

Monstres, cordes, fantasmes i clars de lluna*

PILAR BAYER

1 Què és un clar de lluna?

Les expressions *clair de lune*, *moonshine*, *Mondschein* s'han emprat per designar obres musicals i literàries diverses. Recordem, per exemple, el *Clair de Lune* de Claude Debussy (1862-1918), una composició per a piano, breu i intimista, inspirada en un poema de Paul Verlaine (1844-1896) del mateix títol. Tanmateix, el sintagma *clar de lluna* ha adquirit en els darrers anys un significat propi en matemàtiques. John H. Conway introduí la denominació *moonshine* per referir-se a certes coincidències numèriques, detectades gràcies a l'ús dels ordinadors.

D'entrada, per poder parlar de clars de lluna en el sentit de Conway ens calen nombres grans. Els nombres petits són poc expressius. Ningú no se sorprèn, ni cerca cap explicació addicional, quan obté nombres com ara 1, 5, 8... com a resultat d'operacions matemàtiques diverses. En el context matemàtic, es produeix un *clar de lluna* quan dos càlculs realitzats en àmbits diferents proporcionen el mateix resultat numèric, i aquest és un nombre gran, prou significatiu. Els clars de lluna ens alerten que certs conceptes matemàtics, en aparença independents, poden tenir lligams en comú.

Començarem per considerar el clar de lluna detectat per John McKay l'any 1977. McKay s'adonà que els termes de la identitat

$$1 + 196\,883 = 196\,884$$

són presents en dos càlculs completament diferents. El nombre 196 883 sorgeix en l'estudi d'un objecte matemàtic modern: el monstre de Fischer-Griess. El nombre 196 884 ho fa en el d'un objecte matemàtic clàssic: la funció J de Klein. Atès que tant la funció J de Klein com el monstre de Fischer-Griess són objectes matemàtics amb pedigrí, l'observació de McKay no fou endebades.

* Aquest text reproduïx una conferència impartida el 27 de març de 1998 a l'Institut d'Estudis Catalans amb motiu de la Primera Trobada Matemàtica. Felicito la Societat Catalana de Matemàtiques per l'inici d'aquesta sèrie de trobades, que desitjo que sigui ben llarga i profitosa. El tema objecte de la conferència fou exposat per l'autora a la Facultat de Física de la Universitat de Barcelona, el 22 d'abril de 1997.

2 Grups finits simples

Abans de parlar del monstre, ho farem una mica sobre els grups finits simples. Els grups finits simples —els grups finits sense subgrups normals no trivials— són els blocs constituents en què es desintegren els grups finits.

La determinació de tots els grups finits simples és una obra monumental, edificada sota les directrius de R. Brauer i D. Gorenstein per una munió de matemàtics. Gorenstein anomenà *guerra dels trenta anys* el període 1950–1980 durant el qual s'acomplí el teorema de classificació d'aquests grups. Els milers de pàgines d'articles que configuren el teorema es troben avui sota el procés de revisió GLS (Gorenstein-Lyons-Solomon). El treball final es preveu que comprendrà uns dotze volums, que seran editats per l'American Mathematical Society.

D'acord amb el teorema de classificació, la llista completa dels grups finits simples és composta de quatre classes, cadascuna de les quals conté una quantitat infinita d'elements, i una classe finita:

- els grups cíclics d'ordre primer C_p ;
- els grups alternats A_n , $n \geq 5$;
- els grups lineals clàssics sobre cossos finits:
 $\text{PSL}(n, q)$, $(n, q) \neq (2, 2), (2, 3)$; $\text{PSU}(n, q)$, $(n, q) \neq (2, 2), (2, 3), (3, 2)$;
 $\text{PSp}(2n, q)$, $(n, q) \neq (1, 2), (1, 3), (2, 2)$; $\text{P}\Omega^\epsilon(n, q)$;
- els grups excepcionals de Chevalley i uns grups de Chevalley torçats:
 $E_6(q)$; $E_7(q)$; $E_8(q)$; $F_4(q)$; $G_2(q)$; ${}^2B_2(2^{2m+1})$; ${}^3D_4(q)$; ${}^2E_6(q)$; ${}^2F_4(2)'$, grup de Tits; ${}^2F_4(2^{2m+1})$, $m \geq 1$; ${}^2G_2(3^{2m+1})$;
- els vint-i-sis grups esporàdics:
els grups de Mathieu $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$;
els grups de Janko J_1, J_2, J_3, J_4 ;
els grups de Conway Co_1, Co_2, Co_3 ;
els grups de Fischer $Fi_{22}, Fi_{23}, Fi'_{24}$;
HS; Mc; Suz; Ru; Ly; ON;
el monstre $M = F_1$;
la família del monstre, integrada pels monstres petits o *baby monsters* F_2, F_3, F_5, F_7 .

Cadascuna d'aquestes nissagues de grups té la seva pròpia història. Així, la classe dels grups cíclics d'ordre primer comprèn els grups considerats per C. F. Gauss (1777–1855) en relació amb el problema de les seccions del cercle; es tracta, doncs, d'una família de grups estudiada amb anterioritat a la introducció del terme *grup* per E. Galois (1811–1832). El grup de rotacions de l'icosàedre, A_5 , fou estudiat per F. Klein (1849–1925) en relació amb el problema de la resolució de la quintica. E. L. Mathieu descobrí el primer grup esporàdic, el grup M_{12} , l'any 1861; avui, trobem els grups de Mathieu lligats a la teoria de codis. Els grups de Conway tenen el seu paper en problemes d'apilament d'esferes. Etcètera.

La generació dels grups simples de les sèries tercera i quarta segueix unes pautes generals, adaptades dels grups de Lie clàssics. Ben al contrari, la construcció dels grups simples esporàdics requereix tècniques pròpies de cada cas.

L'estratègia proposada per Brauer per a la caracterització de grups finits simples fou, a grans trets, la següent:

En un grup finit simple, G , no abelià, triï's una involució, $w \in G$, $w^2 = 1$, i vegeu que els possibles tipus d'isomorfia de G queden determinats pel tipus d'isomorfia del centralitzador de la involució,

$$C_G(w) = \{g \in G \mid gw = wg\}.$$

R. Solomon comenta, divertit, que l'important teorema de W. Feit - J. G. Thompson dels anys seixanta, segons el qual tot grup d'ordre senar és resoluble, proporcionarà un gran impuls al programa de Brauer, ja que, com a mínim, sabem que tot grup simple no abelià conté involucions!

3 El monstre i el nombre 196 883

El monstre és el grup esporàdic més gran. El seu nombre d'elements és, aproximadament, igual a 10^{54} :

$$\begin{aligned} \#M &= 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000 \\ &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71. \end{aligned}$$

Com que el nombre de nucleons (protons i neutrons) de l'univers conegut s'estima en 10^{79} , ens adonem de seguida que la taula de multiplicar del monstre no ens hi cap! També crida l'atenció que l'ordre del monstre és un nombre altament factoritzable; és a dir, els seus factors primers són molt petits en relació amb $\#M$.

La manera més natural d'estudiar els grups és realitzant-los com a grup d'automorfismes (simetries) d'objectes diversos. Els objectes sobre els quals opera un grup poden provenir de la matemàtica, la física, la química, la geologia, la biologia, l'art o bé de qualsevol context on la noció de simetria sigui present.

A partir d'ara, G denotarà un grup finit. Quan l'ordre d'un grup és una mica gran, la seva taula de multiplicar no és de cap utilitat. Sovint, l'estudi d'un grup es fonamenta en el de les seves representacions lineals, a partir de les quals es confecciona la taula de caràcters del grup.

Una representació lineal ordinària de G és un homomorfisme de G en un grup d'automorfismes d'un espai vectorial V , que suposarem complex i de dimensió finita igual a d ,

$$\rho : G \rightarrow \text{Aut}(V) \simeq \mathbf{GL}(d, \mathbb{C}).$$

L'enter d s'anomena *grau de la representació*. L'exemple més senzill és la representació trivial, definida per $\rho_1(g) = (1)$, per a tot $g \in G$. La representació trivial és, doncs, de grau 1.

