Teoría de Representaciones de Grupos Finitos: Problemas locales

por

Gabriel Navarro

En este artículo, analizamos los principales problemas abiertos en la teoría local de representaciones de grupos finitos, así como ciertos refinamientos de los mismos realizados por el autor.

1 . Introducción

Después de la clasificación de los grupos finitos simples, gran parte de los problemas más relevantes en Teoría de Grupos Finitos están centrados en decidir si determinados invariantes de un grupo finito G pueden ser calculados localmente. Principalmente, estos problemas son:

(1) La conjeturas de McKay y Alperin-McKay.

(2) La conjetura de pesos de Alperin (AWC).

(3) Las conjeturas de Dade.

(4) La conjetura de Broué.

Hay otras conjeturas relacionadas de parecida importancia (como la conjetura $k(B)$ o la conjetura de la altura cero, ambas de R. Brauer) pero son de una naturaleza ligeramente distinta a las que aquí nos interesan.

Las conjeturas (1), (2), (3) y (4) están interrelacionadas. Por ejemplo, las conjeturas de Dade implican la conjetura de Alperin-McKay y la AWC (de hecho, fueron creadas con ese propósito; aunque al precio de ser más difíciles de estudiar). La conjetura de Alperin-McKay implica la de McKay; o la conjetura de Broué implica la de Alperin-McKay, pero sólo en determinados casos. En resumen, desearíamos tener sólo una conjetura, aunque de momento nadie ha dado con ella.

Se tiene la casi total certeza de que todas estas conjeturas son verdaderas. El número de familias de grupos para las que han sido probadas, o los datos experimentales dejan pocas dudas. Sin embargo, nadie tiene una explicación del porqué. La conclusión es que hay una parte fundamental de la Teoría de Representaciones de Grupos Finitos que está por descubrir.

Como en otras partes de las Matemáticas, la teoría de grupos finitos tiene conceptos locales y globales que deben ser relacionados. La teoría local de grupos finitos empieza con un primo p, fijo, que divide el **orden** $|G|$ de un grupo finito G. Los p**-subgrupos** de G son los subgrupos de orden una potencia de

p. Para cada potencia p^d que divide a $|G|$, el grupo G tiene p-subgrupos de orden p^d. Los p-subgrupos de **Sylow** P de G (aquellos que tienen orden la mayor potencia de p que divide a $|G|$) son los p-subgrupos más importantes, entre otros motivos, porque todo p-subgrupo está contenido en algún Sylow. En general, dos p-subgrupos de orden p^d tienen poca relación entre sí. Sin embargo, si P y Q son p-subgrupos de Sylow de G, entonces P y Q son conjugados en G; es decir, existe un elemento $g \in G$ tal que

$$P = Q^g = g^{-1}Qg\,.$$

Necesitamos saber cómo los p-subgrupos «viven» en G, y así consideramos los **subgrupos locales** de G. Estos son los **normalizadores** de los p-subgrupos $Q > 1$ de G; es decir, los subgrupos de la forma

$$\mathbf{N}_G(Q) = \{g \in G \mid Q^g = Q\}\,.$$

Así, nos interesan los p-subgrupos de G y los subgrupos más grandes de G en los que éstos son normales. Un subgrupo local distinguido es $\mathbf{N}_G(P)$, el normalizador de un p-subgrupo de Sylow P de G.

La principal idea de la teoría local de grupos finitos es: ¿Cuánto saben los subgrupos locales de G? ¿Cómo la estructura de G se refleja y es reflejada en sus subgrupos locales? El ejemplo perfecto de un teorema local es el teorema clásico de Frobenius: *un grupo finito G tiene un p-complemento normal si y sólo si sus subgrupos locales lo tienen*. (Un **p-complemento normal** Y de X es un subgrupo normal de X de orden no divisible por p y de **índice** $|X|/|Y|$ una potencia de p). Es decir, el teorema de Frobenius nos dice que si los subgrupos locales de G verifican cierta condición, entonces G tiene un subgrupo normal no trivial. En particular, G no es simple.

Por simplicidad, en este artículo nos centraremos en la conjetura de McKay. Las ideas que aquí exponemos, sin embargo, pueden y deben también aplicarse a todas las demás conjeturas.

