Butlletí de la Societat Catalana de Matemàtiques
Vol. 11, núm. 1, 1996. Pàgs. 0–0.

Bellesa i Matemàtiques: al voltant de la paraula simetria*

Amparo López

> La paraula *simetria* designa aquell tipus de concordança entre les parts que les fa constitutives d'un tot. Bellesa i simetria tenen interessos en comú.
>
> **Hermann Weyl**

La citació elegida pertany a l'obra *Simetria* que recull quatre conferències pronunciades a la Universitat de Princeton el febrer de 1951 que l'autor, eminent físic i matemàtic, qualifica al pròleg com el seu cant del cigne abans de retirar-se de la docència. En aquest pròleg, Weyl descriu així llurs objectius: *exposar la gran varietat d'aplicacions del principi de simetria a les arts i a la natura; i aclarir, pas a pas, el significat filosoficomatemàtic de la idea de simetria, partint de la noció poc precisa de simetria com a harmonia de proporcions fins a desembocar a la idea general d'invariància d'una configuració d'elements sota l'acció d'un grup d'automorfismes.*

La fascinació que vaig sentir, fa ja molts anys, en llegir l'obra de Weyl, és una de les causes de l'elecció del títol i desenvolupament de la present exposició; d'altres són la importància creixent de la noció de simetria a la física i de la noció de grup d'automorfismes d'una estructura matemàtica com a objecte que conté informació, i, en les situacions més favorables, tota la informació, sobre l'estructura.

En aquest context intentaré:

1. Posar de manifest com les matemàtiques, en elucidar i fer rigorós el concepte de simetria, ajuden a captar què és *allò que és bell*. En aquest punt exposaré el contingut matemàtic de diverses manifestacions de la simetria en el món artístic; però no podré, per falta de temps, seguir, pas a pas, el camí que va de la simetria com a dada sensorial fins al seu significat matemàtic. La citada obra de Weyl, la lectura de la qual recomano vivament, compleix de sobres aquest recorregut.
2. Portar a la llum de la consideració algunes teories matemàtiques en les quals el joc *estructura–grup dels seus automorfismes o simetries* es realitzi de manera exemplar. L'elecció d'aquestes teories no obeeix a criteris objectius perquè tals criteris no existeixen, sinó que respon en última instància a la sensibilitat personal.

*La versió en llengua castellana d'aquest treball va aparèixer a *Publicaciones del Departamento de Matemáticas de la Universidad de Murcia*, **13**, (1995).

1 Rerefons matemàtic de la simetria artística

Començaré fixant la meva atenció en aquesta joia gòtica que és Santa Maria del Mar a Barcelona. Situats enfront de la façana principal flanquejada per dues torres octogonals, si la despullem, amb la imaginació, de llurs escultures exemptes i la dobleguem per l'eix vertical que passa pel centre de la seva porta, observem que els dos costats se sobreposen; hom enuncia aquest fet dient que la façana té simetria bilateral (les escultures seran el *granum salis*, la picardia asimètrica que ressalta encara més el canemàs simètric bàsic).

Però els matemàtics parlem en aquest cas de simetria especular o axial, i la definim així: si els vectors e_1, e_2 formen una base ortonormal del pla euclidià $\mathbb{R}^2$, la simetria d'eix e_1 és la transformació del pla en ell mateix definida per la matriu:

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

La transformació σ és involutiva, és a dir $\sigma^2 = \mathrm{Id}$.

També sabem que si B és la matriu d'un canvi de base ortonormal, la simetria mencionada, que està determinada pel seu eix e_1, es descriu en la nova base per la matriu $B\sigma B^t = B\sigma B^{-1}$. I d'una figura que és invariant per la simetria d'eix e_1 es diu que té aquest eix com a eix de simetria.

Torno de nou a Santa Maria del Mar. La planta de les seves torres és un octògon. Si al seu pla base fem un gir d'amplitud $\frac{\pi}{4}$ rad amb centre, el centre de l'octògon, és evident que la torre s'aplica en ella mateixa; per això es diu que té simetria rotacional d'ordre 8.

Matemàticament, un gir al pla d'amplitud α s'expressa en una base ortonormal mitjançant la matriu:

$$\sigma = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Aquí, un canvi a la base ortonormal afecta poc l'expressió del gir: la matriu és la mateixa si la nova base té la mateixa orientació que l'antiga i únicament s'ha de substituir α per $-\alpha$ si la nova base té l'orientació oposada.

Però la nostra torre no sols té simetria rotacional d'ordre 8 sinó també simetria axial respecte de les rectes que uneixen vèrtexs oposats i de les rectes que uneixen els punts mitjans de costats oposats de l'octògon base; i és natural preguntar-se quin és el conjunt de totes les seves simetries i fins i tot si existeix algun altre tipus de simetria. La resposta adequada només es pot obtenir després de formular el problema amb precisió; i això és el que farem seguidament. El meu objectiu en presentar els exemples anteriors era assenyalar, en i mitjançant dos casos concrets, l'enorme paper de la simetria en la creació de formes belles tant a les arts plàstiques com a l'arquitectura. Haig d'advertir que als exemples arquitectònics es tracta pròpiament amb figures espacials, però aquí ens limitarem al tractament matemàtic del pla.

1.1 Grups de simetria de figures planes finites

En les nostres definicions de simetria axial i rotacional apareixen involucrats angles o el concepte d'ortogonalitat i a més a més, si ens preguntem per transformacions que deixin invariants certes figures planes finites, és a dir acotades, hauran de ser transformacions que deixin fix un punt i que conservin la distància.

1.1.1 La noció d'isometria del pla euclidià D'aquesta manera, ens veiem obligats a considerar les aplicacions del pla vectorial euclidià (només en aquest es defineix un

concepte de distància i angle) que conserven el producte escalar o tensor euclidià habitual; però aquestes es diuen isometries i el seu conjunt té estructura de grup amb la composició: el grup ortogonal del pla euclidià, usualment denotat per $\mathrm{O}(2)$. Com bé sap fins i tot un estudiant de primer, un element de $\mathrm{O}(2)$ és o un gir o una simetria axial; el seu determinant decideix si és una cosa o una altra: 1 per al gir i -1 per a la simetria.

Si $\mathcal{F}$ és una figura plana finita amb centre a l'origen de coordenades, el conjunt d'isometries que la deixen invariant és un subgrup $G \subset \mathrm{O}(2)$, anomenat grup de simetria o d'automorfismes de $\mathcal{F}$; el raonament del paràgraf anterior mostra que les simetries de figures planes finites només poden ser girs o simetries axials.

Entre les figures planes acotades, la circumferència unitat S^1 ocupa un lloc especial, ja que el seu grup de simetria és el grup total $\mathrm{O}(2)$, de manera que aquest queda caracteritzat com el conjunt de les aplicacions lineals de $\mathbb{R}^2$ que deixen invariant S^1. La frase anterior enuncia el contingut matemàtic precís de la vella noció mítica dels grecs que considerava la circumferència com la figura perfecta quant a immutable.

Amb vista a determinar els subgrups de $\mathrm{O}(2)$ que són grups de simetria de figures planes finites, anem a recordar certes propietats d'aquest grup.

a) Com que un element de $\mathrm{O}(2)$ és un gir o una simetria, per a tot subgrup G es té el morfisme de grups:

$$\begin{aligned} \phi\colon G &\longrightarrow \{\pm 1\} \\ g &\longrightarrow \det g. \end{aligned}$$

El seu nucli H és el subgrup dels girs de G; i per tant o bé $G = H$, o bé existeix a G una simetria axial σ i l'índex de H en G és dos, i així $G = H \cup \sigma H$.

b) Sigui $\mathrm{SO}(2)$ el conjunt dels girs de $\mathrm{O}(2)$. Per a l'apartat anterior, $\mathrm{SO}(2) \simeq \mathrm{S}^1$ és un subgrup normal de $\mathrm{O}(2)$; però aquesta condició la comparteix amb tots els seus subgrups H com es posa de manifiest en el que segueix: si g és un gir i σ és una simetria axial, σg és una altra simetria axial (el seu determinant és -1) i en conseqüència:

$$(\sigma g)^2 = \mathrm{Id} \iff \sigma g = g^{-1}\sigma \iff \sigma g \sigma = g^{-1}.$$

c) Tot subgrup infinit H de $\mathrm{SO}(2)$ és dens, o amb altres paraules, tot gir es pot aproximar tant com es vulgui per elements de H.

La demostració d'aquest resultat s'inclou en un apèndix al final, però ara ens interessa assenyalar la seva traducció al llenguatge de grups de simetries de figures planes: si el grup de simetria G d'una tal figura $\mathcal{F}$ fos infinit i $x \in \mathcal{F}$, $\mathcal{F}$ contindria un subconjunt dens de la circumferència de centre a l'origen i que passa pel punt x; per tant, les figures tancades (aquelles que podem dibuixar) tindran grup de simetria finit o grup de simetria coincident amb $\mathrm{O}(2)$ o $\mathrm{SO}(2)$.

D'aquesta manera, es justifica el fet que limitem la nostra atenció als subgrups finits.

1.1.2 Subgrups finits de $\mathrm{O}(2)$ Començarem per determinar els subgrups finits de $\mathrm{SO}(2) \simeq \mathrm{S}^1$.

Si $H \subset \mathrm{S}^1$ té ordre n, el teorema de Lagrange permet afirmar:

$$H \subset \{z \in \mathrm{S}^1 \mid z^n = 1\}$$

on $\{z \in \mathrm{S}^1 \mid z^n = 1\}$ és el conjunt de les arrels complexes n-èsimes de la unitat i, per tant, consta de n elements.

En conseqüència, $H = \{z \in \mathrm{S}^1 \mid z^n = 1\}$, cosa que ens assegura que els únics subgrups finits de S^1 són els grups d'arrels n-èsimes de la unitat ($n \geq 1$). La traducció al llenguatge de girs és així: per a cada natural $n \geq 1$ existeix un únic subgrup d'ordre n de $\mathrm{SO}(2)$: el grup cíclic generat pel gir d'amplitud $2\pi/n$.

D'aquesta manera disposem d'una primera família de subgrups finits de $\mathrm{O}(2)$:

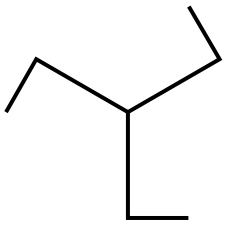
$$C_n = \langle g_{\frac{2\pi}{n}} \rangle, \qquad n \geq 1.$$

Si $n \geq 3$, considerem el polígon regular de n costats amb vèrtexs, els punts $\left(\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n}\right)$, $k = 0, 1, \cdots, n-1$. No és difícil observar geomètricament i demostrar analíticament que les isometries que el deixen fix són els girs $g_{\frac{2\pi}{n}}$ i les n simetries respecte dels eixos que es defineixen de la manera següent: el primer és l'eix de les x i la resta es construeix inductivament agafant com a eix següent la recta que forma un angle d'amplitud π/n amb l'últim eix construït. Aquest conjunt d'isometries forma un grup: el grup dihèdric D_n, que està generat per $g_{\frac{2\pi}{n}}$ i la simetria σ respecte de l'eix de les x. L'expressió de D_n, mitjançant generadors i relacions, és $\langle g, \sigma \mid \sigma^2 = g^n = 1, \sigma g = g^{n-1}\sigma \rangle$ ja que es disposa de la igualtat:

$$\sigma g_{\frac{2\pi}{n}} = g_{\frac{2\pi}{n}}^{n-1} \sigma.$$

Completem la llista dels grups D_n definint: $D_1 = \langle \sigma \rangle$ on σ designa la simetria axial respecte de l'eix de les x (D_1 és per tant cíclic d'ordre 2); i D_2 com el grup que consta dels girs d'amplitud π i 2π i de les simetries els eixos de les quals són l'eix de les x i l'eix de les y (s'observa immediatament que D_2 és un grup d'ordre 4 no cíclic).

Per construcció, D_n és el grup de les isometries que deixen fix el polígon regular de n costats; i resulta evident que C_n és el grup d'isometries que deixen fixa la figura següent: el conjunt dels raigs que uneixen l'origen amb els vèrtexs del polígon regular de n costats es completa afegint una pota ortogonal a cada raig pel seu extrem i de manera que els girs, però no les simetries axials de D_n, transformin potes en potes. A continuació es dibuixa una tal figura per a $n = 3$.



Triquetrum romà, antic símbol màgic, el grup de simetria del qual és C_3

Si $\mathcal{F}$ és una figura plana finita amb centre a l'origen de coordenades i grup de simetria $G \subset \mathrm{O}(2)$; i si $f \in \mathrm{O}(2)$, fàcilment es comprova que el grup de simetria de la figura $f\mathcal{F}$ és fGf^{-1}. Tot i així, és natural entendre que $\mathcal{F}$ i $f\mathcal{F}$ tenen el mateix tipus de simetria; això ens indica que el problema de determinar els tipus finits de simetries equival matemàticament al càlcul de les classes de conjugació dels subgrups finits de $\mathrm{O}(2)$. I a això últim respon el següent:

1 TEOREMA *$\{C_n, D_n \mid n \geq 1\}$ és una família completa de representants de les classes de conjugació dels subgrups finits de* $\mathrm{O}(2)$.