El caràcter $\chi : G \rightarrow \mathbb{C}$ d'una representació ρ és donat per la fórmula

$$\chi(g) = \text{Tr}(\rho(g)), \quad g \in G,$$

on $\text{Tr}(-)$ denota la traça d'un endomorfisme. Els caràcters són funcions centrals; és a dir, són constants sobre cada classe de conjugació:

$$\chi(hgh^{-1}) = \chi(g), \quad \text{per a tot } h \in G.$$

Una representació d'un grup s'anomena *irreductible* quan no es descompon en suma directa de representacions de grau més petit. Es diu aleshores que el seu

caràcter és irreductible. Tota representació és suma directa de representacions irreductibles; per tant, tot caràcter és suma de caràcters irreductibles.

Dues representacions de G són isomorfs si, i només si, tenen el mateix caràcter. Les entrades de la taula de caràcters d'un grup proporcionen els valors dels caràcters irreductibles sobre les diferents classes de conjugació del grup. Per tant, calcular la taula de caràcters d'un grup equival a interpretar-lo com a grup de matrius, fidelment o no, de totes les maneres possibles. Amb tot, la taula de caràcters no determina el grup unívocament; és a dir, grups no isomorfs poden tenir taules de caràcters idèntiques.

L'encapçalament de les columnes d'una taula de caràcters és donat pel *nom* de les classes de conjugació del grup. Una denominació de la forma rA , rB , rC , on r és un nombre, posa de manifest que el grup G conté tres classes de conjugació d'elements d'ordre r . La classe $1A$ és la de l'element neutre $e \in G$. L'encapçalament de les files és donat pels caràcters de les representacions irreductibles. Un important teorema garanteix que les taules de caràcters són sempre quadrades. Com que el nombre de classes de conjugació d'un grup no abelià és inferior al seu nombre d'elements, la taula de caràcters d'un grup no abelià té moltes menys entrades que la seva taula de multiplicar.

Les entrades de la primera fila d'una taula de caràcters són sempre iguals a 1, ja que provenen del caràcter trivial, χ_1 . Ja que l'aplicació lineal $\rho(e)$ és sempre la identitat, les entrades $d_i = \text{Tr}(\text{Id} | \mathbb{C}^{d_i})$ de la primera columna d'una taula de caràcters proporcionen els graus de les diferents representacions irreductibles del grup.

| A_5 | 1A | 2A | 3A | 5A | 5B |
|----------|----|----|----|-------------------------|-------------------------|
| χ_1 | 1 | 1 | 1 | 1 | 1 |
| χ_2 | 3 | -1 | 0 | $1 + \zeta + \zeta^4$ | $1 + \zeta^2 + \zeta^3$ |
| χ_3 | 3 | -1 | 0 | $1 + \zeta^2 + \zeta^3$ | $1 + \zeta + \zeta^4$ |
| χ_4 | 4 | 0 | 1 | -1 | -1 |
| χ_5 | 5 | 1 | -1 | 0 | 0 |

TAULA 1. Taula de caràcters del grup alternat A_5 ($\zeta = e^{2\pi i/5}$).

El càlcul de la taula de caràcters d'un grup obeeix lleis molt precises, basades principalment en les relacions d'ortogonalitat dels caràcters. Sovint, el càlcul d'un caràcter es pot portar a terme sense el coneixement explícit de la representació matricial que l'origina. A la vegada, les representacions dels subgrups indueixen representacions del grup, els components irreductibles de les quals formen part, necessàriament, de la taula de caràcters. Com veurem a la secció següent, la taula de caràcters del monstre va ser calculada abans que l'existència d'aquest grup hagués estat provada.

4 Els clars de lluna del monstre

L'any 1973, B. Fischer i R. L. Griess, basant-se en l'estructura d'un possible centralitzador d'una involució, conjecturaren l'existència del monstre, un grup simple esporàdic que havia de contenir com a subquocients la majoria dels altres grups

simples esporàdics. L'any 1975, Conway i S. P. Norton posaren de manifest que, si el monstre existia, el grau mínim d'una representació no trivial hauria de ser 196 883. Com l'existència de certs elements de la taula periòdica, o bé de certes partícules elementals, l'existència del monstre fou predita molt abans d'obtenir-ne la prova.

L'any 1978, B. Fischer, D. Livingstone i M. P. Thorne calcularen la taula de caràcters del monstre. Conjecturalment, els elements del monstre es repartien en 194 classes de conjugació, per tant, la taula és 194×194 . Sense problemes, la podem consultar a l'atles dels grups finits [14].

La primera columna de la taula de caràcters del monstre comença amb els nombres

$$d_1 = 1, \quad d_2 = 196\,883.$$

Hem localitzat els nombres del primer terme del clar de lluna de McKay. El nombre 196 883 és, doncs, la dimensió més petita per a la qual el monstre s'identifica —un cop provada l'existència— amb un subgrup de matrius: $M \subseteq \mathbf{GL}(196\,883, \mathbb{C})$.

En operar en la taula de caràcters del monstre, McKay, Thompson, Conway i Norton s'adonaren d'altres clars de lluna. De fet, totes les entrades de la primera columna de la taula de caràcters del monstre, d_i , resultaren igualment inquietants. En sumar-les, segons una llei difícil d'inferir, s'obtenien, misteriosament, els primers coeficients de Fourier de l'anomenada *funció J de Klein*:

$$\begin{aligned} d_1 + d_2 &= 1 + 196\,883 = 196\,884; \\ d_1 + d_2 + d_3 &= 1 + 196\,883 + 21\,296\,876 = 21\,493\,760; \\ 2d_1 + 2d_2 + d_3 + d_4 &= 2 + 393\,766 + 21\,296\,876 + 84\,260\,9326 = 86\,429\,970; \\ (\dots) \end{aligned}$$

Per tant, la identitat descoberta per McKay només era la primera d'una família d'identitats, que es presumia infinita.

L'any 1982, Griess pogué demostrar l'existència del monstre. Per a tal fi, construí una \mathbb{Q} -àlgebra escaient, \mathcal{B} , amb unitat, commutativa i no associativa, proveïda d'una forma bilineal, de dimensió 196 884, i n'obtingué el monstre com un subgrup del grup d'automorfismes: $M \subseteq \text{Aut}(\mathcal{B})$. Sota l'acció de M , l'espai vectorial subjacent a \mathcal{B} és suma directa de submòduls,

$$\mathcal{B} = \langle 1 \rangle \perp \mathcal{B}_0.$$

El submòdul \mathcal{B}_0 proporciona la representació irreductible de M de dimensió 196 883.

En la construcció del monstre hi intervé la xarxa de Leech Λ_{24} (vegeu la secció següent). De fet, el monstre conté una involució, w , tal que el seu centralitzador, $C_M(w)$, és una extensió central del grup simple de Conway Co_1 per un 2-grup extraespecial d'ordre 2^{25} . A la vegada,

$$Co_0 / \langle \pm 1 \rangle = Co_1,$$

on Co_0 és el grup d'automorfismes de la xarxa de Leech.

Amb anterioritat a l'obtenció del monstre per Griess, la prova de l'existència d'alguns grups esporàdics s'havia completat amb l'ús dels ordinadors. Per contra, la construcció de Griess és de natura algebraica. J. Tits resumeix aquest fet dient que el monstre naixé alliberat de pecat original. Griess realitzà els càlculs manualment, la

qual cosa permeté, a més, deslliurar de l'ús dels ordinadors l'existència de qualsevol grup simple esporàdic que sigui un subgrup, o bé un subquocient, del monstre.

L'any 1985, Tits i Conway simplificaren la demostració de Griess de l'existència del monstre. A més, Tits provà la igualtat

$$M = \text{Aut}(\mathcal{B}).$$

L'any 1975, en el decurs d'una conferència de Tits sobre el monstre, A. P. Ogg havia detectat, també, altres clars de lluna. Fixem-nos que la llista de divisors primers de l'ordre del monstre:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71,$$

no conté tots els primers ≤ 71 . Exactament, hi manquen el primers

$$37, 43, 53, 61, 67.$$

Ogg s'adonà que els primers que divideixen l'ordre del monstre coincideixen exactament amb uns primers obtinguts per ell arran d'uns càlculs molt concrets en el context de les corbes modulars. La recerca d'Ogg, un teòric dels nombres, s'havia portat a terme amb independència de la recerca dels teòrics dels grups.

