxim Kontsevich	Rusia	I.H.E.S.
1998	Curtis T. McMullen	Estados Unidos	U. de Harvard
2002	Vladimir Voevodsky	Rusia	I.E.A. de Princeton
2002	Laurent Lafforgue	Francia	I.H.E.S.
2006	Andrei Okounkov	Rusia	U. de Princeton
2006	Grigori Perelman	Rusia	I. Steklov
2006	Terence Tao	Australia	U. de California
2006	Wendelin Werner	Francia	U. de París-Sud
2010	Elon Lindenstrauss	Israel	U. de Jerusalén
2010	Ngo Bao Chau	Francia-Vietnam	I.E.A. de Princeton
2010	Stanislav Smirnov	Rusia	U. de Ginebra
2010	Cédric Villani	Francia	I. Henri Poincaré

§3. Las líneas de investigación

"Yo no aprendí en los libros ninguna receta
para la composición de un poema, [...]
en el curso de mi vida he encontrado siempre en
alguna parte la aseveración necesaria,
la fórmula que me aguardaba..."
Pablo Neruda.
Discurso de recepción del
Premio Nobel de Literatura, 1971.

Desde la creación de las Medallas Fields en 1936, y siendo fieles a su carácter internacional, a la diversidad de áreas en las que se han concedido y a la precoz obtención de resultados de la máxima calidad por parte de los premiados, podemos decir que los portadores de este galardón han abanderado la investigación matemática mundial de casi todo el siglo XX y el principio del XXI, lidiando y a menudo resolviendo los más importantes problemas abiertos de las matemáticas. No es intención de este artículo describir la profundidad, amplitud e importancia de los trabajos realizados, por razones obvias de espacio y de desconocimiento del que escribe estas líneas. Pero sí se intentará dar una visión global de los campos en los que los medallistas Fields han hecho aportaciones notables.

Sin duda, una de las constantes es la teoría de números. Son importantes las aportaciones de Atle Selberg, que trabajó en teoría analítica de números, en especial en la Hipótesis de Riemann; Jean Pierre Serre, del que destaca la conjetura sobre representaciones módulo-p, que conectó el Último Teorema de Fermat con la geometría aritmética; Klaus Roth, por sus trabajos en subconjuntos de enteros de densidad positiva[1], los cuales, demostró, contienen infinitas progresiones aritméticas de longitud 3 (primer caso no trivial del que más tarde sería el Teorema de Szemerédi); Alan Baker, que trabajó en métodos efectivos en teoría de números y Ecuaciones Diofánticas; o Enrico Bombieri, famoso por sus contribuciones en la Hipótesis de Riemann y del que destaca el Teorema de Bombieri-Vinogradov sobre la densidad de los números primos y el error respecto del teorema de los números primos.

Por otra parte, quizás el problema que más medallas Fields ha recabado sea la Conjetura de Poincaré. Prácticamente cada avance en la misma ha significado una Medalla Fields. Tienen especial relevancia la demostración de Stephen Smale de la conjetura para dimensión mayor o igual que cinco;

[1] La densidad de un conjunto infinito de enteros A se define como
$\rho(A) = \limsup_{x\to\infty} \frac{|\{a \leq x \ : \ a \in A\}|}{x}$.

los trabajos de William Thurston, que enuncia la más general Conjetura de Geometrización; la demostración de Michael Freedman de la conjetura para dimensión cuatro y, finalmente, la demostración de Grigori Perelman de la Conjetura de Geometrización de Thurston, que incluye como caso particular la Conjetura de Poincaré para dimensión 3.

Otros medallistas Fields que han contribuido a la geometría y la topología son Sergei Novikov, David Mumford, René Thom, Simon Donaldson, Gerard Faltings, Shigefumi Mori, Vladimir Voevodsky y muy especialmente John Milnor, cuyo trabajo particular más famoso versa sobre la existencia de esferas 7-dimensionales con estructura diferencial no estándar.

Un campo que, por su amplitud, también ha obtenido numerosas medallas Fields es el álgebra. Mencionaremos a John Thomson, por sus trabajos en grupos finitos; Daniel Quillen (fallecido en 2011), que trabajó en K-teoría algebraica, Teoría de las Categorías y representaciones modulares en teoría de grupos, Vladimir Drinfeld, que hizo importantes contribuciones sobre cuerpos finitos y teoría de números; Efim Zelmanov, conocido por su trabajo en el problema de Burnside; Richard E. Borcherds, también prolífico en teoría de números, teoría de grupos y álgebras infinito-dimensionales; y Laurent Lafforgue, partícipe del *Programa de Langlands*[2], trabaja en teoría de Galois, teoría algebraica de números, teoría de la representación y análisis.

En análisis matemático, son importantes las contribuciones de Lars Ahlfors al análisis complejo; Laurent Schwartz a la teoría de distribuciones; Kunihiko Kodaira al análisis funcional; Lars Hörmander y Pierre L. Lions a las EDP's; Charles L. Fefferman al análisis de Fourier, las EDP's y el análisis armónico (habiendo realizado su doctorado con Stein), Jean Bourgain al estudio de los espacios de Banach, análisis armónico, EDP's, al *problema de Kakeya*[3] y la aritmética combinatoria y Tim Gowers, que entre otros muchos, tiene trabajos en análisis funcional y combinatoria aplicados al estudio de espacios de Banach.

También ha habido medallistas Fields por trabajos en física teórica. Este es el caso de Shing-Tung Yau, que ha trabajado entre la geometría y la física. Es importante su prueba del Teorema de la energía positiva en Relatividad

[2]El programa de Langlands es una serie de conjeturas formuladas por primera vez por el matemático canadiense Robert P. Langlands en 1967 y que conjeturaban una correspondencia entre la teoría de números y el Análisis (es decir, el estudio de las funciones) por medio de las denominadas representaciones de Galois. Desde entonces, estas conjeturas han supuesto un desafiante programa de investigación, todavía inacabado.

[3]Kakeya, matemático japonés, planteó en el año 1917 el problema de hallar el área mínima que barre en el plano un segmento de longitud 1 al dar la vuelta completa. Más tarde, Besicovitch demostró que existen conjuntos de medida de Lebesgue nula que tienen la propiedad de contener un segmento unidad en todas las direcciones. Entender las propiedades de estos conjuntos se ha convertido en un objetivo importante del Análisis Armónico.

General. Otro caso similar es el de Edward Witten, quien tiene trabajos sobre partículas elementales, teoría cuántica de campos y topología geométrica aplicada a la obtención de invariantes cuánticos.

Como "rareza", nombraremos a Paul Cohen, único premiado por sus investigaciones en teoría de conjuntos y lógica matemática, que demostró la independencia de la hipótesis del continuo de la axiomática Zermelo-Fraenkel con el axioma de elección (ZFC).

En cualquier caso, muchos medallistas Fields destacan por su polivalencia y capacidad para trabajar en ramas muy variadas, así como por utilizar métodos de teorías específicas en problemas pertenecientes a disciplinas aparentemente lejanas. Algunos ejemplos claros son Michael Atiyah, creador de la K-teoría topológica, autor del Teorema de los índices de Atiyah-Singer y de numerosos trabajos en teoría de representaciones, ecuaciones del calor sobre variedades y Teoría de Campo Gauge; otro matemático importante a este respecto es Grothendieck, que trabajó simultáneamente en aritmética, geometría algebraica y topología, dando un gran impulso a estas áreas (es curioso hacer notar que incluso tiene un trabajo seminal en análisis funcional); y también consideraremos en este sentido a Alain Connes, por sus contribuciones al análisis funcional, las álgebras de Von Neuman, la K-teoría de operadores y las álgebras de operadores, con aplicaciones a la teoría de números, la geometría diferencial y la física de partículas.

§4. Las últimas Fields

"El premio es completamente irrelevante para mí.
Cualquiera puede entender que si la prueba es correcta
no se necesita ningún otro reconocimiento".
Grigori Perelman.

Por una razón de cercanía temporal, y porque tal vez sean algo menos conocidos, haremos una mención especial a los últimos ocho medallistas Fields, galardonados en los ICM's de Madrid en 2006 y Hyderabad (India) en 2010. Los galardonados en el ICM de Madrid 2006 fueron los siguientes [4]:

- Andrei Okounkov, "por sus contribuciones en la interacción entre probabilidad, teoría de representaciones y la geometría algebraica".
- Grigori Perelman, "por sus contribuciones a la geometría y su revolucionaria profundización en la estructura geométrica y analítica del flujo de Ricci".
- Terence Tao, "por sus contribuciones a las ecuaciones en derivadas parciales, combinatoria, análisis armónico y teoría de números aditiva".

- Wendelin Werner, "por sus contribuciones al desarrollo de la evolución estocástica de Loewner, la geometría del movimiento browniano de dos dimensiones y la teoría conforme de campos".

Andrei Okounkov

El trabajo de Andrei Okounkov conecta diferentes áreas de las matemáticas, proporcionando nuevas perspectivas en problemas que se presentan en física. Okounkov toca una gran variedad de áreas, dos referencias claras son el uso de nociones de aleatoriedad y las ideas clásicas de la teoría de representaciones. Okounkov ha utilizado ideas procedentes de la teoría cuántica de campos para demostrar una sorprendente conexión entre las matrices aleatorias y las subsucesiones crecientes en las permutaciones del grupo simétrico. Quizá la siguiente cita muestre un poco lo inusual de su relación con las matemáticas y justifique en parte la originalidad de su trabajo [5]:

Figura 3: Medallistas Fields en 2006.

"Lo que quizá fue menos usual es el camino que me llevó a las matemáticas. No fui a escuelas especiales ni a olimpiadas. Llegué tras estudiar económicas y hacer el servicio militar. Tuve familia antes que artículos. Como resultado, mi mente no es probablemente tan rápida como hubiera sido con una formación más temprana en matemáticas. Pero quizás también tuve algunas ventajas sobre mis compañeros más jóvenes. Tenía una visión más amplia del universo y una mejor idea acerca del lugar en el que se sitúan las matemáticas".

Grigori Perelman

Grigori Perelman se ha hecho mundialmente conocido por su renuncia a la Medalla Fields, al premio de un millón de dólares concedido por el Instituto Clay de Matemáticas por la resolución de la conjetura de Poincaré, uno de los siete *Problemas del Milenio*, e incluso a su puesto en el Instituto Steklov de San Petesburgo. Su motivación radica en la sensación de aislamiento de la comunidad matemática, y su rechazo a las formas habituales de revisión de artículos y publicación en las revistas matemáticas.

En cualquier caso, la brillantez y originalidad de sus trabajos, que han proporcionado una forma de resolver dos importantes problemas de la topología, la conjetura de Poincaré y la conjetura de geometrización de Thurston, están fuera de toda duda. La conjetura de Poincaré pertenece a la topología, y se refiere a las variedades de dimensión 3. La pregunta al respecto (de una forma muy simplificada) es: ¿puede cada 3-variedad simplemente conexa (sin agujeros) ser deformada hasta convertirse en una 3-esfera? La conjetura de Poincaré afirma que la respuesta es sí. El trabajo de Perelman se basa en el análisis del *flujo de Ricci*, una ecuación de evolución introducida por Richard Hamilton en 1982, similar a la ecuación del calor, que describe cómo fluye el calor de la parte más caliente de un objeto a la más fría, hasta homogeneizar la temperatura de manera uniforme en todo el objeto. La idea de Hamilton fue utilizar el flujo de Ricci para homogeneizar las 3-variedades y mostrar que su geometría se ajusta a la clasificación de Thurston. La principal contribución de Perelman fue conseguir resolver el problema de las singularidades, que son regiones donde la geometría, en lugar de evolucionar hacia la homogeneidad, muestra repentinos e incontrolados cambios. Al método utilizado lo denominó "surgery" (cirugía).

