Logică matematică
CURS 2

Andrei Sipoș

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

Relații binare

Propoziție-Definiție

Fie R o mulțime. Următoarele afirmații sunt echivalente:

- există A și B astfel încât $R \subseteq A \times B$;
- elementele lui R sunt perechi ordonate, adică pentru orice $z \in R$ există x, y cu $z = (x, y)$.

În acest caz, R se numește **relație (binară)**, iar dacă A și B sunt ca mai sus, spunem că R este o relație **între** A și B. Dacă A este astfel încât R este între A și A, spunem că R este o relație **pe** A.

Demonstrație

Implicația „$\Rightarrow$" este evidentă. Pentru implicația „$\Leftarrow$", notăm mulțimea $\bigcup\bigcup R$ atât cu A, cât și cu B. Fie $z \in R$. Atunci există x, y cu $z = \{\{x\}, \{x, y\}\} \in R$. Așadar, $\{x\}$, $\{x, y\} \in \bigcup R$ și deci x, $y \in \bigcup\bigcup R$. Ca urmare, $(x, y) \in \bigcup\bigcup R \times \bigcup\bigcup R = A \times B$.

Observăm și că A și B **nu sunt unice** cu acea proprietate! De exemplu, $\emptyset$ este o relație pe $\emptyset$, dar și pe $\{\emptyset\}$.

Grafice și funcții

Definiție

Dacă A este o mulțime, notăm cu Δ_A și denumim **relația diagonală** pe A acea relație pe A definită prin

$$\{p \in A \times A \mid \text{există } a \text{ cu } p = (a, a)\}.$$

Definiție

Fie A, B mulțimi și R o relație între A și B. Spunem că R este **grafic între** A **și** B dacă pentru orice $a \in A$ există și este unic $b \in B$ astfel încât $(a, b) \in R$.

Definiție

Fie A, B mulțimi. Spunem că f este **funcție între** A **și** B (și notăm aceasta cu $f : A \to B$) dacă există R un grafic între A și B astfel încât $f = (A, B, R)$. A se numește **domeniul** lui f, B **codomeniul** lui f, iar R **graficul** lui f. Pentru orice $a \in A$ vom nota cu $f(a)$ acel unic $b \in B$ cu $(a, b) \in R$.

Detalii de codificare

Un grafic și o funcție sunt mulțimi, dar ele nu sunt aceeași mulțime! Avem nevoie de includerea codomeniului în „codificarea" noțiunii de funcție pentru a putea formaliza corect surjectivitatea.

Propoziție

Fie R o relație binară. Următoarele afirmații sunt echivalente:

- există A și B astfel încât R este grafic între A și B;
- pentru orice x, y, z cu (x, y), $(x, z) \in R$, avem $y = z$, și vom nota $R(x) := y = z$.

Propoziție

Fie R o relație binară și A, B, C, D astfel încât R este grafic atât între A și B, cât și între C și D. Atunci $A = C$.

Aceste două propoziții (care se vor demonstra la seminar) ne arată că domeniul unei funcții este complet determinat de grafic (și îl putem numi **domeniul graficului**), ca urmare el ar fi putut să nu fie inclus în modul de definiție. El este inclus, totuși, prin tradiție.

Notații despre funcții

Pentru orice mulțime A, avem că (A, A, Δ_A) este funcție. O numim **funcția identică pe A** sau **funcția identitate pe A** și o notăm cu id_A.

Dacă avem P o proprietate exprimabilă în limbajul teoriei mulțimilor (ca și la Axioma comprehensiunii, sensul exact al cuvântului va putea fi deslușit abia când se va introduce logica de ordinul I), iar pentru orice x există și este unic y cu $P((x, y))$, putem spune că ea denotă o **operație** F și vom nota acel y cu $F(x)$. Deseori, acest „$F(x)$" va fi și el exprimabil.

Acum, dacă A și B sunt mulțimi iar P este o proprietate care definește o operație notată cu F, astfel încât, pentru orice $x \in A$, $F(x) \in B$, atunci, când vom spune de acum încolo „fie $f : A \to B$ astfel încât pentru orice $x \in A$, $f(x) := F(x)$" sau „fie $f : A \to B$ definită prin $x \mapsto F(x)$", vom înțelege prin aceasta că definim relația

$$R := \{p \in A \times B \mid P(p)\}$$

și apoi definim f ca fiind egal cu tripletul (A, B, R).

Funcții și mulțimi

Observăm că dacă A, B sunt mulțimi, iar $f : A \to B$, atunci $f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B)$, ca urmare putem defini mulțimea tuturor funcțiilor de la A la B, notată cu B^A, prin

$$\{f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B) \mid f \text{ funcție}\}.$$

Definiție

Fie A, B și $f : A \to B$. Fie $X \subseteq A$ și $Y \subseteq B$. Atunci:

- notăm cu $f_*(X)$ și numim **imaginea directă** a lui X prin f mulțimea
$$\{y \in B \mid \text{există } x \in X \text{ cu } f(x) = y\};$$
- notăm cu $f^*(Y)$ și numim **imaginea inversă** a lui Y prin f mulțimea
$$\{x \in A \mid f(x) \in Y\};$$
- notăm cu $\mathrm{Im} f$ și numim **imaginea** lui f mulțimea $f_*(A)$.

