Butlletí de la Societat Catalana de Matemàtiques
Vol. 32, núm. 2, 2017. Pàg. 133–153. DOI: 10.2436/20.2002.01.76

Definibilitat en estructures matemàtiques

Enrique Casanovas Ruiz-Fornells

Resum: Discutim la noció de definibilitat de relacions, funcions i elements d'una estructura matemàtica mitjançant el llenguatge formal de la lògica de primer ordre en el context de la teoria de models. A través de l'exposició d'una sèrie d'exemples de problemes de definibilitat basats en sistemes numèrics familiars per a tot matemàtic, mostrem que l'anàlisi de la complexitat de les relacions definibles en una estructura aporta informació valuosa sobre qüestions de decidibilitat i categoricitat de la seva teoria.

Paraules clau: definibilitat, teoria de models, axiomes, decidibilitat, categoricitat.

Classificació MSC2010: 03C07, 03C40, 03C45.

1 Introducció

En el desenvolupament de qualsevol disciplina matemàtica és habitual alternar l'enunciat i la demostració de teoremes amb la introducció de definicions. Mitjançant una definició s'introdueix la notació que permet abreujar els enunciats posteriors i facilitar-ne la comprensió. No cal gaire discussió sobre els criteris que han de complir les definicions, més enllà que han d'evitar circularitats i que, en el cas de la definició d'operacions, han de demostrar-se prèviament unes condicions d'existència i unicitat dels valors. Una altra cosa diferent és explicar què significa que un objecte matemàtic concret, com un número natural o real o una relació entre números, sigui definible. Per a això en primer lloc cal aclarir el context, especificar en quin domini d'objectes o números estem treballant, quines altres nocions es pressuposen ja introduïdes i en quin llenguatge pot enunciar-se la definició. Però fins i tot després de tot això poden sorgir problemes.

Una versió preliminar d'aquest article es va exposar a la lliçó inaugural del curs 2016–2017 de la Facultat de Matemàtiques i Informàtica de la Universitat de Barcelona.

A principis del segle XX, en el context de la crisi de fonaments de les matemàtiques, es van donar a conèixer diverses paradoxes relatives a la definibilitat. El 1906 B. Russell escriu l'article [16], en el qual exposa l'anomenada *paradoxa de Berry*. Pot formular-se com l'observació que el menor número natural que no és definible mitjançant menys de disset paraules de l'idioma català és, com s'aprecia comptant paraules de la frase anterior, definible mitjançant setze paraules. Russell, que atribueix aquesta paradoxa a un bibliotecari de la biblioteca Bodleian d'Oxford anomenat M. G. G. Berry, enuncia la paradoxa en termes de frases de menys de divuit síl·labes de l'idioma francès. Una altra paradoxa similar que Russell discuteix és la *paradoxa de Richard*, proposada originàriament per J. Richard a [14]. En aquest cas es consideren tots els números reals definibles, i se'n fa una llista $r_0, r_1, \ldots$ ordenant-los d'acord amb la longitud de la seva definició i d'acord amb un ordre especificat per a les definicions que tinguin la mateixa longitud, per exemple, aplicant l'ordre lexicogràfic en aquest cas. Mitjançant el mètode de diagonalització es pot definir a continuació un número real r que difereix de r_n en el n-èsim dígit decimal, un número real definible que no apareix en la llista de tots els números reals definibles.

A la vista d'aquests exemples, és natural sospitar que la noció de número definible és poc rigorosa i ha de ser evitada en els raonaments matemàtics. El 1931 A. Tarski constata, a [23], que aquesta és l'opinió general dels matemàtics i es proposa argumentar en contra en un cas particular. En el citat article, Tarski mostra que els conjunts definibles de números reals en el grup ordenat additiu real són caracteritzables com a unions finites d'intervals (incloent-hi semirectes) i punts. El llenguatge que Tarski especifica perquè es puguin escriure les possibles definicions és un llenguatge formal, el llenguatge de la lògica de primer ordre. Molt pocs anys després, el mateix Tarski va mostrar que és possible definir la noció de veritat per a enunciats d'aquest llenguatge amb tota generalitat i precisió: es pot definir rigorosament una relació $\vDash$ tal que per a cada estructura matemàtica $\mathcal{M}$, per a cada fórmula de la lògica de primer ordre $\varphi(x_1, \ldots, x_n)$ i cada ènupla $a_1, \ldots, a_n$ d'elements de l'univers o domini de $\mathcal{M}$, $\mathcal{M} \vDash \varphi(a_1, \ldots, a_n)$ si i només si $\varphi(x_1, \ldots, x_n)$ és certa a $\mathcal{M}$ en fer correspondre les variables $x_1, \ldots, x_n$ amb $a_1, \ldots, a_n$. Com indicarem més endavant, a partir d'aquesta noció és fàcil caracteritzar les relacions, les operacions i els elements definibles en l'estructura $\mathcal{M}$. Les paradoxes de la definibilitat no sorgeixen quan el llenguatge en el qual es donen les possibles definicions és el llenguatge formal de la lògica de primer ordre.

El nostre propòsit en aquest article és il·lustrar alguns aspectes de la teoria de models aprofitant l'exposició de resultats sobre definibilitat en estructures matemàtiques. La *teoria de models* és la branca de la lògica matemàtica en la qual s'investiguen les estructures amb ajuda dels llenguatges formals de primer ordre. S'hi estudien les teories matemàtiques i els seus *models*, que són les estructures en les quals són certs els enunciats de les teories. La tesi que defensem és que l'anàlisi de les relacions definibles en una estructura aporta informació essencial per a entendre problemes de decidibilitat i categoricitat de teories i, més generalment, contribueix a posar un cert ordre en els dife-

rents tipus de teories i en la classificació dels seus models. Exemplificarem constantment les nostres afirmacions amb estructures matemàtiques que ens són molt familiars a tots i que provenen de l'aritmètica, de la teoria de grups i de la teoria de cossos.

2 Preliminars

Per a la discussió i l'exposició dels resultats necessitem introduir amb una certa precisió la noció d'estructura matemàtica i del llenguatge de primer ordre associat. No ho farem amb tot el rigor, entenent que el lector interessat coneix aquests temes o bé en tindrà prou amb una descripció succinta, suficient per a seguir l'argumentació. Per a més detalls es recomana acudir a un manual de lògica, com per exemple el de H. B. Enderton [3]. Les estructures matemàtiques són els objectes amb els quals habitualment els matemàtics treballen: conjunts en els quals estan establertes unes relacions i unes operacions. És important tenir ben present que no només el canvi de conjunt, sinó també el canvi, addició o supressió d'operacions o relacions, determina un canvi d'estructura. No és el mateix discutir els números naturals amb la suma, que amb la suma i el producte.

Si M és un conjunt i $n \geq 1$ és un número natural, amb M^n ens referim al producte cartesià de M iterat n vegades: $M \times \cdots \times M$. En altres termes, M^n és el conjunt de totes les ènuples $(a_1, \ldots, a_n)$ que poden obtenir-se amb elements a_i de M.

Una *estructura* és un objecte matemàtic de la forma

$$\mathcal{M} = (M, R_1, R_2, \ldots, f_1, f_2, \ldots, c_1, c_2, \ldots),$$

on

- M és un conjunt no buit, l'*univers* de l'estructura.
- $R_i \subseteq M^{n_i}$ és una relació a M.
- $f_i \colon M^{m_i} \to M$ és una operació a M.
- $c_i \in M$ és un element destacat de M, una constant de M.

Una estructura pot tenir poques o moltes relacions, operacions i elements destacats i hi poden faltar alguns d'aquests ingredients. Alguns exemples familiars contribuiran a millorar-ne la comprensió:

- Els cossos de números racionals $(\mathbb{Q}, +, -, \cdot, 0, 1)$, de números reals $(\mathbb{R}, +, -, \cdot, 0, 1)$ i de números complexos $(\mathbb{C}, +, -, \cdot, 0, 1)$.
- Grups, com el dels enters $(\mathbb{Z}, +, 0)$ o el de Prüfer $(\mathbb{Z}_{p^\infty}, +, 0)$, i grups ordenats com $(\mathbb{Z}, +, <, 0)$ o $(\mathbb{Q}, +, <, 0)$.
- Conjunts ordenats, com $(\mathbb{Q}, <)$ i $(\mathbb{Z}, <)$.
- Els números naturals amb diverses operacions i relacions, com $(\mathbb{N}, +, 0)$, $(\mathbb{N}, S)$ (on S és la funció successor) i $(\mathbb{N}, +, \cdot, <, 0, 1)$.

Implícitament hem acceptat que les relacions, les operacions i les constants d'una estructura es poden enumerar mitjançant números naturals. Això no és sempre així i ens fa perdre una mica de generalitat, però també ens permetrà eliminar alguns tecnicismes en l'enunciat de resultats. En tot cas, els exemples més naturals són d'aquest tipus o fins i tot més simples, i molt sovint tenen només un nombre finit de relacions, d'operacions i d'individus destacats.

