Butlletí de la Societat Catalana de Matemàtiques
Vol. 20, núm. 2, 2005. Pàg. 129–136

L'àlgebra de grup: problemes de Brauer números 1 i 2

Gabriel Navarro

Resum En aquesta nota introduïm l'àlgebra complexa $\mathbb{C}G$ d'un grup finit G i els cèlebres problemes primer i segon de Brauer. Finalment proposem els que al nostre parer són els reptes més importants en l'estudi de $\mathbb{C}G$.

Paraules clau: àlgebres de grups, caràcters, problemes primer i segon de Brauer.

Classificació MSC2000: 20C15.

1 Grups finits

Una de les frases famoses (atribuïda a E. T. Bell) sobre la teoria de grups és «on hi ha caos, els grups ordenen»... excepte quan el caos es troba a la mateixa teoria de grups. El concepte de grup, com avui el coneixem i que tan natural ens pareix, ha trigat, però, més de dos mil anys a descobrir-se. Els grups estan per tot arreu a les matemàtiques i formen l'estructura fonamental i bàsica, la mínima que probablement té interès estudiar. On hi ha una certa simetria, quan en una equació pots canviar la x per la y... és segur que darrere hi ha un grup. Aquesta estructura bàsica té una riquesa i una profunditat sorprenents. Però l'estructura és tan mínima que, per on comencem a estudiar els grups? Amb quines eines comptem?

Amb poques. Estem interessats en els conjunts G on tenim definida una *operació*... que són molts. Per exemple, sumar funcions, multiplicar números, compondre aplicacions, multiplicar matrius. És a dir, per a cada dos elements $x, y \in G$, tenim definit un $x \cdot y \in G$. Totes les possibles operacions en G no són interessants: de fet, la immensa majoria no ho són. Com tots sabem, G és *grup* si

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

per a tots $x, y, z \in G$; si existeix un element $1 \in G$ tal que

$$x \cdot 1 = 1 \cdot x = x$$

per a tot $x \in G$; i si per a tot $x \in G$ existeix un $y \in G$ tal que

$$x \cdot y = y \cdot x = 1\,.$$

Aquestes són les lleis naturals que la nostra experiència matemàtica ens ha dictat.

En aquest article, només considerem grups amb un número finit d'elements. Els grups amb pocs elements són massa petits per a ser interessants: $G = \{1\}$ (el grup *trivial*), $G = \{\pm 1\}$ (el grup amb dos elements), $G = \{1, \omega, \omega^2\}$, on $\omega^3 = 1$ (per exemple, $\omega = \frac{1+\sqrt{3}i}{2}$). Si $n > 0$ és un enter, sempre hi ha un grup amb n elements molt senzill:

$$C_n = \{e^{\frac{2\pi ik}{n}} \mid 1 \leq k \leq n\}$$

que és el grup *cíclic* de les arrels n-simes de la unitat en $\mathbb{C}$. Hi ha dos tipus de grups amb quatre elements: $G = C_4$ o $H = \{(\pm 1, \pm 1)\}$. Aquests dos grups no són *isomorfs* perquè no hi existeix cap aplicació bijectiva

$$\alpha\colon G \to H$$

tal que

$$\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y)\,,$$

per a tots $x, y \in G$. (En H tenim $h^2 = 1$ per a tot $h \in H$, i açò no és veritat en G.)

Tots aquests grups del paràgraf d'abans són *abelians*: són grups on

$$x \cdot y = y \cdot x$$

per a tots $x, y \in G$. Els grups abelians són massa particulars i no reflecteixen l'essència general dels grups. El primer grup finit no abelià és el grup S_3 de simetries del triangle equilàter, un grup amb sis elements. Aquest grup és isomorf al grup d'aplicacions bijectives (*permutacions*) d'un conjunt de tres elements en ell mateix. Si volem un exemple de grup en qui pensar al llarg d'aquest article, jo recomanaria $G = S_n$ (el grup de les permutacions d'un conjunt de n elements), o el grup $GL(n, q)$ de les matrius invertibles $n \times n$ sobre un cos de q elements.