Terence Tao

La trayectoria profesional de Terence Tao es abrumadora. Obtuvo el grado de doctor en matemáticas a los 21 años en la Universidad de Princeton. Ha escrito numerosos trabajos de investigación con más de 30 colaboradores y sus intereses abarcan una gran variedad de disciplinas matemáticas, incluyendo análisis armónico, ecuaciones en derivadas parciales no lineales y combinatoria. Vamos a reseñar aquí dos de sus resultados: el primero, con Ben Green, consiste en la demostración de que el conjunto de números primos, pese a su escasez (no tienen densidad positiva, luego escapan al teorema de Szemerédi) contiene progresiones aritméticas de cualquier longitud. El segundo es un artículo subido al arXiv en febrero de este año, en el que demuestra que todo número impar mayor que 1 es suma de a lo sumo 5 números primos [6], que va en la dirección de la Conjetura de Goldbach (todo número par es suma de a lo sumo dos primos) y utiliza el método del círculo de Hardy-Littlewood.

Otra contribución importante de Tao es al problema de Kakeya. En los últimos años ha sido uno de los principales investigadores del problema de Kakeya n-dimensional, y de sus conexiones con otros problemas en análisis de Fourier y ondas no lineales.

Wendelin Werner

El trabajo de Wendelin Werner muestra una fructífera relación entre las matemáticas y la física. La investigación de Werner ha desarrollado un nuevo marco conceptual para entender fenómenos críticos que aparecen en sistemas físicos. Sus métodos combinan teoría de la probabilidad con ideas de análisis complejo clásico. Se puede decir que por primera vez se concedió una medalla Fields a un probabilista.

Una de las motivaciones del trabajo de Werner es la física estadística, área en la que la probabilidad es usada para analizar el comportamiento a gran escala de sistemas complejos, integrados por muchas partículas.

Un resultado importante de Werner, junto con Lawler y Schramm, es la demostración de la conjetura de Benoit Mandelbrot según la cual la dimensión fractal de la frontera exterior de la trayectoria de un movimiento browniano en el plano es 4/3. Resolver esta conjetura parecía fuera del alcance de las técnicas probabilísticas clásicas. La demostración se basa en relacionar las trayectorias del movimiento browniano con los *clusters* de percolación continuos (los conjuntos del plano que permanecen conectados tras un proceso de percolación aleatoria).

Por último, los galardonados en el ICM de 2010 en Hyderabad fueron los siguientes [7]:

Elon Lindenstrauss

“Por sus resultados en la medida de la rigidez en teoría ergódica y sus aplicaciones a la teoría de números”.

La teoría ergódica trata (a grandes rasgos) de los sistemas dinámicos. Se dice que un tal sistema es *ergódico* cuando tiene el mismo comportamiento tanto en el tiempo como en el espacio.

Hay un concepto de medida invariante sobre el sistema. Los resultados de Lindenstrauss se pueden describir brevemente como que existen pocas medidas invariantes.

De modo sorprendente, Lindenstrauss ha trasladado sus herramientas de teoría ergódica a las aproximaciones diofánticas. Su trabajo es una continuación de los de Dirichlet y Littlewood. En concreto, dados $\alpha, \beta \in \mathbb{R}$ y un $\varepsilon > 0$, Littlewood conjetura que existen infinitos números racionales p/q y r/q tales que

$$\left|\alpha - \frac{p}{q}\right| \left|\beta - \frac{r}{q}\right| < \frac{\varepsilon}{q^3}$$

La conjetura quedó abierta durante mucho tiempo. Lindenstrauss, en colaboración con Einsieder y Katok, prueba que el conjunto de pares (α, β) para los que falla la conjetura de Littlewood tiene *dimensión Hausdorff* uno (para una breve definición de dimensión Hausdorff, véase [8]).

Figura 4: Medallistas Fields en 2010.

Otros trabajos importantes de Elon Lindenstrauss están en el ámbito del caos cuántico, analizado desde un punto de vista aritmético. Tiene especial relevancia la prueba de una conjetura de Rudnick y Sarnak sobre *ergodicidad cuántica única* [7].

Ngo Bao-Chau

“Por su demostración del lema fundamental en la teoría de formas automorfas mediante la introducción de nuevos métodos álgebro-geométricos”.

El *lema fundamental* es una pieza clave para el desarrollo del programa de Langlands. La novedad de Ngo es el empleo de fibraciones de Hitchin. La idea es de naturaleza geométrica y es una construcción inspirada por cuestiones de física fundamental (para mayor detalle véase de nuevo [7]).

Stanislav Smirnov

“Por la prueba de la invarianza conforme del modelo de percolación y del modelo plano de Ising en física estadística”.

El trabajo de Smirnov se centra en los llamados procesos de percolación, que parten del estudio de difusión de líquidos a través de medios porosos. Los métodos de Smirnov le han permitido también abordar el modelo de Ising, que describe fenómenos en el magnetismo, en el movimiento de los gases, en el procesado de imágenes y en ecología.

Cédric Villani

“Por sus pruebas del amortiguamiento de Landau y de la convergencia al equilibrio de la ecuación de Boltzmann”.

Su primer gran resultado científico fue el estudio de la teoría de Boltzmann sobre la difusión de gases. Este descubrimiento es el punto de partida de la moderna teoría de la entropía que constituye una de las evidencias más claramente observables desde un punto de vista experimental de la flecha del tiempo.

La contribución de Villani es estudiar el comportamiento de los sistemas considerados por Boltzmann a largo plazo, es decir, los efectos de la entropía tras un largo período de tiempo. Tiene especial interés a este respecto un artículo de Villani con Desvilletes y otro con Toscani.

Otro aspecto de la obra de Villani relacionado con la entropía tiene que ver con la afirmación de Landau de que un plasma alcanza equilibrio sin que esto suponga un aumento de la entropía. Una descripción más detallada, así como referencias a los artículos originales puede verse en [7].

§5. Unas últimas reflexiones

“Es evidente que necesitamos más financiación, sobre todo acompañada de una planificación que evite las continuas improvisaciones que Gobierno tras Gobierno está sufriendo la ciencia española”.

Manuel de León.
El País, 24 de agosto de 2010.

Después de leer sobre las medallas Fields, me surge una pregunta ¿cabe esperar que algún investigador de nuestro país consiga próximamente una medalla Fields?

En las últimas décadas, las matemáticas españolas han experimentado un importante crecimiento en volumen, calidad y presencia internacional, de lo que sin duda fue escaparate el ICM de Madrid en 2006.

Sin embargo, faltan muchas cosas por hacer para mejorar la investigación científica española. Efim Zelmanov, en la entrevista concedida a esta revista, afirma que en España hay poca abundancia de investigadores extranjeros, la cual es imprescindible para formar buenos equipos de investigación, evitar la posible “endogamia”, favorecer la renovación y el flujo de ideas y aprovechar la potencia de la colaboración internacional. Desde luego, este no es el único problema de la ciencia española. Lo que es claro es que para mejorar la situación es necesaria la convicción de que la investigación científica es imprescindible para el éxito de nuestra sociedad a medio plazo. Cabe preguntarse si vamos en la dirección correcta. Quizás todavía arrastremos una histórica falta de tradición científica, o el soporte social aún no sea el suficiente, pero a la postre, las políticas científicas gubernamentales no satisfacen las necesidades de un sistema de investigación que pretende situarse en la primera línea internacional.

En mi opinión, la investigación científica, y en particular la ciencia de base, más allá de patentes o aplicaciones directas al tejido económico, que por supuesto son necesarias, es imprescindible para la buena salud de una sociedad floreciente. Que un investigador afincado aquí consiga una medalla Fields será un gran éxito, y tendremos muchísimo más que celebrar que el mero galardón, pues será señal de que vamos por el buen camino.

Referencias

[1] Guillermo P. Curbera: *Mathematicians of the World, Unite! The International Congress of Mathematicians: A Human Endeavor.*
AK Peters (2009).

[2] Adolfo Quirós Gracián: *Las Medallas Fields.*
La Gaceta de la RSME, Vol 1, nº 2 (1998).

[3] José Luis Fernández Pérez y Adolfo Quirós Gracián: *Las Medallas Fields y los Congresos Internacionales de Matemáticos.*
La Gaceta de la RSME, Vol 3, nº 2 (2000).

[4] Adolfo Quirós Gracián: *Las Medallas Fields y otros galardones del ICM 2006.*
La Gaceta de la RSME, Vol 9, nº 3 (2006).

[5] *Entrevista a Andrei Okounkov, Medalla Fields en el ICM Madrid 2006.*
La Gaceta de la RSME, Vol 9, nº 3 (2006).

[6] Terence Tao. *What's new.* `http://terrytao.wordpress.com/`

[7] Leovigildo Alonso Tarrío y Ana Jeremías López: *Las Medallas Fields 2010.*
La Gaceta de la RSME, Vol 14, nº 1 (2011).

[8] Irene González y Juan Rojo: *El Conjunto de Cantor.*
Matgazine, nº 1 (2011).

Víctor Arnaiz Solórzano
Estudiante de la Universidad Complutense de Madrid
`vicarsol@gmail.com`


I WANT YOU
TO JOIN
MATGAZINE

La Biblioteca, de luto

Sección a cargo de

Ángel D. Martínez Martínez

Como siempre, invitamos a los lectores a enviar reseñas a

`matgazine@gmail.com`

En esta ocasión, y como novedad, incluimos una breve subsección acerca de «literatura». Sin más dilación proseguimos.

La teoría de Galois según Artin

By learning the masters, not the pupils.
(Niels Henrik Abel)

En esta primera reseña trataremos dos libros de Artin, ambos sobre la misma temática: la teoría de Galois clásica[1]. Parafraseando a Julio Cortázar cada libro tiene un número determinado de lectores, finito; en ocasiones éstos abarcan un par de generaciones, rara vez más. Los que nos ocupan llevan más de medio siglo a sus espaldas y podrían pertenecer a esta segunda categoría. Por nuestra parte hemos de enfatizar el auténtico privilegio de disfrutar en primera persona, y no a través de terceros, de la voz de uno de los más distinguidos artistas de las Matemáticas del siglo XX. Pese a que podría pensarse que (por acumular lustros desde su primera publicación) están más que amortizados, éstos procuran al lector una cercanía con la materia casi inexistente en otros trabajos; que se limitan a compendiar y organizar los resultados que consideran oportunos. No en balde la maestría de Artin es proverbial, figurando entre sus alumnos más renombrados Serge Lang, John Tate, H. Zassenhauss y Max Zorn[2]. Tras esta digresión comenzamos la reseña propiamente dicha.

El primer texto al que nos referiremos, *Modern Higher Algebra. Galois theory* [A1], fue publicado en 1947 basado en las notas de unas clases del autor tomadas por Albert A. Blank. El segundo, *Galois theory: lectures delivered at the University of Notre Dame* [A2] publicado con anterioridad en 1942, fue fruto del interés de Artin en desarrollar el teorema fundamental de la teoría

[1] Para el primerizo apuntar que existen más teorías de Galois (e.g. diferencial, de recubrimientos, etc.).

[2] Resulta curioso que E. Artin denominase *“lema innombrable”* al que hoy conocemos como *lema de Zorn* (véase [A4] p.8).

de Galois sin la necesidad de emplear el teorema del elemento primitivo como parte sustancial de su prueba. De los tres capítulos que contiene, el último se debe a A. N. Milgram. Cada uno de ellos complementa al otro en cierto sentido. El primero resulta una peripatética introducción de lectura suave, el segundo viene a ser la versión condensada y ligeramente ampliada del primero. ¡Y basta de preliminares!