PROVA: Pel que s'ha dit anteriorment, si G és un grup finit que només consta de girs:

$$G = C_n, \quad \text{on } n = \operatorname{ord} G.$$

Si pel contrari G conté alguna simetria axial σ_1 i H és el subgrup de llurs girs, aleshores $G = H \cup \sigma_1 H$. Com dues simetries axials són sempre conjugades i els subgrups de $\mathrm{SO}(2)$ són subgrups invariants de $\mathrm{O}(2)$, es pot assegurar:

$$G \text{ i } D_n \quad (n = \operatorname{ord} H) \quad \text{són subgrups conjugats.}$$

En això anterior s'ha demostrat que tot subgrup finit de $\mathrm{O}(2)$ és conjugat d'un de la nostra llista; queda per veure que dos subgrups qualssevol de la mencionada llista no són conjugats. I això es dedueix del següent: Atès que la conjugació deixa invariant el determinant, un grup de la família C_n no pot ésser mai conjugat d'un de la família D_n; i dins de cadascuna de les famílies és evident que no pot haver-hi dos conjugats puix tenen ordre diferent (no obstant això, C_2 i D_1 són isomorfs, cosa que posa de manifest que la relació de conjugació és més fina, distingeix més que la d'isomorfia). □

1.2 Grups de simetria d'arabescs

Fins aquí hem centrat la nostra atenció en les figures finites; passem a considerar sanefes o frisos que solen consistir en la repetició periòdica i teòricament il·limitada d'un motiu o figura bàsics. En conseqüència, una sanefa és invariant per translació. D'aquesta manera, ens veiem obligats a considerar un nou tipus de simetria: la de translació, que és una isometria de l'espai euclidià afí.

Ja que hem detectat aquest nou tipus de simetria, anem a aplicar-lo a una situació més complexa: la dels ornaments de dimensió dos. Pensem en els bells arabescs que decoren les parets de l'Alhambra; si els analitzem ens adonem que en ells el motiu bàsic, que és una figura finita, es repeteix periòdicament segons dues direccions independents, en general no ortogonals entre elles, que anomenarem e_1, e_2. Per tant, el grup G d'automorfismes d'un tal arabesc, que imaginarem estès indefinidament en el pla, conté el subgrup de les translacions $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$; i ara ens preguntem quants són els possibles tipus per a G.

La resposta final és que existeixen exactament 17 tipus de simetria d'arabescs i que a l'Alhambra hi ha exemples de cadascun d'ells. Seguidament, intentaré exposar les idees matemàtiques bàsiques que permeten demostrar l'afirmació anterior.

En el pla afí, a diferència del que passa en el pla vectorial, no hi ha cap punt privilegiat. Un moviment o automorfisme del pla euclidià és una transformació que conserva la distància, però que en general no deixa fix cap punt, i és senzill comprovar que és el producte d'una translació per una isometria al voltant d'un punt prefixat O qualsevol. Matemàticament això s'expressa dient que el grup dels moviments $\mathcal{M}(2)$ és el producte semidirecte del grup de les translacions T ($\simeq \mathbb{R}^2$) pel grup $\mathrm{O}(2)$ o amb més precisió:

a) T és un subgrup normal de $\mathcal{M}(2)$.
b) $\mathrm{O}(2)$ actua sobre T: $f\tau_x = \tau_f x$, $f \in \mathrm{O}(2)$, $\tau_x \in T$.
   D'aquesta manera, T té estructura de $\mathbb{R}[\mathrm{O}(2)]-$mòdul.

c) Un moviment queda descrit per un parell $(\tau_x, f) \in T \times \mathrm{O}(2)$ i la composició en $\mathcal{M}(2)$ s'expressa en aquesta terminologia per la fórmula: $(\tau_x, f)(\tau_y, f_1) = (\tau_x + fy, ff_1)$. A més, es comprova fàcilment que:

$$(\tau_a, f)(\tau_x, \mathrm{Id})(\tau_a, f)^{-1} = (\tau_f x, \mathrm{Id}), \qquad \forall \tau_x \in T$$

cosa que assegura que l'acció de $\mathrm{O}(2)$ sobre T, que és l'acció ordinària de $\mathrm{O}(2)$ sobre $\mathbb{R}^2$, està definida per l'acció de $\mathcal{M}(2)$ sobre T mitjançant automorfismes interns (T és normal a $\mathcal{M}(2)$).

d) En particular això anterior implica que es disposa de la successió exacta de grups:

$$0 \longrightarrow T \longrightarrow \mathcal{M}(2) \xrightarrow{p} \mathrm{O}(2) \longrightarrow 1 \tag{1}$$

on $p(\tau_x, f) = f$.

Com hem vist anteriorment, un arabesc es caracteritza per ser invariant exactament per un reticle de translacions, $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ i per tant el seu grup de simetria G verifica: $G \cap T = L$. En conseqüència, la successió exacta (1) dóna lloc a la successió exacta:

$$0 \longrightarrow L \longrightarrow G \xrightarrow{p} H \longrightarrow 1$$

on: $H = \{h \in \mathrm{O}(2) \mid \exists(\tau_a, h) \in G \text{ per a algun } \tau_a \in T\}$. Observeu que en general $h \in H$ no implica que $(\mathrm{Id}, h) \in G$.

D'aquesta manera, hem associat a l'arabesc no només el seu grup de simetria G sinó també un subgrup H del grup $\mathrm{O}(2)$; però, i aquest és un punt clau, H actua fidelment sobre el reticle L, és a dir:

a) Els elements de H transformen L en ell mateix i aquesta acció està induïda per la de G sobre L mitjançant automorfismes interns:

$$(\tau_a, h)(\tau_x, \mathrm{Id})(\tau_a, h)^{-1} = (\tau_h x, \mathrm{Id}), \qquad \tau_x \in L,\ (\tau_a, h) \in G,$$

cosa que implica, per la normalitat de L en G, que: $hL = L$, $\forall h \in H$.

b) L'aplicació:

$$\begin{aligned} \varphi \colon H &\longrightarrow \mathrm{Aut}_{\mathbb{Z}}(L) \\ h &\longrightarrow h \colon \tau_x \mapsto \tau_h x \end{aligned}$$

és un morfisme injectiu de grups, puix L conté dos vectors linealment independents.

Això implica, en primer lloc, que $H \in \mathrm{O}(2)$ ha de ser finit, puix recordem que si no ho fos, tot gir del pla es podria aproximar per girs de H i en aquest cas el reticle contindria punts tan pròxims com es volgués, però això manifestament és impossible; per tant, H és isomorf a un dels de la nostra llista $\{C_n, D_n \mid n \geq 1\}$.

En segon lloc, H és isomorf a un subgrup finit de $\mathrm{Aut}_{\mathbb{Z}}(L)$; però, com és ben sabut, cada sistema de generadors o base de L defineix un isomorfisme $\alpha \colon \mathrm{Aut}_{\mathbb{Z}}(L) \to \mathrm{GL}(2, \mathbb{Z})$ de manera que si es considera el canvi de base en L definit per $A \in \mathrm{GL}(2, \mathbb{Z})$, l'isomorfisme definit per la nova base és:

$$\begin{aligned} \alpha' \colon \mathrm{Aut}_{\mathbb{Z}}(L) &\longrightarrow \mathrm{GL}(2, \mathbb{Z}) \\ h &\longrightarrow A^{-1}\alpha(h)A. \end{aligned}$$

Això permet entendre l'acció de H sobre L com una classe de conjugació de subgrups finits de $\mathrm{GL}(2,\mathbb{Z})$, cosa que, com anem a veure, imposa fortes restriccions a H.

Com a primera aproximació al problema, descrivim la situació sobre els racionals mitjançant el següent:

2 Teorema de restricció cristallogràfica *Si un element de* $\mathrm{GL}(2,\mathbb{Q})$ *té ordre finit* n*, llavors* $n = 1, 2, 3, 4$ *o* 6*.*

Prova: Si $f \in \mathrm{GL}(2,\mathbb{Q})$ té ordre n, el seu polinomi anul·lador és un divisor de $t^n - 1$. Però els divisors a $\mathbb{Q}[t]$ de $t^n - 1$ són els polinomis ciclotòmics: $P_r(t)$, $r \mid n$ (polinomi definidor sobre $\mathbb{Q}$ d'una arrel primitiva r-èsima de la unitat). +s ben sabut que els polinomis $P_r(t)$ es defineixen recurrentment i que el seu grau ve donat per la funció d'Euler: $\varphi(r)$.

El problema es redueix ara a calcular els naturals n per als quals $\varphi(r) \leq 2$; i aquests són $1, 2, 3, 4, 6$. (Es recorda que:

$$\varphi(p_1^{r_1} \cdots p_s^{r_s}) = p_1^{r_1-1}(p_1 - 1) \cdots p_s^{r_s-1}(p_s - 1)).$$

Per a aquests valors de n, els polinomis ciclotòmics són:

$$P_1(t) = t - 1, \qquad P_2(t) = t + 1, \qquad P_3(t) = t^2 + t + 1,$$
$$P_4(t) = t^2 + 1, \qquad P_6(t) = t^2 - t + 1.$$

A partir d'això anterior s'observa immediatament que les classes de conjugació d'elements d'ordre finit de $\mathrm{GL}(2,\mathbb{Q})$ admeten com a representants:

$$g_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{amb polinomi característic } (t-1)^2 \text{ i ordre 1;}$$
$$g_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{amb polinomi característic } (t+1)^2 \text{ i ordre 2;}$$
$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{amb polinomi característic } t^2 - 1 \text{ i ordre 2;}$$
$$g_3 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{amb polinomi característic } t^2 + t + 1 \text{ i ordre 3;}$$
$$g_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{amb polinomi característic } t^2 + 1 \text{ i ordre 4;}$$
$$g_6 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{amb polinomi característic } t^2 - t + 1 \text{ i ordre 6.}$$

En aquesta llista es fa patent que la classe de conjugació està determinada tant pel seu polinomi característic com pel parell: (el seu ordre, el seu determinant). El determinant distingeix les classes d'ordre dos, g_2 i σ perquè aquesta última és l'única classe amb determinant -1. □

Sigui $\sigma' = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; és immediat veure que σ i σ' són elements conjugats i que es té la llista de subgrups finits de $\mathrm{GL}(2,\mathbb{Q})$, dos qualssevol d'ells no conjugats:

$$\begin{array}{ccccc} \langle g_1\rangle, & \langle g_2\rangle, & \langle g_3\rangle, & \langle g_4\rangle, & \langle g_6\rangle, \\ \langle \sigma', g_1\rangle, & \langle \sigma', g_2\rangle, & \langle \sigma', g_3\rangle, & \langle \sigma', g_4\rangle, & \langle \sigma', g_6\rangle. \end{array} \tag{2}$$

Aquesta llista descriu les classes de conjugació dels subgrups finits de $\mathrm{GL}(2,\mathbb{Q})$ segons mostra el següent:

3 Teorema *Si H és un subgrup finit de* $\mathrm{GL}(2,\mathbb{Q})$*, H és conjugat d'un de la llista (2) a* $\mathrm{GL}(2,\mathbb{Q})$.

Prova: La recolzarem sobre el *teorema de Maschke*, que assegura que per a tot subgrup finit H de $\mathrm{GL}(n,\mathbb{R})$ existeix una mètrica euclidiana T_2 sobre $\mathbb{R}^n$ per la qual H és un subgrup d'isometries. La seva demostració és realment senzilla: si $(-,-)$ designa una mètrica euclidiana qualsevol basta definir

$$\mathrm{T}_2(x,y) = \sum_h \in H(hx,hy)$$

per a obtenir una mètrica euclidiana que verifiqui les condicions de l'enunciat. A la demostració ha quedat patent que existeixen nombroses mètriques (de fet, una infinitud indexada pel conjunt $\mathrm{GL}(n,\mathbb{R})/\mathrm{O}(2)$) que verifiquen l'enunciat.

Si H és un subgrup finit de $\mathrm{GL}(2,\mathbb{Q}) \subset \mathrm{GL}(2,\mathbb{R})$, el teorema de Maschke ens diu que existeix $A \in \mathrm{GL}(2,\mathbb{R})$ tal que:

$$AHA^{-1} = C_n \quad \text{o bé} \quad AHA^{-1} = D_n, \qquad n = 1,2,3,4,6.$$

Si $AHA^{-1} = C_n$, H està generat per un element $\overline{g}_n$ d'ordre n i determinant 1; cosa que ens assegura (vegeu la llista de les classes de conjugació d'elements d'ordre finit) que $\overline{g}_n$ és conjugat a $\mathrm{GL}(2,\mathbb{Q})$ de g_n. Això demostra que H i $\langle g_n\rangle$ són subgrups conjugats a $\mathrm{GL}(2,\mathbb{Q})$.