Las **representaciones** complejas de un grupo G son los homomorfismos de grupos

$$\mathcal{X} : G \to \mathrm{GL}(m, \mathbb{C})\,.$$

De alguna manera, queremos conocer G a través de sus representaciones como grupos de matrices complejas. Las representaciones más sencillas son las **representaciones lineales** (cuando $m = 1$) y son simplemente los homomorfismos de grupos

$$\mathcal{X} : G \to \mathbb{C}^\times\,.$$

Las representaciones lineales fueron introducidas y estudiadas por Gauss, Dedekind y Dirichlet en sus investigaciones en Teoría Algebraica de Números. Sin embargo, estas representaciones sólo determinan la parte menos interesante de G: sus cocientes abelianos. Por ejemplo, un grupo G simple no abeliano, no tiene representaciones lineales (salvo la **trivial** $g \mapsto 1$ para $g \in G$).

Volviendo al caso general, la representación $\mathcal{X} : G \to \mathrm{GL}(m, \mathbb{C})$ origina la función $\chi : G \to \mathbb{C}$ definida por

$$\chi(g) = \mathrm{traza}(\mathcal{X}(g))$$

para $g \in G$, llamada **carácter** de la representación. Los caracteres son **funciones de clase** pues si $g, h \in G$ entonces

$$\chi(g) = \chi(g^h)\,,$$

puesto que las matrices $\mathcal{X}(g)$ y $\mathcal{X}(g^h) = \mathcal{X}(h)^{-1}\mathcal{X}(g)\mathcal{X}(h)$ son semejantes. Decimos que dos representaciones $\mathcal{X}$ e $\mathcal{Y}$ de G son **semejantes** si existe una matriz regular M tal que

$$M^{-1}\mathcal{X}(g)M = \mathcal{Y}(g)$$

para todo $g \in G$. Está claro que dos representaciones semejantes tienen el mismo carácter, pero sorprendentemente, dos representaciones con el mismo carácter son necesariamente semejantes: el carácter por tanto ***conoce*** su representación (hasta la semejanza).

La suma de dos caracteres es un carácter (basta considerar la suma diagonal por bloques de las representaciones), y por tanto es natural nuestro interés en los caracteres que no son suma de otros dos: los caracteres **irreducibles** de G. El conjunto de estos caracteres se denota $\mathrm{Irr}(G)$.

Un resultado básico de la teoría de caracteres es que

$$|\mathrm{Irr}(G)| = k(G)$$

es el número de clases de conjugación de G. Más aún, $\mathrm{Irr}(G)$ es una base ortonormal del espacio vectorial complejo de las funciones de clase $\theta : G \to \mathbb{C}$ con el producto hermitiano

$$[\theta, \varphi] = \frac{1}{|G|}\sum_{g\in G}\theta(g)\overline{\varphi(g)}\,.$$

Así, todo grupo finito G tiene asociada canónicamente una matriz compleja

$$X(G) = (\chi_i(x_j))$$

de tamaño $k(G) \times k(G)$, dada por los valores de los caracteres irreducibles χ_i sobre los representantes x_j de las distintas clases de conjugación de G. ¿Cuánto sabe $X(G)$ de G? es una de las preguntas clásicas de la teoría de caracteres.

Los **grados** $\chi(1)$ de los caracteres irreducibles χ de G no son números cualquiera. Por ejemplo, se tiene que

$$|G| = \sum_{\chi\in\mathrm{Irr}(G)}\chi(1)^2\,.$$

Utilizando propiedades básicas de los enteros algebraicos es sencillo demostrar que si $\chi \in \mathrm{Irr}(G)$, entonces $\chi(1)$ divide a $|G|$. De hecho, el conjunto de grados refleja parte de la estructura del grupo. Por ejemplo, todos los grados son 1 si y sólo si G es abeliano (esto es una consecuencia directa de la ecuación de grados anterior). O todos los grados son no divisibles por nuestro primo p si y sólo si un p-subgrupo de Sylow P de G es normal y abeliano (esto es el teorema de Ito-Michler y se sigue de la clasificación de los grupos finitos simples).

Nosotros estamos interesados en el conjunto $\mathrm{Irr}_{p'}(G)$ de los caracteres irreducibles $\chi \in \mathrm{Irr}(G)$ de grado no divisible por p, y nuestro objetivo es contar cuántos hay localmente. La conjetura de McKay da la solución perfecta al problema.