En lògica matemàtica s'utilitzen llenguatges formals de primer ordre per a caracteritzar, en la mesura del possible, les estructures per les quals hom s'interessa i per a estudiar-ne els conjunts, les relacions i les operacions. Un *llenguatge de primer ordre* apropiat per a l'estructura $\mathcal{M}$ fa ús de símbols corresponents a les relacions, funcions i elements destacats de l'estructura així com de variables, quantificadors i connectors lògics. Sempre té, a més, un símbol per a la igualtat, amb el qual es poden construir equacions. A la pràctica, molt sovint no distingim amb notació diferent les relacions, les operacions i els elements destacats d'una estructura dels símbols del llenguatge formal que s'usen per a anomenar-los.

Els *termes* del llenguatge són les expressions que s'obtenen a partir de les constants i de les variables mitjançant l'aplicació dels símbols corresponents a les operacions. Per exemple, $(0+x)\cdot(z+(y+x))$ és un terme del llenguatge de l'aritmètica. Les *fórmules* s'obtenen per mitjà dels connectors booleans $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ i mitjançant quantificadors elementals $\forall x$, $\exists x$ a partir de les *fórmules atòmiques*, que al seu torn es defineixen com a equacions entre termes $t_1 = t_2$ i predicacions bàsiques entre termes de la forma $R_i(t_1,\ldots,t_{n_i})$. Els *enunciats* són fórmules en les quals totes les variables que apareixen han estat quantificades. Les variables que en una fórmula no s'han quantificat es diuen *variables lliures*. És habitual usar la notació $\varphi(x_1,\ldots,x_n)$ per a referir-se a una fórmula les variables lliures de la qual estiguin en la llista $x_1,\ldots,x_n$. És important tenir ben present que els possibles valors de les variables són elements de l'univers de l'estructura, no subconjunts seus o objectes més complexos.

Els enunciats del llenguatge formal de $\mathcal{M}$ són sempre o certs o falsos en $\mathcal{M}$, la qual cosa no vol dir que tinguem un algorisme per a decidir en cada cas si ho són o no. El tenim en el cas de les estructures finites, però no en general. Per exemple, si $\mathrm{Prim}(y)$ és la fórmula $1 < y \wedge \forall z_1 z_2\ (y = z_1 \cdot z_2 \rightarrow (z_1 = 1 \vee z_1 = y))$, llavors l'enunciat $\forall x\,\exists y\ (x < y \wedge \mathrm{Prim}(y))$ significa a $(\mathbb{N},+,\cdot,<,0,1)$ que hi ha primers arbitràriament grans i, per tant, que hi ha infinits números primers, que sabem que és cert. No obstant això, l'enunciat $\forall x\ (1+1+1+1+1 < x \rightarrow \exists u\,\exists v\,\exists w\ (x = u+v+w \wedge \mathrm{Prim}(u)\wedge\mathrm{Prim}(v)\wedge\mathrm{Prim}(w)))$ expressa en aquesta mateixa estructura que tot número major que cinc és suma de tres primers. Es tracta de la conjectura de Goldbach, que no sabem si és certa o no.

Escrivim $\mathcal{M} \vDash \sigma$ per indicar que l'enunciat σ *és cert a* $\mathcal{M}$. Un dels grans mèrits de Tarski consisteix a proporcionar una definició matemàticament inobjectable de la relació $\vDash$, la relació de *satisfacció*. És una definició recursiva que segueix les fases de construcció de l'enunciat. Com que els enunciats es construeixen mitjançant un procés recursiu a partir de fórmules atòmiques

amb connectors i quantificacions, i en les fases intermèdies del procés no es tenen enunciats, sinó fórmules amb variables lliures, cal definir la relació de satisfacció per a aquestes. Llavors, fa falta també considerar una llista d'elements de l'estructura que correspongui a les variables lliures de la fórmula. Recordem que la notació $\varphi(x_1,\ldots,x_n)$ indica que les variables lliures de la fórmula φ són en la llista $x_1,\ldots,x_n$. Per exemple, en el llenguatge d'anells $\varphi(x,y)$ pot ser la fórmula $\exists z\ (x = y + z \cdot z)$, que diu que x és la suma de y amb un quadrat. Escrivim $\mathcal{M} \vDash \varphi(a_1,\ldots,a_n)$ per indicar que la fórmula és cert a $\mathcal{M}$ en fer correspondre les variables $x_1,\ldots,x_n$ amb els elements $a_1,\ldots,a_n \in M$, és a dir, que la ènupla $(a_1,\ldots,a_n)$ *satisfà* la fórmula a $\mathcal{M}$. Per exemple, la fórmula $\varphi(x,y)$ que acabem de donar la satisfan en el cos real tots els parells (a,b) de números reals tals que $a \geq b$; però en el cos complex la satisfan tots els parells de números complexos sense restriccions.

Una vegada es disposa de la noció de veritat en una estructura, es pot introduir la noció de *conseqüència lògica*. Es diu que un enunciat σ és conseqüència d'un conjunt d'enunciats Σ (o que Σ *implica* σ) si σ és certa en totes les estructures en les quals són certs tots els enunciats de Σ. En la lògica de primer ordre tenim un *teorema de completitud*, que garanteix que les conseqüències lògiques de Σ, en el sentit anterior, són precisament els enunciats que són demostrables a partir dels enunciats de Σ.

3 Teories

Les teories són conjunts d'enunciats. És convenient que els enunciats que siguin conseqüència lògica d'una teoria T, els seus *teoremes*, es considerin també elements de T. Per això, es defineix una *teoria* com un conjunt d'enunciats T que té la propietat que totes les seves conseqüències (en el llenguatge de T) pertanyen a T. Un cas particular és el de la *teoria d'una estructura* $\mathcal{M}$; és el conjunt $\mathrm{Th}(\mathcal{M})$ format pels enunciats del seu llenguatge formal de primer ordre que són certs en aquesta estructura, és a dir:

$$\mathrm{Th}(\mathcal{M}) = \{\sigma \mid \mathcal{M} \vDash \sigma\}.$$

Es diu que una estructura $\mathcal{M}$ és un *model* d'una teoria T si tots els enunciats de T són certs a $\mathcal{M}$, és a dir, si $T \subseteq \mathrm{Th}(\mathcal{M})$.

Una de les portes d'entrada a la teoria de models es traspassa en observar que dues estructures poden tenir la mateixa teoria i no ser isomorfes. Per a explicar aquest fet i d'altres que vindran tot seguit necessitarem parlar de dues relacions entre estructures, la *isomorfia*, $\cong$, i l'*equivalència elemental*, $\equiv$. Ambdues s'estableixen entre estructures que tenen el mateix llenguatge. La noció d'isomorfia és la que s'usa habitualment en àlgebra.

- $\mathcal{M} \cong \mathcal{N}$ si i només si hi ha una bijecció f entre els universos M i N que transforma les relacions, operacions i constants de $\mathcal{M}$ en les corresponents de $\mathcal{N}$, és a dir, per a cada relació R_i de $\mathcal{M}$, $f(R_i) = \{(f(a_1),\ldots,f(a_n)) \mid (a_1,\ldots,a_n) \in R_i\}$ és la corresponent relació de $\mathcal{N}$, i de manera similar per a operacions i individus destacats.

- $\mathcal{M} \equiv \mathcal{N}$ si i només si els enunciats del llenguatge formal de primer ordre que són certs a $\mathcal{M}$ i a $\mathcal{N}$ són els mateixos, és a dir, si i només si $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$.

Observem que $\mathcal{M} \cong \mathcal{N}$ indica que $\mathcal{M}$ i $\mathcal{N}$ són indistingibles per les seves propietats matemàtiques, mentre que $\mathcal{M} \equiv \mathcal{N}$ diu simplement que no les podem distingir mitjançant les propietats que poden expressar-se en el llenguatge formal de la lògica de primer ordre. Aquestes nocions pertanyen als aspectes més elementals de la teoria de models. Com a text de referència per a aquestes qüestions i, en general, per a tot el que segueix, recomanem el llibre de K. Tent i M. Ziegler (vegeu [25]).

Les preguntes inicials que, des de la perspectiva de la teoria de models, hom es pot plantejar sobre una estructura $\mathcal{M}$ inclouen molt probablement les següents:

1. És possible especificar una llista d'axiomes per a la teoria de $\mathcal{M}$?
2. Existeix un algorisme per a decidir quins enunciats són certs a $\mathcal{M}$?
3. Quines són les estructures $\mathcal{N}$ tals que $\mathcal{M} \equiv \mathcal{N}$?
4. Quines relacions, operacions i elements són definibles a $\mathcal{M}$?