El mateix raonament mostra que si $AHA^{-1} = D_1$, aleshores H és conjugat a $\mathrm{GL}(2,\mathbb{Q})$ de $\langle \sigma', g_1\rangle$; i que si $AHA^{-1} = D_2$, llavors H és conjugat a $\mathrm{GL}(2,\mathbb{Q})$ de $\langle \sigma', g_2\rangle$.

Per als casos restants, H conjugat a $\mathrm{GL}(2,\mathbb{R})$ de D_n, $n = 3,4,6$, es precisa d'una argumentació més fina: $AHA^{-1} = D_n$ amb $A \in \mathrm{GL}(2,\mathbb{R})$ implica que existeixen elements $\overline{\sigma}$ de determinant -1 i $\overline{g}_n$ de determinant 1 tals que:

$$H = \langle \overline{\sigma}, \overline{g}_n \mid \overline{\sigma}^2 = \overline{g}_n^n = 1, \overline{\sigma}\ \overline{g}_n = \overline{g}_n^{n-1}\overline{\sigma}\rangle.$$

En particular, $\overline{\sigma}\,\overline{g}_n^{n-1} \in H$ té determinant -1 i ordre finit, per això és conjugat a $\mathrm{GL}(2,\mathbb{Q})$ de σ' i per tant existeix $0 \neq u \in \mathbb{Q}^2$ tal que $\overline{\sigma}\,\overline{g}_n^{n-1}(u) = u$. Si $e = \overline{g}_n^{n-1}(u)$, en ser $n \leq 3$ resulta que e, u formen una base de $\mathbb{Q}^2$, en la qual les matrius associades a $\overline{\sigma}$ i a $\overline{g}_n$ són respectivament σ' i g_n. Això demostra que H és un conjugat a $\mathrm{GL}(2,\mathbb{Q})$ del subgrup $\langle \sigma', g_n\rangle$. □

El teorema ha quedat demostrat i a la nostra llista de classes de conjugació de subgrups finits de $\mathrm{GL}(2,\mathbb{Q})$ podem reconèixer els nostres vells coneguts C_n i D_n, només que expressats en una base adequada als racionals; això justifica l'abús de llenguatge de designar-los mitjançant les mateixes lletres.

Però hem de passar als enters i aquí ens apareix el problema següent: $\mathrm{GL}(2,\mathbb{Z})$ és un subgrup de $\mathrm{GL}(2,\mathbb{Q})$ i, per tant, pot passar que subgrups conjugats a $\mathrm{GL}(2,\mathbb{Q})$ no ho siguin a $\mathrm{GL}(2,\mathbb{Z})$; i, en efecte, una comprovació immediata mostra que les matrius:

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

no són conjugades a $\mathrm{GL}(2,\mathbb{Z})$ ja que no existeix cap matriu B tal que ella i la seva inversa tinguin coeficients enters i que verifiqui: $B\sigma B^{-1} = \sigma'$. Per aquesta raó, a la llista de les classes de conjugació de subgrups de $\mathrm{GL}(2,\mathbb{Z})$ apareixen no només els grups de la llista (2) sinó també els grups $\langle \sigma, g_1\rangle$ i $\langle \sigma, g_2\rangle$; però tampoc aquests són suficients per a obtenir totes les classes de conjugació, com mostra el següent:

4 Teorema *Les classes de conjugació dels subgrups finits de* $\mathrm{GL}(2,\mathbb{Z})$ *estan descrites per la llista de grups següent, dos qualssevol d'ells no conjugats entre ells:*

$$\begin{array}{lll} C_1 = \langle g_1 \rangle, & D_1' = \langle \sigma', g_1 \rangle, & D_1'' = \langle \sigma, g_1 \rangle, \\ C_2 = \langle g_2 \rangle, & D_2' = \langle \sigma', g_2 \rangle, & D_2'' = \langle \sigma, g_2 \rangle, \\ C_3 = \langle g_3 \rangle, & D_3' = \langle \sigma', g_3 \rangle, & D_3'' = \langle -\sigma', g_3 \rangle, \\ C_4 = \langle g_4 \rangle, & D_4 = \langle \sigma', g_4 \rangle, & \\ C_6 = \langle g_6 \rangle, & D_6 = \langle \sigma', g_6 \rangle. & \end{array} \tag{3}$$

La demostració, relegada a un apèndix, es basa en certs resultats de formes quadràtiques enteres. Aquests fan el paper, actuen com a substituts, del teorema de classificació d'endomorfismes d'un espai vectorial, que, com s'observa en el que hem vist anteriorment, és decisiu per a trobar les classes de conjugació dels subgrups d'ordre finit en el grup lineal sobre un cos.

Els teoremes anteriors no només demostren que els 13 grups de la llista (3) constitueixen les úniques possibilitats per a l'acció fidel de H sobre L sinó que contenen la informació sobre les restriccions que l'acció de H imposa al reticle. Per obtenir la llista bastarà amb explicitar per a cadascun dels mencionats 13 grups el tipus de base de L, inclosa la seva descripció mètrica.

+s evident que C_1 i C_2 deixen fix qualsevol reticle.

Si l'acció és segons C_n, $n = 3, 4, 6$, i puix que $g_n = \left(\begin{smallmatrix} 0 & -1 \\ 1 & \tau_n \end{smallmatrix}\right)$ on τ_n és la traça de g_n, el reticle admet un sistema de generadors del tipus $\{e, g_n(e)\}$; però g_n no és més que el gir de $\frac{2\pi}{n}$ rad expressat en una base adequada al reticle L i per tant no ortonormal. D'aquesta manera, queda patent que H és el grup generat pel gir de $\frac{2\pi}{n}$ rad i que L admet un sistema de generadors format per dos vectors de la mateixa longitud i tals que el seu angle és de $\frac{2\pi}{n}$ rad. Particularitzant s'obté: per a C_4, el reticle admet un sistema de generadors format per dos vectors ortogonals de la mateixa longitud. Per a C_3, es té un sistema de generadors $\{e, g_3(e)\}$ format per dos vectors d'igual longitud i angle de $\frac{2\pi}{3}$ rad, però és immediat comprovar que els vectors d'igual longitud: $e, -g_3^2(e)$, l'angle dels quals és de $\frac{2\pi}{6}$ rad segueixen generant L; això posa de manifest que C_3 i C_6 imposen les mateixes condicions sobre L: *L admet un sistema de generadors format per dos vectors d'igual longitud i tals que el seu angle és de* $\frac{2\pi}{6}$ rad.

Si l'acció és segons D_1' i puix que $\sigma' = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, el reticle admet un sistema de generadors del tipus $\{e, \sigma'(e)\}$; però σ' no és més que la simetria axial d'eix $e + \sigma'(e)$ expressada en la base $e, \sigma'(e)$ adequada al reticle L. Això assegura que L admet un sistema de generadors $\{e_1, e_2\}$ on els vectors e_1, e_2 tenen la mateixa longitud i el seu angle no està subjecte a cap restricció; i H és el grup generat per la simetria axial amb eix en la bisectriu de l'angle format per e_1 i e_2.

Si l'acció és segons D_1'' i puix que $\sigma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, el reticle admet un sistema de generadors del tipus $\{e_1, e_2\}$ per al qual existeix una simetria axial tal que deixa fix e_1 i transforma e_2 en $-e_2$. Aixòanterior permet afirmar que H és el grup generat per una simetria axial i que el reticle admet com a sistema de generadors un parell de vectors ortogonals: $\{e_1, e_2\}$ tal que el primer d'ells defineix l'eix de la simetria que genera H.

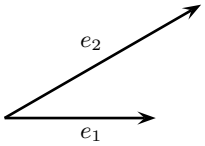
Raonant de manera anàloga, o sigui atenent no a H i L per separat sinó a la seva interrelació que ve donada per l'expressió dels elements de $H \subset \mathrm{O}(2)$ en una base que generi el reticle L, s'obté, per a les restants accions de H, el següent:

- Si l'acció és per D_2', el reticle $L = \langle e_1, e_2 \rangle$ amb e_1, e_2 vectors de la mateixa longitud

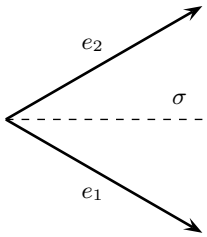
i angle qualsevol; i els elements de H són, a més de $\pm\,\mathrm{Id}$, les simetries axials amb eixos e_1+e_2 i e_1-e_2 (bisectrius dels vectors de la base de L).

- Si l'acció és per D_2'', el reticle $L=\langle e_1,e_2\rangle$ amb e_1,e_2 vectors ortogonals i els elements de H són, a més de $\pm\,\mathrm{Id}$, les simetries axials amb eixos e_1 i e_2.
- Si l'acció és per D_3', el reticle $L=\langle e_1, e_2=g_3(e_1)\rangle$, és a dir, e_1,e_2 són vectors d'igual longitud que formen un angle de $\frac{2\pi}{3}$ rad; i H està generat pelgir de $\frac{2\pi}{3}$ rad i la simetria axial amb eix $e_1+e_2=g_3^2(e_1)$ (tingueu en compte que la descripció de σ' assegura que $\sigma'(e_1)=e_2=g_3(e_1)$).
- Si l'acció és per D_3'', el reticle $L=\langle e_1, e_2=g_3(e_1)\rangle$, o sigui e_1,e_2 són vectors d'igual longitud que formen un angle de $\frac{2\pi}{3}$ rad; i H està generat pel gir de $\frac{2\pi}{3}$ rad i la simetria axial amb eix e_1-e_2.
- Si l'acció és per D_4, el reticle $L=\langle e_1,e_2\rangle$ on e_1,e_2 són vectors ortogonals i d'igual longitud; i H està generat pel gir de $\frac{\pi}{2}$ rad i la simetria axial amb eix e_1+e_2 (diagonal del quadrat de costats e_1,e_2).
- Si l'acció és per D_6, el reticle $L=\langle e_1, e_2=g_6(e_1)\rangle$, és a dir e_1,e_2 són vectors d'igual longitud que formen un angle de $\frac{\pi}{3}$ rad; i H està generat pel gir de $\frac{\pi}{3}$ rad i la simetria axial amb eix e_1+e_2.

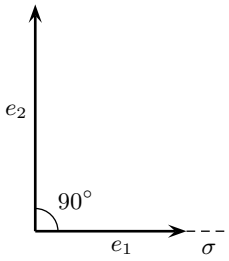
Els dibuixos següents, en els quals els vectors e_1,e_2 representen un sistema de generadors del reticle i en els quals l'eix d'una simetria axial es dibuixa mitjançant una recta a traços, pretenen visualitzar el que s'ha dit fins aquí.



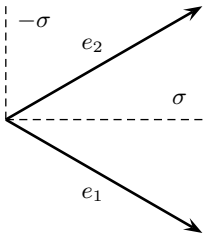
$H=\langle \mathrm{Id}\rangle$, $H=\langle -\,\mathrm{Id}\rangle$
Acció definidida per C_1 i C_2



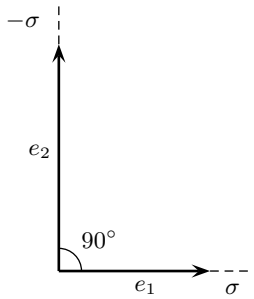
$H=\langle\sigma\rangle$
Acció definida per D_1'



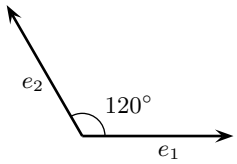
$H=\langle\sigma\rangle$
Acció definidida per D_1''



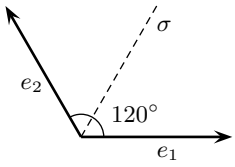
$H=\langle\pm\sigma\rangle$
Acció definida per D_2'



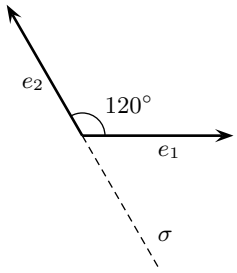
$H = \langle \pm\sigma \rangle$
Acció definidida per D_2''



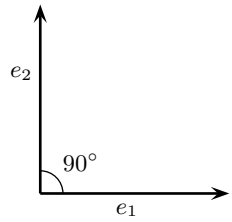
$H = \langle g_1 20° \rangle$
Acció definida per C_3



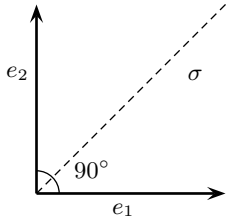
$H = \langle \sigma, g_1 20° \rangle$
Acció definidida per D_3'



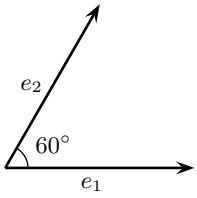
$H = \langle \sigma, g_1 20° \rangle$
Acció definida per D_3''



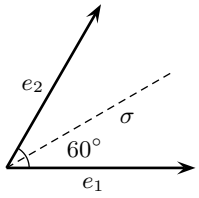
$H = \langle g_9 0° \rangle$
Acció definidida per C_4



$H = \langle \sigma, g_9 0° \rangle$
Acció definida per D_4



$H = \langle g_6 0° \rangle$
Acció definidida per C_6



$H = \langle \sigma, g_9 0° \rangle$
Acció definida per D_6

Si a la taula anterior es pren el producte semidirecte del reticle L pel grup H corresponent, s'obtenen 13 grups de simetria d'arabescs.