CONJETURA DE MCKAY. *Si P es un p-Sylow de G, entonces*

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(\mathbf{N}_G(P))| .$$

Por qué estos dos números coinciden, o incluso, por qué pueden ser sencillamente comparados, es un misterio profundo. Los grupos G y $\mathbf{N}_G(P)$ son tan distintos desde el punto de vista de la teoría de grupos ($\mathbf{N}_G(P)$ tiene un p-Sylow normal cuando G puede ser hasta simple), son tan diferentes en tamaño, que es sorprendente que puedan de alguna manera estar relacionados. Tomemos por ejemplo el grupo simple no abeliano más pequeño, el grupo alternado $G = A_5$. Los grados de los caracteres irreducibles complejos de G son $1, 3, 3, 4, 5$. Si $p = 5$, entonces $\mathbf{N}_G(P)$ es el grupo dihédrico de orden 10 que tiene grados de caracteres irreducibles $1, 1, 2, 2$. Los dos grupos tienen exactamente 4 caracteres irreducibles de grado no divisible por 5, como McKay predice.

La conjetura de McKay trata de las representaciones de los grupos, pero también tiene consecuencias para la Teoría de Grupos Finitos: si P es abeliano, entonces $\mathrm{Irr}_{p'}(\mathbf{N}_G(P)) = \mathrm{Irr}(\mathbf{N}_G(P))$ (por el teorema de Ito-Michler que hemos mencionado) y por tanto McKay implica que

$$k(\mathbf{N}_G(P)) \leq k(G) .$$

No se sabe cómo probar esto directamente, ni siquiera en el caso en que $|P| = p$. Este hecho, sin embargo, no es aislado. Muchos teoremas sobre grupos finitos sólo han podido ser demostrados mediante representaciones.

Si McKay cuenta caracteres χ con $\chi(1)_p = 1$ (n_p es la mayor potencia de p que divide el entero n), la conjetura de pesos de Alperin, en su expresión por Knörr-Robinson, cuenta caracteres exactamente en el extremo opuesto: cuando $\chi(1)_p = |G|_p$. Estos caracteres son los llamados de **defecto cero**, y tienen mucha importancia en teoría de representaciones. Las conjeturas de Dade cuentan localmente los caracteres de cualquier *defecto*. (Los caracteres de grado no divisible por p tienen defecto máximo y los de defecto cero, mínimo).

2 . Congruencias

La conjetura de McKay fue formulada en 1972. (De hecho, fue nada más que una observación que J. McKay hizo para $p = 2$ y ciertos grupos simples). Fue probada para grupos de orden impar por M. Isaacs, para grupos resolubles por T. Wolf; para grupos simétricos por J. Olsson o para $GL(n, q)$, en la característica natural, por J. Alperin. Hace relativamente poco, R. A. Wilson la comprobó para todos los grupos esporádicos. Lo que queremos decir es que hay pocas (o ninguna) duda de que la conjetura de McKay es cierta. Como a J. Alperin le gusta decir, si esto fuera Física en lugar de Matemáticas, la conjetura de McKay habría sido simplemente aceptada como verdadera desde hace ya tiempo.

Después de casi 30 años desde su formulación, fue quizá extraordinario encontrar algo nuevo en ella. Y esto fue lo que nos ocurrió a M. Isaacs y al autor de este artículo recientemente. Supongamos que el primo p es mayor que 3. Dado un entero positivo k, contamos

$$M_k(G) = |\{\chi \in \mathrm{Irr}_{p'}(G) \mid \chi(1) \equiv \pm k \bmod p\}| .$$

De esta manera, partimos el conjunto $\mathrm{Irr}_{p'}(G)$ en distintos tipos de caracteres según la congruencia de sus grados módulo p. McKay, pues, predice que

$$\sum_{k=1}^{\frac{p-1}{2}} M_k(G) = \sum_{k=1}^{\frac{p-1}{2}} M_k(\mathbf{N}_G(P)) .$$

Nosotros propusimos lo siguiente:

Conjetura de McKay (con congruencias). *Si P es un p-Sylow de G, entonces*

$$M_k(G) = M_k(\mathbf{N}_G(P))$$

para todo k.

