Butlletí de la Societat Catalana de Matemàtiques
Vol. 28, núm. 1, 2013. Pàg. 5–49. DOI: 10.2436/20.2002.01.46

Teories de primer ordre i els problemes de Tarski

Resum: A principis del segle XX, les matemàtiques varen viure una crisi de fonaments coneguda com a *Grundlagenkrise der Mathematik*. Com a resposta a la necessitat de formalització de les matemàtiques, la lògica matemàtica va experimentar un desenvolupament profund. Aquest desenvolupament va derivar en el naixement de diverses branques de les matemàtiques, entre les quals la teoria de models, que estudia les estructures algebraiques des de la perspectiva de la lògica matemàtica. En aquest article presentem aquest punt de vista, mostrant tant la seva potència com les seves limitacions.

Comencem amb l'estudi del cos dels nombres complexos i dels nombres reals revisant els teoremes clàssics de Tarski. Continuem presentant alguns resultats de teoria de grups, com els teoremes de Szmielew sobre la teoria de primer ordre dels grups abelians. Acabem amb un resum de la solució recent dels problemes de Tarski sobre la teoria elemental dels grups lliures.

Paraules clau: teoria de models, teories de primer ordre, teoria elemental de grups, geometria algebraica sobre grups, problemes de Tarski.

Classificació MSC2010: 03-02, 20-02.

Introducció

Una de les qüestions recurrents en matemàtiques des dels seus orígens és l'essència dels conceptes matemàtics, així com els criteris per a la validació de demostracions. En contrast amb la idea platònica que els teoremes matemàtics són veritats absolutes indiscutibles, el segle XIX va ser un segle de dubtes. Diversos esdeveniments, com el desenvolupament de les geometries no euclidianes (que posaven en evidència que el cinquè axioma d'Euclides no era necessàriament vàlid) o l'aparició de nombroses paradoxes (com la de Russell, popularitzada amb la versió del barber) varen derivar, a principis del segle XX, en una seriosa crisi dels fonaments de les matemàtiques. Aquests focus de

El present article es basa en la xerrada impartida per l'autora a la Tretzena Trobada Matemàtica de la Societat Catalana de Matemàtiques, que va tenir lloc l'11 de juny de 2010 a Barcelona.

controvèrsia varen posar en evidència la necessitat de formalització de les matemàtiques. Amb l'objectiu de resoldre aquests conflictes i d'imposar rigor varen aparèixer diferents escoles de pensament, sent la formalista la més predominant. Els conceptes d'*axioma*, *proposició* i *demostració* es varen formalitzar i així van poder ser tractats com a objectes matemàtics. Es varen fixar un llenguatge sintàctic formal i unes regles d'inferència utilitzades per a deduir de forma finitista conclusions a partir d'un conjunt fixat d'axiomes. El llibre de Hilbert *Grundlagen der Geometrie* ('Fonaments de geometria') publicat el 1899 assenyala el canvi cap a aquest mètode axiomàtic modern. El problema de determinar un sistema d'axiomes i de provar-ne la consistència utilitzant sistemes formals va ser explícitament formulat, en el cas de l'aritmètica, en el segon problema de la famosa llista de problemes que Hilbert va proposar el 1900 en el Congrés Internacional de Matemàtiques i, amb tota la seva generalitat, en el projecte que es coneix avui en dia com el *programa de Hilbert*. Des d'aquest punt de vista podem dir que l'atmosfera matemàtica de principis del segle XX és representada pel programa formalista de Hilbert així com pel punt de vista logicista de Frege i de Russell segons el qual les matemàtiques no es poden separar de la lògica.

Amb el desenvolupament de la lògica matemàtica, la teoria que havia de servir per a l'estudi dels fonaments matemàtics es va convertir, en si mateixa, en objecte d'estudi matemàtic, denominat per Hilbert *metamatemàtica*. A mitjan segle XX Tarski va suggerir que la lògica matemàtica no s'hauria de restringir tan sols als fonaments matemàtics sinó que se n'hauria d'estendre l'ús per a estudiar estructures algebraiques. Continuant idees de Löwenheim, Skolem, Gödel i altres, Tarski va introduir semàntica en la lògica, i es va convertir així en un dels pares fundadors del que avui en dia es coneix com a *teoria de models*.

Des d'aquesta perspectiva, doncs, les estructures algebraiques no tan sols es poden estudiar des d'un punt de vista algebraic, sinó també des d'un punt de vista lògic: en lloc de determinar propietats algebraiques de l'objecte, hom determina les sentències que en són certes; i en lloc de classificar els objectes mòdul isomorfia, hom els classifica mòdul equivalència elemental.

Un dels objectius principals d'aquest article és introduir el lector en els problemes de Tarski i motivar així aquesta vessant model-teorètica de l'estudi d'estructures algebraiques. Com la majoria dels grans problemes matemàtics, els problemes de Tarski tenen una formulació senzilla però, en contrast, la seva solució ha estat un dels resultats més profunds de la teoria geomètrica de grups. El 2006, Zlil Sela va demostrar que els grups lliures no abelians són elementalment equivalents; és a dir, tot i que els podem diferenciar algebraicament mitjançant el seu rang, no es poden distingir des d'un punt de vista model-teorètic. Olga Kharlampovich i Alexei Myasnikov varen demostrar, a més a més, que existeix un algoritme que determina quines sentències són certes en un grup lliure.

Ambdues demostracions són molt llargues, tècnicament complexes i, en certa manera, poc enteses a dia d'avui. No obstant això, i tot i la diferència tècnica, a grans trets l'estratègia d'atac és la mateixa que la duta a terme en

l'estudi model-teorètic d'estructures algebraiques clàssiques com el cos dels nombres complexos i els grups abelians lliures: determinar un conjunt d'eliminació i estudiar-lo. En la primera part de l'article introduïm els conceptes bàsics, plantegem els problemes centrals i revisem informalment els resultats i estratègies principals de l'estudi de les teories dels anells i dels grups clàssics. Aquesta introducció a la teoria de models segueix una línia d'exposició tradicional, centrada en l'eliminació de quantificadors, ja que ens sembla la més natural per a aproximar-nos a la solució dels problemes de Tarski. S'aconsella al lector interessat en un punt de vista més actual de la teoria de models llegir els articles expositius [29] i [54].

Des de la seva formulació, els problemes de Tarski han motivat el desenvolupament d'un gran nombre de tècniques i mètodes que s'han convertit en eines fonamentals en l'estudi modern dels grups i han ajudat a establir noves connexions entre diverses branques de les matemàtiques com la geometria, els sistemes dinàmics i la teoria de grups. Aquestes tècniques són el tema central de la segona part. Cal remarcar que, tot i que esmentem molts resultats per tal de fer natural la seqüència d'avenços, aquest article no pretén pas ser una revisió històrica i cal tenir en compte que la llista de treballs citats s'adapta a l'exposició i és, per tant, parcial i incompleta.

Part I: Elements de la teoria de models

1 Nocions bàsiques

Per a entendre més bé els objectius i les motivacions d'aquest estudi lògic, necessitem introduir unes quantes definicions bàsiques. Tots els conceptes que introduirem en aquesta secció són estàndards i es poden trobar en la majoria de la literatura especialitzada [10, 24, 42]. Ens agradaria puntualitzar que, per simplificar i abreujar l'exposició, ens hem pres algunes llibertats d'imprecisió i d'omissió.

Fent un exercici de simplificació, podem dir que una llengua es desenvolupa a partir de tres pilars diferents: l'alfabet, les paraules i una gramàtica (unes normes per a la construcció de frases). El perfil que seguim en lògica és similar: definim un llenguatge (o alfabet), en determinem els termes (o paraules) i utilitzem unes normes (connectors lògics com $=$, $\vee$, ...) per a crear frases.

El llenguatge està format per un conjunt de funcions, relacions i constants que constituiran el nostre alfabet. Com en la majoria de les llengües, les lletres de l'alfabet o, en el nostre cas, les funcions, relacions i constants no tenen per si mateixes cap significat associat, són senzillament símbols.

DEFINICIÓ 1. Un *llenguatge* $\mathcal{L}$ és una terna formada per:

- un conjunt de símbols funció $\mathcal{F}$ i un nombre positiu n_f per a cada $f \in \mathcal{F}$,
- un conjunt de símbols relació $\mathcal{R}$ i un nombre positiu n_r per a cada $r \in \mathcal{R}$,
- i un conjunt de símbols constant C.

El nombre n_f determina el nombre de variables del símbol funció f i el nombre n_r determina l'enaritat del símbol relació r.

Ara recordarem uns quants exemples típics de llenguatges comunament utilitzats.

EXEMPLE.

- El llenguatge dels monoides $\mathcal{L}_M = \{\cdot, 1\}$, on $\cdot$ és un símbol funció binari i 1 un símbol constant.
- El llenguatge dels grups $\mathcal{L}_G = \{\cdot, ^{-1}, 1\}$, on $\cdot$ és un símbol funció binari, $^{-1}$ és un símbol funció unari i 1 un símbol constant.
- El llenguatge dels anells $\mathcal{L}_A = \{+, -, \cdot, 0, 1\}$ on $+$, $-$ i $\cdot$ són símbols funció binaris i 0 i 1 símbols constants.
- El llenguatge dels anells ordenats $\mathcal{L}_O = \mathcal{L}_A \cup \{<\}$, on $<$ és un símbol relació binari.

Un cop establert el llenguatge, podem determinar el conjunt de paraules, els termes. El conjunt de termes conté el conjunt de constants del llenguatge, un conjunt comptable de variables i es completa de forma recursiva aplicant les funcions del llenguatge a termes ja definits.

DEFINICIÓ 2. Sigui $\mathcal{L}$ un llenguatge i $\{x_1, \dots, x_n, \dots\}$ un conjunt comptable de variables. El conjunt de *$\mathcal{L}$-termes* és el menor conjunt $\mathcal{T}$ tal que:

- $c \in \mathcal{T}$ per a cada símbol constant $c \in C$,
- $x_i \in \mathcal{T}$, per a cada símbol variable x_i, $i = 1, 2, \dots$,
- si $t_1, \dots, t_{n_f} \in \mathcal{T}$ i $f \in \mathcal{F}$, llavors $f(t_1, \dots, t_{n_f}) \in \mathcal{T}$.

Quan el conjunt de relacions $\mathcal{R}$ d'un llenguatge és buit, el llenguatge s'anomena *funcional* o *algebraic*.

Tot i no ser una notació habitual, en aquest article escriurem $t(X)$ per remarcar que les variables que apareixen en el terme t són les variables $X = \{x_{i_1}, \dots, x_{i_n}\}$.

Finalment, un cop tenim definits els termes del nostre llenguatge podem descriure el procés de creació de frases o, en el nostre cas, de fórmules. Les fórmules es poden organitzar segons el seu nivell de complexitat, les més senzilles són les fórmules atòmiques.

DEFINICIÓ 3. Anomenem *fórmula atòmica* qualsevol expressió dels dos tipus següents:

- $(t_1 = t_2)$ on t_1, t_2 són $\mathcal{L}$-termes,
- $r(t_1, \dots, t_{r_n})$ on $r \in \mathcal{R}$ i $t_1, \dots, t_{r_n}$ són $\mathcal{L}$-termes.

Les fórmules es construeixen a partir de fórmules atòmiques, negant-les, prenent-ne conjuncions i disjuncions, i quantificant-ne les variables.

DEFINICIÓ 4. Una *combinació booleana* Ψ és una disjunció de conjuncions de fórmules atòmiques i les seves negacions

$$\Psi = \bigvee_{i=1}^{m} \Psi_i, \quad \text{on} \quad \Psi_i = \bigwedge_{j=1}^{n_i} \varphi_j^i \wedge \bigwedge_{k=1}^{r_i} \neg \psi_k^i,$$

i on les φ_j^i, ψ_k^i són fórmules atòmiques.

DEFINICIÓ 5. Una *fórmula*[1] Φ *amb variables lliures* $Z = \{z_1, \ldots, z_k\}$ *i variables lligades* $X = \{x_1, \ldots, x_l\}$ (amb $X \cap Z = \emptyset$) és una expressió de la forma

$$Q_1 x_1 \, Q_2 x_2 \, \ldots \, Q_l x_l \, \Psi(X, Z),$$

on cada $Q_k \in \{\forall, \exists\}$ i $\Psi(X, Z)$ és una combinació booleana de fórmules atòmiques en les variables $X \cup Z$. Els símbols $\forall$ i $\exists$ s'anomenem *quantificadors* (*universal* i *existencial*, respectivament).

DEFINICIÓ 6. Una fórmula Φ s'anomena *sentència* si Φ no conté variables lliures, o, equivalentment, totes les variables són lligades, és a dir, estan «quantificades» per un quantificador universal o existencial.

EXEMPLE. Sigui $\mathcal{L}_A = \{+, -, \cdot, 0, 1\}$ el llenguatge d'anells.

- La fórmula $x_1 \cdot x_2 = x_2 \cdot x_1$ és una fórmula atòmica.
- La fórmula $\forall x_1 \, (x_1 \cdot x_2 = x_2 \cdot x_1)$ és una fórmula amb variable lliure x_2.
- La fórmula $\forall x_1 \, \forall x_2 \, (x_1 \cdot x_2 = x_2 \cdot x_1)$ és una sentència.

DEFINICIÓ 7.

- La fórmula Φ s'anomena *universal* (resp. *existencial*) si tots els quantificadors són universals (resp. existencials), *i. e.*, $Q_k = \forall$ (resp. $Q_k = \exists$) per a tot $k = 1, \ldots, l$.
- La fórmula Φ s'anomena $\forall\exists$*-fórmula* si existeix $l' \in \{1, \ldots, l-1\}$ tal que $Q_j = \forall$ per a tot $1 \leq j \leq l'$ i $Q_k = \exists$ per a tot $l' < k \leq l$. D'una manera anàloga podem definir $\exists\forall$-fórmula, $\forall\exists\forall$-fórmula, etc.
- La fórmula Φ s'anomena *positiva* si no conté negacions de fórmules atòmiques, *i. e.*, la combinació booleana Ψ és de la forma $\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n_i} \varphi_j^i$, amb les φ_j^i atòmiques.

En certa mesura, tots estem familiaritzats amb el concepte de *fórmula* tot i que potser no se'ns havia introduït formalment. En aquest punt, fem un parell d'observacions per evitar possibles malentesos:

1 La definició que donem de *fórmula* és de fet la definició de *fórmula en forma normal prenexa*. Això no comporta cap restricció, ja que tota fórmula en el sentit ordinari és lògicament equivalent a una en la forma normal prenexa.

- Les fórmules que considerem són *finites*, per tant, no inclouen expressions del tipus $(x = 0 \vee \bigwedge_{n=1}^{\infty} x^n \neq 0)$.
- Només es permet quantificar *elements*, per tant, l'expressió «per a tot ideal d'un anell...» no es pot expressar mitjançant una fórmula en el llenguatge d'anells.

Aquestes són restriccions de la lògica anomenada *de primer ordre*. Hi ha altres lògiques d'ordre superior que permeten quantificar funcions, relacions, etc. En aquest article només considerarem lògica de primer ordre.

Des del punt de vista lògic, les funcions, les relacions i les constants són símbols mancats de contingut. És via les estructures (els models) i les corresponents interpretacions de les funcions, relacions i constants en aquestes estructures que hom els dóna semàntica. Aquest és el tema central de la teoria de models: la classificació i construcció d'estructures a través del llenguatge formal lògic.

Fixat un llenguatge $\mathcal{L}$, una $\mathcal{L}$-estructura (o un $\mathcal{L}$-model) és un conjunt no buit amb les corresponents «interpretacions» de les funcions, relacions i constants. Formalment,

DEFINICIÓ 8. Una *$\mathcal{L}$-estructura $\mathcal{M}$* és:

- un conjunt M no buit que anomenem *univers*;
- una funció $f^{\mathcal{M}}\colon M^{n_f} \to M$ per a cada símbol funció $f \in \mathcal{F}$;
- un conjunt $r^{\mathcal{M}} \subset M^{n_r}$ per a cada símbol relació $r \in \mathcal{R}$;
- un element $c^{\mathcal{M}} \in M$ per a cada símbol constant $c \in C$.

Quan el llenguatge $\mathcal{L}$ se sobreentén en el context, sovint anomenem les $\mathcal{L}$-estructures senzillament *estructures*.

Per exemple, fixem el llenguatge de grups $\mathcal{L}_G = \{\cdot, ^{-1}, 1\}$. En aquest llenguatge, $\mathcal{G} = (\mathbb{R}, \cdot, \mathrm{id}, 1)$ és una $\mathcal{L}_G$-estructura on interpretem el símbol funció $\cdot$ com la funció multiplicació de nombres reals, el símbol $^{-1}$ com la funció identitat i el símbol constant 1 com l'element neutre 1. Però també podem donar una estructura diferent a l'univers dels nombres reals, per exemple $\mathcal{G}' = (\mathbb{R}, +, -, 0)$ és una $\mathcal{L}_G$-estructura on interpretem el símbol funció $\cdot$ com la funció suma de nombres reals, el símbol $^{-1}$ com la funció invers (respecte a la suma, *i. e.*, $-(n) = -n$) i el símbol constant 1 com l'element 0.