Hem d'explicar què és una llista d'axiomes i hem d'acabar de precisar què significa ser definible. El nostre propòsit és mostrar com l'última pregunta està molt relacionada amb les anteriors. Avancem alguna informació sobre les respostes possibles:

- Les dues primeres preguntes, adequadament formulades, són equivalents i molt sovint no tenen resposta positiva.
- Excepte en casos trivials, la resposta a la tercera pregunta és que no són únicament les estructures isomorfes a $\mathcal{M}$.

Donar *axiomes* per a una teoria vol dir escollir alguns dels seus enunciats de manera que els altres s'obtinguin a partir d'aquests com a *teoremes*, com a enunciats demostrats. En un sentit trivial, sempre és possible trobar un conjunt d'axiomes per a una teoria: n'hi ha prou amb prendre com a axiomes tots els enunciats de la teoria. Això, clarament, no té interès. Volem un conjunt simple d'axiomes, si és possible finit. Aquesta exigència es pot traduir en el fet que, almenys, es pugui determinar amb precisió, mitjançant algun algorisme, quins enunciats són axiomes i quins no ho són. Aquesta discussió pressuposa que tenim un context efectiu, és a dir, un context en el qual té sentit aplicar algorismes, i, per tant, els enunciats del llenguatge de primer ordre es donen de manera sintàcticament verificable i les llistes d'axiomes poden ser generades de manera computable. Direm que una teoria T és *axiomatitzable* si és possible donar una llista efectiva (generada per un algorisme) d'axiomes per a T. La teoria T és *decidible* si existeix algun algorisme aplicable als enunciats del llenguatge formal per a resoldre si són o no teoremes de T. Finalment, la teoria T és *completa* si, per a cada enunciat σ del llenguatge formal de T, o bé σ és un teorema de T o bé ho és $\neg\sigma$.

La teoria $\mathrm{Th}(\mathcal{M})$ d'una estructura $\mathcal{M}$ és sempre una teoria completa. Per a aquest tipus de teories, axiomatitzabilitat i decidibilitat són equivalents: es pot donar una llista efectiva d'axiomes si i només si hi ha un algorisme per a decidir quins enunciats són els seus teoremes. Això no passa, en general, amb teories incompletes. Per exemple, l'aritmètica de Peano de primer ordre, de la qual després parlarem detalladament, és axiomatitzable però indecidible. D'altra banda, encara que per a una teoria completa axiomatitzabilitat i decidibilitat són equivalents, no és obvi com es pot obtenir un bon conjunt d'axiomes a partir d'un algorisme de decisió per als teoremes, ni tampoc és obvi com es pot obtenir un bon algorisme de decisió per als teoremes a partir d'una llista efectiva d'axiomes.

Com és ben sabut, K. Gödel va demostrar el 1931 (vegeu [5]) que no és possible axiomatitzar l'aritmètica, és a dir, la teoria completa de $(\mathbb{N}, +, \cdot, <, 0, 1)$. L'aritmètica de Peano de primer ordre no és més que un fragment d'aquesta teoria. Contràriament a això, A. Tarski va mostrar el 1951 (vegeu [23] i [24]) que la teoria del cos dels números complexos sí que és decidible i també va demostrar la decidibilitat de la teoria del cos ordenat dels números reals. En el primer cas, la seva teoria és la dels cossos algebraicament tancats de característica zero, i en el segon, és la dels cossos ordenats reals tancats, és a dir, els cossos ordenats que satisfan el teorema del valor intermedi per a polinomis.

Pel que fa a la quarta pregunta, la descripció de les relacions definibles en casos concrets, el mètode més habitual està basat en l'*eliminació de quantificadors*. En general no és fàcil dir quines relacions són definibles en una estructura $\mathcal{M}$, però tenim moltes més opcions d'èxit caracteritzant les relacions definibles mitjançant fórmules sense quantificadors, ja que, al cap i a la fi, són simplement les combinacions booleanes de les relacions definibles mitjançant fórmules atòmiques. Que una teoria T tingui eliminació de quantificadors significa que per a cada $n \geq 1$ i cada fórmula $\varphi(x_1, \ldots, x_n)$ del llenguatge de T existeix una fórmula sense quantificadors $\psi(x_1, \ldots, x_n)$ per a la qual T implica $\forall x_1 \ldots x_n \ (\varphi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n))$. Si la teoria $\mathrm{Th}(\mathcal{M})$ té eliminació de quantificadors podem aspirar a solucionar el problema de la caracterització de les relacions definibles. Tarski va demostrar que les teories del cos complex i del cos real ordenat que acabem d'esmentar tenen eliminació de quantificadors. Gràcies a això, sabem quins són els subconjunts de $\mathbb{C}$ definibles a $(\mathbb{C}, +, -, \cdot, 0, 1)$: són els subconjunts finits i els seus complementaris. I els subconjunts definibles de $\mathbb{C}^n$ (les relacions n-àries definibles) són els conjunts construïbles de la topologia de Zariski. Pel que fa als números reals, els subconjunts de $\mathbb{R}$ definibles a $(\mathbb{R}, +, -, \cdot, <, 0, 1)$ són les unions finites d'intervals (incloent-hi semirectes) i punts. I les relacions n-àries definibles són els subconjunts semialgebraics de $\mathbb{R}^n$. En canvi, en el cas de $(\mathbb{N}, +, \cdot, <, 0, 1)$ no tenim eliminació de quantificadors i les relacions definibles són d'una gran complexitat.

De vegades la teoria de l'estructura $\mathcal{M}$ que ens interessa no té eliminació de quantificadors, però podem ampliar el llenguatge de manera natural, afegint-hi

relacions, operacions o elements definibles sense paràmetres, de manera que finalment s'obtingui una estructura la teoria de la qual tingui eliminació de quantificadors. I això pot bastar per a obtenir una caracterització raonable de les relacions definibles a $\mathcal{M}$. Això és el que passa en el cas del cos real $(\mathbb{R}, +, -, \cdot, 0, 1)$, ja que afegint la relació d'ordre $<$ s'obté el cos ordenat real, la teoria del qual sí que té eliminació de quantificadors.

4 Axiomatització

Ara especificarem alguns conjunts d'axiomes per a algunes teories d'interès especial. En tots els casos, l'axiomatització s'estableix en el llenguatge formal de la lògica de primer ordre. Comencem amb l'*aritmètica de Peano*, el sistema formal habitual per a l'aritmètica. Té els axiomes següents:

1. $\forall xy\ (x + 1 = y + 1 \to x = y)$.
2. $\forall x\ x + 1 \neq 0$.
3. $\forall x\ x + 0 = x$.
4. $\forall xy\ x + (y + 1) = (x + y) + 1$.
5. $\forall x\ x \cdot 0 = 0$.
6. $\forall xy\ x \cdot (y + 1) = (x \cdot y) + x$.
7. $\forall xy\ (x < y \leftrightarrow \exists z\ (x + z = y \wedge z \neq 0))$.
8. Principi d'inducció: per a cada fórmula $\varphi(x_1, \ldots, x_n, y)$

$$\forall x_1 \ldots x_n\ (\varphi(x_1, \ldots, x_n, 0) \wedge \forall y\ (\varphi(x_1, \ldots, x_n, y) \to \\ \to \varphi(x_1, \ldots, x_n, y + 1)) \to \forall y\, \varphi(x_1, \ldots, x_n, y)).$$

De vegades es prefereix usar la funció de successió $S(x) = x + 1$ en comptes del número 1 (definible per la seva banda com $1 = S(0)$) i es prefereix enunciar el sistema d'axiomes en el llenguatge $\{S, +, \cdot, 0, <\}$. Simplement cal canviar les expressions de la forma $t + 1$ per $S(t)$ en els axiomes. Els axiomes 1 i 2 especifiquen que S és una funció injectiva i que 0 no forma part del seu recorregut. Els axiomes 3 i 4 donen la definició recursiva de la suma, i els axiomes 5 i 6, la definició recursiva del producte. L'ordre $<$ s'introdueix a l'axioma 7 mitjançant una definició explícita. De fet, l'ordre és perfectament prescindible, i podríem presentar l'aritmètica sense tenir-lo en compte.

A l'axioma 8 es presenta el principi d'inducció en forma d'esquema axiomàtic. Hi ha tantes instàncies particulars de l'axioma com fórmules del llenguatge de primer ordre. No pot substituir-se per un únic axioma que quantifiqui sobre conjunts de números naturals ja que, com hem indicat, en el llenguatge de primer ordre només podem quantificar sobre elements de l'univers de l'estructura. Els matemàtics sovint estan acostumats a formular el principi d'inducció mitjançant un únic axioma que quantifica sobre conjunts de números naturals, però aquesta forma del principi d'inducció no pot expressar-se en la lògica de primer ordre; la seva formulació pertany a la teoria de conjunts o a la

lògica de segon ordre. D'altra banda, reflexionant-hi una mica, es veu que les aplicacions habituals del principi d'inducció en la demostració de teoremes aritmètics, encara que aparentment s'efectuïn per a subconjunts arbitraris de $\mathbb{N}$, en realitat es fan per a subconjunts definibles i són, per això, casos particulars del nostre esquema 8.

