ACADEMIA ASTURIANA DE CIENCIA E INGENIERÍA

PASEO POR EL ALGEBRA: DE LAS ESTRUCTURAS ALGEBRAICAS A LAS APLICACIONES EN CRIPTOGRAFÍA

DISCURSO PRESENTADO EN EL ACTO DE SU INCORPORACIÓN COMO ACADÉMICA DE NÚMERO POR LA

PROF. CONSUELO MARTÍNEZ LÓPEZ

Y CONTESTACIÓN DE LA

ILMA. SRA. ROSA MENÉNDEZ LÓPEZ

Académica de número de la Academia Asturiana
de Ciencia e Ingeniería

EL DÍA 17 DE ENERO DE 2025

c/ San Francisco. Edificio Histórico - Universidad de Oviedo
OVIEDO

ISBN: 978-84-09-67240-0
D.L.: AS 02874-2024

Imprime: Cízero Digital

PASEO POR EL ÁLGEBRA: DE LAS ESTRUCTURAS ALGEBRAICAS A LAS APLICACIONES EN CRIPTOGRAFÍA

DISCURSO DE INGRESO DE LA

PROF. CONSUELO MARTÍNEZ LÓPEZ

AACI
ACADEMIA ASTURIANA
DE CIENCIA E INGENIERIA

DEDICATORIA

A Carlota, con el deseo de que pueda vivir en un mundo con más libertad, en el que ninguna mujer se vea privada de su voz y sus derechos, un mundo más justo y solidario.

Agradecimientos

Quiero empezar con unas palabras de reconocimiento y agradecimiento.

En primer lugar, a la familia en la que tuve la suerte de nacer y criarme, con unos padres que nos educaron, a mis hermanos y a mí, en valores y en libertad, abriendo un mundo de posibilidades limitado únicamente por nuestras capacidades y no por condicionantes de género, creando un ambiente de libertad de expresión en el que se podían manifestar, con respeto al resto, las opiniones de cada uno, plantear dudas o mostrar discrepancias. ¡Y hacer preguntas! A Santos, que siempre ha entendido y apoyado mi dedicación profesional y que es muy consciente de la importancia que tiene para mí la ciencia, en general, y las matemáticas en particular. Y a David, nuestro hijo, que siempre ha aceptado, con ironía incluso, que no tiene una madre "al uso" y aunque eso le ha generado algunos problemas, al final, le ha permitido disfrutar de unas interesantes experiencias vitales.

Gracias a todos mis colegas de la Academia Asturiana de Ciencias e Ingeniería, dirigida por Mario Díaz, a quien debemos, sin duda, la existencia de la Academia. El ambiente de colaboración creado y las cualidades de sus integrantes hacen que sea un privilegio y un regalo pertenecer a ella.

Gracias a todos los que, de un modo u otro, han compartido una parte de mi camino profesional, como "maestros" en el sentido más hermoso de la palabra, enseñándome con su ejemplo, ¿cómo si no?, la seriedad en el trabajo, la preocupación por hacer las cosas bien y la profesionalidad. Y gracias también a los que me permitieron identificar aquello que yo no quería hacer. Y gracias a los alumnos que han jalonado mi trayectoria. Cada año académico, aprendo algo nuevo de ellos. En particular, gracias a los distintos alumnos que han trabajado conmigo como doctorandos, muchos de ellos entrañables colegas en la actualidad. El flujo de la relación entre "alumnos" y "maestros", en ambas direcciones es de una increíble riqueza, aunque no se perciba de forma inmediata.

Gracias a todos mis colaboradores en la investigación. La posibilidad de trabajar, compartir ideas, explorar nuevos caminos, con gente de distintos países y culturas es una de los mayores atractivos de nuestra actividad investigadora.

Y gracias a todos los amigos que han venido a acompañarnos y a compartir este momento con nosotros.

ÍNDICE

1. Algo de historia

Soy consciente de que me dedico a un campo de trabajo, dentro de las matemáticas, que es poco conocido para el gran público y cuyo nombre genera temores, debido a la sensación de moverse en un terreno pantanoso, con teorías abstractas y complicadas que no se sabe muy bien qué objetivo tienen.

Por ello, mi propósito ha sido diseñar un recorrido histórico sobre este fascinante campo de trabajo, que me sedujo desde el primer momento, realizando un viaje a través del Álgebra, que nos permita apreciar su interés y su belleza, y ponga de relieve su increíble evolución y mi modesta contribución. Espero que al final de nuestro trayecto, el álgebra se haya convertido en algo más cercano y familiar. Se teme, especialmente, lo que no se conoce.

El origen de la palabra Álgebra, como sucede con muchas palabras en nuestra lengua que empiezan por el prefijo "al", es árabe. En efecto hay tres figuras relevantes, pertenecientes al mundo árabe, que aparecen ligadas al comienzo de la historia del álgebra: Tabit ben Qurro, Omar Khayyam y Al-Khwarizmi.

Pero nos concentraremos en el último de ellos, de cuyo nombre se deriva también la palabra "algoritmo", tan usada actualmente, principalmente por el auge de la informática y la Inteligencia Artificial.

Al-Khwarizmi presenta contribuciones variadas en distintos temas: contribuciones matemáticas, un calendario y su tratado de Álgebra. Se considera que fue el primer autor islámico que escribió sobre las soluciones de los problemas de al-jabr y al-muqabala en una ecuación. Al-jabr denota el proceso de sumar cantidades iguales en los términos de una ecuación para eliminar coeficientes negativos o bien multiplicar en ambos lados por la misma cantidad para eliminar fracciones. Este proceso al-jabr (que se traduce habitualmente por reducción) da nombre a la disciplina que nos ocupa: Álgebra.

Al-muqabala se refiere al proceso de eliminar términos en una ecuación para transformarla en otra más simple.

Por tanto, como escribió Al-Khwarizmi, el objetivo inicial del Álgebra era la búsqueda de soluciones de ecuaciones, realizando transformaciones sucesivas que permitieran pasar de la ecuación inicial a otra, con las mismas soluciones, y con un aspecto "más amistoso".

Es importante notar que se conoce como teorema fundamental del Álgebra al siguiente resultado probado por Gauss:

"Todo polinomio con coeficientes reales se factoriza como producto de factores lineales o cuadráticos."

Es decir, el álgebra se desarrolla de modo ligado a los polinomios y a las soluciones de ecuaciones polinómicas. Este hecho explica porqué el problema de la resolución de ecuaciones por radicales, que comentaremos más adelante, fue un problema central durante siglos.

Creo que es importante llamar la atención sobre la importancia del lenguaje matemático. Las matemáticas, en general, y el álgebra, en particular, tienen un lenguaje propio y preciso, que se traduce en una notación específica al escribir.

Podemos ilustrar esta afirmación con un ejemplo. Podemos leer en un texto antiguo: "Hallar un cuadrado que es igual a cuarenta cosas menos cuatro cuadrados". La notación actual sería:

$$\textit{Resolver la ecuación} \quad X^2 = 40X - 4X^2.$$

Todos estaremos de acuerdo en que el lenguaje matemático es mucho más conciso y preciso. Pero ¡hay que acostumbrarse y familiarizarse con él!

Al-Khwarizmi encontró las soluciones de las ecuaciones de segundo grado, estudiando, de forma separada, seis tipos de ecuaciones para manejar únicamente coeficientes y soluciones positivas. Utilizó construcciones geométricas para justificar la resolución, siguiendo métodos similares a los desarrollados por los babilonios varios siglos antes.

El estudio de las ecuaciones, en particular de las cúbicas, continuó durante la edad Media, llegando a ser un tema de alto interés entre los matemáticos italianos del Renacimiento.

Hay un alto número de matemáticos italianos, bien conocidos y con importantes contribuciones en las matemáticas y en particular en Álgebra: Leonardo de Pisa (conocido como Fibonacci), Luca Pacioli, Scipione del Fierro, Cardano, … Estos matemáticos conocían los métodos de al-jabr y al-muqabala que hemos comentado anteriormente.

Merece la pena señalar que la matemática italiana se vio influenciada por el cambio experimentado en el comercio. Durante la Edad Media, el comercio consistía, esencialmente, en un intercambio de mercancías realizado por mercaderes que se desplazaban para visitar a potenciales clientes y que tenían en su cabeza toda la información que necesitaban. A partir del siglo XIII, se perfecciona la navegación, lo que permite desplazarse a lugares más lejanos y la economía europea se transforma por la creciente circulación de monedas. Entran en escena los banqueros, se empiezan a usar letras de cambio y aparece una economía internacional. La mayoría de los grupos comerciales tenían centros en ciudades italianas como Florencia. Surge

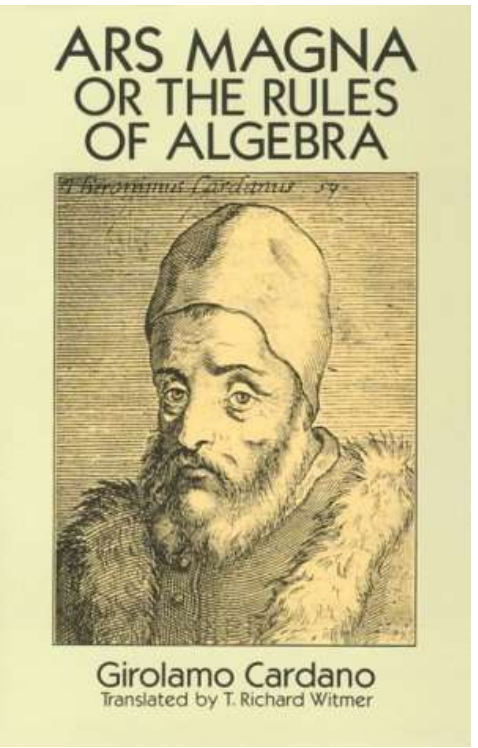
así la necesidad de calcular precios, garantizar los pagos y hacer previsiones de pérdidas y ganancias.

Se precisaba un sistema de numeración eficiente para operar, por lo que el sistema de numeración romano es sustituido por el indo-arábico (actual) y aparecen los "*abacistas*", precursores de los actuales contables. Notemos que *abacus*, en latín, denota el dispositivo utilizado para calcular, mientras que la palabra italiana "*abbaco*" significa *aritmética práctica*.

Aunque Leonardo de Pisa nació en esta localidad, durante su infancia y adolescencia, vivió en Argelia, dónde su padre trabajaba como comerciante. Allí se familiarizó con las operaciones con números indo-arábicos. A su regreso a Italia se centró en temas matemáticos y, en particular, en el estudio de soluciones de ecuaciones cúbicas. Escribió varios trabajos, algunos de los cuales han sobrevivido hasta nuestros días (como el Liber Abacci). La conocida sucesión de Fibonacci:

$$0,1,1,2,3,5,8, \ldots.$$

cuyos dos primeros términos son 0 y 1 y, a partir del tercero, cada término es la suma de los dos precedentes, le debe su nombre, ya que el apodo de Leonardo de Pisa era *Fibonacci*.



Portada de la traducción al inglés del Ars Magna

Finalmente, la solución de las ecuaciones cúbicas (de grado 3) se debe a los matemáticos italianos: Scipione del Fierro, Tartaglia y Cardano y aparece explicada en la célebre "Ars Magna" del último autor.

Ferrari empezó, con 14 años, siendo sirviente de Cardano y llegó a ser un brillante matemático, amigo y secretario suyo. A Ferrari se debe el método que permite reducir cualquier ecuación de grado 4 a una ecuación de grado 3 y, por tanto, resolverla.

Varios matemáticos brillantes, como Abel, se enfrentaron al reto de resolver las ecuaciones de grado 5. Finalmente, Abel probó que la ecuación de grado 5 no se podía resolver. Pero la respuesta no era suficientemente satisfactoria para los matemáticos. ¿Es el grado 5 singular? ¿Cuál es la razón de que no se pueda resolver? ¿Qué ocurre con los grados superiores?

Se considera que el álgebra moderna empieza con Galois, si bien hay varios matemáticos que pueden considerarse precursores suyos y que han tenido también un papel muy importante en el diseño de esta nueva disciplina como Waring, Vandermonde, Ruffini, Cauchy, … Y fundamentalmente, Lagrange, Abel y Gauss.

Evariste Galois

Galois cierra el problema de la resolución de ecuaciones algebraicas e inicia una nueva era para esta disciplina. Galois está rodeado de un halo de misterio, inconformismo y romanticismo. Su muerte, antes de cumplir los 21 años, en un duelo y el hecho de haber obtenido unos resultados sorprendentes que modificaron totalmente la fisonomía del álgebra, le han convertido en un mito que atrae muchísima atención. Se

han escrito muchos libros sobre Galois, pero yo creo que sabemos muy poco sobre él, salvo que fue un revolucionario, nada convencional, e indudablemente un genio, capaz de cerrar un problema milenario usando conexiones matemáticas que nadie antes había imaginado. Y además nos legó un valiosísimo regalo, *los cuerpos finitos*, que se llaman cuerpos de Galois en su honor.

2. Estructuras algebraicas

Independientemente de cuándo fechemos el nacimiento del álgebra moderna, con Galois o antes de él, creo que la idea general entre los algebristas es que la estructura actual del álgebra se debe fundamentalmente a Emmy Noether. En mi opinión, las estructuras algebraicas son el corazón del Álgebra actual. Noether estudió y relacionó distintas estructuras algebraicas y le debemos el formalismo actual de esta disciplina. No puedo ocultar mi inmensa admiración por una de las mentes matemáticas más brillantes de la historia. Su contribución y su legado no se restringen al álgebra, sino que alcanzan a la física.

Consiguió relacionar las simetrías de la acción de un sistema físico con sus leyes de conservación, resolviendo así un problema que preocupaba a Einstein. En palabras del físico Fez Gursey:

"*La clave de la relación entre las leyes de simetría y las leyes de conservación en física está en el celebrado teorema de Emmy Noether que asegura que un sistema dinámico descrito por una acción bajo un grupo de Lie con n parámetros admite n invariantes (cantidades conservadas) que permanecen constantes durante la evolución del sistema*."

No es extraño que E. Noether se ganara el respeto y la admiración no solo de Einstein, que la consideraba el mayor genio matemático desde que comenzó la educación universitaria para mujeres, sino también de matemáticos de la talla de Félix Klein o David Hilbert. Notemos que Emmy Noether ingresó en la Universidad de Erlangen el año 1904, primer año que se admitieron mujeres en dicha universidad.

El algebrista e historiador de las matemáticas, van der Warden, dice, en alusión a la contribución de Emmy Noether, que su esencia está reflejada por la siguiente máxima:

"*Todas las relaciones entre números, funciones y operaciones llegan a ser claras, susceptibles de generalización y fructíferas cuando se separan de ejemplos específicos y se buscan las conexiones conceptuales entre ellas.*"

Pero ¿cómo encajan las estructuras algebraicas con el hecho de que, en sus inicios, se considerara que el objetivo fundamental del álgebra era la resolución de ecuaciones algebraicas? ¿Como se llega al papel que tienen las estructuras algebraicas en el contexto actual?

Emmy Noether

Empecemos por entender lo que son las estructuras. Pensemos en el conjunto de enteros con la suma y el conjunto de racionales no nulos con el producto. Si analizamos su comportamiento nos damos cuenta de que comparten todas las

propiedades esenciales. En ambos casos tenemos definidas operaciones, en los correspondientes conjuntos, que son conmutativas, asociativas (no necesitamos usar paréntesis) y en ambos casos hay un elemento distinguido (el 0 y el 1 respectivamente) que cumple que al operar cualquier otro con él recuperamos el elemento inicial (lo llamamos elemento neutro) y para cada elemento hay otro (que llamaremos su inverso) que al operarlo con el primero da como resultado el neutro (para cada entero hay otro que sumado con él nos da 0 y para cada racional no nulo hay otro que multiplicado por el primero nos da el 1). Por tanto, los enteros con la suma y los racionales no nulos con el producto tienen la misma estructura. Ambos son ejemplos de grupos (conmutativos o abelianos, en honor de Abel). Al estudiar grupos abelianos, en general, incluimos las propiedades de todos los conjuntos, numéricos o no, con una operación que replica las propiedades de los enteros con la suma. Si olvidamos la conmutatividad obtenemos un grupo: las permutaciones de un conjunto finito, los movimientos que fijan un cubo, los movimientos del plano afín euclídeo.

Una estructura no es más que un conjunto con una o varias operaciones (internas o externas) que satisfacen una serie de propiedades. Los grupos son la estructura que nos permite estudiar, matemáticamente, la noción de simetría (en el mundo animal, en las partículas físicas, en configuraciones de compuestos químicos, en cristales etc.). De ahí su importancia.

