Logică matematică
CURS 13

Andrei Sipoș

Facultatea de Matematică și Informatică, DL Mate, Anul I
Semestrul II, 2023/2024

Fundamentele matematicii

Motto

"Everyone knows what a curve is, until he has studied enough mathematics to become confused through the countless number of possible exceptions."

– Felix Klein

Demonstrații formale

Atât în logica propozițională, cât și în logica de ordinul I, avem de-a face cu următoarea echivalență (caracterizare): pentru orice mulțime de enunțuri Γ și orice formulă φ, avem că $\Gamma \vdash \varphi$ **dacă și numai dacă** există $n \in \mathbb{N}$ și un șir finit de formule $(\varphi_i)_{i \leq n}$ astfel încât $\varphi_n = \varphi$, iar pentru orice $i \leq n$, φ_i este fie axiomă a sistemului deductiv, fie element al lui Γ, fie se obține din formule care o precedă printr-una dintre regulile de deducție – regula (MP) sau regula generalizării.

Demonstrația echivalenței este aproape imediată, făcându-se într-unul din sensuri prin inducție pe deducția sintactică, iar în celălalt prin inducție după acel n.

Un șir finit ca mai sus se va numi **demonstrație formală** (relativă la Γ). Membrul drept al echivalenței se poate lua și ca definiție a semnului $\vdash$, dar, după cum s-a văzut, nu a fost nevoie. El justifică, însă, folosirea sintagmei „deducție sintactică" și este crucial în raționamentele filosofice care privesc aceste logici.

Argumentul de „strângere”

În primul rând, ne putem întreba: de ce aceste concepte formale, indicate de semnele $\vdash$ și $\models$, corespund conceptului informal de „adevăr universal”?

Un răspuns ne este dat de așa-numitul argument de „strângere” al lui Kreisel. El pornește de la următoarele premise necontroversate:

- Orice enunț demonstrabil (teoremă formală) este „universal adevărat”.
- Orice enunț „universal adevărat” este, în particular, adevărat în orice structură (deci valid).

Se obține, așadar, următoarea imagine:

$$\vdash \varphi \quad \Rightarrow \quad \varphi \text{ este „universal adevărat”} \quad \Rightarrow \quad \models \varphi$$

Teorema de completitudine (i.e. faptul că $\models \varphi$ implică $\vdash \varphi$) devine ultima premisă a argumentului, cea care „strânge” conceptul informal între cele două concepte formale, garantând egalitatea celor trei.

Mai apoi, putem să ne întrebăm cum putem realiza vechea promisiune de a fundamenta teoria mulțimilor (ZFC) pe logică.

Așa cum s-a văzut și am și evidențiat, noi am fundamentat logica de ordinul întâi pe teoria mulțimilor (inclusiv formulele erau mulțimi!), ca urmare apare problema prefigurată de a găsi un alt fundament pentru logică, pentru a nu avea referințe circulare.

În primul, să observăm că **nu putem fundamenta ceva pe nimic**. Mereu, când dorim să facem matematică și să o comunicăm altora, ne bazăm pe faptul că există anumite idei și concepte pe care le avem dinainte presupuse tacit.

Să vedem, însă, ce are de spus filosofia matematicii despre asemenea chestiuni.

Filosofia matematicii

Simplificând masiv, există în genere două mari moduri de a fundamenta filosofic matematica:

- **platonism**, în care obiectele matematice (chiar și infinite) „există" într-un sens abstract (în genul formelor lui Platon), iar noi avem acces la ele doar prin obiecte finite, tangibile (precum demonstrațiile);
- **formalism** (sau chiar **finitism**, deși ele diferă), în care doar despre obiectele matematice finite se poate spune că „există" cu adevărat, iar cele infinite sunt doar anumite ficțiuni, povești pe care le spunem pentru a putea avea o intuiție productivă.

Noi vom avea o abordare mai **agnostică** – după cum am spus și anterior, ne vom baza pe anumite intuiții comune pe care le avem cu toții și pe care le dorim a fi **minimale** (vezi și „jocurile de limbaj" ale lui Wittgenstein).