Proprietăți ale funcțiilor

Mai definim **imaginea** unui grafic ca fiind imaginea unei funcții care îl are ca grafic. Știm din cele anterioare că există o asemenea funcție și putem arăta că imaginea nu depinde de funcția aleasă.

Definiție

Fie A, B și $f : A \to B$. Spunem că:

- f este **injectivă** sau **injecție** dacă pentru orice $x, y \in A$ cu $x \neq y$, avem $f(x) \neq f(y)$;
- f este **surjectivă** sau **surjecție** dacă $\mathrm{Im} f = B$, mai exact dacă pentru orice $y \in B$ există $x \in A$ cu $f(x) = y$;
- f este **bijectivă** sau **bijecție** dacă este injectivă și surjectivă.

Compunerea funcțiilor

Definiție

Fie A, B, C și $f : A \to B$, $g : B \to C$. Definim funcția $g \circ f : A \to C$ (citim „g compus cu f"; ea se notează uneori cu $f; g$, caz în care citim „f succedat de g"), pentru orice $x \in A$, prin

$$(g \circ f)(x) := g(f(x)).$$

Proprietăți elementare

Fie A, B, C, D și $f : A \to B$, $g : B \to C$, $h : C \to D$. Atunci:

- $(h \circ g) \circ f = h \circ (g \circ f)$;
- $f \circ \mathrm{id}_A = f$; $\mathrm{id}_B \circ f = f$.

Restricția graficelor și funcțiilor

Definiție

Fie R un grafic și X o submulțime a domeniului său. Notăm cu $R_{|X}$ și citim „R restricționat la X" mulțimea

$$\{p \in R \mid \text{există } a, b \text{ cu } a \in X \text{ și } p = (a, b)\}.$$

Așadar, domeniul lui $R_{|X}$ este X, iar, pentru orice $a \in X$, $R_{|X}(a) = R(a)$.

Definiție

Fie $f = (A, B, R)$ o funcție și $X \subseteq A$. Definim funcția $f_{|X} := (X, B, R_{|X})$ și o numim „f restricționat la X". Așadar, $f_{|X} : X \to B$ (citim „f restricționat la X") și, pentru orice $x \in X$, $f_{|X}(x) = f(x)$.

Funcții inversabile

Definiție

Fie A, B, $f : A \to B$. Dacă $g : B \to A$, $g \circ f = \mathrm{id}_A$ și $f \circ g = \mathrm{id}_B$, spunem că f este **inversabilă** iar g este **inversa** sa.

O inversă, dacă există, este unică. Mai exact, dacă avem A, B, $f : A \to B$, iar g_1, $g_2 : B \to A$ sunt inverse ale lui f, atunci $g_1 = g_2$, iar aceasta se poate demonstra doar folosind proprietățile elementare ale compunerii:

$$g_1 = g_1 \circ \mathrm{id}_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_A \circ g_2 = g_2.$$

Următorul rezultat se demonstrează ușor:

Propoziție

O funcție este inversabilă dacă și numai dacă este bijectivă.

Comportamentul mulțimii vide față de funcții

Fie A o mulțime. Se pune întrebarea: există $f : \emptyset \to A$? Dacă da, cum arată? Presupunem că ar exista o asemenea f. Atunci există R cu $f = (\emptyset, A, R)$ și $R \subseteq \emptyset \times A = \emptyset$, deci $R = \emptyset$ și $f = (\emptyset, A, \emptyset)$. Aceasta este într-adevăr o funcție. Ca urmare, există o unică funcție de la $\emptyset$ la A, anume $(\emptyset, A, \emptyset)$, pe care o numim **funcția vidă a lui** A. Așadar, avem că $A^\emptyset = A^0$ este un singleton. Spunem că $\emptyset$ este **mulțimea inițială**.

Dar invers? Există o funcție $g : A \to \emptyset$? Dacă A este nevidă, atunci există $a \in A$, și deci $g(a) \in \emptyset$, o contradicție, dat fiind că nu există $b \in \emptyset$. Ca urmare, funcția există doar când $A = \emptyset$, și atunci $g = (\emptyset, \emptyset, \emptyset)$ (caz particular al celui din paragraful precedent).

Comportamentul singleton-urilor față de funcții

Fixăm X un singleton – de exemplu, putem lua $X := 1 = \{\emptyset\}$, dar alegerea precisă a lui X nu va conta.

Fie A o mulțime. Atunci există o unică funcție de la A la X, anume cea care duce orice element din A în unicul element al lui X. De aceea, spunem că orice singleton este **mulțime terminală** (noțiune **duală** celei de mulțime inițială).