Simetría en el mundo mineral

Estructuras importantes con dos operaciones son los anillos, que cumplen las mismas propiedades que los enteros con la suma y el producto. Notemos que en el conjunto de enteros podemos sumar, restar (aplicando el inverso) y multiplicar, pero no podemos dividir. Si queremos incluir la posibilidad de dividir, necesitamos considerar un cuerpo, otra estructura con dos operaciones. Es la estructura que forman los racionales (o los reales) con la suma y el producto. Los cuerpos forman parte de la estructura de espacio vectorial, por ello juegan un papel esencial en álgebra lineal, una de las partes del álgebra que aparece, como herramienta importante, en todas las ramas de las matemáticas.

A veces se considera que Galois introdujo los grupos, pero en realidad los grupos ya aparecen en trabajos previos de otros matemáticos anteriores, como Lagrange, Ruffini o Cauchy, y lo hacen esencialmente como grupos de transformaciones. Pero el nombre de "grupo" se debe a Galois. De hecho, Galois estudió en profundidad las estructuras de grupos y cuerpos. Es clara la razón de su interés en los grupos al relacionarlos con las ecuaciones, pero no conocemos los motivos que le llevaron a la construcción de los cuerpos finitos.

Intentemos volver a mirar, con los ojos de Galois, el problema que dio nombre a nuestra disciplina.

Los matemáticos griegos, los musulmanes o los italianos del Renacimiento habían tratado de encontrar soluciones a ecuaciones concretas, empezando por las de grado 2 y parando ante el muro que representaron las ecuaciones de grado 5.

Todos hemos aprendido en la escuela que las raíces de una ecuación cuadrática:

$$a\,X^2 + b\,X + c = 0$$

vienen dadas por:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Galois replanteó el problema del siguiente modo: Dada una ecuación algebraica de grado n ¿existe una fórmula que permita encontrar las soluciones de una ecuación en función de sus coeficientes e involucrando sumas y restas, multiplicaciones y divisiones y extracción de raíces?

Hoy, gracias a Galois, sabemos que tal fórmula existe para las ecuaciones de grado 2, 3 y 4, pero no para las de grado mayor o igual a 5. Notemos que esto no significa que no podamos encontrar una fórmula para algunas ecuaciones concretas de grado 5, pero siempre habrá ecuaciones de grado 5 para las cuales esa fórmula no valga.

La idea genial de Galois fue asociar a cada ecuación un grupo (esencialmente un grupo de permutaciones de sus raíces) y demostrar que existe una fórmula para expresar

las raíces en función de los coeficientes, como se ha indicado anteriormente, si y solo si el grupo asociado a la ecuación es un grupo resoluble.

Los grupos conmutativos son resolubles y, de modo intuitivo e informal, un grupo resoluble es un grupo que se puede construir a trozos usando grupos conmutativos. Sabemos que para cada n, existen ecuaciones de grado n que tienen como grupo asociado el grupo de permutaciones de n elementos (grupo simétrico de grado n, S_n) y el grupo S_n es resoluble solo si $n < 5$.

Por tanto, la respuesta de Galois pone en primera línea a las estructuras y deja clara su importancia. Se traduce un problema, formulado en términos de ecuaciones algebraicas y sus soluciones, a un problema de teoría de grupos. Pero los cuerpos siguen jugando un papel importante, puesto que los coeficientes de los polinomios se consideran dentro de un cuerpo para poder realizar con ellos las operaciones indicadas. Y para poder hallar las raíces de una ecuación polinomial, construimos un cuerpo más grande, si hace falta, como se construyeron los complejos, a partir de los números reales, para conseguir que la ecuación $X^2 + 1 = 0$ tuviera soluciones.

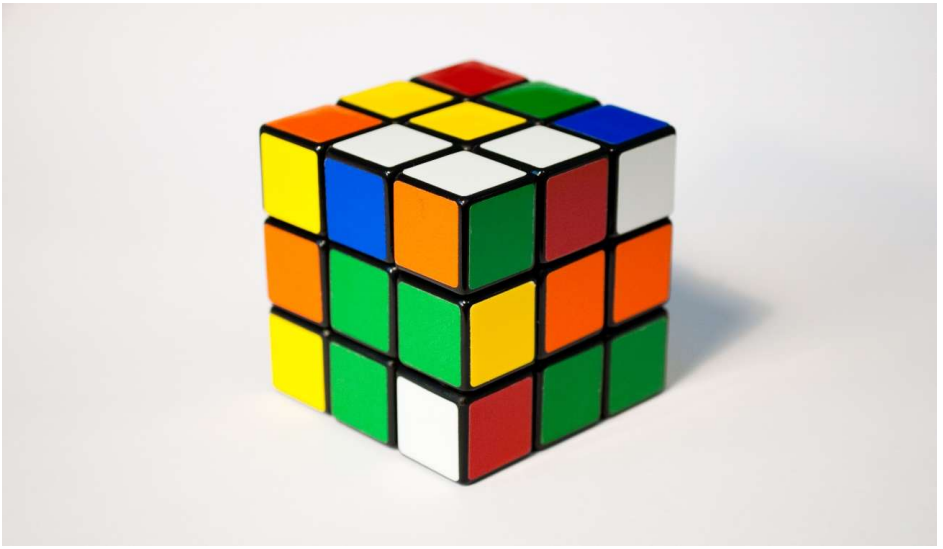
3. Grupos y Álgebras

Mi flechazo con el álgebra se produjo en el tercer curso de carrera, gracias a una profesora, Maria Jesús Iranzo, excelente profesional y apasionada por su trabajo. Como la mayoría de los miembros del Departamento de Álgebra de la Universidad de Zaragoza, su área de trabajo era la teoría de grupos, a la que se dedicó hasta su jubilación en la Universidad de Valencia, a la que se trasladó antes de que yo terminara mis estudios. Por tanto, resultó bastante natural que el tema de mi tesis doctoral fuera de teoría de grupos, en mi caso grupos infinitos, realizada bajo la dirección de Javier Otal.

Podemos decir que la disciplina de álgebra, que hasta el siglo dieciocho era el estudio de soluciones de ecuaciones polinómicas, pasó a ser, en el siglo XX, el estudio de sistemas axiomáticos abstractos. La transición se produce a lo largo del siglo XIX, cuando van apareciendo las distintas estructuras: grupos, anillos (conmutativos y no conmutativos), cuerpos, espacios vectoriales, … Los grupos y los cuerpos juegan el papel esencial en la teoría de Galois; en teoría algebraica de números aparecen los anillos conmutativos y los cuerpos; en la teoría de representaciones de grupos se utilizan grupos, álgebra lineal y álgebras no conmutativas. El álgebra se convierte en un organismo, cuyas partes están conectadas y en continua evolución. Y su corazón lo forman las estructuras algebraicas. En este proceso de formalización y abstracción el papel de E. Noether ha sido crucial. Es natural que I. Kaplansky la llamara "*la madre del álgebra*".

3.1 – Grupos

Antes de 1870 solo se consideraban dos tipos de grupos: grupos de permutaciones (o de sustituciones, en la terminología de la época) y grupos de transformaciones geométricas. En 1870 aparece el tratado de Camille Jordan sobre grupos y se empiezan a suceder importantes cambios. La noción de grupo abstracto empieza a tomar forma, gracias a Kronecker, Cayley y Weber fundamentalmente. Se debe a Kronecker la definición moderna de grupo, por medio de axiomas, para el caso de grupo abelianos y a Weber en el caso general, primero para grupos finitos y luego para grupos infinitos. Casi al mismo tiempo, Walter von Dyck dio también una definición formal de grupo, diferente a la dada por Weber, pero equivalente. Una vez introducida esta noción, el problema de estudiar la estructura de los grupos, independientemente del modo en que se representen, se convirtió en el problema central de la teoría.



La resolución del cubo de Rubik se basa en teoría de grupos

El desarrollo de las geometrías no euclídeas también está ligado a la teoría de grupos. F. Klein escribió dos artículos esenciales. En el segundo de ellos, ya habla de grupo de transformaciones de la geometría. Si consideramos un grupo diferente de transformaciones cambiamos de una geometría a otra: geometría afín, geometría euclídea, geometría parabólica, geometría hiperbólica. En esta idea se sustenta el famoso "Programa de Erlangen", que defiende que cada tipo de geometría estudia las propiedades que son invariantes bajo el grupo de transformaciones considerado, por

tanto, lo importante no son ya los objetos geométricos, sino el grupo concreto de transformaciones que interesa y las propiedades que deja invariantes dicho grupo.

F. Klein fue contemporáneo de Sophus Lie y parece que llegaron a ser muy buenos amigos. Su relación tuvo una influencia muy positiva en el desarrollo de la teoría de grupos continuos. Más tarde, sus investigaciones siguieron caminos diferentes. Klein consiguió clasificar los grupos finitos de rotaciones euclídeas, mientras que S. Lie desarrolló una teoría de integración de ecuaciones diferenciales, lo que le llevó a considerar grupos de transformaciones que dejan invariante una ecuación diferencial y a ser el padre de la teoría de grupos de Lie.

A diferencia de lo que ocurre en cuerpos finitos, donde sabemos que todo cuerpo finito tiene un número de elementos que es necesariamente una potencia de un primo (no hay cuerpos de 6 o de 20 elementos) y para cada potencia de primo hay esencialmente un cuerpo con ese número de elementos, cuerpo que sabemos cómo representar y cómo operar con sus elementos, la situación en grupos finitos no abelianos es totalmente diferente. Para grupos abelianos la teoría se conoce perfectamente. Podemos saber cuántos grupos abelianos hay conteniendo una cantidad fija (y arbitraria) n de elementos. Además, si nos dan dos grupos abelianos con el mismo número de elementos n, podemos saber si son dos versiones del mismo grupo o corresponden a grupos distintos. Y el proceso para llegar a la respuesta es perfectamente conocido. Pero ni la forma de trabajar ni los resultados conocidos para grupos abelianos finitos son exportables a grupos cualesquiera. Y los métodos de trabajo que se utilizan en grupos finitos tampoco dan los frutos deseados en grupos infinitos. Pronto se vio que el problema de clasificar grupos finitos era un problema de una magnitud inabordable, por lo que la investigación se centró en distintas clases de grupos.

Podemos señalar las 4 fases que han marcado la evolución de la teoría de grupos.

- En el álgebra clásica, podemos considerar que los grupos deben su aparición a Lagrange (1780).
- En 1801 Gauss escribe su libro Disquisitions Arithmeticae, donde unifica todo lo conocido anteriormente relativo a teoría de números. Se puede considerar que aquí se inicia el estudio de los grupos abelianos, aunque sin usar terminología de teoría de grupos
- Con el programa de Erlangen, desarrollado por Klein cien años después del trabajo de Lagrange sobre grupos de permutaciones (de las raíces de una ecuación polinómica) y ochenta años después de que Gauss iniciase la teoría de los grupos abelianos, pone de relieve la importancia de la Geometría en la evolución de la teoría de grupos.

- El análisis influyó también. En 1874 Lie introdujo su teoría general de grupos de transformaciones continuas, hoy denominados grupos de Lie. El objetivo de Lie era continuar el trabajo de Abel y Galois, pero usando ecuaciones diferenciales en lugar de ecuaciones algebraicas.

Por tanto, vemos cómo, a lo largo de la historia, van apareciendo distintos tipos de grupos. Inicialmente grupos de permutaciones, luego grupos abelianos, grupos de transformaciones geométricas o grupos de Lie. Es decir, al principio aparecen ejemplos concretos de grupos y la abstracción del concepto de grupo se va abriendo paso lentamente. Una vez que Cayley dio la definición abstracta de grupo se produjo una explosión en el estudio de esta estructura. ¿Qué necesitamos para tener un grupo? Simplemente un conjunto G no vacío y una ley de composición interna (operación del grupo),

$$G \times G \rightarrow G, \qquad (a, b) \rightarrow ab.$$

Además, la operación interna tiene que cumplir tres condiciones:

Asociativa, es decir, $(ab)c = a(bc)$ para elementos cualesquiera a, b, c de G,

Existe *elemento neutro* "1" que cumple $a1 = 1a = a$ para cualquier a en G,

Para cada elemento a en G existe un (único) elemento (su *inverso*) a^{-1} cumpliendo que $a\, a^{-1} = 1 = a^{-1}\, a$. ¡Eso es todo!

3.2 – Álgebras

En este párrafo solo consideramos álgebras asociativas, por lo que álgebra se considera como sinónimo de álgebra asociativa.

Euler conocía la representación en el plano de los números complejos, pero no llegó a dar una construcción explícita de las operaciones de suma y producto de números complejos, siendo Wessel, Argand, Warren y Gauss los que lo hicieron. Además, el nombre *números complejos* se debe a Gauss.

Un poco más tarde, Willian Rowan Hamilton definió los números complejos como pares de números reales, con las correspondientes operaciones de suma y multiplicación. Este hecho le llevó a considerar cuaternas de números reales y a la definición de sumas y productos de cuaternas. Así llegó a construir una estructura, el álgebra de los cuaternios, que ha tenido una gran importancia y aplicaciones en geometría y física, entre otras.

La estructura de álgebra aglutina varias estructuras de "forma armoniosa". Si F es un cuerpo, un álgebra sobre F (o F-álgebra) asociativa $\boldsymbol{a}$ es un F-espacio vectorial (por tanto, tiene una operación suma + cumpliendo que $(\boldsymbol{a}, +)$ es un grupo abeliano) y tiene un producto asociativo de elementos, que es distributivo respecto de la suma y permite intercambiar posición con los elementos del cuerpo. El ejemplo más sencillo de álgebra sobre un cuerpo lo forman las matrices cuadradas de tamaño n sobre el cuerpo F con la suma y el producto usual de matrices.

La teoría de grupos abstractos y la de álgebras asociativas se desarrollaron en paralelo. El problema de clasificar grupos finitos se corresponde con el problema de clasificar álgebras asociativas de dimensión finita. En mi opinión se estableció una simbiosis entre ambas estructuras que favoreció a las dos. Los problemas y técnicas en cada una de estas estructuras inspiraron problemas y métodos de trabajo en la otra, generando una actividad impresionante a lo largo del siglo XX, que continúa su expansión en lo que llevamos del nuevo siglo.

Pero revisemos, muy rápidamente, la historia, más joven y desconocida, de la teoría de álgebras.

En 1870 Benjamin Pierce defendió en Washington, en la National Academy of Sciences, la memoria de título "*Linear Associative Algebras*". En dicha memoria introduce la noción de elemento idempotente ($e^2 = e$) y elemento nilpotente ($e^n = 0$ para algún $n > 1$). La existencia de un elemento idempotente en el álgebra permite obtener una descomposición (llamada actualmente descomposición de Peirce) que ha sido una herramienta de gran importancia en el estudio de las álgebras.

El primero en desarrollar una teoría general de álgebras sobre cuerpos arbitrarios fue Maclagan Wedderburn que usó la noción de radical (nilpotente) del álgebra $\boldsymbol{a}$ (el mayor ideal nilpotente del álgebra) para probar el (hoy conocido como) Teorema Principal de Wedderburn: Toda álgebra se descompone como suma de su radical y una subálgebra semisimple (con radical nulo). Toda álgebra semisimple se expresa, de forma única como suma de álgebras simples (álgebras sin ideales no triviales). Toda álgebra simple es un álgebra de matrices sobre un álgebra de división.

Emil Artin extendió el Teorema principal de Wedderburn a anillos que satisfacen la condición de cadena descendente sobre ideales a izquierda (o a derecha).

Las condiciones de cadena ascendente fueron introducidas por E. Noether que, junto con sus alumnos, estudió una nueva definición de radical, como la unión de todos los nilideales (cuyos elementos son todos nilpotentes), con la que pudieron extender el teorema de Wedderburn a anillos más generales que los considerados por E. Artin.

Sin embargo, no lograron desarrollar una teoría de estructura satisfactoria para anillos sin condiciones de finitud. Natan Jacobson consiguió hacerlo en dos trabajos publicados en 1943. En ellos define una nueva noción de radical para anillos arbitrarios, a través de la noción de módulo y representación. El radical de Jacobson resulta ser la intersección de los núcleos de las representaciones irreducibles del anillo. Además, admite una caracterización en términos de ideales a derecha modulares. Con este nuevo radical se puede recuperar el teorema de Wedderburn para anillos cualesquiera, tomando como anillos semisimples aquellos cuyo radical de Jacobson es trivial.

A lo largo del siglo XX la investigación en grupos y álgebras no solo se ha desarrollado en paralelo, sino que se han realimentado: ideas y problemas relacionados con una estructura han inspirado problemas similares en la otra. Y, en muchas ocasiones, la solución de un problema concreto en una estructura ha venido de la mano de un resultado de la otra estructura.