Calculabilitate

Vom alege să avem la bază noțiunile intuitive de număr natural și de funcție calculabilă.

După cum am spus în Introducerea istorică, există mai multe moduri de a defini funcția calculabilă (mașini Turing etc.). Acesta nefiind un curs de calculabilitate, ne vom baza pe cunoștințele de programare dobândite în liceu, anume limbajul C (sau chiar pseudocodul) și modul cum sunt implementați în el algoritmi standard, precum algoritmul lui Euclid sau cei de sortare.

Vom spune, deci, că o funcție $f : \mathbb{N} \to \mathbb{N}$ este **calculabilă** dacă există un program C care o calculează. (Aceasta nu este o definiție neriguroasă, cu condiția de a fi fost precizat în detaliu, în prealabil, cum arată și cum este rulat un program C, lucru care se poate face la un curs de semantica limbajelor de programare.) Putem extinde imediat definiția și la alte tipuri de date nenumerice (cum ar fi șirurile de caractere, cum vom vrea să fie formulele), luând în calcul că acestea pot fi (și chiar sunt, în practică) codificate ca numere.

Teza Church-Turing

Cum putem ști că aceste concepte formale de program C, mașină Turing etc. corespund celui informal de calculabilitate? Așa cum am mai spus, această corespondență poartă numele de **teza Church-Turing**.

Există argumente în favoarea tezei ce seamănă cu cel de „strângere" de mai devreme (de aceea am dorit să fie menționat). Un alt argument este că orice definiție gândită pentru calculabilitate s-a dovedit a fi echivalent cu cele ale lui Church și Turing. Mai mult, orice încercare de a fundamenta calculabilitatea pe legi mai profunde ale fizicii (avem exemplul faimos al **calculului cuantic**) nu a condus la creșterea clasei de funcții calculabile, ci doar (fapt nedemonstrat, dar bănuit puternic) la cea a **vitezei** de calcul.

Vom accepta, deci, teza Church-Turing.

Mulțimi decidabile

Spunem că $A \subseteq \mathbb{N}$ (sau, din nou, putem lucra și cu date nenumerice, ca șirurile de caractere) este **decidabilă** dacă $\chi_A : \mathbb{N} \to 2$ este calculabilă, i.e. dacă există un program (o **procedură de decizie**) care primește ca intrare un număr natural și returnează 1 dacă el este în A și 0 dacă nu este.

De exemplu, dacă Q este cel mult numărabilă, avem că $E(Q) \subseteq \mathrm{Seq}(S(Q))$ este decidabilă, iar dacă σ este o signatură de ordinul I numărabilă, avem că F_σ și E_σ, ca submulțimi ale lui $\mathrm{Seq}(S_\sigma)$, sunt decidabile.

Cum mulțimea programelor (oricum le-am formaliza) este numărabilă, iar mulțimea submulțimilor lui $\mathbb{N}$ este infinită, nenumărabilă, avem că **există mulțimi nedecidabile**.

Mulțimi recursiv enumerabile

Spunem că $A \subseteq \mathbb{N}$ (cu aceleași precizări) este **recursiv enumerabilă** dacă există un program care primește ca intrare un număr natural și returnează 1 dacă el este în A, iar în caz că nu este, nu se oprește.

Orice mulțime decidabilă este recursiv enumerabilă: putem construi un program care apelează procedura de decizie a mulțimii: în caz că aceea returnează 1, va returna și el 1, iar în caz că returnează 0, programul va intra într-o buclă infinită. Programul verifică atunci condiția din definiția enumerabilității recursive.

Deși folosim, pentru intuiție, termenul de „mulțime", noi nu avem nevoie (neapărat) de teoria mulțimilor pentru a le fundamenta, putând gândi în mare parte doar în termeni de aceste programe/proceduri concrete, formalizate, aproximativ vorbind, într-un sistem deductiv „finitar", pe care nu îl vom detalia.