Cal prestar atenció a l'ambigüitat del nom *llenguatge de grups*. El llenguatge $\mathcal{L}$ s'anomena *llenguatge de grups* perquè tots els grups indueixen de forma natural una $\mathcal{L}_G$-estructura: l'univers és el conjunt d'elements del grup, el símbol funció $\cdot$ s'interpreta com l'operació en el grup, el símbol funció $^{-1}$ com la funció invers i el símbol constant 1 com l'element neutre del grup. Però, en general, les $\mathcal{L}_G$-estructures no són necessàriament grups! Per exemple, $\mathcal{N} = (\mathbb{N}, f, \mathrm{id}, 5)$, on l'univers és el conjunt de nombres naturals i $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ és la funció definida per $f(n, m) := 2n + 3m$, és una $\mathcal{L}_G$-estructura. El conjunt de grups, però, es pot «distingir» dins el conjunt de $\mathcal{L}_G$-estructures: els grups són $\mathcal{L}_G$-estructures que satisfan un cert conjunt de sentències —els axiomes dels grups.

Les fórmules són expressions sintàctiques que adquireixen significat un cop les relacionem amb una estructura. Com hem comentat, la semàntica dels símbols funció i de les constants es determina via les interpretacions. En canvi, els símbols lògics sempre tenen el mateix significat, independentment de l'estructura. Així, el connector lògic $\wedge$ pren el significat «i», el connector $\vee$, «o», el quantificador $\forall$, «per a tot», etc.

Si considerem un anell A (amb les interpretacions naturals de les funcions i constants del llenguatge d'anells), el significat de la fórmula $\forall x_1\, \forall x_2\, (x_1 \cdot x_2 = x_2 \cdot x_1)$ en A és «per a tot element a_1 de A i tot element a_2 de A, el producte d'a_1 per a_2 és igual al producte d'a_2 per a_1».

D'aquesta manera, donada una sentència i una estructura d'un mateix llenguatge, la (interpretació d'aquesta) sentència és certa o no en l'estructura. En l'exemple anterior, la sentència $\forall x_1\, \forall x_2\, (x_1 \cdot x_2 = x_2 \cdot x_1)$ és certa en un anell A si i només si l'anell és commutatiu. Veiem, doncs, que les sentències que són certes en una estructura determinen propietats d'aquesta estructura.

En canvi, donada una fórmula $\phi(z_1, \ldots, z_k)$ amb variables lliures $z_1, \ldots, z_k$ i una estructura $\mathcal{M}$, la fórmula ϕ no determina propietats generals de l'estructura, sinó que determina propietats dels elements $(m_1, \ldots, m_k) \in M^k$ per als quals ϕ és certa. En altres paraules, podem determinar si (la interpretació d')una fórmula és certa o no en una estructura un cop especifiquem els valors que prenen les seves variables lliures. Continuant amb el nostre exemple, la fórmula $\forall x_1\, (x_1 \cdot x_2 = x_2 \cdot x_1)$ és certa en un anell A si interpretem la variable lliure x_2 en un element del centre de l'anell.

Un conjunt $S \subset M^k$ d'una $\mathcal{L}$-estructura $\mathcal{M}$ s'anomena *definible* si existeix una fórmula $\phi(z_1, \ldots, z_k)$ amb variables lliures $z_1, \ldots, z_k$ tal que una kàtupla $(m_1, \ldots, m_k) \in M^k$ pertany a S si i només si la fórmula ϕ és certa per a $(m_1, \ldots, m_k)$.

DEFINICIÓ 9. Donada una $\mathcal{L}$-estructura $\mathcal{M}$, el conjunt de sentències que són certes en $\mathcal{M}$ s'anomena *teoria elemental* de $\mathcal{M}$ i el denotarem per $\mathrm{Th}(\mathcal{M})$.

Diem que dues $\mathcal{L}$-estructures $\mathcal{M}$ i $\mathcal{N}$ són *elementalment equivalents*, i ho denotem per $\mathcal{M} \equiv \mathcal{N}$, si les corresponents teories elementals coincideixen, és a dir, si $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$.

És fàcil de demostrar (utilitzant inducció en la complexitat de les fórmules) que si dues $\mathcal{L}$-estructures són isomorfes, llavors són elementalment equivalents. Però en general el recíproc no és cert (veurem exemples en les seccions següents).

Tal com veurem més endavant, sovint és important considerar només fragments de la teoria elemental d'una estructura en lloc de tota la teoria.

DEFINICIÓ 10. La *teoria universal* (resp. *existencial*, *positiva*) d'una estructura $\mathcal{M}$ és el conjunt de sentències universals (resp. existencials, positives) que són certes en $\mathcal{M}$; la denotem per $\mathrm{Th}_\forall(\mathcal{M})$ (resp. $\mathrm{Th}_\exists(\mathcal{M})$, $\mathrm{Th}^+(\mathcal{M})$).

Diem que dues estructures $\mathcal{M}$ i $\mathcal{N}$ són *universalment equivalents* (resp. *existencialment equivalents*) i ho denotem per $\mathcal{M} \equiv_\forall \mathcal{N}$ (resp. $\mathcal{M} \equiv_\exists \mathcal{N}$) si $\mathrm{Th}_\forall(\mathcal{M}) = \mathrm{Th}_\forall(\mathcal{N})$ (resp. $\mathrm{Th}_\exists(\mathcal{M}) = \mathrm{Th}_\exists(\mathcal{N})$).

La negació d'una sentència universal és equivalent a una sentència existencial. D'aquesta dualitat obtenim que dues estructures són universalment equivalents si i només si són existencialment equivalents, *i. e.*, $\mathcal{M} \equiv_\forall \mathcal{N} \Leftrightarrow \mathcal{M} \equiv_\exists \mathcal{N}$.

D'una manera similar, definim la $\forall\exists$-*teoria* d'una estructura $\mathcal{A}$ com el conjunt de $\forall\exists$-sentències que són certes en l'estructura i la denotem per $\mathrm{Th}_{\forall\exists}(\mathcal{A})$.

2 Problemes principals

En aquesta secció formulem els problemes que ens concerniran en l'estudi d'estructures algebraiques des del punt de vista model-teorètic. D'una manera molt genèrica podem dir que una part important de les matemàtiques se centra en l'estudi de certes propietats d'una classe d'objectes: les propietats algebraiques dels anells (en teoria d'anells, en geometria algebraica), les propietats homotòpiques dels espais (en topologia algebraica), etc. Així doncs, un primer pas natural és identificar els objectes que satisfan les mateixes propietats i per tant reduir l'estudi a les classes d'equivalència. Les qüestions bàsiques des d'aquest punt de vista són determinar els objectes que pertanyen a la mateixa classe d'equivalència (determinar quins anells són isomorfs, quins espais són homotòpicament equivalents, etc.); determinar les propietats que satisfan els objectes d'una certa classe d'equivalència (determinar el grup d'homologia d'una classe d'espais homotòpics, etc.). En el nostre cas, ens interessa estudiar les propietats de primer ordre de les estructures algebraiques.

Determinar les classes d'equivalència

Un dels objectius principals és determinar les classes d'equivalència mòdul equivalència elemental i mòdul equivalència universal, *i. e.*, donada una $\mathcal{L}$-estructura $\mathcal{M}$ determinar les $\mathcal{L}$-estructures que són elementalment equivalents a $\mathcal{M}$ i les que són universalment equivalents a $\mathcal{M}$. Sorprenentment, veurem que aquestes classes són tant o més naturals que les classes mòdul isomorfia.

A vegades, però, el problema de classificar *totes* les estructures elementalment (resp. universalment) equivalents a una de fixada és massa complicat. Una restricció natural del problema és determinar els elements de la classe d'equivalència d'una cardinalitat determinada o, per exemple, classificar les estructures *finitament generades* que són elementalment equivalents a una de donada. Encara en una perspectiva més reduïda, sovint ens pot interessar senzillament, donada una classe d'estructures, determinar quines són elementalment equivalents entre si.

Un cop determinades les classes elementals (resp. universals), podem estudiar quines propietats són invariants elementals.

Decidibilitat de les teories

Quan estudiem una estructura $\mathcal{M}$, a part d'interessar-nos per les estructures que tenen la mateixa teoria que $\mathcal{M}$, hom es pot interessar directament per la mateixa teoria, és a dir, per entendre quines són les sentències que són certes en $\mathcal{M}$ i quines no.

Precisant una mica més, hom vol determinar la *decidibilitat* de la teoria elemental de $\mathcal{M}$ o, en altres paraules, determinar l'existència d'un algoritme que accepti com a entrada una sentència ϕ del llenguatge i retorni «sí», si ϕ pertany a la teoria elemental de $\mathcal{M}$, i «no», altrament. Com en el problema anterior, hom pot restringir-se a fragments de la teoria, com per exemple determinar la decidibilitat de la teoria existencial.

En tot anell, les fórmules atòmiques són equivalents a una equació polinòmica amb coeficients enters i, de fet, tal com veurem més endavant, les fórmules atòmiques són la generalització natural del concepte d'*equació*. Amb aquesta terminologia, el problema de compatibilitat de sistemes d'equacions en un anell es correspon al problema de decidibilitat de la teoria existencial positiva de l'anell. Per tant, determinar la decidibilitat de la teoria d'una estructura o d'un fragment d'aquesta teoria ens proporciona una gran quantitat d'informació no només model-teorètica sinó també algebraica. A més a més, la teoria de models ens ofereix un marc teòric que no només ens permet generalitzar el problema de compatibilitat d'equacions en un anell al problema de decidibilitat de la teoria elemental, sinó que també ens permet formular aquests tipus de problemes per a estructures arbitràries.

Conjunts definibles

Els problemes que hem enunciat fins ara s'ocupen de l'estudi de la teoria elemental d'una estructura. Les sentències són un cas particular de fórmules i, per tant, hom pot anar un pas més enllà i estudiar fórmules i, més concretament, els conjunts i relacions definibles a través de fórmules.

Els exemples més senzills de conjunts definibles són aquells que són definits per fórmules atòmiques. Ja hem comentat que les fórmules atòmiques en un anell són senzillament equacions polinòmiques i, per tant, els conjunts definibles per fórmules atòmiques són exactament els conjunts algebraics.

Propietats de la teoria

Encara que no entrarem en detalls ni definicions, hi ha moltes propietats de la teoria d'una estructura que són essencials des del punt de vista lògic. Per exemple, l'estabilitat de la teoria d'una estructura mesura la complexitat de la classificació de les estructures elementalment equivalents a ella: informalment, si la teoria no és estable vol dir que hi ha massa estructures elementalment equivalents a ella i que aquestes són massa complicades per a poder esperar una classificació raonable. En general, doncs, un dels problemes és estudiar les propietats (model-teorètiques) de la teoria d'una estructura.

3 Anells i cossos

En aquesta secció presentem una sèrie de resultats en l'estudi d'estructures clàssiques (els cossos dels nombres complexos, reals, racionals, i l'anell dels nombres enters) des de la perspectiva de la teoria de models. Per a una exposició més formal i detallada el lector pot consultar [42, 23, 24]. El llenguatge que considerem en tota aquesta secció és el llenguatge d'anells $\mathcal{L}_A = \{+, -, \cdot, 1, 0\}$. Tots els cossos i anells amb les interpretacions naturals són estructures del llenguatge d'anells i és sota aquestes consideracions que els estudiarem.

Nombres complexos

El cos dels nombres complexos va ser un dels primers a ser estudiat a finals dels anys quaranta per Tarski. La seva teoria és probablement una de les més ben enteses i un dels millors exemples d'estructura on podem resoldre la majoria dels problemes que hem formulat en la secció anterior. Recopilem diversos resultats de la teoria del cos dels nombres complexos:

TEOREMA 11.

- *Una $\mathcal{L}_A$-estructura F és elementalment equivalent al cos dels nombres complexos $\mathbb{C}$ si i només si F és un cos algebraicament tancat de característica zero* [67].
- *Una $\mathcal{L}_A$-estructura F és universalment equivalent al cos dels nombres complexos $\mathbb{C}$ si i només si F és un domini d'integritat de característica zero* [67].
- *La teoria elemental de $\mathbb{C}$ és decidible* [67].
- *Els conjunts definibles en $\mathbb{C}^n$, $n \in \mathbb{N}$, són combinacions booleanes (*i. e.*, amb les operacions conjuntistes de reunió, intersecció, complementari) de varietats algebraiques.*
- *La propietat «ser algebraicament tancat» és un invariant lògic, mentre que el grau de transcendència no ho és.*
- *La teoria elemental dels nombres complexos és estable.*

Però, com es demostra un teorema com aquest?

Primer comencem observant un fet general. Els axiomes dels cossos es poden expressar mitjançant fórmules del llenguatge d'anells:

- L'operació + és associativa: $\forall x\, \forall y\, \forall z\, \big((x + y) + z = x + (y + z)\big)$.
- L'operació + és commutativa: $\forall x\, \forall y\, (x + y = y + x)$.
- ...

Com que el cos dels nombres complexos satisfà aquests axiomes, tota estructura elementalment equivalent al cos dels nombres complexos també els satisfà i, per tant, és un cos. Evidentment aquest fenomen és general: si una estructura pertany a una classe axiomatitzable en el llenguatge (classe de cossos, anells,

grups, grups abelians…), llavors tota estructura elementalment equivalent pertany a la mateixa classe.

Els axiomes dels cossos ens permeten simplificar l'estructura de les fórmules: és fàcil demostrar que tota fórmula atòmica és equivalent (mòdul els axiomes dels cossos) a una equació polinòmica amb coeficients enters.

En particular, les sentències atòmiques són equivalents a expressions de la forma $n = 0$, $n \in \mathbb{Z}$. Per a determinar quines sentències atòmiques pertanyen a la teoria elemental dels nombres complexos només ens cal observar que $\mathbb{C}$ és un cos de característica zero, *i. e.*, tot nombre complex satisfà el conjunt infinit de fórmules

$$\{x = 0 \vee (\underbrace{x + \cdots + x}_{n \text{ vegades}} \neq 0) \mid n \in \mathbb{N}\}.$$

Obtenim com a conseqüència que les úniques sentències atòmiques que pertanyen a la teoria $\mathrm{Th}(\mathbb{C})$ són les equivalents a $(0 = 0)$ i, a més a més, que tot cos elementalment equivalent al cos dels nombres complexos és un cos de característica zero.

Les sentències següents que cal considerar són les sentències existencials (en una variable) positives o, més familiarment, sentències de la forma $\exists x\ (p(x) = 0)$, on $p(x)$ és un polinomi (amb coeficients enters). En aquest cas, per a decidir quines d'aquestes sentències pertanyen a la teoria del cos dels nombres complexos només ens cal notar que el cos dels nombres complexos és algebraicament tancat i, per tant, tot polinomi (no constant) té arrels.

La condició «ser algebraicament tancat» torna a ser una propietat de primer ordre expressada pel conjunt infinit de fórmules:

$$\Big\{\forall a_0\, \forall a_1 \ldots \forall a_n \Big(\underbrace{\exists x (a_0 + a_1 x + \cdots + a_n x^n = 0)}_{\text{(l'equació té solució)}} \vee \underbrace{(a_1 = \cdots = a_n = 0 \wedge a_0 \neq 0)}_{\text{(el polinomi és constant)}}\Big) \Big| \, n \in \mathbb{N}\Big\}.$$

Per tant, tota $\mathcal{L}_A$-estructura elementalment equivalent a $\mathbb{C}$ és un cos algebraicament tancat.

En general, determinant propietats d'una estructura fixada $\mathcal{M}$ que es poden definir mitjançant fórmules imposem restriccions en les estructures elementalment equivalents a $\mathcal{M}$; és a dir, reduïm el conjunt que conté les estructures elementalment equivalents a $\mathcal{M}$. El problema, doncs, és decidir quan aquest conjunt és exactament la classe d'equivalència elemental de $\mathcal{M}$ o, en altres paraules, determinar quan una classe és de fet una classe d'equivalència elemental. En el nostre cas, imposant condicions hem vist que tota estructura elementalment equivalent al cos dels nombres complexos és un cos algebraicament tancat de característica zero. La qüestió és: és la classe de cossos algebraicament tancats de característica zero una classe elemental? Una de les tècniques més eficients per a demostrar que una classe és elemental és l'eliminació de quantificadors.

Abans de formular exactament en què es basa aquesta tècnica revisem uns quants exemples.

Com hem observat anteriorment, la fórmula ϕ

$$\exists x\,(ax^2 + bx + c = 0),$$

on $a, b, c \in \mathbb{Z}$, és certa en el cos dels nombres complexos si i només si $a \neq 0 \vee b \neq 0 \vee c = 0$. Així doncs, la fórmula ϕ és equivalent a una fórmula sense quantificadors.

Per una altra banda, la fórmula ϕ

$$\exists x\,(ax^2 + bx + c \neq 0)$$

és certa en el cos dels nombres complexos si i només si $a \neq 0 \vee b \neq 0 \vee c \neq 0$, ja que els polinomis en una variable tenen un nombre finit d'arrels i els cossos algebraicament tancats són infinits.

Una mica més complicada, la fórmula ϕ

$$\forall x\,\exists y\,(xy^7 + x^4 + 1 = 0)$$

és certa en $\mathbb{C}$ si i només si també ho és la fórmula $\forall x\,(x \neq 0 \vee x^4 + 1 = 0)$ (el polinomi considerat en la variable y i «paràmetre» x no és un polinomi constant no trivial); alhora aquesta fórmula és certa si i només si $\forall x\,(x \neq 0 \vee 0 + 1 = 0)$ si i només si $\forall x\,(x \neq 0)$ si i només si $0 \neq 0$. Un altre cop, la sentència ϕ és equivalent a una fórmula sense quantificador.