Para explicar con más claridad lo indicado anteriormente y entender lo que quiero decir cuando hablo de una "*simbiosis de grupos y álgebras*", vamos a ver en detalle un ejemplo concreto y muy importante.

Bunside fue un matemático inglés que se interesó, de modo especial, por el estudio de los grupos infinitos. Sus resultados y las preguntas planteadas por Burnside marcaron la actividad en álgebra en el siglo XX. En particular, se planteó la cuestión de qué condiciones hacen un grupo finito. Es claro que un grupo finito es finitamente generado, es decir, todos los elementos del grupo se pueden expresar utilizando un número finito de elementos y operaciones entre ellos. Además, para cada elemento a del grupo hay un menor entero positivo n tal que al multiplicar a consigo mismo n veces recuperamos el elemento neutro. Dicho n se llama orden del elemento a.

Por tanto, un grupo finito es finitamente generado y todos sus elementos tienen orden finito. Burnside se preguntó por el resultado recíproco, lo que se conoce como problema general de Burnside.

Este problema se resistió mucho tiempo a todos los intentos de encontrar una respuesta, pero estimuló notablemente la investigación en teoría de grupos. Y no solo en teoría de grupos, sino también en teoría de álgebras. Por ello, el propio Burnside planteó una versión más débil. Este nuevo problema, denominado problema ordinario de Burnside, considera grupos finitamente generados con exponente finito m, es decir, los órdenes de los elementos del grupo están acotados y se pregunta, como en el problema anterior, si las dos condiciones indicadas, ser finitamente generado y tener exponente finito garantizan la finitud del grupo.

William Burnside, 1852-1927

Es claro que la respuesta es afirmativa si el exponente es 2, porque en ese caso el grupo es abeliano (¡algo que saben los alumnos de matemáticas desde segundo de carrera!). El caso de exponente 3 fue demostrado por el propio Burnside. Sanov lo probó para exponente 4. Y M. Hall lo hizo para exponente 6. No se conoce ningún otro valor de m para el que se pueda asegurar que todo grupo finitamente generado con ese exponente es finito.

Pronto aparecieron problemas en teoría de álgebras y de anillos que representan el análogo de los problemas de Burnside y que fueron planteados, independientemente, a mediados del siglo XX por Alexander Kurosh y Jacob Levitsky. Los elementos de orden finito en grupos son sustituidos por elementos nilpotentes en el caso de anillos y por elementos algebraicos (raíces de polinomios) en el caso de álgebras. Recordemos que un elemento a de un anillo R se dice nilpotente si existe un número natural n mayor que 1 cumpliendo $a^n = 0$. Si todos los elementos del anillo son nilpotentes, el anillo se dice *nil*. El anillo es *nilpotente*, con índice de nilpotencia n si cualquier producto de n elementos del anillo es 0.

El problema general de Kurosh-Levistsky plantea si un anillo nil y finitamente generado es nilpotente. La versión de álgebras sería: ¿Es finito dimensional un álgebra algebraica (todos sus elementos son algebraicas) finitamente generada?

Del mismo modo que en grupos, se debilitaron las condiciones en el problema general para plantear los correspondientes problemas ordinarios de Kurosh-Levitsky:

- ¿Es nilpotente un anillo finitamente generado y nil, con el índice de nilpotencia de sus elementos acotado superiormente?
- ¿Es finito dimensional un álgebra algebraica finitamente generada si existe un numero natural n tal que todos sus elementos son raíces de un polinomio de grado a lo sumo n?

No solo se produjo un flujo de ideas entre los investigadores de ambos problemas, sino que finalmente resultaron estar relacionados y la respuesta, negativa, al primer problema planteado por Burnside vino de la mano de las álgebras. N. Jacobson, ya mencionado anteriormente, fue quien tendió el puente que permitió circular entre los dos tipos de estructuras y los correspondientes problemas. Jacobson probó que, si partimos de una F-álgebra nil R, tomamos su envoltura unital, $R^* = R + F1$ con el producto definido de forma natural, es decir,

$$(a + a1)(b + b1) = ab + ab + ba + ab1,$$

entonces el subconjunto $\mathcal{G}$ en R^* dado por

$$\mathcal{G} = \{1 + a \mid a \text{ en } R\}$$

resulta ser un grupo con el producto de R^*. Además, si R es finitamente generado, $\mathcal{G}$ es finitamente generado. Si F es un cuerpo de característica p, (por ejemplo, si F es un cuerpo finito de Galois con p^t elementos), entonces $\mathcal{G}$ es un p-grupo. Además, si R no es nilpotente, entonces $\mathcal{G}$ no es finito.

En 1968 Eugeny Golod, usando una construcción general de Igor Shafarevich, construyó un álgebra sobre un cuerpo de característica p (con p un primo entero arbitrario) que es finitamente generada y nil, pero no nilpotente. Esta álgebra es un contraejemplo al problema general de Kurosh y Levitsky y, junto con el resultado puente de Jacobson, el grupo $\mathcal{G} = 1 + R$ proporciona un contraejemplo al problema general de Burnside.

En cambio, los problemas ordinarios siguieron caminos separados.

En lo que respecta al problema ordinario de Burnside, se sabe que solo hay cuatro exponentes: 2,3,4 y 6 para los que se conoce que la respuesta es positiva. Pero, en 1968, Novikov y Adian construyeron, para cada $n > 4380$, un grupo infinito que tiene exponente n y es finitamente generado. Un poco más tarde, en 1975, Adian rebajó la cota a 665. Por tanto, tanto el problema general como el problema ordinario de Burnside, tienen respuesta negativa.

Curiosamente, mientras que el ejemplo de Golod sigue siendo el único contraejemplo conocido al problema general de Kurosh- Levitzky, se han construido otros grupos que son contraejemplos al problema general de Burnside. Así aparecieron en 1979 los grupos de Suschansky, en 1980 los grupos de Grigorchuck y en 1983 los grupos de Gupta-Sidki.

Todos estos grupos son *"irremediablemente infinitos"* y no hay esperanza de que métodos propios de grupos finitos se puedan adaptar para estudiarlos. En cambio, hay otros grupos que se pueden estudiar utilizando métodos de grupos finitos, como ocurre en los grupos profinitos, que se pueden ver como grupos de Galois de extensiones de Galois de cuerpos en el caso infinito. De hecho, para esta clase de grupos y otras clases de grupos (residualmente finitos) para asegurar que se cumple el problema ordinario de Burnside basta probar el siguiente problema, que se bautizó como problema restringido de Burnside:

"Fijados dos enteros positivos, m y n ¿Hay una cantidad finita de grupos finitos que puedan ser generados por m elementos y tengan exponente n?"

Este nuevo problema de grupos también resultó estar conectado con álgebras, pero en este caso, no con álgebras asociativas, sino con álgebras de Lie y otras álgebras no asociativas.

4. Álgebras no asociativas

Como ya se ha indicado, S. Lie desarrolló la teoría de grupos de Lie, que son grupos de transformaciones. La idea de Lie de pasar de transformaciones a transformaciones infinitesimales fue decisiva. Las transformaciones infinitesimales forman un espacio vectorial complejo y se puede definir su *conmutador*,

$$[A, B] = AB - BA.$$

Esta notación se debe a Jacobi, que también probó que cumple la conocida como identidad de Jacobi,

$$[A, [B, C]] + [C, [A, B]] + [B, [C, A]] = 0.$$

Aparecen así las álgebras de Lie. Si F es un cuerpo, una F-álgebra de Lie es un F-espacio vectorial con una operación *corchete* de forma que tenemos un álgebra, es *decir,* para todo λ en el cuerpo F y para cualesquiera elementos *a, b* en el álgebra $\boldsymbol{a}$ se tiene que $\lambda[a, b] = [\lambda a, b] = [a, \lambda b]$ y además cumple $[a, a] = 0$ y la identidad de Jacobi.

El resultado central, que establece que todo grupo de Lie define un álgebra de Lie y que esta álgebra de Lie define la estructura del grupo de Lie, liga las dos estructuras, grupos y álgebras de Lie, de forma indisoluble.

Las álgebras de Lie no son asociativas, pero cumplen la identidad de Jacobi, que podemos considerar que palía la falta de la propiedad asociativa. Forman la clase más estudiada de álgebras no asociativas y la más importante por su estrecha relación con los grupos de Lie.

En las álgebras de Lie el cuadrado de cualquier elemento es 0. Usualmente las álgebras de Lie se consideran en característica distinta de 2 y, por tanto, son anticonmutativas.

Las álgebras de Lie son, sin duda, las álgebras no asociativas mejor conocidas fuera del ámbito puramente algebraico. Juegan un papel importante en distintas teorías físicas, como la teoría de cuerdas, por ejemplo. Pero si el hecho de romper la conmutatividad en una estructura ya representa un grado mayor de complicación (pensemos en lo que ocurre con los grupos), romper la asociatividad es impactante, incluso para los matemáticos. Considerar álgebras no asociativas, de modo totalmente general, no permite estudiarlas ni llegar a algún resultado de estructura medianamente aceptable. Por eso, en general, se estudian álgebras que satisfacen alguna identidad que sustituye, en cierto modo, a la asociatividad. Es lo que sucede con las álgebras de Jordan, que resultaron ser la llave para resolver el problema restringido de Burnside en el caso de exponente potencia de 2. Pero, ¿qué son las álgebras de Jordan y como aparecen en matemáticas?

Las álgebras de Jordan fueron creadas por Pascual Jordan, Eugene Wigner y John von Neumann, en un intento de construir un álgebra de observables para la mecánica cuántica y la teoría de campos. Los observables en mecánica cuántica son matrices hermitianas, el equivalente de las matrices simétricas trabajando con complejos. Pero el producto usual de dos matrices simétricas no es una matriz simétrica. Por tanto, si queremos definir una operación de modo que el resultado de operar dos

matrices simétricas sea, de nuevo, una matriz simétrica tenemos que usar otro producto, por ejemplo

$$\mathbf{A} \cdot \mathbf{B} = \mathbf{AB} + \mathbf{BA}$$

Este nuevo producto, a diferencia del producto usual de matrices, es conmutativo, pero deja de ser asociativo. De hecho, cumple la *identidad de Jordan*, es decir,

$$(a^2 b)\, a \;=\; a^2 (ba).$$

Si bien las álgebras de Jordan no resultaron de mucha utilidad para el objetivo que se crearon, en física, han sido importantes en matemáticas y, como hemos mencionado, permitieron resolver un problema centenario que ocupó algunas de las mentes matemáticas más brillantes del siglo XX.

Una de las razones de su importante papel matemático está en su estrecha conexión con las álgebras de Lie y con las álgebras asociativas, actuando como una especie de puente entre ambas estructuras.

Otra clase importante de álgebras no asociativas son las álgebras alternativas, que se pueden caracterizar (gracias a un resultado de Artin) como aquellas álgebras en las que cualquier par de elementos generan una subálgebra asociativa (es decir, en expresiones que involucren solo dos elementos, no tenemos que preocuparnos de los paréntesis). Notemos que la respuesta al problema ordinario de Kurosh-Levitsky no solo es afirmativa en el caso asociativo, sino también en el caso de álgebras alternativas, de Lie y de Jordan.

Como toda álgebra asociativa se puede ver como álgebra alternativa, el problema general de Kurosh-Levitsky (PGK-L) también tiene respuesta negativa para las álgebras alternativas. Por otra parte sabemos que si consideramos un álgebra asociativa $\boldsymbol{\mathcal{A}}$, esta álgebra define un álgebra de Jordan (respectivamente un álgebra de Lie) considerando en el nuevo producto $a.\, b = ab + ba$ (respectivamente $[a, b] = ab - ba$), dónde la yuxtaposición representa el producto asociativo original en $\boldsymbol{\mathcal{A}}$. Usando este hecho, se llega a probar que el PGK-L tiene respuesta negativa en las álgebras de Jordan.

Pero notemos que en un álgebra de Lie todo elemento tiene cuadrado cero. Por tanto, si trasladamos la definición de elemento nilpotente directamente del caso asociativo, tendríamos que todo elemento de un álgebra de Lie es nilpotente, con lo que el PGK-L no tendría ningún interés en el caso de álgebras de Lie. Si L es un álgebra de Lie y a

un elemento suyo, tenemos la aplicación adjunta, $\mathrm{ad}(a)$, en L dada por: $\mathrm{ad}(a)(b) = [a, b]$.

Un elemento a del álgebra de Lie L se dice nilpotente con índice de nilpotencia n, si $\mathrm{ad}(a)^n = 0$, pero $\mathrm{ad}(a)^{n-1} \neq 0$. Con esta reformulación de la noción de elemento nilpotente, el correspondiente PGK-L tiene claro interés matemático y tiene respuesta afirmativa.

En resumen, el problema ordinario de Kurosh-Levitsky tuvo respuesta positiva no solo en el caso asociativo, sino también en el caso de Lie, alternativo y de Jordan. Para llegar a probar el resultado se desarrolló la teoría de PI-álgebras (álgebras que satisfacen las identidades polinomiales) que ha resultado de gran ayuda e interés.

Toda álgebra de Jordan permite construir un álgebra de Lie a través de un proceso debido a Jacques Tits, Issai Kantor y Max Koecher y denominado habitualmente la TKK construcción. Y el álgebra de Jordan contiene toda la información necesaria para trabajar con esa álgebra de Lie. Recíprocamente, muchas importantes álgebras de Lie se pueden conseguir a partir de un álgebra de Jordan a través del proceso mencionado. Por tanto, esas álgebras de Lie se pueden estudiar usando métodos de Jordan, más cercanos a los asociativos y, por tanto, más sencillos.

Y es en este ambiente, entre grupos, álgebras y superálgebras no asociativas y relaciones entre ellos en el que se ha centrado mi actividad investigadora en matemáticas. De hecho, la mayor parte de mi actividad corresponde al estudio de álgebras y superálgebras no asociativas, fundamentalmente en el caso de Jordan, tanto finito como infinito dimensional, incluyendo teoremas de estructura y representaciones.

En las álgebras de Jordan hay un operador, que juega un papel tan importante como la multiplicación a derecha o a izquierda en el caso asociativo. Si J es un álgebra de Jordan y s es un elemento cualquiera suyo, el operador $\mathrm{U}(s)$ actúa como:

$$z\mathrm{U}(s) = (sz)s + s(zs) - s^2z.$$

Sin entrar en detalles, paso a mencionar algunas de mis contribuciones en teoría de Jordan.

He estudiado la dimensión de Gelfand-Kirillow en álgebras de Jordan. Notemos que esta definición se usa para poder comparar algebras infinito-dimensionales, dónde la dimensión deja de ser un concepto útil. Hemos encontrado relaciones entre la dimensión de Gelfand Kirillov de un álgebra de Jordan y la correspondiente

dimensión de su envolvente asociativa (en el caso especial) y su envolvente multiplicativa.

En un trabajo conjunto con E. Zelmanov hemos probado que no existen álgebras de Jordan cuya dimensión sea estrictamente mayor que 1 y estrictamente menor que 2, resultado que se conocía en el caso asociativo. También hemos estudiado la estructura de las álgebras de Jordan semiprimas, finitamente generadas con dimensión de Gelfand-Kirillow igual a 1.

En respuesta a una conjetura de N. Jacobson sobre la posibilidad de extender un resultado sobre anillos de cociente en caso asociativo al caso de Jordan, hemos probado que un álgebra de Jordan tiene un anillo de fracciones respecto a una mónada S si y solo si se cumple la condición de Ore (para cualquier elemento s en J y cualquier operador multiplicación W, existe otro elemento s' y otro operador multiplicación W' cumpliendo que $WU(s) = U(s')W'$). Una mónada S es un subconjunto cerrado para cuadrados, transformaciones por $U(s)$, cuando s es cualquier elemento de S y cumpliendo que dos conjuntos $SU(s)$ y $SU(t)$ se cortan siempre para cualesquiera s, t en S. Por tanto, se ha confirmado la conjetura de Jacobson.

En el caso de las álgebras de dimensión finita, se suele imponer alguna condición de finitud para poder obtener algún resultado de estructura. Una de las condiciones más naturales es la de considerar álgebras graduadas, pues son especialmente importantes (son las que aparecen ligadas a los grupos como veremos). Hemos dado la estructura de las álgebras de Jordan simples y de las primas, graduadas sobre los enteros y con crecimiento 1. También hemos obtenido la estructura de las álgebras de Lie, primas no degeneradas, $\mathbb{Z}$-graduadas de crecimiento 1. En ambos casos trabajamos sobre un cuerpo algebraicamente cerrado de característica 0.