Caracterizarea mulțimilor recursiv enumerabile

Propoziție

O mulțime este recursiv enumerabilă dacă și numai dacă există un program care nu acceptă date de intrare, rulează la infinit, iar pe parcursul rulării afișează exact acele numere (respectiv șiruri etc.) care sunt elemente ale mulțimii. (Un asemenea program oferă, în fond, o enumerare a mulțimii, de unde provine și termenul.)

Demonstrație

Pentru „$\Rightarrow$”, rulăm în paralel (de ce putem face asta?) programul din definiția enumerabilității recursive dând ca intrare, pe rând, fiecare număr natural, iar atunci când vreuna dintre cópii returnează 1, afișăm numărul corespunzător.

Pentru „$\Leftarrow$”, dacă avem un număr dat ca intrare, așteptăm ca programul din enunțul propoziției să îl afișeze, iar în acel moment, returnăm 1.

Cazul logicii propoziționale

Când Q este numărabilă, mulțimea acelor șiruri din $\mathrm{Seq}(E(Q))$ ce sunt demonstrații formale este decidabilă. În particular, ea este recursiv enumerabilă. Observăm că putem modifica un program ce enumeră toate demonstrațiile formale pentru a afișa doar concluziile lor. Astfel, se observă că mulțimea **tautologiilor** este recursiv enumerabilă.

Dar, mai mult, cum pentru orice $\varphi \in E(Q)$, $Var(\varphi)$ este finită, putem decide dacă φ este tautologie doar uitându-ne la tabelul de adevăr construit de la $Var(\varphi)$. Avem, deci, o procedură de decizie pentru mulțimea tautologiilor, care este, așadar, decidabilă.

Aceste fapte ne arată că sistemul de deducție pentru logica propozițională nu este strict necesar. El a fost studiat doar pentru dobândirea intuiției asupra sistemelor de deducție în general.

Cazul logicii de ordinul I

Când avem de-a face cu o signatură de ordinul I numărabilă, prima parte a raționamentului anterior încă funcționează, iar ca urmare mulțimea demonstrațiilor este decidabilă, iar cea a formulelor valide este recursiv enumerabilă. Acesta este conținutul **real** al teoremei de completitudine, numit, uneori, **teorema de completitudine abstractă**.

Apare întrebarea: există o procedură de decizie pentru mulțimea formulelor valide? Răspunsul, după cum am spus și în Introducerea istorică, a fost dat de Church și Turing și este unul **negativ**. Este de remarcat că pentru a justifica acest fapt, avem nevoie de o definiție precisă a calculabilității (așa cum au oferit ei), nu ne mai sunt suficiente argumente informale precum cele precedente.

Ca fapt divers, cazul când avem doar simboluri de relație de aritate cel mult 1 admite o procedură de decizie. Logica de ordinul I devine nedecidabilă imediat când apare măcar un simbol de relație de aritate 2 (de ex. cazul grafurilor).

Cazul mulțimilor de formule

Se observă și că raționamentul inițial se păstrează și în cazul în cazul în care avem o mulțime decidabilă de enunțuri $\Gamma \subseteq E_\sigma$ ca mulțime de premise, în sensul că mulțimea demonstrațiilor relative la Γ este decidabilă, iar mulțimea consecințelor sintactice ale lui Γ este recursiv enumerabilă.

Acestea sunt, în fond, proprietățile pe care le dorim, atunci când considerăm o mulțime Γ care să poată fundamenta matematica: vrem să putem decide dacă un șir de enunțuri este o demonstrație, altfel însăși noțiunea de demonstrație nu ar avea sens!

Din nou aritmetica

Se observă că mulțimile PA, SOA, așa acum au fost introduse în capitolul anterior, sunt mulțimi decidabile. Ele pot, așadar, servi ca fundament al matematicii.

Am observat că există modele non-standard ale aritmeticii, adică structuri neizomorfe cu structura $\mathcal{N}$ care sunt elementar echivalente cu ea, adică satisfac $Th(\mathcal{N})$. Ele pot fi chiar numărabile, după cum am văzut; însă, spunem acum, nu pot fi calculabile (**teorema lui Tennenbaum**).