Vrem acum, invers, să găsim toate funcțiile de la X la A. Pentru a găsi o asemenea funcție, trebuie doar să selectăm elementul din A în care va fi dus acel unic element al lui X. Așadar, funcțiile de la X la A sunt în corespondență biunivocă cu elementele lui A. În particular, pentru orice $a \in A$, notăm $\langle a \rangle := \{(0, a)\}$ și, apoi, $[a]_A := (1, A, \langle a \rangle)$, acea unică funcție cu domeniul 1 și codomeniul A care duce singurul element al lui 1 în a.

Familii

Fie I o mulțime. Numim **familie indexată după** I un grafic al cărui domeniu este I. Dacă F este o familie indexată după I, vom nota, pentru orice $i \in I$, acea unică mulțime x pentru care $(i, x) \in F$ cu F_i. De asemenea, vom mai scrie $(F_i)_{i \in I}$ în loc de F.

Definim **reuniunea** și **intersecția**, ca familie, ale lui F – notate cu $\bigcup_{i \in I} F_i$, respectiv cu $\bigcap_{i \in I} F_i$ – ca fiind reuniunea, respectiv intersecția (ultima doar în cazul în care $I \neq \emptyset$) a imaginii ca grafic a lui F.

Mai definim **produsul cartezian** al lui F, notat cu $\prod_{i \in I} F_i$, ca fiind mulțimea tuturor familiilor f indexate după I cu proprietatea că pentru orice $i \in I$, $f_i \in F_i$. Această mulțime există deoarece orice asemenea f este element al lui

$$\mathcal{P}\left(I \times \bigcup_{i \in I} F_i\right).$$

Tipuri de relații binare pe o mulțime

Definiție

Fie A o mulțime și R o relație pe A. Pentru orice x, $y \in A$, vom scrie xRy în loc de $(x, y) \in R$. Spunem că R este:

- **reflexivă** dacă pentru orice $x \in A$, xRx;
- **simetrică** dacă pentru orice x, $y \in A$ cu xRy, avem yRx;
- **tranzitivă** dacă pentru orice x, y, $z \in A$ cu xRy și yRz, avem xRz;
- **de echivalență** dacă este reflexivă, simetrică și tranzitivă;
- **totală** dacă pentru orice x, $y \in A$, avem xRy sau yRx;
- **antisimetrică** dacă pentru orice x, $y \in A$ cu xRy și yRx avem $x = y$;
- **de ordine parțială** (de obicei ele sunt notate cu $\leq$) dacă este reflexivă, antisimetrică și tranzitivă;
- **ireflexivă** dacă pentru orice $x \in A$, nu avem xRx;
- **asimetrică** dacă pentru orice x, $y \in A$ cu xRy, nu avem yRx.

Relații de ordine strictă

Propoziție-Definiție

Fie A o mulțime și R o relație tranzitivă pe A. Următoarele afirmații sunt echivalente:

- R este ireflexivă;
- R este asimetrică.

În acest caz, R se numește relație **de ordine strictă** (de obicei ele sunt notate cu $<$).

Demonstrație

Pentru implicația „$\Rightarrow$”, fie x, $y \in A$ cu xRy. Dacă am avea yRx, din tranzitivitate am deduce xRx, contradicție. Invers, fie x și presupunem xRx. Atunci, din asimetrie, nu avem xRx, contradicție.

Legătura dintre cele două tipuri de relație de ordine

Propoziție

Fie A o mulțime.

- Dacă $\leq$ este o relație de ordine parțială pe A și dacă definim $<\subseteq A \times A$ ca fiind mulțimea tuturor perechilor (a, b) cu proprietatea că $a \leq b$ și $a \neq b$, atunci $<$ este o relație de ordine strictă pe A.
- Dacă $<$ este o relație de ordine strictă pe A și dacă definim $\leq\subseteq A \times A$ ca fiind mulțimea tuturor perechilor (a, b) cu proprietatea că $a < b$ sau $a = b$, atunci $\leq$ este o relație de ordine parțială pe A.

Se observă ușor și că cele două operații sunt inverse una celeilalte.

Demonstrație

Exercițiu de seminar.

Putem, deci, lucra interșanjabil cu cele două tipuri de relație, folosind semnele $<$ și $\leq$ după cum ne este convenabil.

Firește, multe dintre aceste noțiuni au fost deja studiate într-o anume formă la cursurile de algebră sau analiză. Aici insistăm în special pe chestiunile care țin de axiomatizare și formalizare (de exemplu, fundamentarea existenței anumitor mulțimi, după cum am văzut) și pe noțiuni adiacente care ne vor servi mai târziu mai mult decât ar servi altor cursuri.