Com ja hem avançat abans, Gödel va demostrar que aquest sistema d'axiomes de l'aritmètica de Peano és insuficient per a l'aritmètica completa, no és una llista d'axiomes per a $\mathrm{Th}(\mathbb{N}, +, \cdot, <, 0, 1)$. No obstant això, sí que serveix per a la gran majoria dels problemes aritmètics habituals, i no és fàcil trobar enunciats aritmètics certs que no poden ser obtinguts com a teoremes seus. Atès que no és una teoria completa, no es pot concloure la decidibilitat de l'aritmètica de Peano a partir de la seva axiomatitzabilitat. Ja s'ha comentat abans que a més és una teoria indecidible. És clar quins són els axiomes, però no hi ha cap algorisme que ens serveixi per a dir quins són els seus teoremes.

Fixem-nos en la teoria de cossos, i en particular en els cossos real i complex. És habitual en teoria de models tractar els cossos en el llenguatge d'anells $\{+, -, \cdot, 0, 1\}$ i la teoria de cossos ordenats en el llenguatge d'anells ordenats $\{+, -, \cdot, <, 0, 1\}$. No tenim, per tant, l'operació de divisió disponible de manera explícita, tot i que indirectament puguem parlar-ne. No s'hi podria afegir de manera immediata, ja que és una operació parcial. Podria afegir-s'hi definint la divisió per zero d'una manera arbitrària. Però no hi ha cap necessitat de fer-ho, simplement n'hi ha prou amb el llenguatge d'anells per a tots els propòsits, i tot és més simple en aquest llenguatge.

La *teoria de cossos* té una llista senzilla i bastant previsible d'axiomes. N'hi ha prou amb especificar que $0 \neq 1$, que $+$ i $\cdot$ són operacions associatives i commutatives, que $\cdot$ és distributiva respecte a $+$, que 0 és l'element neutre en la suma i que $-x$ és l'oposat de x respecte de la suma, que 1 és l'element neutre del producte i que tot element diferent de zero té un invers respecte del producte. Ens estalviem donar la llista d'aquests axiomes, que són coneguts de sobres.

La teoria de *cossos algebraicament tancats* s'obté afegint a la teoria de cossos els axiomes que garanteixen l'existència de zeros de tots els polinomis no constants. Això pot aconseguir-se amb els enunciats següents per a cada $n \geq 1$:

$$\forall y_0 \dots y_n \left(y_n \neq 0 \to \exists x \sum_{i=0}^{n} y_i x^i = 0 \right).$$

Observem que en aquesta última fórmula la potència x^i és una abreviació del producte de x amb si mateix i vegades, mentre que el subíndex de y_i és el que correspon a l'enumeració de les variables $y_0, \dots, y_n$.

La teoria dels *cossos algebraicament tancats de característica un número primer* p, ACF_p, s'obté afegint a més l'axioma que determina la característica:

$$\varphi_p := \underbrace{1 + 1 + \cdots + 1}_{p \text{ vegades}} = 0.$$

La teoria dels *cossos algebraicament tancats de característica zero*, ACF_0, s'obté afegint a la teoria de cossos algebraicament tancats els axiomes $\neg\varphi_p$ per a cada primer p.

ACF_0 és la teoria del cos complex i ACF_p és la teoria del cos $\widetilde{\mathbb{F}_p}$, la clausura algebraica del cos de p elements $\mathbb{F}_p$. Són, per tant, teories completes axiomatitzables i per això teories decidibles.

La teoria de *cossos reals tancats* pot formular-se en el llenguatge d'anells o en el d'anells ordenats. La versió sense ordre és la teoria RCF, que s'axiomatitza afegint a la teoria de cossos els axiomes següents:

1. $\forall x_1 \dots x_n \; x_1^2 + \cdots + x_n^2 \neq -1$ per a cada $n \geq 1$.
2. $\forall x \exists y \; (y^2 = x \vee y^2 = -x)$.
3. $\forall y_0 \dots y_{2n+1} \; (y_{2n+1} \neq 0 \to \exists x \sum_{i=0}^{2n+1} y_i x^i = 0)$ per a $n \geq 0$.

No és necessari especificar la característica, ja que els axiomes de l'apartat 1 ja impliquen que no pot ser un número primer. Els cossos en els quals valen aquests axiomes es diuen *formalment reals*. A l'apartat 2 es postula l'existència d'arrels quadrades i a l'apartat 3 es garanteix l'existència de zeros de polinomis de grau senar.

RCF és la teoria de $(\mathbb{R}, +, -, \cdot, 0, 1)$. Com en el cas del cos complex, va ser Tarski qui ho va demostrar. I com en el cas complex, la teoria és completa i axiomatitzable i per això decidible.

Considerem ara la teoria del cos real amb ordre, que té l'avantatge d'eliminar els quantificadors. La teoria $RCOF$ del cos ordenat real $(\mathbb{R}, +, -, \cdot, <, 0, 1)$ es pot axiomatitzar afegint simplement a RCF la definició explícita de l'ordre:

$$\forall x y \; (x < y \leftrightarrow x \neq y \wedge \exists z \, x + z^2 = y).$$

Alternativament podem axiomatitzar $RCOF$ partint de la teoria de *cossos ordenats*, que té els axiomes següents addicionals als de la teoria de cossos:

1. $\forall x \; x \not< x$.
2. $\forall x y z \; (x < y \wedge y < z \to x < z)$.
3. $\forall x y \; (x < y \vee x = y \vee y < x)$.
4. $\forall x y z \; (x < y \to x + z < y + z)$.
5. $\forall x y z \; (x < y \wedge 0 < z \to x \cdot z < y \cdot z)$.

S'afegeixen llavors axiomes que garanteixen que tot polinomi que passa de positiu a negatiu en un interval té un zero en l'interval. Això es pot aconseguir amb els axiomes següents per a cada $n \geq 0$:

$$\forall y_0 \dots y_n \, \forall x_1 x_2 \left(x_1 < x_2 \wedge \sum_{i=0}^{n} y_i x_1^i > 0 \wedge \sum_{i=0}^{n} y_i x_2^i < 0 \to \right.$$
$$\left. \to \exists x \left(x_1 < x \wedge x < x_2 \wedge \sum_{i=0}^{n} y_i x^i = 0 \right) \right).$$

Les demostracions de la decidibilitat d'aquestes teories de cossos que es van donar originàriament es basaven en mètodes efectius d'eliminació de quantificadors.

5 Definibilitat

Ara comentarem amb més detall algunes qüestions de definibilitat. La manera més directa d'explicar què significa que una relació, una operació o un element d'una estructura sigui definible és apel·lant a les fórmules del llenguatge formal de primer ordre que es poden fer servir per a donar les definicions.

Una relació $R \subseteq M^n$ és *definible* a $\mathcal{M}$ sobre el conjunt $A \subseteq M$ (és A-definible a $\mathcal{M}$) si hi ha una fórmula $\varphi(x_1, \ldots, x_n)$ en el llenguatge ampliat amb noms per als elements de A tal que

$$R = \{(a_1, \ldots, a_n) \in M^n \mid \mathcal{M} \vDash \varphi(a_1, \ldots, a_n)\},$$

és a dir, R està formada per les ènuples de M que satisfan la fórmula a $\mathcal{M}$. En el cas d'una operació, es diu que és definible si ho és el seu graf i, finalment, diem que un element a és definible si ho és el seu conjunt unitari $\{a\}$. Es diu que els elements de A que apareixen en la fórmula són *paràmetres* de la definició.

De vegades no fem servir paràmetres en les definicions. Una relació, operació o individu és *definible sense paràmetres* a $\mathcal{M}$ si és A-definible per al cas $A = \emptyset$. Això significa simplement que en la fórmula $\varphi(x_1, \ldots, x_n)$ que usem per a definir no fem servir cap nom addicional. Hi ha una gran diferència entre definir amb paràmetres o sense. Per exemple, tot conjunt finit $\{a_1, \ldots, a_n\}$ és definible amb paràmetres en qualsevol estructura que contingui els seus elements: n'hi ha prou amb considerar la disjunció $(x = a_1 \vee \cdots \vee x = a_n)$; però no és normal que els conjunts finits puguin definir-se sense paràmetres.

La definibilitat està molt relacionada amb la invariància. Una relació, una operació o un individu són *invariants* a $\mathcal{M}$ si els automorfismes de $\mathcal{M}$ els respecten. Les relacions, operacions i individus definibles sense paràmetres són invariants, però el recíproc no és cert en general. En comentarem algun exemple més endavant, i també donarem exemples en els quals la invariància i la definibilitat sense paràmetres coincideixen. En general, podem fer servir que una relació no és invariant per a demostrar que no és definible sense paràmetres.