Ce are special acest $Th(\mathcal{N})$? Este ceea ce se numește o mulțime **completă**, după cum vom vedea în continuare.

Mulțimi complete

Numim o mulțime $\Gamma \subseteq E_\sigma$ **completă** dacă este satisfiabilă, iar pentru orice $\varphi \in E_\sigma$, avem $\Gamma \models \varphi$ sau $\Gamma \models \neg\varphi$.

Propoziție

Fie $\mathcal{A}$ o σ-structură. Atunci $Th(\mathcal{A})$ este completă.

Demonstrație

Clar, $\mathcal{A} \models Th(\mathcal{A})$, deci $Th(\mathcal{A})$ este satisfiabilă. Fie $\varphi \in E_\sigma$. Presupunem $Th(\mathcal{A}) \not\models \varphi$. Atunci $\varphi \notin Th(\mathcal{A})$, deci $\mathcal{A} \not\models \varphi$. Avem că $\mathcal{A} \models \neg\varphi$, deci $\neg\varphi \in Th(\mathcal{A})$ și $Th(\mathcal{A}) \models \neg\varphi$.

Observăm că dacă Γ și Σ verifică $\Gamma \sim \Sigma$, avem că mulțimea consecințelor lui Γ este egală cu mulțimea consecințelor lui Σ.

Mulțimi complete

Propoziție

Fie $\mathcal{A}$ o σ-structură. Avem că mulțimea consecințelor lui $Th(\mathcal{A})$ este $Th(\mathcal{A})$.

Demonstrație

Fie φ cu $Th(\mathcal{A}) \models \varphi$. Cum $\mathcal{A} \models Th(\mathcal{A})$, avem $\mathcal{A} \models \varphi$, deci $\varphi \in Th(\mathcal{A})$.

Propoziție

Fie $\mathcal{A}$ o σ-structură și Γ completă cu $\mathcal{A} \models \Gamma$. Atunci $\Gamma \sim Th(\mathcal{A})$.

Demonstrație

Fie $\mathcal{B}$ o σ-structură. Dacă $\mathcal{B} \models \Gamma$ și $\varphi \in Th(\mathcal{A})$, atunci $\mathcal{A} \not\models \neg\varphi$, deci $\Gamma \not\models \neg\varphi$. Cum Γ este completă, $\Gamma \models \varphi$ și deci $\mathcal{B} \models \varphi$.

Dacă $\mathcal{B} \models Th(\mathcal{A})$ și $\varphi \in \Gamma$, atunci $\mathcal{A} \models \varphi$, deci $\varphi \in Th(\mathcal{A})$ și $\mathcal{B} \models \varphi$.

Consecințe decidabile

Propoziție

Fie Γ o mulțime completă astfel încât mulțimea consecințelor ei este recursiv enumerabilă. Atunci mulțimea consecințelor ei este decidabilă.

Demonstrație

Vrem să construim o procedură de decizie pentru mulțimea consecințelor lui Γ. Fie φ intrarea acelei proceduri. Rulăm programul ce enumeră mulțimea consecințelor lui Γ, iar în momentul în care îl afișează pe φ sau pe $\neg\varphi$ (ceea ce necesar se va întâmpla, Γ fiind completă), returnăm, după caz, 1 sau 0.

Incompletitudine

Putem descrie, așadar, acel $Th(\mathcal{N})$, i.e. să avem că ar fi o mulțime recursiv enumerabilă? Răspunsul este nu și a fost dat de Gödel.