Hom pot demostrar que, de fet, aquest fenomen és general; és a dir, que utilitzant els axiomes dels cossos i els axiomes de cos algebraicament tancat, qualsevol fórmula és equivalent a una fórmula sense quantificadors. Quan la teoria d'una estructura té aquesta propietat diem que la teoria té *eliminació de quantificadors*.

Com que en la teoria dels nombres complexos, tota fórmula és equivalent a una sense quantificadors, per a decidir quins cossos algebraicament tancats són elementalment equivalents entre si només ens cal determinar quins satisfan les mateixes sentències sense quantificadors. Les sentències sense quantificadors en la teoria dels cossos són combinacions booleanes de sentències atòmiques dels tipus $n = 0$ i $n \neq 0$, $n \in \mathbb{Z}$. Podem concloure, doncs, que dos cossos algebraicament tancats són elementalment equivalents si i només si tenen la mateixa característica. En altres paraules, podem dir que la teoria dels nombres complexos es pot axiomatitzar mitjançant els axiomes dels cossos, els axiomes de cos algebraicament tancat i els axiomes de característica zero.

En particular, el cos dels nombres algebraics és elementalment equivalent al cos dels nombres complexos, però en canvi no són isomorfs. Aquest és el primer exemple on podem veure la diferència entre les classes mòdul equivalència elemental i mòdul isomorfia. Noteu també que tot i que les classes d'equivalència elemental són definides per propietats lògiques, en aquest cas la seva descripció és completament algebraica.

Com a conseqüència de l'eliminació de quantificadors obtenim que la teoria del cos dels nombres complexos és decidible i que els conjunts definibles són exactament els conjunts construïbles, *i. e.*, combinacions booleanes de conjunts algebraics. D'aquesta descripció podem deduir que els conjunts definibles són o bé finits o bé cofinits (*i. e.*, de complementari finit). Quan els conjunts definibles d'una teoria satisfan aquesta propietat diem que la teoria és *fortament minimal*. El fet que la teoria dels nombres complexos és fortament minimal implica que aquesta teoria és estable. Com ja hem comentat, l'estabilitat és una propietat essencial en la teoria de models, ja que defineix una línia divisòria fonamental entre les teories «accessibles» (de les quals podem entendre els models) i les «massa complicades». En el cas de la teoria dels nombres complexos, hom pot demostrar que per a cada cardinal infinit existeix un únic model de la teoria (mòdul isomorfia de cossos): l'únic model de cardinalitat $\aleph_0$ de la teoria dels nombres complexos és el cos dels nombres algebraics, l'únic model de cardinalitat $\aleph_1$ és el cos dels nombres complexos, etc.

L'eliminació de quantificadors també proporciona una demostració alternativa del teorema clàssic de Chevalley. En geometria algebraica, el teorema de Chevalley afirma que la projecció d'un conjunt construïble és construïble. Com que les projeccions es corresponen a quantificadors existencials, el teorema de Chevalley es pot reformular dient que tot conjunt definible per una fórmula existencial és definible per una combinació booleana de fórmules.

Una altra conseqüència immediata de l'eliminació de quantificadors és la model-completesa de la teoria dels nombres complexos. La teoria d'una estructura és *model-completa* si tota fórmula és equivalent en la teoria a una fórmula existencial. Robinson [58] va introduir aquest concepte i es va adonar que, de fet, la demostració que la teoria dels nombres complexos és model-completa és essencialment la mateixa que el *Nullstellensatz* de Hilbert.

Tal com acabem de mostrar, quan es pot dur a terme, el mètode d'eliminació de quantificadors proporciona una quantitat immensa d'informació de la teoria i dels conjunts definibles. És, sens dubte, un dels mètodes més directes per a l'accés a una teoria. En general, però, hi ha poques teories que gaudeixin d'eliminació de quantificadors. Per exemple, dins la classe de cossos infinits en el llenguatge d'anells, les teories dels cossos algebraicament tancats són les úniques que tenen eliminació de quantificadors [34].

Nombres reals

De moment, l'única tècnica que hem presentat per a determinar la classe elemental d'una teoria és l'eliminació de quantificadors. Però si, com hem comentat, el fet que un teoria tingui eliminació de quantificadors no és habitual, com podem estudiar altres teories?

Presentem en el teorema següent uns quants resultats de la teoria del cos dels nombres reals i tot seguit discutim superficialment el mètode per a demostrar-los.

TEOREMA 12.

- *Una $\mathcal{L}_A$-estructura F és elementalment equivalent al cos dels nombres reals $\mathbb{R}$ si i només si F és un cos real-tancat*[2] [68].
- *Una $\mathcal{L}_A$-estructura F és universalment equivalent al cos dels nombres reals $\mathbb{R}$ si i només si F és un domini d'integritat de característica zero* [68].
- *La teoria elemental del cos dels nombres reals $\mathbb{R}$ és decidible* [68].
- *La teoria elemental del cos dels nombres reals és model-completa i inestable.*

Hem vist que en el cas del cos dels nombres complexos, la propietat de ser algebraicament tancat és crucial per a obtenir l'eliminació de quantificadors. El cos dels nombres reals no és algebraicament tancat, però satisfà que tot polinomi de grau senar (no constant) té arrels; és a dir, en el cos dels nombres reals, per a cada $n \in \mathbb{N}$ la sentència

$$\exists x \left(a_{2n+1}x^{2n+1} + \cdots + a_1 x + a_0 = 0 \right)$$

és certa si la sentència sense quantificadors

$$a_{2n+1} \neq 0 \vee \left(\bigvee_{i=0}^{n-1} \left(a_{2i+1} \neq 0 \wedge \left(\bigwedge_{j>2i+1}^{2n+1} a_j = 0 \right) \right) \right) \vee a_0 = 0$$

(que diu que el polinomi és de grau senar i no constant) també ho és.

Però, en canvi, la sentència

$$\exists x \left(ax^2 + bx + c = 0 \right),$$

on $a, b, c \in \mathbb{Z}$, és certa en els nombres reals si i només si la sentència $(a \neq 0 \vee b \neq 0 \vee c = 0) \wedge (\exists y\, (y^2 = b^2 - 4ac))$ és certa (*i. e.*, l'equació no és constant no trivial i l'arrel quadrada del radicand existeix). En general, les equacions polinòmiques de grau parell es redueixen a una fórmula existencial, però no podem assegurar que es redueixin a una sense quantificadors.

Quan una teoria no té eliminació de quantificadors, no podem reduir l'estudi de la teoria a l'estudi de fórmules sense quantificadors, però podem intentar reduir-la a una família de fórmules Φ com més senzilla millor. En altres paraules, l'objectiu és determinar una família de fórmules Φ de manera que tota fórmula del llenguatge sigui equivalent (en la teoria de l'estructura) a una combinació booleana de fórmules de Φ; aquest conjunt de fórmules Φ s'anomena *conjunt d'eliminació*. En aquests termes més generals, el fet que una teoria tingui eliminació de quantificadors és equivalent a dir que el conjunt de fórmules atòmiques és un conjunt d'eliminació per a la teoria.

Tarski va demostrar que el conjunt de fórmules

$$\Phi := \{\exists y\, (y^2 = t(X)) \mid t(X) \text{ és un } \mathcal{L}_A\text{-terme que no conté la variable } y\}$$

2 El concepte de *cos real-tancat* és definit a la pàgina 20.

és un conjunt d'eliminació per a la teoria dels cossos que satisfan que tot polinomi (no constant) de grau senar té una arrel al cos i, per tant, per a la teoria del cos dels nombres reals.

Així doncs, dins d'aquesta classe (la dels cossos que satisfan que tot polinomi no constant de grau senar té una arrel al cos) hem de determinar els cossos per als quals una sentència $\phi \in \Phi$ és certa si i només si ho és en $\mathbb{R}$.

Observem que cap de les fórmules de la família

$$\{\exists x_1 \dots \exists x_n \, (-1 = x_1^2 + \cdots + x_n^2) \mid n \in \mathbb{N}\}$$

és certa en $\mathbb{R}$ i per tant tampoc ho és en un cos elementalment equivalent a $\mathbb{R}$.

El fet que el nombre -1 no es pugui expressar com a suma de quadrats en un cos és suficient per a determinar una ordenació del cos, i el converteix en un cos ordenat (el recíproc també és cert, en un cos ordenat el -1 no es pot expressar com a suma de quadrats). Per tant, tot cos elementalment equivalent a $\mathbb{R}$ admet una estructura de cos ordenat. A més a més, com a conseqüència obtenim que la característica d'un cos elementalment equivalent a $\mathbb{R}$ és 0, ja que en un cos de característica p el -1 és suma d'uns.

Enriquim el llenguatge dels anells, i obtenim el llenguatge dels anells ordenats $\mathcal{L}_O = \mathcal{L}_A \cup \{<\}$, on $<$ és un nou símbol relació, binari, i considerem el cos dels nombres reals amb les interpretacions naturals com una estructura d'aquest llenguatge. Aleshores, com que la fórmula $\forall a \, \exists b \, (b^2 = a \vee b^2 = -a)$ és certa en $\mathbb{R}$, cada fórmula $\exists y \, (y^2 = t(X))$ del conjunt d'eliminació Φ és equivalent a la fórmula $t(X) \geq 0$ i, en particular, és equivalent a una fórmula sense quantificadors (en el llenguatge de cossos ordenats!).

Així doncs, la teoria del cos dels nombres reals no té eliminació de quantificadors en el llenguatge d'anells, però la teoria del cos *ordenat* dels nombres reals sí que té eliminació de quantificadors en el llenguatge de cossos ordenats. De fet, Macintyre, McKenna i Van den Dries [36] varen demostrar que l'única teoria d'un cos ordenat (en el llenguatge d'anells ordenats) que admet eliminació de quantificadors és la teoria del cos dels nombres reals.

En general, quan enriquim un llenguatge (incrementant el nombre de funcions, relacions o constants) podem augmentar la complexitat dels conjunts definibles així com la del conjunt de propietats de primer ordre (propietats que es poden definir mitjançant fórmules). Però en aquest cas la relació d'ordre $<$ es pot definir dins la teoria del cos dels nombres reals en el llenguatge d'anells: $x \leq y$ si i només si $\exists z \, (x + z^2 = y)$. Per tant, les teories del cos dels nombres reals com a anell i com a anell ordenat (i els conjunts definibles en les dues estructures) són «equivalents», *i. e.*, per a tota sentència (resp. fórmula) ϕ del llenguatge d'anells ordenats existeix una sentència (resp. fórmula) ϕ' del llenguatge d'anells tal que ϕ és certa en $(\mathbb{R}, +, -, \cdot, 0, 1, <)$ si i només si ϕ' és certa en $(\mathbb{R}, +, -, \cdot, 0, 1)$ (resp. els conjunts definits per ϕ i per ϕ' coincideixen).

Aquest exemple ens mostra que l'«eliminació de quantificadors» és molt sensible al llenguatge de les classes d'estructures que considerem. També cal remarcar que hom ha de ser prudent enriquint el llenguatge. En el cas del cos dels nombres reals, com acabem de comentar, la relació d'ordre que afegim al

llenguatge no varia els conjunts definibles ni les propietats elementals. En general, però, hi ha un truc model-teorètic que mostra com donada una estructura podem enriquir suficientment un llenguatge perquè la teoria d'aquesta estructura tingui eliminació de quantificadors (en aquest nou llenguatge enriquit). L'únic que estem fent amb aquest truc és transferir la dificultat d'una fórmula al conjunt de fórmules sense quantificadors. És a dir, el fet que l'eliminació de quantificadors ens permeti reduir l'estudi de la teoria a l'estudi de les fórmules sense quantificadors en el nou llenguatge enriquit, no ens ajuda gens ja que en aquest nou llenguatge les fórmules sense quantificadors són tan complicades com ho eren les fórmules generals en el llenguatge original. Per tant, l'objectiu és enriquir el llenguatge perquè, per una banda, la teoria tingui eliminació de quantificadors, però, per l'altra, continuem tenint control de les fórmules sense quantificadors.

Si revisem les propietats del cos dels nombres reals que hem utilitzat per a poder definir la relació d'ordre i derivar l'eliminació de quantificadors, obtenim que una $\mathcal{L}_A$-estructura F és elementalment equivalent al cos dels nombres reals si i només si F és un cos que satisfà les propietats següents:

- -1 no es pot expressar com a suma de quadrats d'elements del cos (o, equivalentment, F és un cos ordenat),
- $\forall a\, \exists b\, (b^2 = a \vee b^2 = -a)$ (o, equivalentment, existeix l'arrel quadrada de tot nombre positiu),
- i tot polinomi (no constant) de grau senar té una arrel al cos.

Els cossos que satisfan aquests axiomes s'anomenen *cossos real-tancats*.

Com a conseqüència de l'eliminació de quantificadors en el llenguatge d'anells ordenats, obtenim que la teoria dels nombres reals és model-completa i decidible i que els conjunts definibles són exactament els semialgebraics, *i. e.*, combinacions booleanes de conjunts de la forma $\{(x_1, \ldots, x_n) \mid p(x_1, \ldots, x_n) > 0\}$ on $p(x_1, \ldots, x_n) \in \mathbb{R}[X_1, \ldots, X_n]$. Aquests primers resultats varen marcar el començament d'una branca anomenada *geometria algebraica real*.

Abraham Robinson va utilitzar la model-completesa de la teoria dels cossos real-tancats per a donar una demostració més conceptual del 17è problema de Hilbert sobre formes definides, demostrat originalment per Artin. Una altra de les aplicacions típiques de la model-completesa és la demostració de la versió real del *Nullstellensatz*.

En contrast amb l'estabilitat de la teoria dels nombres complexos, la teoria dels nombres reals no és estable! Així doncs, és d'esperar que hi hagi una gran diversitat de cossos real-tancats. Per exemple, dins la classe de cossos elementalment equivalents a $\mathbb{R}$ hi trobem el cos dels nombres algebraics reals, el cos dels nombres computables, el cos dels nombres superreals o el cos dels nombres hiperreals. Entre altres coses podem deduir que la propietat de ser un cos arquimedià no és un invariant de primer ordre ja que els nombres reals són un cos arquimedià però, per exemple, el cos dels nombres hiperreals no ho és.

Estudis similars del cos dels nombres p-àdics varen ser duts a terme per Ax i Kochen [3, 4, 5] i, independentment, per Ershov [16, 17, 18]. En particular, varen demostrar que la teoria de cada cos de nombres p-àdics és decidible i model-completa (en el llenguatge de cossos amb valoracions). A més a més, varen determinar les classes d'equivalència dels cossos de nombres p-àdics. Aquesta àrea va guanyar rellevància quan Ax-Kochen-Ershov varen utitlitzar la teoria de models dels cossos de nombres p-àdics per a resoldre un problema d'Artin sobre solucions d'equacions sobre els p-àdics. Macintyre va presentar el 1976 una perspectiva diferent per a estudiar aquests cossos. Ell va demostrar que enriquint el llenguatge d'anells amb relacions P_n que determinen el conjunt d'elements no nuls del cos de la forma a^n, la teoria dels nombres p-àdics té eliminació de quantificadors. Denef [15] va utilitzar aquests resultats per a demostrar la racionalitat de diverses sèries de Poincaré provinents de conjunts algebraics sobre els p-àdics resolent una qüestió de Serre i Oesterlé.

Nombres racionals i nombres enters

Com hem comentat a la introducció, el 1920 Hilbert va proposar el projecte conegut com a *programa de Hilbert* amb l'objectiu de formular de manera sòlida i completa els fonaments de les matemàtiques. L'objectiu era basar totes les teories matemàtiques existents en un sistema finit i complet d'axiomes i demostrar-ne la consistència. En el cas particular de la teoria aritmètica, el problema havia estat ja explícitament formulat per Hilbert al segon problema de la seva llista de 1900.

Però el 1931, els sorprenents teoremes d'incompletesa de Gödel varen evidenciar que l'ambiciós pla de Hilbert era impossible de dur a terme, com a mínim de la manera en què s'havia formulat. En el primer teorema, Gödel va demostrar que la teoria de l'aritmètica no és completa: existeix una sentència en el llenguatge d'anells que és certa en els nombres naturals però que no es pot deduir des dels axiomes de l'aritmètica de Peano (és «indemostrable»). De fet, cap extensió de l'aritmètica de Peano recursiva i consistent (és a dir, cap teoria consistent generada per un conjunt d'axiomes efectivament recognoscibles i que interpreti l'aritmètica) pot ser completa: podem trobar una sentència ϕ tal que ni ϕ ni la seva negació $\neg\phi$ poden ser demostrades en la teoria. El primer teorema d'incompletesa no tracta directament la consistència de la teoria de l'aritmètica. Gödel va refinar el resultat en el segon teorema, en què va demostrar que cap d'aquestes teories (extensions de l'aritmètica de Peano recursives i consistents) pot demostrar la seva pròpia consistència. Una de les conseqüències importants dels teoremes de Gödel és la indecidibilitat de la teoria elemental dels nombres enters. Per al lector interessat en els teoremes d'incompletesa, recomanem l'interessant article de Bernard R. Hodgson publicat en aquest BUTLLETÍ [25].

Per la necessitat d'entendre els resultats de Gödel i com a resultat del debat que s'instaurà, es varen desenvolupar diverses branques de la lògica matemàtica com la teoria de la recursió, la teoria de la demostració i la teoria

de la computació. Aquestes línies d'investigació es poden interpretar com a continuacions naturals del programa original de Hilbert.