En [A1] el autor no se limita ni a desarrollar la materia por el manido estilo *Definición-Teorema* ni a explicarnos cuán buena será en función de qué problemas clásicos permitió resolver. En su lugar consigue trasladar al lector la intuición y perspectiva necesarios para que cada paso resulte evidente, para que el camino en sí mismo fructifique y no haya que atravesar un desierto estéril con la esperanza de encontrar un oasis que nos ampare. El libro comienza ofreciendo sucintas (pero necesarias para la continuidad de la exposición) discusiones sobre aspectos básicos de la teoría de grupos, anillos, cuerpos, álgebra lineal y polinomios sobre un cuerpo. Decir que el primer problema propuesto puede resultar poco iluminador pero cobra sentido capítulos más tarde. A continuación desarrolla aspectos básicos sobre la factorización de elementos, divisibilidad e ideales en un anillo. En el cuarto capítulo, tras una discusión relativa a relaciones de equivalencia, introduce aspectos básicos de la aritmética modular y observa que el procedimiento puede emplearse para construir extensiones de cuerpos. Tal y como intuitivamente se construye la extensión $\mathbb{C}/\mathbb{R}$; es decir, *añadiendo i (solución de* $x^2 + 1 = 0$*) a* $\mathbb{R}$. El resto del capítulo lo dedica al concepto de automorfismo, que más tarde tendrá un papel central. Antes de finalizarlo, mediante el estudio de ejemplos concretos, adelanta las implicaciones (y motiva el estudio) de la teoría de Galois; concretamente expone la posibilidad de utilizarla para determinar la constructibilidad de polígonos regulares con regla y compás. Llegados a este punto y tras una buena parte del libro rodada llega un capítulo de mayor extensión dedicado exclusivamente a la teoría de Galois. Los dos últimos capítulos dedican su contenido a resultados sobre irreducibilidad (criterio de Eisenstein), raíces primitivas de la unidad, las extensiones ciclotómicas que generan, construcciones con regla y compás, teorema de Steinitz, grupos de permutaciones, resolución de ecuaciones por radicales (teorema de Abel) y solubilidad (que difiere del anterior en característica finita[3]). Contiene 52 ejercicios intercalados con el texto.

En segundo lugar [A2] más terso y breve, pero elegantemente estructurado, posee unos contenidos comparables a los del anterior. Es preciso mencionar

[3]Esbozando los que se conocen hoy en día como polinomios de Artin-Schreier.

algunos de los puntos en los que difieren. Las principales diferencias son la incorporación al corpus de [A2] de una discusión (para el resto del volumen prácticamente irrelevante) acerca de la teoría de determinantes sobre un cuerpo (existencia, unicidad, desarrollo del determinante y regla de Cramer), la utilización de extensiones de Kummer en la demostración del teorema de Abel o la fina demostración acerca de la no solubilidad del grupo simétrico S_n para $n > 4$. Por último comentar que no contiene ejercicios.

No podemos concluir la reseña sin advertir que la nomenclatura de Artin es ligeramente distinta al estándar actual, e.g. los cuerpos que considera no requieren de la conmutatividad del producto o denomina extensiones normales a las que ahora se conocen como extensiones de Galois. Insistir en que éste no es impedimento para el completo disfrute del par de piezas.

Requisitos: [A1] no requiere más que cierta madurez en la lectura. Por otra parte [A2] requiere además cierta fluidez en rudimentos de álgebra básica (relativos a grupos, cuerpos, anillos de polinomios sobre los mismos e ideales).

Referencias

Las ediciones originales fueron [A1] y [A2]; no en balde ambos han sido reeditados en [A3] y [A4] respectivamente. Esto último tiene su importancia para aquellos a los que el continente tiene tanta importancia como el contenido.

[A1] Artin, Emil – *Modern Higher Algebra. Galois theory.* Notes by Albert A. Blank.

[A2] Artin, Emil – *Galois theory: lectures delivered at the University of Notre Dame.* University of Notre Dame, 1942[4].

[A3] Artin, Emil – *Algebra with Galois theory.* Notes by Albert A. Blank. Courant 15 (AMS-CIMS), 2007. 126 páginas.

[A4] Artin, Emil – *Exposition by Emil Artin: a selection.* Editor: Michael Rosen. History of Mathematics Sources (AMS-LMS), 2007. 43 páginas.

[4]Este libro pertenece al dominio público y una reedición de 1971 escaneada puede obtenerse en `http://projecteuclid.org`.

Uno de teoría analítica de números

Muchos de los aspectos que toca el libro que nos ocupa: *Introduction to analytic number theory* [C]; han tenido, están teniendo o se espera que tengan un progreso análogo en generalizaciones más allá de lo que el autor deja entrever. Es así que [C] contiene resultados que, además de su interés intrínseco, sirven como motivación de técnicas con un alcance mayor. Como opertura sienta las bases, tanto notacional como conceptualmente, de la aritmética modular básica. Los primeros dos capítulos incluyen entre sus resultados más notables el pequeño teorema de Fermat, la generalización debida a Euler de éste, la demostración de Euclides sobre la infinitud de números primos o que $F_5 = 2^{2^5} + 1$, el quinto número de Fermat, no es primo. También es reseñable el hecho de que contenga tres demostraciones diferentes del teorema de factorización única de números enteros[5]. Finaliza el capítulo con un teorema de Lagrange que acota el número de soluciones de un polinomio de grado n sobre un cuerpo con un número primo de elementos.

El siguiente ofrece una sucinta introducción a la *aproximación diofántica*[6] aportando pruebas de resultados sobre la bondad de la aproximación de números reales por racionales y aplicaciones a la expresabilidad de números como suma de dos cuadrados. Premonizando el teorema de Dirichlet (que habrá de esperar hasta el décimo capítulo) prueba que existen infinitos primos en cada una de las sucesiones de la forma $4k \pm 1$. Concluye la sección con un teorema de Hurwitz que refina algunos de los resultados del capítulo.

El par que sobrevienen centran su estudio en dos clásicos de la teoría de números: el teorema de Lagrange sobre sumas de cuatro cuadrados y la reciprocidad cuadrática. El primero de ellos comienza introduciendo el símbolo de Legendre, pasando por el teorema de Wilson, el criterio de Euler sobre restos cuadráticos de primos impares[7], el teorema de Euler sobre expresabilidad como suma de dos cuadrados de primos $p \equiv 1 \pmod 4$ y, finalmente, el mentado teorema de Lagrange. En el siguiente se enuncia y establece la veracidad de la célebre ley de reciprocidad cuadrática. La prueba es en cierto sentido obscura al emplear sumas de Gauss, pero tiene la ventaja de manifestar la fuerza del análisis al servicio de la teoría de números (¡siendo el primer ejemplo del paradigma que estudia este libro!). Recordemos que K. F. Gauss encontró ni más ni menos que ocho demostraciones de la misma. Un hecho que también despertó el interés de Yu. Manin, quien se pronunció al respecto:

---

[5] Una de ellas utilizando secuencias de Farey, a las que dedica un parágrafo.

[6] Por supuesto no en estos términos.

[7] Que bien puede tomarse como definición del símbolo de Legendre para éstos.

"When I was very young I was extremely intereseted in the fact that Gauß found seven or eight proofs of the quadratic reci procity law. What bothered me was why he needed seven or eight proofs. Every time I gained some more understanding of number theory I better understood Gauß' mind. Of course he was not looking for more convincing arguments – one proof is sufficiently convincing. The point is, that proving is the way we are discovering new territories, new features of the mathematical landscape." ([L], p.22).

El capítulo finaliza con la aplicabilidad de esta ley al cálculo explícito del símbolo de Legendre y ofreciendo la conocida ley complementaria para primos pares.

A continuación el autor vuelve a cambiar de tercio y nos ofrece un brevísimo capítulo dedicado a funciones aritméticas. En él estudia el comportamiento en media de ciertas funciones de interés aritmético así como resultados relativos a funciones multiplicativas (e.g. la función de Möbius o la de Euler). También contiene un interesante resultado sobre números perfectos y primos de Mersenne. Con esto nos referimos a la equivalencia:

$$2^{n-1}(2^n - 1) \text{ número perfecto par } \Leftrightarrow 2^n - 1 \text{ primo (de Mersenne)}$$

Una de las implicaciones es conocida desde la antigüedad clásica y la otra se debe a Euler. Dada la relativa tecnicidad del resto de resultados que componen el capítulo omitimos su descripción. (Rogamos disculpen las molestias.)

En el séptimo se incluye la prueba debida a Euler acerca de la infinitud de primos que, en cierta forma, inspirará la prueba de Dirichlet sobre la infinitud de primos en sucesiones aritméticas $ax+b$ con $(a,b)=1$. Incluye (entre otros) un resultado de Chebyshev cercano al teorema del número primo, teorema que servirá de broche final al volumen; y, una prueba del postulado de Bertrand, que asegura que:

«*entre n número natural y $2n$ siempre existe un primo p*».

También incluye la identidad de Euler (convenientemente generalizada). En los siguientes el autor vuelve a dar un giro y pasa a discutir los teoremas de equidistribución de Weyl sobre sucesiones en la recta real y la circunferencia, un teorema de Minkowski, lema de Birkoff y sus aplicaciones a ciertas ecuaciones con coeficientes enteros.

Los últimos capítulos introducen la función ζ de Riemann, unos mínimos de teoría de caracteres y tras el estudio de las series de Dirichlet (de las que las funciones-L son casos especiales) prueba el mentado teorema de Dirichlet. Concluye el libro con una selección de clásicos acerca del teorema del número primo (Hadamard-de la Vallée Poussin, teorema de Wiener-Ikehara y enunciados equivalentes al mismo). Incluye un apéndice con notas comentadas y referencias históricas correspondientes a cada capítulo. No contiene ejercicios.

Como se puede apreciar el autor consigue, en apenas 140 páginas, exponer elegantemente una gran cantidad de resultados clásicos.

Requisitos: los primeros capítulos no requieren más que cierta madurez; conforme el libro avanza comienza a requerir conocimientos básicos de análisis complejo así como cierta solvencia en su uso. Salvo por esta última excepción el libro es esencialmente autocontenido.

Referencias

[C] Chandrasekharan, Komaravolu - *Introduction to analytic number theory.* Springer-Verlag, 1968. 140 páginas.

[L] Lemmermeyer, Franz - *Reciprocity laws. From Euler to Eisenstein.* Springer Monographs in Mathematics, 2000.

«Literatura»

Esta sección nace con la intención de acercar artículos interesantes y asequibles a quien, en principio, pueda estar interesado. En muchas ocasiones este tipo de documentos supera cualquier libro de texto (bien sea por su frescura, su eminente valor histórico o la inexistencia de una exposición que incluya esos conocimientos). Es ilustrativo el hecho de que cuando alquien se refiere a un resultado que está en la «literatura», rara vez se está refiriendo a un libro de texto, sino a una publicación. Esperamos que disfrutéis las sugerencias de este número. Los autores de los artículos escogidos para esta ocasión son: Milnor (a quien conocéis de capítulos anteriores) y Fürstenberg (¡a quien deberíais conocer!).

Topología y números primos

En esta breve nota, de apenas un párrafo, el autor nos deleita con una de las pruebas más fascinantes[8] sobre la infinitud de números primos. Decir más, sería decir de más.

Requisitos: basta conocer la noción de *topología* sobre un conjunto.

Referencia: Fürstenberg, Hillel – *On the infinitude of primes.* The American Mathematical Monthly, 1955. Un párrafo.

Milnor, Brouwer y la bola peluda

En este breve artículo Milnor provee sendas demostraciones del teorema de la bola peluda y el punto fijo de Brouwer. Estos resultados ya se encontraban en el "Topología" del mismo autor (pp.14&30). Lo que las hace diferentes es su carácter elemental[9] ya que requieren muy poco para su comprensión. Mencionar que de nuevo hace aparición el teorema de aproximación de Weierstrass.

Requisitos: rudimentos de topología y análisis en el espacio euclídeo.

Referencia: John W. Milnor – *Analytic proofs of the "hairy ball" theorem and Brouwer's fixed point theorem.* The American Mathematical Monthly, 1978. 4 páginas.

[8] Junto con las aportadas por Euclides y Euler, que bien podéis consultar en [C].