5 La xarxa de Leech

Sigui $L \simeq \mathbb{Z}^n$ una xarxa quadràtica. És a dir, L és un grup abelià lliure de rang n , dotat d'una forma \mathbb{Z} -bilineal i simètrica, que suposarem valorada en els racionals:

$$\langle \cdot, \cdot \rangle: L \times L \rightarrow \frac{1}{r}\mathbb{Z}.$$

Sigui \mathbb{F} un cos de característica zero. En fer extensió d'escalars, podem incloure L en el \mathbb{F} -espai vectorial $L_{\mathbb{F}} = L \otimes_{\mathbb{Z}} \mathbb{F}$, i considerar-hi la \mathbb{F} -forma bilineal simètrica corresponent. A partir d'ara, suposarem que les formes bilineals són no degenerades. Donat $m \in \mathbb{Q}$, posarem

$$L_m := \{\alpha \in L \mid \langle \alpha, \alpha \rangle = m\}.$$

La xarxa L s'anomena *parella* quan

$$\langle \alpha, \alpha \rangle \in 2\mathbb{Z}, \quad \text{per a tot } \alpha \in L;$$

s'anomena *entera* quan

$$\langle \alpha, \beta \rangle \in \mathbb{Z}, \quad \text{per a tot } \alpha, \beta \in L;$$

s'anomena *definida positiva* quan

$$\langle \alpha, \alpha \rangle > 0, \quad \text{per a tot } \alpha \in L, \alpha \neq 0.$$

Equivalentment, L és definida positiva si, i només si, l'espai vectorial quadràtic $L_{\mathbb{R}}$ és euclidià. La fórmula de polarització,

$$\langle \alpha, \beta \rangle = \frac{1}{2}(\langle \alpha + \beta, \alpha + \beta \rangle - \langle \alpha, \alpha \rangle - \langle \beta, \beta \rangle), \quad \alpha, \beta \in L,$$

posa de manifest que tota xarxa parella és entera.

La xarxa dual L^* es defineix com

$$L^* = \{\alpha \in L_{\mathbb{Q}} \mid \langle \alpha, L \rangle \subset \mathbb{Z}\}.$$

Per tant, L és entera si, i només si $L \subseteq L^*$. Una xarxa L es diu que és autodual quan

$$L = L^*.$$

Una xarxa L és autodual si, i només si, és unimodular; és a dir,

$$|\det(\langle \alpha_i, \alpha_j \rangle)| = 1,$$

on $\{\alpha_1, \dots, \alpha_n\}$ denota una \mathbb{Z} -base de L .

L'estudi de les xarxes quadràtiques es complica molt en augmentar-ne el rang. Per això, és aconsellable centrar-se en l'estudi de les xarxes autoduals. Si designem per \mathcal{L}_n el conjunt de les classes d'isomorfia de xarxes parelles, de rang n , definides positives i autoduals, es té que $\mathcal{L}_n \neq \emptyset$ si, i només si, $n \equiv 0 \pmod{8}$. A més,

$$\#\mathcal{L}_8 = 1, \quad \#\mathcal{L}_{16} = 2, \quad \#\mathcal{L}_{24} = 24, \quad \#\mathcal{L}_{32} > 8 \cdot 10^7.$$

En les dimensions petites, hi trobem dues xarxes especialment interessants: la xarxa d'arrels, $\Gamma_8 \in \mathcal{L}_8$, del grup de Lie E_8 , i la xarxa de Leech, $\Lambda_{24} \in \mathcal{L}_{24}$.

La xarxa Γ_8 conté 240 vectors α tals que $\langle \alpha, \alpha \rangle = 2$, per la qual cosa, $\dim E_8 = 248$.

Es pot provar que, en un conjunt de 24 elements, existeix un únic codi binari autodual de tipus II que no té elements de pes 4. És el codi de Golay C_{24} . Es tracta d'un codi corrector d'errors altament eficient. El grup d'automorfismes del codi de Golay és el grup de Mathieu M_{24} :

$$M_{24} = \text{Aut}(C_{24}).$$

La xarxa de Leech es pot construir a partir del codi de Golay. Fou descoberta en relació amb un problema d'apilament d'esferes en \mathbb{R}^{24} . La xarxa de Leech defineix l'únic element de \mathcal{L}_{24} sense vectors curts; és a dir, tal que

$$\Lambda_{24,2} = \{\alpha \in \Lambda_{24} \mid \langle \alpha, \alpha \rangle = 2\} = \emptyset.$$

El grup ortogonal de Λ_{24} (l'estabilitzador en $\mathbf{GL}(24, \mathbb{Z})$) és el grup Co_0 ,

$$Co_0 = \text{Aut}(\Lambda_{24}).$$

El grup anterior no és simple, sinó extensió central del grup de Conway Co_1 per un grup cíclic d'ordre 2. El grup Co_0 conté com a subquocients un total de 12 grups simples esporàdics i, en particular, conté com a subgrups els grups simples esporàdics: $Co_1, Co_2, Co_3, M_{12}, M_{22}, M_{23}, M_{24}$.

6 La funció J de Klein i el nombre 196 884

En aquesta secció, identificarem el nombre del segon terme de la identitat de McKay: 196 884.

Considerem el grup especial lineal, $\mathbf{SL}(2, \mathbb{R})$, format per les matrius 2×2 reals de determinant igual a 1, així com també el grup modular, $\mathbf{SL}(2, \mathbb{Z})$, subgrup discret

de l'anterior, format per les matrius enteres. El grup modular és generat per les matrius

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Sigui $\mathcal{H} := \{z \in \mathbb{C} \mid \Im z > 0\}$ el semiplà superior complex. $\mathbf{SL}(2, \mathbb{R})$ opera en \mathcal{H} per mitjà del quocient $\mathbf{PSL}(2, \mathbb{R}) = \mathbf{SL}(2, \mathbb{R}) / \langle \pm 1 \rangle$. L'acció és definida per

$$\gamma(z) = \frac{az + b}{cz + d}, \quad \text{per a } \gamma = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad z \in \mathcal{H}.$$

S'obtenen així tots els isomorfismes analítics de \mathcal{H} . L'acció del grup modular en \mathcal{H} és discontinua. La regió

$$\{z \in \mathcal{H} \mid |\Re(z)| \leq 1/2, |z| \geq 1\}$$

és un domini fonamental de $\mathbf{PSL}(2, \mathbb{Z}) \backslash \mathcal{H}$.

Gauss utilitzà el grup modular per classificar les representacions d'enters per formes quadràtiques binàries i enteres. Coneixia bé l'acció de $\mathbf{PSL}(2, \mathbb{Z})$ en \mathcal{H} .

L'any 1877, Richard Dedekind construï una funció definida sobre \mathcal{H} i invariant per $\mathbf{PSL}(2, \mathbb{Z})$. L'anomenà *Valenzfunktion* i la designà per v . A més,

$$v(e^{\frac{\pi i}{3}}) = 0, \quad v(i) = 1, \quad v(i\infty) = \infty.$$

Klein féu un ús ampli de la funció $j = 1728v$, coneguda avui sota els noms de *funció j de Klein*, *invariant modular*, *funció modular el·líptica*, etc.

La funció j és holomorfa en \mathcal{H} i meromorfa en $\mathcal{H} \cup \{i\infty\}$. Té un pol simple en l'infinit, de residu 1. Les equacions funcionals

$$j(z+1) = j(z), \quad j\left(-\frac{1}{z}\right) = j(z),$$

expressen la invariància de j respecte de $\mathbf{PSL}(2, \mathbb{Z})$. Per definició, una funció meromorfa de $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ i invariant sota l'acció de $\mathbf{PSL}(2, \mathbb{Z})$ és una funció modular de nivell 1. El conjunt d'aquestes funcions és el cos $\mathbb{C}(j)$.

És a dir, tota funció modular de nivell 1 s'expressa com a funció racional de j de coeficients complexos.