Com que la teoria de l'aritmètica és molt complexa i, en particular, indecidible, hom pot interessar-se per fragments més senzills d'aquesta teoria. Com ja hem comentat anteriorment, el problema de la compatibilitat d'un sistema d'equacions amb coeficients i solucions enteres es pot interpretar com el problema de la decidibilitat del conjunt de fórmules positives existencials. Aquest problema es coneix com el 10è problema de Hilbert. De fet, Hilbert no va preguntar si el problema era decidible o no, ja que en aquell moment no es concebia que un problema «no es pogués resoldre». Senzillament demanava: «idear un procés que en un nombre finit d'operacions determini, donada una equació diofàntica en un nombre arbitrari de variables, si l'equació té o no solucions enteres». Hem de tenir en compte que un gran nombre de problemes matemàtics, especialment de teoria de nombres, es redueixen a l'estudi d'equacions diofàntiques i que una solució positiva del 10è problema de Hilbert tindria conseqüències impressionants. Per exemple, resoldria a la vegada: l'últim teorema de Fermat (resolt recentment per Wiles), la conjectura de Goldbach (encara un problema obert), la hipòtesi de Riemann (encara un problema obert), la conjectura dels quatre colors (resolta per Appel, Haken i Koch), etc.; per a veure com aquests problemes es poden reduir a un problema d'equacions diofàntiques podeu consultar l'interessant article de Matiyasevich [43].

Encara que moltes d'aquestes reduccions no es coneixien en aquella època, Emil Post ja va declarar el 1944 que el 10è problema de Hilbert «suplicava una demostració d'indecidibilitat». No va ser fins al 1970 que Matiyasevich va demostrar, basant-se en resultats de Julia Robinson, Martin Davis i Hilary Putnam, que en efecte el problema diofàntic és indecidible. La idea és que el conjunt d'aturada d'una màquina de Turing és definible en la teoria existencial positiva de l'aritmètica, i aquest és un dels exemples principals de problema indecidible. Notem que la indecidibilitat del problema diofàntic no implica pas que existeixin equacions diofàntiques per a les quals no puguem decidir si tenen solucions enteres o no! El problema demanava un algoritme «únic i universal» per a resoldre qualsevol equació diofàntica. De fet, en teoria de nombres des de Diofant s'ha demostrat l'existència i la inexistència de solucions de moltes equacions diofàntiques, però per a famílies d'equacions diferents s'han necessitat mètodes diferents i tècniques diferents .

Molta gent es pregunta per què Hilbert va enunciar el 10è problema només per a l'anell dels nombres enters i no per al dels nombres racionals. En l'article [43], Matiyasevich dóna una resposta convincent: Hilbert era un optimista i creia que el problema diofàntic era decidible. Com que el problema de compatibilitat d'equacions en coeficients i solucions racionals es pot reduir al problema diofàntic, una solució positiva d'aquest problema també resoldria el problema en el cas dels nombres racionals. Però la solució en el cas diofàntic ha estat negativa, així doncs què podem dir del problema de compatibilitat d'equacions en l'anell dels nombres racionals? Absolutament res, és un problema obert important dins d'aquesta àrea.

El que sí que es coneix és que la teoria elemental de l'anell dels nombres racionals és indecidible. Julia Robinson, en un resultat remarcable, va mostrar una fórmula explícita que defineix l'anell dels nombres enters dins l'anell dels nombres racionals. Per tant, la indecidibilitat de la teoria de l'aritmètica implica la indecidibilitat de la teoria dels nombres racionals.

Així doncs, en el lleguatge d'anells podem contrastar el comportament exemplar de la teoria elemental dels nombres complexos i la bona estructura dels models d'aquesta teoria (la teoria és decidible, té eliminació de quantificadors, és estable i categòrica); amb el bon comportament de la teoria dels nombres reals a pesar de la complexitat dels models d'aquesta teoria (la teoria és decidible, model-completa però inestable); amb la inaccessibilitat de la teoria dels nombres racionals i dels nombres enters, i l'extrema complexitat dels models d'aquestes teories (les teories són indecidibles i inestables).

4 Grups

En la secció anterior hem vist que l'estudi model-teorètic dels anells varia des del bon comportament dels nombres complexos fins al comportament difícil dels nombres enters. En aquesta secció ens centrarem en el món dels grups.

Grups finits

Primer de tot, cal que observem que els grups finits es poden determinar completament mitjançant una fórmula en el llenguatge de grups. En efecte, donat un grup finit G d'ordre n, podem expressar mitjançant una fórmula que existeixen n elements diferents, tals que qualsevol altre element del grup és un dels anteriors i podem descriure la seva taula de multiplicació; per tant, un grup finit satisfà aquesta fórmula si i només si és isomorf a G, és a dir, les classes d'equivalència elemental coincideixen amb les d'isomorfia.

Cal remarcar que aquest fet, la coincidència de les classes d'equivalència elemental i d'isomorfia, és cert per a qualsevol estructura finita (cossos finits, anells finits, etc.) d'un llenguatge finit.

Grups abelians

En la seva tesi doctoral *Arithmetical properties of Abelian groups* [66], Wanda Szmielew, estudiant d'en Tarski, va dur a terme un estudi sistemàtic dels grups abelians.

És habitual utilitzar la notació additiva per al llenguatge de grups per a estudiar els grups abelians; és a dir, considerem el llenguatge $\mathcal{L}_G = \{+, -, 0\}$ on $+$ és un símbol funció binari, $-$ és un símbol funció unari i 0 és un símbol constant.

Donat un grup abelià sense torsió A, definim

$$\alpha_p(A) = \begin{cases} \dim {}^{A}\!/_{pA}, & \text{si és finita;} \\ \infty, & \text{altrament.} \end{cases}$$

La *característica de Szmielew* associada a un grup abelià sense torsió A és la successió

$$\chi(A) = \langle \alpha_p(A) \mid p \text{ nombre primer} \rangle.$$

Un dels resultats principals de la tesi de Szmielew va ser el següent.

Teorema 13 (Szmielew [66]).

- *Una $\mathcal{L}_G$ estructura G és elementalment equivalent a un grup abelià sense torsió A si i només si G és un grup abelià sense torsió i $\chi(A) = \chi(G)$.*
- *La teoria d'un grup abelià sense torsió és decidible.*

Corol·lari 14.

- *Si A és un grup abelià sense torsió i D és un grup divisible sense torsió, llavors A i $A \oplus D$ són elementalment equivalents.*
- *Tots els grups abelians divisibles sense torsió són elementalment equivalents entre si.*
- *Dos grups abelians finitament generats sense torsió són elementalment equivalents si i només si són isomorfs,* i. e., $\mathbb{Z}^k \equiv \mathbb{Z}^m \Leftrightarrow n = m$.

De fet, Szmielew va introduir uns invariants més generals per classificar tots els grups abelians (amb torsió i sense), però per simplicitat aquí només hem enunciat el cas sense torsió.

L'esperit de la demostració d'aquest teorema és semblant a la demostració que Tarski va presentar per al cas dels nombres reals. Szmielew va demostrar que el conjunt {fórmules atòmiques} $\cup$ {p divideix $t(X)$} és un conjunt d'eliminació de quantificadors, on p és un nombre primer i $t(X)$ és un terme del llenguatge. Si enriquim el llenguatge de grups amb la família infinita de relacions unàries «p divideix un nombre», obtenim que la teoria d'un grup abelià sense torsió té eliminació de quantificadors. Cal observar que per a cada p fix, la relació unària «p divideix un nombre» es pot definir en el llenguatge de grups: p divideix x si i només si $\exists y$ tal que $x = \underbrace{y + \cdots + y}_{p \text{ vegades}}$. Per tant, les teories en els dos llenguatges són equivalents. Un altre cop, de l'eliminació de quantificadors de la teoria dels grups abelians en el llenguatge enriquit obtenim la model-completesa i la decidibilitat de la teoria així com l'estructura dels conjunts definibles.

Aquest elegant resultat va ser el primer a evidenciar que les classes elementals poden ser de vegades més naturals que les d'isomorfia. El teorema fonamental dels grups abelians afirma que tot grup abelià finitament generat està completament determinat pel subgrup de torsió i el rang del sumand lliure. Així com els grups abelians finitament generats tenen un comportament molt estructurat, els grups abelians infinitament generats són una font de fenòmens extravagants. Hi ha grups abelians que no es poden expressar com a suma directa de subgrups; d'altres que són, simultàniament, suma directa de dos

grups abelians indescomponibles i suma directa de n grups abelians indescomponibles, etc. Aquests comportaments fan que la classificació dels grups abelians mòdul isomorfia sigui pràcticament impossible.

Per contra, la classificació elemental a través dels invariants de Szmielew és extremament algebraica i natural. A més a més, si restringim el problema de classificació elemental a la classe de grups abelians finitament generats obtenim que dos grups abelians finitament generats són elementalment equivalents si i només si són isomorfs. Per tant, podem veure la classificació elemental com una extensió natural del teorema fonamental dels grups abelians.

Moltes altres propietats de la teoria dels grups abelians han estat determinades. Rogers [59] i Macintyre [35] varen donar una classificació dels grups abelians que tenen teories superestables i totalment transcendentals en termes dels invariants de Szmielew. En particular, les teories dels grups abelians lliures finitament generats sense torsió són (super)estables però no totalment transcendentals.

Grups nilpotents

La classe de grups que es considera més propera a la classe dels grups abelians és la formada pels grups «gairebé abelians», formalment anomenats *grups nilpotents*. La classe dels grups nilpotents conté la classe dels grups abelians i apareix de manera natural a la teoria de Galois i a la teoria d'àlgebres de Lie, entre d'altres.

Recordem que la *sèrie central descendent* d'un grup G és la sèrie descendent de subgrups:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n \trianglerighteq \cdots$$

on $G_{n+1} = [G_n, G]$ és el subgrup de G generat per tots els commutadors $[x, y] = x^{-1}y^{-1}xy$, $x \in G_n$, $y \in G$.

Un grup s'anomena *nilpotent* si la sèrie central descendent acaba en el subgrup trivial en un nombre finit de passos; és a dir, existeix un nombre natural n tal que en la sèrie central descendent tenim que $G_n = 1$. Si un grup és nilpotent el nombre n s'anomena *classe de nilpotència*.

En contrast amb la decidibilitat de la teoria dels grups abelians, Mal'cev va demostrar que la teoria del grup de matrius unitriangulars $UT_3(\mathbb{Z})$ (*i. e.*, la teoria del grup lliure nilpotent de rang 2 i classe de nilpotència 2) és indecidible [40]. Un altre cop, la idea principal és que existeix una fórmula que defineix l'*anell* dels enters dins el grup $UT_3(\mathbb{Z})$. Ershov va demostrar que $UT_3(\mathbb{Z})$ també es pot definir mitjançant una fórmula de primer ordre en tot grup nilpotent finitament generat que no sigui virtualment abelià[3] [19]. Els resultats de Mal'cev i Ershov impliquen directament la indecidibilitat de la teoria de tot grup nilpotent finitament generat (no virtualment abelià).

En el cas dels grups nilpotents, no tan sols la teoria elemental és indecidible, sinó que també ho és el problema de compatibilitat d'equacions. El 1977,

3 Diem que un grup és *virtualment abelià* si conté un subgrup abelià d'índex finit.

Roman'kov va demostrar que existeix un grup nilpotent tal que el problema de compatibilitat d'equacions en aquest grup és indecidible [60]. El 1984, Repin va refinar aquest resultat i va demostrar que la teoria d'un grup lliure nilpotent és indecidible si la classe de nilpotència és prou gran [57].

La decidibilitat de la teoria existencial del grup lliure nilpotent de classe 2 és un problema molt profund; de fet, Roman'kov va demostrar que és equivalent a la decidibilitat del problema de la compatibilitat de la teoria dels nombres racionals, que, com ja hem comentat, és un dels problemes oberts importants de l'àrea [61].

Així doncs, hem vist que en classes de grups que són pròximes, com la classe de grups abelians i la de grups nilpotents, els problemes poden tenir solucions completament oposades.

Però tot i que les teories de (la majoria) dels grups nilpotents són indecidibles, hi ha alguns resultats positius en la classificació elemental. Com hem dit, la classificació elemental dels grups abelians finitament generats coincideix amb la classificació mòdul isomorfia. Kargapolov va conjecturar el mateix fenomen en la classe de grups nilpotents: dos grups nilpotents finitament generats són elementalment equivalents si i només si són isomorfs. Zil'ber va donar un contraexemple a la conjectura de Kargapolov [70]. Finalment, Oger va demostrar que la conjectura de Kargapolov és «gairebé certa»: dos grups finitament generats nilpotents G i H són elementalment equivalents si i només si $G \times \mathbb{Z} \simeq H \times \mathbb{Z}$; vegeu [51].

Fora del món finitament generat només es tenen resultats parcials per a les classes de grups R-nilpotents —complecions de Hall de grups nilpotents amb anell R [7, 49]. Fora d'aquestes classes, el problema de classificació és obert.

Part II: Els problemes de Tarski

Tots els resultats de grups i anells que hem revisat fins ara són resultats clàssics de l'àrea i, en certa manera, les tècniques utilitzades en les demostracions entren dins del que avui en dia podem classificar com a estàndards. El problema de classificació dels grups lliures va ser proposat per Tarski l'any 1945 i va ser resolt l'any 2006 per Kharlampovich i Myasnikov [28] i, independentment, per Sela [63]. Durant tots aquests anys, l'estudi dels problemes de Tarski ha impulsat i propiciat el desenvolupament de tècniques que avui en dia s'han convertit en crucials en la teoria geomètrica de grups.

Recordem que un grup lliure F de rang k és l'objecte lliure de la categoria de grups corresponent al conjunt $\{a_1, \ldots, a_k\}$. Des d'un punt de vista més combinatori, els elements del grup F estan en correspondència bijectiva amb el conjunt de paraules en l'alfabet $a_1^{\pm 1}, \ldots, a_k^{\pm 1}$ que no contenen subparaules del tipus $a_i a_i^{-1}$ o $a_i^{-1} a_i$, $i = 1, \ldots, k$. Els elements a_i s'anomenen *generadors del grup lliure* F i, de vegades, per remarcar aquest fet escrivim $F(a_1, \ldots, a_k)$.

El primer gran pas: el procés de Makanin-Razborov i la decidibilitat de les teories universal i positiva dels grups lliures

L'estudi de la teoria elemental dels grups lliures va començar amb l'estudi d'equacions. Una equació amb coeficients en el grup lliure $F(a_1, \dots, a_k)$ és una expressió del tipus $w = 1$, on w és un element del grup lliure amb generadors $a_1, \dots, a_k, x_1, \dots, x_n$ per a un cert nombre natural n. Considerem el grup F com el grup de coeficients de les equacions i els elements x_j, $j = 1, \dots, n$ com a variables. Seguint aquesta filosofia, denotem aquest grup lliure per $F[x_1, \dots, x_n]$. Per exemple,

$$[x, y][z, t][a_3, a_4]^{-1}[a_1, a_2]^{-1} = 1 \tag{1}$$

és una equació amb coeficients a_1, a_2, a_3, a_4 i variables x, y, z, t.

Una solució d'una equació en variables $x_1, \dots, x_n$ és una ènupla d'elements $(f_1, \dots, f_n) \in F^n$ tal que després de substituir x_j per f_j en l'expressió w obtenim un paraula que representa l'element trivial en el grup F. Més formalment, una solució és un homomorfisme $\theta\colon F[x_1, \dots, x_n] \to F$ tal que $\theta(a_i) = a_i$ per a tot $i = 1, \dots, k$ i $w \in \operatorname{Ker}\theta$.

Observem que tota solució θ indueix un homomorfisme

$$\theta'\colon {}^{F[x_1, \dots, x_n]}\!/_{\operatorname{ncl}(w)} \to F$$

on $\operatorname{ncl}(w)$ és la clausura normal del subgrup generat per l'element $w \in F[x_1, \dots, x_n]$. Abusant de la notació, sovint denotem θ' per θ. (Més endavant formalitzarem tots aquests conceptes i els posarem en el context de la teoria de models però, de moment, permeteu-nos continuar informalment.)

Continuant amb l'exemple anterior, l'ènupla (a_1, a_2, a_3, a_4) és una solució de l'equació (1) així com també ho és l'homomorfisme induït per

$$x \mapsto a_1,\ y \mapsto a_1 a_2,\ z \mapsto a_3 a_4 a_3,\ t \mapsto a_3 a_4$$

(es comprova mitjançant càlcul directe i recordant que $[x, y] = x^{-1}y^{-1}xy$).

Unes de les primeres equacions que van estudiar-se varen ser les equacions en una variable. A [32], Roger Lyndon va resoldre el problema de compatibilitat i va donar una descripció del conjunt de solucions d'una equació en una variable (amb coeficients en un grup lliure). Lyndon va demostrar que el conjunt de solucions d'una equació en una variable es pot descriure mitjançant un sistema finit de «paraules paramètriques» (una espècie de versió no commutativa de la descripció de solucions d'un sistema lineal d'equacions). Aquestes paraules paramètriques eren complicades i el nombre de paràmetres era dependent del tipus d'equació. K. I. Appel [2] i A. A. Lorents [30, 31] varen continuar l'estudi i varen donar una forma exacta de les paraules paramètriques independentment del tipus d'equació (en una variable).

Aquesta descripció paramètrica de les solucions d'una equació en una variable va donar peu a la conjectura que el conjunt de solucions de sistemes arbitraris d'equacions en un grup lliure es podia descriure utilitzant un nombre

finit de paraules paramètriques. El 1968 Appel [2] va demostrar que hi ha equacions en tres variables tals que el seu conjunt de solucions no pot ser parametritzat, va posar així una limitació al mètode de Lyndon.