És possible també caracteritzar les relacions definibles en una estructura sense necessitat d'utilitzar el llenguatge formal. Es pot evitar la lògica i, en lloc d'introduir la noció de definibilitat mitjançant fórmules i mitjançant la relació $\vDash$ de satisfacció (com acabem de fer), podem adoptar la presentació següent de la definibilitat:

Sigui $\mathcal{M} = (M, R_1, R_2, \ldots, f_1, f_2, \ldots, c_1, c_2, \ldots)$ una estructura i sigui $A \subseteq M$. Es pot veure fàcilment que les relacions $R \subseteq M^n$ A-definibles a $\mathcal{M}$ són els elements de D_n, on $(D_n \mid n \in \mathbb{N}, n > 0)$ és la menor col·lecció de subconjunts $D_n \subseteq \mathcal{P}(M^n)$ tal que:

1. $\{a\} \in D_1$ per a cada $a \in A$ i $\{c_1\}, \{c_2\}, \ldots \in D_1$.
2. $R_i \in D_n$ si $R_i \subseteq M^n$.
3. $f_i \in D_{n+1}$ si $f_i \colon M^n \to M$.
4. $\{(a, a) \mid a \in M\} \in D_2$.

5. Cada D_n és tancat respecte de les operacions booleanes: si $R, S \in D_n$, aleshores
$$R \cap S, \quad R \cup S, \quad R \setminus S \in D_n.$$

6. Si $R \in D_{n+1}$, aleshores
$$\mathrm{dom}(R) = \{(a_1, \ldots, a_n) \mid (a_1, \ldots, a_n, b) \in R \text{ per a algun } b \in M\} \in D_n.$$

7. Si $R \in D_n$, aleshores
$$R \times M = \{(a_1, \ldots, a_n, b) \mid b \in M \text{ i } (a_1, \ldots, a_n) \in R\} \in D_{n+1}.$$

8. Si $R \in D_n$ i π és una permutació de $\{1, \ldots, n\}$, aleshores
$$R_\pi = \{(a_{\pi(1)}, \ldots, a_{\pi(n)}) \mid (a_1, \ldots, a_n) \in R\} \in D_n.$$

Observeu que 1–4 especifiquen només que unes determinades relacions són A-definibles, mentre que 5–8 donen procediments per a obtenir relacions A-definibles a partir d'altres relacions A-definibles. Les relacions A-definibles 1–4 són la igualtat, les relacions pròpies de $\mathcal{M}$, els grafs de les seves operacions i els conjunts unitaris, tant dels elements de A com dels elements destacats de $\mathcal{M}$. Els procediments de generació de noves relacions A-definibles són operacions booleanes, projeccions (o dominis), productes cartesians i reordenacions d'ènuples associades a permutacions d'índexs.

Considerem alguns exemples de definibilitat sense paràmetres en estructures familiars. És clar que 0 és definible a $(\mathbb{N}, S)$ mitjançant la fórmula $\forall y\ \neg S(y) = x$. I llavors cada número natural també és definible: n'hi ha prou amb aplicar S a 0 el nombre adequat de vegades. Però 0 no és definible sense paràmetres a $(\mathbb{Z}, S)$, ja que no és invariant: hi ha automorfismes d'aquesta estructura que transformen 0 en qualsevol altre enter. El mateix passa amb els altres enters, cap és definible sense paràmetres.

A $(\mathbb{N}, +)$ sí que es pot definir sense paràmetres el zero, i a més l'ordre i cada número natural: 0 es defineix mitjançant $x + x = x$, l'ordre $x < y$ es defineix amb $\exists z\ (x + z = y \wedge z \neq 0)$, el número 1 es defineix amb $0 < x \wedge \neg\exists y\ (0 < y \wedge y < x)$ i cada número natural $n \geq 2$ es defineix amb $x = 1 + \cdots + 1$ (n vegades). Una conseqüència del fet que puguem definir sense paràmetres el zero, l'ordre i l'u és que no només la teoria de $(\mathbb{N}, +, \cdot, <, 0, 1)$ no és axiomatitzable, sinó que tampoc ho és la de $(\mathbb{N}, +, \cdot)$. En general, si les relacions, operacions i elements destacats d'una estructura $\mathcal{M}$ són definibles sense paràmetres en una altra estructura $\mathcal{N}$ que té el mateix univers, llavors l'axiomatitzabilitat de $\mathrm{Th}(\mathcal{N})$ implica l'axiomatitzabilitat de $\mathrm{Th}(\mathcal{M})$.

No tots els resultats sobre definibilitat es resolen de manera senzilla, exhibint una fórmula breu. Per exemple, Gödel va mostrar el 1931 a [5] que l'exponenciació (igual que totes les funcions recursives) és definible sense paràmetres a $(\mathbb{N}, +, \cdot)$, però la fórmula que la defineix ni és breu ni s'entén bé sense explicacions addicionals.

6 Aritmètica

L'aritmètica de la suma i el producte té una gran complexitat: no podem axiomatitzar-la ni donar un algorisme que decideixi quins són els enunciats aritmètics que són certs. No obstant això, si prescindim del producte i ens quedem únicament amb la suma, les coses canvien radicalment. M. Presburger va mostrar el 1930 (vegeu [12]) que la teoria de $(\mathbb{N}, +)$ és decidible. I a més va indicar com es pot ampliar el llenguatge formal mitjançant definicions de manera que hi hagi eliminació de quantificadors. La teoria es diu *aritmètica de Presburger* en el seu honor.

L'aritmètica de Presburger té eliminació de quantificadors si s'afegeixen al llenguatge 0, 1, $<$ i les relacions (també definibles sense paràmetres) de congruència mòdul n per a cada natural $n \geq 2$. La relació de congruència $\equiv_n$ es defineix a $(\mathbb{N}, +)$ mitjançant la fórmula $\varphi(x, y)$ següent:

$$\exists z\,(x = y + \underbrace{z + \cdots + z}_{n \text{ vegades}}) \vee \exists z\,(y = x + \underbrace{z + \cdots + z}_{n \text{ vegades}}).$$

Un sistema d'axiomes per a l'aritmètica de Presburger s'obté restringint l'axiomàtica de l'aritmètica de Peano al llenguatge $\{+, 0, 1\}$, eliminant la definició recursiva del producte i, si es vol tenir eliminació de quantificadors, fent servir les definicions de l'ordre $<$ i de les congruències $\equiv_n$.

Un altre fragment tractable de l'aritmètica és l'aritmètica del producte. Th. Skolem va demostrar el 1930 (vegeu [22] i [2]) que la teoria de $(\mathbb{N}, \cdot)$ és decidible (i, per tant, axiomatitzable). En conseqüència, la suma no és definible sense paràmetres a $(\mathbb{N}, \cdot)$ i el producte no ho és a $(\mathbb{N}, +)$. Observeu que, no obstant això, el producte és invariant a $(\mathbb{N}, +)$. J. Robinson va demostrar el 1949 a [15] que la suma és definible sense paràmetres a $(\mathbb{N}, \cdot, S)$ i a $(\mathbb{N}, \cdot, <)$, i, per tant, les teories d'aquestes estructures no són axiomatitzables; també va demostrar que la suma i el producte són definibles a partir de l'operació S de successor i de la relació de divisibilitat. Per a definir la suma $x + y = z$ a $(\mathbb{N}, \cdot, S)$ es pot utilitzar la fórmula

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

Com que S és definible a partir de l'ordre, això explica que també la suma pugui definir-se a $(\mathbb{N}, \cdot, <)$.

J. L. Lagrange va establir el 1770 que tot número natural és suma de quatre quadrats. Una conseqüència és que el conjunt $\mathbb{N}$ dels números naturals és definible sense paràmetres a $(\mathbb{Z}, +, \cdot)$ i, per tant, la seva teoria no és axiomatitzable. Més recentment, el 1949, Robinson va demostrar que $\mathbb{N}$ és definible sense paràmetres en el cos $(\mathbb{Q}, +, \cdot, -, 0, 1)$ i, per tant, la teoria d'aquest cos tampoc és axiomatitzable (vegeu [15]). En general, si l'univers d'una estructura $\mathcal{M}$ és definible sense paràmetres en una estructura $\mathcal{N}$ i les operacions, relacions i constants de $\mathcal{M}$ són també definibles sense paràmetres a $\mathcal{N}$ (per exemple, si són la restricció de les de $\mathcal{N}$ a l'univers M de $\mathcal{M}$), llavors l'axiomatitzabilitat de $\mathcal{N}$ implica l'axiomatitzabilitat de $\mathcal{M}$.