[9] ¡Y no sólo la acepción que esta palabra tiene matemáticamente hablando!

If one proves the equality of two numbers a and b by showing first that "a is less than or equal to b" and then "a is greater than or equal to b", it is unfair, one should instead show that they are really equal by disclosing the inner ground for their equality.

(Emmy Noether)

Problemas y Soluciones

Sección a cargo de

Gabriel Fürstenheim Milerud

Las soluciones a los problemas deben enviarse, preferiblemente, al encargado de la sección a

`problemas.matgazine@gmail.com`

en formato TEX. Una forma alternativa es entregarlas en mano en la asociación Lewis Carroll. El plazo de entrega termina el 15 de Septiembre del 2012.
También solicitamos a los lectores problemas originales (con solución) o problemas poco conocidos adecuadamente documentados. Para su publicación se valorará su interés matemático. Para incitar más vuestra colaboración, los autores de soluciones que escojamos publicar recibirán el siguiente ejemplar de la revista gratuitamente. Asimismo, si proponéis algún problema que sea seleccionado también recibiréis gratis el siguiente número.
Los problemas están organizados en orden creciente de dificultad, donde • indicará que un problema es difícil y •• que es especialmente complicado. Los problemas de los cuales no tengamos solución irán marcados con $\star$

Problemas

Problema 18. *Propuesto por la redacción*

1. Un ratón empieza en el centro de un disco y desea escapar del mismo. Para ello debe sobrepasar al gato, que sólo se puede mover por la circunferencia. Si la velocidad máxima del gato es cuatro veces la velocidad máxima del ratón, encontrar cómo se tiene que mover el ratón para poder escapar.[1]

2. $\star$ El problema es el mismo que en el apartado anterior pero ahora la velocidad máxima del gato es k veces la del ratón. ¿Cuál es el mayor k para el cual el ratón puede escapar?

[1] Si queréis experimentar con el problema es posible jugar en internet en la dirección `http://finofilipino.com/post/3187556573/el-juego-del-raton-y-el-gato`

Problema 19. *Propuesto por la redacción*

Dos amigos eligen alternativamente un número del 1 al 9 sin poder repetir. El primero que consigue sumar 15 utilizando exactamente tres de los números que tiene es el que gana. ¿Quién tiene la estrategia ganadora?

Problema 20. *Propuesto por la redacción*

Un rey tiene 1000 botellas de vino, una de ellas envenenada. Para identificar cuál es contrata a un Matemático y pone a su disposición siervos prescindibles. El Matemático puede dar a cada siervo una “bebida” (combinación de vinos) y si uno de ellos era el envenenado el siervo muere. Como el rey tiene prisa el Matemático debe dar todas las bebidas a la vez para que cuando se vean los siervos que han muerto y los que han vivido determinar cuál era la botella. Demostrar que es posible llevar a cabo la tarea dando de beber a sólo 10 siervos.

Problema 21 (El problema de la pizza). *Propuesto por la redacción*

1. Dos amigos, Antonio y Belén, desean compartir una pizza circular. Ambos tienen hambre así que cada trozo debe tener la misma área. Sin embargo, su cortador de pizzas está muy estropeado por lo que desean que la longitud del corte sea lo menor posible. Demostrar que tienen que cortar la pizza por la mitad.
2. $\star$ ¿Cómo deben cortar la pizza si en lugar de 2 amigos hay n amigos?

Problema 22. *Propuesto por la redacción*

1. Sea $g\colon \mathbb{R} \to \mathbb{R}$ una función arbitraria. ¿Existe siempre una función $f\colon \mathbb{R} \to \mathbb{R}$ tal que $f(f(x)) = g(x)$ para todo $x \in \mathbb{R}$?
2. Si a la g del primer apartado se le pide que sea continua. ¿Existe siempre una función continua f que satisface esa identidad?

Soluciones

Problema 12. *Propuesto por J.M. Conde Calero, profesor de la U. de Alicante*

¿Existen números enteros positivos u, v, w, z tales que $u^3+v^3+w^3+z^3 = 100^{100}$?

Solución enviada por Adrián Franco Rubio U. Zaragoza. También resuelto por Disoluto García Martínez, estudiante de la U. Complutense

La respuesta a la pregunta planteada es afirmativa. Veamos que podemos encontrar cuatro números u,v,w,z que satisfagan la igualdad. Para ello haremos uso de la siguiente expresión:

$$\sum_{j=1}^{n} j^3 = \left(\frac{n(n+1)}{2}\right)^2 = {T_n}^2$$

donde T_n denota el n-ésimo número triangular. La demostración por inducción de esta propiedad no es complicada.
Una vez establecido esto, el problema está prácticamente resuelto cuando nos damos cuenta de que 100 es el cuadrado del cuarto número triangular, 10, lo que nos permite escribirlo como la suma de cuatro cubos consecutivos:

$$1^3 + 2^3 + 3^3 + 4^3 = 100$$

Y sin más que multiplicar por 100^{99} podemos llegar a la expresión del enunciado. En consecuencia, para

$$u = 100^{33} \quad v = 2 \cdot 100^{33} \quad w = 3 \cdot 100^{33} \quad z = 4 \cdot 100^{33}$$

así como para todas sus permutaciones se cumple la ecuación del enunciado y queda demostrada la existencia de soluciones de la misma. □

Problema 13. *Propuesto por Daniel Estévez Sánchez, estudiante en la UAM*

Sea K un subcuerpo de $\mathbb{C}$, A una matriz $n \times n$ con entradas en K tal que $L = \lim_{n\to\infty} A^n$ existe como matriz en $\mathbb{C}$. Demostrar que L tiene todas sus entradas en K.

Solución enviada por el proponente

Probaremos de hecho que en estas condiciones, la matriz L puede calcularse algebraicamente mediante operaciones en K usando el siguiente algoritmo. A partir de esto, resulta claro que L ha de tener todas sus entradas en K.

Algoritmo. Sea $p(x) = \det(A - xI)$ el polinomio característico de la matriz A. Sea $r(x) = \operatorname{mcd}\{p(x), (x-1)^n\}$. Ponemos $q_1(x) = p(x)/r(x)$. Entonces $q_1(1) \neq 0$ y podemos poner $q(x) = q_1(x)/q_1(1)$. Entonces L puede calcularse como

$$L = q(A).$$

A la vista del algoritmo, puesto que A tiene entradas en K, $p \in K[x]$, y se sigue que $r, q_1, q \in K[x]$, por lo que $L = q(A)$ tiene entradas en K.

Dedicaremos el resto de este texto a probar que en efecto $L = q(A)$.

Primero observamos que, bajo las condiciones del enunciado, los autovalores de A están contenidos en $\{z : |z| < 1\} \cup \{1\}$. Si $v \neq 0$ y $Av = \lambda v$, se tiene

$$\lim_{n\to\infty} A^n v = \lim_{n\to\infty} \lambda^n v = Lv.$$

De ahí se sigue que o bien $\lambda = 1$ o bien $|\lambda| < 1$.

En caso de que A no tenga el autovalor 1, el radio espectral de A, $\rho(A) < 1$, y por tanto $L = 0$. También, $r(x) = 1$ y

$$q(A) = q_1(1)^{-1} q_1(A) = p(1)^{-1} p(A) = 0 = L.$$

Por tanto, el caso en el que A no tiene el autovalor 1 es trivial, y basta examinar el caso en el que A sí tiene el autovalor 1.

En este caso, veamos que la multiplicidad algebraica y geométrica del autovalor 1 coinciden. Supongamos que, por contra, no coinciden. Entonces se tiene $\ker(A - I) \subsetneq \ker(A - I)^2$. Tomamos $v \in \ker(A - I)^2 \setminus \ker(A - I)$, y llamamos $w = (A - I)v \neq 0$. Entonces $Aw = w$ y $Av = v + w$. De ahí se tiene que

$$Lv = \lim_{n\to\infty} A^n v = \lim_{n\to\infty} v + nw.$$

Contradicción, pues $||v + nw|| \to \infty$.

Ahora escribimos la forma de Jordan de A, $A = PJP^{-1}$. Dados los resultados anteriores, podemos elegir J de la forma

$$J = \begin{pmatrix} I_{k\times k} & 0 \\ 0 & \hat{J} \end{pmatrix},$$

donde k es la multiplicidad del autovalor 1 y $\rho(\hat{J}) < 1$.

Ahora, definiendo

$$J_0 = \begin{pmatrix} I_{k\times k} & 0 \\ 0 & 0 \end{pmatrix},$$

puesto que $\hat{J}^n \to 0$,

$$L = \lim_{n\to\infty} PJ^nP^{-1} = PJ_0P^{-1}.$$

Basta por tanto ver que $q(J) = J_0$, en cuyo caso

$$q(A) = Pq(J)P^{-1} = PJ_0P^{-1} = L.$$

Observamos que $r(x) = (x-1)^k$. Puesto que $p(x)$ es el polinomio característico de A, se tiene $p(A) = p(J) = 0$. Esto implica $p(\hat{J}) = 0$. Como $\hat{J}$ no tiene el autovalor 1, $r(\hat{J}) = (\hat{J} - I)^k$ es invertible. Por tanto, ya que

$$q_1(\hat{J})r(\hat{J}) = p(\hat{J}) = 0,$$

ha de tenerse $q_1(\hat{J}) = q(\hat{J}) = 0$. Además, se tiene $q(1) = 1$.

Esto implica que

$$q(J) = \begin{pmatrix} q(I_{k\times k}) & 0 \\ 0 & q(\hat{J}) \end{pmatrix} = J_0,$$

como queríamos demostrar.

Observación 1. Este resultado tiene aplicación práctica para calcular el estado estacionario de una cadena de Markov cuyas transiciones vienen dadas por una matriz estocástica A.

Generalmente tendremos $K = \mathbb{Q}$ y la forma usual de calcular L es numéricamente mediante la identidad anteriormente obtenida $L = PJ_0P^{-1}$, empleando un método numérico para obtener P y J a partir de A.

El cálculo de J, y por tanto el de P requiere calcular las raíces del polinomio característico de A, lo cual en general ha de hacerse numéricamente. Además, en general J y P no tienen entradas en K, por lo que no es claro que $L = PJ_0P^{-1}$ sí las tenga.

Este algoritmo prueba que no sólo L sí tiene entradas en K, sino que además puede calcularse algebraicamente mediante operaciones en K. La complejidad del algoritmo descrito es de $O(n^4)$, siendo la parte más costosa la evaluación de q en A.

□

Problema 14. *Propuesto por Luis Ángel Calvo Pascual, doctorando en el ICMAT*

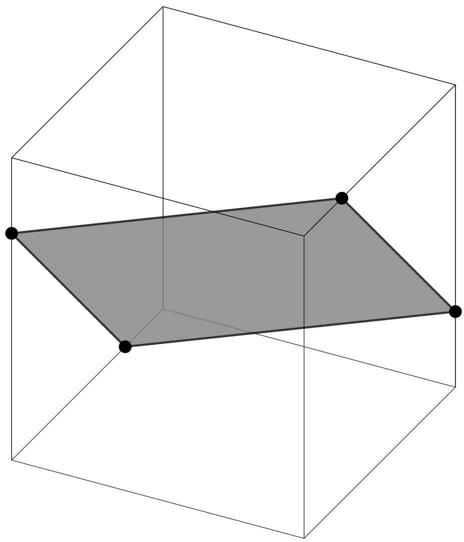
¿Cuál es el mayor cuadrado que se puede inscribir en un cubo?

Solución propuesta por la redacción. Fuente original de la solución
`http://www.artofproblemsolving.com/Forum/viewtopic.php?p=354518`

El mayor cuadrado que se puede inscribir tiene los lados de longitud $\frac{3\sqrt{2}}{4}$. Por ejemplo el cuadrado con vértices en los puntos $(3/4, 0, 0)$, $(0, 3/4, 0)$, $(1, 1/4, 1)$ y $(1/4, 1, 1)$. Para que el problema esté completo hay que comprobar que no hay un cuadrado inscrito con lado mayor que éste.