5. El problema restringido de Burnside

Alexei Kostrikin, empezó a interesarse por el problema restringido de Burnside (PRB) en 1950, obteniendo importantes resultados parciales. De hecho, demostró el PRB para el caso particular de grupos en los que todos los elementos distintos de 1 tienen orden p (para todo elemento g del grupo $\mathcal{G}$ se tiene que $g^p = 1$). Este problema generó una notable actividad investigadora en la segunda mitad del siglo XX, tanto en la teoría de grupos como en la de álgebras asociativas y no asociativas. Porque la respuesta al problema restringido de Burnside vino de la mano de las álgebras no

asociativas, concretamente de la mano de álgebras de Lie y de álgebras de Jordan, para el caso de exponente potencia de 2.

Efim Zelmanov en su nombramiento como "Doctor Honoris Causa" por la Universidad de Oviedo

En la solución final de dicho problema, por la que se otorgó la medalla Fields a Efim Zelmanov en 1994, se utilizaron los resultados previos de Kostrikin y algunos de los resultados más profundos de teoría de grupos, como el teorema de reducción de Hall y Higman, que permite reducir el PRB, en el caso general, al mismo problema para grupos de exponente potencia de primo, siempre que se cumplan unas condiciones previas. La clasificación de los grupos simples finitos es, sin duda, uno de los resultados cumbre de las matemáticas del siglo XX. En particular, dicha clasificación asegura que siempre se dan las condiciones precisas para aplicar el teorema de reducción de Hall y Higman. El hecho de trabajar con grupos que tienen exponente potencia de un primo permite asociar a cada uno de estos grupos un álgebra de Lie y reformular el problema en el lenguaje de las álgebras de Lie.

Esto es lo que hizo Zelmanov, para grupos de exponente potencia de *p*, con *p* un primo impar, extendiendo el resultado de Kostrikin para grupos de exponente primo impar *p*. Pero la técnica utilizada no funcionaba cuando el primo es el 2. Y es en este punto dónde entran en escena las álgebras de Jordan. En sus investigaciones previas sobre álgebras de Jordan, Zelmanov había cambiado la fisonomía de este campo de trabajo. En la demostración del problema reducido de Burnside para grupos de exponente potencia de 2 muestra su ingenio y su dominio técnico.

Veamos, con un poco más de detalle cómo se pasa de un problema en grupos a un problema de álgebras de Lie. Empecemos por ver cómo se construye un álgebra de Lie asociada a un grupo. Para ello utilizaremos la noción de conmutador, que juega un importante papel en teoría de grupos.

Si $\mathcal{G}$ es un grupo, x, y son elementos suyos, el conmutador de los elementos viene definido por $(x, y) = x^{-1}y^{-1}xy$, siendo x^{-1} el elemento inverso del elemento x para la operación del grupo. Notemos que el conmutador mide, en cierto modo, lo lejos que están los elementos del grupo de conmutar, dado que el conmutador de dos elementos en un grupo es el elemento neutro si y solo si dichos elementos conmutan. Por inducción se pueden definir conmutadores de longitud arbitraria,

$$(x_1, x_2, \dots, x_n) = ((x_1, x_2, \dots, x_{n-1}), x_n).$$

De este modo se puede construir una cadena descendente de subgrupos de $\mathcal{G}$, empezando por el grupo $\mathcal{G} = \mathcal{G}_1 \geq \mathcal{G}_2 \geq \mathcal{G}_3 \geq \dots$ de modo que para un índice i fijo, el subgupo $\mathcal{G}_i$ está generado por las potencias p^j del conmutador $((x_1, x_2, \dots, x_{n-1}), x_n)$ cumpliendo que $np^j \geq i$.

Los factores de esta serie, $\mathcal{G}_i \,/\, \mathcal{G}_{i+1}$, son grupos p-elementales abelianos, es decir, son grupos abelianos cuyos elementos tienen todos orden p. Es bien conocido que estos grupos se pueden ver, de modo natural, como espacios vectoriales sobre el cuerpo de Galois de p elementos GF(p).

De este modo se puede construir un álgebra de Lie graduada ligada a $\mathcal{G}$, $\mathrm{L_p}(\mathcal{G})$, como

$$\mathrm{L_p}(\mathcal{G}) = \bigoplus_{i \geq 1} \mathcal{G}_i/\mathcal{G}_{i+1},$$

donde el producto viene definido por la regla

$$[a_i\, \mathcal{G}_{i+1}, b_s\, \mathcal{G}_{s+1}] = (a_i, b_s)\, \mathcal{G}_{i+s+1}$$

En la demostración del PRB para grupos de exponente p, Kostrikin considera el álgebra de Lie $\mathrm{L_p}(\mathcal{G})$ y utiliza un importante resultado suyo que había demostrado previamente:

Si $p \geq 3$ y L es un álgebra de Lie sobre el cuerpo de p elementos, GF(p) que satisface la identidad de Engel E_{p-1}, entonces L es localmente nilpotente.

La identidad E_{p-1} nos dice que $[\ldots [[x, y], y]\ \ldots, y] = 0$, donde el elemento y aparece $p - 1$ veces, donde x, y son elementos cualesquiera del álgebra de Lie L.

Ya hemos indicado que los métodos propios de grupos finitos pueden usarse también en algunos grupos infinitos. La clase de los grupos residualmente finitos es un ejemplo. Los grupos encontrados como contraejemplo al problema general de Burnside pertenecen a esta clase: grupos de Grigorchuck, grupos de Sushansky, grupos de Gupta-Sidki.

Un grupo residualmente finito es un grupo que se puede aproximar por grupos finitos. Un grupo residualmente p-grupo es un grupo que se puede aproximar por p-grupos finitos. En estos grupos se puede definir una topología ligada a la estructura de grupo. Si esta topología tiene buenas propiedades (es completa) el grupo $\mathcal{G}$ es un grupo profinito (respectivamente un pro-p-grupo). En el lenguaje algebraico actual, un pro-p-grupo es un límite inverso de p-grupos finitos.

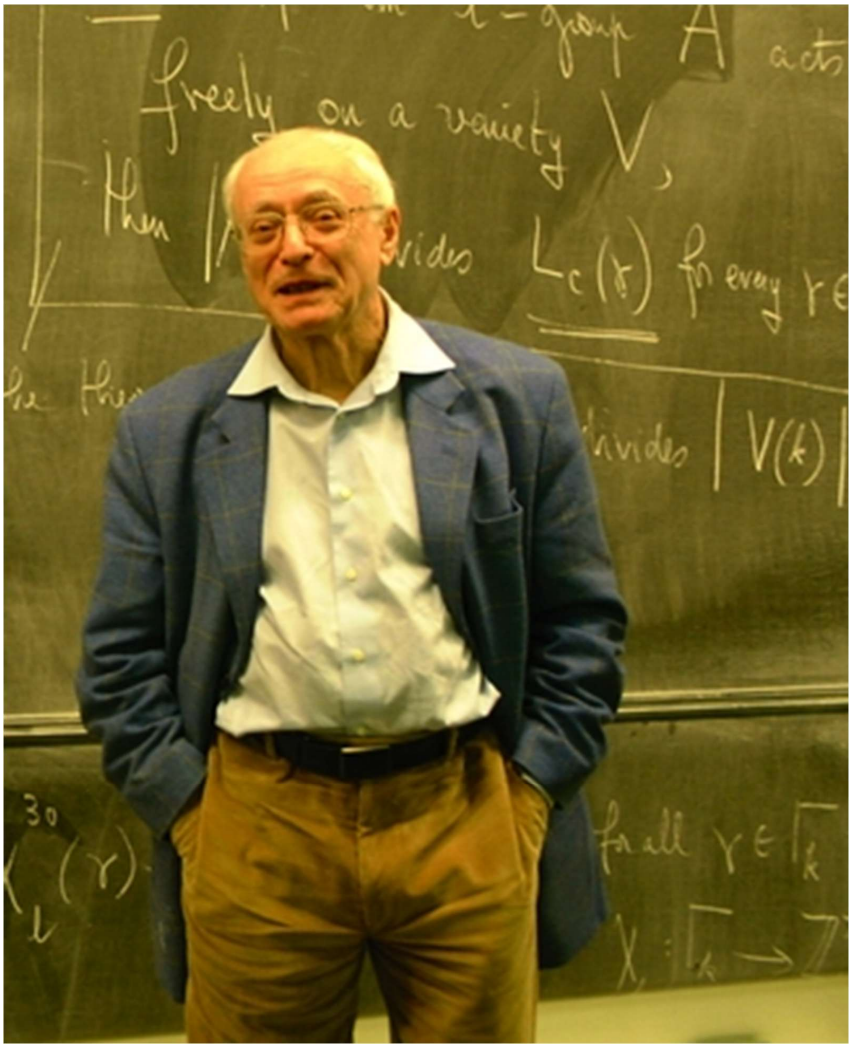
De modo análogo, se puede definir la noción de grupo pro-nilpotente, como un límite inverso de grupos nilpotentes.

Un resultado, casi inmediato, que se obtiene al aplicar el PRB a los pro-p-grupos es que un pro-p-grupo periódico (todos sus elementos tienen orden finito) es localmente finito (sus subgrupos finitamente generados son finitos).

Podemos citar otras consecuencias del PRB.

- Si $\mathcal{G}$ es un pro-p-grupo, entonces o bien contiene el grupo libre de rango 2 como subgrupo o bien el álgebra $\mathrm{L_p}(\mathcal{G})$ satisface una identidad polinomial.
- Un grupo periódico, residualmente p-grupo, finitamente generado que satisface una identidad polinomial es finito.

En un pro-p-grupo finitamente generado todo subgrupo de índice finito es abierto. Intuitivamente, esto significa que la topología de un pro-p-grupo está controlada por su estructura algebraica. ¿Qué ocurre si consideramos grupos profinitos en lugar de pro-p-grupos? El brillante matemático francés Jean Pierre Serre planteó esta pregunta y conjeturó una respuesta afirmativa. Serre obtuvo la medalla Fields en 1954, año en el que cumplió 28 años, siendo el matemático que ha recibido la medalla Fields siendo más joven. También recibió el premio Abel en 2003, el primer año que se otorgó.



Jean Pierre Serre

Intentando contestar a esta conjetura, Aner Shalev plantea otro problema intermedio: ¿Es cierto que el grupo $\mathcal{G}^n$, generado por las potencias n-simas de elementos del grupo $\mathcal{G}$, es un subgrupo cerrado de $\mathcal{G}$, siendo $\mathcal{G}$ un grupo profinito finitamente generado?

En [63] se da una respuesta parcial a la pregunta realizada por Shalev, probando que el resultado de pro-p-grupos finitamente generados sigue siendo cierto para grupos pro-nilpotentes finitos. Este resultado se puede reformular, en términos de grupos finitos y, en [65] se extiende este resultado, en su reformulación en términos de grupos finitos, a una clase más amplia que la clase de grupos nilpotentes finitos (grupos con altura de Fitting acotada) y en [76] se prueba para la clase de los grupos simples finitos.

Finalmente, Nikolov y Segal probaron el resultado para grupos finitos resolubles y luego, usando un razonamiento similar al que se usa en el ya mencionado teorema de reducción de Hall y Higmann, lo extendieron a todos los grupos finitos, dando así una respuesta positiva a la conjetura de Serre:

"*En todo grupo profinito finitamente generado sus subgrupos de índice finito son abiertos*"

Notemos que todo elemento del subgrupo $\mathcal{G}^n$ se puede expresar como un producto finito de potencias n-simas de elementos de $\mathcal{G}$, pero el número de factores varia de unos elementos a otros. La versión equivalente a la pregunta planteada por Shalev, pero en términos de grupos finitos, se plantea la existencia de una cota uniforme para el número de factores potencias n-simas de elementos del grupo que se aplique a todos los elementos de $\mathcal{G}^n$.

Estos problemas están ligados a la noción de subgrupo verbal y elipticidad, tema en el que también se ha desarrollado mi actividad investigadora. Una palabra w es un elemento del grupo libre. Si $\mathcal{G}$ es un grupo, al sustituir los generadores del grupo libre por elementos arbitrarios de $\mathcal{G}$ de todos los modos posibles podemos generar un subgrupo de $\mathcal{G}$ que se llama subgrupo verbal, $w(\mathcal{G})$. Los subgrupos verbales se han estudiado tanto en grupos finitos como infinitos. Por ejemplo, si consideramos como palabra $w = (x, y) = x^{-1}y^{-1}xy$ en el grupo libre de rango 2, el correspondiente subgrupo verbal es el grupo derivado.

Se dice que una palabra w es elíptica en $\mathcal{G}$ (o tiene anchura finita n) si cada elemento del subgrupo verbal se puede expresar como un producto de n elementos, siendo cada uno de ellos (o su inverso) un elemento obtenido al sustituir en la palabra w las variables (los generadores del grupo libre) por elementos arbitrarios. Cuando una palabra w es elíptica en una clase de grupos con la misma anchura verbal en todos ellos, decimos que w es uniformemente elíptica en esa clase de grupos.

El punto de conexión entre la elipticidad y el problema planteado por Serre está en el siguiente resultado demostrado por B. Hartley: Una palabra w tiene anchura finita en un grupo profinito si y solo si $w(\mathcal{G})$ es cerrado en $\mathcal{G}$.

Con E. Zelmanov hemos estudiado el concepto de elipticidad en pro-p-grupos, sustituyendo el grupo libre por su pro-p-compleción, extendiendo la noción de identidades lineales en álgebras a palabras multilineales en grupos.

En los últimos años se ha desarrollado una activa línea de trabajo en la que se trata de demostrar que un grupo tiene exponente finito sabiendo que ciertos elementos del grupo tienen orden finito. En este tipo de resultados, se usa, de modo esencial, un resultado publicado por E. Zelmanov en 2017 (aunque había sido anunciado mucho antes) que a su vez se basa en el PRB. En dicho resultado se prueba la nilpotencia de un álgebra de Lie que satisface una identidad polinomial y en el que todo producto de generadores es nilpotente.

Este resultado de álgebras de Lie tiene importantes implicaciones en teoría de grupos, como la siguiente, por citar un ejemplo.

Si $\mathcal{G}$ es un grupo periódico, finitamente generado y residualmente p-grupo que cumple que la correspondiente álgebra de Lie $L_p(\mathcal{G})$ satisface una identidad polinomial, entonces $\mathcal{G}$ es finito.

Trabajar con característica cero o con característica prima es muy diferente. Se sabe que, en característica cero, si un álgebra de Lie, graduada por un grupo abeliano, cumple que sus componentes homogéneas son finito dimensionales y los elementos homogéneos son ad-nil, entonces el álgebra es necesariamente localmente nilpotente. Este resultado tiene importantes consecuencias en álgebras asociativas, de Lie y de Jordan. Pero no es cierto en característica prima. Las álgebras de Lie ligadas a los grupos de Grigorchuck son un contraejemplo. En un trabajo con E. Zelmanov probamos que no existen grupos en característica cero que puedan considerarse análogos a los grupos de Grigorchuck.

6. Superálgebras

Las superálgebras aparecen en matemáticas en 1955 de la mano de I. Kaplansky. Pero adquieren relevancia después de que los físicos las declararan interesantes por su relación con la supersimetría.

Las superálgebras juegan un papel importante en el estudio de la supersimetría y en teorías de supergravedad. Tienen aplicaciones en Física Cuántica, en Simetría

Superdinámica o en Física Nuclear. Y es debido a estas aplicaciones que nos interesa estudiar generadores explícitos de superálgebras, obtener teoremas de estructura o conocer sus representaciones. Una superálgebra no es mas que un álgebra $\mathbb{Z}_2$-graduada, es decir, $A = A_0 + A_1$, siendo $\mathbb{Z}_2 = \{0,1\}$. Esto significa que $A_0 A_0 \subseteq A_0$, $A_0 A_1 \subseteq A_1$, $A_1 A_0 \subseteq A_1$ y $A_1 A_1 \subseteq A_0$. La parte par, A_0, es una subálgebra y A_1, la parte impar, se puede ver como un módulo sobre A_0. Los elementos de A_0 se llaman elementos pares y los elementos de A_1 se llaman impares. Todos ellos, elementos pares y elementos impares, se llaman elementos homogéneos y tienen como paridad 0 o 1, según que sean pares o impares.

Las superálgebras asociativas son álgebras asociativas que tienen una $\mathbb{Z}_2$-graduación.

Pero una superálgebra de Lie no es un álgebra de Lie. Dos elementos homogéneos anticonmutan si y solo si uno de ellos es par. Dos elementos impares conmutan. En lugar de la identidad de Jacobi se satisface otra identidad, la superidentidad de Jacobi, que se obtiene poniendo signo menos delante de algunos términos de la identidad de Jacobi, dependiendo de la paridad de los elementos implicados.