Problemes diferents conduïren a l'estudi de la funció j . Recordem, entre d'altres:

- la classificació de les formes quadràtiques binàries enteres;
- la classificació de les integrals el·líptiques i de les corbes el·líptiques;
- la resolució d'equacions algebraiques en una indeterminada ultra la utilització de radicals;
- la integració d'equacions diferencials;
- problemes d'uniformització de superfícies de Riemann.

La funció j estableix un isomorfisme analític entre $\mathbf{PSL}(2, \mathbb{Z}) \backslash \mathcal{H} \cup \{i\infty\}$ i l'esfera de Riemann $\mathbb{C} \cup \{\infty\}$; equivalentment, proporciona una bijecció

$$j: \mathbf{PSL}(2, \mathbb{Z}) \backslash \mathcal{H} \cup \{i\infty\} \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}),$$

on $\mathbb{P}^1(\mathbb{C})$ és la recta projectiva complexa.

| | | @ | @ | @ |
|-----|------|--------------------------------|-------------------|-----------------|
| | | 808DI742479451287588645 | 83095629624528523 | 139511839126 |
| | | 990496171075700575436800000000 | 82355161088000000 | 336328171520000 |
| | | <i>p</i> potència | A | A |
| | | <i>p'</i> part | A | A |
| | ind. | 1A | 2A | 2B |
| X1 | + | 1 | 1 | 1 |
| X2 | + | 196883 | 4371 | 275 |
| X3 | + | 21296876 | 91884 | -2324 |
| X4 | + | 842609326 | 1139374 | 12974 |
| X5 | + | 18538750076 | 8507516 | 123004 |
| X6 | + | 19360062527 | 9362495 | -58305 |
| X7 | + | 293553734298 | 53981850 | 98970 |
| X8 | + | 3879214937598 | 337044990 | -690690 |
| X9 | + | 36173193327999 | 1354188159 | 2864511 |
| X10 | + | 125510727015275 | 3215883115 | 1219435 |
| X11 | + | 190292345709543 | 2814161895 | 10249191 |
| X12 | + | 222879856734249 | 3864186921 | -7196631 |
| X13 | + | 1044868466775133 | 9223504989 | -15756195 |
| X14 | + | 1109944460516150 | 9697078070 | 26155830 |
| X15 | + | 2374124840062976 | 22509162496 | 410009 |
| X16 | 0 | 8980616927734375 | -2720265625 | 39414375 |
| X17 | 0 | 8980616927734375 | -2720265625 | 39414375 |
| X18 | + | -15178147608537368 | 72990279960 | -29873896 |
| X19 | + | 39660520552077425 | 128459630705 | 47061105 |
| X20 | + | 60359800576579350 | 143552415510 | 71276310 |
| X21 | + | 251098487132187500 | 336140827500 | 339995500 |
| X22 | + | 290568421805921077 | 444043629365 | 45093685 |
| X23 | + | 336041615485626050 | 536115345090 | -288233790 |
| X24 | + | 2500435234254428856 | 1864421481144 | 319494840 |
| X25 | + | 2986480825407204125 | 1612726090525 | -385717475 |
| X26 | 0 | 3503434660075044981 | -89143381899 | 755269515 |
| X27 | 0 | 3503434660075044981 | -89143381899 | -755269515 |
| X28 | + | 3605718753596953125 | 2239938073125 | 284185125 |

TAULA 2: Inici de la taula de caràcters del monstre.

La propietat de periodicitat $j(z + 1) = j(z)$ implica que j és desenvolupable en sèrie de Fourier a l'entorn de la punta de l'infinit:

$$\begin{aligned}
 j(z) &= \frac{1}{q} + 744 + 196\,884\,q + 21\,493\,760\,q^2 + 864\,299\,970\,q^3 \\
 &\quad + 20\,245\,856\,256\,q^4 + \dots \\
 &= \frac{1}{q} + 744 + \sum_{n \geq 1} c(n)q^n, \quad q = e^{2\pi iz}.
 \end{aligned}$$

Normalitzarem la funció j escrivint:

$$J(z) = j(z) - 744.$$

Ens adonem que el coeficient de Fourier $c(1) = 196\,884$ és el nombre que intervé en el clar de lluna detectat per McKay.

Sigui σ_k la funció aritmètica que assigna a cada enter $n > 0$ la suma de les potències k -èsimes dels seus divisors: $\sigma_k(n) = \sum_{d|n} d^k$. Una expressió exacta de la funció J és la donada per

$$J(z) + 744 = \frac{(1 + 240 \sum_{n>0} \sigma_3(n) q^n)^3}{q \prod_{n>0} (1 - q^n)^{24}}.$$

En la igualtat anterior s'aparellen una suma infinita amb un producte infinit. El denominador, que és la potència 24 de la funció η de Dedekind, coincideix amb la funció discriminant normalitzada:

$$\eta(z) = q^{1/24} \prod_{n>0} (1 - q^n), \quad \Delta(z) = (2\pi)^{12} \eta(z)^{24}.$$

El numerador és la potència tercera de la sèrie d'Eisenstein de pes 4 normalitzada:

$$E_4(z) = 1 + 240 \sum_{n>0} \sigma_3(n) q^n.$$

Coincideix amb la funció theta de la xarxa $\Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8$.

Els coeficients de Fourier de la funció J són nombres naturals. Aquesta propietat la fa molt rellevant des del punt de vista aritmètic. Per calcular aquests coeficients podem, també, fer servir la fórmula:

$$c(n) = \frac{65520}{691} (\sigma_{11}(n+1) - \tau(n+1)) - \tau(n+2) - 24\tau(n+1) - \sum_{k=1}^{n-1} c(k)\tau(n+1-k).$$

Ara, l'aplicació $n \mapsto \tau(n)$ és la funció de Ramanujan, on

$$(2\pi)^{-12} \Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n.$$

De l'expressió anterior es dedueix, de passada, la congruència de Ramanujan $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$.

En calcular uns quants termes del desenvolupament de J , s'observa que cadascun dels coeficients de Fourier es pot expressar com a suma de nombres que figuren en la primera columna de la taula de caràcters del monstre:

$$\begin{aligned} c(1) &= d_1 + d_2; \\ c(2) &= d_1 + d_2 + d_3; \\ c(3) &= 2d_1 + 2d_2 + d_3 + d_4; \\ (\dots) \end{aligned}$$

Posem les taules 2 i 3 a l'abast de qui desitgi contemplar personalment aquests clars de lluna.

| n | $c(n)$ |
|-----|--------------------------------|
| -1 | 1 |
| 0 | 744 |
| 1 | 196884 |
| 2 | 21493760 |
| 3 | 864299970 |
| 4 | 20245850256 |
| 5 | 333202640600 |
| 6 | 4252023300096 |
| 7 | 44656994071935 |
| 8 | 401490886656000 |
| 9 | 3176440229784420 |
| 10 | 22567393309593600 |
| 11 | 146211911499519294 |
| 12 | 874313719685775360 |
| 13 | 4872010111798142520 |
| 14 | 25497827389410525184 |
| 15 | 126142916465781843075 |
| 16 | 593121772421445058560 |
| 17 | 2662842413150775245160 |
| 18 | 11459912788444786513920 |
| 19 | 47438786801234168813250 |
| 20 | 189449976248893390028800 |
| 21 | 731811377318137519245696 |
| 22 | 2740630712513624654929920 |
| 23 | 9971041659937182693533820 |
| 24 | 35307453186561427099877376 |
| 25 | 121883284330422510433351500 |
| 26 | 410789960190307909157638114 |
| 27 | 1353563541518646878675077500 |
| 28 | 4365689224858876634610401280 |
| 29 | 13798375834642999925542288376 |
| 30 | 42780782244213262567058227200 |
| 31 | 130233693825770295128044873221 |
| 32 | 389608006170995911894300098560 |

TAULA 3: Coeficients de Fourier de la funció j .

7 Paràmetres principals

Com la primera columna de la taula de caràcters del monstre, les altres 193 columnes també ocasionen clars de lluna a doll.

El grup $\Gamma_0(1) := \mathbf{SL}(2, \mathbb{Z})$ és un exemple de grup fuchsian. Les funcions meromorfes a \mathcal{H} i invariants sota l'acció d'un grup fuchsian s'anomenen *funcions automorfes*. La funció J , doncs, n'és un exemple.