În ceea ce privește capitolul actual, vom considera cunoscute noțiunile de clasă de echivalență, mulțime-cât, element minim, maxim, minimal, maximal, minorant, majorant, infimum, supremum și proprietățile lor elementare. Reamintim și definiția:

Definiție

Fie A o mulțime și $\leq$ o relație de ordine parțială pe A. Spunem că $\leq$ este o relație de **bună ordine** dacă orice submulțime nevidă B a lui A are element minim.

Numere naturale

Reamintim că am notat, pentru orice x, $x^+ := x \cup \{x\}$ și am definit „numerele” 0, 1, 2, 3 în felul următor:

$$\begin{aligned}
0 &:= \emptyset && = \emptyset \\
1 &:= 0^+ = 0 \cup \{0\} = \{0\} && = \{\emptyset\} \\
2 &:= 1^+ = 1 \cup \{1\} = \{0, 1\} && = \{\emptyset, \{\emptyset\}\} \\
3 &:= 2^+ = 2 \cup \{2\} = \{0, 1, 2\} && = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}
\end{aligned}$$

Intuitiv, lista ar putea continua, punând pentru orice n, $n + 1$ ca fiind n^+, în felul acesta fiecare număr natural devenind mulțimea predecesorilor săi, dar nu putem zice riguros „pentru orice n” – am avea o referință circulară. O vom rezolva prin a defini mai întâi mulțimea numerelor naturale.

Mulțimi inductive

Observăm că mulțimea numerelor naturale, oricum ar fi ea definită, trebuie să conțină pe $\emptyset$, iar pentru orice x din ea, trebuie să conțină și pe x^+. Astfel formulăm:

Definiție

O mulțime A se numește **inductivă** dacă $\emptyset \in A$ și pentru orice $x \in A$, $x^+ \in A$.

O asemenea mulțime este clar (intuitiv vorbind, deoarece nu am introdus deocamdată conceptul) infinită. Axiomele de până acum permit ca toate mulțimile care există să fie finite. Ca urmare, avem nevoie de una nouă:

Axioma infinitului

Există o mulțime inductivă.

O proprietate imediată este aceea ce spune că dacă F este o mulțime nevidă ale cărei elemente sunt mulțimi inductive, atunci și $\bigcap F$ este inductivă. În particular, dacă x și y sunt inductive, $x \cap y$ este inductivă.

Mulțimi minimal inductive

Nu este suficient ca mulțimea pe care o dorim să conțină toate acele elemente, ci mai vrem și să nu conțină altele în plus.

Definiție

O mulțime inductivă A se numește **minimal inductivă** dacă pentru orice B inductivă cu $B \subseteq A$ avem $B = A$.

Propoziție

Fie A minimal inductivă. Atunci, pentru orice B inductivă avem $A \subseteq B$. În particular, există cel mult o mulțime minimal inductivă.

Demonstrație

Dacă B este ca în enunț, atunci $A \cap B$ este inductivă și $A \cap B \subseteq A$, deci $A \cap B = A$, i.e. $A \subseteq B$.

Mulțimea numerelor naturale

Propoziție

Există (și este deci unică) o mulțime minimal inductivă.

Demonstrație

Fie u o mulțime inductivă și notăm

$$F := \{x \in \mathcal{P}(u) \mid x \text{ inductivă}\}.$$

Cum $u \in F$, $F \neq \emptyset$, iar F conține numai mulțimi inductive. Așadar și $y := \bigcap F$ este inductivă. Vom arăta că y este minimal inductivă. Fie $z \subseteq y$ inductivă. Dat fiind că $u \in F$ și $y = \bigcap F$, avem $y \subseteq u$, și deci, cum $z \subseteq y$, $z \subseteq u$. Deci, din definiția lui F, $z \in F$, deci și $y \subseteq z$, ceea ce trebuia demonstrat.

Această unică mulțime minimal inductivă o vom numi **mulțimea numerelor naturale** și o vom nota cu $\mathbb{N}$.

Principiul inducției

Faptul că $\mathbb{N}$ este minimal inductivă se poate reformula în felul următor.

Principiul inducției (Principiul I de inducție)

Fie $A \subseteq \mathbb{N}$ astfel încât $0 \in A$ și pentru orice $n \in A$, avem $n^+ \in A$.

Atunci $A = \mathbb{N}$.

Folosind acest principiu, vom putea construi relațiile și operațiile uzuale pe $\mathbb{N}$ și demonstra proprietățile lor cunoscute.

Relația de ordine

Având în vedere că gândim un număr ca fiind mulțimea predecesorilor săi (lucru pe care îl presupunem cunoscut acum și îl vom demonstra la seminar), vom defini, pentru orice n, $m \in \mathbb{N}$, $n < m$ exact atunci când $n \in m$.