Del mismo modo una superálgebra de Jordan no es un álgebra de Jordan. Ahora dos elementos homogéneos conmutan si y solo si uno de ellos es par y dos elementos impares anticonmutan. Como la identidad de Jacobi no es lineal, tenemos que linealizarla en primer lugar. La superidentidad de Jordan se obtiene de la identidad linealizada de Jordan aplicando la misma regla que antes, poner signo menos delante de algunos términos de la identidad dependiendo de la paridad de los elementos que aparecen en dichos términos.

El primer capítulo de la enciclopedia de matemáticas [87], que hemos realizado con Zelmanov, está dedicado a las superálgebras de Jordan.

Como hemos indicado, conocer las superálgebras simples es un problema esencial. Simple significa que no contiene ningún ideal distinto del cero y del total. Notemos que en este contexto los ideales (y las subsuperálgebras) se consideran homogéneos, es decir, si un elemento $a = a_0 + a_1$ está en el ideal, sus componentes homogéneas a_0 y a_1 también están en el ideal. En un ideal el producto de un elemento suyo por uno de la superálgebra está siempre en el ideal. En el caso finito dimensional, cuando la característica del cuerpo es 0, la clasificación de las álgebras de Lie simples se debe a V. Kac. Usando la estrecha conexión entre estructuras de Lie y de Jordan, Kac obtuvo (con una adición posterior de I. Kantor) la clasificación para las superálgebras de Jordan simples.

En el caso de característica prima no se conoce la clasificación de las superálgebras de Lie simples finito-dimensionales. Por tanto, no podemos aplicar el método usado en característica cero para clasificar las superálgebras de Jordan finito-dimensionales simples. Pero se conocen todas las superálgebras de Jordan simples. La clasificación

se hizo separando dos casos. Cuando la parte par es semisimple, la clasificación sigue las mismas pautas que en característica cero y los autores de la misma son M. Racine y E. Zelmanov. Si la parte impar no es semisimple, no se siguen los patrones de característica cero, apareciendo nuevas e interesantes superálgebras. El caso de clasificación de superálgebras de Jordan simples unitales con parte par no semisimple lo hicimos en un trabajo conjunto con E. Zelmanov. Fue también Zelmanov quien estudió las superálgebras de Jordan simples no unitales.

En este último caso aparecen unas superálgebras de Jordan nuevas, las superálgebras de Cheng-Kac, a las que llegamos inspirados en las álgebras de Cheng-Kac (infinito dimensionales), construidas por Cheng y Kac como ejemplo de álgebras superconformales. Este tipo de superálgebras aparecieron por el interés de los físicos en superálgebras de Lie que sean extensiones del álgebra de Virasoro. Kac y van der Leur han conjeturado la clasificación de las álgebras superconformales y las álgebras de Cheng- Kac son parte de esa conjetura. Aunque la conjetura, en su generalidad, permanece abierta, nosotros, en un trabajo conjunto con V. Kac y E. Zelmanov, probamos que es cierta en el caso de que las álgebras superconformales provengan de una superálgebra de Jordan. En ese trabajo, en particular, se prueba que las álgebras de Cheng-Kac provienen de una superálgebra de Jordan, a la que denominamos del mismo modo. Vimos que esa construcción se podía realizar también en el caso de característica prima y así aparecieron las superálgebras de Cheng Kac, que, en el caso simple, tenían que aparecer en la clasificación de las superálgebras de Jordan simples en característica prima con parte par no semisimple.

Junto con E. Zelmanov hemos estudiado superálgebras definidas por corchetes, tipo al que pertenecen las superálgebras simples que aparecen en nuestro teorema de clasificación junto con las álgebras de Cheng-Kac.

La teoría de la representación de álgebras de Jordan semisimples se debe a N. Jacobson, que probó que todo bimódulo sobre un álgebra de Jordan semisimple es completamente reducible. Este hecho le permitió determinar todos los bimódulos irreducibles sobre las álgebras de Jordan simples finito-dimensionales.

La situación en el caso de superálgebras es diferente. Ya no es cierto que una superálgebra de Jordan (o de Lie) semisimple (con radical resoluble cero) sea suma directa de superálgebras simples. De hecho, en el caso de superálgebras hay que diferenciar entre módulos unitales y módulos a un lado y se puede ver que el problema de encontrar todos los bimódulos sobre una superálgebra de Jordan se reduce a estudiar los módulos unitales y los módulos a un lado. Y estos últimos se corresponden con los módulos a izquierda (o derecha) sobre el álgebra envolvente universal del álgebra de Jordan, que es una superálgebra asociativa. En una serie de trabajos conjuntos con Zelmanov estudiamos los bimódulos sobre las superálgebras simples de Jordan (en dimensión finita). Curiosamente, los casos especiales, en los

que se marca un comportamiento claramente distinto en álgebras y superálgebras, solo aparecen en dimensiones pequeñas.

El problema de las representaciones de superálgebras infinito dimensionales es más complicado, aunque es un tema en el que llevamos tiempo trabajando y que esperamos que, eventualmente, nos ayude a dar una respuesta afirmativa a la conjetura de Kac y van de Leur sobre álgebras superconformales.

En el caso de álgebras de Lie, el estudio de aquellas álgebras infinito dimensionales que están graduadas por un sistema raíz ha jugado un importante papel. El mismo problema ha sido considerado en superálgebras. Los casos que presentan situaciones singulares, con respecto al caso de álgebras, corresponden a las superálgebras graduadas por el sistema raíz $A(n,n)$ y a las superálgebras graduadas por los sistemas raíz $P(n)$ y $Q(n)$. Las primeras fueron estudiadas en un trabajo conjunto con G. Benkart y A. Elduque y las segundas en un trabajo conjunto con E. Zelmanov.

7. Aplicaciones en Teoría de la Información

Como ya se ha mencionado anteriormente, debemos a Galois los cuerpos finitos, también relacionados con los polinomios, porque se construyen a partir de ellos. Pero, ¿para qué sirven los cuerpos finitos? Durante mucho tiempo solo se consideraban de utilidad los cuerpos infinitos, fundamentalmente los números racionales, reales, complejos. Los cuerpos finitos parecían una creación de los algebristas, sin ninguna utilidad, y que solo les interesaban a ellos. El uso de los ordenadores y la necesidad de usar secuencias de ceros y unos para introducir la información en los ordenadores dio un protagonismo inesperado a los cuerpos finitos. La teoría de la información no habría podido desarrollarse sin los cuerpos finitos. El envío de la información a través de un canal, una vez digitalizada, también generó la necesidad de proteger dicha información, bien su integridad o bien su confidencialidad. De esta manera nacen los códigos correctores, si lo que queremos es proteger los mensajes de ruido (cualquier circunstancia que modifique el mensaje enviado) o la criptografía, si lo que queremos es proteger el mensaje de miradas indiscretas y no autorizadas. En ambos casos, los cuerpos finitos juegan un papel esencial. También los grupos y las álgebras aparecen como actores destacados en este escenario.

En los últimos años, dentro de nuestro grupo, hemos incluido, como línea de trabajo, las aplicaciones algebraicas tanto en la teoría de códigos correctores de errores como en criptografía. En concreto, hemos explorado, y lo seguimos haciendo, el uso de diversas estructuras algebraicas en ambos campos.

Grupo de doctorandos en distintos periodos durante la celebración de una reunión de cátedras de ciberseguridad en el Aula Magna de la Universidad de Oviedo

7.1 – Teoría de códigos correctores

A diferencia de los códigos que se utilizan para cifrar un mensaje, cuyo objetivo es proteger la confidencialidad, manteniéndolo el mensaje oculto, salvo para el legítimo destinatario, los códigos correctores de errores pretenden asegurar la integridad de un mensaje que se transmite por un canal afectado de ruido (se llama ruido a cualquier perturbación en un canal que pueda modificar la información que circula por él) y que puede sufrir errores en el proceso de transmisión. En este caso, lo que preocupa es que el receptor pueda recuperar el mensaje tal como se envió, en su totalidad. Por eso, el primer paso es ser capaces de detectar que se han producido errores y el segundo es corregirlos. ¿Por qué es tan importante asegurar que el mensaje se pueda recuperar de forma íntegra? Podemos pensar que siempre se puede volver a enviar el mensaje si detectamos que se han cometido errores durante el proceso de transmisión. Pero no siempre es posible volver a enviar la información por segunda vez, no solo por el coste que representa el uso del canal, sino porque es posible que la información deje de estar disponible. Pensemos en un satélite artificial que envía imágenes de la luna a la tierra. Si se producen errores durante el envío, no

podemos recuperar la imagen enviada, porque el satélite ya no estará en la misma posición respecto a la luna.

Usualmente se consideran códigos lineales. Un ejemplo bien conocido es el código control de paridad. En este caso, los mensajes son secuencias de $n-1$ elementos de un cuerpo finito $\mathbb{F}$ y se codifican como secuencias de longitud n con la propiedad de que la suma de las componentes de la n-tupla es 0. En este caso, una n-tupla cualquiera de $\mathbb{F}^n$, sea $(\alpha_1, \alpha_2, \dots, \alpha_n)$, pertenece al código $\mathfrak{C}$ si y solo si la suma de sus componentes es 0. Si se produce un único error, el vector que obtenemos no está en $\mathfrak{C}$, por tanto detectamos que se ha producido un error, pero no podemos corregirlo sin saber la posición del error. Si se producen dos o más errores, podemos recuperar un elemento de $\mathfrak{C}$ y, en ese caso, no detectamos que se han producido errores. El código control de paridad se puede identificar con un subespacio concreto de dimensión $n-1$ del espacio vectorial de dimensión n. Es un código que solo permite detectar un error y no permite corregir ninguno.

Para construir un código lineal corrector de errores, se considera $\mathbb{F}^n$, el espacio vectorial de dimensión n sobre un cuerpo finito $\mathbb{F}$, y el código $\mathfrak{C}$ es un subespacio vectorial suyo.

En el caso general, cada mensaje a enviar se identifica con uno de los vectores del subespacio $\mathfrak{C}$. Supongamos que $\mathfrak{C}$ tiene dimensión k. Los parámetros n y k se llaman, respectivamente, *longitud* y *dimensión* del código. Si al recibir un mensaje comprobamos que el elemento que hemos recibido no está en el subespacio $\mathfrak{C}$, podemos asegurar que se han producido errores durante la transmisión. Por supuesto, siempre puede ocurrir que se produzcan errores, pero el número de ellos sea mayor que la capacidad correctora del código $\mathfrak{C}$. En este caso, el código no nos permite corregir los errores producidos

Todo código lineal tiene una matriz generadora $\mathcal{G}$. Se trata de una matriz de k filas y n columnas con la propiedad de que los elementos del código $\mathfrak{C}$ se obtienen al multiplicar todas las k tuplas de $\mathbb{F}$ por la matriz $\mathcal{G}$, es decir,

$$\mathfrak{C} = \{(\beta_1, \beta_2, \dots, \beta_k)\mathcal{G} \mid (\beta_1, \beta_2, \dots, \beta_k) \in \mathbb{F}^k\}.$$

Se define el *peso de Hamming* de un vector $\boldsymbol{u}$ de $\mathbb{F}^n$ como el número de componentes distintas de cero del vector. La distancia de Hamming de dos elementos $\boldsymbol{u}$, $\boldsymbol{v}$ de $\mathbb{F}^n$ es el peso de Hamming de $\boldsymbol{u}-\boldsymbol{v}$ o, equivalentemente, el número de posiciones en las que $\boldsymbol{u}$ y $\boldsymbol{v}$ tienen un elemento diferente de $\mathbb{F}$. El menor peso posible d de un elemento no nulo $\boldsymbol{u} \in \mathfrak{C}$ se llama distancia mínima del código. La distancia entre dos elementos cualesquiera de $\mathfrak{C}$ es mayor o igual que d.

El número máximo de errores que puede corregir un código de distancia mínima d es la parte entera de $(d-1)/2$ y puede detectar hasta $d-1$ errores.

Por tanto, la terna (n, k, d) determina las propiedades correctoras del código. Interesa que tanto k como d sean lo más cercanos posible a n, para corregir muchos errores y de forma económica. Pero estos intereses son contrapuestos, ya que se verifica la denominada cota de Singleton: $k + d \leq n + 1$.

Como hemos indicado el objetivo de los códigos correctores es detectar y corregir los errores producidos durante el envío de la información, siempre que el número de errores no supere los que puede corregir por su capacidad. Si se han producido m errores, con $m < (d-1)/2$, y recibimos una palabra $u \in \mathbb{F}^n$, para recuperar el mensaje debemos encontrar la única palabra de $\mathfrak{C}$ que está a distancia de Hamming m de u.

En general, si consideramos un código lineal arbitrario no sabemos cómo descodificar la palabra recibida, aunque el número de errores producido sea inferior a la capacidad correctora del código. El problema de descodificación de un código lineal arbitrario es NP-completo, lo que tiene dos consecuencias inmediatas. En primer lugar, que no todos los códigos lineales pueden ser usados de modo efectivo como códigos correctores y, por ello, hay que diseñarlos de modo adecuado, usualmente aprovechando ciertas propiedades algebraicas y/o geométricas. Y, en segundo lugar, el problema de descodificación de un código lineal se podría utilizar para sustentar la seguridad de un esquema de cifrado resistente a los ataques de un ordenador cuántico.

Dentro de nuestro grupo hemos trabajado con distintas clases de códigos y también se han estudiado estructuras, asociativas y no asociativas que podrían ser usadas para el diseño de códigos con buenas propiedades. En particular hemos trabajado con códigos grupos. Supongamos que $\mathbb{F}$ es un cuerpo y $\boldsymbol{\mathcal{G}} = \{g_1, g_2, \ldots, g_n\}$ es un grupo finito con n elementos. Podemos construir un $\mathbb{F}$-espacio vectorial de dimensión n en el que los elementos de la base son los elementos del grupo. Es decir, consideramos el conjunto de todas las combinaciones lineales formales de elementos del grupo: $\mathbb{F}[\boldsymbol{\mathcal{G}}] = \{\alpha_1 g_1 + \cdots + \alpha_n g_n \mid \alpha_k \in \mathbb{F}\}$.

Usando las operaciones de suma y producto del cuerpo $\mathbb{F}$ es claro cómo definir una estructura de $\mathbb{F}$-espacio vectorial en $\mathbb{F}[\boldsymbol{\mathcal{G}}]$. Pero también podemos definir un producto en $\mathbb{F}[\boldsymbol{\mathcal{G}}]$ utilizando el producto de $\boldsymbol{\mathcal{G}}$. Es decir, $\mathbb{F}[\boldsymbol{\mathcal{G}}]$ es una $\mathbb{F}$-álgebra asociativa. Si en lugar de considerar un subespacio cualquiera, tomamos como código un subespacio que sobrevive a los productos por elementos del álgebra tenemos un código grupo (es decir, un ideal). Si solo sobrevive a los productos por la izquierda, tenemos un código grupo a izquierda (es decir, un ideal a izquierda).

Este tipo de códigos han sido ampliamente estudiados, en particular por nuestro grupo de investigación. Se conocía la existencia de códigos grupos a izquierda asociados a un grupo no abeliano con propiedades diferentes de los códigos grupo a izquierda construidos con los grupos abelianos del mismo orden n. Pero durante un

tiempo se desconocía si ocurría lo mismo con códigos grupo. Nosotros consideramos este problema como tema central de una tesis doctoral en el grupo de investigación. Se consiguió probar que también se cumplía en códigos grupo. Usando grupos no abelianos se podían conseguir códigos grupo que no se obtenían con los abelianos. Además, llegamos a probar que el mismo resultado se podía obtener con cuerpos de cualquier característica. Pero durante un tiempo no estaba claro el interés de trabajar con grupos no abelianos, más complicados que los abelianos, porque los ejemplos que se habían obtenido tenían peores parámetros (la terna longitud, dimensión y distancia mínima, mencionada anteriormente) que los códigos grupo obtenidos a partir de grupos abelianos. Finalmente, se consiguió un ejemplo de código con parámetros óptimos que no se podían conseguir en códigos grupo obtenidos a partir de un grupo abeliano. Esos resultados justificaban el trabajo con códigos grupo construidos con grupos no abelianos.

7.2 – Criptografía

Aunque la criptografía sea muy antigua, prácticamente tanto como los sistemas de escritura, dado que existe un interés general en la protección de los secretos, los sistemas criptográficos, hasta mitad del siglo pasado, hacían poco uso del álgebra o de cualquier clase de matemáticas sofisticadas. Todos los esquemas de cifrado anteriores se basaban en la misma idea: emisor y receptor se ponían de acuerdo en un modo de cifrar los mensajes y por tanto también conocían el procedimiento para descifrar un mensaje cifrado, es decir, compartían la clave de cifrado que coincidía, esencialmente, con la de descifrado. Es lo que se denomina criptografía de clave privada. Dado que su uso fundamental se restringía, básicamente, al uso diplomático o comercial, la criptografía existente era suficiente para satisfacer las necesidades de esos momentos, aunque la evolución ha sido constante, tratando de subsanar las debilidades encontradas y presentando opciones renovadas continuamente.