2 L'àlgebra de grup

Com s'estudien els grups finits? Hi ha dues maneres fonamentals. L'una consisteix a mirar-hi a dintre: els tipus de *subgrups* que té, com aquests es relacionen entre ells... L'altra és estudiar les *representacions* del grup, que és com

mirar els grups *des de fora*. Sembla que va ser Cayley el primer que va tenir la idea meravellosa de construir l'àlgebra d'un grup, que és l'essència de la teoria de representacions. Quan construeixes l'àlgebra del grup, de sobte ¡pots aplicar teoria d'anells per a estudiar grups!

Què és l'àlgebra d'un grup finit G? Si ens centrem en el cas més senzill, l'àlgebra complexa de G és el conjunt $\mathbb{C}G$ de *sumes formals*

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

on $a_g \in \mathbb{C}$. L'expressió «sumes formals» ens indica que dos elements

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

són iguals si i només si $a_g = b_g$ per a tot $g \in G$. És a dir, $\mathbb{C}G$ és l'espai vectorial sobre $\mathbb{C}$ amb base G. Aleshores, en $\mathbb{C}G$ es poden sumar elements:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g\,;$$

es poden multiplicar elements de $\mathbb{C}G$ per elements de $\mathbb{C}$:

$$a\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} (a a_g) g\,;$$

però sobretot, i més important, en $\mathbb{C}G$ es poden multiplicar elements:

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} a_g b_h (gh)\,.$$

Amb aquestes operacions $\mathbb{C}G$ és una *àlgebra* sobre $\mathbb{C}$. (Una àlgebra és un espai vectorial, que també és un anell, amb operacions compatibles. L'exemple canònic d'una àlgebra és

$$\mathrm{Mat}_n(\mathbb{C})\,,$$

l'àlgebra de matrius $n \times n$ amb entrades en $\mathbb{C}$.)

En general, si A és una àlgebra sobre $\mathbb{C}$, els *ideals* de A són els subespais I de A tals que

$$xIy \subseteq I$$

per a tots $x, y \in A$. Els ideals I de A són importants perquè ens permeten definir l'*àlgebra quocient* A/I. Les àlgebres que no tenen ideals (excepte 0 i A) es diuen *simples*. No és gaire difícil provar que les àlgebres $\mathrm{Mat}_n(\mathbb{C})$ són simples.

El teorema de Wedderbun ens clarifica com són totes les àlgebres sobre $\mathbb{C}$.

1 TEOREMA (WEDDERBURN) *Siga A una àlgebra de dimensió finita sobre $\mathbb{C}$. Aleshores A té un número finit d'ideals minimals $\{B_1, \dots, B_k\}$, i*

$$A = B_1 \oplus \cdots \oplus B_k .$$

També

$$B_i \cong \mathrm{Mat}_{n_i}(\mathbb{C})$$

per a alguns enters n_i unívocament definits.

És a dir, qualsevol àlgebra de dimensió finita sobre $\mathbb{C}$, i en particular l'àlgebra d'un grup G finit és suma directa

$$\mathbb{C}G = \mathrm{Mat}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{n_k}(\mathbb{C}) \tag{1}$$

per a alguns enters n_i unívocament determinats per G. Els números n_i són *els graus dels caràcters* de G.

Abans de continuar amb l'estudi de l'àlgebra de grup sobre $\mathbb{C}$, fem una petita digressió. Si canviem $\mathbb{C}$ per un cos no algebraicament tancat (i encara més si canviem $\mathbb{C}$ per un anell R) la fórmula (1) ja no té per què ser certa. Si R és anell, podem construir RG de la mateixa manera que hem construït $\mathbb{C}G$, i el que obtenim és la *R-àlgebra RG*. El 1940, G. Higman proposà un problema molt famós: és veritat que l'àlgebra $\mathbb{Z}G$ determina G? El 2001, M. Hertweck va trobar un contraexemple en [4]. (El lector interessat a conèixer la història d'aquest problema pot llegir [11].)

3 El problema número 1 de Brauer

En el seu celebrat article [1], el problema número 1 de Brauer proposa: Quines $\mathbb{C}$-àlgebres són àlgebres de grup?