Vom demonstra acum că pentru orice $n \in \mathbb{N}$, $0 \leq n$ – observând atât folosirea Principiului inducției, cât și faptul că putem vorbi de $\leq$ imediat ce l-am introdus pe $<$. Formăm

$$A := \{n \in \mathbb{N} \mid 0 \leq n\}.$$

Cum $0 = 0$, $0 \leq 0$, deci $0 \in A$. Fie $n \in A$. Atunci $0 \leq n$, adică $0 \in n$ sau $0 = n$. Așadar, $0 \in n \cup \{n\}$, ceea ce înseamnă că $0 < n^+$. Deci $0 \leq n^+$, i.e. $n^+ \in A$, ceea ce trebuia demonstrat.

Un alt rezultat imediat spune că pentru orice k, $n \in \mathbb{N}$, $k < n^+$ dacă și numai dacă $k \leq n$.

Principiul inducției complete

Acum putem demonstra următoarea variantă, aparent mai tare, deseori folosită în matematică, a Principiului inducției.

Principiul inducției complete (Principiul al II-lea de inducție)

Fie $A \subseteq \mathbb{N}$ astfel încât pentru orice $n \in \mathbb{N}$ ce verifică faptul că pentru orice $k \in \mathbb{N}$ cu $k < n$ avem $k \in A$, avem $n \in A$.
Atunci $A = \mathbb{N}$.

Demonstrație

Fie $B := \{n \in \mathbb{N} \mid \text{pentru orice } k \in \mathbb{N} \text{ cu } k < n \text{ avem } k \in A\}$. Clar $B \subseteq A$, deci e suficient să arătăm $B = \mathbb{N}$, lucru pentru care folosim Principiul inducției.

Trivial, $0 \in B$. Dacă $n \in B$, atunci $n \in A$, deci pentru orice $k \leq n$, $k \in A$. Dar aceasta înseamnă că pentru orice $k < n^+$, $k \in A$, deci, din definiția lui B, $n^+ \in B$.

În continuare, vom demonstra proprietățile uzuale ale relației de ordine pe $\mathbb{N}$ cu ajutorul celor două principii de inducție.

Tranzitivitatea

Demonstrăm că $<$ este tranzitivă, adică că pentru orice k, m, $n \in \mathbb{N}$ cu $k < m$ și $m < n$, avem $k < n$.

Fie k, m cu $k < m$. Demonstrăm prin inducție după n că dacă $m < n$, atunci $k < n$.

Pentru $n = 0$, știm că nu putem avea $m < 0$ (ar însemna $m \in \emptyset$), deci concluzia este trivial adevărată.

Presupunem acum că dacă $m < n$, atunci $k < n$ și vrem să arătăm că dacă $m < n^+$, atunci $k < n^+$. Presupunem $m < n^+$, deci $m < n$ sau $m = n$. Dacă $m < n$, avem din ipoteza de inducție $k < n$, deci $k < n^+$, iar dacă $m = n$, avem că $k < n$ (și deci din nou că $k < n^+$) din faptul că $k < m$.

Ireflexivitatea

Demonstrăm acum că $<$ este ireflexivă, adică că pentru orice $n \in \mathbb{N}$, nu avem $n < n$.

Clar, nu avem $0 < 0$ (fiindcă $\emptyset \notin \emptyset$). Pentru pasul de inducție, trebuie să arătăm că pentru orice n, dacă $n^+ < n^+$, avem $n < n$.

Fie $n \in \mathbb{N}$. Dacă $n^+ < n^+$, atunci $n^+ < n$ – caz în care, cum $n < n^+$, ne folosim de tranzitivitate pentru a deduce $n < n$ – sau $n^+ = n$, caz în care $n < n$ rezultă imediat.

Am demonstrat, deci, că $<$ este relație de ordine strictă. În particular, a fost mai ușor să demonstrăm astfel decât dacă ar fi fost să demonstrăm direct că $\leq$ este relație de ordine parțială.

Injectivitatea operației de succesor

Lemă

Fie $n, m \in \mathbb{N}$ cu $n^+ = m^+$. Atunci $n = m$.

Demonstrație

Presupunem $n \neq m$. Avem

$$m \cup \{m\} = n \cup \{n\},$$

deci $m \in n \cup \{n\}$, iar cum $m \neq n$, avem $m \in n$, deci $m < n$, iar pe de altă parte avem $n \in m \cup \{m\}$, iar cum $n \neq m$, avem $n \in m$, deci $n < m$. Dar faptul că $m < n$ și $n < m$ contrazice asimetria lui $<$.

O proprietate

Demonstrăm acum următorul rezultat ajutător.

Lemă

Pentru orice $n, m \in \mathbb{N}$ cu $n < m$, avem $n^+ \leq m$.

Demonstrație

Fie n și demonstrăm prin inducție după m. Cazul $m = 0$ este trivial, cum nu este posibil ca $n < 0$.

Presupunem adevărat că dacă $n < m$, avem $n^+ \leq m$ și demonstrăm că dacă $n < m^+$, avem $n^+ \leq m^+$. Presupunem, deci $n < m^+$. Atunci $n < m$ sau $n = m$. Dacă $n < m$, din ipoteza de inducție avem $n^+ \leq m$, deci $n^+ \leq m^+$. Dacă $n = m$, atunci $n^+ = m^+$ și deci $n^+ \leq m^+$.