Després d'aquest llarg recorregut sobre l'estructura dels grups de simetria d'un arabesc, tornem al problema de la seva classificació sota el criteri d'isomorfia. Una primera pregunta s'imposa: entre els 13 grups, que són producte semidirecte del reticle L per un

grup finit H, n'hi poden haver dos que siguin isomorfs? La resposta negativa ens la dóna la següent:

5 PROPOSICIÓ *Sigui $\varphi\colon G \longrightarrow G_1$ un isomorfisme entre els grups de simetria d'arabescs G i G_1:*

$$0 \longrightarrow L \longrightarrow G \xrightarrow{p} H \longrightarrow 1,$$
$$0 \longrightarrow L_1 \longrightarrow G_1 \xrightarrow{p_1} H_1 \longrightarrow 1.$$

Es verifica:

a) φ restringit a L és un isomorfisme de L a L_1.

b) φ defineix de manera natural, per pas al quocient, un isomorfisme $\overline{\varphi}\colon H \to H_1$. Identificant H i H_1 mitjançant aquest isomorfisme, φ és un isomorfisme de $\mathbb{Z}[H]-$mòduls de L a L_1, o en altres paraules l'acció de H és la mateixa sobre L que sobre L_1.

PROVA: Començaré recordant alguna cosa de geometria plana elemental: un gir seguit d'una translació és un altre gir (evidentment amb centre diferent) i una simetria axial seguida d'una translació és o una simetria o un lliscament, és a dir, una simetria d'eix paral·lel al de la primera seguida d'una translació al llarg de l'eix. D'aquesta manera, tot moviment del pla és un gir, una simetria axial, una translació o un lliscament; girs i simetries axials són d'ordre finit mentre que translacions i lliscaments tenen ordre infinit. +s també evident que una simetria axial i una translació commuten si i només si es tracta d'una translació al llarg de l'eix de la simetria.

a) Per l'isomorfisme φ, una translació $\tau \in G$ s'aplica en un element $g_1 \in G_1$ d'ordre infinit, el qual per tant ha de ser una translació o un lliscament. Si g_1 és un lliscament, sigui $\tau_1 \in G_1$ una translació que no commuti amb g_1 (basta prendre una translació en una direcció diferent de la de l'eix de g_1); i sigui $g \in G$ tal que $\varphi g = \tau_1$. Si g és un lliscament, $g^2 \in G$ és una translació, per la qual cosa commuta amb τ. Per això, tant si g és una translació com si és un lliscament, es pot assegurar:

$$g_1\tau_1^2 = \varphi(\tau)\varphi(g^2) = \varphi(\tau g^2) = \varphi(g^2)\varphi(\tau) = \tau_1^2 g_1$$

i la contradicció a què hem arribat (g_1 és un lliscament amb eix no coincident amb la direcció de la translació τ_1^2 i per tant no poden commutar) demostra que g_1 és una translació.

b) A partir de l'apartat *a* anterior és immediat que φ defineix, per pas al quocient, un isomorfisme de H en H_1. Tenint en compte que l'acció de H sobre L ve donada per l'acció per conjugació de G sobre L, es té la igualtat òbvia:

$$\begin{aligned}\varphi(\tau_x, \mathrm{Id}) &= \varphi\left((\tau_a, h)(\tau_x, \mathrm{Id})(\tau_a, h)^{-1}\right)\\ &= \varphi(\tau_a, h)\varphi(\tau_x, \mathrm{Id})\left(\varphi(\tau_a, h)\right)^{-1}\end{aligned}$$

que es pot escriure en la forma: $\varphi(hx) = \overline{\varphi}(h)(\varphi x)$. □

Aquesta proposició, en afirmar que dos grups de simetria isomorfs corresponen a la mateixa acció del grup finit H sobre el reticle L, indica el programa per a trobar tots els grups de simetria d'arabescs: per a cadascuna de les 13 accions de H sobre L s'han de

trobar les classes d'isomorfia de grups G que siguin extensió de L per l'acció de H. Aquest problema, en el qual no entraré i per al qual remeto a Hiller, es tracta a les matemàtiques actuals mitjançant el grup de cohomologia $H^2(H, L)$ que mesura el nombre de classes d'extensions de L per H. En particular, si $H^2(H, L) = 0$, només existeix una extensió de L per H, que és el producte semidirecte; això és el que passa per als grups:

$$C_1,\ C_2,\ C_3,\ C_4,\ C_6,\ D_1',\ D_2',\ D_3',\ D_3'',\ D_6.$$

En canvi, $H^2(D_1'', L) = H^2(D_4, L) \simeq \mathbb{Z}/(2)$ i $H^2(D_2'', L) \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Això demostra que hi ha exactament 18 classes d'extensions de $\mathbb{Z}^2$ per a un subgrup finit de $\mathrm{GL}(2, \mathbb{Z})$. Però extensions diferents poden donar grups isomorfs i això passa únicament per a dues de les classes d'extensions de L per D_2''. D'aquesta manera s'obtindrien els 17 tipus anunciats.

L'anàlisi anterior dóna una idea de la quantitat de coneixement matemàtic implícit en la creació d'arabescs. També el món de l'art guarda en el seu si ombres o vestigis que esperen ser portats a la llum de la idea matemàtica.

2 Estructura matemàtica — grup dels seus automorfismes o simetries

En aquest apartat intentaré posar de manifest el joc *estructura — grup dels seus automorfismes*, considerant-lo en dues teories matemàtiques concretes.

2.1 Resolució per radicals de les equacions algebraiques i teoria de Galois

Considerem el polinomi separable (és a dir, sense arrels múltiples) de grau n amb coeficients racionals

$$f_n(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Pel teorema fonamental de l'àlgebra, aquest polinomi té n arrels complexes $\alpha_1, \ldots, \alpha_n$ i per tant es verifica

$$f_n(x) = x^n + a_1 x^{n-1} + \cdots + a_n = (x - \alpha_1) \cdots (x - \alpha_n).$$

Aquesta igualtat polinòmica dóna lloc a les fórmules de Cardano:

$$a_1 = -(\alpha_1 + \cdots + \alpha_n), \quad a_2 = \sum_i < j \alpha_i \alpha_j, \quad \ldots, \quad a_n = (-1)^n \alpha_1 \cdots \alpha_n.$$

D'aquí prové, de manera natural, la definició dels anomenats polinomis simètrics elementals en n variables:

$$\begin{aligned} s_1(x_1, \ldots, x_n) &= -(x_1 + \cdots + x_n), \\ s_2(x_1, \ldots, x_n) &= \sum_i < j x_i x_j, \\ &\vdots \\ s_n(x_1, \ldots, x_n) &= (-1)^n x_1 \cdots x_n. \end{aligned}$$

Sota quines condicions $\alpha_1, \ldots, \alpha_n$ es poden expressar en funció dels coeficients $a_1, \ldots, a_n$ utilitzant només les operacions aritmètiques elementals i l'extracció d'arrels? Aquest és

el famós problema de la resolubilitat per radicals de les equacions algebraiques; un problema que va atreure l'atenció dels matemàtics des que Cardano va resoldre en el s. XVI l'equació general de grau 3. Per a $n \geq 5$ el problema va romandre obert fins que Abel i sobretot Galois, que va morir quan tenia 21 anys, el 1832, li varen donar una solució brillant.

Si $K = \mathbb{Q}(a_1, \ldots, a_n)$ és el cos de les funcions racionals sobre $\mathbb{Q}$ en $a_1, \ldots, a_n$, podem considerar l'ideal I dels polinomis

$$P(y_1, \ldots, y_n) \in K[y_1, \ldots, y_n] \quad \text{tals que} \quad P(\alpha_1, \ldots, \alpha_n) = 0;$$

per exemple, $s_i(y_1, \ldots, y_n) - a_i$, $f_n(y_i)$, són polinomis que pertanyen a I.

Amb aquesta notació, $K[y_1, \ldots, y_n]/I \simeq K[\alpha_1, \ldots, \alpha_n]$.

Però si ens hi fixem bé, els polinomis de I són les relacions o *lleis* que lliguen les arrels $\alpha_1, \ldots, \alpha_n$. Aquestes arrels no formen només un conjunt de n elements, sinó un conjunt de n elements amb uns certs lligams: els lligams definits per I.

Si un automorfisme sempre és una aplicació que conserva l'estructura, en el nostre cas els automorfismes han de ser les bijeccions del conjunt $\alpha_1, \ldots, \alpha_n$ que deixin invariants les relacions existents entre els seus elements. Però, amb la composició, aquests automorfismes tenen estructura de grup: el subgrup del grup simètric $\mathcal{S}_n$ format per les permutacions σ tals que $P \in I \Longrightarrow P \circ \sigma \in I$. I aquest és el grup de Galois associat a l'equació $f_n(x)$. En la literatura actual s'acostuma a definir el grup de Galois com el grup dels automorfismes del cos $K[\alpha_1, \ldots, \alpha_n]$ que deixen fixos els elements del cos K; però és senzill de veure que les dues definicions coincideixen.

Així, es fa evident que el grup de Galois conté informació sobre el conjunt de les arrels, i el teorema principal de la teoria de Galois afirma que aquesta informació és suficient per trobar les arrels de l'equació (sempre i que s'hagi pogut determinar el seu grup de Galois). I també és clar que com més relacions hi hagi entre les arrels, més petit serà el grup de Galois, i per tant més fàcil serà de determinar aquestes arrels.

El teorema citat és tan conegut que ni tan sols l'enunciaré; però sí que vull donar una idea de com s'aplica aquesta teoria a dos problemes famosos, un dels quals ja ha estat esmentat:

2.1.1 La resolució per radicals En la seva breu memòria, Galois caracteritza les equacions algebraiques que es poden resoldre per radicals com aquelles on totes les arrels són funcions racionals de dues d'elles qualssevol. Aquesta propietat es reflectirà en el seu grup de Galois i aquest reflex és la definició actual de grup resoluble: G és resoluble si conté una cadena de subgrups

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = 1$$

on cadascun d'ells és un subgrup normal del que el precedeix i els quocients $G_i/G_i + 1$ són abelians.

Quan parlem de l'equació general de grau n, ens referim al fet que els seus coeficients són nombres arbitraris, la qual cosa es tradueix matemàticament dient que $a_1, \ldots, a_n$ són indeterminades i per tant K és el cos de funcions racionals sobre $\mathbb{Q}$ en n variables.

En aquest cas, el grup de Galois és el grup $\mathcal{S}_n$ total, i és fàcil de demostrar que si $n \geq 5$ llavors $\mathcal{S}_n$ no és resoluble. Per tant, per a $n \geq 5$ no existeix cap fórmula general —vàlida per a tots els coeficients— que expressi les arrels de l'equació algebraica en funció dels coeficients fent servir només radicals.

2.1.2 Els polígons regulars construïbles amb regle i compàs Els vèrtexs d'un polígon regular de n costats corresponen a les arrels n-èsimes de la unitat, és a dir, són les arrels del polinomi $x^n - 1 \in \mathbb{Q}[x]$.

Si suposem en particular que $n = p$ és un nombre primer, s'obté:

$$x^p - 1 = (x - 1)(x^{p-1} + \cdots + 1),$$

on $x^{p-1} + \cdots + 1$ és un polinomi irreductible a $\mathbb{Q}[x]$. No és pas difícil de veure que el grup de Galois del polinomi ciclotòmic $x^{p-1} + \cdots + 1$ és un grup cíclic d'ordre $p - 1$: si $\varepsilon \neq 1$ és una arrel p-èsima de la unitat, els elements del grup de Galois són les permutacions corresponents a les aplicacions $\varepsilon \mapsto \varepsilon^i$, $i = 1, \ldots, p - 1$. Per tant, en aquest cas el grup de Galois és $G = \mathbb{Z}/(p - 1)$.

Que un punt es pugui construir fent servir només el regle i el compàs es tradueix algebraicament en el fet que les seves coordenades es puguin obtenir a partir de $\mathbb{Q}$ per una successió d'extensions quadràtiques. Per tant, en el nostre cas, el polígon serà construïble amb regle i compàs si i només si existeix una cadena de cossos

$$\mathbb{Q}[\varepsilon] = K \supset K_1 \supset \cdots \supset K_n = \mathbb{Q}$$

on cadascun d'ells té dimensió 2 sobre el següent.

Però el teorema fonamental de la teoria de Galois —aquell que no he enunciat— diu entre d'altres coses que la llei que assigna a cada subgrup H del grup de Galois G el subcòs k de K format pels elements que són fixos per totes les permutacions de H, estableix una correspondència bijectiva entre subcossos i subgrups que verifica

$$\dim_{\mathbb{Q}} k = \operatorname{ord} G / \operatorname{ord} H = \operatorname{ind} H.$$

Per tant, la traducció en termes del grup de Galois G de la constructibilitat amb regle i compàs és l'existència d'una cadena de subgrups

$$G = G_0 \supset \cdots \supset G_n = 0$$

on cadascun d'ells té índex 2 en l'anterior, la qual cosa exigeix que l'ordre de G sigui una potència de 2.