Por ejemplo, en el caso anterior $G = A_5$ y $p = 5$, sabemos que los caracteres irreducibles de $\mathbf{N}_G(P)$ son $1, 1, 2, 2$. La forma congruente de McKay predice que A_5 debe tener exactamente dos caracteres irreducibles de grado congruente con ± 1 modulo 5 y exactamente otros dos de grado congruente con ± 2 modulo 5. Los grados de los caracteres irreducibles de A_5 de grado no divisible por 5 son $1, 3, 3, 4$.

Si la conjetura de McKay era ya un misterio, esta observación la hace todavía más atractiva. Nos indica que debe existir una biyección

$$^* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$$

que satisfaga

$$\chi(1) \equiv \pm \chi^*(1) \bmod p$$

para todo $\chi \in \mathrm{Irr}_{p'}(G)$ (cuando McKay sólo garantiza la existencia de una biyección cualquiera). (Esto sugiere la existencia de ***isometrías*** entre ambos conjuntos de caracteres). Nosotros comprobamos nuestra conjetura para grupos resolubles, para grupos con p-Sylow P cíclico, para $GL(n,q)$ y $SL(n,q)$ (en la característica natural), y para los grupos esporádicos. Casi al mismo tiempo, P. Fong verificó nuestra conjetura para grupos simétricos.

¿Qué sentido tiene generalizar una conjetura que ni siquiera ha sido probada? Nuestro propósito al formular el refinamiento de McKay era obvio: cuanto más fuerte es una conjetura, más fácil debe ser de probar, pues disponemos de más datos sobre la naturaleza de la misma. Desafortunadamente, a día de hoy, todavía nadie ha dado una explicación del porqué de las congruencias en McKay.

3 . AUTOMORFISMOS DE GALOIS

Pero había más.

Supongamos de nuevo que G es un grupo finito, de orden n, y sea $\mathcal{X}$ cualquier representación de G. Si $g \in G$, entonces $\mathcal{X}(g)^n = I$ y por tanto la matriz $\mathcal{X}(g)$ es semejante a una matriz diagonal cuyas entradas son raíces n-ésimas de la unidad. Por tanto, si χ es un carácter de G, entonces

$$\chi(g) \in \mathbb{Q}_n \,,$$

donde $\mathbb{Q}_n$ es el n-ésimo cuerpo ciclotómico. En un teorema excepcional, R. Brauer probó que todo carácter irreducible χ puede ser de hecho originado por una representación

$$\mathcal{X} : G \to \mathrm{GL}(m, \mathbb{Q}_n)\,.$$

Es decir, no es necesario considerar todo el cuerpo $\mathbb{C}$ para obtener las representaciones de G: es suficiente $\mathbb{Q}_n$. (Este es un resultado con consecuencias en la Teoría de Números). Utilizando el teorema de Brauer, está claro que el grupo de Galois $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ actúa de forma natural sobre $\mathrm{Irr}(G)$. Si $\chi \in \mathrm{Irr}(G)$ y $\sigma \in \mathcal{G}$, la función χ^σ definida por

$$\chi^\sigma(g) = \chi(g)^\sigma$$

para $g \in G$ también es un carácter irreducible de G.

Intentando hallar nuevas relaciones entre $\mathrm{Irr}_{p'}(G)$ e $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$, ya sabíamos que no podía existir una biyección

$$^* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$$

que conmutara con la acción de ***todos*** los elementos de $\mathcal{G}$. Por ejemplo, esto implicaría que los conjuntos $\mathrm{Irr}_{p'}(G)$ e $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ tienen el mismo número de caracteres con valores racionales, y esto es falso (el grupo $GL(2,3)$ de matrices inversibles de tamaño 2×2 sobre el cuerpo de 3 elementos es un contraejemplo, para $p = 2$). Pero ¿no era esto pedir demasiado? Al fin y al cabo, ¡$\mathcal{G}$ «ignora» la existencia de nuestro primo p! Era por tanto natural buscar un subgrupo $\mathcal{H}$ de $\mathcal{G}$ canónicamente asociado al primo p y esperar que este subgrupo sí conmutara con una biyección en McKay. Experimentalmente, llegamos a la conclusión que el subgrupo $\mathcal{H}$ no podía ser otro que el conjunto de todos los $\sigma \in \mathcal{G}$ que envían las raíces de orden no divisible por p, a una p-potencia suya.