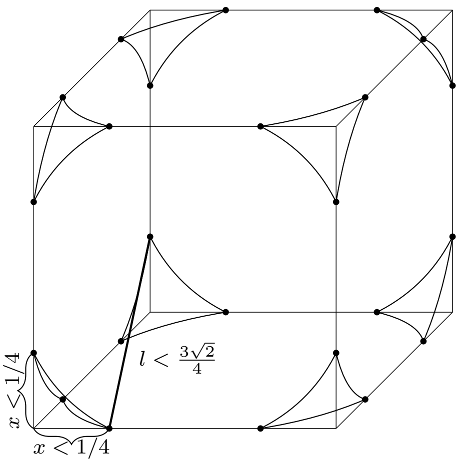
Primero observamos que podemos considerar que el centro del cuadrado es el mismo que el del cubo. Eso se consigue trasladando el cubo en las direcciones de cada eje sucesivamente. Supongamos por ejemplo que la primera coordenada no fuera un medio, es decir que el centro tuviera coordenadas (a, b, c) con $a < 1/2$ (el caso $a > 1/2$ es idéntico). Por ser el centro cualquier otro punto (x, y, z) del cuadrado tiene que tener coordenada $0 < x < 2a$. Por ello al trasladar el cubo a lo largo del primer eje, es decir, hacer $(x + \lambda, y, z)$ para todos los puntos del cuadrado, Como $\lambda \in [0, 1/2 - a]$ (pues queremos que la primera coordenada del cuadrado llegue a ser un medio), el resto de puntos del cuadrado tendrán coordenadas $0 < \lambda < x < 2a + \lambda \leq 1/2 + a$ así que nunca se saldrán del cubo. Repitiendo en todos los ejes se consigue que el centro del cuadrado y del cubo coincidan.

El Cuadrado Óptimo (I)



Por Pitágoras, un cuadrado de lado l tiene distancia r del centro a cualquier vértice $l\sqrt{2}/2$. Si queremos que el lado sea mayor que el que tenemos, $\frac{3\sqrt{2}}{4}$, esta distancia r será mayor que $3/4$. Como teníamos que el centro del cuadrado coincidía con el centro del cubo, en caso de existir tal cuadrado tendría sus vértices en una esfera de centro el del cubo y radio r mayor que $3/4$. Además tiene que estar en el cubo, así que cada vértice tiene que estar en uno de las 8 partes que tiene la intersección de la esfera con el cubo (una por cada esquina del cubo). Cada una de estas partes, triángulos esféricos, se puede incribir en un cubo de lado x, donde x es la altura a la que corta la esfera con la arista. Este x va a ser estrictamente menor que si la esfera tuviera radio $3/4$ y en ese caso vale $\frac{1}{2} - \sqrt{\left(\frac{3}{4}\right)^2 - \left(\frac{\sqrt{2}}{2}\right)^2} = \frac{1}{4}$ (justamente una de las coordenadas de los puntos de nuestro cuadrado). Cada uno de los cuatro vértices del cuadrado inscrito estará en uno de los 8 triángulos esféricos, por tanto dos vértices están en esquinas consecutivas. Sin embargo, los dos triángulos esféricos y de hecho los dos cuadrados de lado x se pueden incribir en un rectángulo de lados x, x, 1 y dos puntos en un rectángulo están a distancia menor que la que hay entre dos esquinas opuestas, que es $\sqrt{1^2 + x^2 + x^2} < \sqrt{1^2 + 1/4^2 + 1/4^1} = \frac{3\sqrt{2}}{4}$ que es la cota que ya teníamos. Recapitulando, si el cuadrado tiene lado más grande que $\frac{3\sqrt{2}}{4}$, entonces está en una esfera lo suficientemente grande como para que dos vértices contiguos del cuadrado estén más próximos que $\frac{3\sqrt{2}}{4}$, por tanto no puede existir tal cuadrado y el nuestro era máximo.

El Cuadrado Óptimo (II)



Cabe mencionar que la generalización de este problema sigue abierta: hallar el mayor n-cubo que se puede inscribir en un m-cubo. El problema que hemos resuelto corresponde al caso con $n = 2$ y $m = 3$.

□

Problema 15. *Propuesto por la redacción*

Dos ciudades A y B están conectadas por dos carreteras C_1 y C_2 que no se cortan. Sabemos que dos coches pueden salir de A y llegar a B yendo por carreteras diferentes y manteniendo siempre una distancia menor que l entre ellos. Supongamos que dos furgonetas son tan anchas que se chocan si están a distancia menor que l. ¿Pueden estas dos furgonetas recorrer los caminos en direcciones contrarias sin chocarse?

Solución enviada por Santiago Biec Amigo. La fuente original del problema es "Ordinary differential Equations" de V.I. Arnold

Por el enunciado del problema existen $\gamma_1, \gamma_2 : [0,1] \longrightarrow Mundo$, tales que $\gamma_1(0) = \gamma_2(0) = A$, $\gamma_1(1) = \gamma_2(1) = B$ y $d(\gamma_1(t), \gamma_2(t)) < l \; \forall t \in [0,1]$.

Nos preguntamos que si las furgonetas pudiendo frenar o volver hacia atrás pueden hacer el trayecto (una en sentido opuesto) permaneciendo suficientemente alejadas. Esto lo formalizaremos componiendo a las funciones γ_1 y γ_2 con $\varphi_1, \varphi_2 : [0,1] \longrightarrow [0,1]$ continuas, sobreyectivas, en general no inyectivas y cumplir $\varphi_1(0) = 0$, $\varphi_1(1) = 1$, $\varphi_2(1) = 0$, $\varphi_2(0) = 1$, $d(\gamma_1(\varphi_1(t)), \gamma_2(\varphi_2(t))) > l \; \forall t \in [0,1]$.

Vamos a ver que por el Principio de intervalos encajados de Cantor existe $t_0 \in [0,1]$ tal que $\varphi_1(t_0) = \varphi_2(t_0)$. Para los que no sean doctos en el cálculo: φ_1, φ_2 son dos curvas contenidas en el cuadrado $[0,1] \times [0,1]$; φ_1 une el punto $(0,0)$ con el $(1,1)$ y φ_2 une las otras dos esquinas, intuitivamente se van a cortar en un punto al que denotaremos $(t_0, T_0) \in [0,1] \times [0,1]$ con $\varphi_1(t_0) = \varphi_2(t_0) = T_0$.

Vamos a construir una sucesión de intervalos $(a_n, b_n)_{n \in \mathbb{N}}$ tal que $b_n - a_n = 1/2^n$, $\varphi_1(a_n) \leq \varphi_2(a_n)$ y $\varphi_1(b_n) \geq \varphi_2(b_n)$; y con esto habremos terminado ya que tendremos que existe un punto t_0 donde $\varphi_1(t_0) \leq \varphi_2(t_0)$ y $\varphi_1(t_0) \geq \varphi_2(t_0)$.

Tomamos $a_0 = 0$ y $b_0 = 1$ donde se cumple trivialmente. Definimos la sucesión de forma inductiva: si $\varphi_1(a_n) \leq \varphi_2(a_n)$ haremos $a_{n+1} = \frac{b_n + a_n}{2}$, $b_{n+1} = b_n$ pero si $\varphi_1(a_n) > \varphi_2(a_n)$ haremos $b_{n+1} = \frac{b_n + a_n}{2}$, $a_{n+1} = a_n$.

Por tanto $d(\gamma_1(\varphi_1(t_0)), \gamma_2(\varphi_2(t_0))) = d(\gamma_1(T_0), \gamma_2(T_0)) \leq l$ ya que $T_0 \in [0,1]$ contradiciendo lo que nos preguntábamos. $\square$

Problema 16. *Propuesto por J.M. Conde Calero, profesor de la U. de Alicante*

Sea $h(t)$ un polinomio cuyos coeficientes son enteros no negativos. ¿Es cierto que h está determinado únicamente por los valores de $h(2)$ y $h(h(2))$?

Solución enviada por Miguel Ambrona, estudiante de la UCM. También resuelto por Pedro Bibiloni, estudiante de la UPC

Es cierto si $h(2) \neq 2$.

1. Si resulta que $h(2) = 2$ entonces $h(h(2)) = h(2) = 2$ y hay dos posibles polinomios con coeficientes enteros no negativos verificando lo anterior. Éstos son $h(t) = t$ y $h(t) = 2$.

2. Supongamos que $h(2) \neq h(h(2))$.
   Llamamos $\alpha = h(2)$ por simplicidad y sea $h(t) = a_n t^n + \cdots + a_2 t^2 + a_1 t + a_0$.
   Con seguridad sabemos que $\alpha > a_i \ \forall i \in \{0, \ldots, n\}$, ya que $h(t)$ no puede ser un polinomio constante ($h(2) \neq h(h(2))$).

   Tenemos que $h(\alpha) = a_n \alpha^n + \cdots + a_2 \alpha^2 + a_1 \alpha + a_0$ y como $0 \leq a_i < \alpha$ para cada i, podemos decir que $(a_n \ldots a_2 a_1 a_0)_\alpha$ es la representación de $h(\alpha)$ en base α, que es única. Por lo tanto, dados $h(2)$ y $h(h(2))$ distintos, el único polinomio h posible es aquél que tiene como coeficientes los "símbolos" de la representación de $h(h(2))$ en base $h(2)$ y es único.

3. Para completar el análisis queda ver qué pasa si $h(2) = h(h(2)) \neq 2$.
   Pero si el polinomio h no es constante y lo evalúas en dos valores (positivos) distintos, devuelve valores distintos. En definitiva, como $h(2)$ es positivo y $h(h(2)) = h(2)$ el polinomio $h(t)$ es constante y debe ser necesariamente el polinomio $h(t) = h(2)$.

$\square$

Problema 17. ●● *Propuesto por Ángel David Martínez, alumno de Máster en la UB*

Sea $f\colon [0,1] \to \mathbb{R}$ una función de clase C^∞, tal que para todo $x \in [0,1]$ existe n_x de manera que $f^{(n_x)}(x) = 0$ Donde $f^{(n_x)}$ es la derivada n_x-ésima. Demostrar que f es un polinomio.

Solución enviada por el proponente. Fuente original de la demostración: Análisis Real. UB. pp. 23-24 de Joan L. Cerdà

Una de las direcciones del problema propuesto es trivial. Nos limitamos por tanto a probar la restante. Antes de nada, recordemos qué decía el teorema de Baire (1889): «*si G_n es una sucesión de abiertos densos en un espacio métrico completo X, su intersección también es densa en él*». Una de las formas en la que se suele presentar es que «*un espacio métrico completo X no vacío no puede ser unión numerable de conjuntos tales que int($\bar{E}_n$) es vacío*»[2]. Esta será la forma en la que lo utilizaremos. En primer lugar definamos los siguientes subconjuntos cerrados de I:

$$C_n := \{x \in I : f^{(n)}(x) = 0\}$$

que, por hipótesis, satisfacen $I = \bigcup_n C_n$. Dado que I es un espacio métrico completo no vacío, algún C_n tiene interior no vacío. Por tanto, existe un

[2]Los conjuntos con esta propiedad se denominan *nowhere dense*.

subintervalo abierto $J \in \mathcal{T}_I$ no vacío tal que f es un polinomio en J (¿Cómo? ¡Escríbelo!). Como el argumento vuelve a aplicarse a $I \setminus J$, aplicando el lema de Zorn se obtiene un abierto $A \in \mathcal{T}_I$ maximal tal que f es un polinomio en cada una de sus componentes arconexas. Ahora bien, su complementario $R = I \setminus A$ es cerrado en I y, *a posteriori*, espacio métrico completo; probaremos a continuación que cada conjunto de la unión $R = \bigcup_n (R \cap C_n)$ es vacío y como consecuencia que $I = A$ tal y como queríamos.