Teorema I de incompletitudine a lui Gödel

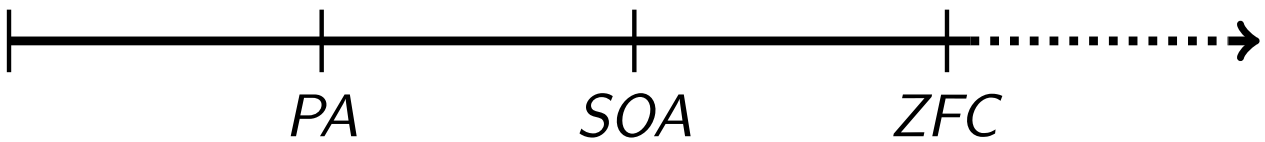
Fie $\Gamma \subseteq E_{\sigma_{\mathrm{ar}}}$ recursiv enumerabilă astfel încât $\Gamma \models PA$. Atunci Γ nu este completă, i.e. există φ astfel încât $\Gamma \not\models \varphi$ și $\Gamma \not\models \neg\varphi$.

Corolar

$Th(\mathcal{N})$ nu este recursiv enumerabilă.

Ierarhia Gödel

Așadar, cum am spus și în Introducerea istorică, nu avem un singur fundament (complet) al matematicii, ci o ierarhie, numită **ierarhia Gödel**, de asemenea sisteme incomplete:



În continuare, vom detalia cazul teoriei mulțimilor ZFC.

ZFC

Ce vom face este, deci, să arătăm că teoria mulțimilor ZFC se poate codifica ca o mulțime decidabilă de enunțuri peste o signatură numărabilă.

Signatura va fi notată cu $\sigma_\in$ și va conține un singur simbol, anume un simbol de relație de aritate 2, notat cu $\in$. Se observă folosirea exclusivă a sa este justificată, i.e. notațiile folosite uzual în teoria mulțimilor se pot reduce la el în logica de ordinul I, și le vom folosi drept prescurtări, de pildă:

$$\begin{array}{l|r} \emptyset \in x & \exists y(y \in x \wedge \forall z \neg(z \in y)) \\ x = \{z\} & \forall u(u \in x \leftrightarrow u = z) \\ x = u \cap v & \forall z(z \in x \leftrightarrow (z \in u \wedge z \in v)) \\ x \subseteq y & \forall z(z \in x \rightarrow z \in y) \end{array}$$

Axiomele ZFC

În continuare vom vedea cum sunt formalizate axiomele ZFC în această signatură.

- Axioma extensionalității:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

- Axioma perechii:

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

- Axioma reuniunii:

$$\forall F \exists x \forall z ((\exists y (z \in y \wedge y \in F)) \rightarrow z \in x).$$

- Axioma mulțimii părților:

$$\forall x \exists y \forall z (z \subseteq x \rightarrow z \in y).$$

Axiomele ZFC

- Axioma infinitului:

$$\exists A(\emptyset \in A \wedge \forall x(x \in A \rightarrow x \cup \{x\} \in A).$$

- Axioma regularității:

$$\forall a(\neg(a = \emptyset) \rightarrow \exists b(b \in a \wedge a \cap b = \emptyset)).$$

Axioma alegerii are o formulare mai lungă (dar nu mai complicată), drept care o vom omite.

Unde vom avea, într-adevăr, o problemă, va fi exact acolo unde am avut-o deja, anume la explicitarea acelor „proprietăți" din Axioma comprehensiunii și Axioma înlocuirii. O vom trata doar pe prima dintre ele, cealaltă formalizându-se analog.

Axioma comprehensiunii, formal

Naiv, axioma comprehensiunii s-ar scrie ca

$$\forall P \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge P(z)).$$

Însă o asemenea „cuantificare după predicate" nu este posibilă (după cum am mai spus) decât într-o logică de ordin superior (ceea ce, până la urmă, ne-ar conduce la o referință circulară, pe care dorim să o evităm).

Soluția este (exact ca la *PA*) de a înlocui acea unică axiomă de mai sus cu o familie **infinită** de axiome, câte una pentru fiecare proprietate P formalizabilă ca formulă φ peste signatura $\sigma_{\in}$, în felul următor (simplificând puțin):

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \varphi).$$

Sistemul ZFC

După ce formalizăm astfel și Axioma înlocuirii, notăm mulțimea de axiome care rezultă cu ZFC. Observăm, deci, că sistemul acesta nu are doar nouă axiome, cum ne-am fi așteptat, ci un număr numărabil. (Se poate chiar demonstra că nu există o mulțime finită $\Gamma \subseteq E_{\sigma_\in}$ cu $\Gamma \sim ZFC$.) Totuși, este adevărat lucrul pe care-l doream, anume faptul că ZFC este o mulțime decidabilă, și, prin urmare, mulțimea ZFC-demonstrațiilor este și ea decidabilă, iar mulțimea consecințelor lui ZFC este recursiv enumerabilă.