Ordine totală

Folosind lema anterioară, putem arăta că $\leq$ este o relație de ordine totală pe $\mathbb{N}$, deci că pentru orice m, $n \in \mathbb{N}$, avem $m \leq n$ sau $n \leq m$. Fie m și demonstrăm prin inducție după n.

Știm că pentru orice $m \in \mathbb{N}$, $0 \leq m$, ceea ce ne asigură pasul de bază.

Presupunem adevărată ipoteza de inducție, deci că avem $m \leq n$ sau $n < m$. Dacă $m \leq n$, atunci $m < n^+$. Dacă $n < m$, din lemă avem că $n^+ \leq m$, iar demonstrația este încheiată.

Bună ordine

Relația $\leq$ pe $\mathbb{N}$ este și exemplul *par excellence* de bună ordine, am putea spune chiar prototipul definiției.

Pentru a demonstra aceasta, fie $X \subseteq \mathbb{N}$ ce nu admite minim. Vrem să arătăm $X = \emptyset$, adică $\mathbb{N} \setminus X = \mathbb{N}$.

Din Principiul inducției complete, e suficient să arătăm că pentru orice n astfel încât pentru orice $k < n$ avem $k \notin X$, avem $n \notin X$. Presupunem că este fals, deci că există $n \in X$ astfel încât pentru orice $k < n$, $k \notin X$. Dar atunci, pentru orice $m \in X$, nu avem $m < n$, deci $n \leq m$. Ca urmare, n este minimul lui X, contradicție.

Fie A o mulțime. Numim **șir** A-valuat o familie care are imaginea inclusă în A și care are drept domeniu fie un număr natural n (caz în care îl numim **șir finit** de lungime n), fie pe $\mathbb{N}$ (caz în care îl numim **șir infinit**). Vom scrie șirurile finite și folosind notații precum

$$(a_i)_{i<n}.$$

Observăm că orice șir A-valuat aparține mulțimii $\mathcal{P}(\mathbb{N} \times A)$. Ca urmare, există mulțimea tuturor șirurilor A-valuate. Vom nota mulțimea tuturor șirurilor A-valuate *finite* cu $\mathrm{Seq}_{\mathrm{fin}}(A)$, iar pentru orice $n \in \mathbb{N}$, vom nota mulțimea tuturor șirurilor A-valuate de lungime n cu $\mathrm{Seq}_n(A)$.

Menționăm că aceste șiruri reprezintă formalizarea listelor de lungime arbitrară pe care am semnalizat-o anterior.

Definiții recursive

În matematică, se folosesc deseori (după cum am amintit și în Introducerea istorică) definiții recursive. Vom da de această dată ca exemplu definiția funcției factorial:

$$f(0) := 1, \qquad f(n+1) := (n+1) \cdot f(n).$$

Astfel de definiții enumeră condiții pe care o funcție trebuie să le satisfacă și lasă să se înțeleagă că există și este unică o asemenea funcție. Acest lucru nu este însă imediat și trebuie demonstrat.

Teorema recursiei

Fie A o mulțime, $a \in A$, $g : A \times \mathbb{N} \to A$. Atunci există și este unică o funcție $f : \mathbb{N} \to A$ astfel încât $f(0) = a$ și pentru orice $n \in \mathbb{N}$, $f(n^+) = g(f(n), n)$.

Unicitatea rezultă imediat prin inducție. Existența o arătăm în continuare.

Fie X mulțimea tuturor acelor $R \in \mathcal{P}(\mathbb{N} \times A)$ cu proprietatea că $(0, a) \in R$ și pentru orice $n \in \mathbb{N}$, $z \in A$ cu $(n, z) \in R$ avem $(n^+, g(z, n)) \in R$. Atunci X este o mulțime Moore pe $\mathbb{N} \times A$ și putem lua pe S ca fiind minimul ei. Este suficient să arătăm că S este grafic între $\mathbb{N}$ și A, i.e. că pentru orice $n \in \mathbb{N}$ există și este unic $b \in A$ cu $(n, b) \in S$.

Existența rezultă imediat (exercițiu!). Pentru unicitate, considerăm B mulțimea acelor $n \in \mathbb{N}$ cu proprietatea că există și este unic $b \in A$ cu $(n, b) \in S$. Arătăm prin inducție că $B = \mathbb{N}$. Pentru 0, cum $(0, a) \in S$, presupunând prin absurd că ar exista $b \neq a$ cu $(0, b) \in S$, se arată (exercițiu!) că $S \setminus \{(0, b)\} \in X$, contrazicând faptul că S este minim. Presupunem acum că $n \in B$ și vrem $n^+ \in B$. Fie z cu $(n, z) \in S$, atunci avem $(n^+, g(z, n)) \in S$. La fel, presupunem că ar exista $b \neq g(z, n)$ cu $(n^+, b) \in S$, se arată (exercițiu!) că $S \setminus \{(n^+, b)\} \in X$, contrazicând faptul că S este minim.