Per reconèixer els clars de lluna que produeixen la resta de columnes de la taula de caràcters del monstre, necessitem introduir altres funcions automorfes, a més de la funció J . Un índex dels grups fuchsians implicats el trobem en la llista de primers calculada per Ogg.

Sigui $N \geq 1$ un enter. El grup modular de nivell N és definit per

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(1) \mid c \equiv 0 \pmod{N} \right\}.$$

És un subgrup de $\Gamma_0(1)$ i, com a tal, opera discontinuament en \mathcal{H} .

La funció $J_N(z) := J(Nz)$ és invariant respecte de $\Gamma_0(N)$. Les funcions $J(z), J_N(z)$ satisfan una equació polinòmica de coeficients enters, anomenada *equació modular de nivell N* :

$$\Phi_N(X, Y) \in \mathbb{Z}[X, Y], \quad \Phi_N(J, J_N) = 0.$$

La corba projectiva associada a l'equació anterior és la corba modular $X_0(N)$, de nivell N . Els seus punts complexos són donats per

$$\Gamma_0(N) \backslash \mathcal{H} \cup \{\text{punts}\} \xrightarrow{\sim} X_0(N)(\mathbb{C}).$$

El cos de funcions de $X_0(N)$ és $\mathbb{C}(X_0(N)) = \mathbb{C}(J, J_N)$. Com a superfície de Riemann compacta, $X_0(N)(\mathbb{C})$ és suma connexa de g tors, on g és el gènere de $X_0(N)$. Com ja hem fet notar més amunt, $g(X_0(1)) = 0$.

Les corbes de gènere zero es caracteritzen pel fet que el seu cos de funcions és isomorf al cos de les funcions racionals en una indeterminada, $\mathbb{C}(T)$. Una funció generatriu, imatge de T , d'un cos de funcions de gènere zero s'anomena *paràmetre principal* o *Hauptmodul* del cos.

La matriu $w_N = \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix}$ pertany al normalitzador de $\Gamma_0(N)$ en $\mathbf{SL}(2, \mathbb{R})$.

Defineix sobre \mathcal{H} una involució $w_N(z) = -1/Nz$, dita *d'Atkin*. Cal que introduïm la corba

$$X_0^+(N) = X_0(N) / \langle w_N \rangle,$$

quocient de la corba modular de nivell N per la involució d'Atkin.

L'any 1974, Ogg havia provat que, per a N primer, les corbes $X_0^+(N)$ són de gènere zero si, i només si,

$$N = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71.$$

Per als valors $N = 37, 43, 53, 61$, les corbes $X_0^+(N)$ són de gènere 1. La corba $X_0^+(67)$ és de gènere 2.

Les funcions que considerarem tot seguit són invariants per la translació $z \rightarrow z+1$, de manera que es poden escriure en sèrie de potències de $q = e^{2\pi iz}$. Donat el cas, normalitzarem els paràmetres principals de manera que el seu desenvolupament de Fourier tingui el terme constant igual a zero.

La funció J és el paràmetre principal de la corba de gènere zero $X_0^+(1) = X_0(1)$. Notem que la funció j no està normalitzada, ja que $J = j - 744$.

Quan el gènere de $X_0^+(N)$ sigui zero, designarem per H_N el seu paràmetre principal, normalitzat. Així, $J = H_1$. Els paràmetres principals no solen ser difícils de calcular. Per exemple, el paràmetre principal de nivell 27 és donat per la funció

$$H_{27}(z) = \left(\frac{\eta(3z)\eta(9z)}{\eta(z)\eta(27z)} \right)^3.$$

Per tant, els nivells calculats per Ogg són els nivells primers per als quals existeixen paràmetres principals:

$$H_2, H_3, H_5, H_7, H_{11}, H_{13}, H_{17}, H_{19}, H_{23}, H_{29}, H_{31}, H_{41}, H_{47}, H_{59}, H_{71}.$$

No n'existeixen en els nivells 37, 43, 53, 61, 67, ni en cap nivell primer > 71 .

Fixem-nos que els primers que s'obtenen d'aquesta manera són, exactament, els primers que divideixen l'ordre del monstre. Ogg prometé una ampolla de *Jack Daniels* a qui fos capaç de justificar el perquè d'aquesta coincidència sorprenent.

8 Les conjectures de Conway-Norton-Thompson

Influenciats per les observacions d'Ogg i McKay, i basant-se en una forta experimentació numèrica, Conway, Norton i Thompson formularen, l'any 1979, les conjectures següents:

C1. Cal que existeixi un espai vectorial graduat,

$$V = V_{-1} \oplus V_0 \oplus V_1 \oplus V_2 \oplus \dots,$$

en el qual operi el monstre, M . L'acció de M en V ha de preservar la gradació. Per a cada n , V_n és un espai vectorial de dimensió finita igual a $c(n)$, el coeficient n -èsim de Fourier de la funció J .

C2. Per a cada element $m \in M$, cal que existeixi un grup fuchsà de gènere zero $\Gamma_m \subset \text{SL}(2, \mathbb{R})$ de tal manera que la sèrie de Thompson associada a l'acció anterior i definida per

$$T_m(z) := q^{-1} + \sum_{n=1}^{\infty} \text{Tr}(m | V_n) q^n$$

sigui un paràmetre principal de la corba $X(\Gamma_m)$. Notem que la sèrie T_m és un invariant de la classe de conjugació de m .

C3. En general, el subgrup Γ_m normalitza un subgrup $\Gamma_0(Nt)$, per a un cert $t | \text{mcd}(24, N)$, on N és l'ordre de m . Quan m és d'ordre primer, aleshores cal que se satisfaci la igualtat $\Gamma_m = \langle \Gamma_0(N), w_N \rangle$, per tant, $X(\Gamma_m) = X_0^+(N)$ i $T_m = H_N$.

Les conjectures anteriors explicarien els clars de lluna detectats per Ogg: si un primer p divideix $\#M$, la sèrie de Thompson d'un element d'ordre p del monstre proporciona el paràmetre principal, H_p , de la corba $X_0^+(p)$, per tant, aquesta està obligada a ser de gènere zero. Com que, pel teorema d'Ogg, no hi ha corbes $X_0^+(p)$ de gènere zero per a p més gran que 71, aquest nombre és el primer més gran que divideix l'ordre del monstre.

Les 194 classes de conjugació del monstre han de proporcionar un total de 171 sèries de Thompson diferents, ja que la presència de classes de conjugació racionals és causa de coincidències. Norton i Conway identificaren conjecturalment les 171 funcions automorfes que corresponien a les sèries de Thompson, i comproven la igualtat d'uns quants coeficients.

Les conjectures **C1**, **C2**, **C3** han estat totes demostrades. En el que segueix, esmentarem els principis en què la seva prova es fonamenta.

9 Àlgebres d'operadors de vèrtexs

La construcció del monstre com a grup d'automorfismes de l'àlgebra de Griess resultà del tot insuficient per comprendre els clars de lluna. Per aconseguir una visió més acurada del monstre, ha calgut interpretar aquest grup com a grup d'automorfismes d'un objecte molt més sofisticat: una àlgebra d'operadors de vèrtexs.

Per establir els lligams precisos entre la teoria de grups finits i la teoria de funcions automorfes que predeien les conjeitures de Conway-Norton-Thompson, els matemàtics han fet ús de l'experiència adquirida pels físics teòrics en la teoria de cordes. La noció d'àlgebra d'operadors de vèrtexs fa abstracció de molts dels conceptes d'aquesta teoria.

En el context que ens ocupa, alguns dels conceptes que esmentarem són relativament nous. No hi ha encara unanimitat ni en les definicions ni en les notacions. Ens limitarem a apropar-nos-hi.

En la definició d'àlgebra d'operadors de vèrtexs (AOV), hi intervenen els elements que segueixen.