En un intent de generalitzar els resultats obtinguts per a les equacions en una variable, Hmelevski va suggerir un mètode més general que involucrava funcions paramètriques i va resoldre tant el problema de compatibilitat com el de descripció del conjunt de solucions de certes equacions en *dues* variables. Ozhigov va continuar en aquestes línies i a [53] va aconseguir generalitzar el mètode per a resoldre el problema de compatibilitat i la descripció de solucions d'un sistema arbitrari d'equacions en dues variables.

Però, un altre cop, el mètode era insuficient. En l'article [55], A. A. Razborov va demostrar que hi ha equacions tals que el seu conjunt de solucions no es pot representar per una superposició d'un nombre finit de funcions paramètriques. Tots els intents d'estudiar les equacions en tres variables des d'aquest punt de vista no varen tenir èxit.

Tornant als anys seixanta, l'altre tipus d'equacions que va ser estudiat va ser la classe d'equacions quadràtiques (equacions on totes les variables apareixen en la forma x o x^{-1} un màxim de dos cops) en connexió amb els grups fonamentals de superfícies i els seus automorfismes.

La primera equació que va ser estudiada va ser l'equació commutador: $[x, y] = [a_1, a_2]$; vegeu [50]. Mal'cev va donar una descripció del conjunt de solucions de l'equació commutador en termes d'automorfismes i solucions minimals [41]. Com ja hem comentat, si

$$G = F[x, y]/\mathrm{ncl}([x, y] = [a_1, a_2]),$$

llavors les solucions de l'equació són homomorfismes

$$\theta\colon G \to F.$$

És fàcil de veure que, per a tot automorfisme α del grup G (que fixa el grup de constants F) i per a tota solució θ, la composició $\alpha \circ \theta$ és també una solució de l'equació $[x, y] = [a_1, a_2]$. Mal'cev va demostrar que, de fet, existeix un nombre finit de solucions «minimals» que precompostes amb automorfismes «generen» tot el conjunt de solucions. Més concretament, va demostrar que existeix un nombre finit de solucions $\theta_1, \ldots, \theta_m$ tal que per a tota solució θ de l'equació existeix un automorfisme α del grup G de manera que $\theta = \alpha \circ \theta_i$ per a algun $i = 1, \ldots, m$. És a dir, Mal'cev va donar una «parametrització» del conjunt de solucions en termes d'un conjunt finit de solucions minimals i utilitzant automorfismes com a paràmetres. El grup G és el grup fonamental del tor (superfície compacta de gènere 1) i, des d'aquesta perspectiva, la descripció de solucions de l'equació $[x, y] = [a_1, a_2]$ es redueix a la ben coneguda descripció dels automorfismes del (grup fonamental del) tor.

Les idees de Mal'cev varen ser desenvolupades per Comerford i Edmunds, a [12], i per R. I. Grigorchuk i P. F. Kurchanov, a [21], i van donar lloc a un mètode general per a descriure el conjunt de solucions d'equacions quadràtiques. La

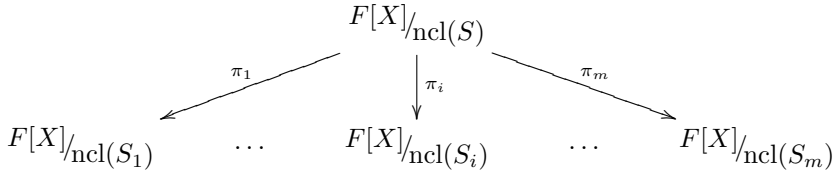
descripció de solucions també va ser donada de manera independent i des d'una perspectiva geomètrica per M. Culler [13] i A. Yu. Ol'shanskiĭ [52].

Tots els mètodes utilitzats per a estudiar aquests casos particulars d'equacions no semblava que es poguessin generalitzar per a sistemes arbitraris d'equacions. Després d'uns quants anys d'estancament, varen començar a aparèixer dubtes sobre la decidibilitat del problema de compatibilitat d'equacions sobre els grups lliures. De fet, seguint un suggeriment de Markov, Matiyasevich va intentar aproximar la indecidibilitat de la teoria de l'aritmètica via la indecidibilitat d'equacions sobre els monoides lliures.

Al final dels anys setanta, en un treball original i sorprenent, Makanin va presentar un algoritme que resolia la compatibilitat de qualsevol sistema d'equacions sobre els monoides lliures i cinc anys després, sobre els grups lliures [37, 38]. Retornant al punt de vista lògic, una de les principals conseqüències del treball de Makanin va ser la decidibilitat de la teoria universal dels grups lliures [39]. A [44], Merzlyakov va demostrar que la teoria positiva dels grups lliures admet eliminació de quantificadors i, per tant, la decidibilitat de la teoria positiva es redueix al problema de compatibilitat d'equacions. Combinant, doncs, els resultats de Makanin i de Merzlyakov s'obté la decidibilitat de la teoria positiva dels grups lliures [39].

En la seva tesi doctoral [56], Razborov va desenvolupar l'algoritme de Makanin per donar una descripció efectiva del conjunt de solucions de qualsevol sistema d'equacions sobre un grup lliure en termes del que es coneix avui en dia com els *diagrames de Makanin-Razborov*.

En general, la descripció de solucions d'equacions quadràtiques no s'estén a sistemes arbitraris d'equacions: no sempre existeix un nombre finit de solucions que precompostes amb automorfismes descriguin totes les solucions. Però Razborov va demostrar que, donat un sistema d'equacions S, o bé el sistema és «constant» (les equacions són de la forma $x_j = a_i$ on no necessàriament totes les variables apareixen en el sistema d'equacions) o bé podem construir efectivament un nombre finit de quocients propis

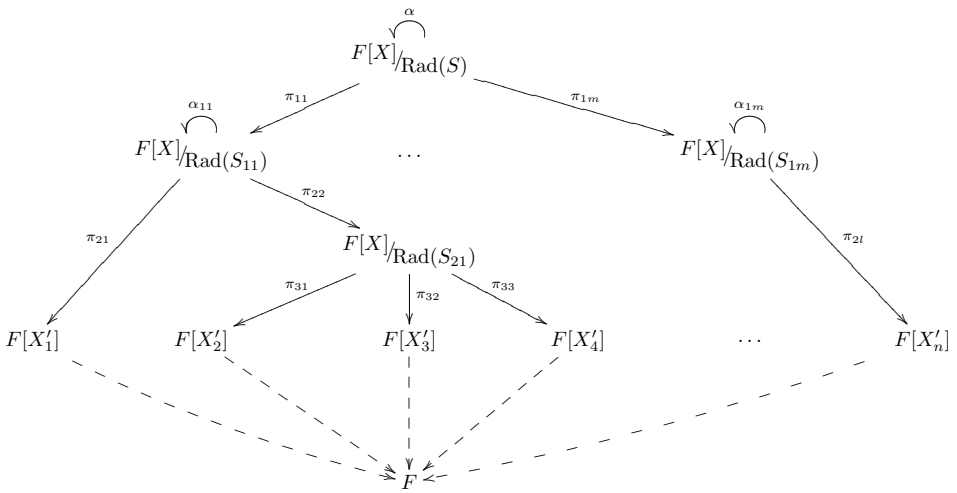


de manera que tota solució del sistema d'equacions S és la composició d'un automorfisme del grup $F[X]/\mathrm{ncl}(S)$, un dels epimorfismes π_i i una solució del sistema d'equacions S_i, per a cert $i \in \{1, \ldots, m\}$. Si repetim el procés per a cadascun dels sistemes d'equacions S_i, $i = 1, \ldots, m$, i successivament per a tots els seus quocients, obtenim un diagrama (en principi potser infinit) que descriu totes les solucions. El 1986, V. S. Guba va demostrar que els grups

lliures es comporten com els anells noetherians i que, en particular, aquest tipus de seqüències d'epimorfismes estabilitzen [22]. El resultat de Guba ens permet concloure que el diagrama que construïm és, de fet, finit.

A més a més, un cop construït el diagrama, el fet que no puguem aplicar el resultat als últims quocients implica que aquests corresponen a sistemes d'equacions constants. Notem que si S' és un sistema d'equacions constant, llavors el grup $F[X]/_{\mathrm{ncl}(S')}$ és isomorf al grup lliure $F[X']$, on $X' \subset X$ és el subconjunt de variables lliures (les variables que no apareixen a les equacions de la forma $x_j = a_i$). Llavors, el conjunt de solucions del sistema S' és el conjunt de (tots) els homomorfismes de $F[X']$ a F.

Per tant, els diagrames de Makanin-Razborov descriuren el conjunt de solucions d'un sistema d'equacions S mitjançant grups (coneguts) d'automorfismes dels quocients que apareixen al diagrama, els corresponents epimorfismes i, finalment, els homomorfismes de grups lliures.



La necessitat d'estructura: geometria algebraica

Una de les conseqüències implícites del procés de Makanin-Razborov va ser l'evidència que les equacions i les varietats algebraiques són objectes naturals d'estudi per a altres estructures a part dels cossos i els anells. Aquesta conscienciació va portar al desenvolupament de la geometria algebraica sobre grups primer [6] i, recentment, al desenvolupament del que avui en dia es coneix com a *geometria algebraica universal* [14]. Totes les nocions clàssiques de la geometria algebraica de varietats tenen la seva anàloga model-teorètica: varietats, ideals, radical, topologia de Zariski, etc. Definirem uns quants conceptes que, per una banda, ens serviran per a la resta de l'exposició i, per l'altra, ens permetran fer-nos una idea del tipus de generalitzacions a les quals ens hem referit.

El primer pas en geometria algebraica és fixar el cos de coeficients K. A partir d'aquí, l'estudi de varietats algebraiques correspon a l'estudi d'àlgebres finitament generades sobre K. Similarment, donat un llenguatge $\mathcal{L}$ (que d'ara endavant suposem funcional per simplicitat), el primer pas és determinar una $\mathcal{L}$-estructura $\mathcal{A}$, que representa el paper de cos de coeficients. L'objectiu, doncs, és estudiar estructures finitament generades «sobre» $\mathcal{A}$ o, en altres paraules, $\mathcal{L}$-estructures que contenen una còpia designada d'$\mathcal{A}$ i són generades per $\mathcal{A}$ i un nombre finit d'elements. Aquestes estructures les anomenarem *$\mathcal{A}$-estructures* i es poden definir des de dos punts de vista equivalents: categòric i axiomàtic. La definició següent correspon al punt de vista categòric.

DEFINICIÓ 15. Una *$\mathcal{A}$-estructura* és un parell $(\mathcal{B}, \lambda)$ on $\mathcal{B}$ és una $\mathcal{L}$-estructura i $\lambda\colon \mathcal{A} \to \mathcal{B}$ és un morfisme injectiu.

Normalment, abusarem del llenguatge i identificarem la còpia $\lambda(\mathcal{A})$ amb $\mathcal{A}$. Des del punt de vista lògic, les $\mathcal{A}$-estructures són estructures del llenguatge enriquit $\mathcal{L}_\mathcal{A} = \mathcal{L} \cup \{c_a \mid a \in \mathcal{A}\}$, on c_a són símbols constants, que satisfan les mateixes sentències atòmiques i les seves negacions que l'estructura $\mathcal{A}$ (*i. e.*, la subestructura d'una $\mathcal{A}$-estructura formada per les interpretacions de les constants c_a és una estructura isomorfa a $\mathcal{A}$).

En aquesta categoria, els *$\mathcal{A}$-morfismes* són morfismes de $\mathcal{L}$-estructures tals que la seva restricció a $\mathcal{A}$ és la identitat. Els nuclis dels $\mathcal{A}$-morfismes són els *ideals*.

DEFINICIÓ 16. Fixat un nombre natural n, denotem per $\mathcal{A}[X]$ el conjunt de termes del llenguatge $\mathcal{L}_\mathcal{A}$ en variables $X = \{x_1, \dots, x_n\}$.

Observem que les constants són termes i que les funcions en termes són, un altre cop, termes. Per tant, sota aquestes interpretacions naturals hom converteix $\mathcal{A}[X]$ en una $\mathcal{L}_\mathcal{A}$-estructura que s'anomena la *$\mathcal{L}_\mathcal{A}$-estructura lliure amb base X*. Tal com indica el nom, $\mathcal{A}[X]$ és un objecte lliure de la categoria d'$\mathcal{A}$-estructures. Com suggerim amb la notació, la $\mathcal{L}_\mathcal{A}$-estructura $\mathcal{A}[X]$ representa el paper de l'àlgebra de polinomis en n variables sobre un cos. Els elements d'$\mathcal{A}[X]$ s'interpreten com els polinomis amb coeficients en $\mathcal{A}$.

Una *equació* amb coeficients en $\mathcal{A}$ i variables X és una expressió del tipus $t(X) = t'(X)$ on $t(X), t'(X) \in \mathcal{A}[X]$ o, equivalentment, és una fórmula atòmica del llenguatge $\mathcal{L}_\mathcal{A}$ amb variables lliures X. Un conjunt (finit o infinit) d'equacions s'anomena *sistema d'equacions*.

Donat un sistema d'equacions $S(X)$ amb variables X una *solució* és una ènupla $\bar{a} = (a_1, \dots, a_n) \in \mathcal{A}^n$ tal que tota fórmula atòmica $s(X) \in S(X)$ avaluada en $\bar{a}$ és certa en $\mathcal{A}$. El conjunt de solucions s'anomena un *conjunt algebraic* i es denota per $V_\mathcal{A}(S)$. Com que $\mathcal{A}[X]$ és un objecte lliure, per a cada ènupla $\bar{a} = (a_1, \dots, a_n) \in V_\mathcal{A}(S)$, la funció $x_i \to a_i$ s'estén a un morfisme $h_{\bar{a}}\colon \mathcal{A}[X] \to \mathcal{A}$. Definim *(l'ideal) radical* $\mathrm{Rad}(S)$ *associat al sistema d'equacions S* com la intersecció de tots els nuclis de (morfismes $h_{\bar{a}}$ induïts per) les solucions

$\bar{a} \in V_{\mathcal{A}}(S)$, *i. e.*,

$$\mathrm{Rad}(S) = \bigcap_{\bar{a} \in V_{\mathcal{A}}(S)} \mathrm{Ker}\, h_{\bar{a}}.$$

Des del punt de vista lògic, el radical es pot caracteritzar com el conjunt de conseqüències del sistema S; és a dir, el radical $\mathrm{Rad}(S)$ coincideix amb el subconjunt de fórmules atòmiques $\{\phi(X) \mid \phi(\bar{a}) \text{ és certa en } \mathcal{A}, \forall \bar{a} \in V_{\mathcal{A}}(S)\}$.

DEFINICIÓ 17. Donat un sistema d'equacions $S(X)$ en variables X sobre $\mathcal{A}$, l'*estructura de coordenades* és l'estructura definida per $\mathcal{A}[X]/\mathrm{Rad}(S)$.

És fàcil demostrar que les interpretacions induïdes de les funcions i les constants de l'àlgebra lliure $\mathcal{A}[X]$ al quocient $\mathcal{A}[X]/\mathrm{Rad}(S)$ estan ben definides; per a tota funció f del llenguatge posem $f^{\mathcal{A}}(\overline{a_1}, \ldots, \overline{a_n}) := \overline{f^{\mathcal{A}}(a_1, \ldots, a_n)}$ on $\overline{a}$ denota la classe d'equivalència de l'element a en el quocient $\mathcal{A}[X]/\mathrm{Rad}(S)$ i interpretem tot símbol constant c per $\overline{c^{\mathcal{A}}}$. Per tant, si el conjunt algebraic $V_{\mathcal{A}}(S)$ no és buit, el quocient $\mathcal{A}[X]/\mathrm{Rad}(S)$ és una $\mathcal{A}$-estructura.

No entrarem en detalls, però com en geometria algebraica clàssica, hom pot definir les categories de conjunts algebraics sobre $\mathcal{A}$ i d'$\mathcal{A}$-estructures de coordenades i demostrar que aquestes dues categories són dualment equivalents.

La *topologia de Zariski en* $\mathcal{A}^n$, $n \geq 1$ és la topologia que té com a prebase de conjunts tancats els conjunts algebraics; és a dir, un conjunt és tancat en aquesta topologia si es pot obtenir a partir d'unions finites i interseccions arbitràries de conjunts algebraics. Un conjunt $Y \subseteq \mathcal{A}^n$ s'anomena *reductible* si es pot expressar com la unió de dos subconjunts propis tancats; altrament, el conjunt Y s'anomena *irreductible*. En particular, un conjunt algebraic és irreductible si i només si no es pot descompondre com una unió finita de conjunts algebraics propis.

Diem que un espai topològic és *noetherià* si tota cadena de conjunts tancats propis estabilitza. Recordem que en una topologia noetheriana, la base de la topologia conté tots els conjunts tancats de la topologia i tot conjunt tancat Y és la unió finita de conjunts tancats irreductibles, les components irreductibles: $Y = Y_1 \cup \cdots \cup Y_m$. A més a més, si $Y_i \not\subseteq Y_j$, $i \neq j$ llavors la descomposició és única (mòdul permutació de les components).

DEFINICIÓ 18. L'estructura $\mathcal{A}$ s'anomena *equacionalment noetheriana* si tot sistema d'equacions S sobre $\mathcal{A}$ és equivalent a un subsistema $S_0 \subset S$ finit, *i. e.*, per a tot sistema d'equacions S existeix un subsistema finit $S_0 \subset S$ tal que $V_{\mathcal{A}}(S) = V_{\mathcal{A}}(S_0)$.