Teorema recursiei complete

Oarecum analog Principiului inducției complete, avem următoarea teoremă, care ne permite să definim funcții ce depind de valori ale lor dinaintea celei precedente pasului curent, de exemplu șirul lui Fibonacci dat ca exemplu în Introducerea istorică.

Teorema recursiei complete

Fie A o mulțime, $g : \mathrm{Seq}_{\mathrm{fin}}(A) \to A$. Atunci există și este unică o funcție $f : \mathbb{N} \to A$ astfel încât pentru orice $n \in \mathbb{N}$, $f(n) = g((f(i))_{i<n})$.

Schițăm doar demonstrația. Construim, folosind Teorema recursiei, $F : \mathbb{N} \to \mathrm{Seq}_{\mathrm{fin}}(A)$, prin $F(0) := \emptyset$ și pentru orice $n \in \mathbb{N}$, $F(n^+) := F(n) \cup \{(n, g(F(n)))\}$.

Atunci $f := (\mathbb{N}, A, \bigcup \mathrm{Im} F)$ este funcția căutată.

Teorema recursiei parametrizate

În aplicații pe care le vom vedea imediat, vom avea nevoie și de următoarea formă aparent mai puternică de recursie.

Teorema recursiei parametrizate

Fie A, P mulțimi, $a : P \to A$, $g : P \times A \times \mathbb{N} \to A$. Atunci există și este unică o funcție $f : P \times \mathbb{N} \to A$ astfel încât pentru orice $p \in P$, $f(p, 0) = a(p)$ și pentru orice $p \in P$ și $n \in \mathbb{N}$, $f(p, n^+) = g(p, f(p, n), n)$.

Pentru a o demonstra, definim $G : A^P \times \mathbb{N} \to A^P$, pentru orice $x \in A^P$, $n \in \mathbb{N}$, $p \in P$, prin $G(x, n)(p) := g(p, x(p), n)$ și apoi definim funcția $F : \mathbb{N} \to A^P$ recursiv, prin $F(0) := a$ și pentru orice $n \in \mathbb{N}$, $F(n^+) := G(F(n), n)$. Atunci putem defini f, pentru orice $p \in P$ și $n \in \mathbb{N}$, prin $f(p, n) := F(n)(p)$. Putem acum verifica:

$$\begin{aligned} f(p, 0) &= F(0)(p) = a(p) \\ f(p, n^+) &= F(n^+)(p) = G(F(n), n)(p) = g(p, F(n)(p), n) \\ &= g(p, f(p, n), n). \end{aligned}$$

Adunarea

Dacă în Teorema recursiei parametrizate luăm $A := \mathbb{N}$, $P := \mathbb{N}$, $a := \mathrm{id}_{\mathbb{N}}$ și $g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definită, pentru orice a, b, $c \in \mathbb{N}$, prin $g(a, b, c) := b^+$, obținem că există o unică funcție $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ce verifică:

- pentru orice $m \in \mathbb{N}$, $+(m, 0) = m$;
- pentru orice m, $n \in \mathbb{N}$, $+(m, n^+) = (+(m, n))^+$.

Vom numi funcția $+$ **adunarea numerelor naturale** și vom nota, pentru orice m, $n \in \mathbb{N}$, $m + n := +(m, n)$. De pildă, putem calcula:

$$1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2.$$

$$1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3.$$

Comutativitatea adunării

În acest moment, putem demonstra că adunarea este comutativă, adică că pentru orice m, $n \in \mathbb{N}$, $m + n = n + m$.

Demonstrăm prin inducție dublă, după n iar apoi după m. Pentru $n = 0$ și $m = 0$, obținem $0 + 0 = 0 + 0$, adevărat, iar la pasul inductiv pentru m avem

$$m^+ + 0 = m^+ = (m + 0)^+ = (0 + m)^+ = 0 + m^+.$$

La pasul inductiv pentru n, avem pentru $m = 0$ că

$$0 + n^+ = (0 + n)^+ = (n + 0)^+ = n^+ = n^+ + 0,$$

iar la pasul inductiv pentru m avem

$$\begin{aligned} m^+ + n^+ &= (m^+ + n)^+ = (n + m^+)^+ = (n + m)^{++} = (m + n)^{++} \\ &= (m + n^+)^+ = (n^+ + m)^+ = n^+ + m^+. \end{aligned}$$

Comentarii

În acest mod, se pot demonstra și alte proprietăți ale adunării numerelor naturale și se pot introduce și celelalte operații uzuale pe $\mathbb{N}$ (înmulțirea, ridicarea la putere) împreună cu proprietățile lor.