Pero el increíble avance de los ordenadores y de la teoría de la información exigía otro tipo de criptografía y hubiera sido inviables sin la criptografía de clave pública, que permitió que un altísimo número de usuarios de la red pudiera enviar mensajes a otro usuario (pensemos en un banco, en una oficina de Hacienda, o en un servidor de comercio electrónico) de forma segura. La criptografía de clave pública implica un impresionante cambio conceptual. Si en la criptografía de clave privada cada pareja de usuarios tenía que compartir (y mantener secreta) una clave para comunicarse entre ellos, en la criptografía de clave pública cada usuario tiene un par de claves: una clave pública, que puede conocer cualquier usuario de la red, y que tiene que usar dicho usuario para enviar mensajes cifrados al propietario de la clave, y una clave privada, que solo puede conocer el propietario, y que le permite descifrar cualquier mensaje, cifrado con su clave pública, que reciba. Para lograr esto se requiere un uso

masivo de matemáticas y es aquí donde las estructuras algebraicas juegan un importante papel.

La idea revolucionaria en la que se basó la criptografía de clave pública aparece por vez primera en 1976, en un trabajo de Diffie y Hellman en el que hacen una propuesta que influyó en la actividad posterior y cambió dramáticamente el aspecto de la criptografía del siglo XX.

Suponiendo que existe una función $f: M \to C$ cumpliendo que es fácil determinar la imagen $f(m)$ de cualquier elemento m de M, pero es prácticamente inviable calcular un elemento de M a partir del conocimiento de su imagen, debido al coste computacional que exige, aunque formalmente sepamos como hacerlo. Pero en muchas ocasiones existe una *trampa*, es decir, una información adicional que, si la conocemos, nos permite hacer, en un tiempo razonable, el cálculo que deseamos. Las funciones que cumplen esta condición son las denominadas "*funciones de una vía*" (aunque no existe necesariamente una trampa para cada una de ellas).

Supongamos que un usuario, que llamaremos A, conoce una función de una vía f y una trampa que (idealmente) solo A conoce. En tal caso, A puede diseñar fácilmente un procedimiento de cifrado de clave pública que permita a cualquier otro usuario enviarle mensajes de forma segura a través de un canal público.

Cada mensaje se identifica con un elemento de M, de forma conocida. Si B quiere enviar el mensaje m a A, calcula $f(m)$ y se lo envía a A. Recordemos que es computacionalmente sencillo calcular la imagen de m por f y la función f es conocida por todos los usuarios. Cuando A recibe $f(m)$, puede usar su clave secreta, (gracias a la *trampa* que solo A conoce), para recuperar m. Cualquier otro usuario, que esté observando en la red, puede interceptar el mensaje y conocer $f(m)$, pero le será imposible recuperar m a partir de $f(m)$, en un tiempo asumible, sin conocer la *trampa*.

Existen varias funciones de una vía conocidas en matemáticas. Una de ellas se basa en el conocido como problema del logaritmo discreto en grupos, que es utilizada por Diffie y Helman en la propuesta de un protocolo de intercambio de clave. Estos protocolos permiten a dos usuarios intercambiar una clave segura a través de un canal inseguro.

Notemos que el intercambio de clave es el proceso más sensible en el uso de esquemas de clave privada. El protocolo expuesto por Diffie y Hellman en su influyente trabajo tiene los siguientes pasos:

Paso 1. A y B seleccionan un grupo multiplicativo finito $\boldsymbol{G}$ y un elemento suyo $\boldsymbol{g}$ (ambos públicos).

Paso 2. A genera aleatoriamente un entero positivo s, calcula $\boldsymbol{g}^s$ y se lo envía a B.

Paso 3. B genera aleatoriamente un entero positivo r, calcula $\boldsymbol{g}^r$ y se lo envía a A.

Paso 4. A, que ha recibido $\boldsymbol{g}^r$, calcula $(\boldsymbol{g}^r)^s$ en $\boldsymbol{\mathcal{G}}$.

Paso 5. B, que ha recibido $\boldsymbol{g}^s$, calcula $(\boldsymbol{g}^s)^r$ en $\boldsymbol{\mathcal{G}}$.

Al final del proceso A y B comparten un elemento secreto común, el elemento $\boldsymbol{g}^{sr} = \boldsymbol{g}^{rs}$ de $\boldsymbol{\mathcal{G}}$. Cualquier otro usuario que intercepte la comunicación a través del canal conoce los elementos $\boldsymbol{g}^s$ y $\boldsymbol{g}^r$. Pero no sabe cómo recuperar s (o r) a partir de ellos y por tanto no puede calcular $\boldsymbol{g}^{sr}$. Este problema no es difícil en todos los grupos, por tanto, el grupo $\boldsymbol{\mathcal{G}}$ tiene que elegirse de modo adecuado.

Por ejemplo, si $\boldsymbol{\mathcal{G}}$ es el grupo multiplicativo de los enteros no nulos módulo un primo p, es decir, es el grupo multiplicativo del cuerpo de Galois con p elementos, entonces se sabe que el problema es computacional difícil si p es suficientemente grande. De nuevo aparece la importancia de los cuerpos finitos. Aunque más adelante se propuso usar, en lugar del grupo multiplicative de un cuerpo finito, el grupo aditivo ligado a una curva elíptica, con el fin de conseguir cifrados más eficientes, los cuerpos finitos siguen teniendo un gran protagonismo, dado que las curvas elípticas son curvas sobre un cuerpo finito. Y por supuesto, esta nueva propuesta obliga a utilizar técnicas matemáticas más sofisticadas.

Este problema (encontrar un algoritmo eficiente que permita calcular $\boldsymbol{g}^{ab}$ a partir del grupo $\boldsymbol{\mathcal{G}}$, $\boldsymbol{g}^a$ y $\boldsymbol{g}^b$) se conoce como problema de Diffie-Hellman. Este problema está relacionado con el problema del logaritmo discreto: encontrar un algoritmo eficiente que permita encontrar el entero a conociendo el grupo $\boldsymbol{\mathcal{G}}$, y los elementos $\boldsymbol{g}$ y $\boldsymbol{g}^a$.

Hasta la fecha ambos problemas son intratables (con un ordenador clásico) y se conjetura que son computacionalmente equivalentes.

Solo dos años después de la aparición del trabajo de Diffie y Hellman con la sugerencia de utilizar funciones de una vía para construir esquemas de cifrado de clave pública, R. Rivest, A. Shamir y L. Adleman hicieron una propuesta concreta que llegaría a ser conocida internacionalmente por las iniciales de sus creadores, el esquema RSA.

El problema de una vía en el que se basa el RSA hunde sus raíces en cuestiones clásicas de la Teoría Algebraica de Números y que es bien conocido desde la escuela, la dificultad de factorizar un número "*grande*" en sus factores primos.

Para construir la clave en un esquema RSA el usuario A debe seguir los siguientes pasos: En primer lugar A elige dos primos p y q y calcula $n = pq$. En consecuencia, tanto A como los usuarios que quieran mandar un mensaje a A van a trabajar en el anillo $\mathbb{Z}_n$, de las clases de restos módulo n. Sus unidades (elementos que admiten inverso respecto a la multiplicación) forman un grupo $\mathbb{Z}_n^*$ cuyo orden es la denominada función de Euler de n, $\phi(n) = (p-1)(q-1)$ (la función de Euler de un número n es el número de enteros menores que n y relativamente primos con n).

Por tanto, es fácil calcular la función de Euler de un número n si conocemos su factorización en primos, pero es computacionalmente imposible hacerlo en otro caso). Notemos que A puede calcular fácilmente el orden del grupo de las unidades $\mathbb{Z}_n^*$ puesto que conoce la factorización de n. Sin conocer dicha factorización, calcular el orden del grupo de las unidades $\mathbb{Z}_n^*$ es un problema tan complicado como factorizar n, es decir, requiere un tiempo que puede ser inasumible. Para asegurarse de que la clave es segura, hay que elegir adecuadamente los primos p y q, que deben tener al menos 300 dígitos y cumplir una serie de propiedades.

En segundo lugar, el usuario A escoge un entero positivo e, $1 < e < \phi(n)$ y relativamente primo con $\phi(n)$.

Usando el algoritmo euclídeo de la división es fácil encontrar el inverso multiplicativo de e en Z_n*, es decir, encontrar el único elemento d, $1 < d < \phi(n)$ que cumple que $ed = 1 + t\,\phi(n)$.

La clave pública de A es el par (n, e) y la clave secreta (que le va a permitir a A recuperar los mensajes) es d.

Ambos problemas, factorizar un natural n que es producto de dos primos grandes y el problema de encontrar el inverso de un elemento arbitrario e de $\mathbb{Z}_n^*$ tienen la misma dificultad computacional. Son problemas de una vía equivalentes y en ambos casos, la trampa es el conocimiento de la factorización de n. Si conocemos la factorización de n conocemos $\phi(n)$ y también podemos encontrar el inverso de cualquier elemento de $\mathbb{Z}_n^*$ con una sencilla aplicación del algoritmo euclídeo de la división.

Veamos cómo se realizan los procesos de cifrado y de descifrado:

Cifrado: Cada mensaje m a enviar se identifica con un número menor que n, siendo (n, e) la clave secreta de A, usando un procedimiento que es conocido, de antemano, por todos los usuarios. Para cifrar el mensaje, se calcula la potencia m^e y se halla su resto módulo n. Es decir, el texto cifrado es c, $c = m^e \mod n$.

Descifrado: El usuario A recibe el texto cifrado c. Para descifrarlo solo tiene que calcular c^d, siendo d su clave privada, puesto que conocemos, por teoría elemental de números, que $c^d = (m^e)^d = m$, por ser e y d inversos en el grupo $\mathbb{Z}_n^*$.

ElGamal propuso, en 1985, un esquema de clave pública que se basa en el problema del logaritmo discreto en el grupo cíclico multiplicativo de un cuerpo finito $\mathbb{Z}_p$, siendo p un primo.

De nuevo los mensajes se identifican con enteros positivos menores que p y se elige un generador g del grupo multiplicativo $\mathbb{Z}_p^*$.

Cada usuario, sea A, elige aleatoriamente un entero positivo a, que va a constituir su clave privada, mientras que la clave pública es g^a. Si otro usuario le quiere enviar un mensaje m al usuario A, primero escoge aleatoriamente un número μ y calcula el elemento g^μ en $\mathbb{Z}_p^*$. Luego, usando la clave pública de A, g^a, calcula los elementos de $\mathbb{Z}_p^*$ siguientes: $(g^a)^\mu$ y $m(g^a)^\mu$. Y envía a A el par $(g^\mu, m\, g^{a\mu})$.

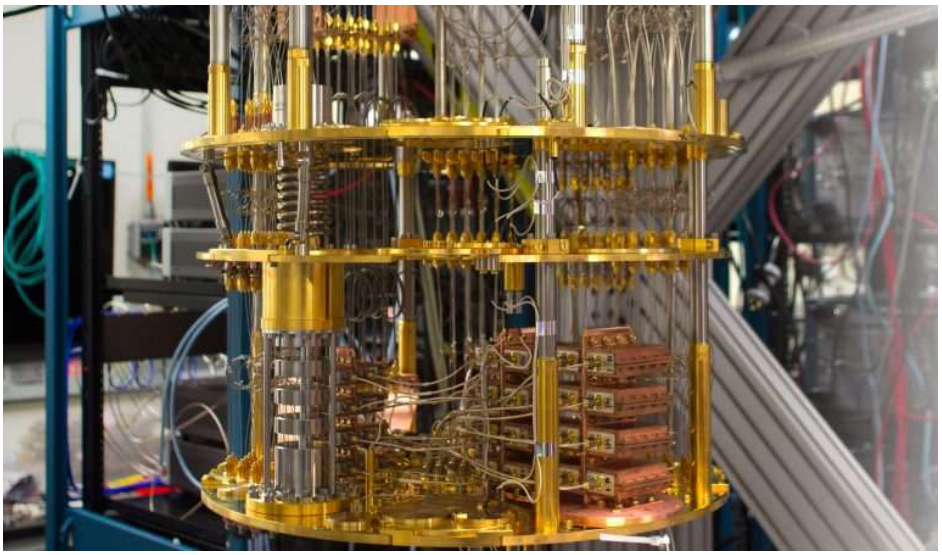
Para descifrar el mensaje A utiliza su clave privada a y calcula el elemento $(g^\mu)^a = g^{a\mu}$. Luego, simplemente necesita calcular $(m\, g^{a\mu})(g^{a\mu})^{-1}$.

Descifrar el mensaje sin conocer la clave privada (es decir, a), requiere resolver el problema del logaritmo discreto en el grupo $\mathbb{Z}_p^*$ y, como ya hemos señalado, si p es suficientemente grande, este es un problema muy costoso computacionalmente (usando un ordenador clásico).

El uso de la criptografía de clave pública permitió también el desarrollo de esquemas de firma digital. Tanto el esquema RSA como ElGamal tienen sus correspondientes esquemas de firma digital asociados. Además, como se ha indicado, se tienen esquemas de intercambio de clave, entre dos o varios usuarios, lo que permite intercambiar una clave privada a través de un esquema de intercambio de clave y luego continuar la comunicación usando un esquema de clave privada, con la clave intercambiada. Notemos que los esquemas de clave privada son más rápidos y eficientes que los de clave pública.

Pero cuando se tenía casi una situación idílica en el ámbito de la criptografía con esquemas seguros, variados y eficientes, un nuevo actor ha entrado en escena generando una notable preocupación. Se trata de la anunciada y posible aparición del ordenador cuántico. Durante un tiempo, su existencia parecía ciencia-ficción, pero hoy en día es ya una realidad, si bien se necesita mejorar su capacidad. Sin embargo, la necesidad de prepararse para la existencia de ordenadores cuánticos que representen una amenaza real para los esquemas actuales de cifrado es cada vez más acuciante, debido a que ya se conocen algoritmos cuánticos que permitirían, con un ordenador cuántico de la capacidad necesaria, romper los esquemas de cifrado de clave pública más utilizados actualmente.

En efecto, ya en 1984, Peter Shor encontró un algoritmo cuántico de factorización que requiere, para su ejecución, tiempo polinomial en el tamaño del número que se desea factorizar, a diferencia de los algoritmos 'clásicos' en los que el tiempo de ejecución crece exponencialmente. La primera consecuencia de este algoritmo es que se rompería la seguridad del RSA si alguien dispone del ordenador cuántico adecuado. En el mismo trabajo aparece un algoritmo para la resolución del problema del logaritmo discreto, cuyo tiempo de ejecución crece polinomialmente con el tamaño del grupo. Por tanto, los criptosistemas basados en ElGamal se verían afectados del mismo modo que el RSA ante la presencia de un ordenador cuántico.



Ordenador cuántico

Esta es la causa del auge actual de la denominada criptografía postcuántica, pues es indudable que se necesitan esquemas de cifrado que sigan siendo seguros frente a los ordenadores cuánticos, esquemas que se denominan esquemas postcuánticos. No parece viable encontrar un problema algorítmico cuya seguridad frente a ataques cuánticos sea demostrable. Al igual que sucede en el caso clásico, los esfuerzos se centran en encontrar problemas algorítmicos aparentemente seguros frente al ordenador cuántico, es decir, se cree que son seguros porque han resistido todos los ataques sufridos hasta el momento.

Basados en argumentos de complejidad teórica, los expertos creen que los problemas NP-duros son resistentes frente a ataques con un ordenador cuántico.

La clase de problemas de decisión que se pueden resolver en tiempo polinomial usando una máquina de Turing determinista se llama clase P. La clase de problemas de decisión que se pueden resolver en tiempo polinomial usando una máquina de Turing no determinista se denota NP.

Un importante problema abierto es el de saber si las clases P y NP coinciden o no. Este problema es uno de los que aparece en la lista de la Fundación Clay de los llamados problemas del millón de dólares.

Los problemas NP-completos son los problemas más difíciles de la clase NP. Los problemas NP-completos son NP-duros, es decir, cualquier problema en la clase NP se puede reducer, en tiempo polynomial, a cualquier problema NP-duro. Dicho de otro modo, un problema NP duro es, al menos, tan difícil como cualquier NP-problema. Además, se sabe que hay problemas NP-duros que no son NP.