Conjetura de McKay (con acción de Galois). *Sea G un grupo finito. Si $\sigma \in \mathcal{H}$, entonces σ fija el mismo número de caracteres en $\mathrm{Irr}_{p'}(G)$ que en $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$.*

Mientras que McKay propone que los conjuntos $\mathrm{Irr}_{p'}(G)$ e $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ tienen el mismo cardinal (el caso $\sigma = 1$ de nuestra conjetura), la versión de McKay con acción de Galois predice algo todavía más profundo: que hay una conexión no trivial entre los valores de los caracteres de ambos conjuntos. Hay consecuencias no triviales de esta conjetura, de las que hablaremos después.

Nuestra conjetura ha sido comprobada para grupos resolubles (por Dade y A. Turull). También, ha sido comprobada para grupos simétricos por P. Fong. Nosotros la comprobamos para todos los grupos esporádicos y para grupos con p-Sylow cíclico.

Los datos empíricos sugieren que podemos combinar la forma congruente con la forma de Galois de McKay. De hecho, Dade ha anunciado una versión de sus conjeturas de acuerdo con esta idea.

Aunque sea obvio, la pregunta «por qué $\mathcal{H}$» no podrá ser respondida con exactitud hasta que la conjetura de McKay no sea debidamente entendida. De todos modos, tuvimos la convicción de que $\mathcal{H}$ era el subgrupo apropiado que buscábamos cuando probamos el siguiente resultado elemental (ciertamente clave para probar el caso P cíclico):

Teorema 1 *Si R_n es el anillo de enteros algebraicos de $\mathbb{Q}_n$, entonces $\mathcal{H}$ es el subgrupo de $\mathcal{G}$ que estabiliza todos los ideales primos de R_n que contienen a p.*

4 . Bloques

Aunque en esta exposición habría sido posible evitarlos, el lector no tendría una imagen completa de los problemas que tratamos si no mencionásemos los bloques de Brauer. Aunque nuestras conjeturas tratan de representaciones **ordinarias** (sobre el cuerpo $\mathbb{C}$), éstas están íntimamente relacionadas con las representaciones **modulares** (sobre cuerpos de característica p), como vamos a ver. De hecho, las representaciones modulares nos permiten probar resultados profundos sobre las representaciones complejas.

En su forma básica, la teoría de representaciones modulares empieza de la siguiente manera. Sea G un grupo finito de orden n y sea $\mathcal{P}$ un ideal primo de R_n que contiene a p, donde de nuevo R_n es el anillo de enteros algebraicos en $\mathbb{Q}_n$.

Entonces $F = R_n/\mathcal{P}$ es un cuerpo de característica p. Consideramos FG, el **álgebra** del grupo G sobre el cuerpo F. (Ésta no es más que el conjunto de sumas formales

$$\sum_{g \in G} a_g g$$

con $a_g \in F$ y con la multiplicación naturalmente asociada a G.)

Podemos escribir

$$FG = B_1 \oplus \cdots \oplus B_s$$

como suma de ideales indescomponibles de FG. Las álgebras B_i son los **bloques de Brauer** de G (que denotamos por $\mathrm{Bl}(G)$). Si V es un FG-módulo, entonces

$$V = VB_1 \oplus \cdots \oplus VB_s\,,$$

y vemos que si V es **irreducible** (no tiene submódulos) entonces necesariamente existe un único bloque B tal que $VB = V$ (al cual decimos que V **pertenece**). En particular, cualquier F-representación irreducible

$$\mathcal{X} : G \to \mathrm{GL}(m, F)$$

(que de manera natural tiene asociada el módulo irreducible $V = F^m$) pertenece a un único bloque B de G.

Lo que hace que la teoría modular sea tan rica y complicada es que no sólo trata de las representaciones de G sobre F sino de cómo éstas se relacionan con las representaciones complejas. Ya hemos dicho que Brauer probó que las representaciones de G pueden ser obtenidas en $\mathbb{Q}_n$. Pero todavía se podía concretar más. Si $\chi \in \mathrm{Irr}(G)$, entonces χ puede ser también originado por una representación $\mathcal{X}$ con entradas en S, donde