En vista del teorema de Wedderburn, el problema 1 és equivalent a preguntar: donada una sèrie de números $n_1, \dots, n_k$, quan existeix un grup finit G amb

$$\mathbb{C}G = \mathrm{Mat}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{n_k}(\mathbb{C}) \ ?$$

Aquesta sembla una pregunta massa general per a poder ser contestada apropiadament, però ens «obliga» a buscar la relació entre els números n_i, la multiplicitat amb què apareixen, i l'estructura de G.

Si calculem dimensions en l'equació (1), tenim

$$|G| = \sum_{j=1}^{k} n_j^2 . \tag{2}$$

Com $\mathbb{C}G$ és una àlgebra commutativa si i només si G és abelià, si aplicam (1) llavors els grups abelians són exactament els grups G tals que $\mathbb{C}G$ és una suma directa d'àlgebres isomorfes a $\mathbb{C}$. En particular, $\mathbb{C} \oplus \cdots \oplus \mathbb{C}$ (n vegades) sempre és una àlgebra de grup: l'àlgebra de qualsevol grup abelià d'ordre n.

Utilitzant aquest argument i l'equació (2) tenim que l'àlgebra del grup $G = S_3$ (grup no abelià d'ordre 6) és

$$\mathbb{C} \oplus \mathbb{C} \oplus \mathrm{Mat}_2(\mathbb{C}) .$$

De seguida, calcularem el número r de n_i que són iguals a 1. Pel teorema de Wedderburn, tenim que r és el número d'ideals de $\mathbb{C}G$ amb dimensió 1. Per exemple,

$$\langle \sum_{g \in G} g \rangle$$

és un ideal de dimensió 1. En general, si l'espai vectorial generat per $0 \neq v \in \mathbb{C}G$ és un ideal, aleshores l'equació $vg = a_g v$ determina un homomorfisme de grups

$$\chi \colon G \to \mathbb{C}^\times$$

definit per $\chi(g) = a_g$. El recíproc també és veritat: cada homomorfisme $\chi \colon G \to \mathbb{C}^\times$ determina un ideal generat per un element diferent de zero, i comprovem fàcilment que el número d'uns en la descomposició de Wedderburn de $\mathbb{C}G$ és el número d'homomorfismes de grups $\chi \colon G \to \mathbb{C}^\times$. Aquest és molt fàcil de calcular utilitzant teoria elemental de grups: és l'ordre del grup

$$G/G' ,$$

on G' és el menor subgrup normal N de G tal que G/N és abelià. En particular, deduïm que r és un divisor de $|G|$. És a dir,

$$r \text{ divideix } \sum_{j=1}^{k} n_j^2 . \tag{3}$$

També es pot dir alguna cosa sobre el nombre k d'ideals en el teorema de Wedderburn. El centre d'una àlgebra A és la subàlgebra $\mathbf{Z}(A) = \{z \in A \mid za = az \text{ per a tot } a \in A\}$. Per exemple, si $K = \mathrm{cl}_G(x) = \{g^{-1}xg \mid g \in G\}$ és la *classe de conjugació* de x, tenim

$$\hat{K} = \sum_{y \in K} y \in \mathbf{Z}(\mathbb{C}G)$$

perquè

$$g^{-1}\hat{K}g = \hat{K}$$

per a tot $g \in G$. Com les matrius escalars són les úniques que commuten amb totes les matrius, utilitzant l'equació (1) tenim

$$k = \dim_{\mathbb{C}}(\mathbf{Z}(\mathbb{C}G)) .$$

D'altra banda, és molt fàcil comprovar que els elements $\{\hat{K} \mid K \in \mathrm{cl}(G)\}$ formen una base de $\mathbf{Z}(\mathbb{C}G)$ (on $\mathrm{cl}(G)$ és el conjunt de les classes de conjugació de G). Deduïm que

$$k = |\mathrm{cl}(G)| . \tag{4}$$

L'equació (4) ja ens dóna una restricció general important per als números n_i que venen d'una àlgebra de grup. El teorema de Landau sobre el nombre de classes de conjugació k d'un grup finit d'ordre n, afirma que hi ha una determinada funció f tal que $n \leq f(k)$. Es pot deduir que si n és gran, aleshores k no pot ser petit. Molt recentment, uns resultats de A. Moretó en [8] indiquen que si n és gran, aleshores ha d'existir un j tal que n_j es repeteix moltes vegades. Aquesta seria una altra restricció important al problema de Brauer.