LEMA 19. *Les afirmacions següents són equivalents.*

- *L'estructura $\mathcal{A}$ és equacionalment noetheriana.*
- *La topologia de Zariski en $\mathcal{A}^n$ és noetheriana, per a tot nombre natural n.*
- *Tota cadena d'epimorfismes propis $C_0 \to C_1 \to \cdots$ d'estructures de coordenades sobre $\mathcal{A}$ és finita.*

Per tant, si una estructura és equacionalment noetheriana, l'estudi de conjunts algebraics es redueix a l'estudi dels conjunts algebraics irreductibles, també anomenats *varietats algebraiques*.

Un dels problemes més importants de geometria algebraica és la classificació mòdul isomorfia dels conjunts algebraics sobre $\mathcal{A}$. Utilitzant la dualitat de categories, el problema és equivalent a la classificació mòdul isomorfia de les $\mathcal{A}$-estructures de coordenades. A més a més, com ja hem comentat, si $\mathcal{A}$ és equacionalment noetheriana, és suficient la classificació d'$\mathcal{A}$-estructures de coordenades de les varietats algebraiques sobre $\mathcal{A}$. Veiem, doncs, a continuació, que les $\mathcal{A}$-estructures de coordenades de les varietats algebraiques sobre $\mathcal{A}$ admeten una rica caracterització.

DEFINICIÓ 20. Diem que una $\mathcal{A}$-estructura $\mathcal{B}$ és *$\mathcal{A}$-separada per $\mathcal{A}$* si per a tot parell d'elements $b_1, b_2 \in \mathcal{B}$, $b_1 \neq b_2$ en $\mathcal{B}$ existeix un $\mathcal{A}$-morfisme $\theta\colon \mathcal{B} \to \mathcal{A}$ que els separa, *i. e.*, $\theta(b_1) \neq \theta(b_2)$ en $\mathcal{A}$.

Diem que una $\mathcal{A}$-estructura $\mathcal{B}$ és *$\mathcal{A}$-discriminada per $\mathcal{A}$* si per a tot nombre natural n i per a tot conjunt d'n elements $b_1, \ldots, b_n \in \mathcal{B}$ existeix un $\mathcal{A}$-morfisme $\theta\colon \mathcal{B} \to \mathcal{A}$ injectiu en el conjunt $b_1, \ldots, b_n$, és a dir, $\theta(b_i) \neq \theta(b_j)$ en $\mathcal{A}$ si $b_i \neq b_j$ en $\mathcal{B}$, $i, j = 1, \ldots, n$.

LEMA 21. *Tota $\mathcal{A}$-estructura $\mathcal{B}$ finitament generada és una $\mathcal{A}$-estructura de coordenades d'un conjunt algebraic (no buit) sobre $\mathcal{A}$ si i només si és $\mathcal{A}$-separada per $\mathcal{A}$.*

Tota $\mathcal{A}$-estructura $\mathcal{B}$ finitament generada és una $\mathcal{A}$-estructura de coordenades d'una varietat algebraica (no buida) sobre $\mathcal{A}$ si i només si és $\mathcal{A}$-discriminada per $\mathcal{A}$.

Aquest lema estableix connexions entre geometria algebraica i àlgebra universal. Aquestes interaccions amb àlgebra universal ens proporcionen moltes maneres de caracteritzar les $\mathcal{A}$-estructures de coordenades.

No és difícil de veure que la categoria d'$\mathcal{A}$-estructures $\mathcal{A}$-separades per $\mathcal{A}$ coincideix amb la prevarietat d'$\mathcal{A}$, o, en altres paraules, la categoria d'$\mathcal{A}$-estructures $\mathcal{A}$-separades per $\mathcal{A}$ és la menor classe que conté $\mathcal{A}$ i és tancada per la formació de productes directes i de subestructures. És un resultat bàsic d'àlgebra universal que tota estructura de la prevarietat d'$\mathcal{A}$ pertany a la quasivarietat d'$\mathcal{A}$ (la classe d'estructures que satisfan les mateixes quasiidentitats que $\mathcal{A}$). En general, el recíproc no és cert, però si l'estructura $\mathcal{A}$ és equacionalment noetheriana, llavors les $\mathcal{A}$-estructures finitament generades de la prevarietat i la quasivarietat coincideixen. Utilitzant fets d'àlgebra universal obtenim els teoremes següents.

TEOREMA 22. *Sigui $\mathcal{A}$ una estructura noetheriana del llenguatge $\mathcal{L}_{\mathcal{A}}$. Per a tota $\mathcal{A}$-estructura C finitament generada, les condicions següents són equivalents:*

- *C és una $\mathcal{A}$-estructura de coordenades sobre $\mathcal{A}$;*
- *C és $\mathcal{A}$-separada per $\mathcal{A}$;*

- *les teories de quasiidentitats d'$\mathcal{A}$ i de C coincideixen,* i. e., $\mathrm{Th}_{qi}(\mathcal{A}) = \mathrm{Th}_{qi}(C)$*;*
- *existeix un $\mathcal{A}$-monomorfisme de C a una potència (directa) d'$\mathcal{A}$, i*
- *C és producte subdirecte d'un nombre finit d'$\mathcal{A}$-estructures de coordenades corresponents a varietats algebraiques sobre $\mathcal{A}$.*

TEOREMA 23. *Sigui $\mathcal{A}$ una estructura noetheriana del llenguatge $\mathcal{L}_{\mathcal{A}}$. Per a tota $\mathcal{A}$-estructura C finitament generada, les condicions següents són equivalents:*

- *C és una $\mathcal{A}$-estructura de coordenades d'una varietat algebraica sobre $\mathcal{A}$;*
- *C és $\mathcal{A}$-discriminada per $\mathcal{A}$;*
- *les teories existencials i universals d'$\mathcal{A}$ i de C coincideixen respectivament,* i. e., $\mathrm{Th}_{\exists}(\mathcal{A}) = \mathrm{Th}_{\exists}(C)$ *i* $\mathrm{Th}_{\forall}(\mathcal{A}) = \mathrm{Th}_{\forall}(C)$*;*
- *existeix un $\mathcal{A}$-monomorfisme de C a l'ultrapotència d'$\mathcal{A}$, i*
- *C és una $\mathcal{A}$-estructura límit: és el límit de subestructures d'$\mathcal{A}$.*

Aquestes caracteritzacions ens proporcionen eines per a demostrar propietats algebraiques de les estructures de coordenades. Per exemple, la propietat «ser equacionalment noetherià» es pot descriure mitjançant quasiidentitats: si $\mathcal{A}$ és noetheriana, per a tot sistema S, sigui S_0 un subsistema finit tal que $V_{\mathcal{A}}(S) = V_{\mathcal{A}}(S_0)$. Llavors el conjunt de quasiidentitats

$$\{\forall a_1 \ldots \forall a_n \bigcap_{(s_0 = s_0') \in S_0} s_0(a_1, \ldots, a_n) = s_0'(a_1, \ldots, a_n) \rightarrow \\ \rightarrow s(a_1, \ldots, a_n) = s'(a_1, \ldots, a_n) \mid \forall (s = s') \in S\} \quad (2)$$

pertany a la teoria de quasiidentitats d'$\mathcal{A}$. Com que tota $\mathcal{A}$-estructura de coordenades satisfà les mateixes quasiidentitats que $\mathcal{A}$, obtenim de manera immediata que si $\mathcal{A}$ és equacionalment noetheriana, també ho és tota $\mathcal{A}$-estructura de coordenades. Hi ha moltes condicions que es poden expressar amb quasiidentitats: si una estructura és abeliana, nilpotent, sense torsió, etc., llavors tota estructura de coordenades també ho és; obtenim trivialment que un grup nilpotent o amb torsió no és un grup de coordenades sobre un grup lliure. Un altre exemple en el món dels grups: si G és un grup lineal (*i. e.*, G és isomorf a un subgrup del grup general de matrius $GL_n(R)$, per a un cert nombre natural n i cert anell commutatiu R) també ho és tot G-grup de coordenades d'una varietat algebraica.

Varietats irreductibles i la classe universal dels grups lliures

Retornem al nostre objectiu principal: caracteritzar algebraicament les classes d'equivalència universal (existencial) i elemental dels grups lliures. Com a conseqüència del teorema 23, la classe d'equivalència universal d'un grup lliure F és precisament la classe de grups de coordenades de varietats algebraiques sobre F. L'objectiu d'aquesta secció és determinar l'estructura algebraica d'aquests grups de coordenades.

El resultat de Razborov sobre la descripció de solucions de sistemes d'equacions sobre el grup lliure va ser originalment molt qüestionat. Superficialment, el resultat es llegia com una descripció efectiva del conjunt de solucions, però, vist des d'aquesta perspectiva, hom podria senzillament enumerar els elements del grup lliure i comprovar si són solucions o no, i aquesta descripció també és efectiva.

No va ser fins a finals dels anys noranta amb el llenguatge de geometria algebraica sobre grups que Olga Kharlampovich i Alexei Myasnikov varen tornar a revisar el resultat de Razborov i en varen extreure la vertadera essència: el procés de Makanin-Razborov determina d'una manera efectiva l'estructura algebraica dels grups de coordenades sobre els grups lliures [26].

De fet, el que varen demostrar és que el procés de Makanin-Razborov es pot interpretar com un anàleg no commutatiu dels processos d'eliminació clàssics de la geometria algebraica on les components bàsiques tornen a ser les equacions quadràtiques!

Un sistema finit d'equacions s'anomena *triangular quasiquadràtic* amb coeficients en un grup lliure F si és de la forma

$$\begin{aligned} S_1(X_1, X_2, \ldots, X_n) &= 1, \\ S_2(X_2, \ldots, X_n,) &= 1, \\ \vdots \qquad & \quad \vdots \\ S_n(X_n) &= 1, \end{aligned}$$

on per a cada i el sistema $S_i = 1$ és

- o bé quadràtic en variables X_i,
- o bé un sistema abelià ($[x_i, x_{i'}] = 1$, $[x_i, u] = 1$ per a tot $x_i, x_{i'} \in X_i$ i $u \in {}^{F[X_{i+1}, \ldots, X_n]}\!/_{\mathrm{Rad}(s_{i+1}, \ldots, S_n)}$ no és una potència pròpia, *i. e.*, si $u = v^k$ llavors $k = \pm 1$),
- o bé S_i és buit.

Un sistema quasiquadràtic s'anomena *regular* si per a cada i, o bé $S_i = 1$ és quadràtic regular (qualsevol quadràtic llevat de tres excepcions de gènere petit) o bé S_i és buit.

Un sistema triangular quasiquadràtic s'anomena *no degenerat* i es denota per *NTQ,* si cada sistema $S_i = 1$ té una solució en el grup de coordenades ${F[X_{i+1}, \ldots, X_n]}\!/_{\mathrm{Rad}(S_{i+1}, \ldots, S_n)}$.

Kharlampovich i Myasnikov varen demostrar que utilitzant el procés de Makanin-Razborov podem obtenir la informació següent.

Teorema 24.

- *Donat un sistema d'equacions S sobre un grup lliure fixat, hom pot determinar efectivament les presentacions dels grups de coordenades corresponents a les components irreductibles del conjunt algebraic $V(S)$.*

- *Tot grup de coordenades d'una varietat algebraica és subgrup d'un grup de coordenades corresponent a un sistema NTQ, i el sistema NTQ es pot determinar efectivament.*

Notem que el segon resultat correspon als teoremes d'extensió en la teoria clàssica d'eliminació per a polinomis sobre un cos algebraicament tancat.

Així doncs, el procés de Makanin-Razborov ens permet fer encara una altra reducció en l'estudi de grups de coordenades de varietats algebraiques (o, equivalentment, en l'estudi de grups finitament generats universalment equivalents al grup lliure): és suficient estudiar els grups de coordenades corresponents a sistemes NTQ (i els seus subgrups). Per a entendre la seva estructura algebraica, hem de descriure l'ideal radical d'un sistema d'equacions NTQ; és a dir, necessitem un anàleg del *Nullstellensatz* per als sistemes NTQ.

El gran avantatge dels sistemes NTQ és que es poden construir inductivament a partir de peces senzilles: equacions quadràtiques i abelianes. La idea és determinar el radical dels sistemes d'equacions quadràtiques i abelianes com a cas base i utilitzar inducció per a estudiar els radicals dels sistemes NTQ.

Observem que el radical d'un sistema d'equacions S és el menor ideal radical que conté la clausura normal $\mathrm{ncl}(S)$ de S. En el cas que el grup $F[X]/\mathrm{ncl}(S)$ sigui discriminat per F, obtenim com a conseqüència del teorema 23 que la clausura normal $\mathrm{ncl}(S)$ és un ideal radical i, per tant, coincideix amb el radical del sistema S.

Si el sistema d'equacions S és abelià, llavors el subgrup de $F[X]/\mathrm{ncl}(S)$ generat per les variables és un grup abelià lliure finitament generat i és fàcil demostrar que, en aquest cas, el grup és discriminat pel grup lliure F i, per tant, el radical d'un sistema abelià coincideix amb la seva clausura normal.

Per a estudiar els radicals de les equacions quadràtiques i, més en general, dels sistemes NTQ, hem de retornar (sorprenentment!) al treball de Lyndon. Lyndon, mentre estudiava les equacions en una variable, va introduir el $\mathbb{Z}[t]$-grup $F^{\mathbb{Z}[t]}$ on $F(a_1,\dots,a_k)$ és el grup lliure de rang k [33]. En general, donat un anell R commutatiu amb unitat, un R-grup G és un grup equipat amb una acció de l'anell R:

$$\begin{aligned} R \times G &\longrightarrow G \\ (r, g) &\longmapsto g^r \end{aligned}$$

tal que

- $g^1 = g$, $g^0 = g$, $g^{r+s} = g^r g^s$, $g^{rs} = (g^r)^s$;
- $(h^{-1}gh)^r = h^{-1}g^r h$;
- si g i h commuten, llavors $(gh)^r = g^r h^r$,

per a tot parell $g, h \in G$ i per a tot parell $r, s \in R$. Notem que, en particular, si el grup G és abelià, llavors els R-grups són senzillament mòduls sobre l'anell R. Per tant, podem veure els R-grups com una versió no abeliana dels mòduls. Observem també que tot grup té una estructura natural de $\mathbb{Z}$-grup on l'acció és definida a través de la potenciació.

Un R-homomorfisme θ del R-grup G al R-grup H és un homomorfisme de grups que satisfà $\theta(g^r) = \theta(g)^r$. Donat un anell R, els R-grups (juntament amb els R-homomorfismes) formen una categoria. L'objecte lliure de la categoria de $\mathbb{Z}[t]$-grups per al conjunt $a_1, \ldots, a_k$ és el $\mathbb{Z}[t]$-grup $F^{\mathbb{Z}[t]}$.

Lyndon va demostrar que el grup $F^{\mathbb{Z}[t]}$ és discriminat pel grup F. Com que tot subgrup d'un grup discriminat per F és també discriminat per F, podem concloure que tots els F-subgrups de $F^{\mathbb{Z}[t]}$ finitament generats són grups de coordenades de varietats algebraiques sobre el grup lliure. Myasnikov i Remeslennikov varen estudiar el grup $F^{\mathbb{Z}[t]}$ des d'un punt de vista algebraic i varen conjecturar un recíproc del resultat de Lyndon: tots els grups de coordenades de varietats algebraiques sobre el grup lliure F són subgrups del grup $F^{\mathbb{Z}[t]}$; vegeu [48].

Kharlampovich i Myasnikov varen demostrar que els grups $F[X]/\mathrm{ncl}(S)$, on S és un sistema d'equacions quadràtiques (menys en els tres casos excepcionals), són subgrups del grup de Lyndon $F^{\mathbb{Z}[t]}$ i per tant són grups discriminats per F [27]. En altres paraules, l'ideal radical generat per una equació quadràtica coincideix amb la seva clausura normal.

Utilitzant inducció, també varen demostrar que els grups $F[X]/\mathrm{ncl}(S)$, on S és un sistema d'equacions NTQ (si S_i no són equacions quadràtiques excepcionals), són subgrups del grup de Lyndon $F^{\mathbb{Z}[t]}$.

Per tant, el grup de Lyndon $F^{\mathbb{Z}[t]}$ no tan sols és útil per a determinar els ideals radicals dels sistemes d'equacions NTQ sinó que, en vista del teorema 24, és un univers on trobem tots els grups de la classe de grups finitament generats universalment equivalents al grup lliure.

Resumint, doncs, obtenim el teorema següent que caracteritza algebraicament la classe d'equivalència universal del grup lliure F.

TEOREMA 25. *Donat un F-grup C, les afirmacions següents són equivalents:*

- *C és un grup de coordenades d'una varietat algebraica sobre un grup lliure F;*
- *C és universalment equivalent a F;*
- *C és un F-subgrup finitament generat del grup $F^{\mathbb{Z}[t]}$.*

Aquest resultat i l'estructura algebraica del grup $F^{\mathbb{Z}[t]}$ varen ser utilitzats per a demostrar tant que els grups de coordenades de varietats algebraiques són finitament presentables, com diverses propietats algorítmiques d'aquests grups (la decidibilitat del problema de la paraula, la del de conjugació, la del d'isomorfisme, la del de pertinença, etc.).