El número 1 no és definible sense paràmetres a $(\mathbb{Z}, +)$ (ja que no és invariant), però el número 0 sí que ho és; tampoc són definibles $<$ i $\mathbb{N}$ en no ser invariants. Si hi afegim el número 1, les coses canvien. L'ordre enter $<$ segueix sense ser definible sense paràmetres a $(\mathbb{Z}, +, 0, 1)$, però ja no podem fer servir l'argument que no és invariant. De fet, és invariant. La raó per la qual no es pot definir l'ordre en aquest cas és més profunda. Les teories de $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}, +, 0, 1)$ i $(\mathbb{Z}, +, <, 0, 1)$ són axiomatitzables, són variacions de l'aritmètica de Presburger. Però en els dos primers casos les teories són *estables*, i una de les característiques de les teories estables és que no s'hi pot definir cap ordre no trivial. En tots tres casos és possible obtenir eliminació de quantificadors si s'hi afegeix l'aplicació $a \mapsto -a$ i les relacions de congruència $\equiv_n$, totes definibles sense paràmetres.

Resumint la situació que hem trobat en l'aritmètica:

- Són axiomatitzables (i decidibles) les teories de $(\mathbb{N}, +)$, de $(\mathbb{N}, \cdot)$, de $(\mathbb{Z}, +)$, de $(\mathbb{Z}, +, 1)$ i de $(\mathbb{Z}, +, <, 1)$.
- No són axiomatitzables (ni decidibles) les teories de $(\mathbb{N}, +, \cdot)$, de $(\mathbb{N}, \cdot, S)$, de $(\mathbb{N}, \cdot, <)$, de $(\mathbb{Z}, +, \cdot)$ ni de $(\mathbb{Q}, +, \cdot, -, 0, 1)$.

7 Cossos

Ja hem comentat que quan una teoria té eliminació de quantificadors sol ser relativament senzill descriure les seves relacions definibles, ja que habitualment les fórmules sense quantificació són manejables i comprensibles. En el context de la teoria de cossos hi ha nombrosos resultats d'eliminació de quantificadors. En els casos més notables l'eliminació té lloc directament en el llenguatge d'anells o en el llenguatge d'anells ordenats.

Tarski va demostrar el 1951 a [24] que la teoria del cos complex $(\mathbb{C}, +, \cdot, -, 0, 1)$ (la teoria ACF_0 dels cossos algebraicament tancats de característica zero) té eliminació de quantificadors. A. Macintyre va demostrar el 1971 a [7] que si la teoria d'un cos té eliminació de quantificadors en el llenguatge d'anells, el cos és algebraicament tancat. Tarski va demostrar també el 1951 que la teoria de $(\mathbb{R}, +, \cdot, -, <, 0, 1)$ (la teoria $RCOF$ dels cossos ordenats reals tancats) té eliminació de quantificadors. L'ordre $<$ és necessari per a això. A. Macintyre, K. McKenna i L. van den Dries van demostrar el 1983 (vegeu [8]) que aquest és fonamentalment l'únic cas: si la teoria d'un cos ordenat té eliminació de quantificadors en el llenguatge d'anells ordenats, el cos és real tancat.

Ni $\mathbb{N}$ ni $\mathbb{Z}$ ni $\mathbb{Q}$ són definibles sense paràmetres a $(\mathbb{R}, +, \cdot, -, 0, 1)$. Si ho fossin, la complexitat lògica de l'aritmètica l'heretarien els números reals i la seva teoria no seria axiomatitzable. Pel mateix motiu, tampoc són definibles sense paràmetres a $(\mathbb{C}, +, \cdot, -, 0, 1)$. Però, per un altre motiu, sabem fins i tot que aquests conjunts tampoc es poden definir en aquests cossos amb l'ajuda de paràmetres. La raó és que, gràcies a l'eliminació de quantificadors, coneixem molt bé els conjunts que es poden definir amb paràmetres en aquest tipus d'estructures: són únicament els conjunts finits i els cofinits en el cos complex

i són les unions finites d'intervals i de punts en el cos real. Però d'això en parlarem més endavant.

Curiosament, $\mathbb{Z}$ sí que és definible sense paràmetres en el cos exponencial complex $(\mathbb{C}, +, \cdot, -, e^x, 0, 1)$ i, per tant, la seva teoria no és axiomatitzable. Es pot definir $\mathbb{Z}$ amb la fórmula $\varphi(x)$ següent:

$$\forall y z\, (z \cdot z = -1 \wedge e^{y \cdot z} = 1 \rightarrow e^{x \cdot y \cdot z} = 1).$$

8 Categoricitat

Ens centrarem ara en la tercera de les preguntes que hem formulat al principi, la relativa a l'isomorfisme i l'equivalència elemental. La qüestió més immediata és si les teories completes de primer ordre determinen, excepte isomorfisme, els seus models i les estructures que les satisfan. També aquí la definibilitat hi té alguna cosa a veure.

Necessitem parlar una mica de cardinalitats infinites per a poder parlar de categoricitat, però ens limitarem als prerequisits mínims. Dos conjunts A, B tenen la mateixa grandària o cardinalitat ($|A| = |B|$) quan existeix una bijecció entre ells. L'ordre $|A| \leq |B|$ entre cardinalitats es defineix per l'existència d'una funció injectiva de A a B. Els números cardinals $0, 1, 2, \ldots, \aleph_0, \aleph_1, \ldots$ comencen amb els números naturals i continuen amb les cardinalitats dels conjunts infinits. El menor número cardinal infinit és $\omega = \aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. A cada cardinal el segueix immediatament un altre en l'ordre. El successor de $\aleph_0$ és $\omega_1 = \aleph_1$, el primer cardinal no numerable. El cardinal del continu és $|\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0} \geq \aleph_1$. Un text bàsic i clar sobre aquests temes és [4].

No passa mai que tots els models d'una teoria completa siguin isomorfs entre si, tret que estiguem en el cas trivial (a aquest efecte) de la teoria d'una estructura finita. En altres paraules, només les teories de les estructures finites són categòriques. Això és degut al teorema de Löwenheim-Skolem: si $\mathcal{M}$ és una estructura infinita, llavors per a cada cardinal infinit κ hi ha una estructura $\mathcal{N}$ de cardinalitat κ tal que $\mathcal{M} \equiv \mathcal{N}$. Versions parcials d'aquest teorema es deuen a L. Löwenheim (1915) i T. Skolem (1928), però la versió completa és posterior i té aportacions d'A. Tarski. Com que la teoria de $\mathcal{M}$ té models de cardinalitats infinites diverses, té models no isomorfs per raons molt poderoses. Podem considerar casos concrets. Per exemple, se sap que $(\mathbb{R}, +, <, 0) \equiv (\mathbb{Q}, +, <, 0)$ però (per raons de cardinalitat) $(\mathbb{R}, +, <, 0) \not\cong (\mathbb{Q}, +, <, 0)$. De manera similar, si $\widetilde{\mathbb{Q}}$ és la clausura algebraica de $\mathbb{Q}$, $(\mathbb{C}, +, \cdot, -, 0, 1) \equiv (\widetilde{\mathbb{Q}}, +, \cdot, -, 0, 1)$ i, altra vegada per raons de cardinalitat, $(\mathbb{C}, +, \cdot, -, 0, 1) \not\cong (\widetilde{\mathbb{Q}}, +, \cdot, -, 0, 1)$.

Un succedani força satisfactori de la categoricitat és la categoricitat en cardinal. Diem que una teoria és *κ-categòrica* si té algun model de cardinalitat κ i tots els seus models de cardinalitat κ són isomorfs. M. Morley va demostrar el 1965 a [10] que una teoria T és categòrica en un cardinal $\geq \aleph_1$ si i només si és categòrica en tots els cardinals $\geq \aleph_1$. Per tant, les opcions es redueixen a $\aleph_0$-categoricitat i $\aleph_1$-categoricitat (categoricitat en tots els cardinals $\geq \aleph_1$). Un exemple de teoria $\aleph_0$-categòrica i $\aleph_1$-categòrica el constitueixen els espais

vectorials infinits sobre $\mathbb{F}_p$. Els espais vectorials es tracten de dues maneres alternatives en la teoria de models. La primera opció seria considerar que l'univers és la unió dels vectors amb els elements del cos, afegint-hi un predicat per separar-los. Segons la segona opció, que és la més habitual i és la que aquí considerem, l'univers estaria format exclusivament pels vectors. Els elements del cos intervenen indirectament, mitjançant les operacions de producte per un escalar. Les operacions són la suma de vectors i els productes $v \mapsto \lambda \cdot v$ associats als elements λ del cos.

Existeixen teories no $\aleph_0$-categòriques però sí $\aleph_1$-categòriques, per exemple, la teoria dels cossos algebraicament tancats de característica zero o la dels espais vectorials sobre $\mathbb{Q}$. També hi ha teories $\aleph_0$-categòriques que no són $\aleph_1$-categòriques. L'ordre dens sense extrems, que és tant la teoria de $(\mathbb{Q}, <)$ com la de $(\mathbb{R}, <)$, i la teoria de les àlgebres de Boole sense àtoms en són dos exemples. Finalment, hi ha també teories que no són categòriques en cap cardinal, com la teoria *RCF* dels cossos reals tancats.