$$S = \{\alpha/\beta | \alpha \in R_n, \beta \in R_n - \mathcal{P}\}$$

es el anillo local de $\mathcal{P}$-enteros. Utilizando el homomorfismo natural de anillos $^* : S \to F$, vemos que el carácter complejo χ tiene asociada una FG-representación $\mathcal{X}^*$, que puede ser o no irreducible. Lo que es sorprendente es que todas las *constituyentes irreducibles* de $\mathcal{X}^*$ pertenecen al mismo bloque B (al cual decimos que χ **pertenece**). Así, vemos que no sólo los FG-módulos irreducibles están partidos en bloques, sino también el conjunto de los caracteres irreducibles complejos de G: $\mathrm{Irr}(G)$ es la unión disjunta de los «bloques» $\mathrm{Irr}(B)$ para $B \in \mathrm{Bl}(G)$ asociados canónicamente al primo p. En el caso, sin interés, de que p no divida $|G|$, los bloques son los caracteres irreducibles de G.

Brauer probó que cada bloque B tiene unívocamente asociado un p-subgrupo D de G, el **grupo defecto** del bloque, el cual, en cierto modo, mide la complejidad del mismo. (Por ejemplo, $D = 1$ si y sólo si $\mathrm{Irr}(B) = \{\chi\}$ si y sólo si χ tiene defecto cero. La famosa conjetura $k(B)$ de Brauer que tantos problemas ha originado establece que $|\mathrm{Irr}(B)| \leq |D|$. Después de muchos años de trabajo, esta conjetura acaba de ser probada sólo para grupos p-resolubles).

Designamos por $\mathrm{Bl}(G|D)$ el conjunto de bloques B de G con grupo defecto D. El primer teorema principal de Brauer, otro ejemplo de la importancia de la localidad en la teoría de grupos, afirma que existe una biyección canónica

$$\mathrm{Bl}(G|D) \to \mathrm{Bl}(\mathbf{N}_G(D)|D)\,.$$

Así, cada bloque B de un grupo finito G determina canónicamente otro bloque b de un subgrupo local, y por tanto «más sencillo». Muchos especialistas, el más influyente M. Broué, creen que la solución a todos los problemas que aquí mencionamos está en hallar la relación exacta entre las álgebras B y b y la categoría de sus módulos.

Otro hecho básico en teoría de bloques es que si $|G|_p = p^a$ y $|D| = p^d$, entonces

$$\min_{\chi \in \mathrm{Irr}(B)}\{\chi(1)_p\} = p^{a-d}\,.$$

De esta manera, si $\chi \in \mathrm{Irr}(B)$, entonces podemos escribir

$$\chi(1)_p = p^{a-d+h}$$

donde h es un entero no negativo (la **altura** de χ). Observamos que $\chi \in \mathrm{Irr}(G)$ tiene grado no divisible por p (los caracteres de los que se ocupa McKay) si y sólo si D es un p-subgrupo de Sylow de G y $h = 0$. (Ahora, tenemos los ingredientes para enunciar la conjetura de la altura cero de Brauer: *D es abeliano si y sólo si todos los caracteres irreducibles de B tienen altura cero*. Ninguna de las dos implicaciones ha sido demostrada).

La conjetura de Alperin-McKay es la versión de la conjetura de McKay para bloques de Brauer.

Conjetura de Alperin-McKay. *Si B y b son bloques correspondientes de Brauer, entonces B y b tienen el mismo número de caracteres de altura cero.*

Ahora, tanto la versión congruente como la de Galois de la conjetura de McKay, admiten una versión en bloques. Por ejemplo, sabemos que $\mathcal{H}$ estabiliza a cualquier ideal primo $\mathcal{P}$ de R_n que contenga a p. Así, $\mathcal{H}$ actúa naturalmente sobre F, sobre las F-representaciones y sobre los bloques. Además, conmuta con la biyección del primer teorema principal de Brauer. Nuestra versión de Alperin-McKay con acción de Galois establece que si $\sigma \in \mathcal{H}$, entonces σ fija el mismo número de caracteres de altura cero en B que en b. La forma congruente se establece en términos parecidos.

La teoría de bloques nos ayudó a probar, por fin, el siguiente teorema.

Teorema 2 *Supongamos que $P \in \mathrm{Syl}_p(G)$ es cíclico. Entonces las formas congruentes y de Galois de la conjetura de McKay son ciertas.*

La demostración utiliza teoría de representaciones modulares, y específicamente, la teoría de Dade de bloques con defecto cíclico.