La següent relació que els números n_i han de satisfer és una mica més profunda i té a veure amb propietats dels enters algebraics: els números n_i divideixen l'ordre de G. És a dir:

$$n_i \text{ divideix } \sum_{j=1}^{k} n_j^2 . \tag{5}$$

Per a grups d'ordre n petit, totes aquestes relacions són suficients per a calcular els n_i. Per exemple, si G té ordre $n = 15 = \sum_{j=1}^{k} n_j^2$, i existeix algun $n_i > 1$, aleshores n_i hauria de ser un divisor de 15. L'única possibilitat seria $n_i = 3$, però tindríem $r = 6$, que no divideix 15. Deduïm que tots els n_i són uns i, per tant, que G és abelià.

Ja hem dit que l'àlgebra $\mathbb{C} \oplus \cdots \oplus \mathbb{C}$ és una àlgebra de grup. Sembla que el següent cas a considerar és

$$A = \mathbb{C} \oplus \cdots \oplus \mathbb{C} \oplus \mathrm{Mat}_m(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_m(\mathbb{C}) , \tag{6}$$

on suposem que $\mathbb{C}$ apareix r vegades i m apareix t vegades. Si A és àlgebra de grup, aleshores m divideix r per (5) i r divideix $m^2 t$ per (3). Però aquestes dues condicions no són suficients per a garantir que A siga una àlgebra de grup. Per exemple, es pot comprovar que

$$\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathrm{Mat}_5(\mathbb{C})$$

no és una àlgebra de grup. Un estudi amb deteniment d'aquest cas (6) ens fa pensar que el problema número 1 de Brauer no té probablement una bona resposta.

4 El problema número 2 de Brauer

El problema número 2 de Brauer pregunta: Quan dos grups no isomorfs tenen àlgebres de grups isomorfes? En altres paraules, què sap $\mathbb{C}G$ de G? Segons la nostra opinió, aquest és un problema molt més interessant. És notable que varen passar molts anys des que Brauer va proposar el problema número 2 fins que M. Isaacs va provar el següent en [6].

2 TEOREMA (ISAACS) *Siguen G i H dos grups finits amb $\mathbb{C}G \cong \mathbb{C}H$. Si G és nilpotent, aleshores H és nilpotent.*

Uns anys després nosaltres vam provar el mateix resultat per a cossos K algebraicament tancats de característica p, [9].

Recordem que un grup és *nilpotent* si i sols si els seus subgrups de Sylow són normals. (Donat un número primer p, els p-subgrups de Sylow de G són els subgrups d'ordre la major potència de p que divideix $|G|$. Aquests subgrups existeixen i són conjugats.) En altres paraules, G és nilpotent si

$$G = P_1 \times \cdots \times P_n\,,$$

on els subgrups P_i tenen ordre potència de número primer.

Uns anys després i amb un argument molt simple, J. Cossey i T. Hawkes, van provar en [2] que $\mathbb{C}G$ determina $|G/\mathbf{O}^p(G)|$ per a cada número primer p. (El subgrup $\mathbf{O}^p(G)$ és el menor normal N de G tal que $|G/N|$ és una potència de p.) Com és fàcil de comprovar, G és nilpotent si i sols si p no divideix $|G/\mathbf{O}^p(G)|$ per a tot número primer (i com a consequència s'obté el teorema d'Isaacs).

Altres classes de grups estudiats han estat els *superresolubles* i els *p-descomponibles*. Els primers no són detectables per l'àlgebra de grup ([3]) i els segons sí ([7]), cosa que no és massa sorprenent, segons la nostra opinió.

Nosaltres considerem que hi ha dos problemes fonamentals sobre l'àlgebra de grup que s'han de resoldre. Pensem que l'àlgebra de grup $\mathbb{C}G$ està relacionada amb les *propietats aritmètiques* de G, i que són aquestes les que val la pena estudiar.