Se saben força coses de les teories $\aleph_0$-categòriques. Hi ha un resultat cèlebre que C. Ryll-Nardzewski va demostrar el 1959 a [17] i que les caracteritza en termes del nombre de relacions definibles que tenen:

Les condicions següents són equivalents per a una teoria $T = \mathrm{Th}(\mathcal{M})$:

1. T és $\aleph_0$-categòrica.
2. Per a cada $n \geq 1$, només hi ha un nombre finit de relacions $R \subseteq M^n$ que siguin definibles sense paràmetres a $\mathcal{M}$.
3. Per a cada $A \subseteq M$ finit, només hi ha un nombre finit de subconjunts $X \subseteq M$ que siguin A-definibles a $\mathcal{M}$.

Es pot demostrar a partir d'això que si $\mathcal{M}$ és una estructura numerable i la seva teoria és $\aleph_0$-categòrica, llavors tota relació invariant de $\mathcal{M}$ és definible a $\mathcal{M}$ sense paràmetres.

Veurem en la secció següent que també l'anàlisi de les relacions definibles té a veure amb la $\aleph_1$-categoricitat.

9 Minimalitat i o-minimalitat

Es diu que l'estructura $\mathcal{M}$ és *minimal* si tots els subconjunts del seu univers M que són definibles amb paràmetres són o bé finits o bé cofinits. Observeu que això significa que només es poden definir els conjunts que en qualsevol cas són definibles sempre (amb ajuda del símbol d'igualtat). D'altra banda, les estructures minimals poden tenir relacions enàries definibles de gran complexitat per a $n \geq 2$; només s'imposa una limitació en el cas $n = 1$. Una estructura $\mathcal{M}$ és *fortament minimal* quan és minimal i també ho és tota estructura $\mathcal{N} \equiv \mathcal{M}$. Per exemple, $(\mathbb{N}, <)$ és minimal, però no és fortament minimal. Una teoria és fortament minimal si els seus models ho són, és a dir, si en els seus models els únics conjunts definibles amb paràmetres són els finits i els cofinits. W. Marsh va demostrar el 1966 que les teories fortament minimals són $\aleph_1$-categòriques. Aquest resultat va ser incorporat a l'article [1] de J. T. Baldwin i A. H. Lachlan.

Entre les teories que hem considerat hi ha exemples que són fortament minimals. L'exemple més elemental és el de la teoria d'un conjunt infinit. En aquest cas l'estructura es redueix al seu univers, no hi ha més relacions que la igualtat i no hi ha operacions ni elements destacats. També la teoria de qualsevol espai vectorial és fortament minimal. I ho són també les teories ACF_0 i ACF_p de cossos algebraicament tancats, les teories del successor en els números naturals i en els enters, $\mathrm{Th}(\mathbb{N}, S)$ i $\mathrm{Th}(\mathbb{Z}, S)$, i la teoria dels grups abelians sense torsió $\mathrm{Th}(\mathbb{Q}, +) = \mathrm{Th}(\mathbb{R}, +)$.

La minimalitat té altres conseqüències estructurals. J. Reineke va demostrar el 1975 a [13] que tot grup minimal és abelià. A. Macintyre va demostrar el 1971 a [7] que tot cos amb teoria $\aleph_1$-categòrica és algebraicament tancat i per això fortament minimal. Hi ha una conjectura oberta sobre aquest tema, la conjectura de Podewski, segons la qual tot cos minimal és algebraicament tancat. F. O. Wagner va demostrar el 2000 a [28] que la conjectura de Podewski és certa quan la característica és un número primer.

Les estructures ordenades no són mai fortament minimals. Però hi ha una noció anàloga a la minimalitat que s'adapta de manera natural a les estructures totalment ordenades: la *o-minimalitat*. Va ser introduïda per A. Pillay i C. Steinhorn el 1986 a [11] inspirant-se en uns treballs previs de Lou van den Dries, i avui en dia constitueix una àrea autònoma de la teoria de models, estretament associada a la geometria algebraica real. Un text de referència és [27].

Una estructura totalment ordenada és *o-minimal* si els únics conjunts definibles amb paràmetres són unions finites d'intervals (incloent-hi semirectes) i punts. Això significa que els conjunts definibles són els que serien en qualsevol cas definibles si tinguéssim eliminació de quantificadors en el llenguatge de l'ordre. A diferència del que passa en el cas minimal, si una estructura és o-minimal, totes les estructures que li són equivalents també ho són i es diu que la seva teoria completa és o-minimal. Per tant, no té sentit distingir entre o-minimal i fortament o-minimal. Són estructures o-minimals l'ordre dels racionals $(\mathbb{Q}, <)$ i el cos ordenat dels números reals $(\mathbb{R}, +, -, \cdot, <, 0, 1)$. No obstant, l'aritmètica dels enters $(\mathbb{Z}, +, -, \cdot, <, 0, 1)$ no és o-minimal. A. Pillay i C. Steinhorn van demostrar el 1986 que si un anell ordenat és o-minimal, llavors és elementalment equivalent al cos ordenat real.

Tarski va plantejar el 1967 si la teoria del cos exponencial real $(\mathbb{R}, +, -, \cdot, e^x, <, 0, 1)$ és axiomatitzable. El 1996 A. J. Wilkie va demostrar que $(\mathbb{R}, +, -, \cdot, e^x, <, 0, 1)$ és o-minimal (vegeu [30]). La conjectura de Schanuel per als reals diu que si $r_1, \ldots, r_n \in \mathbb{R}$ són linealment independents sobre $\mathbb{Q}$, el grau de transcendència de $\mathbb{Q}(r_1, \ldots, r_n, e^{r_1}, \ldots, e^{r_n})$ sobre $\mathbb{Q}$ és major o igual que n. A. Macintyre i A. J. Wilkie van demostrar el 1996 a [9] que si la conjectura de Schanuel és certa, la teoria de $(\mathbb{R}, +, -, \cdot, e^x, <, 0, 1)$ és axiomatitzable. Però aquesta conjectura està lluny de ser resolta. L. van den Dries va mostrar el 1984 a [26] que la teoria de $(\mathbb{R}, +, -, \cdot, e^x, <, 0, 1)$ no té eliminació de quantificadors i A. J. Wilkie va demostrar a [30] que és *model-completa*, és a dir, que tota fórmula és equivalent a una fórmula de la forma $\exists y_1, \ldots, y_m \, \varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, on a φ no hi ha quantificadors. La model-completitud és una condició sobre

la complexitat de les relacions definibles no tan bona com l'eliminació de quantificadors, però prou satisfactòria en molts casos.

10 Dimensió i estabilitat

Els models de les teories fortament minimals i els de les teories o-minimals tenen una dimensió que es defineix en termes de geometria combinatòria.

Un *operador de clausura finitari* és un conjunt X juntament amb una operació cl que assigna a cada subconjunt A de X un altre subconjunt $cl(A)$ de X (la seva *clausura*) i compleix les condicions següents:

1. $A \subseteq cl(A)$.
2. Si $A \subseteq B$, aleshores $cl(A) \subseteq cl(B)$.
3. $cl(cl(A)) \subseteq cl(A)$.
4. Si $a \in cl(A)$, aleshores existeix $A_0 \subseteq A$ finit tal que $a \in cl(A_0)$.

Una *pregeometria* és un operador de clausura finitari que compleix addicionalment la *condició d'intercanvi*: si $a, b \in X$ i $a \in cl(A \cup \{b\}) \setminus cl(A)$, llavors $b \in cl(A \cup \{a\})$. En una pregeometria diem que $a \in X$ és *independent* de $A \subseteq X$ si $a \notin cl(A)$. Diem que $A \subseteq X$ és *independent* si cada $a \in A$ és independent de $A \setminus \{a\}$. Una *base* de $A \subseteq X$ és un subconjunt independent maximal de A. Totes les bases de A tenen el mateix cardinal, que es diu *dimensió* de A.

La *clausura algebraica* d'un subconjunt A d'una estructura $\mathcal{M}$ és el conjunt $acl(A) \subseteq M$ format pels elements de M que pertanyen a algun conjunt finit definit mitjançant una fórmula amb paràmetres en A. La terminologia està motivada pel paral·lelisme que hi ha amb la clausura algebraica en un cos, obtinguda afegint zeros de polinomis. L'univers M amb l'operació acl és un cas particular d'operador de clausura finitari. Si $\mathcal{M}$ és fortament minimal o és o-minimal, la clausura algebraica acl compleix la condició d'intercanvi i, per tant, defineix una pregeometria a M. En el context o-minimal, la clausura algebraica $acl(A)$ coincideix a més amb la *clausura definible* $dcl(A)$, que és la col·lecció dels elements de M que són A-definibles. Per tant, en les estructures fortament minimals i en les estructures o-minimals tenim una dimensió algebraica (és a dir, provinent de l'operador acl de clausura algebraica) ben definida.