En primer lugar observemos que algún $R \cap C_{n_0}$ tiene algún punto interior y, que no es aislado en R. En efecto, basta aplicar la segunda versión de Baire a la descomposición de R anterior y tener en cuenta que en ningún caso y puede ser un punto aislado (pues contradiría la maximalidad de A)[3]. Es decir, existe un abierto $I_y \in \mathcal{T}_I$ tal que

$$y \in I_y \cap R \subseteq R \cap C_{n_0} \subseteq C_{n_0}$$

Claro que, como y no es aislado, existe una sucesión monótona $\{r_k\}_{k=1}^{\infty} \subset I_y \cap R$ que converge a y. Pero entonces $f^{(n_0)}(r_k) = 0$ y el teorema de Rolle asegura la existencia de otra sucesión $\{y_k\}_{k=1}^{\infty}$ cuyo elemento k-ésimo está entre r_k y r_{k+1} cumpliendo que $f^{(n_0+1)}(y_k) = 0$. De la continuidad de esta derivada y la construcción se sigue que $f^{(n_0+1)}(y) = 0$. Ahora está claro que $f^{(n)}(y) = 0$ para todo $n \geq n_0$. El argumento aplica para todo elemento en la intersección $I_y \cap R$ y, por tanto, ésta está incluida en C_n para $n \geq n_0$.

Finalmente veamos que, de hecho, $I_y \subset C_{n_0}$. Sea $x \in I_y \setminus R$ en cuya arco-componente conexa I_x en A la función f puede expresarse como un polinomio P y ésta es tal que alguno de sus extremos $e \in I_y \cap R$. Así de la continuidad y lo anterior $P^{(n)}(e) = f^{(n)}(e) = 0$ para todo $n \geq n_0$. Como consecuencia el grado de P es a lo sumo n_0, que prueba la inclusión que buscábamos y concluye la demostración ya que esto implica $y \in A$ contrariamente a lo supuesto.

Esta curiosa caracterización de los polinomios en un intervalo se debe a los matemáticos españoles E. Corominas y F. Sunyer Balaguer (1954). $\square$

[3]Basta emplear la continuidad de las derivadas de f; como a ambos lados del punto aislado la función f viene dada por un polinomio, para n suficientemente grande $f^{(n)}$ se anula en un entorno del punto.

Curiosidades

Sección a cargo de

Pablo Portilla Cuadrado

Cerillas y grupos

Javier Culebras Gómez

Supón que tu profesora de Álgebra te propone un juego en el que básicamente te da una caja de cerillas y te dice que sólo puedes colocarlas cabeza arriba:=$\uparrow$ o cabeza abajo:=$\downarrow$, pero te dice que sólo saques tres cerillas y te comenta 2 movimientos que puedes realizar con ellas:

1. d: Movimiento que consiste en mover la cerilla situada a la izquierda a la derecha del todo sin darle la vuelta.
   Ejemplo:
   $$\downarrow\uparrow\uparrow\rightsquigarrow\uparrow\uparrow\downarrow\rightsquigarrow\uparrow\downarrow\uparrow$$
2. f: Movimiento que consiste en darle la vuelta a todas las cerillas sin moverlas de sitio.
   Ejemplo:
   $$\uparrow\uparrow\downarrow\rightsquigarrow\downarrow\downarrow\uparrow$$

Después te realiza una serie de preguntas: ¿De cuántas formas diferentes puedes colocar 3 cerillas? ¿Cuántos y cuáles son los movimientos posibles componiendo d y f sucesivamente (usamos «$\circ$» para denotar hacer un movimiento detrás de otro)? Si todos los movimientos posibles son los elementos del conjunto G, ¿puedes darme su tabla de composición y demostrarme que $(G,\circ)$ tiene estructura de grupo? ¿Es un grupo cíclico?

Las posibles formas de colocar 3 cerillas se puede calcular fácilmente mediante variaciones con repetición: $V^R_{2,3} = 2^3 = 8$. Y si estamos en el caso de n cerillas es $V^R_{2,n} = 2^n$. Sin embargo, si sabemos que hay n cerillas y tienes m formas posibles de colocar cada cerilla, el número de formas posibles también se calcula mediante variaciones con repetición $V^R_{m,n} = m^n$.

Las diferentes formas que tenemos de poner las cerillas son básicamente las distintas aplicaciones que se pueden definir entre el conjunto $A = \{1, 2, \ldots, n\}$ y el conjunto B cuyo cardinal es m, las m formas posibles de colocar cada cerilla. En este caso para $n = 3$ y suponiendo que sólo puedes colocarlas cabeza arriba o cabeza abajo,tenemos que $A = \{1, 2, 3\}$ y $B = \{\uparrow, \downarrow\}$ Todas las formas posibles de colocar las cerillas son los elementos de un conjunto que llamaremos

$$C = \{\uparrow\uparrow\uparrow, \downarrow\downarrow\downarrow, \downarrow\uparrow\uparrow, \downarrow\downarrow\uparrow, \uparrow\downarrow\uparrow, \uparrow\uparrow\downarrow, \downarrow\uparrow\downarrow, \uparrow\downarrow\downarrow\}$$

Ahora vamos a averiguar los movimientos posibles componiendo d y f sucesivamente. A partir de ahora, tendremos en cuenta que los elementos del conjunto G son aplicaciones, y cumplirán la ley asociativa para la composición como todas las aplicaciones. Por ello, omitiremos los paréntesis al escribir las composiciones. Los movimientos que pensamos nada más empezar son estos:

Id		d	f	$d \circ f$	d^2	$d^2 \circ f$
$\uparrow\uparrow\uparrow$	$\rightsquigarrow$	$\uparrow\uparrow\uparrow$	$\downarrow\downarrow\downarrow$	$\downarrow\downarrow\downarrow$	$\uparrow\uparrow\uparrow$	$\downarrow\downarrow\downarrow$
$\downarrow\downarrow\downarrow$	$\rightsquigarrow$	$\downarrow\downarrow\downarrow$	$\uparrow\uparrow\uparrow$	$\uparrow\uparrow\uparrow$	$\downarrow\downarrow\downarrow$	$\uparrow\uparrow\uparrow$
$\uparrow\uparrow\downarrow$	$\rightsquigarrow$	$\uparrow\downarrow\uparrow$	$\downarrow\downarrow\uparrow$	$\downarrow\uparrow\downarrow$	$\downarrow\uparrow\uparrow$	$\uparrow\downarrow\downarrow$
$\uparrow\downarrow\uparrow$	$\rightsquigarrow$	$\downarrow\uparrow\uparrow$	$\downarrow\uparrow\downarrow$	$\uparrow\downarrow\downarrow$	$\uparrow\uparrow\downarrow$	$\downarrow\downarrow\uparrow$
$\downarrow\uparrow\uparrow$	$\rightsquigarrow$	$\uparrow\uparrow\downarrow$	$\uparrow\downarrow\downarrow$	$\downarrow\downarrow\uparrow$	$\uparrow\downarrow\uparrow$	$\downarrow\uparrow\downarrow$
$\downarrow\downarrow\uparrow$	$\rightsquigarrow$	$\downarrow\uparrow\downarrow$	$\uparrow\uparrow\downarrow$	$\uparrow\downarrow\uparrow$	$\uparrow\downarrow\downarrow$	$\downarrow\uparrow\uparrow$
$\downarrow\uparrow\downarrow$	$\rightsquigarrow$	$\uparrow\downarrow\downarrow$	$\uparrow\downarrow\uparrow$	$\downarrow\uparrow\uparrow$	$\downarrow\downarrow\uparrow$	$\uparrow\uparrow\downarrow$
$\uparrow\downarrow\downarrow$	$\rightsquigarrow$	$\downarrow\downarrow\uparrow$	$\downarrow\uparrow\uparrow$	$\uparrow\uparrow\downarrow$	$\downarrow\uparrow\downarrow$	$\uparrow\downarrow\uparrow$

Por tanto hemos conseguido al menos 6 movimientos posibles: $d, f, d^2, f^2, d\circ f, d^2 \circ f$. Cada movimiento transforma el conjunto C en el mismo conjunto C, pero cada uno de una forma diferente. Es necesario utilizar cada movimiento con todo el conjunto C, para no llegar a conclusiones erróneas, como por ejemplo $d \circ f \circ d = f$ ó $f \circ d = f$. Podemos apreciar que si operamos $d \circ d \circ d = d^3$ hemos conseguido las mismas secuencias (en el mismo orden). Lo mismo sucede cuando operamos $f \circ f$, con lo que deducimos que ambos movimientos son el elemento neutro o identidad (el que compuesto con cualquier otro da el mismo, al que llamaremos e) $f^2 = d^3 = e$. Por tanto hemos conseguido 6 movimientos posibles: También podemos afirmar que $d \circ f = f \circ d$ y que $d^2 \circ f = f \circ d^2$. Con esto podemos concluir que cualquier otro movimiento que hallemos compuesto con d y f será uno de los seis que ya tenemos, por ejemplo:

- $d^4 \circ f^5 = d^3 \circ d \circ f^2 \circ f^2 \circ f = e \circ d \circ e \circ e \circ f = d \circ f$
- $d^8 \circ f^3 = d^3 \circ d^3 \circ d^2 \circ f^2 \circ f = e \circ e \circ d^2 \circ e \circ f = d^2 \circ f$

Por lo que se puede comprobar que cualquier movimiento que se coja nos dará cualquiera de los 6 movimientos anteriormente mencionados y que los 6 movimientos son los elementos de un conjunto que llamaremos G:

$$G = \{d, f, d^2, e, d \circ f, d^2 \circ f\}$$

Vamos a construir su tabla de composición:

$\circ$	d	f	d^2	e	$d \circ f$	$d^2 \circ f$
d	d^2	$d \circ f$	e	d	$d^2 \circ f$	f
f	$d \circ f$	e	$d^2 \circ f$	f	d	d^2
d^2	e	$d^2 \circ f$	d	d^2	f	$d \circ f$
e	d	f	d^2	e	$d \circ f$	$d^2 \circ f$
$d \circ f$	$d^2 \circ f$	d	f	$d \circ f$	d^2	e
$d^2 \circ f$	f	d^2	$d \circ f$	$d^2 \circ f$	e	d

Ahora hay que demostrar que (G,$\circ$) tiene estructura de grupo:

1. «$\circ$» es ley de composición interna:
   Operando 2 elementos cualesquiera del conjunto G, obtenemos otro elemento del conjunto G. Es decir: $\forall a, b \in G$ se verifica $a \circ b \in G$ como vemos en la tabla anterior.

2. «$\circ$» es asociativa, es decir $\forall a, b, c \in G$ se verifica que $(a \circ b) \circ c = a \circ (b \circ c)$. Esto se puede comprobar bien en la tabla, o mucho mejor, usando el hecho de que los elementos de G son aplicaciones y la composición de aplicaciones es asociativa.

3. Existe un elemento neutro, que es el movimiento identidad que anteriormente habíamos visto, que era $e = f^2 = d^3$. En la tabla vemos que cualquier movimiento compuesto con e nos da el mismo movimiento. Es decir:
   $$\exists e \in G | \forall a \in G : a \circ e = e \circ a = a$$
   Ejemplo: Para $f \in G \; | f \circ e = e \circ f = f$

4. Todo elemento de G tiene simétrico (como se aprecia en la tabla). Es decir $\forall a, \exists a^{-1} | a \circ a^{-1} = a^{-1} \circ a = e$.

5. Se cumple la propiedad conmutativa: se puede apreciar en la tabla de composición ya que es simétrica respecto a la diagonal principal.

Entonces, como se cumplen las 4 primeras propiedades y además la conmutatividad, es un grupo abeliano. Ahora vamos a afrontar la pregunta de si el grupo es cíclico:

Definición 1. Dado un grupo G, diremos que G es cíclico si existe $a \in G$, denominado generador de G, tal que todo elemento de G o es el neutro, o es a o la composición de a consigo mismo un cierto número de veces, o es a^{-1} o la composición de a^{-1} consigo mismo un cierto número de veces.