Però $G = \mathbb{Z}/(p - 1)$ té ordre $p - 1$; en conseqüència, la condició necessària i suficient per tal que el polígon regular de p costats sigui construïble és:

$$p = 1 + 2^r.$$

Ara bé, $1 + 2^r$ només pot ser primer si $r = 2^s$, i per tant la llista de polígons regulars amb un nombre primer de costats i construïbles comença així:

$$3 = 1 + 2, \quad 5 = 1 + 2^2, \quad 17 = 1 + 2^{2^2}, \quad 257 = 1 + 2^{2^3}.$$

2.2 Grups quàntics i geometria no commutativa

El darrer exemple en el qual intentaré fer palesa la rellevància de la simetria serà el dels grups quàntics, un tema ben actual en la investigació matemàtica d'avui.

Començaré fent un xic d'història. La geometria clàssica d'Euclides estudia les propietats d'uns certs subconjunts del pla i de l'espai: triangles, cercles, prismes, etc. Són crucials les nocions de semblança i congruència de figures, així com la possibilitat de mesurar les longituds i els angles. En aquestes nocions hi ha implícita la idea de grup de

transformacions o d'automorfismes de l'espai. En l'apartat I hem parlat un xic d'això en el pla, ja que dir que dues figures són congruents és el mateix que afirmar que existeix un moviment que aplica l'una en l'altra. Abans hem definit el grup O(2) imposant que els seus elements conservessin la distància; però també és possible, seguint F. Klein (*Una geometria és l'estudi dels invariants per l'acció d'un grup*), d'enfocar-ho a l'inrevés: partint del grup ortogonal i buscant els seus invariants, entre els quals hi trobem la distància.

Amb la introducció de les coordenades, Descartes va aconseguir una traducció algebraica de la geometria: els subconjunts de l'espai es poden definir mitjançant relacions entre les seves coordenades, i els automorfismes com a funcions de l'espai en ell mateix.

Matemàticament, una relació entre les coordenades s'escriu com

$$f(x, y, z) = 0,$$

on f pertany a una determinada classe de funcions. L'elecció d'aquesta classe depèn del tipus de propietats geomètriques que hom vulgui estudiar; i així s'obtenen totes les geometries: l'algebraica si les funcions són polinomis, la diferencial si les funcions són diferenciables, la topologia si les funcions són contínues, etc. Tot això és ben conegut.

En algunes situacions bàsiques, la traducció dels espais geomètrics en termes de funcions és totalment fidel. Per tal de captar el significat del que acabem de dir, anirà bé de recordar algunes nocions de geometria algebraica.

El teorema dels zeros de Hilbert assegura que sobre un cos algebraicament tancat (per exemple, $\mathbb{C}$) la llei que assigna a una varietat algebraica afí V el seu anell de funcions polinòmiques és una antiequivalència categorial entre la categoria de les varietats algebraiques afins i la categoria de les àlgebres complexes commutatives finitament generades i sense radical.

El tecnicisme *antiequivalència categorial* pretén expressar que essencialment és el mateix treballar en una categoria que en l'altra, ja que, donada una àlgebra complexa commutativa finitament generada i sense radical A, és possible recuperar o crear —com us agradi més— la varietat algebraica afí que té A com a anell de funcions polinòmiques. El prefix *anti* es refereix al fet que els morfismes canvien de sentit en passar d'una categoria a l'altra.

Fixem-nos en l'anell de polinomis $\mathbb{C}[x, y]$: els seus ideals maximals, segons el teorema dels zeros de Hilbert que hem esmentat, són de la forma $(x - \alpha, y - \beta)$ amb $(\alpha, \beta) \in \mathbb{C}^2$. Aixòindica que per a cada ideal maximal $\mathfrak{p}$ es compleix que $\mathbb{C}[x, y]/\mathfrak{p} \simeq \mathbb{C}$ i d'aquesta manera queda establerta una correspondència bijectiva entre els ideals maximals de $\mathbb{C}[x, y]$ (el conjunt dels quals serà designat per $\mathrm{Spec}_M\, \mathbb{C}[x, y] \sim \mathbb{C}^2$) i els morfismes de $\mathbb{C}$-àlgebres de $\mathbb{C}[x, y]$ en $\mathbb{C}$:

$$\begin{aligned} \mathfrak{p} = (x - \alpha, y - \beta) \longleftrightarrow \varphi\colon \mathbb{C}[x, y] &\longrightarrow \mathbb{C} \simeq \mathbb{C}[x, y]/\mathfrak{p} \\ p(x, y) &\longrightarrow p(\alpha, \beta). \end{aligned}$$

Si $p = p(x, y) \in \mathbb{C}[x, y]$, tenim definida de manera natural una aplicació:

$$\begin{aligned} \tilde{p}\colon \mathrm{Spec}_M\, \mathbb{C}[x, y] &\longrightarrow \mathbb{C} \\ \mathfrak{p} = (x - \alpha, y - \beta) &\longrightarrow p(\alpha, \beta) \end{aligned}$$

i la seva traducció

$$\begin{aligned} \tilde{p}\colon \mathrm{Hom}_{\mathbb{C}}\, -alg(\mathbb{C}[x, y], \mathbb{C}) &\longrightarrow \mathbb{C} \\ \varphi &\longrightarrow \varphi(p). \end{aligned}$$

Una altra vegada el teorema dels zeros de Hilbert ens assegura que l'aplicació

$$\begin{aligned} \mathbb{C}[x,y] &\longrightarrow \mathrm{F}(\mathrm{Spec}_M\, \mathbb{C}[x,y], \mathbb{C}) \\ p &\longrightarrow \tilde{p} \end{aligned}$$

és una representació fidel (el seu nucli és trivial) dels polinomis com a funcions sobre l'espectre.

Tot el que acabem de dir fa veure com és de natural identificar

$$\mathrm{Hom}_{\mathbb{C}} - alg\,(\mathbb{C}[x,y], \mathbb{C}) \sim \mathbb{C}^2$$

amb la varietat associada a $\mathbb{C}[x,y]$, sobre la qual $\mathbb{C}[x,y]$ es representa fidelment com a funcions.

Sobre $\mathbb{C}^2$ actua el grup lineal $\mathrm{GL}(2,\mathbb{C})$, el qual al seu torn té estructura de varietat algebraica afí i el seu anell de funcions polinòmiques és

$$A = \mathbb{C}[x_1 1, x_1 2, x_2 1, x_2 2, t]/(t(x_1 1 x_2 2 - x_1 2 x_2 1) - 1).$$

Però l'estructura de grup de $\mathrm{GL}(2,\mathbb{C})$ queda reflectida en el seu anell de polinomis A, definint així el que s'anomena tècnicament una comultiplicació i fent de A una àlgebra de Hopf. Aquesta àlgebra A és commutativa, però la seva comultiplicació no ho és pas; aquest resultat no és cap sorpresa, ja que el grup no és commutatiu i per tant tampoc ho ha de ser el seu reflex en A.

Anàlogament, el grup $\mathrm{SL}(2,\mathbb{C})$ és una varietat algebraica afí i el seu anell de funcions polinòmiques,

$$B = \mathbb{C}[x_1 1, x_1 2, x_2 1, x_2 2]/(x_1 1 x_2 2 - x_1 2 x_2 1 - 1),$$

té estructura d'àlgebra de Hopf. Tots dos grups, $\mathrm{SL}(2,\mathbb{C})$ i $\mathrm{GL}(2,\mathbb{C})$, són grups d'automorfismes o de simetries de $\mathbb{C}^2$.

La noció d'esquema de Grothendieck ens fa tornar a la geometria, ja que amb aquesta noció es demostra en particular que tot anell commutatiu defineix un espai —el seu espectre— sobre el qual l'anell es realitza com un anell de funcions, tant localment com global (el feix estructural). Hi ha alguna manera de generalitzar aquesta idea a anells no commutatius? Fins avui, cap dels intents que s'han fet no ha pogut superar l'entrebanc que suposa el fet de no disposar d'una noció escaient de localització no commutativa; peròl'estímul per atacar aquest problema no només prové de les matemàtiques, sinó també de la mecànica quàntica. +s ben conegut que a la mecànica quàntica els observables, que en termes matemàtics són operadors autoadjunts d'un espai de Hilbert complex, no sempre commuten. Dos observables commuten si i només si corresponen a magnituds que es poden mesurar simultàniament amb tanta precisió teòrica com es vulgui; però el famós principi d'indeterminació de Heisenberg afirma que si es mesuren simultàniament uns certs parells de magnituds, com per exemple la posició i la velocitat, llavors el producte dels errors comesos sempre és més gran que una certa constant que s'expressa en termes de la cèlebre constant $\hbar$ de Planck. Així doncs, l'anell d'observables de la mecànica quàntica no és commutatiu.

La idea de geometritzar uns certs anells no commutatius pot ser fructífera si al problema l'anomenem solució. M'explicaré: considerem la categoria de les àlgebres complexes associatives; si A i B són dos elements d'aquesta categoria, els homomorfismes de $\mathrm{Hom}_{\mathbb{C}} - alg(A,B)$ s'anomenen B-punts de l'espai (definit per) A. En particular, si $\varphi\colon A \to B$ és injectiu, es diu que φ és un B-punt genèric ($\varphi A \simeq A$ i per tant no es

perd informació). Observem que en aquesta situació no podem limitar-nos a prendre homomorfismes en $\mathbb{C}$, ja que $\mathbb{C}$ és commutatiu i A no ho és, per la qual cosa hi ha molt pocs $\mathbb{C}$-punts (en alguns casos només el trivial) i, per tant, el nucli de la representació de A com a funcions sobre el conjunt dels $\mathbb{C}$-punts és molt gran.

En sintonia amb el cas clàssic o commutatiu es pot dir que un objecte de la geometria complexa no commutativa o quàntica és un objecte de la categoria oposada a la categoria de les àlgebres complexes associatives; i seguint en aquesta mateixa línia podem recórrer al concepte general d'àlgebra complexa de Hopf (sense exigir que la multiplicació sigui commutativa) per tal de definir el grup de simetries o d'automorfismes de les geometries no commutatives, geometries en les quals els punts no es *veuen*.

Em posaré en el cas més senzill possible i espero que així s'entengui una mica millor el que acabem de dir. Si $0 \neq q \in \mathbb{C}$, considerem les àlgebres complexes

$$A_q^{2|0} = \frac{\mathbb{C}\langle x, y\rangle}{(xy - q^{-1}yx)}, \qquad A_q^{0|2} = \frac{\mathbb{C}\langle \xi, \eta\rangle}{(\xi^2, \eta^2, \xi\eta + q\eta\xi)},$$

on $\mathbb{C}\langle x, y\rangle$ designa l'àlgebra complexa associativa lliure amb generadors $\{x, y\}$, és a dir, l'àlgebra tensorial de $\mathbb{C}^2$.

Aquestes dues àlgebres són duals en el sentit precís següent: totes dues estan generades per la seva capa de grau 1 ($\simeq \mathbb{C}^2$) i les seves relacions estan generades per les relacions de grau 2; ara bé, si considerem (x, y) i (ξ, η) com a coordenades, respectivament en $\mathbb{C}^2$ i en el seu dual, resulta que l'espai de les relacions d'ordre dos de $A_q^{0|2}$ és exactament l'incident o ortogonal de l'espai de les relacions d'ordre dos de $A_q^{2|0}$. Observem immediatament que

$$A_1^{2|0} = \frac{\mathbb{C}\langle x, y\rangle}{(xy - yx)} = \mathbb{C}[x, y], \qquad \text{anell de polinomis,}$$

$$A_1^{0|2} = \frac{\mathbb{C}\langle x, y\rangle}{(\xi^2, \eta^2, \xi\eta + q\eta\xi)} = \Lambda\mathbb{C}^2, \qquad \text{àlgebra exterior de } \mathbb{C}^2.$$

Per tant, el pla quàntic $A_q^{2|0}$ es pot considerar com una deformació del pla ordinari; alhora, $A_q^{0|2}$ seria una deformació del *pla* de la supergeometria.

Com es pot generalitzar al cas quàntic el grup lineal $\mathrm{GL}(2, \mathbb{C})$ o grup d'automorfismes del pla complex? Recordem alguns resultats de l'àlgebra lineal elemental per a un pla vectorial complex E.

a) $\mathrm{End}_{\mathbb{C}} E \simeq E' \otimes E$, on E' és el dual de E. Després d'haver escollit una base de E, els seus endomorfismes es realitzen mitjançant les matrius $\mathrm{M}(2, \mathbb{C})$.

b) Hi ha un isomorfisme canònic

$$\begin{aligned} \mathrm{End}_{\mathbb{C}} E &\xrightarrow{\sim} \mathrm{End}_{\mathbb{C}} E' \\ f &\longrightarrow f' \end{aligned}$$

on f' és l'aplicació dual o transposada de f.