Problema A Siguen G i H dos grups finits amb $\mathbb{C}G \cong \mathbb{C}H$. Si G és resoluble, és H resoluble?

Aquest problema va ser mencionat per primera vegada (creiem) a [5] i sembla molt difícil d'atacar. Un grup G és resoluble si, per exemple, té una cadena de subgrups

$$1 = G_0 < G_1 < \cdots < G_k < G_{k+1} = G\,,$$

on $G_i \lhd G$ i G_i/G_{i+1} és un grup abelià. (Els grups resolubles apareixen històricament lligats a Galois i a la resolubilitat d'equacions polinòmiques per radicals i són ben importants.) Però, com l'existència d'aquests subgrups normals reflecteix i es reflexa en els números n_i?

El problema B sembla fonamental.

Problema B Siguen G i H dos grups finits amb $\mathbb{C}G \cong \mathbb{C}H$, i siga p un número primer. Si G té un p-Sylow normal, té H un p-Sylow normal?

El problema B va ser proposat en [10] i algunes consideracions i alguns casos els tractàrem allí. Nosaltres creiem que el futur de l'estudi de l'àlgebra de grup $\mathbb{C}G$ depèn de la resolució o no dels problemes A i B.

Per a acabar. Un problema relacionat amb el problema 2 de Brauer és estudiar què determina el conjunt $\mathrm{cd}(G)$ dels graus de caràcters d'un grup finit G.

Com ja sabem, conèixer $\mathbb{C}G$ és conèixer $\mathrm{cd}(G)$ amb la *multiplicitat* en què apareix cada grau de caràcter n_i. És molt fàcil comprovar que el conjunt $\mathrm{cd}(G)$ no determina si G té un p-Sylow normal. Per exemple $\mathrm{cd}(S_3) = \mathrm{cd}(D_4) = \{1, 2\}$, on D_4 és el grup de simetries del quadrat, i S_3 no té un 2-Sylow normal. Però sí que és un problema obert conèixer si $\mathrm{cd}(G)$ determina si G és resoluble. Aquest problema sembla que trigarà molts anys a ser provat.

Agraïments. A Pasqual Sala per la seva ajuda. Aquest article està finançat pel Ministeri d'Educació i Ciència, projecte MTM2004-06067-C02-01.

Referències

[1] Brauer, R. «Representations of finite groups». A: *Lectures on Modern Mathematics*. Vol. I, Nova York, 1963.

[2] Cossey, J.; Hawkes, T. «Computing the order of the nilpotent residual of a finite group from knowledge of its group algebra». *Arch. Math.* [Basilea], 60, núm. 2 (1993), 115–120.

[3] Hawkes, T. «On groups with isomorphic complex group algebras». *J. Algebra*, 167, núm. 3 (1994), 557–577.

[4] Hertweck, M. «A counterexample to the isomorphism problem for integral group rings». *Ann. of Math.*, (2) 154, núm. 1 (2001), 115–138.

[5] Huppert, B. *Research in representation theory at Mainz* (1984–1990). *Representation theory of finite groups and finite-dimensional algebras* (Bielefeld, 1991), 17–36, Progr. Math., 95, Birkhäuser, Basilea, 1991.

[6] Isaacs, I. M. «Recovering information about a group from its complex group algebra». *Arch. Math.* [Basilea] 47, núm. 4 (1986), 293–295.

[7] Mattarei, S. «Retrieving information about a group from its character degrees or from its class sizes». *Preprint*.

[8] Moretó, A. «Complex group algebras of finite groups: Brauer's problem 1». [En línia] *Electron. Res. Announc. Amer. Math. Soc.*, 11 (2005), 34–39.

[9] Navarro, G. «Two groups with isomorphic group algebras». *Arch. Math.* [Basilea] 55, núm. 1 (1990), 35–37.

[10] Navarro, G. *Problems on characters and Sylow subgroups*. Finite groups 2003, 275–281. Berlín: Walter de Gruyter GmbH Co. KG, 2004.

[11] Passman, D. *Mathematical Reviews*, MR1847590 (2002e:20010).

Facultat de Matemàtiques
Universitat de València
46100 Burjassot, València
gabriel.navarro@uv.es