La comunidad criptográfica se ha centrado en buscar problemas NP-duros en los que puedan basarse esquemas de cifrado postcuánticos. Muchas de las propuestas se han quedado en el camino hacia la consecución de estándares de esquemas de cifrado y de firma digital postcuánticos promovido por el NIST. Otros han conseguido sobrevivir a las distintas fases del proceso y se siguen buscando esquemas que mejoren las propuestas existentes y sigan mostrando resistencia a ataques con ordenadores cuánticos.

Algunos de los esquemas que parecen más prometedores están basados en problemas conectados con estructuras algebraicas.

1. Criptografía basada en retículos

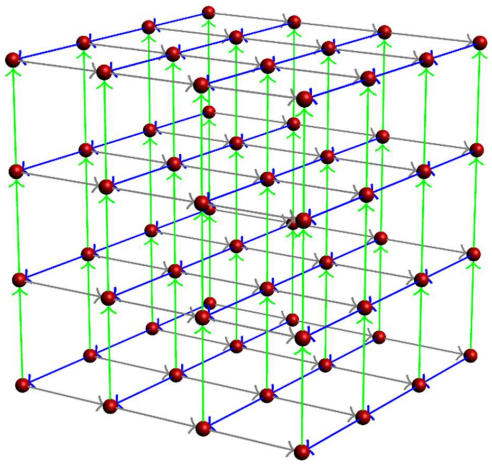
Los retículos son estructuras ligadas al espacio vectorial real de dimension n, $\mathbb{R}^n$. Si fijamos k un entero positive, menor o igual que n, y $b_1, b_2, \dots, b_k$ vectores (es decir, n-tuplas de números reales) linealmente independientes, podemos construir la matriz $B = (b_1, b_2, \dots, b_k)$ con n filas y k columnas y cuyas columnas son precisamente los vectores $b_1, b_2, \dots, b_k$ fijados. El retículo $L = L(B)$ es el conjunto de todas las combinaciones lineales enteras de los elementos $b_1, b_2, \dots, b_k$, es decir,

$$L(B) = \left\{ \sum_{i=0}^{k} x_i \, b_i \;\middle|\; x_i \in \mathbb{Z} \right\}.$$

La matriz B se llama base de $L(B)$. Pero podemos fijar otra familia de vectores linealmente independientes, obteniendo otra matriz distinta (aunque con el mismo número de filas y columnas) y de modo que el correspondiente retículo siga siendo $L(B)$. De hecho, si $k > 1$, el retículo $L(B)$ tiene infinitas bases. Cualquier matriz BT, dónde T es una matriz de tamaño k con elementos enteros y determinante 1 o -1 (en lenguaje matemático, T es un elemento del grupo general lineal $GL_k(\mathbb{Z})$) es una base del retículo $L(B)$ y todas sus bases tienen esta forma.

Por tanto, en la teoría de retículos aparecen también los espacios vectoriales y los grupos.

Pensemos que si $k = 2$, los elementos de un retículo dibujan una red en el plano afín. Si $k = 3$, tendríamos una red espacial. El entero k es la dimension del retículo $L(B)$.



Retículo tridimensional

En teoría de retículos se conocen varios problemas que son NP-duros. El que se usa en criptografía es el llamado problema del vector más corto, SVP de sus iniciales en inglés (*shortest vector problem*). Este problema plantea la búsqueda, de un vector no nulo de un retículo $L(B)$ dado, cuya norma (usualmente euclídea) sea minimal.

Otro problema, relacionado con el anterior, es el del vector más cercano, CVP (*closest vector problem*) abreviadamente. En este caso, fijado un vector $\boldsymbol{w}$ de $\mathbb{R}^n$, se trata de encontrar otro vector $\boldsymbol{v}$ en L de forma que la distancia de $\boldsymbol{v}$ a $\boldsymbol{w}$ sea minimal. Este problema es también NP-duro. Un inconveniente de los esquemas basados en retículos es que los problemas que se usan en criptografía no son los dos problemas mencionados, que se sabe que son NP-duros, sino los problemas denominados αSVP y αCVP, siendo α una función definida sobre los enteros positivos y que toma valores en los números reales mayores o iguales a 1. Supongamos que $\boldsymbol{v}$ es uno de los vectores más cortos del retículo L, y llamamos λ a su longitud. Entonces el problema αSVP busca un vector en el retículo cuya longitud sea a lo sumo $\alpha(k)\,\lambda$. Análogamente, el problema αCVP busca un vector $\boldsymbol{u}$ que cumpla: $d(\boldsymbol{u},\boldsymbol{w}) \leq \alpha(k)\min d(\boldsymbol{t},\boldsymbol{w})$, cuando $\boldsymbol{t}$ recorre el retículo $L = L(B)$.

El problema de reducción de base de un retículo es otro problema importante. Su objetivo es encontrar una base B' de $L(B)$ formada por *vectores cortos* (fijados n, k y B). Hay distintos tipos de reducciones, existiendo algoritmos que ejecutan la reducción en tiempo polinomial, como es el caso en el algoritmo diseñado por Lenstra, Lenstra y Lovács (LLL-reducción).

Los algoritmos más eficientes que existen para resolver los problemas αSVP y αCVP realizan, en primer lugar, un proceso de reducción de base. De ahí su importancia.

La idea subyacente al diseño de esquemas basados en retículos es simple. Se selecciona un retículo $L(B)$ y se identifican los mensajes en claro con elementos de B. Para cifrar el mensaje $\boldsymbol{v}$ se toma un vector muy corto $\boldsymbol{e}$ de $\mathbb{R}^n$ y se cifra $\boldsymbol{v}$ como $\boldsymbol{v} + \boldsymbol{e} = \boldsymbol{c}$. Para descifrar $\boldsymbol{c}$ necesitamos resolver el problema CVP con $\boldsymbol{c}$, es decir, el vector del retículo más cercano a $\boldsymbol{c}$ proporciona el mensaje original $\boldsymbol{v}$.

Desafortunadamente, para conseguir esquemas de cifrado seguro hay que modificar los problemas de retículos en los que se basa, por lo que ya no tenemos la certeza de estar usando un problema NP-duro para diseñar el esquema. Además, se suele introducir estructura extra en el retículo, con el objetivo de reducir la longitud de clave y mejorar la eficiencia. Es el caso de KYBER, reciente ganador de una competición postcuántica del NIST, que hace uso del *aprendizaje con errores basado en módulos*. De nuevo las estructuras algebraicas aparecen jugando un papel esencial.

Los esquemas basados en retículos son prometedores, permiten conseguir implementaciones sencillas y tanto el tiempo de cálculo como el espacio de almacenamiento son pequeños. Por otra parte, se les puede aplicar la reducción del caso peor al caso medio, lo que es una importante propiedad. Para entender lo que significa, pensemos en el esquema RSA. Si se quiere construir una instancia de dicho esquema (una realización particular), tenemos que elegir la clave pública, es decir, el par (n, e), con cuidado. Puesto que el RSA ha sido extensamente estudiado, se sabe cómo hay que hacer esta elección para obtener un esquema seguro, pues no todas las elecciones de la clave producen la seguridad que se espera. Por ejemplo, n debe ser producto de dos números primos aleatorios, con aproximadamente el mismo número de dígitos. Pero esto no ocurre siempre. Desconocemos cómo se debe hacer la elección de la clave privada para tener un esquema seguro en muchos casos. Pero si un esquema tiene la propiedad de que se le puede aplicar la reducción de caso peor al caso medio, no tenemos que preocuparnos por como elegimos la clave privada de una instancia concreta. Si el problema algorítmico en el que se basa es un problema NP-duro, cualquier elección de la clave nos permite conseguir un esquema seguro.

Además, algunos de los esquemas de cifrado basados en retículos son cifrados homomórficos, por lo que se puede operar con textos cifrados: la suma del cifrado de dos textos es el cifrado de la suma de ellos y análogamente para el producto.

2. Esquemas basados en códigos correctores

Existen también propuestas de esquemas de cifrado postcuántico basados en códigos correctores. La primera de ellas la hizo McEliece en 1976 y permanece siendo segura a día de hoy, a pesar de los múltiples ataques que se han diseñado para romperla. Este esquema se considera también seguro frente a ataques con un ordenador cuántico y ha sido finalista y candidato a la cuarta ronda de la competición postcuántica del NIST.

Veamos, en líneas generales, como son estos esquemas.

Para empezar, necesitamos un (n, k)-código lineal $\mathfrak{C}$ sobre un cuerpo finito $\mathbb{F}$. Para ello necesitamos conocer una matriz generadora suya, $\mathcal{G}$, que nos permita una descodificación rápida y eficiente. Se seleccionan aleatoriamente, con una distribución uniforme, dos matrices $\mathcal{S}$ y $\mathcal{P}$ cuyos elementos están en el cuerpo $\mathbb{F}$, siendo $\mathcal{S}$ una matriz cuadrada, regular con k filas y $\mathcal{P}$ una matriz permutación, es decir, una matriz cuadrada de n filas en la que cada fila y cada columna tienen un 1 y todos los demás elementos son 0.

Estas dos matrices sirven para camuflar $\mathcal{G}$ en la matriz $\mathcal{G}' = \mathcal{S}\mathcal{G}\mathcal{P}$ lo que nos permite trabajar con el código lineal $\mathfrak{C}'$ que tiene $\mathcal{G}'$ como matriz generadora. Este nuevo código $\mathfrak{C}'$ comparte algunas propiedades del código $\mathfrak{C}$, pero tiene la apariencia de un código lineal arbitrario. Finalmente, se toma como clave publica el par $(\mathcal{G}', t)$, siendo t la capacidad correctora del código $\mathfrak{C}$, mientras que la clave privada está integrada por las matrices $\mathcal{G}$, $\mathcal{S}$ y $\mathcal{P}$.

Los mensajes se identifican con vectores de $\mathbb{F}^k$ y se cifran como vectores de $\mathbb{F}^n$.

Para cifrar un mensaje $m \in \mathbb{F}^{\mathrm{k}}$, se elige un vector aleatorio $e \in \mathbb{F}^{\mathrm{n}}$ de peso menor o igual a t, la capacidad correctora del código $\mathfrak{C}$, y el texto cifrado se calcula como $c = m\mathcal{G}' + e$.

Para descifrar el mensaje cifrado, el receptor legítimo del mismo usa la clave privada que conoce. Puesto que conoce $\mathcal{P}$, puede calcular $\mathcal{P}^{-1}$ (de forma muy simple para las matrices permutación). Así computa:

$$x = c\,\mathcal{P}^{-1} = (m\mathcal{G}' + e)\,\mathcal{P}^{-1} = m\mathcal{S}\mathcal{G} + e\,\mathcal{P}^{-1}.$$

Puesto que $\mathcal{P}$ es una matriz permutación, las palabras $e\,\mathcal{P}^{-1}$ y e tienen ambas peso t.

Por tanto, se ha reducido el problema de descifrado de un texto (un problema de criptografía) a un problema de descodificación con un código lineal (un problema de códigos correctores de errores). Tenemos un código lineal con matriz generadora $\mathcal{G}'' = \mathcal{S}\mathcal{G}$, con capacidad correctora t, se ha enviado un mensaje m, se han producido a lo sumo t errores y recibimos x. El objetivo es descodificar para recuperar m. El problema de descodificación, sin conocer la clave privada de un código lineal, aparentemente arbitrario, del que solo conocemos su matriz generadora $\mathcal{G}''$, se supone que es un problema intratable en un tiempo aceptable. Pero si se conoce la clave privada, se puede transformar el problema en otro de descifrado en el código lineal bueno $\mathfrak{C}$. Se ha enviado el mensaje $\boldsymbol{m}' = \boldsymbol{m}\mathcal{S}$, se han producido a lo sumo t errores en el proceso se necesita recuperar $\boldsymbol{m}'$. Pero para el código $\mathfrak{C}$ se conoce un algoritmo eficiente de descodificación y, por tanto, se puede recuperar $\boldsymbol{m}'$. Para obtener $\boldsymbol{m}$ solo hay que calcular $\boldsymbol{m}'\mathcal{S}^{-1}$.

En la propuesta de McEliece se trabaja con códigos Goppa binarios, que se construyen a partir de un polinomio, lo que condiciona algunas propiedades del código. Para estos códigos existe una matriz generatriz $\mathcal{G}$ que permite una descodificación muy eficiente, que se puede construir a partir del polinomio ligado al código. El esquema de McEliece, para el cual existe también un esquema de firma digital, es rápido, pero su principal problema es la longitud de las claves. Ha habido varias propuestas posteriores de esquemas con la misma estructura, pero usando otro tipo de códigos correctores para los que también se conocen algoritmos eficientes de descodificación. Sin embargo, ninguna de ellas ha sobrevivido a los ataques de criptoanálisis sufridos. Por ello se sigue trabajando en esta línea, buscando alternativas viables a la propuesta de McEliece.

En nuestro grupo de investigación estamos explorando la posibilidad de que los códigos grupo, que hemos comentado anteriormente, puedan permitir el diseño de un esquema eficiente del tipo McEliece. Para ello, por una parte, estamos buscando algoritmos eficientes de descodificación y por otra parte, estamos estudiando propiedades de códigos grupos que permitan identificarlos eficientemente entre los códigos lineales.

Las matemáticas han ocupado mi vida, de un modo u otro, durante los últimos 50 años y me han dado muchísimo a cambio. De hecho, me considero en deuda con ellas y sigo sintiendo la misma pasión que el primer día. Espero haber sido capaz de mostrarles una parte de la belleza y elegancia del edificio de las matemáticas. Y hemos podido vislumbrar el ala que aloja la disciplina de álgebra. Para entrar en ella, hay que aceptar unas normas: esfuerzo, rigor, precisión, abstracción. Pero si se logra, la recompensa merece la pena, pues nos sentiremos deslumbrados por su belleza.

Muchas gracias a todos por su atención.

8. Referencias

[1] Ajtai, M. (1996). Generating hard instances of lattice problems. *Proceedings of the Twenty-eight Annual ACM Symposium on Theory of Computing*. STOC'96: 99-108.

[2] Bai, S. and Galbraith, S. (2014). An improved compression technique for signatures base learning with errors. *Topics in Cryptology*, Lecture Notes in Computer Science 8366: 28-47.

[3] Bai, S. and Galbraith, S. (2014). Lattice decoding attacks on binary LWE. *Information Security and Privacy*, Lecture Notes in Computer Science 8544: 322-337.

[4] Barreiro, E.; Elduque, A.; Martínez, C. (2011). Derivations of the Cheng-Kac Jordan superalgebras. *J. Algebra* 338: 144–156.

[5] Benkart, G.; Elduque, A.; Martínez, C. (2004). A(n,n)-graded Lie superalgebras. *J. Reine Angew. Math.* 573: 139–156.

[6] Bennett, C.H., Bernstein, E., Brassard, G. and Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *SIAM J. Comput.* 26 (5): 1510-1523.

[7] Bernstein B.J. (2009). Introduction to post-quantum cryptography. In: Bernstein, D., Buchmann, J. and Dahmen E. (eds.) *Post-Quantum Cryptography*, Springer, Heidelberg, 1-11.

[8] Bernstein, D., Lange, T., Peters, C. and Schwabe, P. (2011). Faster 2-regular information-set decoding. *Coding and Cryptology*, Lecture Notes in Computer Science 6639: 81-98.

[9] Bohli, Jens-Matthias; Steinwandt, Rainer; González Vasco, María Isabel; Martínez, Consuelo. (2005). Weak keys in MST1. *Des. Codes Cryptogr.* 37 (2005), no. 3: 509–524.

[10] Boneh, D. (1999). Twenty years of Attacks on the RSA Cryptosystem. *Notices Amer. Math. Soc*. 46: 203-213.

[11] Boyar, J. (1989). Inferring Secuences Produced by Pseudorandom Number generators. *J. ACM.* 36: 129-144.

[12] W. Burnside, (1902) On an unsettled Question in the Theory of Discontinuous groups. Q.J. Pure Appl. Math. 33: 230-238.

[13] Chambers, W. G. and Gollmann, D. (1988). Generators for Sequences with Near-Maximal Linear Equivalence. *LEE Proceedings* 135: 67-69.

[14] Couselo, E.; González, S.; Markov, V.; Martínez, C.; Nechaev, A. (2010). Some constructions of linearly optimal group codes. *Linear Algebra Appl.* 433, : 356–364.

[15] Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Trans. Infor. Th*eory 22: 644-654.

[16] Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE* 76 (5): 560-577.

[17] ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Trans. Inform. Theory* 31: 469-472.

[17] Fuster-Sabater, A., De la Guía, D., Hernandez-Encinas, L., Montoya F. y Muñoz M, J. (2004). *Técnicas Criptográficas de Protección de Datos*. Ra-Ma, Madrid.

[19] García-Pillado, C.; González, S.; Martínez, C.; Markov, V.; Nechaev, A. (2013). Group codes over non-abelian groups. *J. Algebra Appl.* 12 (2013), no. 7, 1350037, 20 pp.