În interiorul ZFC, putem dezvolta logica de ordinul I, așa cum am făcut-o în acest curs, împreună cu toate rezultatele ei – compacitate, completitudine, Löwenheim-Skolem în sus etc.

Ipoteza continuumului

În acest moment, putem formaliza, de pildă, chiar și ipoteza continuumului, i.e. faptul că $2^{\aleph_0} = \aleph_1$, ca pe un $\sigma_\in$-enunț, notat cu CH, și putem privi „metarezultatele" lui Gödel și Cohen, ce spun că

$$ZFC \nvdash \neg CH, \text{ respectiv } ZFC \nvdash CH,$$

ca pe niște afirmații despre proceduri definibile finit ce sunt demonstrabile în acel sistem finitar pomenit anterior.

În particular, prima afirmație este echivalentă cu faptul că $ZFC \cup \{CH\}$ este consistentă, afirmație ce se va nota prin

$$Con(ZFC + CH).$$

A doua teoremă de incompletitudine

În general, putem formaliza deducția sintactică din logica de ordinul I și în sisteme mai slabe, ca *PA*, și putem vorbi, acolo, pentru orice Γ recursiv enumerabilă, despre $Con(\Gamma)$. Astfel putem exprima a doua teoremă a lui Gödel.

Teorema II de incompletitudine a lui Gödel

În Teorema I de incompletitudine putem lua φ să fie chiar $Con(\Gamma)$.