D'aquesta manera, f s'estén a un endomorfisme de la capa tensorial (covariant, contravariant o mixta) de qualsevol ordre de E. En particular, si $\Lambda^2_{\mathbb{C}} E' \simeq \mathbb{C}$ és la capa d'ordre dos de l'àlgebra exterior de E', llavors f s'estén a un endomorfisme $\widehat{f} \in \mathrm{End}_{\mathbb{C}} \Lambda^2_{\mathbb{C}} E'$, que és per tant de la forma $\widehat{f} = \lambda\,\mathrm{Id}$, on l'escalar λ és per definició el determinant de$f$. Si la

matriu associada a f en una base e_1, e_2 és $\left(\begin{smallmatrix} b_1 1 & b_2 1 \\ b_1 2 & b_2 2 \end{smallmatrix}\right)$ i ω_1, ω_2 és la base dual de e_1, e_2, es verifica

$$\begin{aligned}\widehat{f}(\omega_1 \wedge \omega_2) &= (b_1 1\omega_1 + b_1 2\omega_2) \wedge (b_2 1\omega_1 + b_2 2\omega_2) \\ &= (b_1 1 b_2 2 - b_1 2 b_2 1)\omega_1 \wedge \omega_2 = (\det f)\omega_1 \wedge \omega_2.\end{aligned}$$

Anem a generalitzar tot això al cas quàntic. Sigui B una àlgebra complexa. Un B-punt de $A_q^{2|0}$ queda determinat pels valors que pren sobre els generadors x, y; per tant, és correcte de dir que $(a, b) \in B^2$ és un B-punt de $A_q^{2|0}$ si i només si $ab - q^{-1}ba = 0$. De manera anàloga, direm que $(\alpha, \beta) \in B^2$ és un B-punt de $A_q^{0|2}$ si $\alpha^2 = \beta^2 = 0$, $\alpha\beta + q\beta\alpha = 0$. Ara considerem $b_1 1, b_2 1, b_1 2, b_2 2 \in B$ que commutin amb $a, b, \alpha, \beta \in B$, on (a, b) és un B-punt genèric de $A_q^{2|0}$ i (α, β) és un B-punt genèric de $A_q^{0|2}$; i escrivim

$$\begin{aligned}\begin{pmatrix} b_1 1 & b_2 1 \\ b_1 2 & b_2 2 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} b_1 1 a + b_2 1 b \\ b_1 2 a + b_2 2 b \end{pmatrix} = \begin{pmatrix} a' \\ b' \end{pmatrix} \\ \begin{pmatrix} b_1 1 & b_2 1 \\ b_1 2 & b_2 2 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} &= \begin{pmatrix} b_1 1 \alpha + b_2 1 \beta \\ b_1 2 \alpha + b_2 2 \beta \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}.\end{aligned}$$

Si exigim (quelcom natural, ja que les matrius actuen tant sobre un espai com sobre el seu dual, i les àlgebres $A_q^{2|0}$ i $A_q^{0|2}$ són duals l'una de l'altra) que (a', b') sigui un B-punt de $A_q^{2|0}$ i que (α', β') sigui un B-punt de $A_q^{0|2}$, s'obtenen les relacions següents:

$$\begin{gathered} b_1 1 b_2 1 = q^{-1} b_2 1 b_1 1, \quad b_1 1 b_1 2 = q^{-1} b_1 2 b_1 1, \\ b_1 2 b_2 2 = q^{-1} b_2 2 b_1 2, \quad b_2 1 b_2 2 = q^{-1} b_2 2 b_2 1, \\ b_1 2 b_2 1 = b_2 1 b_1 2, \quad b_1 1 b_2 2 - b_2 2 b_1 1 = (q^{-1} - q) b_1 2 b_2 1. \end{gathered}$$

A més, es verifica:

$$\begin{aligned}\alpha'\beta' &= (b_1 1\alpha + b_2 1\beta)(b_1 2\alpha + b_2 2\beta) \\ &= b_1 1 b_2 2 \alpha\beta + b_2 1 b_1 2 \beta\alpha \\ &= \left(b_1 1 b_2 2 - q^{-1} b_2 1 b_1 2\right)\alpha\beta.\end{aligned}$$

En vista d'això, és natural de definir l'anell $\mathrm{M}_q(2, \mathbb{C})$ de coordenades de les matrius complexes quàntiques 2×2 de la manera següent:

$$\mathrm{M}_q(2, \mathbb{C}) = \mathbb{C}\langle x_1 1, x_1 2, x_2 1, x_2 2\rangle / I,$$

on I és l'ideal generat pels elements

$$\begin{gathered} x_1 1 x_2 1 - q^{-1} x_2 1 x_1 1, \quad x_1 1 x_1 2 - q^{-1} x_1 2 x_1 1, \\ x_1 2 x_2 2 - q^{-1} x_2 2 x_1 2, \quad x_2 1 x_2 2 - q^{-1} x_2 2 x_2 1, \\ x_1 2 x_2 1 - x_2 1 x_1 2, \quad x_1 1 x_2 2 - x_2 2 x_1 1 - (q^{-1} - q) x_1 2 x_2 1. \end{gathered}$$

Seguint en la mateixa línia, també resulta natural la definició següent de la funció determinant:

$$\det{}_q(x_1 1, x_1 2, x_2 1, x_2 2) = x_1 1 x_2 2 - q^{-1} x_2 1 x_1 2,$$

que ens permet d'anomenar l'anell

$$\mathrm{SL}_q(2,\mathbb{C}) = \frac{\mathbb{C}\langle x_1 1, x_1 2, x_2 1, x_2 2\rangle}{(x_1 1 x_2 2 - q^{-1} x_2 1 x_1 2 - 1, I)}$$

l'anell de coordenades del grup complex quàntic especial lineal 2.

De manera anàloga es defineix l'anell de coordenades del grup complex quàntic lineal 2, però la seva definició és més feixuga, ja que inclou l'exigència que uns certs elements commutin entre ells.

Les definicions anteriors no només són naturals sinó que funcionen raonablement bé; en particular, i seguint la idea del cas clàssic en què el producte de matrius és el reflex de la composició de les seves accions sobre el pla ordinari, l'acció dels B-punts de $\mathrm{M}_q(2,\mathbb{C})$ sobre els B-punts del pla quàntic $A_q^{2|0}$ permet definir sobre aquells una composició (definida només per a parells que commutin entre ells) que es reflecteix a $\mathrm{M}_q(2,\mathbb{C})$ com una comultiplicació. I aquesta comultiplicació dota $\mathrm{SL}_q(2,\mathbb{C})$ d'estructura d'àlgebra de Hopf.

Tot el que hem dit sobre els grups quàntics no passa de ser una indicació: no hem fet més que assenyalar-los; als que vulguin conèixer-los els recomano la lectura de Manin *Quantum Groups and Non-Commutative Geometry.*

Arribats a aquest punt, abusaré un xic més de la indulgència del lector amb unes paraules sobre la bellesa com a criteri de la veritat.

Investigar, també en matemàtiques, és enfrontar-se a un problema del qual no es coneix la solució. El primer que cal fer és intuir o conjecturar el resultat, i només aleshores intentar demostrar que el que s'ha conjecturat és cert. Però quins criteris poden guiar aquest procés d'intuir o conjecturar? No crec que existeixi cap resposta completa, però m'adhereixo a la fe de Poincaré i de molts altres matemàtics i físics il·lustres en la bellesa com a criteri-guia: només estarem en el bon camí si escollim la situació més bonica possible, i si malgrat tot aquest camí acaba resultant fals, llavors caldrà imaginar una solució encara més bella.

Però hi ha un parell de preguntes que cal fer: en quin sentit són bells un resultat, una construcció o una teoria matemàtica? I com es pot fer accessible al no iniciat la bellesa de la ciència a la qual ens dediquem? Els matemàtics ens hem de mantenir en l'horitzó obert per aquestes preguntes, tot assajant esbossos d'una resposta. Potser podem trobar inspiració i força per a aquesta tasca en el vell mite platònic: Eros, atret per la Bellesa i desitjós que aquesta es plasmi en el món, és la força que impulsa no només l'enllaç dels cossos sinó també el caminar de les ments a la recerca del coneixement i de la sensibilitat en la seva tensió cap al que és bell.

Referències

[1] Howard Hiller: *Crystallography and Cohomology of Groups*, Amer. Math. Monthly, **93**. (1986), 765–779.

[2] Yuri I. Manin: *Quantum Groups and Non-Commutative Geometry*, Universitat de Mont-real CRM, 1988.

[3] Yuri I. Manin: *Mathematics and Physics*, Boston, Birkhõuser, 1981.

[4] Hermann Weyl: *Symmetry*, Princeton University Press, 1952. (Hi ha una traducció castellana per McGraw-Hill/Interamericana de España, 1991)

Apèndix I. Subgrups de $\mathrm{SO}(2)$

El primer que farem serà establir el següent resultat trivial sobre subgrups d'un grup topològic.

6 Proposició *Sigui G un grup topològic compacte i H un subgrup infinit. L'element neutre e és un punt d'acumulació de H.*

Prova: Si per a tot $g \in G$ existeix un entorn obert $U(g)$ que no conté infinits punts de H, llavors de $G = \bigcup_g \in GU(g)$ es dedueix, com que G és compacte, que existeix una subfamília finita d'entorns tal que

$$G = \bigcup_i = 1^n U(g_i) \quad \Longrightarrow \quad H = \bigcup_i = 1^n \left(H \cap U(g_i)\right),$$

la qual cosa implicaria que H és finit. Aquesta contradicció ens assegura que existeix un punt $g \in G$ que és d'acumulació de H.

La topologia de G ve determinada pels entorns de l'element neutre; en particular, per a tot entorn obert $U(e)$ i qualsevol $g \in G$ existeix un entorn obert $V(g)$ tal que $V(g)V(g)^{-1} \subset U(e)$. Això ens assegura que e és un punt d'acumulació de H. □

Podem passar a demostrar que:

7 Teorema *Tot subgrup infinit de* $\mathrm{SO}(2)$ *és dens.*

Prova: +s evident que les aplicacions següents són isomorfismes de grups:

$$\begin{aligned} \phi\colon \mathrm{SO}(2) &\longrightarrow \mathrm{S}^1 & \qquad \psi\colon \mathrm{S}^1 &\longrightarrow \mathbb{R}/\mathbb{Z} \\ g_\alpha &\longrightarrow e^{\alpha i} & e^{2\pi\alpha i} &\longrightarrow \{\alpha\} \end{aligned}$$

A més, ψ és un homeomorfisme del grup S^1 amb la topologia induïda per la del pla, en el grup $\mathbb{R}/\mathbb{Z}$ amb la topologia quocient de la recta.

Ara demostrarem el teorema per al grup $\mathbb{R}/\mathbb{Z}$, els elements del qual es poden etiquetar unívocament amb els elements de l'interval $[0, 1)$, ja que aquests dos conjunts estan en correspondència bijectiva.

Una base d'entorns de l'element neutre d'aquest grup està formada pels conjunts

$$V(0, \varepsilon) = \{x \in [0, 1) \mid 0 \leq x < \varepsilon\} \cup \{x \in [0, 1) \mid -\varepsilon < 1 - x \leq 0\}, \quad \varepsilon \in \mathbb{R}.$$

La proposició anterior ens assegura que si H és un subgrup infinit de $\mathbb{R}/\mathbb{Z}$, llavors el conjunt $H \cap V(0, \varepsilon)$ és infinit per a cada ε, la qual cosa implica que existeixen infinits elements $h \in H$ tals que $0 < h < \varepsilon$.

Per tant, per demostrar que H és dens, n'hi ha prou amb veure que per a tot $\alpha \in (0, 1)$ i tot $0 < h \in H$ existeix algun enter n tal que $0 < nh - \alpha \leq h$. Però $n = 1 + [\alpha h^{-1}]$ verifica aquesta condició; així doncs, hem acabat la demostració. □

Apèndix II. Subgrups finits de $\mathrm{GL}(2, \mathbb{Z})$

Alguns resultats sobre formes quadràtiques enteres En aquest apèndix designarem per (a, b, a_1) la forma quadràtica amb coeficients enters $ax^2 + 2bxy + a_1y^2$ i direm que $b^2 - aa_1$

és el seu discriminant. Amb la nomenclatura ææformes equivalents" volem indicar que existeix $A \in \mathrm{GL}(2,\mathbb{Z})$ que passa de l'una a l'altra; és a dir, (a,b,a_1) i (a_1,b_1,a_2) satisfan la relació

$$A\begin{pmatrix} a & b \\ b & a_1 \end{pmatrix} A^t = \begin{pmatrix} a_1 & b_1 \\ b_1 & a_2 \end{pmatrix}.$$

I és clar que dues formes equivalents tenen el mateix discriminant, ja que $\det A = \pm 1$.