- Un espai vectorial graduat sobre \mathbb{Z} :

$$V = \coprod_{n \in \mathbb{Z}} V_n$$

tal que $\dim V_n < \infty$, per a tot n , i $V_n = (0)$, per a n prou petit. Els elements de V s'anomenen *estats*. Els vectors $v \in V_n$ són els estats de pes o nivell n ($\text{wt } v = n$). La suma formal

$$\dim_* V = \sum_{n \in \mathbb{Z}} (\dim V_n) q^n$$

s'anomena *dimensió graduada de V o funció de partició*.

- Uns vectors distingits i una constant distingida:

$$\mathbf{1}, \omega \in V, \quad c \in \mathbb{R},$$

anomenats *vector buit*, *vector conforme*, i *càrrega central o dimensió conforme* de V , respectivament.

- Uns operadors de vèrtexs, dits també *camp conformes* o *camp quàntics*:

$$Y(v, z) = \sum_{n \in \mathbb{Z}} v_n z^{-n-1} \in \text{End}(V)[[z, z^{-1}]], \quad v_n \in \text{End}(V),$$

que creen els estats de V a partir del buit $\mathbf{1}$:

$$\lim_{z \rightarrow 0} Y(v, z)\mathbf{1} = v; \quad Y(\mathbf{1}, z) = 1.$$

Estrictament parlant, els operadors de vèrtexs són una funció generatriu d'una família d'operadors indexada per \mathbb{Z} .

- Una àlgebra d'operadors de V :

$$L_{-1} = D, \quad L_n = \omega_{n+1}, \quad n \geq -1,$$

anomenada *àlgebra de Virasoro* o la part conforme del tensor d'estrès-energia. L'operador D és una derivació de V i el quocient V/DV és una àlgebra de Lie, amb parèntesi de Lie donat per

$$[u, v] = u_0 v.$$

Els operadors de Virasoro aïllen els estats físics i satisfan les relacions

$$[L_m, L_n] = (m - n)L_{m+n} + \frac{1}{12}(m^3 - m)\delta_{m,-n}c,$$

on δ és la funció de Kronecker. Notem que $Y(w, z) = \sum_{n \in \mathbb{Z}} L_n z^{-n-2}$.

- Se satisfà, també, que

$$L_{-2}(\mathbf{1}) = \omega; \quad L_n(\mathbf{1}) = 0, \quad n \geq -1;$$

$$L_0(\omega) = 2\omega; \quad L_1(\omega) = 0; \quad L_2(\omega) = c/2.$$

I, en general,

$$L_0(v) = (n + 1)v, \quad \text{per a tot } v \in V_n.$$

- Els operadors de vèrtexs satisfan la identitat

$$\begin{aligned} z_0^{-1} \delta\left(\frac{z_1 - z_2}{z_0}\right) Y(u, z_1) Y(v, z_2) - z_0^{-1} \delta\left(\frac{z_2 - z_1}{-z_0}\right) Y(v, z_2) Y(u, z_1) = \\ z_2^{-1} \delta\left(\frac{z_1 - z_0}{z_2}\right) Y(Y(u, z_0)v, z_2), \quad \text{on } \delta(z) := \sum_{n \in \mathbb{Z}} z^n. \end{aligned}$$

La igualtat anterior fa el paper d'una identitat de Jacobi (model de ressonància dual). Les AOV no són ni associatives ni commutatives.

Un cop introduït el concepte d'AOV, cal definir les nocions d'homomorfisme d'AOV, d'AOV-mòdul, etc.

A poc a poc, la prova de les conjectures de Conway-Norton-Thompson se centrà en l'obtenció d'una AOV dotada d'una acció del monstre. Calia, doncs, començar per la construcció d'una AOV que satisfés la fórmula de les dimensions:

$$\dim V_n = c(n), \quad \text{per a tot } n.$$

Donada una xarxa quadràtica L , definida positiva i parella, existeix un procediment que li associa una AOV. El procediment generalitza el que fa correspondre a L una àlgebra de Lie, que és com segueix. A partir d'una certa extensió central, determinada per la forma bilineal de L ,

$$1 \rightarrow \langle \pm 1 \rangle \rightarrow \hat{L} \rightarrow L \rightarrow 1,$$

es defineixen

$$\mathfrak{h}_L = L_{\mathbb{F}}, \quad \mathfrak{g}_L = \mathfrak{h}_L \oplus \sum_{\alpha \in \hat{L}_2} \mathbb{F}x_{\alpha},$$

on $\hat{L}_2 := \{\alpha \in \hat{L} \mid \bar{\alpha} \in L_2\}$. Un parèntesi de Lie escaient converteix \mathfrak{g}_L en una àlgebra de Lie i \mathfrak{h}_L en una subàlgebra de Cartan. Es té que $\dim \mathfrak{g} = \text{rg } L + \#L_2$. (Recordem que E_8 és un grup de Lie de rang $248 = 744/3$.)

Imitant la construcció anterior, es defineix una AOV

$$V_L = S(\hat{\mathfrak{h}}_{\mathbb{Z}}^-) \otimes \mathbb{F}[L],$$

on $\mathbb{F}[L]$ denota l'àlgebra de grup de la xarxa L , l'àlgebra

$$\hat{\mathfrak{h}}_{\mathbb{Z}} = \mathfrak{h} \otimes \mathbb{F}[t, t^{-1}] \oplus \mathbb{F}c = \coprod_{\substack{n \in \mathbb{Z} \\ n \neq 0}} \mathfrak{h} \otimes t^n \oplus \mathbb{F}c$$

és una àlgebra de Heisenberg, i $S(\hat{\mathfrak{h}}_{\mathbb{Z}}^-)$ és un espai de Fock. Quan L és la xarxa d'arrels d'una àlgebra de Lie, l'àlgebra d'operadors de vèrtexs V_L permet recuperar l'àlgebra de Lie per mitjà del quocient V/DV . En general, el pes d'un element homogeni $\alpha \in V_L$ és donat per

$$\text{wt } v_\alpha = \frac{1}{2} \langle \alpha, \alpha \rangle.$$

De les definicions, s'obté la fórmula

$$\dim_* V = \frac{\theta_L(q)}{\eta(q)^{\text{rang } L}},$$

on θ_L és la funció θ de L . El denominador de la fórmula prové de la dimensió graduada de $S(\hat{\mathfrak{h}}_{\mathbb{Z}}^-)$.

En considerar les AOV obtingudes a partir de Γ_8 i de Λ_{24} pel procediment esmentat, s'obtenen les dimensions graduades:

$$\begin{aligned} \dim_* V_{\Gamma_8} &= (J(q) + 744)^{1/3}, \\ \dim_* V_{\Lambda_{24}} &= J(q) + 24. \end{aligned}$$

Cap de les dues, doncs, no proporciona la funció J . L'AOV associada a la xarxa de Leech sembla força apropiada, però hi sobra el sumand 24.

10 L'àlgebra natural del monstre

En el període 1984-1988, Frenkel, Lepowsky i Meurman construïren una AOV amb el monstre com a grup d'automorfismes. La denotaren per V^\natural , a fi de fer palesa la seva naturalitat. La construcció de V^\natural ocupa tot un llibre de cinc-centes pàgines.

La definició de V^\natural generalitza les que hem vist abans. La modificació més important la dóna el fet que V^\natural incorpora un sector torçat d'operadors. V^\natural es descompon com segueix:

$$V^\natural = V_{\Lambda_{24}}^+ \oplus (V_{\Lambda_{24}}^T)^+.$$

Cadascun dels seus sumands s'obté a partir de l'AOV associada a la xarxa de Leech $V_{\Lambda_{24}}$. El símbol $+$ denota el subespai fix per la involució canònica del doble recobriments $\hat{\Lambda}_{24}$ de Λ_{24} utilitzat en la construcció de $V_{\Lambda_{24}}$. L'espai torçat $V_{\Lambda_{24}}^T$ es defineix per

$$V_{\Lambda_{24}}^T = S(\hat{\mathfrak{h}}_{\mathbb{Z}+1/2}^-) \otimes T,$$

on

$$\hat{\mathfrak{h}}_{\mathbb{Z}+1/2} = \coprod_{\substack{n \in \mathbb{Z}+1/2 \\ n \neq 0}} \mathfrak{h} \otimes t^n \oplus \mathbb{F}c$$

és una àlgebra de Heisenberg torçada i T és un cert $\hat{\Lambda}_{24}$ -mòdul canònic. V^{\natural} és una AOV de dimensió conforme 24. El sumand $V_{\Lambda_{24}}^+$ és una sub-AOV; el sumand $(V_{\Lambda_{24}}^T)^+$ és un mòdul sobre el primer sumand.