Interpretació geomètrica: la maquinària de Rips

En aquesta secció volem deixar constància del mètode que Sela va utilitzar per a l'estudi de grups de coordenades sobre un grup lliure. Tot i que considerem aquesta perspectiva molt interessant (per una banda, fa ús de la maquinària de Rips —una interpretació geomètrica del procés de Makanin-Razborov que ha pres una gran importància per si mateixa tant en l'àrea de teoria geomètrica

de grups com en altres àrees— i, per l'altra banda, ha permès una «fàcil» generalització per a l'estudi de grups de coordenades sobre altres grups, com els grups hiperbòlics, tòrics relativament hiperbòlics, etc.), només en farem unes pinzellades superficials ja que, en si, la teoria és tècnicament exigent. Els lectors que hi estiguin interessats poden consultar l'article expositiu de Bestvina [8].

La geometrització del procés de Makanin-Razborov en el que avui en dia es coneix com la *maquinària de Rips* ha estat un dels resultats més destacats dels últims trenta anys en teoria geomètrica de grups. El 1872, Klein va proposar estudiar geometria a través dels grups que preserven la seva estructura; des d'aquesta perspectiva, la base de la teoria geomètrica de grups es pot interpretar com un invers del programa de Klein: utilitzar la geometria per a l'estudi de grups. Una de les maneres d'establir aquesta connexió entre espais geomètrics i grups és mitjançant accions; és a dir, hom vol entendre la relació entre les propietats geomètriques d'un espai i l'estructura dels grups que hi actuen (grups de simetries, d'isometries, etc.).

En el llibre *Trees* [65], Serre dóna una caracterització elegant dels grups que tenen un acció «bona» en un arbre simplicial en termes de construccions lliures: un grup actua (sense punts fixos ni inversió d'arestes) en un arbre simplicial si i només si el grup es pot presentar com un producte lliure amalgamat o una extensió HNN. De fet, el grup es pot reconstruir completament utilitzant el graf quocient $G \setminus T$ de l'arbre T per l'acció del grup G i els subgrups estabilitzadors dels vèrtexs i les arestes. L'essència de moltes demostracions combinatòries (el teorema d'Ihara: els subgrups discrets sense torsió del grup $SL_2(\mathbb{Q}_p)$ són lliures; el teorema de Nielsen-Schreier: tot subgrup d'un grup lliure és lliure) va quedar sintetitzada en la teoria de Bass-Serre a través d'arguments topològics molt més senzills. Així doncs, el treball de Bass-Serre no és tan sols un resultat sinó que es va convertir en una tècnica.

El concepte que generalitza d'una manera natural la noció d'*arbre simplicial* és la d'*arbre real*. Els arbres reals varen ser introduïts a mitjan anys setanta per I. M. Chiswell i, independentment, per J. Tits, [11, 69]. Des del punt de vista de Chiswell i continuant idees de Lyndon, si els arbres simplicials són espais mètrics on els grups que admeten una funció de llargada en els nombres enters hi actuen, llavors els arbres reals són espais on els grups que admeten una funció de llargada en els nombres reals hi actuen. Tits els va introduir com a generalitzacions dels «edificis» de Bruhat-Tits. Alperin i Moss varen estudiar-los des d'un punt de vista mètric i varen demostrar que són espais geodèsics on existeix un únic arc que uneix cada parell de punts de l'espai, o, en altres paraules, són senzillament espais 0-hiperbòlics (tot triangle és un trípode) [1]. El primer exemple d'arbre real és la recta real $\mathbb{R}$ (amb la mètrica euclidiana). Notem que el pla real $\mathbb{R}^2$ amb la mètrica euclidiana no és un arbre real, ja que donats dos punts del pla, existeixen infinits arcs que els connecten. En canvi, si considerem el pla real amb la mètrica de París (la distància entre els punts x i y és la distància euclidiana si la recta definida per x i y passa per l'origen o, altrament, la suma de les distàncies euclidianes de x a l'origen i de l'origen a y), llavors és un arbre real.

La teoria d'arbres reals es va tornar prominent amb el treball de Morgan i Shalen, els quals varen establir connexions entre la teoria dels arbres reals, la geometria hiperbòlica i la teoria de laminacions mesurades de Thurston [45, 46, 47]. Més concretament, varen demostrar que si G és un grup finitament generat, llavors l'espai de representacions fidels discretes (vist com a classes de conjugació d'isometries de l'espai hiperbòlic que preserven l'orientació) té una compactificació en la qual els punts ideals s'obtenen mitjançant certes accions del grup G en arbres reals. Aquesta compactificació generalitza la de Thurston de l'espai de Teichmüller.

Des de la introducció dels arbres reals, un dels problemes principals de l'àrea va ser determinar l'estructura dels grups que hi actuen, una generalització de la teoria de Bass-Serre. Lyndon va conjecturar que si un grup finitament generat actua lliurement en un arbre real, llavors aquest és un producte lliure de grups abelians lliures finitament generats. Morgan i Shalen (i, amb menys generalitat, Alperin i Moss) varen donar una resposta negativa a la conjectura de Lyndon demostrant que els grups fonamentals de la majoria de superfícies poden actuar lliurement en un arbre real. Així doncs, Morgan i Shalen varen formular una nova conjectura: un grup finitament generat actua lliurement en un arbre real si i només si aquest és un producte lliure de grups abelians i grups de superfícies (llevat dels casos excepcionals).

L'estiu de 1991, en una sèrie de conferències, Rips va exposar un esquema de la demostració de la conjectura de Morgan-Shalen basada en una interpretació geomètrica del procés de Makanin-Razborov: si un grup finitament presentat actua en un arbre real, l'acció indueix una foliació mesurada (en el 2-complex associat a la presentació del grup) que pot ser analitzada pel procés. De la mateixa manera que el procés original presenta una descomposició del grup en peces conegudes —part quadràtica i part abeliana—, en el llenguatge geomètric també en dóna una descomposició —accions en arbres simplicials, accions en la recta real i accions de superfícies.

Inspirats en les idees de Rips i basant-se en resultats d'Imanishi i Levitt, Gaboriau, Levitt i Paulin varen donar una demostració de la conjectura de Morgan-Shalen, coneguda avui en dia com a *teorema de Rips*, utilitzant propietats dinàmiques de conjunts d'isometries (parcials) de la recta real [20]. Independentment, Bestvina i Feighn varen desenvolupar les idees de Rips i varen generalitzar els resultats determinant l'estructura dels grups que actuen d'una manera estable en un arbre real [9]. De manera similar al cas de la teoria de Bass-Serre, un grup finitament presentat actua en un arbre real si i només si el grup descompon en termes d'estabilitzadors de vèrtexs i arcs.

Com en el cas de la teoria de Bass-Serre, la teoria de Rips ha estat i és molt rellevant per a la teoria de grups, no tan sols com a resultat, sinó com a tècnica per a atacar problemes nous, com a mètode per a simplificar resultats clàssics i com a vincle per a establir connexions amb altres branques de les matemàtiques tals com geometria, topologia de dimensió baixa i sistemes dinàmics. Però d'entre aquestes diverses aplicacions, només ens concentrem en la de l'estudi de les teories universals i elementals dels grups lliures.

Tot seguit explicarem el punt de vista de Sela sobre com utilitzar la teoria d'accions en arbres reals per a l'estudi de grups de coordenades de varietats algebraiques sobre el grup lliure [62].

La idea principal és que si existeix una família infinita d'homomorfismes $\{\phi_i\}_{i\in\mathbb{N}}$, d'un grup finitament generat G a un grup lliure F, llavors obtenim una família infinita d'accions $\{\alpha_i\}_{i\in\mathbb{N}}$ del grup G en un arbre simplicial (el grup G actua en el graf de Cayley del grup lliure —que és un arbre simplicial— via l'homomorfisme).

Utilitzant teoremes de convergència obtenim que les accions α_i convergeixen a una acció α del grup G en un arbre real (que és el límit d'arbres simplicials amb una mètrica normalitzada per les accions α_i). Per tant, podem utilitzar la maquinària de Rips per a determinar una descomposició del grup G', el quocient del grup G pel nucli de l'acció

$$\operatorname{Ker}\alpha = \{g \in G \mid \alpha(g,x) = x \text{ per a tot } x \text{ en l'arbre real}\}.$$

Sela va definir els grups G' obtinguts d'aquesta manera (quocients d'un grup pel nucli d'una acció límit), com a *grups límit* i va demostrar que, de fet, aquests grups són discriminats pel grup F i, per tant, són grups de coordenades de varietats algebraiques sobre els grups lliures.

Per l'altra banda, si un grup G és un grup de coordenades d'una varietat algebraica sobre un grup lliure F, llavors G és discriminat pel grup F i per tant existeixen infinits homomorfismes del grup G a F. Com a conseqüència de l'argument anterior obtenim que G actua en un arbre real. Sela va demostrar que el nucli d'aquesta acció és trivial, *i. e.*, $G = G'$.

Per tant, els grups de coordenades de varietats algebraiques sobre els grups lliures són precisament els grups límit. (Aquesta caracterització dels grups de coordenades de varietats algebraiques sobre els grups lliures va motivar la seva caracterització com a estructures límit; vegeu teorema 23.)

Així doncs, tenim que la teoria d'equacions sobre els grups lliures i el seu motor principal, el procés de Makanin-Razborov, es pot utilitzar per a analitzar accions de grups en arbres reals. Però també podem invertir aquest corrent d'idees i utilitzar les accions en arbres reals per a obtenir resultats estructurals de les varietats algebraiques sobre els grups lliures.

Aquest punt de vista geomètric va permetre generalitzar l'estudi de varietats algebraiques sobre grups hiperbòlics així com sobre grups relativament hiperbòlics: si existeixen infinits homomorfismes d'un grup finitament generat G a un grup hiperbòlic H, obtenim una acció del grup G en el «límit» d'espais hiperbòlics, que és un arbre real, i, per tant, com en el cas de grups lliures, podem tornar a utilitzar la teoria de Rips per a determinar l'estructura dels grups de coordenades.

Teoria elemental dels grups lliures

L'estudi de varietats algebraiques i les classes d'equivalència universal dels grups lliures va ser el primer pas cap a l'estudi de la teoria elemental dels grups

lliures. En aquesta secció fem un resum molt superficial de les idees principals que varen portar a la descripció de la classe elemental dels grups lliures i a la demostració de la decidibilitat de la seva teoria.

El fet principal que ha permès l'estudi de la teoria elemental dels grups lliures és que el conjunt de $\forall\exists$-fórmules és un conjunt d'eliminació de quantificadors. Així doncs, a grans trets, l'estudi de la teoria elemental es redueix a dos passos principals: demostrar que tota fórmula és equivalent en la teoria d'un grup lliure a una $\forall\exists$-fórmula, i estudiar les $\forall\exists$-fórmules (donar un criteri per a validar una $\forall\exists$-sentència en un grup lliure, determinar els grups de coordenades que satisfan les mateixes $\forall\exists$-fórmules que el grup lliure…).

Abans d'endinsar-nos en l'estratègia per a validar una $\forall\exists$-sentència en un grup lliure, volem revisar breument el resultat de Merzlyakov, ja que mostra una situació «ideal» que ens servirà de motivació i guia en el procés de validació.

Merzlyakov va demostrar que la teoria positiva dels grups lliures admet eliminació de quantificadors utilitzant el concepte de «solucions formals». Més concretament, Merzlyakov va demostrar que si una sentència positiva

$$\forall X_1\,\exists Y_1 \ldots \forall X_k\,\exists Y_k\,(S(X,Y)=1)$$

és certa en un grup lliure, llavors podem «expressar les variables Y en funció de les variables X perquè satisfacin la sentència», *i. e.*, podem determinar de manera efectiva paraules $q_1(X_1),\ldots,q_k(X_1,\ldots,X_k)\in F[X_1,\ldots,X_k]$ tals que la sentència $S(X_1,q_1(X_1),\ldots,X_k,q_k(X_1,\ldots,X_k))=1$ és certa en el grup lliure $F[X_1,\ldots,X_k]$. Des d'aquesta perspectiva, el teorema de Merzlyakov es pot interpretar com un anàleg del teorema de la funció implícita. Des del punt de vista de la geometria algebraica, aquest resultat es pot descriure com un *lifting* de solucions d'equacions a punts genèrics de les varietats algebraiques. En el llenguatge de teoria de models, el resultat afirma l'existència de funcions de Skolem per a aquest tipus particular de fórmula.

Tot seguit resumirem el procés per a validar si una $\forall\exists$-sentència és certa o no en un grup lliure. Primer comencem amb una observació que ajuda a simplificar l'estructura d'una $\forall\exists$-fórmula. No és difícil de demostrar que en el grup lliure, per a tot sistema d'equacions S, existeix una única equació s que defineix la mateixa varietat que S, és a dir, $V_F(S)=V_F(s)$. Un resultat anàleg també és cert per a la unió de varietats. Generalitzant més, podem dir que tota $\forall\exists$-sentència és equivalent a una sentència del tipus

$$\forall X\,\exists Y\,(W(X,Y)=1\wedge T(X,Y)\neq 1),$$

on S i T són equacions en les variables $X\cup Y$.

En general, les $\forall\exists$-fórmules no es redueixen a una fórmula universal; és a dir, no podem eliminar quantificadors, però veurem que el procés de validació en certa manera mostra que podem eliminar el quantificador «localment». La idea és subdividir el domini de la variable universal (F^m, si $X=\{x_1,\ldots,x_m\}$) en conjunts (de l'àlgebra booleana universal) on sí que tenim eliminació de quantificadors; és a dir, reduïm la validació de la fórmula a la validació de fórmules universals en subconjunts del domini.

Considerem l'equació positiva $\phi : \forall X \exists Y \, (W(X,Y) = 1)$. Pel teorema de Merzlyakov, existeix una solució formal que designem breument per $P(X)$; és a dir, la sentència $\forall X \exists Y \, (W(X,Y) = 1)$ és certa en F si i només si ho és la sentència $\forall X \, (W(X,P(X)) = 1)$. En general, però, no podem assegurar que per a tot X del domini $T(X,P(X)) \neq 1$. Descomponem, doncs, el domini de la variable universal X en dos subconjunts: la varietat $V_1 = \{X \mid T(X,P(X)) = 1\}$ i la covarietat $S_1 = \{X \mid T(X,P(X)) \neq 1\}$. Utilitzant aquesta partició obtenim que la fórmula ϕ és certa en F si i només si ho és la sentència

$$\forall X \in S_1 \exists Y \, (W(X,Y) = 1 \wedge T(X,Y) \neq 1) \wedge \\ \wedge \forall X \in V_1 \exists Y \, (W(X,Y) = 1 \wedge T(X,Y) \neq 1).$$

Però, per definició de la covarietat S_1, la sentència

$$\forall X \in S_1 \exists Y \, (W(X,Y) = 1 \wedge T(X,Y) \neq 1)$$

és sempre certa, només cal prendre $Y = P(X)$. Per tant, la sentència ϕ és certa en F si i només si ho és la sentència

$$\forall X \in V_1 \exists Y \, (W(X,Y) = 1 \wedge T(X,Y) \neq 1). \tag{3}$$

En aquest punt, l'estratègia que volem seguir en el procés de validació és clara: iterar el procés de subdivisió i demostrar que s'atura en un nombre finit de passos.

Per a poder iterar la subdivisió del domini d'una manera anàloga al primer pas, necessitem una generalització del teorema de Merzlyakov per a varietats, *i. e.*, volem demostrar l'existència de solucions formals per a fórmules del tipus (3), on V_1 és una varietat.

Resulta que si el sistema d'equacions $S(X)$ que defineix la varietat V en la fórmula

$$\forall X \in V \exists Y \, (W(X,Y) = 1 \wedge T(X,Y) \neq 1)$$

és un sistema regular NTQ, es pot demostrar un anàleg del teorema de la funció implícita; és a dir, en aquest cas també podem donar una «parametrització» de les variables Y en funció de les variables X.

A més a més, els requeriments del teorema són òptims; és a dir, els únics grups de coordenades de varietats algebraiques sobre els grups lliures per als quals el teorema de la funció implícita és cert són els grups de coordenades de varietats algebraiques associats a sistemes regulars NTQ. Com a conseqüència obtenim que si un grup finitament generat G és elementalment equivalent a un grup lliure, llavors el grup G és isomorf a un grup de coordenades associat a un sistema regular NTQ.

Tal com volíem, el teorema de la funció implícita és una generalització del teorema de Merzlyakov. Però si revisem el primer pas del procés, l'equació $T(X,P(X))$ que defineix el conjunt algebraic és completament arbitrària. En general, per a un sistema arbitrari d'equacions no existeixen solucions formals

per a les sentències del tipus $\forall X \in V\, \exists Y\, (W(X,Y) = 1)$. Però, un altre cop, podem determinar efectivament un recobriment finit del conjunt $V = \bigcup_{i=1}^{k} V_F(R_i)$ amb varietats associades a sistemes d'equacions R_i regulars NTQ, i llavors podem determinar en aquestes subvarietats les solucions formals; és a dir, l'objectiu és obtenir parametritzacions locals.

Si el teorema de la funció implícita fos vàlid per a tots els conjunts algebraics, el procés que hem descrit aniria imposant relacions a la varietat; és a dir, ens produiria una seqüència d'epimorfismes propis $F[X]/R(V_1) \to F[X]/R(V_2) \to \dots$ Per tant, com que els grups lliures són equacionalment noetherians podríem assegurar que la seqüència estabilitza.