Comprobando los miembros de G, podemos ver que $d^2 \circ f$ y $d \circ f$ son elementos generadores de G.

Nótese que el número total de colocaciones de cerillas es $8 = 2^3 \equiv 2 \mod 3$. Esta congruencia será verdad siempre que el número de cerillas sea primo, y es el enunciado del Pequeño Teorema de Fermat. De hecho, las colocaciones de las cerillas y el grupo de transformaciones de las cerillas nos permiten probar este conocido teorema de teoría de números.

Consideremos que hay un número primo n de cerillas y m posiciones en las que pueden estar. Esto, como sabemos, implica que hay m^n colocaciones de las cerillas. Del grupo de transformaciones, vamos a quedarnos sólo con el subgrupo que genera d, que es cíclico de orden n, como ya hemos comprobado para $n = 3$ y es fácil ver para otros números de cerillas. Ahora, vamos a usar las transformaciones para contar de una forma especial cuántas colocaciones posibles hay, y igualar lo que obtengamos con m^n para dar el teorema.

Al aplicar d varias veces a una colocación de las cerillas, vamos obteniendo n colocaciones distintas (aquí usamos que n es primo), excepto en un caso, que es que todas las cerillas estén colocadas de la misma forma: entonces sólo obtenemos una colocación. Esto proporciona una partición del conjunto de colocaciones según cómo actúa d (las órbitas, que se llaman): obtenemos que las colocaciones quedan agrupadas de n en n, salvo las colocaciones "constantes". Además, de este último tipo tenemos m colocaciones distintas, una por cada posición de las cerillas. Entonces, tenemos que el conjunto total, que tenía cardinal m^n, se puede dividir salvo m elementos en partes de n elementos, es decir, su cardinal es un múltiplo de n más m. Lo que es lo mismo, $m^n = nk + m$, es decir, $m^n \equiv m \mod n$.

Esta es la demostración del teorema que puede encontrarse en [1].

Referencias

1. Arthur Engel: *Problem-Solving Strategies (For Math Olympiads).* Springer-Verlag (1997).

Javier Culebras Gómez
Estudiante de la Universidad de Valencia
`jacugo@alumni.uv.es`

Cómo evitar que el queso se caiga de la pizza, una aplicación de la Geometría Diferencial

Gabriel Fürstenheim Milerud

Resumen

En esta curiosidad presentamos la fundamentación matemática de un conocido método para comer la pizza que evita los efectos adversos de la gravedad

§1. Introducción

Estás pasando una noche tranquila con los amigos, como a nadie le apetece cocinar llamáis a un cierto restaurante y poco tiempo después traen la pizza. Tras cortarla en seis trozos, agarras el que te corresponde. Desgraciadamente la punta de la pizza se dobla por efecto de la gravedad y el queso cae a la mesa. Conclusión, has perdido la mayoría del queso; como además era de cuatro quesos esto es un desastre.

En este artículo damos un método, basado en la geometría diferencial, que evita que esto ocurra. En caso de que no lo conocieras te ahorramos tener que limpiar más veces la mesa de tu amigo, en otro caso te explicamos la razón por la cual funciona. Para ello, empezamos con un resumen muy muy rápido de geometría de superficies.

§2. Un breve paseo por la Geometría de Superficies

Antes de nada es importante explicar qué se entiende por Geometría de Superficies. Ésta es una cuestión complicada, pero digamos que la Geometría de Superficies estudia todo aquello que se puede medir: longitudes, ángulos y áreas. Mientras que para un topólogo una taza de café y un donut son lo mismo, para un geómetra no.

Pero qué significa "medir", en el espacio euclídeo es fácil: dibujamos una recta entre dos puntos y vemos la longitud de la recta. En una esfera ya es un poco más complicado, se traza un círculo máximo que pase por los dos puntos y se mide la distancia. Este procedimiento (tomar geodésicas) no va a ser muy efectivo para cualquier superficie genérica. En este momento recordamos el procedimiento para calcular la longitud de la gráfica de una curva, lo que se hacía era tomar el módulo del vector tangente e integrar en el tiempo.

$$s = \int_a^b \sqrt{1 + (f'(x))^2} \mathrm{d}x$$

Éste es quizás el camino a seguir, quizás tengamos que ser capaces medir la longitud de vectores tangentes y después para calcular distancias integrar el módulo. Ahora bien, para definir la norma en el espacio euclídeo el primer paso era definir un producto escalar (de hecho eran equivalentes por la identidad de polarización), eso es lo que vamos a hacer. Resumiendo, dada una superficie diremos que g es una métrica si en cada plano tangente es un producto escalar, es decir, es una forma bilineal simétrica. Además, para poder recuperar propiedades de la superficie exigiremos que esta métrica varíe suavemente al cambiar el punto de la superficie, en otras palabras que sea diferenciable.

Dada la métrica ya podemos medir cualquier cantidad geométrica. Si queremos medir la longitud de una curva, basta calcular el módulo del vector tangente en cada punto (recordemos que como g es un producto escalar $||u||^2 = g(u, u)$) y después integramos a lo largo de la curva. Si nos dan un triángulo, nos vamos al vértice, consideramos los vectores tangentes a los lados y con la métrica podemos hacer el producto escalar, que como sabemos es $||u|| \cdot ||v|| \cos \widehat{uv}$, despejando tenemos el ángulo (o más bien su coseno).

Un objeto que se puede obtener de la métrica y que apasiona a los geómetras es la curvatura. Si no nos restringimos a superficies una búsqueda rápida en Wikipedia arroja más de 10 tipos diferentes de curvatura. Lo que se busca con la curvatura es conseguir medir cómo se retuerce el espacio.

Es una curiosidad muy conocida que si trazas un triángulo en la esfera la suma de sus ángulos es mayor que 180º. Esto lo podemos ver como que hay demasiado espacio dentro de ese triángulo y sale para arriba, abriendo los ángulos. Lo contrario ocurre en el plano hiperbólico (la silla de montar) donde la suma de los ángulos es de menos de 180º. De nuevo podemos ver esto como que hay poca cosa dentro (de hecho en relatividad la curvatura mide en cierta manera la masa) lo que fuerza que el triángulo se contraiga y los ángulos sean más pequeños. En el punto medio está el plano, donde los ángulos miden 180º.

El objetivo de la curvatura es cuantificar este fenómeno, de hecho la curvatura de la esfera es positiva; la del plano hiperbólico, negativa; la del plano, 0 y este resultado sobre los ángulos de un triángulo depende exclusivamente del signo de la curvatura: una superficie con curvatura positiva tendrá la suma de ángulos mayor de 180º, curvatura negativa menor, curvatura 0 igual.

Volviendo al tema, ¿cómo podemos definir la curvatura? La que nos interesará definir será la curvatura de Gauss (que es de la que hablábamos en los casos anteriores) y de hecho para nuestros fines sólo nos interesa su signo. En el caso de la silla de montar hay curvas que se alejan y curvas que se acercan, en ese caso diremos que la curvatura es negativa. Si observamos una esfera desde dentro, todas los círculos máximos se acercan a nosotros, es decir, todos tienen el mismo comportamiento. En esa situación la curvatura de Gauss es positiva. Más difícil es ver cuándo la curvatura es 0. Si doblamos un papel y nos fijamos en un punto del valle, todas las curvas se acercan a nosotros, salvo la recta del valle que está siempre a la misma distancia. En ese caso la curvatura es 0.

Observamos que esta definición no depende de desde dónde miremos la superficie. Viendo la esfera desde el exterior, todos los círculos se alejan de nosotros, como todos tienen el mismo comportamiento la curvatura es positiva de la misma manera que si la mirábamos desde dentro. Intuitivamente lo que hacemos es asignar un signo positivo a una curva que se aleja, un signo negativo a una que se acerca y un signo 0 a un recta. Si todas las curvas tienen el mismo signo entonces la curvatura de Gauss tiene signo positivo. Si las hay de signos opuestos entonces la curvatura de Gauss tiene signo negativo. Finalmente, si todas tienen el mismo signo salvo una que es una recta entonces la curvatura es 0.

Otra manera de verlo, damos un valor a cada curva que dice si se aleja (positiva), se acerca (negativa) o se queda quieta (0). Elegimos la curva que más se acerque y la curva que más se aleje y multiplicamos estos valores, ésta es la curvatura de Gauss. Esta última definición, la de la curva que más se aleja y la curva que más se acerca, es de hecho la definición rigurosa aunque sin fórmulas.¿Qué tiene todo esto que ver con las pizzas? Estamos cerca ya, no desespere.

Es una constante en matemáticas que una vez se tiene un objeto (en nuestro caso la superficie) se estudia todas las virguerías que se le pueden hacer. De ahí lo del toro y la rosquilla, que sean iguales para un topólogo significa que entre las virguerías que éste se permite está pasar de uno a otro. Para un geómetra una transformación permitida tiene que dejar fija la métrica, que es el objeto que le interesa. A esto se le llama isometría local.

Para poder visualizar lo que ocurre, para un topólogo la materia está hecha de una plastilina muy fina (como la goma de un globo) que se puede estirar apretar y deformar. Para un geómetra la materia está hecha como de un papel, es posible modificarlo pero si se estira se rasga.

Ahora entra en juego el conocido como Teorema Egregio de Gauss, que pone en relación ambos conceptos: el de la curvatura de Gauss y el de las isometrías locales. El teorema se llama así del latín “Egregium”, destacable, aunque quizás le sería más adecuada la acepción anglosajona “atroz”, pues la demostración consiste en dos páginas de cuentas para concluir que la curvatura de Gauss, que se había definido tan arbitrariamente, se puede expresar de hecho en función de unos ciertos coeficientes: los símbolos de Christoffel. Como estos símbolos se pueden definir a su vez en función de la métrica, mediante otra fórmula poco agradable, se concluye que la curvatura de Gauss depende de la métrica. Y esto es lo que dice el teorema:

Teorema 2 (Teorema Egregium de Gauss)**.** Es posible obtener la curvatura de Gauss a partir de la métrica.

Es inmediato darse cuenta de cómo relaciona este teorema la curvatura con las isometrías locales. Si una isometría local preserva la métrica y la métrica determina la curvatura, entonces una isometría preserva la curvatura. De esta manera obtenemos automáticamente que no se puede estirar una esfera hasta conseguir un mapa plano, pues se estaría pasando por una isometría desde una curvatura positiva a otra 0. Por supuesto no se da el recíproco. Es decir, si dos superficies tienen las mismas curvaturas no se tiene por qué poder transformar una en otra.

Un ejemplo que pone de relevancia la fuerza del teorema y que ya permite intuir lo que ocurrirá con la pizza es el ejemplo de un cilindro. Si cogemos un papel es posible doblarlo hasta conseguir un cilindro. Formalmente, un cilindro es localmente isométrico a un plano.

Si recordamos lo que decíamos de las curvas que se alejaban o se acercaban, en el plano todas se quedan quietas y, sin embargo, en el cilindro hay curvas que se alejan (las circunferencias de las secciones) y curvas que se mantienen constantes (las generatrices). Es decir, eso que habíamos definido sobre el comportamiento de las curvas no es algo que se mantenga por isometrías. Sin embargo, su producto o curvatura de Gauss sí se mantiene constante, es 0 en todos los puntos. Finalmente pasamos al caso de la pizza.

§3. Desafiando a la gravedad en la pizza

Como anunciábamos en la introducción, al agarrar una pizza suele ocurrir que la gravedad tira de la punta hacia abajo, ésta se dobla y el queso se cae. La solución a este problema es muy fácil una vez que conocemos el teorema Egregio de Gauss. Basta doblar la pizza transversalmente. Como la curvatura de Gauss que es 0 (pues la pizza es plana originalmente) se tiene que mantener y donde estamos doblando las curvas se están acercando, en la dirección de la punta se debe estirar hasta ser una recta para que la curvatura se mantenga. De esta manera se endereza la punta y el queso no se cae.