8 Teorema de reducció *Si (a,b,a_1) és una forma quadràtica amb coeficients enters de discriminant negatiu i tal que $a > 0$, existeix una forma equivalent $(a_n, b_n, a_n + 1)$ tal que $2|b_n| \le a_n \le a_n + 1$.*

Prova: Sigui $D = -(b^2 - aa_1)$, que per hipòtesi és positiu, la qual cosa implica que $a_1 > 0$. Si la forma donada no verifica la condició enunciada, s'agafa un enter b_1 tal que

$$b_1 \equiv b \pmod{a_1}, \quad -a_1 \le 2b_1 \le a_1.$$

La matriu $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & \frac{b+b_1}{a_1} \end{smallmatrix}\right)$ pertany a $\mathrm{GL}(2,\mathbb{Z})$ i es verifica

$$A\begin{pmatrix} a & b \\ b & a_1 \end{pmatrix} A^t = \begin{pmatrix} a_1 & b_1 \\ b_1 & \frac{D+b_1^2}{a_1} \end{pmatrix},$$

la qual cosa demostra que les formes (a,b,a_1) i (a_1,b_1,a_2), on $a_2 = (D + b_1^2)/a_1$, són equivalents. Per construcció, la forma (a_1,b_1,a_2) compleix $2|b_1| \le a_1$ i, per tant, si $a_1 \le a_2$ ja hem acabat.

Si $a_1 > a_2$, es torna a repetir el procés i s'obté una forma equivalent (a_2,b_2,a_3) tal que $2|b_2| \le a_2$. D'aquesta manera, en un nombre finit de passos $(a_1 > a_2 > a_3 > \cdots)$ s'arriba a obtenir una forma equivalent que compleix les condicions de l'enunciat.

+s de vital importància observar que, per a una tal forma,

$$a_n^2 \le a_n a_n + 1 = D + b_n^2 \le D + \frac{a_n^2}{4} \quad \Longrightarrow \quad a_n \le 2\sqrt{\frac{D}{3}}. \quad \square$$

El teorema anterior (que va ser enunciat i demostrat per Gauss) és una font d'on raja moltíssima informació sobre quins nombres enters són representables, és a dir, són valors assolits per una forma donada. En els corol·laris següents es recull la informació per als casos concrets que necessitarem més endavant.

9 Corol·lari *a) Si (a,b,a_1) és una forma quadràtica amb $D = 1$ i tal que $a > 0$, llavors és equivalent a la forma $(1,0,1)$ i per tant representa 1.*

b) Si (a,b,a_1) és una forma quadràtica amb $D = 1$ i tal que $a < 0$, llavors és equivalent a la forma $(-1,0,-1)$ i per tant representa -1.

Prova:

a) Es pot suposar, pel teorema anterior, que llevat d'equivalència de formes es compleix

$$\left.\begin{array}{c} 2|b| \le a \le 2\sqrt{\frac{1}{3}} \\ a \le a_1 \\ 1 = aa_1 - b^2 \end{array}\right\} \quad \Longrightarrow \quad (a,b,a_1) = (1,0,1).$$

b) +s immediat, ja que per a) la forma $(-a,-b,-a_1)$ és equivalent a la forma $(1,0,1)$. □

10 Corol·lari *a) Si (a,b,a_1) és una forma quadràtica amb $D=3$, $a>0$ i $\{a,a_1\}\subset 2\mathbb{Z}$, llavors és equivalent a la forma $(2,1,2)$ i per tant representa 2.*

b) Si (a,b,a_1) és una forma quadràtica amb $D=3$, $a<0$ i $\{a,a_1\}\subset 2\mathbb{Z}$, llavors és equivalent a la forma $(-2,-1,-2)$ i per tant representa -2.

Prova:

a) Es pot suposar, pel teorema anterior, que llevat d'equivalència de formes es compleix

$$\left.\begin{array}{c} 2|b|\le a\le 2 \\ a\le a_1 \\ 1=aa_1-b^2 \\ a,a_1 \text{ són parells}\end{array}\right\} \implies (a,b,a_1)=(2,1,2).$$

b) Es raona igual que en l'apartat b) del corol·lari anterior. □

11 Teorema *Una forma quadràtica de discriminant 1 és equivalent a la forma $(0,1,0)$ si $\{a_12,a_21\}\subset 2\mathbb{Z}$, o bé a la forma $(1,0,1)$ si a_12,a_21 no satisfan aquesta condició.*

Prova: Si $Q=(a,b,c)$ és una forma d'aquestes, definim la forma biadditiva simètrica

$$\begin{aligned}\Phi\colon \mathbb{Z}^2 &\longrightarrow \mathbb{Z}\\ (u,v) &\longrightarrow \frac{1}{2}\left(Q(u+v)-Q(u)-Q(v)\right).\end{aligned}$$

Es pot recuperar la forma quadràtica Q a partir de la forma Φ, ja que $Q(u)=\Phi(u,u)$.

a) La forma Φ estableix un criteri per a decidir quan dos elements $u=(u_1,u_2), v=(v_1,v_2)$ generen $\mathbb{Z}^2$:

$$u,v \text{ generen } \mathbb{Z}^2 \iff \begin{vmatrix}\Phi(u,u) & \Phi(u,v)\\ \Phi(u,v) & \Phi(v,v)\end{vmatrix}=1.$$

En efecte, la matriu associada a Φ en el sistema de generadors $e_1=(1,0)$, $e_2=(0,1)$ és

$$\begin{pmatrix}\Phi(e_1,e_1) & \Phi(e_1,e_2)\\ \Phi(e_1,e_2) & \Phi(e_2,e_2)\end{pmatrix}=\begin{pmatrix}a & b\\ b & c\end{pmatrix}$$

i és immediat de comprovar que

$$\begin{pmatrix}\Phi(u,u) & \Phi(u,v)\\ \Phi(u,v) & \Phi(v,v)\end{pmatrix}=\begin{pmatrix}u_1 & v_1\\ u_2 & v_2\end{pmatrix}^t\begin{pmatrix}a & b\\ b & c\end{pmatrix}\begin{pmatrix}u_1 & v_1\\ u_2 & v_2\end{pmatrix},$$

d'on, prenent determinants i tenint en compte que $ac-b^2=1$, es dedueix que

$$\begin{vmatrix}\Phi(u,u) & \Phi(u,v)\\ \Phi(u,v) & \Phi(v,v)\end{vmatrix}=\begin{vmatrix}u_1 & v_1\\ u_2 & v_2\end{vmatrix}^2,$$

la qual cosa ens assegura que la matriu $A = \left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$ pertany a $\mathrm{GL}(2,\mathbb{Z})$, és a dir, $\det A = \pm 1$, si i només si

$$\begin{vmatrix} \Phi(u,u) & \Phi(u,v) \\ \Phi(u,v) & \Phi(v,v) \end{vmatrix} = 1.$$

b) Existeixen elements $0 \neq e, v \in \mathbb{Z}^2$ tals que $\Phi(e,e) = 0$ i $\Phi(e,v) = 1$.

En efecte, si $a = 0$, l'element $e = e_1$ verifica $\Phi(e,e) = 0$.

Si $a \neq 0$, l'equació $ax^2 + 2bx + c = 0$ té les solucions $x = (-b \pm 1)/a$, la qual cosa ens diu que la forma Q s'anul·la sobre els elements $(1-b, a)$ i $(-1-b, a)$; almenys un d'ells té les seves dues coordenades no nul·les i, per tant, dividint pel seu màxim comú divisor s'obté un element $0 \neq e$ tal que e no pertany a cap $n\mathbb{Z}^2$ amb $n \geq 2$.

Un element d'un $\mathbb{Z}$-mòdul que verifiqui aquesta darrera condició s'anomena indivisible. Per tant, en tots dos casos existeix un element e indivisible tal que $\Phi(e,e) = 0$.

Que el discriminant sigui 1 implica, tal com es demostra fàcilment, que l'aplicació

$$\begin{aligned} \mathbb{Z}^2 &\longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^2, \mathbb{Z}) \\ u &\longrightarrow \Phi(u,-)\colon v \mapsto \Phi(u,v) \end{aligned}$$

és un isomorfisme de $\mathbb{Z}$-mòduls. En particular, això ens assegura que si e és indivisible també ho és $\Phi(e,-)$.

Però dir que $\Phi(e,-)$ és indivisible és afirmar que $\mathrm{Im}\,\Phi(e,-) = \mathbb{Z}$, ja que si $\mathrm{Im}\,\Phi(e,-) = n\mathbb{Z}$, $n \geq 2$, seria divisible per n. Els raonaments anteriors demostren b).

Ja estem en condicions de demostrar el teorema, partint d'un parell d'elements e, v que satisfacin la condició b).

Si $\{a_1 2, a_2 1\} \subset 2\mathbb{Z}$, la forma quadràtica només pren valors parells; si $Q(v) = 2r$, sigui $u = v - re$. Amb un simple càlcul es veu que

$$\begin{pmatrix} \Phi(e,e) & \Phi(e,v) \\ \Phi(e,v) & \Phi(v,v) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

i per tant aplicant a) es pot assegurar que e, v generen $\mathbb{Z}^2$. A més, és evident que Q expressada en aquest sistema de generadors és la forma $(0,1,0)$, i per tant aquestes dues formes són equivalents.

Si $\{a_1 2, a_2 1\}$ no és contingut a $2\mathbb{Z}$, la forma quadràtica pren algun valor senar. Això permet suposar que el parell e, v verifica a més $\Phi(v,v) = 2r+1$, ja que si v no ho complís, n'hi hauria prou amb triar $w, \overline{v}$ tals que

$$\Phi(w,w) = \text{senar}, \quad \overline{v} = w - + (1 - \Phi(e,w))\, v$$

per obtenir un parell $e, \overline{v}$ que verifiqués

$$\Phi(e,e) = 0, \quad \Phi(e,\overline{v}) = 1, \quad \Phi(\overline{v},\overline{v}) = 2r+1.$$

Ara bé, si prenem $u_1 = \overline{v} - re$ i $u_2 = \overline{v} - (r+1)e$, un simple càlcul mostra que

$$\begin{pmatrix} \Phi(u_1,u_1) & \Phi(u_1,u_2) \\ \Phi(u_1,u_2) & \Phi(u_2,u_2) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

i per tant aplicant a) es pot assegurar que u_1, u_2 generen $\mathbb{Z}^2$. La forma Q expressada en aquest sistema de generadors es converteix en la forma $(1,0,-1)$, la qual cosa ens assegura que aquestes dues formes són equivalents. □

Classes de conjugació d'elements i grups d'ordre finit a $\mathrm{GL}(2,\mathbb{Z})$ Notacions: Per a $n = 3, 4, 6$, escrivim el polinomi ciclotòmic corresponent en la forma $P_n(t) = t^2 - \tau_n t + 1$ i, tal com hem fet en el text de l'exposició, enfoquem la nostra atenció sobre els següents elements de $\mathrm{GL}(2,\mathbb{Q})$:

$$g_3 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad \text{amb polinomi característic } t^2 + t + 1 \text{ i ordre 3;}$$

$$g_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{amb polinomi característic } t^2 + 1 \text{ i ordre 4;}$$

$$g_6 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \qquad \text{amb polinomi característic } t^2 - t + 1 \text{ i ordre 6.}$$

Amb aquesta notació, $\tau_3 = -1$, $\tau_4 = 0$ i $\tau_6 = 1$.

També escriurem

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{amb polinomi característic } t^2 - 1 \text{ i ordre 2;}$$

$$\sigma' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{amb polinomi característic } t^2 - 1 \text{ i ordre 2;}$$

fins i tot, per raons d'uniformitat en la notació, designarem $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ i $g_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

+s evident que tots aquests elements pertanyen a $\mathrm{GL}(2,\mathbb{Z})$; a continuació demostrarem que són una família d'etiquetes per a les classes de conjugació d'elements d'ordre finit d'aquest grup.

12 Proposició *Per a cada $n = 3, 4, 6$, si $\overline{g}_n = \left(\begin{smallmatrix} a_1 1 & a_2 1 \\ a_1 2 & a_2 2 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ és un element de polinomi característic $P_n(t)$, llavors $\overline{g}_n$ és conjugat de g_n a $\mathrm{GL}(2,\mathbb{Z})$.*

Prova: Les condicions sobre $\overline{g}_n$ són equivalents a escriure:

$$\overline{g}_n = \begin{pmatrix} a_1 1 & a_2 1 \\ a_1 2 & \tau_n - a_1 1 \end{pmatrix}, \qquad a_1 1(\tau_n - a_1 1) - a_1 2 a_2 1 = 1.$$

I demostrar que $\overline{g}_n$ és conjugat de g_n és equivalent a veure que existeix $(x, y) \in \mathbb{Z}^2$ tal que (x, y) i $\overline{g}_n(x, y)$ són una base de $\mathbb{Z}^2$; això, al seu torn, equival al fet que l'equació

$$\begin{vmatrix} x & a_1 1 x + a_2 1 y \\ y & a_1 2 x + (\tau_n - a_1 1) y \end{vmatrix} = a_1 2 x^2 + (\tau_n - 2a_1 1)xy - a_2 1 y^2 = \pm 1 \tag{4}$$

tingui solucions enteres.

Per a $n = 4$, $\tau_4 = 0$, l'equació (4) es redueix a

$$a_1 2 x^2 - 2a_1 1 xy - a_2 1 y^2 = \pm 1, \quad D = -(a_1 1^2 + a_1 2 a_2 1) = 1$$

i en aquestes condicions el corol·lari 9 ens assegura que existeix una solució.