El component homogeni V_1^{\natural} coincideix amb l'àlgebra de Griess, \mathcal{B} . El vector

$$\frac{1}{2}\omega$$

és l'element neutre de $\mathcal{B} = V_1^{\natural}$. Si $u, v \in V_1^{\natural}$, la identitat

$$[u_{r+1}, v_s] - [u_r, v_{s+1}] = (u \times v)_{r+s} + \frac{1}{2}\langle u, v \rangle r(r-1)\delta_{r+s,1}$$

permet llegir la multiplicació, \times , de \mathcal{B} . Per tant, l'estructura de V^{\natural} recupera l'estructura d'àlgebra unitària, commutativa i no associativa, de l'àlgebra de Griess, \mathcal{B} .

L'estructura de V^{\natural} és natural, també, des del punt de vista físic. Correspon a una teoria conforme autodual de camps meromorfs sobre un C_2 -orbifold abelià. L'orbifold s'obté en prendre el quocient del tor $\mathbb{R}^{24}/\Lambda_{24}$ per un grup cíclic d'ordre 2. Com a conseqüència de la descomposició en suma directa de V^{\natural} , els operadors de vèrtexs de V^{\natural} es descomponen en una part amb gradació entera i una altra amb gradació semientera:

$$Y(v, z) = Y_{\mathbb{Z}}(v, z) \oplus Y_{\mathbb{Z}+1/2}(v, z).$$

Els camps bosònics provenen del sector no torçat. Els camps fermiònics els defineix el sector torçat.

Descriurem tot seguit els fets bàsics en què es fonamenta l'acció del monstre en V^{\natural} . En la construcció originària de Griess del monstre, aquest s'obtenia a partir d'una involució w i del seu centralitzador $C_M(w)$. El centralitzador de la involució és una extensió central del grup de Conway Co_1 per un 2-grup extraespecial. Recordem que $Co_0 = \text{Aut}(\Lambda_{24})$. El subgrup $C_M(w)$ de M respecta la descomposició en suma directa de V^{\natural} , i proporciona l'acció associada a la xarxa de Leech. La involució w de M intercanvia el sector torçat i el sector no torçat. El monstre és el grup d'automorfismes de V^{\natural} :

$$M = \text{Aut}(V^{\natural}).$$

El grup M és generat per $C_M(w)$ i un grup S_3 de permutacions, que conté la involució principal w . La simetria d'ordre 3 de S_3 és una simetria amagada, originada per la identitat de Jacobi de V^{\natural} . Ara ja se satisfà

$$\dim_* V^{\natural} = J(q).$$

Com que el monstre opera en l'espai graduat V^{\natural} , i aquest té la dimensió graduada correcta, l'acció del monstre en cada subespai V_n^{\natural} proporciona una representació de

M de grau $c(n)$. En descompondre aquestes representacions en suma de representacions irreductibles s'obtenen les igualtats

$$\begin{aligned} V_1^{\natural} &= \chi_1 + \chi_2, \\ 196\,884 &= 1 + 196\,883; \\ V_2^{\natural} &= \chi_1 + \chi_2 + \chi_3, \\ 21\,493\,760 &= 1 + 196\,883 + 21\,296\,876; \\ V_3^{\natural} &= 2\chi_1 + 2\chi_2 + \chi_3 + \chi_4, \\ 864\,299\,970 &= 2 + 393\,766 + 21\,296\,876 + 842\,609\,326; \\ V_5^{\natural} &= 4\chi_1 + 5\chi_2 + 3\chi_3 + 2\chi_4 + \chi_5 + \chi_6 + \chi_7, \\ (\dots) \end{aligned}$$

La igualtat $\mathcal{B} = V_1^{\natural}$ ($\dim V_1^{\natural} = 196\,884$) recupera la primera construcció del monstre com a grup d'automorfismes de l'àlgebra de Griess.

Hem vist, doncs, com la construcció de V^{\natural} permet provar la part de les conjectures de Conway-Norton-Thompson relativa a l'element neutre. És a dir, explica els clars de lluna produïts per la primera columna de la taula de caràcters del monstre. Per acabar, només resta explicar els clars de lluna de les 193 columnes restants!

En general, calcular la sèrie de Thompson T_m per als elements $m \in M$ del centralitzador $C_M(w)$ no és difícil, pel fet que aquests elements conserven la descomposició de V^{\natural} en suma directa. El càlcul de T_m quan m no és del centralitzador requereix un tractament especial. En parlarem en la secció que segueix.

11 L'àlgebra de Lie del monstre

Per explicar la resta de clars de lluna del monstre, ha calgut fer-lo operar no sols en la AOV donada per V^{\natural} , sinó també en una àlgebra de Lie de dimensió no finita. De nou, els matemàtics s'inspiren en els físics.

En les AOV, tots els espais propis per l'operador L_0 són de dimensió finita. Prescindint d'aquesta exigència, s'arriba al concepte d'àlgebra de vèrtexs (AV).

Considerem la xarxa de Lorentz: $II_{1,1} = \mathbb{Z}^2$, que és l'única xarxa indefinida i autodual en dimensió 2. La matriu del producte intern que la defineix és

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

A partir d'un doble recobriment de la xarxa de Lorentz $\hat{II}_{1,1}$, es construeix una AV: $V_{II_{1,1}}$. El producte tensorial d'AV

$$V^{\natural} \otimes V_{II_{1,1}}$$

proporciona una AV de dimensió conforme igual a $24 + 2 = 26$. És a dir, els generadors de l'àlgebra de Virasoro satisfan les relacions

$$[L_m, L_n] = (m - n)L_{m+n} + \frac{26}{12}(m^3 - m)\delta_{m,-n}I.$$

En teoria de cordes, 26 és una dimensió crítica de l'espai-temps. Sigui

$$P^i = \{v \mid L_0(v) = iv, L_j(v) = 0, \text{ si } j > 0\}$$

el subespai de vectors propis de pes i que aïlla l'àlgebra de Virasoro.

Un cert quocient de l'àlgebra de Lie P^1/DP^0 , obtingut en treure'n els estats espuris, proporciona l'àlgebra de Lie del monstre:

$$\mathcal{M} := P^1/DP^0K.$$

Més precisament, \mathcal{M} és una àlgebra de Kac-Moody generalitzada, que té $II_{1,1}$ com a xarxa d'arrels.

\mathcal{M} és graduada sobre $II_{1,1} = \mathbb{Z} \oplus \mathbb{Z}$. En ella hi opera el monstre, preservant-ne la gradació. En tenir present l'estructura de M -mòduls, se satisfà la important relació:

$$\mathcal{M}(r, s) = \begin{cases} V_{rs}^{\frac{1}{2}}, & \text{si } (r, s) \neq (0, 0), \\ \mathbb{R}^2, & \text{altrament.} \end{cases}$$

La fórmula del producte per a la funció J

$$J(p) - J(q) = p^{-1} \prod_{\substack{r > 0 \\ s \geq -1}} (1 - p^r q^s)^{c(rs)}$$

proporciona el denominador de \mathcal{M} .

12 El teorema de Borchers

La construcció de l'àlgebra de Kac-Moody \mathcal{M} de la secció anterior és deguda a R. E. Borchers [5]. Per mitjà de l'acció de M en \mathcal{M} , Borchers ha pogut provar les conjectures de Conway-Norton-Ogg-Thompson, amb tota la seva generalitat.