Referencias

[1] `http://mathoverflow.net/questions/5450/cocktail-party-math`

Gabriel Fürstenheim Milerud
Estudiante de la Universidad Complutense de Madrid
`furstenheim@gmail.com`

♠ Pasatiempos ♠

por

Dawe

1 Tres naves aterrizan a la vez en tres puntos al azar sobre la superficie de un planeta inexplorado. ¿Cuál es la probabilidad de que lo hagan sobre el mismo hemisferio?

2 La proposición: *"Esta proposición es falsa"*, ¿es verdadera o falsa?

3 ¿En cuántas regiones queda dividido el plano al trazar n rectas, de forma que no más de dos rectas se corten en el mismo punto, y sin que haya rectas paralelas?

4 Consideremos los mil primeros números naturales. ¿Podemos asegurar que en cualquier subconjunto formado por 501 de estos números siempre existen dos de ellos tales que uno es múltiplo del otro?

5 Se dispone de un cuerpo sólido en el que la temperatura varía de forma continua entre sus puntos. Se considera una cierta circunferencia en el interior del cuerpo. ¿Puede asegurarse que existan dos puntos en la circunferencia, diametralmente opuestos, con la misma temperatura?

6 Sea P el conjunto formado por los puntos del plano (p, q) que cumplen que:

i) p y q son enteros,
ii) $|p| < 1000$ y $|q| < 1000$,
iii) p y q son primos entre sí.

Tomamos al azar la mitad de los puntos de P, y clavamos alfileres sobre estos puntos. ¿Existe alguna recta que pase por el origen y que deje a cada uno de sus lados la mitad de los alfileres?

Los dos últimos pasatiempos han sido tomados del blog del profesor Juan de Burgos[1]: **El rincón de Gudor** (`http://web.fmetsia.upm.es/gudor/`).

[1] Juan de Burgos es profesor de matemáticas en la Escuela Técnica Superior de Ingenieros Aeronáuticos de la UPM. Desde **Matgazine** le agradecemos que nos hablara de su blog, que tiene todo el espíritu de la divulgación matemática, relatos fantásticos con algo de matemáticas, artículos de opinión, problemas...

Además de los pasatiempos proponemos un pequeño juego, para el que sólo son necesarios papel y lápiz:

Juego de los brotes

Se trata de un juego para dos jugadores. Se dibujan unos pocos puntos (brotes) en una hoja de papel. Por turnos, los jugadores han de unir un brote con otro, que puede ser el mismo, con una línea (rama) y añadir un nuevo brote sobre la línea recién dibujada. A la hora de dibujar nuevas líneas hay que tener en cuenta que:

1. Las ramas pueden tener cualquier trazado, pero no pueden cortarse a sí mismas o a otra ya dibujada.
2. Una rama no puede pasar por un brote que no sea el inicial o el final de la misma.
3. Sólo puede haber tres ramas partiendo de cada brote. Un brote quedará "anulado" cuando se de esta situación.

Pierde el juego el jugador que no es capaz de trazar una nueva rama cumpliendo las condiciones anteriores.

Criptografía

Por fin hemos llegado al último desafío. Como ya dijimos, habrá un premio para el primer lector que resuelva todos los pasatiempos de criptografía aparecidos en los cuatro primeros números de **Matgazine** (que están disponibles en `www.matgazine.tk`). Las soluciones han de mandarse a `matgazine@gmail.com`.

En esta ocasión se ha de recurrir a las soluciones de los problemas anteriores (como ya se había avisado) para dar con el resultado. La cuestión es entender que la pata será gata y viceversa, así como ocurre con gorra y porra (y viceversa).

Dicho esto, la solución se encuentra utilizando todo lo sabido en `http://enigmaco.de/enigma/enigma.swf`.

Y el código es:

HSVSEKVBTFITDPRQNYCRFABSULXGMZK
HNTTURQPFEQSDMPRVOLPGGHROUXVVTHFXCVVKBOMRFTZ

Aquí me despido por el momento de todos los que han intentado resolver esta serie de códigos cifrados. Espero que hayáis disfrutado resolviéndolos tanto como yo poniéndolos a vuestra disposición.

¡Un (último) saludo!

Wirieg

Soluciones a los pasatiempos del *"Sheriff"*

1. ¿Habrá para cualquier conjunto de 10 enteros entre 1 y 100, dos subconjuntos disjuntos cuya suma de elementos sea la misma?

La respuesta es sí.

Hay que aclarar primero que no tienen que contener entre los dos subconjuntos a los 10 elementos. Sea nuestro conjunto A de 10 elementos cualesquiera. Tomemos la familia $\mathcal{P}(A)$ (partes de A), formada por todos los subconjuntos de A, la cual tiene 2^{10} elementos (uno de los cuales es el vacío). A cada uno de los $2^{10} - 1 = 1023$ conjuntos no vacíos de la familia F le asociamos la suma de sus elementos (dando lugar a una lista de 1023 números), ¿pueden ser todos distintos? La suma más grande posible sería $100 + 99 + \cdots + 91 < 1000$, luego debe haber al menos una repetida.

Elegimos dos conjuntos de F con la misma suma (que pueden tener elementos repetidos), y les quitamos a ambos los elementos en común. Esos dos conjuntos son subconjuntos de A con la misma suma.

2. De media, ¿cuántas veces habrá que tirar un dado de n caras para que hayan salido todos los números?

Haremos el caso de 6 caras (más ilustrativo, esto es un pasatiempo) para luego generalizar. Podemos calcular la probabilidad p_i de sacar los 6 números distintos en i tiradas y obtener la esperanza

$$E = \sum_{n=1}^{\infty} i \cdot p_i,$$

pero el cálculo de las p_i puede que resulte muy tedios. Pero sacar un número de cada es lo mismo que (en orden):

- sacar cualquier número (X_6),
- sacar cualquiera de los 5 restantes (X_5),
- sacar cualquiera de los 4 restantes (X_4),
- sacar cualquiera de los 3 restantes (X_3),
- sacar el número restante (X_1).

Una vez convencidos de eso, el problema se reduce a calcular las esperanzas de las X_i y sumarlas:

- $E(X_6) = 1$,
- $E(X_5) = \dfrac{5}{6}\sum_{n=1}^{\infty} n\left(\dfrac{1}{6}\right)^{n-1}$,
- $E(X_4) = \dfrac{4}{6}\sum_{n=1}^{\infty} n\left(\dfrac{2}{6}\right)^{n-1}$,
- $E(X_3) = \dfrac{3}{6}\sum_{n=1}^{\infty} n\left(\dfrac{3}{6}\right)^{n-1}$,
- $E(X_2) = \dfrac{2}{6}\sum_{n=1}^{\infty} n\left(\dfrac{4}{6}\right)^{n-1}$,
- $E(X_1) = \dfrac{1}{6}\sum_{n=1}^{\infty} n\left(\dfrac{5}{6}\right)^{n-1}$,

como, si $x < 1$, se tiene

$$E = \sum_{n=1}^{\infty} nx^{n-1} = \frac{d}{dx}\left(\sum_{n=1}^{\infty} x^n\right) = \frac{d}{dx}\left(\frac{x}{1-x}\right) = \frac{1}{(1-x)^2}$$

donde la segunda igualdad es justificable (aunque yo no lo hago como no lo haría Euler, y me lo creo).

Siendo así, tenemos que $E(X_i) = \frac{6}{i}$, y por tanto la solución es

$$E = \sum_{i=1}^{6} E(X_i) = 6\sum_{i=1}^{6}\frac{1}{i} = 14,7$$

tiradas.

De la misma forma, si el dado es de n caras, de media tendré que tirar $v(n) = n\sum_{i=1}^{n}\frac{1}{i}$ veces. Por curiosidad:

$v(6) = 14,7$
$v(20) \approx 72$
$v(100) \approx 518$
$v(1000) \approx 7485$.

3. Las agujas de las horas y de los minutos de un reloj son indistinguibles. ¿Cuántos momentos hay en el día en que no sepamos qué hora es mirando este reloj?

Aceptamos que las agujas se mueven de forma continua. Establecemos primero una correspondencia entre la posición de una aguja y la circunferencia unidad U del plano complejo, de forma que a una aguja que apunta a las 12 le corresponde $\theta = 0$, a las 3 le corresponde $\theta = \frac{\pi}{2}$, a las 11 $\theta = \frac{11\pi}{6}$, etc.

Es claro que en un reloj normal, si la aguja de las horas está a un ángulo θ de las 12 en sentido de avance, la de los minutos ha de estar a un ángulo 12θ (convénzase el lector con un par de ejemplos). Luego la aplicación que a la posición de la aguja de las horas le asigna la correspondiente de los minutos será $a : U \longrightarrow U$ tal que $a(z) = z^{12}$, es decir, $a(e^{i\theta}) = a^{i12\theta}$.

Una aguja de las horas en posición "confusa" z_0 cumplirá que su correspondiente de los minutos, z_0^{12}, la volverá a tener a ella como correspondiente, es decir, $(z_0^{12})^{12} = z_0$. Luego hemos de encontrar las soluciones de esta última ecuación, excluyendo aquellos z cuyo correspondiente sea sí mismo (por ejemplo, a las 12 en punto no hay confusión), esto es, aquellos z tales que $z_0^{12} = z_0$. Así, buscamos soluciones de

$$\frac{z^{144} - z}{z^{12} - z} = 0.$$

El denominador comparte todas las raíces con el numerador, y por tanto obtenemos $144 - 12 = 132$ soluciones distintas, por lo que habrá 264 momentos en el día (24 horas) en que no sabremos qué hora es.

Manuel López Sheriff

Agradecimientos

No podemos dejar esta sección sin volver a agradecer a quien permite que la revista subsista económicamente: la asociación Lewis Carroll y DECIDE Soluciones.

Y tampoco podemos pasar sin agradecer a toda la gente que la hace posible mediante su trabajo: todos los que habéis colaborado con material de cualquier tipo, en especial los que han decidido en este último número empezar a trabajar con **Matgazine**. Por ello, damos la bienvenida a Irene de Parada, Dawe, Eva Elduque, Jorge Guijarro y David Gigosos. Además, os damos las gracias a los que aún no os habéis animado a escribirnos nada pero habéis corregido todo lo que os hemos echado. Aquí se lleva la palma Laura del Moral, que no duda un instante en revisar cuanto le pidamos.

La ayuda nos ha llegado de muy distintas formas: Ana Rosa Luna y Jaime Mendizábal vendieron muchísimos ejemplares del número 2, y dos profesores de la Complutense nos han ayudado especialmente. Primero, José Manuel Gamboa nos ha puesto en contacto con nuestra nueva imprenta. Y después, Jesús Ruiz se ha tomado trabajo y mucho tiempo para enseñarnos LaTeX y ayudarnos a mejorar enormemente la presentación de **Matgazine**. Ahora, gracias a la nueva plantilla, quien nos releve a cargo de la revista lo tendrá mucho más fácil, al menos con la presentación.

También queremos agradecer a los ponentes del ciclo de conferencias de lógica, a Vicente Muñoz por ayudar a traer a Javier Fresán, a Violeta de Lama por ayudar con el curso, a Pedro Ángel Castillejo de nuevo por organizarlo, y por último a los que vinisteis al curso introductorio de LaTeX que organizamos en la Universidad Complutense, con la colaboración de Fernando Cortina y Miguel Ambrona como profesores. Esperamos que os haya gustado y que, además de usarlo para hacer vuestros trabajos y apuntes de la facultad y del futuro, os planteéis escribir algo para la revista sobre algún tema matemático que os resulte interesante.

Y por último y por supuesto, queremos agradecerte a ti, lector, por acompañarnos otro número más.

A todos,

¡Gracias!

El equipo Matgazine