En una estructura fortament minimal $\mathcal{M}$, la dimensió algebraica és un invariant que determina l'isomorfisme: si $\mathcal{N} \equiv \mathcal{M}$, llavors $\mathcal{M} \cong \mathcal{N}$ si i només si $\mathcal{M}$ i $\mathcal{N}$ tenen la mateixa dimensió. Això explica per què les teories fortament minimals són $\aleph_1$-categòriques: la dimensió d'un model de cardinalitat $\aleph_1$ ha de ser $\aleph_1$.

En una estructura o-minimal, la dimensió no és suficient per a determinar l'isomorfisme. Se sap que si $\mathcal{M}$ és una estructura ordenada, per a cada cardinal $\kappa \geq \aleph_1$, existeixen 2^κ estructures de cardinalitat κ que són elementalment equivalents a $\mathcal{M}$ però no són isomorfes entre si.

La diferència de comportament de la dimensió entre les teories fortament minimals i les o-minimals té a veure amb el fet que les primeres són *teories estables*, mentre que les segones són inestables. Una manera de definir l'estabilitat d'una teoria és en termes de la inexistència de determinats grafs: una teoria és estable si en cap dels seus models $\mathcal{M}$ existeix una relació definible R que ordeni totalment un subconjunt infinit $X \subseteq M^n$, és a dir, el graf que R defineix en el conjunt d'ènuples de X és un ordre total d'aquest conjunt X. Però el conjunt X mateix no ha de ser necessàriament definible i pot ser que la relació R no defineixi ni tan sols un ordre a M^n. Òbviament, qualsevol estructura que tingui un ordre definible no trivial té una teoria inestable. La noció de teoria estable i, per tant, la teoria de l'estabilitat, va ser introduïda per S. Shelah el 1969 a [18]. L'obra fonamental sobre l'estabilitat és el llibre [20] de Shelah. La teoria de l'estabilitat és un conjunt de nocions i tècniques destinades a l'anàlisi dels models de les teories estables. Són exemples de teories estables les dels mòduls, en particular els grups abelians, les teories dels cossos separablement tancats, les teories dels cossos diferencialment tancats i, en particular, les teories ACF_0, ACF_p, $\mathrm{Th}(\mathbb{Z}, +, 0, 1)$ i $\mathrm{Th}(\mathbb{Z}, +, 0)$ ja discutides anteriorment. Es conjectura que tot cos la teoria del qual és estable ha de ser separablement tancat.

En els últims anys les nocions pròpies de l'estabilitat s'han adaptat a l'estudi d'estructures inestables. En aquest sentit tenen una importància especial les *teories simples* i les *teories NIP*. Les primeres inclouen les estables i van ser inicialment considerades per S. Shelah a [19] i després redescobertes i desenvolupades per B. Kim i A. Pillay a partir de 1995 (vegeu [6] i el text [29] de F. O. Wagner). Exemples importants d'estructures amb teories simples són els cossos pseudofinits i els cossos amb automorfismes genèrics. Les teories d'estructures ordenades no són simples.

Les teories NIP inclouen també les estables, però moltes d'aquestes són compatibles amb un ordre. De fet, totes les teories o-minimals són NIP. Un text recent de referència sobre teories NIP és el llibre [21] de P. Simon. El cas més elemental de les teories NIP el constitueixen les anomenades *teories dp-minimals*. No inclouen totes les estables, però sí les fortament minimals, les o-minimals, l'aritmètica de Presburger i exemples nous, com ara les teories dels cossos p-àdics.

Les recerques més recents van molt més enllà de les teories simples i les teories NIP. G. Conant ha dissenyat un mapa, que es pot visitar a `http://www.forkinganddividing.com/`, en el qual es dibuixen els tipus principals de teories que avui s'analitzen, i es representen com a punts d'aquest mapa alguns exemples importants. L'anomena *el mapa de l'univers de la teoria de models*.

Agraïments

Agraeixo a la doctora Carme Cascante, exdegana de la Facultat de Matemàtiques de la Universitat de Barcelona, la invitació que em va fer per a donar la lliçó en què es basa aquest article.

Referències

[1] Baldwin, J. T.; Lachlan, A. H. «On strongly minimal sets». *J. Symbolic Logic*, 36 (1971), 79–96.

[2] Cegielski, P. «Théorie élémentaire de la multiplication des entiers naturels». A: *Model Theory and Arithmetic* (París, 1979–1980). Berlín; Nova York: Springer, 1981, 44–89. (Lecture Notes in Math.; 890)

[3] Enderton, H. B. *A Mathematical Introduction to Logic*. Nova York; Londres: Academic Press, 1972.

[4] Enderton, H. B. *Elements of Set Theory*. Nova York; Londres: Academic Press [Harcourt Brace Jovanovich, Publishers], 1977.

[5] Gödel, K. «Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I». *Monatsh. Math. Phys.*, 38 (1) (1931), 173–198.

[6] Kim, B.; Pillay, A. «Simple theories». Joint AILA-KGS Model Theory Meeting (Florence, 1995). *Ann. Pure Appl. Logic*, 88 (2–3) (1997), 149–164.

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

[8] Macintyre, A.; McKenna, K.; van den Dries, L. «Elimination of quantifiers in algebraic structures». *Adv. in Math.*, 47 (1) (1983), 74–87.

[9] Macintyre, A.; Wilkie, A. J. «On the decidability of the real exponential field». A: *Kreiseliana*. Wellesley, MA: A K Peters, 1996, 441–467.

[10] Morley, M. «Categoricity in power». *Trans. Amer. Math. Soc.*, 114 (1965), 514–538.

[11] Pillay, A.; Steinhorn, C. «Definable sets in ordered structures. I». *Trans. Amer. Math. Soc.*, 295 (2) (1986), 565–592.

[12] Presburger, M. «Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt». A: *Comptes Rendus Premier Congrès des Mathématicienes des Pays Slaves*. Varsòvia, 1930, 92–101, 395.

[13] Reineke, J. «Minimale Gruppen». *Z. Math. Logik Grundlagen Math.*, 21 (4) (1975), 357–359.

[14] Richard, J. «Les principes des mathématiques et le problème des ensembles». *Rev. générale des Sc.*, 16 (12) (1905), 541–542.

[15] Robinson, J. «Definability and decision problems in arithmetic». *J. Symbolic Logic*, 14 (1949), 98–114.

[16] Russell, B. «Les paradoxes de la logique». *Rev. de métaphys. et de morale*, 14 (1906), 627–650.

[17] Ryll-Nardzewski, C. «On the categoricity in power $\leq \aleph_0$». *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys.*, 7 (1959), 545–548.

[18] Shelah, S. «Stable theories». *Israel J. Math.*, 7 (1969), 187–202.

[19] Shelah, S. «Simple unstable theories». *Ann. Math. Logic*, 19 (3) (1980), 177–203.

[20] SHELAH, S. *Classification Theory and the Number of Nonisomorphic Models*. 2a ed. Amsterdam: North-Holland Publishing Co., 1990. (Studies in Logic and the Foundations of Mathematics; 92)

[21] SIMON, P. *A Guide to NIP Theories*. Chicago, IL: Association for Symbolic Logic; Cambridge: Cambridge Scientific Publishers, 2015. (Lecture Notes in Logic; 44)

[22] SKOLEM, TH. *Über einige Satzfunktionen in der Arithmetik*. Oslo: I kommisjon hos J. Dybwad, 1931. (Norske videnskaps-akademi i Oslo. Skrifter. I. Mat.-naturv. klasse; 7)

[23] TARSKI, A. «Sur les ensembles définissables de nombres réels. I». *Fund. Math.*, 17 (1931), 210–239.

[24] TARSKI, A. *A Decision Method for Elementary Algebra and Geometry*. 2a ed. Berkeley; Los Angeles, Calif.: University of California Press, 1951.

[25] TENT, K.; ZIEGLER, M. *A Course in Model Theory*. La Jolla, CA: Association for Symbolic Logic; Cambridge: Cambridge University Press, 2012. (Lecture Notes in Logic; 40)

[26] VAN DEN DRIES, L. «Remarks on Tarski's problem concerning $(\mathbf{R}, +, \cdot, \exp)$». A: *Logic Colloquium '82* (Florence, 1982). Amsterdam: North-Holland, 1984, 97–121. (Stud. Logic Found. Math.; 112)

[27] VAN DEN DRIES, L. *Tame Topology and o-minimal Structures*. Cambridge: Cambridge University Press, 1998. (London Mathematical Society Lecture Note Series; 248)

[28] WAGNER, F. O. «Minimal fields». *J. Symbolic Logic*, 65 (4) (2000), 1833–1835.

[29] WAGNER, F. O. *Simple Theories*. Dordrecht: Kluwer Academic Publishers, 2000. (Mathematics and its Applications; 503)

[30] WILKIE, A. J. «Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function». *J. Amer. Math. Soc.*, 9 (4) (1996), 1051–1094.

DEPARTAMENT DE MATEMÀTIQUES I INFORMÀTICA
UNIVERSITAT DE BARCELONA
e.casanovas@ub.edu