Com tota àlgebra de Kac-Moody generalitzada, l'àlgebra del monstre es descompon en suma directa,

$$\mathcal{M} = E \oplus H \oplus F,$$

on H és una subàlgebra de Cartan, E és la subàlgebra que correspon a les arrels positives i F , a les negatives. El càlcul de l'homologia $H(E)$, així com també la igualtat de M -mòduls virtuals $II_{1,1}$ -graduats

$$\Lambda^*(E) = H_*(E)$$

proporciona la identitat

$$p^{-1} \Lambda^* \left(\sum_{\substack{r > 0 \\ s \in \mathbb{Z}}} V_{rs}^{\frac{1}{2}} p^r q^s \right) = \sum_r V_r^{\frac{1}{2}} p^r - \sum_s V_s^{\frac{1}{2}} q^s.$$

En considerar l'acció de M en aquests mòduls s'obtenen les fórmules, anomenades *de reproducció*,

$$\begin{aligned} & p^{-1} \exp \left(- \sum_{i > 0} \sum_{\substack{r > 0 \\ s \in \mathbb{Z}}} \text{Tr}(m^i \mid V_{rs}^{\frac{1}{2}}) p^{ri} q^{si} / i \right) \\ &= \sum_{r \in \mathbb{Z}} \text{Tr}(m \mid V_r^{\frac{1}{2}}) p^r - \sum_{s \in \mathbb{Z}} \text{Tr}(m \mid V_s^{\frac{1}{2}}) q^s, \quad m \in M. \end{aligned}$$

Referències

- [1] BAYER, P. «Monstruos, cuerdas, fantasmas y claros de luna», *Fronteras de la Ciencia y la Tecnología*, 14 (1997), 11-15.
- [2] BAYER, P., LLORENTE, P., VILA, N. « \widetilde{M}_{12} comme groupe de Galois sur \mathbb{Q} », *C. R. Acad. Sci. Paris*, 303 (1986), 277-280.
- [3] BAYER, P., TRAVESA, A. *Corbes modulares: Taules*, Notes del Seminari de Teoria de Nombres (UB-UAB-UPC), 1 (1992), ISBN: 84-604-3577-6.
- [4] BELAVIN, A. A., POLYAKOV, A. N., ZAMOLODCHIKOV, A. B. «Infinite conformal symmetries in two-dimensional quantum field theory», *Nuclear Physics*, B 241 (1984), 333-380.
- [5] BORCHERDS, R. E. «Monstrous moonshine and monstrous Lie superalgebras», *Invent. math.*, 109 (1992), 405-444.
- [6] BORCHERDS, R. E. «Sporadic Groups and String Theory», *First European Congress of Maths. Paris, 1992*, I, 421-431, Birkhäuser, 1992.
- [7] BORCHERDS, R. E. «Automorphic forms on $O_{s+2,2}(\mathbb{R})^+$ and generalized Kac-Moody algebras», *Proceed. of the int. congress of math., ICM'94, Zurich*, II, 744-752, Birkhäuser, 1995.
- [8] BORCHERDS, R. E. «Automorphic forms on $O_{s+2,2}(\mathbb{R})^+$ and infinite products», *Invent. math.*, 120 (1995), 161-213.
- [9] BORCHERDS, R. E., RYBA, A. J. E. «Modular Moonshine II», *Duke Math. J.*, 83 (1996), 435-459.
- [10] BROUÉ, M. «Séminaire sur les groupes finis», t. I, *Publ. Math. de l'Université de Paris VII* (1983) 105-127.
- [11] CHEN, I., YUI, N. «Singular values of Thompson series», *Groups, Difference Sets, and the Monster*, Proceed. of a Special Research Quarter at The Ohio State University, primavera 1993, Walter de Gruyter, 1996.
- [12] CONWAY, J. H. «Monsters and Moonshine», *The Math. Intelligencer*, 2, n. 4 (1980), 165-171.
- [13] CONWAY, J. H. «A simple construction for the Fischer-Griess monster group», *Invent. math.*, 79 (1980), 513-540.
- [14] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A., WILSON, R. A. *Atlas of Finite groups*, Clarendon Press, 1985.
- [15] CONWAY, J. H., NORTON, S. P. «Monstrous moonshine», *Bull. London Math. Soc.*, 11 (1979) 308-339.
- [16] CONWAY, J. H., SLOANE, N. J. A. *Sphere Packings, Lattices and Groups*, GMW 290, Springer, 1993.
- [17] DEDEKIND, R. «Schreiben an Herrn Borchardt über die Theorie der elliptischen Modul-Functionen» *J. reine u. angew. Math.*, 83 (1877), 265-292.
- [18] DYSON, F. J. «Unfashionable Pursuits», *The Math. Intelligencer*, 5, n. 3 (1983), 47-54.
- [19] FEIT, W., THOMPSON, J. «Solvability of groups of odd order» *Pacific J. Math.*, 13 (1963), 775-1029.
- [20] FRENKEL I., LEPOWSKY, I., MEURMAN, A. *Vertex Operator Algebras and the Monster*, Pure and Applied Mathematics 134, Academic Press, 1988.
- [21] GODDARD, P., THORN, C. B. «Compatibility of the dual Pomeron with unitarity and the absence of ghosts in the dual resonance model», *Physics Letters*, B 40, 2 (1972), 235-238.

- [22] GORENSTEIN, D. *Finite Simple Groups, An introduction to their classification*, Plenum Press, New York, 1982.
- [23] GREEN, M. B., SCHWARZ, J. H., WITTEN, E. *Superstring theory, I-II*, Cambridge monographs on Mathematical Physics, Cambridge University Press, 1988.
- [24] GRIESS, R. L. «A construction of F_1 as automorphisms of a 196,883 dimensional algebra» *Proc. Natl. Acad. Sci. USA*, 78 (1981), 689-691.
- [25] GRIESS, R. L. «The Friendly Giant», *Invent. math.*, 69 (1982), 1-102.
- [26] KAC, V. *Vertex Algebras for Beginners*, AMS, University Lecture Series, 10, 1997.
- [27] LEECH, J. «Notes on Sphere Packings» *Canadian J. Math.*, 19 (1967), 251-267.
- [28] LEPOWSKY, J. «Perspectives on Vertex Operators and the Monster», *Proceed. of Symp. in Pure Maths.*, 48 (1988), 181-197.
- [29] MATHIEU, E. L. «Mémoire sur l'étude des fonctions de plusieurs quantités», *J. de Math. Pures et Appliqués*, 6 (1861), 241-323.
- [30] MIYAMOTO, M. «Representation Theory of Code Vertex Operator Algebras», *J. Algebra*, 201 (1998), 115-150.
- [31] OGG, A. P. «Hyperelliptic modular curves», *Bull. Soc. Math. France*, 102 (1974), 449-462.
- [32] OGG, A. P. «Automorphismes de courbes modulaires», *Séminaire Delange-Pisot-Poitou*, 16e année 1974/75, 7, 7-01-7-08.
- [33] QUEEN, L. «Modular Functions Arising From Some Finite Groups», *Math. of Comp.*, 37 (1981), 547-580.
- [34] SERRE, J-P. *Cours d'Arithmétique*, PUF, 1970.
- [35] SCHEITHAUER, N. R. «Vertex Algebras, Lie Algebras, und Superstrings», *J. Algebra*, 200 (1998), 363-403.
- [36] SHIMURA, G. *Introduction to the Theory of Automorphic Functions*, Iwanami Publ. Comp. i Princeton University Press, 1974.
- [37] SOLOMON, R. «On Finite Simple Groups and Their Classification», *Notices AMS*, 42, 2 (1995), 231-239.
- [38] THOMPSON, J. G. «Finite Groups and Modular Functions», *Bull. London Math. Soc.*, 11 (1979), 347-351.
- [39] THOMPSON, J. G. «A finiteness theorem for subgroups of $\mathbf{PSL}(2, \mathbb{R})$ which are commensurable with $\mathbf{PSL}(2, \mathbb{Z})$ », *Proc. Symp. Pure Math.*, 37 (1979), 533-555.
- [40] TITS, J. «Le Monstre [d'après R. Griess, B. Fischer et al.]», *Astérisque*, 121-122 (1985), Séminaire Bourbaki, 1983-84, 105-122.
- [41] TITS, J. «Le module du "moonshine"», *Astérisque*, 152-153 (1987), Séminaire Bourbaki, 1986-87, 285-303.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
 FACULTAT DE MATEMÀTIQUES
 UNIVERSITAT DE BARCELONA
 GRAN VIA CORTS CATALANES, 585
 08007 BARCELONA
 BAYER@MAT.UB.ES