[20] García-Pillado, C.; González, S.; Markov, V.; Martínez, C.; Nechaev A.; (2016). New examples of non-abelian group codes. *Adv. Math. Commun.* 10, no. 1: 1-10.

[21] García-Pillado, C.; González, S.; Markov, V.; Markova, O.; Martínez, C. (2019). Group codes of dimension 2 and 3 are abelian. *Finite Fields Appl.* 55: 167–176.

[22] Garey, M.R. and Johnson, D.S. (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman, San Francisco.

[23] E. S. Golod (1964). On Nil-algebras and Residually Finite *p*-groups. *Izv. Akad. Nauk SSSR, Ser. Mat.* 28: 272-276.

[24] González, S.; Huguet, Ll.; Martínez, C.; Villafañe, H. (2013). Discrete logarithm like problems and linear recurring sequences. *Adv. Math. Commun.* 7, no. 2: 187–195.

[25] González, S.; Martínez, C. (1990). Periodic Jordan rings and order strutture. *Comm. Algebra* 18, no. 7: 2021–2037.

[26] González, S.; Martínez, C. (1989) Periodic associative rings and order structure. *Algebras Groups Geom.* 6, no. 4: 409–420.

[27] González, S.; Martínez, C. (1988). Order relation in quadratic Jordan rings and a structure theorem. *Proc. Amer. Math. Soc.* 98, no. 1: 51–54.

[28] González, S.; Martínez, C. (2003). Nonassociative algebras: some applications. *Rev. Mat. Iberoamericana* 19, : 385–392.

[29] González, S.; Martínez, C.; Rúa, I. F.; Markov, V. T.; Nechaev, A. A. (2004). Coordinate sets of generalized Galois rings. *J. Algebra Appl.* 3, no. 1: 31–48.

[30] González, S.; Martínez, C.; Markov, V. T.; Nechaev, A. A.; Rúa, I. F.(2005). Cyclic generalized Galois rings. *Comm. Algebra* 33, no. 12: 4467–4478.

[31] González, S.; Markov, V. T.; Martínez, C.; Nechaev, A.; Rúa, I. F. (2004). On cyclic top-associative generalized Galois rings. *Lecture Notes in Comput. Sci., 2948, 25-29.* Springer, Berlin.

[32] González, S.; Martínez, C.; Rúa, I. F. (2007). Symplectic spread-based generalized Kerdock codes. *Des. Codes Cryptogr.* 42, no. 2: 213–226.

[33] González-Vasco, M. I.; Hofheinz, D.; Martínez, C.; Steinwandt, R. (2004). On the security of two public key cryptosystems using non-abelian groups. *Des. Codes Cryptogr.* 32, no. 1-3: 207–216.

[34] González -Vasco, M. I.l; Martínez, C.; Steinwandt, R. (2004). Towards a uniform description of several group based cryptographic primitives. *Des. Codes Cryptogr.* 33, no. 3: 215–226.

[35] González -Vasco, M. I.; Martínez, C.; Steinwandt, R.; Villar, J. L. (2005). A new Cramer-Shoup like methodology for group based provably secure encryption schemes. *Lecture Notes in Comput. Sci.*, 3378, 495-509. Springer, Berlin.

[36] González-Vasco, M. I.; González, S.; Martínez, C.; Suárez Corona, A. (2018). The roll of dices in cryptology. *The Mathematics of the Uncertain,* 493–504, Stud. Syst. Decis. Control 142, Springer, Cham.

[37] González-Vasco, M. I.; Steinwandt. R. (2015). *Group Theoretic Cryptography*. Chapman and Hall https://doi.org/10.1201/b18272.

[38] Hall, M. (1958). Solution of the Burnside Problem for Exponent Six. *Illinois J. Math.* No. 2: 764-786.

[39] Hall, P.; Higman, G. (1956). On the p-length of p-soluble groups and Reduction Theorems of Burnside's Problem. *Proc. London Math. Soc*. 6: 1-42.

[40] Hellman, M. (1979). The mathematics of public-key cryptography. *Scientific American* 24: 130-139.

[41] Heyse, S., Maurich, von I. and Güneysu, T. (2013). Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices. *Cryptographic Hardware and Embedded Systems*, Lecture Notes in Computer Science 8086: 273-292.

[42] Jordan, P.; von Newman, J.; Wigner, E. (1934). On an algebraic generalization of the quantum mechanical formalism. *Annals of Math.* (2) no. 36: 29-64.

[43] Jacobson, N. (1964). *Structure and Representation of Jordan Algebras*. American Mathematical Society, Providence, R.I.

[44] Jacobson, N. (ed.) (1983) *Emmy Noether: Collected Papers.* Springer-Verlag.

[45] Kac, V. (1977). Lie Superalgebras. *Adv. Math.,* 27: 8-96.

[46] Kac, V. (1977). Classification of Simple Z-graded Lie Superalgebras and Simple Jordan Superalgebras. *Comm. Algebra* 5: 1375-1400.

[47] Kac, V.; Martínez, C.; Zelmanov, E. (2001). Graded simple Jordan superalgebras of growth one. *Mem. Amer. Math. Soc.* 150 , no. 711, x+140 pp.

[48] Kantor, I. L. (1992). Jordan and Lie superalgebras determined by a Poisson algebra. *Amer. Math. Soc. Trans.* (2), no. 151: 55-79.

[49] Kaplansky, I. (1980). Superalgebras. *Pacific J. Math*. 86: 93-98.

[50] Khan, D. (1996). *The Codebreakers*. Scribner, New York.

[51] Kleiner, I. (2007). *A History of Abstract Algebra*. Birkhäuser, Boston –Basel- Berlin.

[52] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computatio*n 48 (177): 203-209.

[53] Kostrikin, A.I. (1957). On the Connection Between Periodic Groups and Lie Rings. *Izv. Akad. Nauk SSSR, Ser. Mat.* 21: 289-310.

[54] Kostrikin, A.I. (1959). The Burnside Problem. *Izv. Akad. Nauk SSSR, Ser. Mat.* 23: 3-34.

[55] Lenstra, A., Lenstra, J. and Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261 (4): 515-534.

[56] Lyubashevsky, V., Peikert, C. and Regev, O. (2010). On ideal lattices and learning with errors over rings. *Advances in Cryptology, Eurocrypt 2011*, Lecture Notes in Computer Science 6110: 1-23.

[57] Mann, Avinoam; Martinez, C. (1996). The exponent of finite groups. *Arch. Math. (Basel)* 67 (1996), no. 1: 8–10.

[58] Mann, Avinoam; Martinez, C. (1998). Groups nearly of prime exponent and nearly Engel Lie algebras. *Arch. Math. (Basel)* 71, no. 1: 5–11.

[59] Markova, O. V.; Martínez, C.; Rodrigues, R. L. (2022). Algebras of length one. *J. Pure Appl. Algebra* 226, no. 7, Paper No. 106993, 16 pp.

[60] Martínez, J.; Martínez C. (2017). A computational approach to verbal width in alternating groups. *Computational mathematics, numerical analysis and applications,* 241–244, Springer Ser., 13, *Springer, Cham.*

[61] Martínez, J.; Martínez, C. (2021). Verbal width in the Nottingham group and related Lie algebras. *J. Algebra* 574: 16–326.

[62] Martínez, C. (1983). Estructura de Sylow de ciertos grupos localmente finitos. *Rev. Real Acad. Cienc. Exact. Fís. Natur. Madrid* 77 , no. 1: 173–180.

[63] Martínez, C. (1982). Formaciones producto de S-grupos. *Rev. Acad. Cienc. Zaragoza (2)* 36 (1981): 27–33.

[64] Martínez, C. (1994). On power subgroups of profinite groups. *Trans. Amer. Math. Soc.* 345, no. 2: 865–869.

[65] Martinez, C. (1996). Gel'fand-Kirillov dimension in Jordan algebras. *Trans. Amer. Math. Soc.* 348, no. 1: 119–126.

[66] Martinez, C. (1996). Power subgroups of pro-(finite soluble) groups. Bull. London Math. Soc 28, no. 5, 481–487.

[67] Martínez, C. (2003). Simplicity of Jordan superalgebras and relations with Lie structures. *Irish Math. Soc. Bull.* no. 50: 97–116.

[68] Martínez, C. (2005). On prime Z-graded Lie algebras of growth one. *J. Lie Theory* 15, no. 2: 505–520.

[69] Martínez, C. (2006). Infinite dimensional Lie and Jordan algebras. *Mediterr. J. Math.* 3, no. 2: 273–282.

[70] Martínez, C. (2017) Álgebra y supersimetría. *Gac. R. Soc. Mat. Esp.*20, no. 2: 399–416.

[71] Martínez, C. (2018). Ellipticity of words. *J. Algebra* 500: 242–252.

[72] Martínez, C.; Molina, F. (2023). The syndromes decoding algorithm in group codes. *Finite Fields Appl.* 89, Paper No. 102206, 17 pp.

[73] Martínez, C.; Shestakov, I.; Zelmanov, E. (2001). Jordan superalgebras defined by Brackets. *J. London Math Soc. (2),* 64: 357- 368.

[74] Martínez, C.; Shestakov, I.; Zelmanov, E. (2010). Jordan bimodules over the superalgebras P(n) and Q(n). *Trans. Amer. Math. Soc.* 362, no. 4: 2037–2051.

[75] Martínez, C.; Shestakov, I. (2020). Jordan bimodules over the superalgebra M1|1. *Glasg. Math. J.* 62, no. S1: S6–S13.

[76] Martinez, C.; Zelmanov, E. (1996). Jordan algebras of Gel'fand-Kirillov dimension one. *J. Algebra* 180 , no. 1: 211–238.

[77] Martinez, C.; Zelmanov, E. (1996). Products of powers in finite simple groups. *Israel J. Math.* 96, part B: 469–479.

[78] Martinez, C.; Zelmanov, E. (1997). Simple and prime graded Jordan algebras. *J. Algebra* 194, no. 2: 594–613.

[79] Martínez, C.; Zelmanov, E. (1999). Nil algebras and unipotent groups of finite width. *Adv. Math.* 147, no. 2: 328–344.

[80] Martínez, C.; Zelmanov, E. (2003). Lie superalgebras graded by P(n) and Q(n). *Proc. Natl. Acad. Sci. USA* 100, no. 14: 8130–8137.

[81] Martínez, C.; Zelmanov, E.. (2006). Unital bimodules over the simple Jordan superalgebra D(t). *Trans. Amer. Math. Soc.* 358, no. 8: 3637–3649.

[82] Martínez, C.; Zelmanov, E. (2009). Jordan superalgebras and their representations. *Algebras, representations and applications,* 179–194, Contemp. Math., 483, *Amer. Math. Soc., Providence, RI*.

[83] Martínez, C.; Zelmanov, E. (2010). Representation theory of Jordan superalgebras. I. *Trans. Amer. Math. Soc.* 362, no. 2: 815–846.

[84] Martínez, C.; Zelmanov, E. (2014). Irreducible representations of the exceptional Cheng-Kac superalgebra. *Trans. Amer. Math. Soc.* 366, no. 11: 5853–5876.

[85] Martínez, C.; Zelmanov, E. (2016). On Lie rings of torsion groups. *Bull. Math. Sci.* 6, no. 3: 371–377.

[86] Martínez, C.; Zelmanov, E. (2016). Graded modules over superconformal algebras. Springer Proc. Math. Stat., 160, 41-53. Springer, Cham.

[87] Martínez, C.; Zelmanov, E. (2019). Brackets, superalgebras and spectral gap. *São Paulo J. Math. Sci.* 13, no. 1: 112–132.

[88] Martinez, C.; Zelmanov, E. Jordan superalgebras. *Algebra and applications 1; Non-associative algebras and categories,* 1–25, *ISTE, London,* 2022.

[89] Martínez, C.; Zelmanov, E. (2023). Growth functions of Jordan algebras. *Non-associative algebras and related topics,* 171–183, Springer Proc. Math. Stat., 427, Springer, Cham.

[90] Massey, J. L., (1969). Shift-register sinthesis and BCH decoding. *IEEE Trans. Informat. Theory*, IT 15: 122-127.

[91] Matsuy, M. (1994). Linear Criptanalysis Methods for DES Ciphers. *Proc. Eurocrypt'93*, 386-397. Springer Verlag, Heidelberg.

[92] McEliece, R. J. (1978). A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report* 44: 114-116.

[93] McEliece, R. J. (1987). *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, Dordrecht.

[94] Meier, W. (1993). On the security of the IDEA Block Cipher. *Eurocrypt'93*: 371-385.

[95] Menezes, A. (1993). *Elliptic Curve Public Key Cryptosystem.* Kluwer Academic Publishers, Dordrecht.

[96] Menezes, A., Oorschoot, P. van and Vanstone, S. (1997). *Handbook of Applied Cryptography*. CRC Press, Boca Ratón.

[97] Merkle, R. C. (1979). *Secrecy, Authentication and Public Key Systems.* PhD. Thesis, Stanford University.

[98] Merkle, R.C. (1989). A certified Digital Signature. *Advances in Cryptology – CRYPTO 1989*, Lecture Notes in Computer Science 435: 218-238.

[99] Micciancio, D. (2001). The hardness of the closest vector problem with preporcessing. *IEEE Trans. Inform. Theory* 47 (3): 1212-1215.

[100] Misoczki, R., Tillich, J., Sendrier, N. and Barreto, P.S.L.M. (2013). MDPC-McEliece: New McEliece variants from moderate density parity-check codes. *Proceedings of ISIT, IEEE*: 2019-2073.

[101] National Bureau of Standars (NBS) (1977). *Data Encryption Standard*s. FIPS Publications 46, Washington, DC.

[102] National Institutes of Standards and Technology (NIST) (2001). *Advanced Encryption Standard, AES.* FIPS Publications 197, Washington DC.

[103] Nicolás, A. P.; Martínez, C.; Grassl, M. (2011). Fully ramified characters and Clifford codes. *Comm. Algebra* 39, no. 1: 100–115.

[104] Novikov, P.S. ; Adjan, S. I. (1968). Infinite Periodic Groups I, II, III. *Izv. Akad. Nauk SSSR, Ser. Mat.,* 32; 212-244; 251-524; 709-731.

[105] Persichetti, E. (2013). Secure and anonymous hybrid encryption from coding theory. *PQCrypto*, *Lecture Notes in Computer Science* 7932: 174-187.

[106] Petzoldt, A.; Bulygin, S.; Buchmann, J. (2010). Cyclic Rainbow: a multivariate signature scheme with a partially cyclic public key. *INDOCRYPT,* Lecture Notes in Computer Science 6498: 33-48.

[107] Peters, C. (2010). *Information–set decoding for linear codes over GF(q). Post-Quantum Cryptography,* Lecture Notes in Computer Science 6061: 81-90.

[108] Rabanal, F.; Martínez, C. (2020). Cryptography for big data environments: current status, challenges, and opportunities. *Comput. Math. Methods* 2, e1075, 12 pp.

[109] Racine, M.; Zelmanov, E. (2003). Classification of simple Jordan superalgebras with semisimple even part. *J. Algebra* 270(2): 374-444.

[110] Regev, O. (2005). On lattices, learning with errors, random linear codes and cryptography. *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing,* STOC'05: 84-93.

[111] Sanov, I. N. (1940). Solution of Burnside's Problem for Exponent Four. *Leningrad State Univ. Ann. Math. Ser*. 10: 166-170.

[112] Vasco, M.I. G.; Kharobaei, D.; McKemmie, E. (2024). Applications of Finite Non-abelian Simple Groups to Cryptography in the Quantum Era. *Matemática* 3(2): 588-603.

[113] van der Waerden, B. L. (1985). *A History of Algebra: from Al-Khwarizmi to Emmy Noether*. Springer-Verlag.

[114] Zelmanov, E. I. (1983). On prime Jordan algebras II. *Siberian Math. J.* 24: 73-85.

[115] Zelmanov, E. I. (1984). Lie Algebras with a finite grading. *Math. USSS Sbornik* 124: 353-392.

[116] Zelmanov, E. I. (1987). Engel Lie Algebras. *Dokl. Akad. Nauk SSSR* 292: 265-268.

[117] Zelmanov , E. I. (1989). On Some Problems of Group Theory and Lie Algebras. *Mat. Sb.* 180: 159-167.

[118] Zelmanov, E. I. (1991). The Solution of the Restricted Burnside Problem for Groups of Odd Exponent. *Izv. Math SSSR*, 36: 41-60.

[119] Zelmanov, E. I. (1991). The Solution of the Restricted Burnside Problem for 2- Groups. *Mat. Sb.* 183: 568-592.