Apoi, așa cum s-a studiat la cursurile de algebră și analiză, odată ce aceste fapte sunt complet justificate, se pot construi numerele întregi, raționale, reale. Noi vom presupune în continuare toate faptele aferente lor ca fiind cunoscute.

Dinamici punctate, morfisme

Definiție

Un triplet (A, z, s) se numește **dinamică punctată** dacă $z \in A$ și $s : A \to A$.

De exemplu, $(\mathbb{N}, 0, (\cdot)^+)$ este o dinamică punctată.

Definiție

Fie (A, z, s), (A', z', s') dinamici punctate. Un **morfism** între ele este o funcție $f : A \to A'$ astfel încât $f(z) = z'$ și, pentru orice $a \in A$, $f(s(a)) = s'(f(a))$.

Se observă că, dacă (A, z, s) este o dinamică punctată, $\mathrm{id}_A : A \to A$ este morfism. De asemenea, compunerea a două morfisme este morfism.

Propoziție

Dacă un morfism între două dinamici punctate este bijectiv, atunci funcția inversă lui este tot morfism. Spunem că morfismul este **izomorfism** și că cele două dinamici punctate sunt **izomorfe**.

Dinamici punctate inițiale

Definiție

O dinamică punctată (A, z, s) se numește **inițială** dacă, pentru orice dinamică punctată (A', z', s'), există și este unic un morfism $f : A \to A'$.

Acest tip de enunț este ceea ce se numește în teoria categoriilor (și în algebră în general) o **proprietate de universalitate**. Ca exemplu de dinamică punctată inițială, avem chiar pe $(\mathbb{N}, 0, (\cdot)^+)$ (este o consecință imediată a Teoremei recursiei).

Propoziție

Fie (A, z, s), (A', z', s') dinamici punctate inițiale. Atunci ele sunt izomorfe.

Demonstrație

Din inițialitate, avem morfisme $f : A \to A'$ și $g : A' \to A$. Cum $g \circ f : A \to A$ și $\mathrm{id}_A : A \to A$, rezultă că $g \circ f = \mathrm{id}_A$. Analog, $f \circ g = \mathrm{id}_{A'}$.

Dinamici punctate inițiale (cont.)

Propoziție

Fie (A, z, s), (A', z', s') dinamici punctate izomorfe. Presupunem că (A, z, s) este inițială. Atunci (A', z', s') este inițială.

Demonstrație

Avem un izomorfism $f : A \to A'$. Fie (A'', z'', s'') o dinamică punctată. Vrem să arătăm că există un unic morfism $h : A' \to A''$.

Pentru existență, știm că există un morfism $g : A \to A''$. Luăm $h := g \circ f^{-1}$.

Pentru unicitate, fie h, $h' : A' \to A''$ morfisme. Atunci $h \circ f$, $h' \circ f : A \to A''$ sunt morfisme, deci $h \circ f = h' \circ f$. Compunând la dreapta cu f^{-1}, obținem $h = h'$.

Dinamici punctate Peano

Definiție

O dinamică punctată (A, z, s) se numește **Peano** dacă (i) $z \notin \mathrm{Im} s$; (ii) s este injectivă; (iii) pentru orice $B \subseteq A$ cu $z \in B$ și $s_*(B) \subseteq B$, avem $B = A$.

Această noțiune formalizează **axiomele lui Peano**. Clar, $(\mathbb{N}, 0, (\cdot)^+)$ este o dinamică punctată Peano.

Următoarele două propoziții sunt lăsate ca exercițiu.

Propoziție

Fie (A, z, s), (A', z', s') dinamici punctate izomorfe. Presupunem că (A, z, s) este Peano. Atunci (A', z', s') este Peano.

Propoziție (Teorema lui Dedekind)

Orice dinamică punctată Peano este izomorfă cu $(\mathbb{N}, 0, (\cdot)^+)$.

Legătura dintre concepte

Propoziție

Fie (A, z, s) o dinamică punctată. Atunci ea este inițială dacă și numai dacă ea este Peano.

Demonstrație

De la stânga la dreapta, din inițialitate, avem că (A, z, s) este izomorfă cu $(\mathbb{N}, 0, (\cdot)^+)$, care este Peano. Celălalt sens se demonstrează analog, folosind celelalte propoziții.

Aceste considerente ne arată că putem lucra, în loc de $\mathbb{N}$, cu orice dinamică punctată inițială/Peano, interpretând-o ca formând „numerele naturale”. Așadar, lucrul cu numerele naturale în teoria mulțimilor nu este condiționat de alegerea unui anume „model”. Totuși, ținând cont de asta, la curs și la seminar vom lucra doar cu $\mathbb{N}$-ul deja definit. Similar, avem și pentru $\mathbb{R}$, cu structura sa canonică, o caracterizare până la izomorfism, anume ca fiind unicul corp ordonat complet. De aceea, putem lucra cu mai multe „modele” pentru $\mathbb{R}$ (șiruri Cauchy, tăieturi Dedekind etc.).