El siguiente paso sería intentar probar estas conjeturas en el caso en que P sea abeliano, pero, lamentablemente, no se ha podido extender la teoría de bloques de defecto cíclico a una teoría de bloques con defecto abeliano, aunque esto es algo que se persigue desde hace mucho tiempo.

5 . Consecuencias de la conjetura de McKay con acciones de Galois

Como hemos dicho, uno de los problemas clásicos en Teoría de Caracteres es hallar qué información sobre un grupo finito G contiene su tabla de caracteres $X(G)$. Por ejemplo, $X(G)$ sabe si G es cíclico, abeliano, nilpotente, resoluble ó simple. Sin embargo demostrar que $X(G)$ conoce invariantes locales es algo mucho más difícil. Por ejemplo, no se sabe si $X(G)$ determina el número de p-subgrupos de Sylow de G. Como consecuencia de la forma de Galois de McKay, podemos decidir desde $X(G)$ si un p-subgrupo de Sylow de G es autonormalizante.

Teorema 3 *Sea G un grupo finito y sea $P \in \mathrm{Syl}_p(G)$. Supongamos cierta la forma de Galois de McKay. Entonces $X(G)$ determina si $P = \mathbf{N}_G(P)$.*

Otro problema clásico sobre tablas de caracteres es determinar qué sabe $X(G)$ del p-subgrupo de Sylow P de G. Por ejemplo, R. Brauer preguntó si $X(G)$ determinaba si P es abeliano (problema que se resolvió finalmente utilizando la clasificación). Recordamos que el exponente de un grupo finito G es el menor entero positivo n tal que $g^n = 1$ para todo $g \in G$.

Teorema 4 *Sea G un grupo finito y sea $P \in \mathrm{Syl}_p(G)$. Supongamos cierta la forma de Galois de McKay. Entonces $X(G)$ determina el exponente de P/P'.*

Para finalizar, somos algo pesimistas acerca de la posibilidad de encontrar en un futuro inmediato una demostración de la conjetura de McKay que no utilice la clasificación de los grupos finitos simples. A pesar de que nunca es enteramente satisfactorio probar que un teorema es cierto para todos los grupos porque es cierto para los grupos simples, demostrar la conjetura de McKay sería un logro de gran importancia. Recientemente, trabajando junto con M. Isaacs y G. Malle, hemos reducido la conjetura de McKay a un teorema sobre grupos simples, que esperamos se pueda comprobar próximamente.

Referencias

[1] J. L. Alperin, *The main problem of block theory.* Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975), 341–356. Academic Press, New York, 1976.

[2] J. L. Alperin, *Weights for finite groups.* The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), 369–379, Proc. Sympos. Pure Math., 47, Part 1, Amer. Math. Soc., Providence, RI, 1987.

[3] M. Broué, *Rickard equivalences and block theory*, London Mathematical Society Lecture Note Series 211, 58-79, Cambridge University Press, 1995.

[4] E. C. Dade, Blocks with cyclic defect groups. *Ann. of Math.* (2) **84** (1966), 20–48.

[5] E. C. Dade, Counting characters in blocks. I. *Invent. Math.* **109** (1992), no. 1, 187–10.

[6] E. C. Dade, Counting characters in blocks. II. *J. Reine Angew. Math.* **448** (1994), 97–190.

[7] I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994.

[8] I. M. Isaacs, G. Navarro, New refinements of the McKay conjecture for arbitrary finite groups, *Ann. of Math.* (2) **156** (2002), no. 1, 333–344.

[9] I. M. Isaacs, G. Malle, G. Navarro, A reduction theorem for the McKay conjecture, aceptado en *Invent. Math.*

[10] R. Knörr, G. R. Robinson, Some remarks on a conjecture of Alperin, *J. London Math. Soc.* (2) 39 (1989), 48–60.

[11] J. McKay, Irreducible representations of odd degree. *J. Algebra* **20** (1972) 416–418.

[12] G. Navarro, *Characters and Blocks of Finite Groups*, LMS Note Series 250, Cambridge University Press, 1998.

[13] G. Navarro, The McKay conjecture with Galois automorphisms, *Ann. of Math.* **160** (2004), 1129-1140.

[14] A. Turull, Character correspondences in solvable groups, *J. Algebra* **295** (2006), 157–178.

Gabriel Navarro
Facultat de Matemàtiques
Universitat de València
Burjassot, València 46100
Correo electrónico: gabriel.navarro@uv.es