El problema és que per a recobrir una varietat $V \subset F^m$ amb varietats corresponents a sistemes regulars NTQ, en general no podem fer-ho a dins de F^m i necessitem considerar una varietat equivalent $V' \subset F^{m'}$, $m < m'$ i recobrir-la a dins de $F^{m'}$. Aquest fenomen d'increment de dimensió ambiental no ens permet utilitzar la propietat de ser equacionalment noetherià i és un dels principals obstacles per a demostrar que el procés de verificació de $\forall\exists$-fórmules és finit.

Per a demostrar que el procés és finit, necessitem definir un equivalent de «dimensió» i demostrar que en cada pas del procés aquesta disminueix. Els invariants obvis (com el rang del grup…) no són suficients. Per a establir la noció correcta de *dimensió* és necessari un estudi del comportament de la imatge dels grups de coordenades de varietats algebraiques per homomorfismes. El punt clau per a aquest estudi és l'estructura dels grups de coordenades en termes de la descomposició JSJ i com aquesta descomposició varia a través d'epimorfismes.

Cal remarcar que aquest procés no funciona tan sols per a tot grup lliure no abelià, sinó per a tot grup de coordenades associat a un sistema d'equacions regulars NTQ. Així doncs, com a conseqüència del procés de validació, obtenim que $\mathrm{Th}_{\forall\exists}(F) = \mathrm{Th}_{\forall\exists}(F[X]/\mathrm{Rad}(R))$ per a tot sistema d'equacions regulars NTQ sobre el grup lliure F.

L'eliminació de quantificadors es demostra inductivament. La base d'inducció que necessitem demostrar és que tota $\exists\forall\exists$-fórmula ϕ és equivalent a una combinació booleana de $\forall\exists$-fórmules. Aquesta part és la tècnicament més exigent i consta de tres passos.

El primer pas és uniformitzar el procés de validació de les $\forall\exists$-fórmules. L'objectiu és construir un nombre *finit* de col·leccions de varietats i solucions formals en aquestes varietats de manera que tota $\forall\exists$-fórmula associada a l'especialització de la primera variable existencial de la fórmula ϕ pot ser validada per una de les col·leccions que hem construït. En altres paraules, aquest procés per a la uniformització de demostracions construeix un arbre de conjunts estratificats que ens deixa amb un nombre finit de «formes de demostració». La tècnica tant per a construir com per a aturar aquest procés es basa a uniformitzar els arguments del procés de validació de $\forall\exists$-fórmules.

El segon procés redueix la qüestió de l'existència d'un possible «testimoni» (un valor de la primera variable existencial) amb una demostració vàlida (per a una especialització donada dels paràmetres) a l'estructura de la base dels fibrats de demostracions.

L'últim pas demostra que és possible estratificar la base d'aquest fibrat i que l'existència d'un «testimoni» per a un paràmetre donat només depèn de l'estrat (i no de l'especialització concreta). A més, cada estrat pertany a l'àlgebra booleana de $\forall\exists$-conjunts.

Podem concloure que el $\exists\forall\exists$-conjunt és la unió d'un nombre finit d'estrats del fibrat i, per tant, pertany a l'àlgebra booleana de $\forall\exists$-conjunts.

Resumim els resultats principals de la teoria elemental dels grups lliures.

TEOREMA 26. *Sigui F un grup lliure (no abelià) i G un grup finitament generat.*

- *$G \equiv F$ si i només si $G \equiv_{\forall\exists} F$; vegeu* [28, 63].
- *$G \equiv F$ si i només si G és isomorf a un grup de coordenades associat a un sistema regular NTQ,* i. e., *$G \simeq {}^{F[X]}/_{\mathrm{Rad}(R)}$ on R és un sistema d'equacions regular NTQ; vegeu* [28, 63].
- *En particular, tots els grups lliures no abelians són elementalment equivalents. De fet, el monomorfisme natural de grups lliures $F_k < F_m$, $k < m$, és un monomorfisme elemental* [28, 63].
- *La teoria elemental dels grups lliures és decidible* [28].
- *Tot conjunt definible en un grup lliure pertany a l'àlgebra booleana dels $\forall\exists$-conjunts* [28, 63].
- *La teoria dels grups lliures és estable (però no superestable)* [64].

La demostració completa dels problemes de Tarski va ser publicada recentment, l'any 2006. Avui en dia encara no s'ha trobat una raó conceptual que expliqui per què el conjunt de $\forall\exists$-fórmules és un conjunt d'eliminació de quantificadors o per què una $\forall\exists$-sentència pot ser validada, a part de l'existència dels mateixos processos. Així doncs, encara queda camí per recórrer per a comprendre realment la teoria dels grups lliures.

A part de la importància teòrica d'aquests resultats, cal remarcar el nou punt de vista i les diferents tècniques que apareixen en les demostracions per a l'estudi de teories elementals. Creiem que ens trobem en una primera etapa i que aquestes tècniques es desenvoluparan i es podran aplicar a l'estudi d'altres teories de grups i, més en general, d'estructures algebraiques.

Agraïments

L'autora vol agrair a la Societat Catalana de Matemàtiques haver estat convidada com a conferenciant a la Tretzena Trobada Matemàtica. També vol agrair als professors Josep Maria Font, Ilya Kazachkov i Enric Ventura, així com als revisors els seus comentaris i suggeriments sobre el contingut d'aquest article. Aquest treball ha estat realitzat amb el suport del Programa de Formación de Investigadores del Departamento de Educación, Universidades e Investigación del Gobierno Vasco.

Referències

[1] Alperin, R.; Moss, K. «Complete trees for groups with a real-valued length function». *J. London Math. Soc. (2)*, 31 (1985), 55–68.

[2] Appel, K. I. «One-variable equations in free groups». *Proc. Amer. Math. Soc.*, 19 (1968), 912–918.

[3] Ax, J.; Kochen, S. «Diophantine problems over local fields. I». *Amer. J. Math.*, 87 (1965), 605–630.

[4] Ax, J.; Kochen, S. «Diophantine problems over local fields. II. A complete set of axioms for p-adic number theory». *Amer. J. Math.*, 87 (1965), 631–648.

[5] Ax, J.; Kochen, S. «Diophantine problems over local fields. III. Decidable fields». *Ann. of Math. (2)*, 83 (1966), 437–456.

[6] Baumslag, G.; Myasnikov, A.; Remeslennikov, V. «Algebraic geometry over groups I. Algebraic sets and ideal theory». *J. Algebra*, 219 (1999), 16–79.

[7] Belegradek, O. V. «The model theory of unitriangular groups». *Ann. Pure Appl. Logic*, 68 (1994), 225–261.

[8] Bestvina, M. «$\mathbb{R}$-trees in topology, geometry, and group theory». A: *Handbook of geometric topology*. Amsterdam: North-Holland, 2002, 55–91.

[9] Bestvina, M.; Feighn, M. «Stable actions of groups on real trees». *Invent. Math.*, 121 (2) (1995), 287–321.

[10] Chang, C. C.; Keisler, H. J. *Model theory*. Amsterdam; Londres: North-Holland, 1973.

[11] Chiswell, I. M. «Abstract length functions in groups». *Math. Proc. Cambridge Philos. Soc.*, 80 (3) (1976), 451–463.

[12] Comerford, L. P., Jr.; Edmunds, C. C. «Quadratic equations over free groups and free products». *J. Algebra*, 68 (2) (1981), 276–297.

[13] Culler, M. «Using surfaces to solve equations in free groups». *Topology*, 20 (2) (1981), 133–145.

[14] Daniyarova, E.; Myasnikov, A.; Remeslennikov, V. «Algebraic geometry over algebraic structures II: Foundations». arXiv:1002.3562v3.

[15] Denef, J. «The rationality of the Poincaré series associated to the p-adic points on a variety». *Invent. Math.*, 77 (1) (1984), 1–23.

[16] Ershov, Y. «On elementary theories of local fields». *Algebra i Logika Sem.*, 4 (2) (1965), 5–30.

[17] Ershov, Y. «On elementary theory of maximal normalized fields». *Algebra i Logika Sem.*, 4 (3) (1965), 31–70.

[18] Ershov, Y. «On the elementary theory of maximal normed fields. II». *Algebra i Logika Sem.*, 5 (1) (1966), 5–40.

[19] Ershov, Y. «Elementary group theories». *Dokl. Akad. Nauk SSSR*, 203 (1972), 1240–1243.

[20] Gaboriau, D.; Levitt, G.; Paulin, F. «Pseudogroups of isometries of R and Rips' theorem on free actions on R-trees». *Israel J. Math.*, 87 (1994), 403–428.

[21] Grigorchuk, R. I.; Kurchanov, P. F. «On quadratic equations in free groups». A: *Proceedings of the International Conference on Algebra, Part 1* (Novosibirsk, 1989). Providence, R. I.: American Mathematical Society 1992. (Contemporary Mathematics; 131), 159–171.

[22] Guba, V. S. «Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems». *Mat. Zametki*, 40 (3) (1986), 321–324.

[23] Haskell, D.; Pillay, A.; Steinhorn, C. (ed.) *Model theory, algebra, and geometry*. Cambridge: Cambridge University Press, 2000. (Mathematical Sciences Research Institute Publications; 39)

[24] Hodges, W. *Model theory*. Cambridge: Cambridge University Press, 1993. (Encyclopedia of Mathematics and its Applications; 42)

[25] Hodgson, B. R. «Els treballs d'Hèrcules o els de Sísif? Una visió renovada del fenomen de la incompletesa en lògica matemàtica». *Butlletí de la Societat Catalana de Matemàtiques*, 25 (1) (2010), 31–41.

[26] Kharlampovich, O.; Myasnikov, A. «Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz». *J. Algebra*, 200 (2) (1998), 472–516.

[27] Kharlampovich, O.; Myasnikov, A. «Irreducible affine varieties over a free group. II. Systems in triangular quasi-quadratic form and description of residually free groups». *J. Algebra*, 200 (2) (1998), 517–570.

[28] Kharlampovich, O.; Myasnikov, A. «Elementary theory of free nonabelian groups». *J. Algebra*, 302 (2) (2006), 451–552.

[29] Lascar, D. «Perspective historique sur les rapports entre la théorie des modèles et l'algèbre. Un point de vue tendancieux». *Rev. Histoire Math.*, 4 (2) (1998), 237–260.

[30] Lorents, A. A. «The solution of systems of equations in one unknown in free groups». *Dokl. Akad. Nauk*, 148 (1963), 1253–1256.

[31] Lorents, A. A. «Representations of sets of solutions of systems of equations with one unknown in a free group». *Dokl. Akad. Nauk*, 178 (1968), 290–292.

[32] Lyndon, R. C. «Equations in free groups». *Trans. Amer. Math. Soc.*, 96 (1960), 445–457.

[33] Lyndon, R. C. «Groups with parametric exponents». *Trans. Amer. Math. Soc.*, 96 (1960), 518–533.

[34] Macintyre, A. «On ω_1-categorical theories of fields». *Fund. Math.*, 71 (1) (1971), 1–25.

[35] Macintyre, A. «On ω_1-categorical theories of abelian groups». *Fund. Math.*, 70 (3) (1971), 253–270.

[36] MACINTYRE, A.; MCKENNA, K.; DRIES, L. VAN DEN. «Elimination of quantifiers in algebraic structures». *Adv. in Math.*, 47 (1) (1983), 74–87.

[37] MAKANIN, G. S. «The problem of the solvability of equations in a free semigroup». *Mat. Sb. (N.S.)*, 103(145) (2) (1977), 147–236, 319.

[38] MAKANIN, G. S. «Equations in a free group». *Izv. Akad. Nauk SSSR Ser. Mat.*, 46 (6) (1982), 1199–1273, 1344. Traducció a l'anglès: *Math. USSR-Izv.*, 21 (3) (1983), 546–582.

[39] MAKANIN, G. S. «Decidability of the universal and positive theories of a free group». *Izv. Akad. Nauk SSSR Ser. Mat.*, 48 (4) (1984), 735–749.

[40] MAL'CEV, A. I. «Some correspondences between rings and groups». *Mat. Sb. (N.S.)*, 50 (92) (1960), 257–266.

[41] MAL'CEV, A. I. «On the equation $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ in a free group». *Algebra i Logika Sem.*, 1 (5) (1962), 45–50.

[42] MARKER, D. *Model theory: An introduction*. Nova York: Springer, 2002. (Graduate Texts in Mathematics; 217)

[43] MATIYASEVICH, Y. «Hilbert's tenth problem: What can we do with Diophantine equations?» [en línia]. `http://logic.pdmi.ras.ru/Hilbert10/journal/preprints/H10histe.ps`.

[44] MERZLYAKOV, Y. I. «Positive formulae on free groups». *Algebra i Logika*, 5 (1966), 25–42.

[45] MORGAN, J. W.; SHALEN, P. B. «Valuations, trees, and degenerations of hyperbolic structures. I». *Ann. of Math. (2)*, 120 (3) (1984), 401–476.

[46] MORGAN, J. W.; SHALEN, P. B. «Degenerations of hyperbolic structures. II. Measured laminations in 3-manifolds». *Ann. of Math. (2)*, 127 (2) (1988), 403–456.

[47] MORGAN, J. W.; SHALEN, P. B. «Degenerations of hyperbolic structures. III. Actions of 3-manifold groups on trees and Thurston's compactness theorem». *Ann. of Math. (2)*, 127 (3) (1988), 457–519.

[48] MYASNIKOV, A. G.; REMESLENNIKOV, V. N. «Exponential groups. II. Extensions of centralizers and tensor completion of CSA-groups». *Internat. J. Algebra Comput.*, 6 (6) (1996), 687–711.

[49] MYASNIKOV, A. G.; SOHRABI, M. «Groups elementarily equivalent to a free nilpotent group of finite rank». *Ann. Pure Appl. Logic*, 162 (11) (2011), 916–933.

[50] NIELSEN, J. «Untersuchungen zur Topologie der geschlossenen zweiseitigen Flächen. I, II, III». *Acta Math.*, 50 (1) (1927), 189–358; *Acta Math.*, 53 (1) (1929), 1–76; *Acta Math.*, 58 (1) (1932), 87–167.

[51] OGER, F. «Cancellation and elementary equivalence of finitely generated finite-by-nilpotent groups». *J. London Math. Soc. (2)*, 44 (1) (1991), 173–183.

[52] OL'SHANSKIĬ, A. Y. «Diagrams of homomorphisms of surface groups». *Sibirsk. Mat. Zh.*, 30 (6) (1989), 150–171. Traducció a l'anglès: *Siberian Math. J.*, 30 (6) (1989), 961–979 (1990).

[53] Ozhigov, Y. I. «Equations with two unknowns in a free group». *Dokl. Akad. Nauk SSSR*, 268 (4) (1983), 809–813.

[54] Pillay, A. «Model theory». *Notices Amer. Math. Soc.*, 47 (11) (2000), 1373–1381.

[55] Razborov, A. A. «An equation in a free group whose set of solutions does not allow a representation as a superposition of a finite number of parametric functions». A: *Proceedings of the 9th All-Union Symposium on Group Theory*. Moscou: [s. ll.], 1984, p. 54.

[56] Razborov, A. A. «On systems of equations in a free group». Tesi doctoral. Moscou: Steklov Mathematical Institute, 1987.

[57] Repin, N. N. «Solvability of equations with one indeterminate in nilpotent groups». *Izv. Akad. Nauk SSSR Ser. Mat.*, 48 (6) (1984), 1295–1313.

[58] Robinson, A. *Complete theories*. Amsterdam: North-Holland, 1956.

[59] Rogers, P. K. «Topics in the model theory of abelian and nilpotent groups». Tesi doctoral. Bedford College, London University.

[60] Roman'kov, V. A. «Unsolvability of the problem of endomorphic reducibility in free nilpotent groups and in free rings». *Algebra i Logika*, 16 (4) (1977), 457–471, 494. Traducció a l'anglès: *Algebra and Logic*, 16 (4) (1977), 310–320.

[61] Roman'kov, V. A. «Universal theory of nilpotent groups». *Mat. Zametki*, 25 (4) (1979), 487–495, 635.

[62] Sela, Z. «Diophantine geometry over groups. I. Makanin-Razborov diagrams». *Publ. Math. Inst. Hautes Études Sci.*, 93 (2001), 31–105.

[63] Sela, Z. «Diophantine geometry over groups. VI. The elementary theory of a free group». *Geom. Funct. Anal.*, 16 (3) (2006), 707–730.

[64] Sela, Z. «Diophantine geometry over groups. VII. The elementary theory of a hyperbolic group». *Proc. Lond. Math. Soc. (3)*, 99 (1) (2009), 217–273.

[65] Serre, J.-P. *Trees*. Berlín; Nova York: Springer, 1980.

[66] Szmielew, W. «Elementary properties of Abelian groups». *Fund. Math.*, 41 (1955), 203–271.

[67] Tarski, A. «Arithmetical classes and types of algebraically closed and real closed fields». *Bull. Amer. Math. Soc.*, 55 (1949), 63–64.

[68] Tarski, A. *A decision method for elementary algebra and geometry*. 2a ed. Berkeley; Los Angeles: University of California Press, 1951.

[69] Tits, J. «A "theorem of Lie-Kolchin" for trees». A: *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*. Nova York: Academic Press, 1977, 377–388.

[70] Zil'ber, B. I. «An example of two elementarily equivalent but not isomorphic finitely generated metabelian groups». *Algebra i Logika*, 10 (1971), 309–315.

Mathematical Institute
University of Oxford
24-29 St Giles', Oxford, OX1 3LB, UK
montsecasals@gmail.com