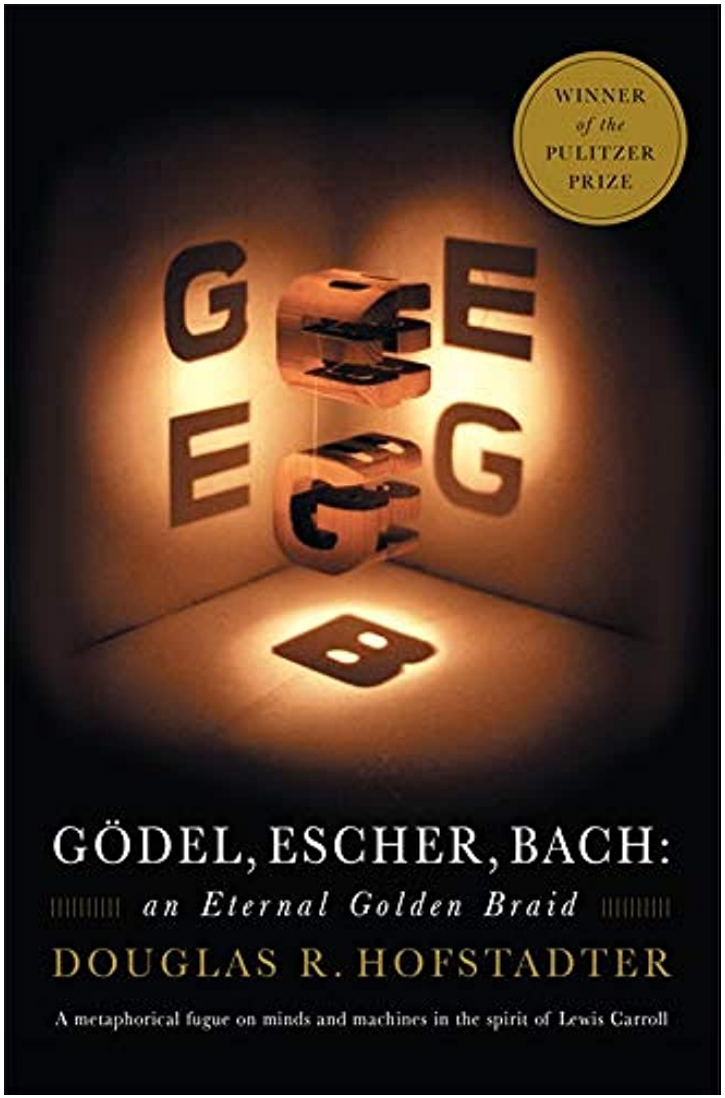
Corolar

$PA \nvdash Con(PA)$, $ZFC \nvdash Con(ZFC)$ etc.

Corolar

Dat fiind un sistem finitar (în particular slab) F, avem $F \nvdash Con(PA)$, $F \nvdash Con(ZFC)$ etc.

O carte pe care o recomand:



...și una mai nouă:

Consistența relativă

Observăm că enunțul $Con(ZFC + CH)$ îl implică, firește, pe $Con(ZFC)$, care exprimă faptul că ZFC este consistentă. Or, tocmai am văzut că a doua teoremă de incompletitudine a lui Gödel spune că aceasta nu este demonstrabilă într-un sistem finitar.

De ce, totuși, rezultatele acestea de independență nu îl contrazic pe acela de incompletitudine? Răspunsul este că nu $Con(ZFC + CH)$ este enunțul demonstrat, de fapt, ci

$$Con(ZFC) \to Con(ZFC + CH),$$

i.e. consistența **relativă** a ipotezei continuumului (și apoi, în cazul rezultatului lui Cohen, a negației ei) peste ZFC.

Consistența în general

Un mod de a ne convinge de consistența sistemelor PA, ZFC este prin argumente extra-matematice (filosofice, ontologice), de exemplu prin intuiția pe care o avem asupra numerelor sau a ierarhiei von Neumann. Firește, rezultatul din acest curs a existenței numerelor naturale ne arată – matematic – $ZFC \models Con(PA)$, dar aceasta nu este ceva filosofic satisfăcător.

O altă soluție – descrisă și în Introducerea istorică – este a demonstra consistența unui sistem într-un sistem **necomparabil** cu el – de exemplu, Gentzen a arătat (în 1936) $Con(PA)$ într-un sistem finitar căruia i-a adăugat inducție până la ordinalul ε_0 (această inducție este doar pentru formule de complexitate redusă, pentru a putea fi incomparabilă cu cea din PA). Nu se cunoaște – încă – echivalentul acestui rezultat pentru SOA sau ZFC.

Acest gen de probleme, mai direct sau mai voalat, este studiat în teoria demonstrației și în general în logica postbelică.

Paradoxul lui Skolem

Admițând *ZFC* ca fiind consistentă, îi putem adăuga pe $Con(ZFC)$ însuși ca pe o axiomă suplimentară și putem deduce, din teorema de completitudine, că există modele pentru *ZFC*.

Nu există aici un concept evident de model standard, dar, clar, ca și în cazul aritmeticii, se poate construi o varietate de modele cu ajutorul Teoremei Löwenheim-Skolem în sus.

Un fapt curios este că, fiind o mulțime de enunțuri într-o signatură numărabilă, *ZFC* admite un model numărabil, chiar dacă în interiorul unui asemenea model există în mod necesar mulțimi pe care modelul le „vede" ca fiind nenumărabile. Acest fapt este denumit **paradoxul lui Skolem** – paradox nu fiindcă exprimă o contradicție, ca în cazul paradoxul lui Russell, ci fiindcă exprimă ceva aparent neverosimil.

Logica drept unealtă

Pe de altă parte, încrederea în *ZFC* și capacitatea acesteia de a formaliza logica de ordinul întâi ne permit să o folosim pe aceasta din urmă ca pe o unealtă utilă în matematică, independent de chestiunile legate de fundamente.

Dezvoltarea teoriei modelelor logicii de ordinul I a declanșat o serie de progrese teoretice, de exemplu în algebră, după cum vom vedea în ultimul capitol.