Per a $n = 3$, $\tau_3 = -1$, l'equació (4) es redueix a

$$a_1 2 x^2 - (1 + 2a_1 1)xy - a_2 1 y^2 = \pm 1, \quad a_1 1^2 + a_1 2 a_2 1 + a_1 1 = -1$$

o equivalentment:

$$2a_1 2 x^2 - 2(1 + 2a_1 1)xy - 2a_2 1 y^2 = \pm 2, \quad D = -4a_1 2 a_2 1 - (1 + 2a_1 1)^2 = 3,$$

d'on el corol·lari 10 ens assegura que existeix una solució.

Per a $n = 6$ es fa el mateix que per a $n = 3$. □

13 Proposició *Si* $\overline{\sigma} = \left(\begin{smallmatrix} a_11 & a_21 \\ a_12 & a_22 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ *és un element de polinomi característic* $t^2 - 1$*, llavors* $\overline{\sigma}$ *és conjugat a* $\mathrm{GL}(2,\mathbb{Z})$ *de* σ *o bé de* σ'*.*

Prova: Les condicions sobre $\overline{\sigma}$ són equivalents a escriure

$$\overline{\sigma} = \begin{pmatrix} a_11 & a_21 \\ a_12 & -a_11 \end{pmatrix}, \qquad a_11^2 + a_12a_21 = 1.$$

I demostrar que $\overline{\sigma}$ és conjugat de σ' és equivalent a veure que existeix $(x, y) \in \mathbb{Z}^2$ tal que (x, y) i $\overline{\sigma}(x, y)$ són una base de $\mathbb{Z}^2$; això, al seu torn, equival al fet que l'equació

$$\begin{vmatrix} x & a_11x + a_21y \\ y & a_12x - a_11y \end{vmatrix} = a_12x^2 - 2a_11xy - a_21y^2 = \pm 1 \tag{5}$$

tingui solucions enteres.

L'equació (5) correspon a una forma quadràtica amb discriminant 1; el teorema 11 ens assegura que una tal forma és equivalent a la forma $(0, 1, 0)$ si $\{a_12, a_21\} \subset 2\mathbb{Z}$, o bé a la forma $(1, 0, 1)$ si a_12, a_21 no satisfan aquesta condició. Per tant, $\overline{\sigma}$ és conjugat de σ' (l'equació (5) té solució entera) si i només si $a_12, a_21 \not\subset 2\mathbb{Z}$.

La proposició quedarà demostrada si veiem que $\overline{\sigma}$ és conjugat a $\mathrm{GL}(2,\mathbb{Z})$ de σ si i només si $\{a_12, a_21\} \subset 2\mathbb{Z}$.

En efecte, si les formes $(a_12, -a_11, -a_21)$ i $(0, 1, 0)$ són equivalents, existeix $e = (\alpha, \beta) \in \mathbb{Z}^2$ que és solució de l'equació (5). Com que a_12, a_21 són parells i a_11 no ho és $(a_11^2 + a_12a_21 = 1)$, els vectors

$$\begin{aligned} u_1 &= \frac{1}{2}(e + \overline{\sigma}e) = \frac{1}{2}\Big((a_11 + 1)\alpha + a_21\beta, a_12\alpha + (1 - a_11)\beta\Big) \\ u_2 &= \frac{1}{2}(e - \overline{\sigma}e) = \frac{1}{2}\Big((1 - a_11)\alpha - a_21\beta, -a_12\alpha + (1 + a_11)\beta\Big) \end{aligned}$$

pertanyen a $\mathbb{Z}^2$ i, evidentement, per construcció, $\overline{\sigma}u_1 = u_1$ i $\overline{\sigma}u_2 = u_2$. A més, u_1, u_2 formen una base, ja que

$$\det(u_1, u_2) = \frac{-2}{4}\det(e, \overline{\sigma}e) = -\frac{1}{2}\begin{vmatrix} \alpha & a_11\alpha + a_21\beta \\ \beta & a_12\alpha - a_11\beta \end{vmatrix} = -1.$$

Això demostra que $\overline{\sigma}$ és conjugat de σ.

La comprovació del æænomés si" encara és més senzilla: dir que $\overline{\sigma}$ és conjugat de σ és afirmar que existeix $A = \left(\begin{smallmatrix} \alpha_11 & \alpha_21 \\ \alpha_12 & \alpha_22 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$ tal que

$$\overline{\sigma} = A\sigma A^{-1} = \pm\begin{pmatrix} \alpha_11\alpha_22 + \alpha_12\alpha_21 & -2\alpha_11\alpha_21 \\ -2\alpha_12\alpha_22 & -(\alpha_11\alpha_22 + \alpha_12\alpha_21) \end{pmatrix},$$

la qual cosa ens assegura que $\overline{\sigma}$ verifica la condició de paritat. □

14 Teorema *Les classes de conjugació d'elements d'ordre finit de* $\mathrm{GL}(2,\mathbb{Z})$ *venen descrites pels elements*

$$g_1,\ g_2,\ g_3,\ g_4,\ g_6,\ \sigma,\ \sigma'.$$

PROVA: $\mathrm{GL}(2,\mathbb{Z})$ és un subgrup de $\mathrm{GL}(2,\mathbb{Q})$ i per tant el teorema de restricció cristallogràfica ens assegura que les proposicions 12 i 13 recullen totes les possibilitats per als elements d'ordre finit diferents de $\pm\mathrm{Id}$ de $\mathrm{GL}(2,\mathbb{Z})$. Per tant, aquestes proposicions mostren la validesa del teorema. □

15 TEOREMA *Les classes de conjugació de subgrups d'ordre finit de* $\mathrm{GL}(2,\mathbb{Z})$ *estan descrites per la llista següent de grups, on no hi ha cap parell de grups que siguin conjugats:*

$$\begin{array}{lll} C_1=\langle g_1\rangle, & D_1'=\langle \sigma', g_1\rangle, & D_1''=\langle \sigma, g_1\rangle,\\ C_2=\langle g_2\rangle, & D_2'=\langle \sigma', g_2\rangle, & D_2''=\langle \sigma, g_2\rangle,\\ C_3=\langle g_3\rangle, & D_3'=\langle \sigma', g_3\rangle, & D_3''=\langle -\sigma', g_3\rangle,\\ C_4=\langle g_4\rangle, & D_4=\langle \sigma', g_4\rangle, & \\ C_6=\langle g_6\rangle, & D_6=\langle \sigma', g_6\rangle. & \end{array}$$

PROVA: Si H és un subgrup finit de $\mathrm{GL}(2,\mathbb{Z})$, també serà un subgrup finit de $\mathrm{GL}(2,\mathbb{Q})$; per tant, pel teorema de classificació per conjugació de subgrups finits d'aquest darrer grup, existeix $A\in\mathrm{GL}(2,\mathbb{Q})$ tal que

$$AHA^{-1}=C_n=\langle g_n\rangle \quad \text{o bé} \quad AHA^{-1}=D_n=\langle \sigma', g_n\rangle,$$

$n=1,2,3,4,6$.

Si $AHA^{-1}=C_n$, llavors H està generat per un element $\overline{g}_n$ de polinomi característic $P_n(t)=t^2-\tau_n t+1$, la qual cosa ens assegura (vegeu 12) que $\overline{g}_n$ és conjugat a $\mathrm{GL}(2,\mathbb{Z})$ de g_n. Això demostra que H i $\langle g_n\rangle$ són subgrups conjugats a $\mathrm{GL}(2,\mathbb{Z})$.

Si $AHA^{-1}=D_1$, llavors H està generat per un element de polinomi característic t^2-1; però aquí, per 13, existeixen exactament dos elements no conjugats σ i σ' que satisfan aquestes condicions. Així doncs, H és conjugat a $\mathrm{GL}(2,\mathbb{Z})$ de $D_1'=\langle\sigma', g_1\rangle$ o bé de $D_1''=\langle\sigma, g_1\rangle$. Si $AHA^{-1}=D_2$, el mateix raonament mostra que H és conjugat a $\mathrm{GL}(2,\mathbb{Z})$ de $D_2'=\langle\sigma', g_2\rangle$ o bé de $D_2''=\langle\sigma, g_2\rangle$.

Per als casos restants, on H és conjugat a $\mathrm{GL}(2,\mathbb{Q})$ de D_n, $n=3,4,6$, cal una argumentació més fina: $AHA^{-1}=D_n$ amb $A\in\mathrm{GL}(2,\mathbb{Q})$ implica que existeixen dos elements de $\mathrm{GL}(2,\mathbb{Z})$, $\overline{\sigma}$ de polinomi característic t^2-1 i $\overline{g}_n$ de polinomi característic $P_n(t)=t^2-\tau_n t+1$, tals que

$$H=\langle \overline{\sigma}, \overline{g}_n \mid \overline{\sigma}^2=\overline{g}_n^n=1, \overline{\sigma}\,\overline{g}_n=\overline{g}_n^{n-1}\overline{\sigma}\rangle.$$

Per tant, podem suposar que, llevat de conjugació a $\mathrm{GL}(2,\mathbb{Z})$, H conté g_n. Com que $\overline{\sigma}\in H$ té polinomi característic t^2-1, és correcte d'escriure

$$\overline{\sigma}=\begin{pmatrix} a_1 1 & a_2 1\\ a_1 2 & -a_1 1\end{pmatrix}, \qquad a_1 1^2+a_1 2 a_2 1=1.$$

Però l'element $\overline{\sigma}g_n$ té determinant -1 i ordre finit, pel fet de pertànyer a H, la qual cosa implica que el seu polinomi característic és t^2-1; per tant

$$\overline{\sigma}g_n=\begin{pmatrix} a_1 1 & a_2 1\\ a_1 2 & -a_1 1\end{pmatrix}\begin{pmatrix} 0 & -1\\ 1 & \tau_n\end{pmatrix}=\begin{pmatrix} a_2 1 & -a_1 1+\tau_n a_2 1\\ -a_1 1 & -a_1 2-\tau_n a_1 1\end{pmatrix}$$

implica que $a_2 1 = a_1 2 + \tau_n a_1 14$. D'aquesta manera, podem assegurar que

$$\overline{\sigma} = \begin{pmatrix} a_1 1 & a_1 2 + \tau_n a_1 1 \\ a_1 2 & -a_1 1 \end{pmatrix},$$

on es verifica que $a_1 1^2 + a_1 2^2 + \tau_n a_1 1 a_1 2 = 1$.

Per això, tindrem una mesura de les possibilitats per a $\overline{\sigma}$ si trobem les solucions enteres de l'equació

$$x^2 + \tau_n xy + y^2 = 1. \tag{6}$$

Si $n = 4$, l'equació (6) es converteix en $x^2 + y^2 = 1$, que no té cap més solució entera que $(\pm 1, 0)$ i $(0, \pm 1)$. D'aquesta manera, $\overline{\sigma}$ és

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{o bé} \quad \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

En qualsevol cas ($g_4^2 = g_2$), existeix $r = 0, 1, 2, 3$ tal que $\overline{\sigma} g_4^r = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, la qual cosa demostra que H és conjugat a $\mathrm{GL}(2, \mathbb{Z})$ de $D_4 = \langle \sigma', g_4 \rangle$.

Si $n = 6$, l'equació (6) es converteix en $x^2 + xy + y^2 = 1$; les seves solucions són de la forma (u, t) on $t^2 + 3u^2 = 4$, és a dir, són $\pm(1, 0)$, $\pm(0, 1)$ i $\pm(1, -1)$. Per tant, les possibilitats per a $\overline{\sigma}$ són:

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{o bé} \quad \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{o bé} \quad \pm \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}.$$

En cap cas no hi ha dificultat en veure que existeix $r = 0, 1, \ldots, 5$ tal que $\overline{\sigma} g_6^r = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, la qual cosa demostra que H és conjugat a $\mathrm{GL}(2, \mathbb{Z})$ de $D_6 = \langle \sigma', g_6 \rangle$.

Si $n = 3$, l'equació (6) es converteix en $x^2 - xy + y^2 = 1$, les solucions de la qual són $\pm(1, 0)$, $\pm(0, 1)$ i $\pm(1, 1)$. Per tant, les possibilitats per a $\overline{\sigma}$ són:

$$\pm \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad \text{o bé} \quad \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{o bé} \quad \pm \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.$$

En aquest moment es fan paleses les diferències amb els casos anteriors; és suficient multiplicar unes quantes matrius per comprovar que

$$\sigma\langle g_3 \rangle = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \right\}$$

$$-\sigma\langle g_3 \rangle = \left\{ -\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, -\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, -\begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \right\}.$$

Així es demostra que H és conjugat a $\mathrm{GL}(2, \mathbb{Z})$ de $D_3' = \langle \sigma', g_3 \rangle$ o bé de $D_3'' = \langle -\sigma', g_3 \rangle$. □

Referències

[1] C. F. Gauss: *Disquisitiones Arithmeticae*, 1801. (Hi ha una traducció anglesa a Yale Univ. Press.)

[2] J.-P. Serre: *Cours d'Arithmétique*, Presses Universitaires de France, 1970.

Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra