

Logică matematică și teoria mulțimilor
Curs Semestrul I
Universitatea „Ștefan cel Mare” din Suceava

Andrei Alexandru

Curs 1: Logică propozițională și a predicatelor

Asumăm că toate obiectele teoriei sunt mulțimi, altfel spus nu se face distincția între elemente și mulțimi.

Definiție 1. Se numește enunț (sau expresie) a limbajului formal un șir finit de simboluri, format după o serie de reguli:

1. Simboluri de tip nume care descriu mulțimi. Sunt două tipuri de nume: nume constant (care determină un obiect bine precizat) și nume variabil (care determină un obiect neprecizat). Există o mulțime infinită de nume: x, y, z, a, A, B, C etc..
2. Paranteze “(” și “)” care au rolul de a delimita porțiuni de expresie pentru a elimina ambiguitățile.
3. Conectori logici care au ca scop construcția de expresii pornind de la expresii date. Astfel, dacă P și Q sunt expresii deja construite atunci:

$(P) \wedge (Q)$ (se citește P și Q)

$(P) \vee (Q)$ (se citește P sau Q)

$\neg(P)$ (se citește non P)

4. Cuantificatori logici:

Cuantificatorul universal: $\forall$ (oricare) o variabilă se referă la toate obiectele dintr-o expresie.

Cuantificatorul existențial: $\exists$ (există) o variabilă se referă la măcar un obiect dintr-o expresie.

Exemplu 1.

1. $(\forall x)P(x)$ - pentru orice x are loc P
2. $(\exists x)P(x)$ - există un x pentru care are loc P

Definiție 2. Fie o expresie P . Spunem că:

- variabila x este liberă în expresia P dacă x apare în P , dar P nu conține nici o cuantificare a lui x (nu avem prezente în P subșiruri de forma $\forall x \dots$ sau $\exists x \dots$). De exemplu: $x > 0$.
- variabila x este legată în expresia P dacă x nu este liberă (există în P subșiruri de forma $\forall x \dots$ sau $\exists x \dots$). De exemplu: $x^2 > 0, \forall x \in \mathbb{R}; \forall x \in \mathbb{R}, x^2 > 0$.

Definiție 3. O expresie P care nu conține variabile libere se numește propoziție.

Definiție 4. O expresie P care conține variabile libere $P(x_1, \dots, x_n)$ se numește predicat. Dacă $x_1, \dots, x_n$ se înlocuiesc cu constantele $c_1, \dots, c_n$, atunci $P(c_1, \dots, c_n)$ este o propoziție.

Definiție 5 (Semantică). Oricărei propoziții i se asociază o unică valoare de adevăr: 0 (propoziție falsă) sau 1 (propoziție adevărată).

Definiție 6. Două propoziții sunt echivalente dacă au aceeași valoare de adevăr.

Definiție 7 (Disjuncția). Fie p și q propoziții. Disjuncția propozițiilor p și q este adevărată dacă cel puțin una dintre propoziții p sau q este adevărată. Se notează $p \vee q$.

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Definiție 8 (Conjuncția). Fie p și q propoziții. Conjuncția propozițiilor p și q este adevărată dacă atât p cât și q sunt adevărate. Se notează $p \wedge q$.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Definiție 9 (Negația). Fie p o propoziție. Negația lui p este adevărată dacă p este falsă. Se notează $\neg p$.

p	$\neg p$
0	1
1	0

Definiție 10 (Implicația). Fie p și q propoziții. Propoziția $\neg p \vee q$ se scrie prescurtat $p \rightarrow q$. Această propoziție înseamnă că dacă p este adevărată, atunci q este adevărată. Astfel spus, $p \rightarrow q$ este adevărată dacă fie p este falsă, fie p este adevărată și atunci q este adevărată. Interpretare: “ p este condiție suficientă pentru q ”, “dacă are loc p , atunci are loc q ”, “din p rezultă q ”, “ q consecință a lui p ”.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Definiție 11 (Echivalența). Fie p și q propoziții. Propoziția $p \leftrightarrow q$ este adevărată dacă au loc implicațiile $p \rightarrow q$ și $q \rightarrow p$. Interpretare: “ p este condiție necesară și suficientă pentru q ”, “are loc p dacă și numai dacă are loc q ”.

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Definiție 12.

Se numește tautologie o propoziție care este întotdeauna adevărată.

Se numește contradicție o propoziție care este întotdeauna falsă.

Demonstrația unei tautologii (contradicții) se face, de regulă, utilizând valorile de adevăr. De exemplu, $(\neg(p \wedge q)) \leftrightarrow (\neg p \vee \neg q)$ deoarece $\neg(p \wedge q)$ este adevărată dacă și numai dacă $\neg p \vee \neg q$ este adevărată :

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Teorema 1. Fie p, q, r propoziții. Avem următoarele tautologii:

1. $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r)), ((p \vee q) \vee r) \leftrightarrow (p \vee (q \vee r))$ (asociativitatea operatorilor $\wedge, \vee$),
2. $(p \wedge q) \leftrightarrow (q \wedge p), (p \vee q) \leftrightarrow (q \vee p)$ (comutativitatea operatorilor $\wedge, \vee$),
3. $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r)), (p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$ (distributivitate),
4. $(\neg(p \wedge q)) \leftrightarrow (\neg p \vee \neg q), (\neg(p \vee q)) \leftrightarrow (\neg p \wedge \neg q)$ (legile lui De Morgan),
5. $\neg(\neg p) \leftrightarrow p$ (legea dublei negații),
6. $p \vee \neg p, \neg(p \wedge \neg p)$ (legea terțului exclus),
7. $(p \wedge \neg p) \rightarrow q$ (pornind de la o contradicție, deducem că orice este adevărat),
8. $\neg(p \rightarrow q) \leftrightarrow (p \wedge \neg q)$ (negarea implicației),
9. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ (regula silogismului),
10. $(p \rightarrow q) \leftrightarrow ((p \wedge \neg q) \rightarrow (r \wedge \neg r))$ (regula de demonstrație prin reducerea la absurd adică din presupunerea că p și $\neg q$ sunt adevărate rezultă o contradicție),
11. $(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \neg q) \rightarrow r)$,
12. $(p \rightarrow q) \leftrightarrow \neg q \rightarrow \neg p$.

Teorema 2 (Tautologii în logica predicatelor). $\forall P, Q, R$ avem:

1. $\neg((\forall x)(P(x)) \leftrightarrow (\exists x)(\neg P(x)))$
 $\neg((\exists x)(P(x)) \leftrightarrow (\forall x)(\neg P(x)))$
2. $((\forall x)(\forall y)(P(x, y)) \leftrightarrow ((\forall y)(\forall x)(P(x, y)))$
 $((\exists x)(\exists y)(P(x, y)) \leftrightarrow ((\exists y)(\exists x)(P(x, y)))$
3. $(\forall x)(P(x)) \rightarrow (\exists x)(P(x))$
4. Fie s o propoziție. Atunci:

$$s \wedge ((\exists x)(p(x)) \leftrightarrow ((\exists x)(s \wedge p(x)))$$

$$s \vee ((\forall x)(q(x)) \leftrightarrow ((\forall x)(s \vee q(x)))$$

Ordinea cuantificatorilor într-un predicat este importantă. De exemplu, fie șirul $(x_n) \subseteq \mathbb{R}$. Spunem că $x_n \rightarrow x$ dacă $\forall \epsilon > 0, \exists n_\epsilon \in \mathbb{N}, \forall n \geq n_\epsilon, |x_n - x| < \epsilon$. Așadar fiecare n_ϵ depinde de ϵ , adică pentru fiecare ϵ am putea avea un alt n_ϵ astfel încât să aibă loc proprietatea menționată. Pe de altă parte, într-un grup $(G, \cdot)$ avem $\exists e \in G, \forall x \in G, x \cdot e = e \cdot x = x$, ceea ce spune că același e (element neutru) există pentru toți acei $x \in G$.

Definiție 13 (Deducția logică). *O propoziție Q este consecință a propozițiilor $P_1, \dots, P_n$ dacă Q este adevărată atunci când $P_1, \dots, P_n$ adevărate. Propozițiile $P_1, \dots, P_n$ se numesc premise iar Q este concluzie.*

Notăție: $\frac{P_1, \dots, P_n}{Q}$

Scheme clasice de deducție:

1. Modus Ponens: $\frac{P, P \rightarrow Q}{Q}$
2. Reducere la absurd: $\frac{P, \neg Q \rightarrow \neg P}{Q}$
3. Silogism: $\frac{P \rightarrow Q, Q \rightarrow R}{P \rightarrow R}$
4. Silogism disjunctiv: $\frac{P \vee Q, \neg P}{Q}$
5. Contrapozitie: $\frac{P \rightarrow Q}{\neg Q \rightarrow \neg P}$
6. Analiza cazurilor: $\frac{P \vee R, P \rightarrow Q, R \rightarrow Q}{Q}$

Definiție 14 (Metode clasice de demonstrație).

1. Reuniunea premiselor: înlocuim $\frac{P}{R \rightarrow Q}$ cu $\frac{P, R}{Q}$,
2. Demonstrație prin contrapozitie: înlocuim $\frac{P, R}{Q}$ cu $\frac{P, \neg Q}{\neg R}$,
3. Demonstrație prin reducere la absurd: în loc de $\frac{P}{Q}$ arătăm că $P \wedge \neg Q$ contradicție.

Curs 2: Mulțimi și operații de mulțimi

Noțiuni primare (de la care pornim în definirea celorlalte concepte):

- mulțime; toate obiectele teoriei sunt mulțimi;
- relație de apartenență: $a \in A$ înseamnă A conține pe a .

Toate elementele unei mulțimi sunt mulțimi.

Axiomele teoriei mulțimilor

Axioma 1 (Axioma extensionalității). *Pentru orice două mulțimi A și B , avem*

$$((\forall a)(a \in A \leftrightarrow a \in B)) \rightarrow A = B$$

Această axiomă precizează faptul că dacă două mulțimi conțin fix aceleași elemente, atunci ele sunt egale. Altfel spus, o mulțime este precis determinată de elementele sale. Implicația inversă este evidentă. Dacă A, B sunt mulțimi, atunci spunem că $A \subseteq B$ (A inclus în B sau A submulțime a lui B) dacă $(\forall a)((a \in A) \rightarrow (a \in B))$. Astfel $A = B \Leftrightarrow A \subseteq B$ și $B \subseteq A$.

Axioma 2 (Axioma mulțimii părților).

$$(\forall A)(\exists P)((\forall a)(a \in P \leftrightarrow a \subseteq A))$$

Pentru orice mulțime A există o mulțime P care conține exact submulțimile lui A . Mai mult, P este unică cu această proprietate din axioma extensionalității.

Axioma 3 (Axioma reuniunii). *Pentru orice mulțime A , există o mulțime având ca elemente toate elementele mulțimilor din A .*

$$(\forall A)(\exists B)(\forall x)((x \in B) \leftrightarrow (\exists c)(c \in A \wedge x \in c))$$

Notăm

$$B = \bigcup_{c \in A} c = \{x \mid x \in c \wedge c \in A\}.$$

Axioma 4 (Axioma schemă a substituției).

Definiție 1. O expresie $E(x, y)$ se numește relație funcțională dacă pentru orice x există cel mult un y astfel încât $E(x, y)$ este adevărată:

$$(\forall x)(\forall y)(\forall z)((E(x, y) \wedge E(x, z)) \rightarrow y = z)$$

Axioma: *Pentru orice relație funcțională $E(x, y)$ avem:*

$$(\forall a)(\exists b)(\forall y)(y \in b \leftrightarrow ((\exists x)(x \in a \wedge E(x, y))))$$

Informal, există imaginea mulțimii a prin relația funcțională E . Această imagine este unică conform axiomei extensionalității.

Proprietate 1 (Proprietatea selecției). *(este o consecință a axiomei schemă a substituției)*

Pentru orice mulțime A și orice expresie $P(x)$, există mulțimea elementelor din A care satisfac proprietatea P .

$$(\forall A)(\exists B)(\forall x)(x \in B \leftrightarrow (x \in A \wedge P(x))).$$

Demonstrație. Fie $E(x, y) : 'x = y \wedge P(y)'$. Evident E este relație funcțională. Din axioma substituției avem

$$\begin{aligned} & (\forall A)(\exists B)(\forall y)(y \in B \leftrightarrow (\exists x)(x \in A \wedge E(x, y))) \\ & (\forall A)(\exists B)(\forall y)(y \in B \leftrightarrow (\exists x)(x \in A \wedge x = y \wedge P(y))) \\ & (\forall A)(\exists B)(\forall y)(y \in B \leftrightarrow (y \in A \wedge P(y))). \end{aligned}$$

□

Observație 1. Pentru $P(x) : 'x \neq x'$ aplicând proprietatea selecției obținem o unică mulțime $\emptyset := \{x \in A \mid x \neq x\}$. Această mulțime este unică și evident nu conține nici un element. Deci $\emptyset \subseteq A$ pentru orice mulțime A .

Observație 2. Se pot defini mulțimile $A \cap B$ și $A - B$ pentru orice mulțimi A și B :

$$\begin{aligned} A \cap B &= \{x \in A \mid x \in B\} \\ A - B &= \{x \in A \mid x \notin B\} \end{aligned}$$

Axioma 5 (Axioma infinității).

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

Teorema 1. Fie a și b două mulțimi. Atunci există c o mulțime care conține doar elementele a și b

$$(\forall a)(\forall b)(\exists c)(\forall x)((x \in c) \leftrightarrow (x = a \vee x = b)).$$

Demonstrație. Știm că $\exists \emptyset$. Din axioma mulțimii părților există $\mathcal{P}(\emptyset)$. Deoarece $\emptyset \subseteq \emptyset$, avem $\emptyset \in \mathcal{P}(\emptyset)$. Mai mult $\mathcal{P}(\emptyset) = \{\emptyset\}$. $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$. Fie expresia $E(x, y)$:

$$E(x, y) : '(x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)'.$$

$E(x, y)$ este relație funcțională și conform axiomei substituției există $\{a, b\}$ - imaginea mulțimii $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$, care este unică conform axiomei extensionalității. □

Fie a și b mulțimi. Atunci, aplicând teorema precedentă mulțimilor a și a avem că există $\{a\}$. Evident există $\{a, b\}$. Aplicând din nou teorema anterioară mulțimilor $\{a\}$ și $\{a, b\}$, există mulțimea

$$\{\{a\}, \{a, b\}\} : \stackrel{not.}{=} (a, b)$$

Observație 3. $\forall a, b, c, d$ mulțimi avem $(a, b) = (c, d) \Leftrightarrow a = c$ și $b = d$. Recursiv definim $(a_1, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$.

Definiție 2. Fie A și B două mulțimi, $a \in A$ și $b \in B$. Atunci $(a, b) = \{\{a\}, \{a, b\}\}$. Cum $\{a\} \in \mathcal{P}(A \cup B)$ și $\{a, b\} \in \mathcal{P}(A \cup B)$, avem $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Conform proprietății selecției putem defini

$$\begin{aligned} A \times B &= \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists a)(\exists b)(x = \{\{a\}, \{a, b\}\} \wedge a \in A \wedge b \in B)\} \\ &= \{(a, b) \mid a \in A \wedge b \in B\}. \end{aligned}$$

Curs 3: Relații binare. Funcții

Definiție 1. Fie A și B două mulțimi. O relație binară între elementele lui A și B este o submulțime $\rho \subseteq A \times B$.

Notăm $(a, b) \in \rho$ cu apb .

Definiție 2. O relație binară $\rho \subseteq A \times B$ se numește funcție dacă $\forall a \in A, \exists! b \in B$ astfel încât apb .

Mai exact: ρ este funcție de la A la $B \Leftrightarrow$

- $\forall a \in A \exists b \in B$ astfel încât $(a, b) \in \rho$
- $(a, b) \in \rho \wedge (a, b') \in \rho \Rightarrow b = b'$

Notăm $(a, b) \in \rho$ cu $\rho(a) = b$.

Definiție 3. Fie A, B, C mulțimi. Fie $\rho \subseteq A \times B$ și $\eta \subseteq B \times C$ două relații binare.

1. Domeniul lui ρ este mulțimea $D_\rho = \{a \in A \mid \exists b \in B \text{ cu } (a, b) \in \rho\}$
2. Imaginea lui ρ este mulțimea $I_\rho = \{b \in B \mid \exists a \in A \text{ cu } (a, b) \in \rho\}$
3. Inversa relației ρ este relația $\rho^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \rho\}$
4. Compusa relațiilor η și ρ este $\eta \circ \rho = \{(a, c) \in A \times C \mid \exists b(b \in B \wedge apb \wedge b\eta c)\}$

Observație 1.

$$(\rho^{-1})^{-1} = \rho$$

$$(\rho \circ \eta \circ \sigma) = (\rho \circ \eta) \circ \sigma = \rho \circ (\eta \circ \sigma)$$

$$(\rho \circ \eta)^{-1} = \eta^{-1} \circ \rho^{-1}$$

Definiție 4. Fie A și B două mulțimi și $X \subseteq A, Y \subseteq B, f : A \rightarrow B$ funcție.

1. Mulțimea $f(X) = \{f(x) \mid x \in X\} \subseteq B$ se numește imaginea lui X prin f .
2. Mulțimea $f^{-1}(Y) = \{x \in A \mid f(x) \in Y\} \subseteq A$ se numește imaginea inversă a lui Y prin f .

Definiție 5. Fie I o mulțime și X o mulțime fixată. O funcție $u : I \rightarrow X$ se numește familie de mulțimi indexată după I .

Notăm $(u(i))_{i \in I}$ cu $(X_i)_{i \in I}$ sau $\{X_i \mid i \in I\}$.

Avem

$$\bigcup_{i \in I} X_i = \{x \in X \mid \exists i \in I \text{ astfel încât } x \in X_i\}$$

$$\bigcap_{i \in I} X_i = \{x \in X \mid \forall i \in I \text{ avem } x \in X_i\}$$

Definim

$$\prod_{i \in I} X_i = \{f : I \rightarrow \bigcup_{i \in I} X_i \mid f(i) \in X_i, \forall i \in I\}$$

Propoziție 1. Fie A, B două mulțimi $f : A \rightarrow B$ o funcție și $(X_i)_{i \in I} \subseteq A, (y_j)_{j \in J} \subseteq B$. Avem

$$\begin{aligned} f\left(\bigcup_{i \in I} X_i\right) &= \bigcup_{i \in I} f(X_i) \\ f\left(\bigcap_{i \in I} X_i\right) &\subseteq \bigcap_{i \in I} f(X_i) \\ f^{-1}\left(\bigcup_{j \in J} Y_j\right) &= \bigcup_{j \in J} f^{-1}(Y_j) \\ f^{-1}\left(\bigcap_{j \in J} Y_j\right) &= \bigcap_{j \in J} f^{-1}(Y_j) \end{aligned}$$

Definiție 6. Fie A și B două mulțimi și $f : A \rightarrow B$ o funcție. Spunem că:

- i) f este injectivă dacă $\forall x, y \in A, f(x) = f(y) \Rightarrow x = y$.
- ii) f este surjectivă dacă $\forall y \in B, \exists x \in A$ astfel încât $f(x) = y$.
- iii) f este bijectivă dacă f este injectivă și surjectivă.
- iv) f este inversabilă dacă $\exists g : B \rightarrow A$ astfel încât $(g \circ f)(x) = x, \forall x \in A$ și $(f \circ g)(y) = y, \forall y \in B$.

Funcția $1_A : A \rightarrow A, 1_A(x) = x$ se numește identitate și este bijectivă.

O funcție $f : A \rightarrow B$ este injectivă dacă și numai dacă $f(\bigcap_{i \in I} X_i) = \bigcap_{i \in I} f(X_i)$ pentru orice familie de mulțimi $(X_i)_{i \in I} \subseteq A$.

Teorema 1. Fie $f : A \rightarrow B$ o funcție. Următoarele afirmații sunt echivalente:

- i) f este injectivă,
- ii) pentru orice mulțime C și pentru orice funcții $g, h : C \rightarrow A$, dacă $f \circ g = f \circ h$ rezultă $g = h$,
- iii) dacă $A \neq \emptyset$ atunci $\exists g : B \rightarrow A$ astfel încât $g \circ f = 1_A$.

Demonstrație. ii) $\Rightarrow$ i). Presupunem prin reducere la absurd că $\exists x_1, x_2 \in A$ cu $x_1 \neq x_2$ și $f(x_1) = f(x_2)$. Fie $C = \{x_1, x_2\}$. Definim $g, h : C \rightarrow A$ prin $g(x_1) = x_1, g(x_2) = x_2, h(x_1) = x_1, h(x_2) = x_1$. Evident, $g \neq h$, dar $f(g(x_2)) = f(x_2) = f(x_1) = f(h(x_2))$ și $f(g(x_1)) = f(x_1) = f(h(x_1))$ adică $f \circ g = f \circ h$.

i) $\Rightarrow$ iii). Definim $g : B \rightarrow A$ prin $g(b) = \begin{cases} f^{-1}(\{b\}), b \in \text{Im} f \\ a_0, b \notin \text{Im} f \end{cases}$ unde $f(A) = \text{Im} f$

este imaginea lui f și $a_0 \in A$ este fixat. Din injectivitatea lui f , avem că $f^{-1}(\{b\})$ este o mulțime formată dintr-un singur element pentru $b \in \text{Im} f$ și, deci, g este bine definită și avem $(g \circ f)(a) = g(f(a)) = a, \forall a \in A$.

iii) $\Rightarrow$ ii). Fie $g : B \rightarrow A$ cu $(g \circ f)(a) = a$. Fie $a_1, a_2 \in A$ astfel încât $f(a_1) = f(a_2)$. Atunci $g(f(a_1)) = g(f(a_2))$ de unde $a_1 = a_2$. Deci f este injectivă. Dacă $f \circ g' = f \circ h'$, atunci $\forall a \in C$ avem că $f(g'(a)) = f(h'(a)) \xrightarrow{f \text{ inj.}} g'(a) = h'(a) \Rightarrow g' = h'$. $\square$

Teorema 2. Fie $f : A \rightarrow B$ o funcție. Următoarele afirmații sunt echivalente:

- i) f este surjectivă,
- ii) pentru orice mulțime C și pentru orice funcții $g, h : B \rightarrow C$, dacă $g \circ f = h \circ f$, atunci $g = h$,
- iii) Există o funcție $g : B \rightarrow A$ astfel încât $f \circ g = 1_B$.

Demonstrație. Exercițiu după cursul în care este prezentată Axioma alegerii. □

Teorema 3. Fie $f : A \rightarrow B$ și $g : B \rightarrow C$ două funcții. Atunci

- i) $g \circ f$ este injectivă $\Rightarrow f$ injectivă,
- ii) $g \circ f$ este surjectivă $\Rightarrow g$ surjectivă,
- iii) f, g sunt injective $\Rightarrow g \circ f$ injectivă,
- i) f, g sunt surjective $\Rightarrow g \circ f$ surjectivă,
- v) f este inversabilă $\Leftrightarrow f$ este bijectivă,
- vi) Fie $f^* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$, $f^*(Y) = f^{-1}(Y)$, $\forall Y \in \mathcal{P}(B)$. Atunci f^* injectivă $\Leftrightarrow f$ surjectivă.

Fie A o mulțime. Se poate demonstra ușor că funcția

$$g : \mathcal{P}(A) \rightarrow \{f : A \rightarrow \{0, 1\} \mid f \text{ funcție}\}$$

$$g(X) = \chi_X \text{ unde } \chi_X : A \rightarrow \{0, 1\}, \chi_X(a) = \begin{cases} 1, a \in X \\ 0, a \in A - X \end{cases} \text{ este bijectivă.}$$

χ_X se numește funcția caracteristică a lui X . Astfel oricărei submulțimi a lui A i se asociază în mod unic funcția sa caracteristică.

Teorema 4. Fie A o mulțime și $B, C \subseteq A$. Avem

1. $\chi_B^2 = \chi_B$, $\chi_\emptyset = 0$, $\chi_A = 1$, unde prin 1 am notat funcția $h : A \rightarrow \{0, 1\}$, $h(x) = 1, \forall x \in A$;
2. $B \subseteq C \Rightarrow \chi_B \leq \chi_C$ (adică $\chi_B(x) \leq \chi_C(x), \forall x \in A$);
3. $B = C \Leftrightarrow \chi_B = \chi_C$;
4. $\chi_{A-B} = 1 - \chi_B$; ($\chi_{C_B} = 1 - \chi_B$) C_B este complementara lui B față de A .
5. $\chi_{B \cap C} = \chi_B \cdot \chi_C$
6. $\chi_{B \cup C} = \chi_B + \chi_C - \chi_B \chi_C$
7. $\chi_{B-C} = \chi_B - \chi_B \chi_C$

Exemplu 1. Fie $A, B \subseteq X$ două mulțimi:

- Demonstrăm că $A - B = A \cap C_B$ (unde, dacă $A, B \subseteq X$, $C_B := X - B$). Avem $\chi_{A-B} = \chi_A - \chi_A \chi_B$. Dar $\chi_{A \cap C_B} = \chi_A(1 - \chi_B) = \chi_A - \chi_A \chi_B$ de unde rezultă $A - B = A \cap C_B$ (conform Teorema 4.3)
- Demonstrăm că $C_{A \cup B} = C_A \cap C_B$. Avem

$$\chi_{C_{A \cup B}} = (1 - \chi_{A \cup B}) = 1 - (\chi_A + \chi_B - \chi_A \chi_B) = 1 - \chi_A - \chi_B + \chi_A \chi_B.$$

$$\chi_{C_A \cap C_B} = \chi_{C_A} \cdot \chi_{C_B} = (1 - \chi_A)(1 - \chi_B) = 1 - \chi_A - \chi_B + \chi_A \chi_B.$$

Curs 4: Relații de echivalență

Fie A o mulțime nevidă și ρ o relație pe A . Spunem că ρ este relație de echivalență dacă:

- ρ este reflexivă: $\forall a \in A, a\rho a$;
- ρ este simetrică: $\forall a, b \in A, a\rho b \rightarrow b\rho a$;
- ρ este tranzitivă: $\forall a, b, c \in A, a\rho b \wedge b\rho c \rightarrow a\rho c$.

Fie A o mulțime și ρ o relație de echivalență pe A .

- Mulțimea $[a]_\rho := \{b \in A \mid b\rho a\}$ se numește clasa de echivalență a lui a . Dacă $b \in [a]_\rho$ spunem că b este echivalent cu a modulo ρ .
- Mulțimea $A/\rho := \{[a]_\rho \mid a \in A\}$ se numește mulțimea factor (cât) a lui A în raport cu ρ .
- Mulțimea $S \subseteq A$ se numește sistem de reprezentanți pentru clasele de echivalență modulo ρ dacă orice element a lui A este echivalent modulo ρ cu exact un element din S . Existența unui sistem de reprezentanți pentru orice mulțime A și orice relație ρ peste A este echivalentă cu axioma alegerii. S este sistem de reprezentanți pentru A și ρ dacă:

$$(\forall a \in A)(\exists s \in S)(a\rho s) \wedge (\forall u, v \in S)((u\rho v) \rightarrow u = v).$$

Exemplu 1. Pe mulțimea numerelor întregi $\mathbb{Z}$ definim relația $\equiv_n$ prin

$$a \equiv_n b : \stackrel{\text{not.}}{=} a \equiv b(\text{mod } n) \Leftrightarrow n \mid a - b$$

$$[a]_{\equiv_n} := [a] = \{b \in \mathbb{Z} \mid n \mid a - b\}$$

$$\mathbb{Z}/\equiv_n := \mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

Propoziție 1. Fie A o mulțime și ρ o relație de echivalență pe A . Fie $a, b \in A$. Atunci următoarele afirmații sunt echivalente:

- i) $a\rho b$
- ii) $a \in [b]_\rho$
- iii) $[a]_\rho = [b]_\rho$.

Demonstrație. i) $\rightarrow$ ii) din definiție.

ii) $\rightarrow$ iii). Fie $c \in [a]_\rho$. Deci $c\rho a$. Deoarece $a \in [b]_\rho$ avem $a\rho b$, deci $c\rho b$ din tranzitivitatea lui ρ . Astfel $c \in [b]_\rho$. Reciproc $d \in [b]_\rho \Rightarrow d\rho b$. Dar $a\rho b$, deci $b\rho a$ din simetria lui ρ . Astfel $d\rho a$ din tranzitivitatea lui ρ , adică $d \in [a]_\rho$. Avem $[a]_\rho \subseteq [b]_\rho$ și $[b]_\rho \subseteq [a]_\rho$ de unde obținem $[a]_\rho = [b]_\rho$.

iii) $\rightarrow$ i). Deoarece $a\rho a$ (ρ este reflexivă) avem că $a \in [a]_\rho$. Întrucât $[a]_\rho = [b]_\rho$, vom avea $a \in [b]_\rho$ adică $a\rho b$. $\square$

Definiție 1. Fie A o mulțime și $P \subseteq \mathcal{P}(A) - \emptyset$. Spunem că P este o partiție a lui A dacă:

$$1. A = \bigcup_{X \in P} X$$

$$2. \forall X_1, X_2 \in P, X_1 \neq X_2 \Rightarrow X_1 \cap X_2 = \emptyset$$

Teorema 1.

1. Dacă ρ este o relație de echivalență pe A , atunci A/ρ este o partiție a lui A .
2. Dacă P este o partiție a lui A , atunci ρ_P este o relație de echivalență peste A , unde $a\rho_P b \Leftrightarrow \exists X \in P$ astfel încât $a, b \in X$.
3. Fie $R(A)$ mulțimea relațiilor de echivalență peste A și $\mathcal{P}(A)$ mulțimea partițiilor lui A . Dacă definim:

$$f : R(A) \rightarrow \mathcal{P}(A), f(\rho) = A/\rho, \forall \rho \in R(A),$$

$$g : \mathcal{P}(A) \rightarrow R(A), g(P) = \rho_P, \forall P \in \mathcal{P}(A).$$

atunci $f \circ g = 1_{\mathcal{P}(A)}$ și $g \circ f = 1_{R(A)}$.

Demonstrație.

1. Din reflexivitatea lui ρ avem $a \in [a]_\rho, \forall a \in A$. Deci $[a]_\rho \neq \emptyset, \forall a \in A$. Fie $[a]_\rho, [b]_\rho \in A/\rho$ cu $[a]_\rho \neq [b]_\rho$. Presupunem prin reducere la absurd că $\exists c \in [a]_\rho \cap [b]_\rho$. Atunci $c \in [a]_\rho$, adică $c\rho a$ și $c \in [b]_\rho$ adică $c\rho b$. Astfel $a\rho c$ și $c\rho b$, deci $a\rho b$ din tranzitivitatea lui ρ . Obținem $[a]_\rho = [b]_\rho$, o contradicție.

Mai rămâne să arătăm că $A = \bigcup_{[a] \in A/\rho} [a]_\rho$. Fie $a \in A$. Atunci $a \in [a]_\rho$ deoarece ρ este reflexivă. Deci $A \subseteq \bigcup_{[a] \in A/\rho} [a]_\rho$.

Incluziunea inversă este evidentă deoarece $b \in [a]_\rho \Rightarrow b \in A$.

2. Știm că $A = \bigcup_{X \in P} X$ și că $\forall X_1, X_2 \in P, X_1 \neq X_2 \Rightarrow X_1 \cap X_2 = \emptyset$. Fie $a \in A$. Atunci $a \in \bigcup_{X \in P} X$, deci $\exists X \in P$ astfel încât $a \in X$. Deci $a\rho_P a$, adică ρ_P este reflexivă. Dacă avem $a\rho_P b$, evident $\exists X \in P$ astfel încât $a, b \in X$, deci și $b, a \in X$, adică $b\rho_P a$, deci ρ_P este simetrică.

Fie acum $a, b, c \in A$ cu $a\rho_P b$ și $b\rho_P c$. Deci $\exists X_1 \in P$ cu $a, b \in X_1$ și $\exists X_2 \in P$ cu $b, c \in X_2$. Cum $b \in X_1 \cap X_2 \Rightarrow X_1 = X_2$.

Deci $a, b, c \in X_1 \Rightarrow a\rho_P c$, prin urmare ρ_P este tranzitivă.

3. Fie $P \in \mathcal{P}(A)$. Arătăm că $f(g(P)) = P$ adică $A/\rho_P = P$ sau, echivalent, $\{[a]_{\rho_P} \mid a \in A\} = P$. Fie $a \in A$. Atunci $[a]_{\rho_P} = \{b \in A \mid b\rho_P a\} = \{b \in A \mid \exists X \in P, a, b \in X\}$. Cum $a \in A = \bigcup_{X \in P} X \Rightarrow \exists! X \in P$ astfel încât $a \in X$. Deci $[a]_{\rho_P} = X \in P$. Astfel $\{[a]_{\rho_P} \mid a \in A\} \subset P$. Reciproc. Fie $X \in P$. Deci $X \neq \emptyset$, adică $\exists x \in X$. Avem $[x]_{\rho_P} = \{y \in A \mid \exists Y \in P, x, y \in Y\}$. Dar $x \in X, x \in Y \Rightarrow x \in X \cap Y$. Cum $X \cap Y = \emptyset$ dacă $X \neq Y$, avem $[x]_{\rho_P} = X$, deci $P \subset \{[a]_{\rho_P} \mid a \in A\}$.

Acum arătăm că $g(f(\rho)) = \rho$ pentru orice $\rho \in R(A)$, adică $\rho_{A/\rho} = \rho, \forall \rho \in R(A)$. Fie $\rho \in R(A)$. Fie $(a, b) \in A \times A$.

Atunci $(a, b) \in \rho_{A/\rho} \Leftrightarrow \exists X \in A/\rho$ astfel încât $a, b \in X \Leftrightarrow \exists z \in A, a, b \in [z]_\rho \Leftrightarrow \exists z \in A, a\rho z \wedge b\rho z \Leftrightarrow a\rho b \Leftrightarrow (a, b) \in \rho$. Deci $\rho_{A/\rho} = \rho$.

□

- Fie $f : A \rightarrow B$ o funcție. Definim relația $\rho := \ker f$ pe mulțimea A prin: $a\rho b \Leftrightarrow f(a) = f(b), \forall a, b \in A$. $\ker f$ este nucleul lui f . Evident $\ker f$ este relație de echivalență.

- Fie ρ o relație de echivalență pe mulțimea A . Funcția $p_\rho : A \rightarrow A/\rho, p_\rho(a) = [a]_\rho$ se numește proiecția canonică a lui A .

Teorema 2. Fie $f : A \rightarrow B$ o funcție și $\ker f$ relația de echivalență pe A : $a \ker f b \Leftrightarrow f(a) = f(b)$. Atunci există o unică funcție bijectivă $\bar{f} : A/\ker f \rightarrow \text{Im} f$ astfel încât $f = i \circ \bar{f} \circ p_{\ker f}$, unde $i : \text{Im} f \rightarrow B, i(x) = x, \forall x \in \text{Im} f$.

Demonstrație. Se definește $\bar{f}([x]_{\ker f}) = f(x)$.

- $\bar{f}$ este bine definită. Presupunem că pentru $x, y \in A/\ker f$ avem $[x]_{\ker f} = [y]_{\ker f}$. Atunci $x \ker f y$, adică $(x, y) \in \ker f$, de unde $f(x) = f(y)$ și deci $\bar{f}([x]_{\ker f}) = \bar{f}([y]_{\ker f})$.
- $\bar{f}$ este injectivă. Presupunem că pentru $x, y \in A$ avem $\bar{f}([x]_{\ker f}) = \bar{f}([y]_{\ker f})$ adică $f(x) = f(y)$, deci $x \ker f y$ de unde $[x]_{\ker f} = [y]_{\ker f}$.
- f surjectivă. Fie $y \in \text{Im} f$. Atunci $\exists x \in A$ astfel încât $f(x) = y$. Deci $\bar{f}([x]_{\ker f}) = y$,
- f unică cu proprietatea din enunț. Fie $g : A/\ker f \rightarrow \text{Im} f$ astfel încât $f = i \circ g \circ p_{\ker f}$. Atunci $(i \circ g) \circ p_{\ker f} = (i \circ \bar{f}) \circ p_{\ker f}$ de unde, deoarece $p_{\ker f}$ este surjectivă, rezultă că $i \circ g = i \circ \bar{f} \xrightarrow{i \text{ inj.}} g = \bar{f}$.

□

Curs 5: Relații de ordine. Latici

Relații de ordine

Fie ρ o relație de ordine pe A . Spunem că ρ este relație de ordine pe A dacă:

1. ρ este reflexivă: $\forall a \in A, a \rho a$;
2. ρ este antisimetrică: $\forall a, b \in A ((a \rho b \text{ și } b \rho a) \rightarrow a = b)$;
3. ρ este tranzitivă: $\forall a, b, c \in A ((a \rho b \text{ și } b \rho c) \rightarrow a \rho c)$.

Notatie. Relațiile de ordine se notează, de regulă, cu $\leq$ sau $\sqsubseteq$.

Fie $\leq$ o relație de ordine peste A . Spunem că $(A, \leq)$ este mulțime ordonată sau mulțime parțial ordonată.

- Dacă $\forall a, b \in A$ avem $a \leq b$ sau $b \leq a$, spunem că $(A, \leq)$ este total ordonată ($\leq$ este relație de ordine totală).

Fie $(A, \leq)$ o mulțime parțial ordonată și $X \subseteq A$.

- Un element $m \in A$ se numește minorant pentru X dacă $m \leq x, \forall x \in X$.
- Un element $M \in A$ se numește majorant pentru X dacă $x \leq M, \forall x \in X$.
- Submulțimea X se numește minorată dacă are un minorant.
- Submulțimea X se numește majorată dacă are un majorant.
- Dacă $m \in X$ este minorant pentru X , spunem că X are un minimum (prim element).
- Dacă $M \in X$ este majorant pentru X , spunem că X are un maximum (ultim element).

Exemplu 1. $(\mathbb{N}, \leq)$ este o mulțime total ordonată. Similar $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ cu relațiile de ordine uzuale sunt total ordonate.

Exemplu 2. $(\mathbb{N}, |)$, unde $|$ este definită prin: $a | b \Leftrightarrow \exists c \in \mathbb{N}$ astfel încât $b = a \cdot c$, este o mulțime parțial ordonată. Totuși $(\mathbb{N}, |)$ nu este total ordonată (de exemplu $3 \nmid 4$ și $4 \nmid 3$). 0 este maximum pentru $(\mathbb{N}, |)$ iar 1 este minimum pentru $(\mathbb{N}, |)$.

Definiție 1. Fie $(A, \leq)$ o mulțime parțial ordonată:

- $m \in A$ se numește element maximal a lui A dacă $\forall x \in A, m \leq x \Rightarrow m = x$ (nu există în A un element mai mare decât m);
- $M \in A$ se numește element minimal a lui A dacă $\forall x \in A, x \leq M \Rightarrow x = M$ (nu există în A un element mai mic decât M).

Definiție 2. Fie $(A, \leq)$ o mulțime parțial ordonată și $X \subseteq A$. Fie $\text{Maj}(X)$ mulțimea majoranților lui X și $\text{Min}(X)$ mulțimea minoranților lui X . Dacă există c care este minimum al lui $\text{Maj}(X)$, atunci $c \in \text{Maj}(X)$ este supremumul lui X . Dacă există d care este maximum al lui $\text{Min}(X)$, atunci $d \in \text{Min}(X)$ este infimumul lui X .

Observație 1. Fie $(A, \leq)$ o mulțime parțial ordonată și $X \subseteq A$.

- Fie $d \in A$. Avem d infimum al lui X (notat $d = \wedge X$ sau $d = \inf X$) dacă și numai dacă:

- $d \leq x, \forall x \in X$ (d este minorant al lui X),
- $\forall d' \in A$ astfel încât $d' \leq x, \forall x \in X \Rightarrow d' \leq d$ (d este mai mare decât orice alt minorant al lui X).

- Fie $c \in A$. Avem c supremum al lui X (notat $c = \vee X$ sau $c = \sup X$) dacă și numai dacă:

- $x \leq c, \forall x \in X$ (c este majorant al lui X),
- $\forall c' \in A$ astfel încât $x \leq c', \forall x \in X \Rightarrow c \leq c'$ (c este mai mic decât orice alt majorant al lui X).

Propoziție 1. Fie $(A, \leq)$ o mulțime parțial ordonată și fie $X, Y \subseteq A$ astfel încât există $\vee X, \vee Y, \wedge X, \wedge Y$. Atunci:

- Dacă $x \in X$ avem $\wedge X \leq x \leq \vee X$,
- Dacă $x \in A$ și $x \leq \wedge X$, rezultă $x \leq y, \forall y \in X$,
- Dacă $y \in A$ și $\vee X \leq y$, rezultă $z \leq y, \forall z \in X$.
- Dacă $X \subseteq Y$, atunci $\vee X \leq \vee Y$ și $\wedge Y \leq \wedge X$.

Demonstrație. Primele trei puncte sunt evidente. Pentru ultimul punct:

Fie $x \in X$. Cum $X \subseteq Y \Rightarrow x \in Y \Rightarrow x \leq \vee Y$. Deci $x \leq \vee Y, \forall x \in X$. Din definiția $\vee X$ avem $\vee X \leq \vee Y$. $\square$

Definiție 3. Fie $(A, \leq)$ o mulțime parțial ordonată. Spunem că $(A, \leq)$ este bine ordonată dacă pentru orice $X \subseteq A, X \neq \emptyset$ avem că X are minimum.

Teorema 1. Dacă $(A, \leq)$ este o mulțime parțial ordonată, următoarele afirmații sunt echivalente:

1. $(A, \leq)$ este bine ordonată
2. $(A, \leq)$ este total ordonată, există m minimul lui A și pentru orice $X \subseteq A$, dacă X satisface proprietățile:

- i) $m \in X$
- ii) pentru orice $a \in A, \{x \in A \mid x \leq a\} \subseteq X \Rightarrow a \in X$

atunci $X = A$.

Demonstrație. 1) $\Rightarrow$ 2). Presupunem că $(A, \leq)$ este bine ordonată. Atunci $\forall a, b \in A, \{a, b\}$ are minimum. Deci $a \leq b$ sau $b \leq a$, de unde A este total ordonată. Evident $\exists m = \text{minimum } A$. Presupunem prin reducere la absurd că există $X \subseteq A$ care satisface condițiile i) și ii) dar $X \neq A$.

Deci $A - X \neq \emptyset$, adică $\exists y = \text{minimum } A - X$. Atunci $y \in A - X$, deci $y \notin X$. Fie $x \in A$ cu $x \leq y$. Atunci $x \in X$ pentru că, altfel, s-ar contrazice definiția lui $y = \text{minimum } A - X$. Deci $\{x \in A \mid x \leq y\} \subseteq X$ și din ii) urmează $y \in X$, contradicție cu $y \notin X$.

2) $\Rightarrow$ 1). Presupunem prin reducere la absurd, că are loc 2) dar $(A, \leq)$ nu este bine ordonată. Atunci $\exists X \subseteq A, X \neq \emptyset$ dar X nu are minimum. Vom avea:

- i') $m \in A - X$ pentru că dacă $m \in X$, cum $X \subseteq A$, am avea $m = \text{minimum } X$, o contradicție.
- ii') Pentru orice $a \in A$, să presupunem că avem $\{x \in A \mid x \leq a\} \subseteq A - X$. Dacă am avea $a \in X$, deoarece A este total ordonată și elementele mai mici decât a aparțin lui $A - X$, s-ar obține $a = \text{minimum } X$, o contradicție. Deci $a \in A - X$ și astfel $A - X$ satisface proprietățile i') și ii'), de unde, conform 2), avem $A - X = A$, adică $X = \emptyset$, o contradicție.

□

Propoziție 2. Fie $(A, \leq)$ o mulțime bine ordonată și $f : A \rightarrow A$ o funcție strict crescătoare, adică $x < y \Rightarrow f(x) < f(y), \forall x, y \in A$. Atunci $a \leq f(a)$ pentru orice $a \in A$.

Demonstrație. Să presupunem că $\exists x_0 \in A$ astfel încât $f(x_0) < x_0$. Astfel $X = \{x \in A \mid f(x) < x\} \neq \emptyset$ și $\exists m = \text{minimum } X, m \in X$. Deci $f(m) < m$. Deoarece f strict crescătoare, avem $f(f(m)) < f(m)$, adică $f(m) \in X$ și deci $m \leq f(m)$, o contradicție. □

Latici

Definiție 4. O mulțime parțial ordonată $(L, \leq)$ se numește latice dacă pentru orice elemente $x, y \in L$ există infimum $\{x, y\} \in L$ și supremum $\{x, y\} \in L$.

Exemplu 3. $(P(X), \subseteq)$ este latice pentru orice mulțime X . Dacă $A, B \subseteq X$, atunci infimum $\{A, B\} = A \cap B$ și supremum $\{A, B\} = A \cup B$.

Exemplu 4. $(\mathbb{N}, |)$ este latice. Dacă $a, b \in \mathbb{N}$ atunci infimum $(a, b) = \text{c.m.m.d.c. } (a, b)$ și supremum $(a, b) = \text{c.m.m.m.c. } (a, b)$.

Teorema 2. O mulțime L poate fi înzestrată cu o relație de ordine laticială $\leq$ dacă și numai dacă există două funcții $\vee : L \times L \rightarrow L$ și $\wedge : L \times L \rightarrow L$ care satisfac proprietățile:

i) asociativitate:

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

$$a \vee (b \vee c) = (a \vee b) \vee c$$

ii) comutativitate:

$$a \wedge b = b \wedge a$$

$$a \vee b = b \vee a$$

iii) absorbție:

$$a \vee (a \wedge b) = a$$

$$a \wedge (a \vee b) = a$$

pentru orice $a, b, c \in L$.

Demonstrație. Dacă $(L, \leq)$ este latice, atunci definim $a \wedge b = \text{infimum}\{a, b\}$, respectiv $a \vee b = \text{supremum}\{a, b\}$.

i) Asociativitate

Fie $x = (a \vee b) \vee c$ și $y = a \vee (b \vee c)$. Avem că $a \vee b \leq x$ și $c \leq x$, de unde $a \leq x, b \leq x, c \leq x$ și deci $a \leq x$ și $(b \vee c) \leq x$ adică $y \leq x$. Analog $x \leq y$. Asociativitatea $\wedge$ este similară.

ii) Comutativitate

Evident $\infimum\{a, b\} = \infimum\{b, a\}$ și $\supremum\{a, b\} = \supremum\{b, a\}$.

iii) Absorbția

Fie $x = a \vee (a \wedge b)$. Avem $a \leq x$. Pe de altă parte $a \wedge b \leq a, a \leq a$ și deci $a \vee (a \wedge b) \leq a$ adică $x \leq a$. Deci $a = x$.

Reciproc, dacă există operațiile binare $\vee, \wedge$ cu proprietățile din enunț, definim $a \leq b \Leftrightarrow a \wedge b = a$. Arătăm că $a \vee b = \supremum\{a, b\}$, respectiv $a \wedge b = \infimum\{a, b\}, \forall a, b \in L$. Pentru început avem $a \vee b = b \Leftrightarrow a \wedge b = a$ (*).

Într-adevăr, conform proprietății de absorbție avem $a \vee b = b \Rightarrow a \wedge (a \vee b) = a \wedge b \Rightarrow a = a \wedge b$. De asemenea $a \wedge b = a \Rightarrow b \vee (a \wedge b) = a \vee b \Rightarrow b = a \vee b$.

Mai mult, dovedim că $a \wedge a = a$ și $a \vee a = a$. (**).

Într-adevăr $a = a \wedge (a \vee a)$ și $a \vee a = a \vee (a \wedge (a \vee a)) = a$. Analog cealaltă proprietate. Să arătăm că $\leq$ este relație de ordine:

- reflexivitatea: $a \leq a \Leftrightarrow a \wedge a = a$, adevărată conform (**).
- antisimetria: $a \leq b$ și $b \leq a \Rightarrow a \wedge b = a$ și $b \wedge a = b$. Dar $a \wedge b = b \wedge a \Rightarrow a = b$.
- tranzitivitatea: fie $a \leq b$ și $b \leq c$. Atunci $a \wedge b = a$ și $b \wedge c = b$. Avem $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a \Rightarrow a \leq c$.

Arătăm că $a \wedge b = \infimum\{a, b\}$, conform (*), vom obține și $a \vee b = \supremum\{a, b\}$. Într-adevăr $a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b \Rightarrow a \wedge b \leq a$. Analog $a \wedge b \leq b$. Fie acum $c \in L$ astfel încât $c \leq a$ și $c \leq b$. Deci $c \wedge a = c$ și $c \wedge b = c$. Atunci $c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c$, deci $c \leq a \wedge b$. Astfel $a \wedge b = \infimum\{a, b\}$. $\square$

Definiție 5. Dacă $(L, \wedge, \vee)$ și $(L', \wedge, \vee)$ sunt latici, o funcție $f : L \rightarrow L'$ este morfism de latici dacă $f(x \wedge y) = f(x) \wedge f(y)$ și $f(x \vee y) = f(x) \vee f(y), \forall x, y \in L$. Dacă f este bijectiv, f se numește izomorfism.

Propoziție 3. Fie $(L, \wedge, \vee), (L', \wedge, \vee)$ două latici și $f : L \rightarrow L'$ o funcție:

- a) Dacă f este morfism de latici atunci $x \leq y \Rightarrow f(x) \leq f(y)$.
- b) Dacă f are proprietatea că $x \leq y \Leftrightarrow f(x) \leq f(y)$ și f este bijectivă, atunci f este morfism de latici.

Demonstrație.

- a) Fie $x, y \in L$ astfel încât $x \leq y$. Avem $x \vee y = y$. Deci $f(x \vee y) = f(y)$, adică $f(y) = f(x \vee y) = f(x) \vee f(y) \Rightarrow f(x) \leq f(y)$.
- b) Fie $x, y \in L$. Avem $x \leq x \vee y$ și $y \leq x \vee y$, deci $f(x) \leq f(x \vee y)$ și $f(y) \leq f(x \vee y)$.

Conform definiției supremului lui $\{f(x), f(y)\}$ ca fiind cel mai mic majorant al acestei mulțimi, avem $f(x) \vee f(y) \leq f(x \vee y)$ (*).

Să presupunem că z este un majorant al lui $f(x)$ și $f(y)$ adică $f(x) \leq z$ și $f(y) \leq z$. Deoarece $z \in L$ vom avea că există $t \in L$ astfel încât $z = f(t)$. Deci $f(x) \leq f(t)$ și $f(y) \leq f(t)$, de unde $x \leq t$ și $y \leq t$, și în final $x \vee y \leq t$, de unde $f(x \vee y) \leq f(t) = z$. Deci $f(x \vee y)$ este cel mai mic majorant al lui $f(x)$ și $f(y)$ adică $f(x \vee y) = f(x) \vee f(y)$. $\square$

Exemplu 5. Fie X, Y mulțimi și $f : X \rightarrow Y$ o funcție:

a) $f^* : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$, $f^*(Z) = f^{-1}(Z)$, $\forall Z \in \mathcal{P}(Y)$ este morfism de latici.

b) $f_* : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$, $f_*(Z) = f(Z)$, $\forall Z \in \mathcal{P}(X)$ este morfism de latici $\Leftrightarrow f$ este injectivă.

Curs 6: Latici complete

Propoziție 1. Fie $(P, \leq)$ o mulțime parțial ordonată. Următoarele afirmații sunt echivalente:

1. Pentru orice submulțime $X \subseteq P$, există cel mai mic majorant (supremum) al lui X , notat $\vee X$.
2. Pentru orice submulțime $X \subseteq P$, există cel mai mare minorant (infimum) al lui X , notat $\wedge X$.

Demonstrație. 1) $\Rightarrow$ 2). Fie $X \subseteq P$ și $D := \text{not.} \cap \{\downarrow x \mid x \in X\}$ unde $\downarrow x = \{y \in P \mid y \leq x\}$. Mai exact, D este mulțimea tuturor minoranților lui X . Conform 1) există $\vee D$. Arătăm că $\vee D = \wedge X$. Fie $x \in X$. Pentru orice $y \in D$, avem $y \leq x$, deci x este majorant al lui D și astfel $\vee D \leq x$. Cum x a fost arbitrar ales din X , avem $\vee D \in D$. Deoarece $\vee D$ este maximal între minoranții lui X și este el însuși un minorant al lui X , avem $\vee D = \wedge X$.

2) $\Rightarrow$ 1) Similar. □

Definiție 1. O mulțime parțial ordonată $(L, \leq)$ care satisface una dintre condițiile echivalente din propoziția anterioară (și, implicit, pe cealaltă) se numește *latice completă*.

Observație 1. $(L, \leq)$ latice completă $\Leftrightarrow \forall X \subseteq L (\exists \vee X \text{ și } \exists \wedge X)$.

Exemplu 1. Orice latice finită $(L, \leq)$ este completă.

Exemplu 2. $([0, 1], \leq)$ este latice completă.

Exemplu 3. $(\mathcal{P}(X), \subseteq)$ este latice completă pentru orice mulțime X . Pentru orice familie de submulțimi $(X_i)_{i \in I} \subseteq X$ avem că $\wedge \{X_i \mid i \in I\} = \bigcap_{i \in I} X_i$ și $\vee \{X_i \mid i \in I\} = \bigcup_{i \in I} X_i$.

Exemplu 4. Fie X o mulțime și $(L, \leq)$ o latice completă. Mulțimea $\mathcal{F} = \{f : X \rightarrow L \mid f \text{ funcție}\}$ formează o latice completă cu relația de ordine $\sqsubseteq$ definită prin $f \sqsubseteq g \Leftrightarrow f(x) \leq g(x), \forall x \in X$. Pentru orice familie $(f_i)_{i \in I} \subseteq \mathcal{F}$, avem $(\bigsqcup_{i \in I} f_i)(x) = \vee_{i \in I} \{f_i(x) \mid i \in I\}$.

Exemplu 5. Fie $(G, \cdot)$ un grup și $\mathcal{L}(G) = \{H \mid H \leq_{sg} G\}$ ($\mathcal{L}(G)$ este mulțimea subgrupurilor lui G). Atunci $(\mathcal{L}(G), \subseteq)$ este latice completă. Pentru orice $(H_i)_{i \in I} \subset \mathcal{L}(G)$ avem $\vee_{i \in I} H_i = [\bigcup_{i \in I} H_i]$ subgrup generat de $\bigcup_{i \in I} H_i$ adică cel mai mic subgrup al lui G care conține pe $\bigcup_{i \in I} H_i$ și $\wedge_{i \in I} H_i = \bigcap_{i \in I} H_i$.

Teorema 1 (Tarski-Knaster).

Fie $(L, \leq)$ o latice completă și $f : L \rightarrow L$ o funcție cu proprietatea că $\forall x, y \in L, x \leq y \Rightarrow f(x) \leq f(y)$.

Fie $P = \{x \in L \mid f(x) = x\}$. Atunci $(P, \leq)$ este nevidă și formează la rândul ei o latice completă.

Demonstrație.

- P este nevidă. Fie $D = \{d \in L \mid d \leq f(d)\}$. Evident $D \neq \emptyset$, deoarece $\wedge L : \stackrel{\text{not.}}{=} 0 \leq f(0)$. Fie $d_0 = \vee D$.

Pentru orice $d \in D$, avem $d \leq d_0$, și deci $f(d) \leq f(d_0)$, adică $d \leq f(d) \leq f(d_0)$. Deci $f(d_0)$ este majorant pentru D și, conform definiției supremumului lui D , avem $d_0 \leq f(d_0)$, adică $d_0 \in D$. Deoarece f păstrează ordinea pe L , pentru orice $x \in D$ avem $x \leq f(x) \Rightarrow f(x) \leq f(f(x)) \Rightarrow f(x) \in D$. Deci $f(d_0) \in D$, adică $f(d_0) \leq d_0$ întrucât d_0 este majorant pentru D . Obținem $f(d_0) = d_0$, deci $D \neq \emptyset$.

- P este latice completă. Evident $P \subseteq L$, deci există $\vee P \in L$. Rămâne să arătăm că $\vee X \in P$ pentru orice $X \subseteq P$ (știm că $\exists \vee X \in L$).

Fie $x \in X$ arbitrar. Avem $x \leq \vee X$, de unde $f(x) \leq f(\vee X) \xrightarrow{x \in P} x = f(x) \leq f(\vee X) \xrightarrow{\text{def. } \vee X} \vee X \leq f(\vee X)$. Fie $y \in L$ cu proprietatea $\vee X \leq y$. Atunci $f(\vee X) \leq f(y)$, deci $\vee X \leq f(\vee X) \leq f(y)$. Deci $\forall y \in L, \vee X \leq y \Rightarrow \vee X \leq f(y)$. (*)

Fie $D' = \{d \in L \mid f(d) \leq d \text{ și } \vee X \leq d\}$. Fie $e = \wedge D'$. Pentru orice $d \in D'$, avem $e \leq d$, deci $f(e) \leq f(d) \leq d$ și conform definiției lui $\wedge D'$, avem $f(e) \leq e$. Mai mult, $\vee X \leq d, \forall d \in D'$, deci $\vee X \leq \wedge D' = e$, deci $e \in D'$. Pentru orice $x \in D'$, avem $f(x) \leq x$, deci $f(f(x)) \leq f(x)$. De asemenea avem $\vee X \leq x$, de unde, conform (*) $\vee X \leq f(x)$, adică $f(x) \in D'$.

Deci $e \in D'$ și $f(e) \in D'$, adică $e \leq f(e)$. Obținem astfel $f(e) = e$, de unde $e \in P$ cu $\vee X \leq e$. Deci $e \in P$ este un majorant al lui X . Fie $e' \in P$ un alt majorant al lui X . Atunci $f(e') = e' \leq e'$ și $\vee X \leq e'$ ($\vee X$ există în L și e' este un majorant al lui X în L). În concluzie $e' \in D'$ și deci $e = \wedge D' \leq e'$. Astfel e este mai mic decât orice majorant al lui X , de unde obținem că e este supremumul lui X în P .

□

Observație 2.

- Cel mai mare element al lui P este $gf_P(f) = \vee\{d \in L \mid d \leq f(d)\}$.
- Cel mai mic element al lui P este $lf_P(f) = \wedge\{d \in L \mid f(d) \leq d\}$.

Curs 7: Latici distributive și Algebre Boole

Propoziție 1. Pentru o latice $(L, \wedge, \vee)$ următoarele afirmații sunt echivalente:

1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \forall a, b, c \in L$
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \forall a, b, c \in L$

Demonstrație. 1) $\Rightarrow$ 2). Fie $a, b, c \in L$. Notăm $x = a \vee b, y = a, z = c$. Atunci $(a \vee b) \wedge (a \vee c) = x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

De asemenea $(x \wedge y) \vee (x \wedge z) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) = a \vee ((a \wedge c) \vee (b \wedge c)) = (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c)$.

2) $\Rightarrow$ 1) analog.

□

Definiție 1. O latice $(L, \wedge, \vee)$ care satisface una dintre condițiile echivalente din propoziția precedentă (și implicit pe cealaltă) se numește latice distributivă.

Observație 1. În orice latice $(L, \wedge, \vee)$ au loc relațiile:

1. $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c), \forall a, b, c \in L$
2. $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c), \forall a, b, c \in L$

Demonstrație. Avem $a \wedge (b \vee c) \geq a \wedge b$ și $a \wedge (b \vee c) \geq a \wedge c$. Deci $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$ (conform definiției supremului). Am folosit relația:

$$a \leq b \Rightarrow \begin{cases} a \vee x \leq b \vee x \\ a \wedge x \leq b \wedge x \end{cases} \quad \forall x \in L.$$

Într-adevăr $a \leq b \Rightarrow a \leq b \leq b \vee x$ și $x \leq b \vee x$. Deci $a \vee x \leq b \vee x$. Similar cealaltă relație. □

Exemplu 1.

1. $(\mathcal{P}(X), \subseteq)$ este latice distributivă pentru orice mulțime X .
2. $(P, \leq)$ este latice distributivă dacă $\leq$ este o relație de ordine totală.
3. Fie $(L, \leq)$ o latice distributivă. Atunci $\mathcal{F} = \{f : X \rightarrow L \mid f \text{ funcție}\}$ este o latice distributivă pentru orice mulțime X , cu relația de ordine $\sqsubseteq$ definită prin $f \sqsubseteq g \Leftrightarrow f(x) \leq g(x), \forall x \in X$.
4. $(\mathbb{N}, |)$ este latice distributivă.

Definiție 2. O latice $(L, \wedge, \vee)$ se numește modulară, dacă, pentru orice $x, y, z \in L, x \leq z \Rightarrow x \vee (y \wedge z) = z \wedge (x \vee y)$.

Propoziție 2. Fie $(L, \wedge, \vee)$ o latice. Următoarele afirmații sunt echivalente:

1. L este latice modulară;

2. Pentru $a, x, y \in L$, avem

$$\begin{cases} a \wedge x = a \wedge y \\ a \vee x = a \vee y \\ x \leq y \end{cases} \Rightarrow x = y.$$

Demonstrație. 1) $\Rightarrow$ 2). Deoarece $x \leq y$, avem $x \vee (a \wedge y) = y \wedge (a \vee x) = y \wedge (a \vee y) = y$. Deci $y = x \vee (a \wedge y) = x \vee (a \wedge x) = x$ conform proprietății de absorbție.

2) $\Rightarrow$ 1). Fie $u, v, w \in L$ cu $u \leq w$. Notăm $x = u \vee (v \wedge w)$ și $y = (u \vee v) \wedge w$.

Avem $u \leq x \stackrel{u \leq w}{=} (u \wedge w) \vee (v \wedge w) \leq w \wedge (u \vee v) = y \leq w$.

Avem de arătat că $x = y$. Întrucât $x \leq y$ este suficient să dovedim că $x \vee v = y \vee v$ și $x \wedge v = y \wedge v$. Deoarece $x \leq y$, avem $x \vee v \leq y \vee v$. Cum $u \leq x$, avem $x \vee v \geq u \vee v \geq (u \vee v) \wedge w = y$. Dar $x \vee v \geq v$ și din definiția supremului avem $x \vee v \geq y \vee v$, adică $x \vee v = y \vee v$.

Deoarece $x \leq y$, avem $x \wedge v \leq y \wedge v$. Dar, pe altă parte $x \wedge v = [u \vee (v \wedge w)] \wedge v \geq (v \wedge w) \wedge v = v \wedge w \geq (v \wedge w) \wedge (u \vee v) = y \wedge v$. Deci $x \wedge v = y \wedge v$. $\square$

Observație 2. Orice latice distributivă este modulară.

Teorema 1. Fie $(L, \wedge, \vee)$ o latice. Următoarele afirmații sunt echivalente:

1. L este o latice distributivă;

2. Pentru $a, x, y \in L$ avem:

$$\begin{cases} a \wedge x = a \wedge y \\ a \vee x = a \vee y \end{cases} \Rightarrow x = y.$$

Demonstrație. 1) $\Rightarrow$ 2). Avem $x = x \vee (a \wedge x) = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = (a \vee y) \wedge (x \vee y) = y \vee (a \wedge x) = y \vee (a \wedge y) = y$.

2) $\Rightarrow$ 1). Fie $a, b, c \in L$. Verificăm că este îndeplinită legea de distributivitate

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Fie $x = [(a \wedge b) \vee c] \wedge (a \vee b)$ și $y = (b \vee c) \wedge [a \vee (b \wedge c)]$. Evident L este modulară (Vom nota “conform” cu “cf.”).

$$\begin{aligned} \bullet \text{ Avem } (a \wedge b) \vee (a \wedge c) &\stackrel{a \wedge b \leq a}{=} a \wedge [(a \wedge b) \vee c] \stackrel{\text{cf. absorbției}}{=} \\ &[(a \vee b) \wedge a] \wedge [(a \wedge b) \vee c] \stackrel{\text{cf. asociativității}}{=} \{[(a \wedge b) \vee c] \wedge (a \vee b)\} \wedge a = x \wedge a. \quad (1) \end{aligned}$$

$$\bullet \text{ Totodată } a \wedge (b \vee c) \stackrel{\text{cf. absorbției}}{=} \{a \wedge [a \vee (b \wedge c)]\} \wedge (b \vee c) \stackrel{\text{cf. asociativității}}{=} \{(b \vee c) \wedge [a \vee (b \wedge c)]\} \wedge a = y \wedge a. \quad (2)$$

$$\begin{aligned} \bullet \text{ Avem } x \wedge b &= [(a \wedge b) \vee c] \wedge (a \vee b) \wedge b \stackrel{\text{cf. absorbției}}{=} b \wedge [(a \wedge b) \vee c] \stackrel{a \wedge b \leq b}{=} \\ &(a \wedge b) \vee (b \wedge c). \quad (3) \end{aligned}$$

$$\begin{aligned} \bullet \text{ Totodată } y \wedge b &= \{(b \vee c) \wedge [a \vee (b \wedge c)]\} \wedge b \stackrel{\text{cf. asociativității}}{=} [b \wedge (b \vee c)] \wedge [a \vee (b \wedge c)] \stackrel{\text{cf. absorbției}}{=} \\ &b \wedge [a \vee (b \wedge c)] \stackrel{b \wedge c \leq b}{=} (b \wedge c) \vee (a \wedge b). \quad (4) \end{aligned}$$

Din (3) și (4) avem $x \wedge b = y \wedge b$. (5)

Avem, de asemenea, $x \vee b = \{[(a \wedge b) \vee c] \wedge (a \vee b)\} \vee b \xrightarrow[\text{modularitate}]{b \leq a \vee b} (a \vee b) \wedge \{b \vee [(a \wedge b) \vee c]\} \xrightarrow{\text{cf. asociativității}} (a \vee b) \wedge \{[b \vee (a \wedge b)] \vee c\} \xrightarrow{\text{cf. absorbției}} (a \vee b) \wedge (b \vee c). \quad (6)$

Totodată $y \vee b = \{(b \vee c) \wedge [a \vee (b \wedge c)]\} \vee b \xrightarrow[\text{cf. modularității}]{b \leq b \vee c} (b \vee c) \wedge \{b \vee [a \vee (b \wedge c)]\} \xrightarrow{\text{cf. asociativității}} (b \vee c) \wedge \{[b \vee (b \wedge c)] \vee a\} = (b \vee c) \wedge (b \vee a). \quad (7)$

Din (6) și (7) avem $x \vee b = y \vee b. \quad (8)$

Din (5) și (8), conform ipotezei avem $x = y$, deci $x \wedge a = y \wedge a$. Conform (1) și (2) rezultă că L este distributivă.

□

Observație 3. *Demonstrația și alte proprietăți ale laticelor distributive pot fi găsite în*

M. Tărnăuceanu. Probleme de algebră. Ed. univ. Al. I. Cuza, 2023.

Teorema 2. *Fie $(L, \wedge, \vee)$ o latice. Avem L distributivă $\Leftrightarrow (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a), \forall a, b, c \in L$.*

Definiție 3. *Fie $(L, \wedge, \vee)$ o latice ce admite un cel mai mic element $0 = \wedge L$ și un cel mai mare element $1 = \vee L$.*

1. *Un element $x' \in L$ se numește complement al lui $x \in L$ dacă $x' \wedge x = 0$ și $x' \vee x = 1$.*
2. *Dacă orice element al lui L admite un complement (respectiv un unic complement), L se numește latice complementată (respectiv latice unic complementată).*

Teorema 3. *Fie $(L, \wedge, \vee)$ o latice distributivă și $x \in L$. Dacă x are un complement, atunci acesta este unic.*

Demonstrație. Presupunem că x are doi complemenți x_1 și x_2 . Atunci $x_1 = x_1 \wedge 1 = x_1 \wedge (x \vee x_2) = (x_1 \wedge x) \vee (x_1 \wedge x_2) = 0 \vee (x_1 \wedge x_2) = x_1 \wedge x_2$. Deci $x_1 \leq x_2$, și analog, $x_2 = x_2 \wedge 1 = x_2 \wedge (x_1 \vee x) = (x_2 \wedge x_1) \vee (x_2 \wedge x) = x_2 \wedge x_1$, deci $x_2 \leq x_1$. Obținem $x_1 = x_2$. □

Definiție 4. *Fie $(L, \wedge, \vee)$ o latice. Dacă L este distributivă, complementată și admite un cel mai mic și un cel mai mare element, atunci L este latice Booleană.*

Propoziție 3. *Fie $(L, \wedge, \vee)$ o latice booleană și $a, b, c \in L$. Atunci*

- a) $0' = 1$ și $1' = 0$
- b) $a'' = a$
- c) $(a \vee b)' = a' \wedge b'$ și $(a \wedge b)' = a' \vee b'$
- d) $a \wedge b = 0 \Leftrightarrow a \leq b'$
- e) $a \leq b \Rightarrow b' \leq a'$

Demonstrație. a) din definiție $0 \wedge 1 = 0$, respectiv $0 \vee 1 = 1$.

b) $a' \wedge a = 0$ și $a \vee a' = 1 \Rightarrow (a')' = a'' = a$.

c) Din distributivitatea lui L avem:

- $(a \vee b) \vee (a' \wedge b') = ((a \vee b) \vee a') \wedge ((a \vee b) \vee b') \xrightarrow{\text{asociativitate}} ((a \vee a') \vee b) \wedge (a \vee (b \vee b')) = (1 \vee b) \wedge (a \vee 1) = 1 \wedge 1 = 1.$
- $(a \vee b) \wedge (a' \wedge b') = (a \wedge (a' \wedge b')) \vee (b \wedge (a' \wedge b')) \xrightarrow{\text{asociativitate}} ((a \wedge a') \wedge b') \vee ((b \wedge b') \wedge a') = (0 \wedge b') \vee (0 \wedge a') = 0 \vee 0 = 0.$

Deci $(a \vee b)' = (a' \wedge b')$ din unicitatea complementului. Analog celelalte relații.

d) $\Rightarrow: a = a \wedge (b \vee b') = \underbrace{(a \wedge b)}_0 \vee (a \wedge b') = a \wedge b'. \text{ Deci } a \leq b'.$

Reciproc $\Leftarrow$: Dacă $a \leq b'$, atunci $a \wedge b \leq b' \wedge b = 0$, deci $a \wedge b = 0$.

e) Dacă $a \leq b \xRightarrow{d)} a \wedge b' = 0$ și $b' \wedge a = 0 \xRightarrow{d)} b' \leq a'.$

□

Exemplu 2. Pentru o mulțime X , $(\mathcal{P}(X), \subseteq) = (P(X), \cap, \cup)$ este latice booleană. Pentru $Y \in \mathcal{P}(X)$, avem $Y' = X - Y$.

Definiție 5. Un inel asociativ $(B, +, \cdot)$ cu element unitar 1 se numește inel Boole dacă $x^2 = x, \forall x \in B$.

Propoziție 4. Fie $(B, +, \cdot)$ un inel Boole. Atunci

a) $x + x = 0, \forall x \in B$,

b) B este comutativ.

Demonstrație. a) $x + x = (x + x)^2 = x + x + x + x \Rightarrow x + x = 0$,

b) $x, y \in B \Rightarrow x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx$. Deci $xy = -yx = (-1)yx = yx$ (deoarece $-yx = yx$ conform punctului a)).

□

Teorema 4 (Stone).

1. Fie $(L, \wedge, \vee, 0, 1, ')$ o latice booleană și definim operațiile:

$$a + b = (a \wedge b') \vee (a' \wedge b),$$

$$a \cdot b = a \wedge b.$$

Atunci $(L, +, \cdot)$ este inel Boole cu element unitar 1.

2. Fie $(B, +, \cdot, 0, 1)$ un inel Boole și definim:

$$a \vee b = a + b + ab,$$

$$a \wedge b = ab.$$

Atunci $(B, \wedge, \vee)$ este latice booleană, $a' = 1 + a, \forall a \in B, \vee B = 1$ și $\wedge B = 0$.

3. Corespondența dintre laticile boolene și inelele Boole stabilită la punctele 1) și 2) este bijectivă.

Demonstrație. Prin calcul direct.

□

Observație 4. Dacă X este o mulțime, atunci laticii Boolene $(P(X), \cap, \cup, \emptyset, X, \subseteq)$ îi corespunde inelul Boole $(\mathcal{P}(X), \Delta, \cap)$ unde $A \Delta B = (A - B) \cup (B - A)$.

Curs 8: Numere naturale. Principiile inducției matematice

Axiomatica Dedekind-Peano

- simbolul $=$ (marchează egalitatea a două obiecte);
- simbolul 0 (notează un număr natural fixat);
- variabile, constante, conectori logici.

Axiomele sunt:

1. Există un număr natural notat 0 .
2. Pentru orice număr natural n există și este unic determinat un număr natural numit succesorul lui n și notat $s(n)$ sau n^+ , $(\forall n)(\exists! s(n))$.
3. Orice două numere naturale cu același succesor sunt egale:

$$(\forall m)(\forall n)(s(m) = s(n) \Rightarrow m = n).$$

4. 0 nu este succesorul nici unui număr natural: $(\forall n)(s(n) \neq 0)$.
5. Pentru orice predicat cu o variabilă $P(n)$ are loc:

$$[P(0) \wedge (\forall n)(P(n) \rightarrow P(s(n)))] \rightarrow (\forall m)P(m).$$

Vom construi un model al acestei teorii axiomatice, mai exact, vom defini o mulțime $\mathbb{N}$, un element $0 \in \mathbb{N}$ și o funcție $s : \mathbb{N} \rightarrow \mathbb{N}$ care să satisfacă axiomele acestei teorii axiomatice.

Reamintim axioma infinității:

$$\exists X[\emptyset \in X \wedge (\forall y)(y \in X \rightarrow y \cup \{y\} \in X)].$$

Prin urmare putem construi șirul $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$. Arătăm în cele ce urmează că există o mulțime care conține doar aceste elemente.

Definiție 1. O mulțime α se numește ordinal dacă are următoarele proprietăți:

1. $(\forall x)(x \in \alpha \rightarrow x \subseteq \alpha)$;
2. Relația de apartenență definește o relație de ordine strictă care este o bună ordine pe α :
 - $\forall x, y, z \in \alpha$, din $x \in y$ și $y \in z$ se obține $x \in z$;
 - $\forall x, y \in \alpha$, din $x \in y$ se obține $y \notin x$;
 - $\forall \beta\{(\beta \subseteq \alpha \wedge \beta \neq \emptyset) \rightarrow \exists x[x \in \beta \wedge \forall y(y \in \beta \rightarrow (x = y \vee x \in y))]\}$

Orice submulțime nevidă a lui α are minimum în raport cu $\in$.

Definiție 2. Fie $(A, \leq)$ o mulțime ordonată. O submulțime B a lui A se numește segment inițial al lui A dacă are proprietatea că, pentru fiecare element $x \in B$, B conține toate elementele mai mici decât x : $\forall x(x \in B \rightarrow (\forall y(y \in A \wedge y \leq x) \rightarrow y \in B))$.

Propoziție 1. Fie $(A, \leq)$ o mulțime bine ordonată și B un segment inițial al lui A . Atunci $B = A$ sau există $a \in A$ astfel încât $B = \{x \in A \mid x \leq a\} \stackrel{\text{not.}}{=} B_a(A)$.

Demonstrație. Presupunem $B \neq A$, deci $A - B \neq \emptyset$, adică $A - B$ are minimum, i.e. $\exists a = \text{minimum } A - B$. Arătăm că $B_a(A) = B$.

Fie $x \in B$. Dacă $a \leq x \Rightarrow a \in B$, contradicție. Cum A este total ordonată, avem $x < a$. Invers, fie $x \in B_a(A)$. Atunci $x \leq a \Rightarrow x \in B$ (pentru că dacă $x \in A - B$ am contrazice faptul că a este minimum $A - B$). $\square$

Corolar 0.1. Fie α un ordinal și B un segment inițial în α . Atunci $B = \alpha$ sau există $\beta \in \alpha$ astfel încât $B = B_\beta(\alpha) = \beta$.

Demonstrație. Întrucât α este bine ordonată din definiție, avem că $B = \alpha$ sau $\exists \beta \in \alpha$ astfel încât $B = B_\beta(\alpha) = \{x \in \alpha \mid x \in \beta\} = \alpha \cap \beta = \beta$. Ultima relație rezultă din faptul că $\beta \in \alpha \Rightarrow \beta \subseteq \alpha$. $\square$

Propoziție 2. Fie α un ordinal și $\beta \in \alpha$. Atunci β este ordinal.

Demonstrație. Conform corolarului precedent, $\beta \in \alpha \Rightarrow \beta \subseteq \alpha$, deci $\beta = B_\beta(\alpha) \subseteq \alpha$. Cum α este bine ordonată, avem că β este bine ordonată în raport cu $\in$.

Acum, dacă $x \in \beta$ și $y \in x$, cum $\beta \in \alpha$, avem $x \in \alpha$, deci $y \in \alpha$. Deci $y, x, \beta \in \alpha$, $y \in x, x \in \beta, y \in \alpha, \in$ tranzitivă pe $\alpha \Rightarrow y \in \beta$. Astfel $\in$ tranzitivă pe β . $\square$

Teorema 1. Pentru orice ordinali α, β avem $\alpha = \beta, \alpha \in \beta$ sau $\beta \in \alpha$.

Demonstrație. Fie $c = \alpha \cap \beta$. Prin calcul direct avem că c este segment inițial în $(\alpha, \in)$. Atunci $c = \alpha$ sau $c \in \alpha$. Analog $c = \beta$ sau $c \in \beta$. Avem cazurile:

- $c = \alpha, c = \beta \Rightarrow \alpha = \beta$;
- $c = \alpha, c \in \beta \Rightarrow \alpha \in \beta$;
- $c \in \alpha, c = \beta \Rightarrow \beta \in \alpha$;
- $c \in \alpha, c \in \beta \Rightarrow c \in \alpha \cap \beta = c$. Dar în α , dacă am avea $c \in c$ atunci pentru că α este ordinal am avea și $c \notin c$, ceea ce contrazice legea terțului exclus. Deci acest caz nu este posibil.

$\square$

Observație 1. Am dovedit că clasa tuturor ordinalilor este total ordonată. Se poate dovedi ușor că această clasă este bine ordonată în raport cu $\in$.

Fie clasa tuturor ordinalilor, avem: $\alpha \subseteq \beta \Leftrightarrow \alpha \in \beta \vee \alpha = \beta$.

Propoziție 3. Pentru orice ordinal α , avem că $\alpha \cup \{\alpha\}$ este ordinal și este cel mai mic ordinal mai mare ca α .

Demonstrație. Din definiție $\alpha \cup \{\alpha\}$ este ordinal $\forall \alpha$ ordinal. Fie β un ordinal mai mare decât α . Avem $\alpha \in \beta \Rightarrow \alpha \subseteq \beta$ deoarece β ordinal. Dar $\alpha \in \beta \Leftrightarrow \{\alpha\} \subseteq \beta$. Deci $\{\alpha\} \cup \alpha \subseteq \beta$. $\square$

Definiție 3.

- Dacă pentru un ordinal α există β astfel încât $\alpha = \beta \cup \{\beta\}$, atunci β este un ordinal unic determinat și se numește predecesorul lui α .
- Un ordinal α este ordinal finit dacă $\alpha = \emptyset$ sau orice element al lui α și α însuși au un predecesor.
- Un ordinal care nu este finit se numește infin.

Observație 2. Dacă α este un ordinal finit, atunci:

1. $\beta \subseteq \alpha$ este ordinal finit;
2. $\alpha \cup \{\alpha\}$ este ordinal finit.

Teorema 2. Există o mulțime ω a tuturor ordinalelor finite.

Demonstrație. Fie X mulțimea construită cu axioma inifinității. Definim $\omega := \{\alpha \in X \mid \alpha \text{ ordinal finit}\}$. Arătăm că ω conține orice ordinal finit. Presupunem, prin absurd, că există un ordinal finit β cu $\beta \notin X$. Cum clasa ordinalelor finite este bine ordonată există un ordinal finit $\gamma = \text{minimum } \{\mu \mid \mu \notin X \wedge \mu \text{ ordinal finit}\}$. Cum $\emptyset \in X$ avem $\gamma \neq \emptyset$. Deci γ are un predecesor δ astfel încât $\gamma = \delta \cup \{\delta\}$. Din proprietatea de minimum a lui γ avem că $\delta \in X$. Dar atunci și $\gamma = \delta \cup \{\delta\} \in X$, contradicție cu $\gamma \notin X$. $\square$

Putem defini acum un model al teoriei axiomatice Dedekind-Peano astfel:

- numerele naturale sunt ordinale finite;
- numărul 0 este mulțimea vidă $\emptyset$;
- $\exists s : \omega \rightarrow \omega, s(\alpha) = \alpha \cup \{\alpha\}$.
- se verifică Principiul inducției pe mulțimea ordinalelor finite, din definiția lui ω .

Dacă $[\emptyset \in P \text{ și } \forall \alpha (\alpha \in P, \alpha \text{ ordinal finit} \rightarrow \alpha \cup \{\alpha\} \in P)]$ atunci vom avea $P = \omega$.

Într-adevăr, dacă $P \neq \omega$, atunci $\omega - P \neq \emptyset \Rightarrow \exists \gamma = \text{minimum } \omega - P$. Cum $\emptyset \in P \Rightarrow \gamma \neq \emptyset$, deci γ are un predecesor β . Dacă $\beta \in \omega - P$ s-ar contrazice alegerea lui γ , deci $\beta \in P$ și $\gamma = \beta \cup \{\beta\} \in P$, o contradicție.

Notăm $0 = \emptyset, 1 = \{\emptyset\}, n + 1 = n \cup \{n\} = s(n)$.

Teorema 3 (Teorema recurenței). Dacă X este o mulțime, $a \in X$ un element fixat și $f : X \rightarrow X$ o funcție, există și este unică o funcție $\varphi : \mathbb{N} \rightarrow X$ cu $\varphi(0) = a$, $\varphi(s(n)) = f(\varphi(n)), \forall n \in \mathbb{N}$.

Corolar 3.1. Dacă $(N', 0', s')$ satisface axiomele lui Dedekind-Peano, atunci $\exists \varphi : \mathbb{N} \rightarrow N'$ astfel încât $\varphi(0) = 0', \varphi \circ s = s' \circ \varphi$ și φ este bijectiv.

Observație 3. Pe baza rezultatelor descrise anterior $\forall m \in \mathbb{N}, \exists ! : s_m : \mathbb{N} \rightarrow \mathbb{N}$ astfel încât $s_m(0) = m$ și $s_m(s(n)) = s(s_m(n))$. Dacă notăm $s_m(n) := m + n$ avem că $m + 0 = m$, $m + s(n) = s(m + n)$.

De asemenea $\forall m \in \mathbb{N}, \exists p_m : \mathbb{N} \rightarrow \mathbb{N}, p_m(0) = 0$ și $p_m(s(n)) = p_m(n) + m$ avem $m \cdot 0 = 0$, $m \cdot s(n) = mn + m$.

Totodată se poate defini relația de ordine strictă $<$ prin:

$$m < n \Leftrightarrow \exists p \in \mathbb{N} - \{0\} \text{ astfel încât } n = m + p.$$

Principiile inducției matematice

P₁ Principiul I al inducției matematice

Fie $n_0 \in \mathbb{N}$ și $P(n)$ este o propoziție care poate fi asociată cu orice număr natural $n \geq n_0$.
(P este predicat de o variabilă)

Dacă:

1. $P(n_0)$ este adevărată,
2. ' $P(m)$ este adevărată' implică ' $P(m+1)$ este adevărată',

atunci $P(n)$ este adevărată pentru orice $n \geq n_0$.

P₂ Principiul al II-lea al inducției matematice

Fie $n_0 \in \mathbb{N}$ și $P(n)$ este o propoziție care poate fi asociată cu orice număr natural $n \geq n_0$.
(P este predicat de o variabilă)

Dacă:

1. $P(n_0)$ este adevărată,
2. ' $P(r)$ este adevărată pentru orice $n_0 \leq r < m$ ' $\Rightarrow$ ' $P(m)$ este adevărată',

atunci $P(n)$ este adevărată pentru orice $n \geq n_0$.

P.B.O. Principiul Bunei Ordonări a numerelor naturale

Oricare ar fi o submulțime $\emptyset \neq S \subseteq \mathbb{N}$, există $l \in S$ astfel încât $l \leq s, \forall s \in S$.

Teorema 4. *Următoarele afirmații sunt echivalente:*

- a) *PI, oricare ar fi $n_0 \in \mathbb{N}$;*
- b) *PII, oricare ar fi $n_0 \in \mathbb{N}$;*
- c) *P.B.O.*

Demonstrație. $PI \Rightarrow P.B.O.$:

Fie $\emptyset \neq S \subseteq \mathbb{N}$, Se consideră propoziția:

$$P(m) : m \leq s, \forall s \in S.$$

Se constată următoarele (pentru $n_0 = 0$):

- 1) $P(0)$ este adevărată deoarece $0 \leq s, \forall s \in S$;
- 2) $S \neq \emptyset \Rightarrow \exists s_0 \in S$. Deoarece $s_0 < s_0 + 1$, avem că $P(s_0 + 1)$ nu este adevărată. Prin urmare $P(m)$ nu este adevărată pentru orice $m \in \mathbb{N}$. Ținând cont de relația logică $\neg(p \rightarrow q) \equiv p \wedge \neg q$ pentru orice propoziții p, q și deoarece $P(0)$ este adevărată, rezultă că nu este adevărată implicația ' $P(m)$ adevărată $\Rightarrow P(m+1)$ adevărată'.

Deci $\exists l \in \mathbb{N}$ astfel încât $P(l)$ este adevărată, dar $P(l+1)$ nu este adevărată.

Deoarece $P(l)$ este adevărată, avem $l \leq s, \forall s \in S$. Afirmăm că $l \in S$. Să presupunem prin reducere la absurd că $l \notin S$. Cum $l \leq s, \forall s \in S$ avem că $l < s, \forall s \in S$. Atunci $l+1 \leq s, \forall s \in S$ și deci $P(l+1)$ este adevărată, contradicție cu alegerea lui l . Astfel $l \in S$, și deci, l este cel mai mic element al lui S .

P.B.O. $\Rightarrow$ PII:

Presupunem că sunt îndeplinite condițiile 1) și 2) din PII.

Notăm cu S mulțimea elementelor $s \in \mathbb{N}$ cu proprietatea că $P(s)$ nu este adevărată, adică $S = \{s \in \mathbb{N} \mid s \geq n_0 \text{ și } P(s) \text{ falsă}\}$.

Demonstrăm că $S = \emptyset$. Presupunem prin reducere la absurd că $S \neq \emptyset$. Conform P.B.O., există $l \in S, l \leq s, \forall s \in S$. Deci $P(r)$ este adevărată pentru orice $n_0 \leq r < l$ (l este cel mai mic element mai mare ca n_0 pentru care $P(l)$ este falsă). Dar din ipoteza 2) a lui PII avem că $P(l)$ este adevărată, contradicție cu $l \in S$.

PII $\Rightarrow$ PI:

Considerăm îndeplinite condițiile 1) și 2) din PI.

Dacă $P(r)$ este adevărată pentru orice $r < m$, $n_0 \leq r$, atunci $m > n_0$ și deci $m - 1 \geq n_0$ și $m - 1 < m$. Astfel $P(m - 1)$ este adevărată și, conform ipotezei 2) de la PI, avem că $P(m)$ este adevărată.

Am obținut că sunt îndeplinite condițiile 1) și 2) de la PII și, prin urmare, conform PII avem că $P(n)$ este adevărată $\forall n \geq n_0$. $\square$

Observație 4. Pentru $n_0 = 0$, avem $PI \Leftrightarrow PII \Leftrightarrow P.B.O.$

Propoziție 4. Fie $(X, \leq)$ o mulțime bine ordonată. Fie $P(x)$ o propoziție care poate fi asociată cu orice $x \in X$. Dacă are lor implicația: ' $P(r)$ este adevărată pentru orice $r < m$ ' implică ' $P(m)$ este adevărată', atunci $P(x)$ este adevărată pentru orice $x \in X$.

Formal: $\{\forall m[\forall r(r < m \rightarrow P(r)) \rightarrow P(m)]\} \rightarrow \forall x P(x)$.

Demonstrație. Fie $S = \{x \in X \mid P(x) \text{ este falsă}\}$. Presupunem, prin absurd că $S \neq \emptyset$, deci S are un cel mai mic element $x_0 \in S$. Astfel $P(r)$ este adevărată pentru orice $r < x_0$. Conform ipotezei $P(x_0)$ este adevărată, contradicție cu $x_0 \in S$. $\square$

Aplicație: Teorema împărțirii cu rest în $\mathbb{N}$

Teorema 5. Pentru orice numere naturale a, b cu $b \neq 0$ există și sunt unic determinate $q, r \in \mathbb{N}$ astfel încât $a = bq + r$ cu $0 \leq r < b$.

Demonstrație. Fie $b \neq 0$ fixat. Demonstrăm prin inducție după $a \in \mathbb{N}$, validitatea proprietății $P(a)$ pentru orice $a \in \mathbb{N}$, unde $P(a) : \exists q \exists r (q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge 0 \leq r < b)$. Evident $P(0)$ este adevărată (luând $q = r = 0$). Mai mult, pentru $a < b$, $P(a)$ este adevărată luând $q = 0, r = a$. Presupunem acum $a \geq b$ și $P(m)$ este adevărată $\forall m \in \mathbb{N}, m < a$. Vom demonstra că $P(a)$ este adevărată. Într-adevăr, cum $a \geq b$, avem $a - b \in \mathbb{N}$ și $a - b < a$, deci $P(a - b)$ este adevărată, adică există $q_1, r_1 \in \mathbb{N}, r_1 < b$ astfel încât $a - b = bq_1 + r_1$, deci $a = b(q_1 + 1) + r_1$ cu $r_1 < b$. Astfel $\exists q = q_1 + 1, r = r_1$ așa încât $a = bq + r$ cu $r < b$.

Pentru a dovedi unicitatea lui q și r , să presupunem că $a = bq + r = bs + t$ cu $r < b, t < b$. Analizăm cazul $q \geq s$ (cazul $q \leq s$ se tratează similar), deci $q - s \geq 0$ și $b(q - s) = t - r$. Cum $t < b \Rightarrow t - r < b$, deci $q - s = 0$ și $t - r = 0$. $\square$

Propoziție 5. Fie $a, b \in \mathbb{R}, b > 0$ și $P(x)$ o propoziție care poate fi asociată cu orice $x \in [a, \infty]$.

Dacă:

1. $P(x)$ este adevărată pentru orice $x \in [a, a + b)$;
2. ' $P(x)$ este adevărată' implică ' $P(x + b)$ este adevărată'

atunci $P(x)$ este adevărată pentru orice $x \geq a$.

Demonstrație. Fie $q(n) : p(x)$ este adevărată $\forall x \in [a+nb, a+(n+1)b), n \in \mathbb{N}$. Din condiția 1) avem că $q(0)$ este adevărată. Arătăm acum că $q(m) \rightarrow q(m+1)$. Fie $x_0 \in [a+(m+1)b, a+(m+2)b)$. Atunci $x_0 - b \in [a+mb, a+(m+1)b)$ și din ipoteza noastră $q(m)$ adevărată, avem $p(x_0 - b)$ este adevărată. Deci $p(x_0 - b + b)$ este adevărată conform condiției 2). Astfel $p(x_0)$ este adevărată. Cum x_0 a fost arbitrar ales din $[a+(m+1)b, a+(m+2)b)$, avem $q(m+1)$ adevărată, adică $q(n)$ adevărată $\forall n \in \mathbb{N}$. $\square$

Pentru $b = \frac{1}{n}$, demonstrați identitatea lui Hermite:

$$[x] + \left[x + \frac{1}{n} \right] + \cdots + \left[x + \frac{n-1}{n} \right] = [nx], \forall x > 0, \forall n \in \mathbb{N}^*.$$

Curs 9: Numere întregi și raționale

Numere întregi

Pe mulțimea $\mathbb{N} \times \mathbb{N}$ definim relația $\sim$ prin:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Se verifică imediat că $\sim$ este relație de echivalență.

Notăm $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim = \{[(a, b)]_{\sim} \mid a, b \in \mathbb{N}\}$. Elementele lui $\mathbb{Z}$ se numesc numere întregi.

Pe mulțimea numerelor întregi definim următoarele operații:

$$[(a, b)]_{\sim} + [(c, d)]_{\sim} = [(a + c, b + d)]_{\sim}$$

$$[(a, b)]_{\sim} \cdot [(c, d)]_{\sim} = [(ac + bd, ad + bc)]_{\sim}$$

Aceste operații sunt bine definite (adică nu depind de alegerea reprezentanților pentru clasele de echivalență). Se verifică imediat că $(\mathbb{Z}, +, \cdot)$ este domeniu de integritate în care elementul neutru la adunare este $[(0, 0)]_{\sim} = \{(n, n) \mid n \in \mathbb{N}\}$ iar elementul neutru la înmulțire este $[(1, 0)]_{\sim} = \{(n + 1, n) \mid n \in \mathbb{N}\}$. Opusul unui element $[(m, n)]_{\sim}$ este $[(n, m)]_{\sim}$.

Pe mulțimea numerelor întregi definim relația $<$ prin:

$$[(a, b)]_{\sim} < [(c, d)]_{\sim}$$

dacă $a + d < b + c$. Această relație este bine definită și reprezintă o ordine totală pe $\mathbb{Z}$.

În plus, pentru orice $x, y, z, t \in \mathbb{Z}$, avem:

1. $x < y, z \leq t \Rightarrow x + z < y + t$,
2. $x < y, z > 0 \Rightarrow xz < yz$,
3. $x < y, z < 0 \Rightarrow xz > yz$
4. $\forall x > 0 \Rightarrow \exists n \in \mathbb{N}$ cu $nx > y$.

Observăm că $\forall [(a, b)]_{\sim} \in \mathbb{Z}$ avem $[(a, b)]_{\sim} = [(a - b, 0)]_{\sim}$ dacă $a \geq b$ și $[(a, b)]_{\sim} = [(0, b - a)]_{\sim}$ dacă $b > a$. Astfel

$$\mathbb{Z} = \{[(a, 0)]_{\sim} \mid a \in \mathbb{N}\} \cup \{[(0, a)]_{\sim} \mid a \in \mathbb{N}\}.$$

Întrucât funcția $\varphi : \mathbb{N} \rightarrow \{[(a, 0)]_{\sim} \mid a \in \mathbb{N}\}$, $f(a) = [(a, 0)]_{\sim}$ este strict crescătoare, bine definită și bijectivă (este chiar un izomorfism de semiinele) putem identifica n cu $[(n, 0)]_{\sim}$ și similar considerăm $-n := [(0, n)]_{\sim}$.

Numere raționale

Pe $\mathbb{Z} \times \mathbb{Z}^*$ definim relația $\sim$ prin:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Avem că $\sim$ este o relație de echivalență. Definim $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \sim = \{[(a, b)]_{\sim} \in \mathbb{Z}\}$. Folosim notația $[(a, b)]_{\sim} := \frac{a}{b}$. Numim număr rațional un element al lui $\mathbb{Q}$. Pe mulțimea $\mathbb{Q}$ se definesc următoarele operații:

$$[(a, b)]_{\sim} + [(c, d)]_{\sim} = [(ad + bc, bd)]_{\sim}$$

$$[(a, b)]_{\sim} \cdot [(c, d)]_{\sim} = [(ac, bd)]_{\sim}$$

Aceste operații sunt bine definite (nu depind de alegerea reprezentanților pentru clasele de echivalență). Se verifică direct că $(\mathbb{Q}, +, \cdot)$ este corp comutativ, unde elementul neutru la adunare este $0 := [(0, 1)]_{\sim} = \{(0, a) \mid a \in \mathbb{Z}^*\}$ și elementul neutru la înmulțire este $1 := [(1, 1)]_{\sim} = \{(a, a) \mid a \in \mathbb{Z}^*\}$. Opusul unui element $[(a, b)]_{\sim}$ este $-[(a, b)]_{\sim} = [(-a, b)]_{\sim} = [(a, -b)]_{\sim}$ în vreme ce inversul unui element $[(a, b)]_{\sim}$ este $[(b, a)]_{\sim}$.

Se definește relația $[(a, b)]_{\sim} \leq [(c, d)]_{\sim} \Leftrightarrow (bc - ad)bd \geq 0$. Se pot demonstra direct proprietățile:

1. $\leq$ este o relație de ordine totală;

2. $\forall x, y, z, t \in \mathbb{Q}$ avem

- $x < y, z \leq t \Rightarrow x + z < y + t$,
- $x < y, z > 0 \Rightarrow xz < yz$,
- $x < y, z < 0 \Rightarrow xz > yz$
- $\forall x > 0 \Rightarrow \exists n \in \mathbb{N}$ cu $nx > y$.

Curs 10: Relația de echipotență. Cardinali

Fie A și B două mulțimi. Spunem că A și B sunt echipotente dacă există o funcție bijectivă $f : A \rightarrow B$ și notăm acest lucru prin $A \sim B$. Pentru orice mulțimi A, B și C au loc:

1. $A \sim A$ (reflexivitate) deoarece $1_A : A \rightarrow A$, $1_A(a) = a, \forall a \in A$ este bijectivă;
2. $A \sim B \Rightarrow B \sim A$ (simetrie) deoarece dacă $f : A \rightarrow B$ este bijectivă, atunci $f^{-1} : B \rightarrow A$ este tot bijectivă;
3. $A \sim B$ și $B \sim C \Rightarrow A \sim C$ (tranzitivitate) deoarece $f : A \rightarrow B$ bijectivă și $g : B \rightarrow C$ bijectivă implică $g \circ f : A \rightarrow C$ bijectivă.

Deci $\sim$ este relație de echivalență. Pentru o mulțime A , clasa de echivalență $[A]_{\sim} = \{B \mid \exists f : B \rightarrow A \text{ bijectivă}\}$ a lui A în raport cu $\sim$ se numește cardinalul lui A și se notează cu $|A|$.

Fie A, B mulțimi. Definim $A+B = \{(0, x) \mid x \in A\} \cup \{(1, y) \mid y \in B\}$. $A+B$ este reuniunea disjunctă a lui A și B .

Pentru două mulțimi X și Y definim:

1. $|X| + |Y| = |X + Y|$ —suma cardinalilor;
2. $|X| \cdot |Y| = |X \times Y|$ —produsul cardinalilor;
3. $|Y|^{|X|} = |\{f : X \rightarrow Y \mid f \text{ funcție}\}|$ —exponentul cardinalilor.

Aceste operații sunt bine definite (nu depind de alegerea reprezentanților pentru clasele de echivalență).

- Presupunem $|X| = |X'|$ și $|Y| = |Y'|$ adică $\exists f : X \rightarrow X'$ și $\exists g : Y \rightarrow Y'$ bijective. Definim $h : X + Y \rightarrow X' + Y'$, $h((0, x)) = (0, f(x)), \forall x \in X$ și $h((1, y)) = (1, g(y)), \forall y \in Y$. Evident h bijectivă $\Rightarrow |X + Y| = |X' + Y'|$.
- Presupunem $|X| = |X'|$ și $|Y| = |Y'|$ adică $\exists f : X \rightarrow X'$ și $\exists g : Y \rightarrow Y'$ bijective. Definim $h : X \times Y \rightarrow X' \times Y'$, $h(x, y) = (f(x), g(y)), \forall (x, y) \in X \times Y$. Avem că h este bijectivă și deci $|X \times Y| = |X' \times Y'|$.
- Presupunem $|X| = |X'|$ și $|Y| = |Y'|$ adică $\exists f : X \rightarrow X'$ și $\exists g : Y \rightarrow Y'$ bijective. Definim $\varphi : Y^X \rightarrow Y'^{X'}$ prin $\varphi(h) = g \circ h \circ f^{-1}, \forall h : X \rightarrow Y$. Cum φ este bijectivă, deci $|Y|^{|X|} = |Y'|^{|X'|}$.

Teorema 1. Fie X, Y, Z mulțimi. Atunci au loc relațiile:

1. $|Z|^{|X| \cdot |Y|} = \left(|Z|^{|Y|}\right)^{|X|}$,
2. $|Z|^{|X| + |Y|} = |Z|^{|X|} \cdot |Z|^{|Y|}$,
3. $(|X| \cdot |Y|)^{|Z|} = |X|^{|Z|} \cdot |Y|^{|Z|}$.

Demonstrație.

1. Definim $\varphi : Z^{X \times Y} \rightarrow (Z^Y)^X$ prin: dacă $f : X \times Y \rightarrow Z$ este o funcție, atunci $\varphi(f) : X \rightarrow Z^Y$ este funcție definită prin $(\varphi(f)(x))(y) = f(x, y), \forall x \in X, \forall y \in Y$.

Definim acum $\psi : (Z^Y)^X \rightarrow Z^{X \times Y}$ astfel: pentru orice funcție $g : X \rightarrow Z^Y$ definim $\psi(g) : X \times Y \rightarrow Z$, $\psi(g)(x, y) = (g(x))(y), \forall x \in X, y \in Y$. Prin calcul direct avem $\psi \circ \varphi = 1_{Z^{X \times Y}}$ și $\varphi \circ \psi = 1_{(Z^Y)^X}$.

Și astfel φ și ψ sunt bijective și sunt inversele una alteia.

2. Definim $\varphi : Z^{X+Y} \rightarrow Z^X \times Z^Y$ astfel: dacă $f : X+Y \rightarrow Z$ este o funcție, $\varphi(f) = (f_1, f_2)$ unde $f_1 : X \rightarrow Z$ și $f_2 : Y \rightarrow Z$ sunt funcții definite prin $f_1(x) = f((0, x)), \forall x \in X$ și $f_2(y) = f((1, y)), \forall y \in Y$. Prin calcul direct obținem că φ este bijectivă.
3. Definim $\varphi : X^Z \times Y^Z \rightarrow (X \times Y)^Z$ prin: $\varphi(f_1, f_2)(z) = (f_1(z), f_2(z)), \forall f_1 \in X^Z, f_2 \in Y^Z, z \in Z$. Prin calcul direct φ este bijectivă.

□

Observație 1. Prin calcul direct se poate arăta că pentru orice mulțimi X, Y, Z avem:

1. $|X| + |Y| = |Y| + |X|$ și $|X| \cdot |Y| = |Y| \cdot |X|$,
2. $(|X| + |Y|) + |Z| = |X| + (|Y| + |Z|)$ și $(|X| \cdot |Y|) \cdot |Z| = |X| \cdot (|Y| \cdot |Z|)$,
3. $|\mathcal{P}(X)| = |\{0, 1\}|^{|X|} = 2^{|X|}$.

Pentru 3) definim $\varphi : \mathcal{P}(X) \rightarrow \{0, 1\}^X$ unde $\varphi(A)$ este funcția caracteristică a lui A , notată χ_A , unde $\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$.

Evident φ este injectivă deoarece $\chi_A = \chi_B \Leftrightarrow A = B$. Pentru orice funcție $f : X \rightarrow \{0, 1\}$ definim $X_f = \{x \in X \mid f(x) = 1\}$. Avem $\varphi(X_f) = \chi_{X_f} = f$, deci φ este surjectivă.

Curs 11: Axioma Alegerii. Ordonarea cardinalilor

Axioma Alegerii

Axioma Alegerii: Pentru orice familie de mulțimi nevide $\mathcal{F}$, există o funcție $f : \mathcal{F} \rightarrow \cup \mathcal{F}$ astfel încât $f(X) \in X, \forall X \in \mathcal{F}$.

Există o serie de rezultate care sunt echivalente cu axioma alegerii (AC):

1. Produsul cartezian al oricărei familii de mulțimi nevide este nevid;
2. Pentru orice funcție surjectivă $f : X \rightarrow Y$, există o funcție $g : Y \rightarrow X$, astfel încât $f \circ g = 1_Y$;
3. Orice mulțime poate fi bine ordonată (Principiul bunei ordonări a lui Zermelo);
4. Orice mulțime inductiv ordonată P (orice mulțime P cu proprietatea că orice submulțime total ordonată a lui P are un majorant în P) conține un element maximal (Lema lui Zorn);
5. Orice mulțime parțial ordonată conține o submulțime total ordonată maximală în raport cu relația de incluziune (principiul lui Hausdorff);
6. Orice mulțime parțial ordonată conține o submulțime cu proprietatea că oricare 2 elemente sunt incomparabile, maximală în raport cu relația de incluziune;
7. În orice pereche de numere cardinale, unul este mai mic decât celălalt sau aceste numere sunt egale (principiul trihotomiei);
8. Pentru orice mulțime infinită X există o funcție bijectivă $f : X \rightarrow X \times X$ (Tarski).

Axioma alegerii este independentă de celelalte axiome ale sistemului Zermelo–Fraenkel (ZF), atât cât și negația ei fiind consistente. Astfel pot fi definite modele atât pentru ZF+AC cât și pentru ZF+¬AC (un model al unei teorii este o structură de obiecte care satisface axiomele acelei teorii). Nici AC, nici ¬AC nu pot fi demonstrate pornind de la celelalte axiome ZF.

Există, de asemenea, o serie de rezultate mai slabe decât axioma alegerii, la rândul lor independente față de celelalte axiome ZF.

- Axioma alegerii dependente (DC): pentru orice mulțime X și orice relație nevidă R peste X cu proprietatea că $\forall x \in X \exists y \in X (xRy)$, există o funcție $f : \mathbb{N} \rightarrow X$, $f(n)Rf(n+1), \forall n \in \mathbb{N}$.
- Axioma alegerii numărabile (CC): Pentru orice familie numărabilă de mulțimi nevide $\mathcal{F}$, există o funcție $f : \mathcal{F} \rightarrow \cup \mathcal{F}$ astfel încât $f(X) \in X, \forall X \in \mathcal{F}$.
- Axioma alegerii peste mulțimi finite (AC(fin)): Pentru orice familie de mulțimi nevide și finite $\mathcal{F}$, există o funcție $f : \mathcal{F} \rightarrow \cup \mathcal{F}$ astfel încât $f(X) \in X, \forall X \in \mathcal{F}$.
- Principiul totalei ordonări (OP): Orice mulțime X poate fi total ordonată.

- Axioma Dedekind-infinitudinii (Fin): Pentru orice mulțime infinită X , există o funcție injectivă $i : \mathbb{N} \rightarrow X$.
- Axioma alegerii peste familii numărabile de mulțimi finite (CC(fin)): Pentru orice familie numărabilă de mulțimi nevide și finite $\mathcal{F}$, există o funcție $f : \mathcal{F} \rightarrow \cup \mathcal{F}$, astfel încât $f(X) \in X, \forall X \in \mathcal{F}$.
- Principiul de selecție Kinna-Wagner (KW): Pentru orice familie $\mathcal{F}$ de mulțimi de cardinalitate cel puțin 2, există o funcție f astfel încât $\emptyset \neq f(X) \subsetneq X, \forall X \in \mathcal{F}$.

Teorema 1. *Au loc următoarele implicații stricte în ZF:*

1. $AC \Rightarrow DC \Rightarrow CC \Rightarrow CC(fin)$;
2. $AC \Rightarrow OP \Rightarrow AC(fin) \Rightarrow CC(fin)$;
3. $CC \Rightarrow Fin \Rightarrow CC(fin)$;
4. $KW \Rightarrow OP$.

Un rezultat chiar mai puternic decât AC este ipoteza generalizată a continuului (GCH) care afirmă:

$$\forall X, \forall Y (X \text{ infinită} \wedge |X| \leq |Y| \leq |\mathcal{P}(X)|) \Rightarrow (|X| = |Y|) \vee (|Y| = |\mathcal{P}(X)|).$$

(orice mulțime Y cu cardinalul poziționat între $|X|$ și $|\mathcal{P}(X)|$ are fie cardinalul egal cu cardinalul lui X , fie cardinalul egal cu cardinalul lui $\mathcal{P}(X)$.)

Teorema 2.

1. $AC \Rightarrow LEM$
2. $GCH \Rightarrow AC$ (implicație strictă)
unde LEM este legea terțului exclus adică $p \vee \neg p$ este adevărată pentru orice propoziție p .

Ordonarea cardinalilor

Fie A și B două mulțimi. Spunem că $|A| \leq |B|$ dacă există $f : A \rightarrow B$ injectivă.

Relația $\leq$ este bine definită (nu depinde de alegerea reprezentărilor pentru clasele de echivalență). Fie A', B' cu $|A| = |A'|$ și $|B| = |B'|$. Dacă $|A| \leq |B|$, avem $\exists f : A \rightarrow B$ injectivă. Dar $\exists g : A \rightarrow A'$ bijectivă și $h : B \rightarrow B'$ bijectivă. Atunci $h \circ f \circ g^{-1} : A' \rightarrow B'$ este injectivă, de unde $|A'| \leq |B'|$.

Relația $\leq$ este reflexivă, deoarece $\exists 1_A : A \rightarrow A, 1_A(a) = a, \forall a \in A$, oricum am considera o mulțime A .

Relația $\leq$ este tranzitivă deoarece $|A| \leq |B|$ și $|B| \leq |C|$ implică faptul că există $f : A \rightarrow B$ injectivă și $g : B \rightarrow C$ injectivă. Deci $g \circ f : A \rightarrow C$ este injectivă, de unde $|A| \leq |C|$.

Relația $\leq$ este antisimetrică. Vom arăta că dacă $|B| \leq |C|$ și $|C| \leq |B|$ atunci $|B| = |C|$.

Teorema 3 (Cantor-Schröder-Bernstein). *Fie B și C două mulțimi cu proprietatea că $|B| \leq |C|$ și $|C| \leq |B|$ atunci $|B| = |C|$.*

Demonstrație. Fie funcțiile injective $f : B \rightarrow C$ și $g : C \rightarrow B$.

Fie $F : \mathcal{P}(B) \rightarrow \mathcal{P}(B)$, $F(X) = B - g(C - f(X))$. Dacă $X \subseteq Y$, prin calcul direct obținem $F(X) \subseteq F(Y)$. (*)

Fie $S = \{X \in \mathcal{P}(B) \mid X \subseteq F(X)\}$. Întrucât $\emptyset \in S$, avem că $S \neq \emptyset$. Fie $T = \bigcup_{X \in S} X$. Vom arăta că $F(T) = T$.

Într-adevăr, fie $X \in S$ arbitrar. Avem $X \subseteq \bigcup_{Y \in S} Y = T \Rightarrow F(X) \subseteq F(T)$. Deci $X \subseteq F(X) \subseteq F(T) \Rightarrow \bigcup_{Y \in S} Y \subseteq F(T) \Rightarrow T \subseteq F(T) \stackrel{(*)}{\Rightarrow} F(T) \subseteq F(F(T)) \Rightarrow F(T) \in S \Rightarrow F(T) \subseteq T$.

Deci $F(T) = T$. Am obținut astfel:

$$T = B - g(C - f(T)), \text{ sau, echivalent}$$

$$B - T = g(C - f(T))(**)$$

Deoarece g este injectivă, pentru orice $x \in B - T$, avem că $g^{-1}(x)$ este o mulțime cu exact un element.

Definim $h : B \rightarrow C$, $h(x) = \begin{cases} f(x), & x \in T \\ g^{-1}(x), & x \in B - T \end{cases}$. Arătăm că h este bijectivă.

- h injectivă.

Fie $x, y \in B$ astfel încât $h(x) = h(y)$. Vom arăta că fie $x, y \in T$, fie $x, y \in B - T$. Într-adevăr, să presupunem prin reducere la absurd că $x \in T, y \in B - T$ (cazul $x \in B - T, y \in T$ se analizează similar). Avem $h(x) = f(x)$ și $h(y) = g^{-1}(y)$. Dacă notăm $g^{-1}(y) = z$, avem $g(z) = y$. Dar $y \in B - T$, deci conform (**), $\exists u \in C - f(T), y = g(u)$.

Deci $g(u) = g(z)$, și cum g injectivă $\Rightarrow z = u$. Aceasta este o contradicție deoarece $z = h(y) = h(x) = f(x) \in f(T)$ iar $u \notin f(T)$. Astfel $x, y \in T$ sau $x, y \in B - T$, de unde, conform injectivității funcțiilor f și g , obținem $x = y$.

- h surjectivă.

Fie $y \in C$ arbitrar. Dacă $y \in f(T)$, există $z \in T$ astfel încât $y = f(z)$ și deci $y = h(z)$. Dacă $y \in C - f(T)$, deoarece $g(C - f(T)) = B - T$, există $x \in B - T$ astfel încât $g(y) = x$. Deci $y \in g^{-1}(x)$. Întrucât $g^{-1}(x)$ este o mulțime cu un singur element, avem că $y = g^{-1}(x), x \in B - T$, adică $y = h(x)$.

□

Teorema 4 (Cantor). Fie X o mulțime. Atunci $|X| \leq |\mathcal{P}(X)|$.

Demonstrație. Fie $i : X \rightarrow \mathcal{P}(X), i(x) = \{x\}, \forall x \in X$. Evident i este injectivă, deci $|X| \leq |\mathcal{P}(X)|$. Să presupunem prin absurd că există $f : X \rightarrow \mathcal{P}(X)$ surjectivă. Fie $Z = \{x \in X \mid x \notin f(x)\}$. Deoarece f este surjectivă, avem că $\exists x_0 \in X, f(x_0) = Z$. Din definiția lui Z avem $x_0 \in Z \Leftrightarrow x_0 \notin f(x_0) = Z$, o contradicție. □

Propoziție 1. În prezența axiomei alegerii, relația de ordine $\leq$ este totală, adică $\forall A, B$ mulțimi avem $|A| \leq |B|$ sau $|B| \leq |A|$.

Demonstrație. Fie $S = \{f : X \rightarrow Y \mid X \subseteq A, Y \subseteq B, f \text{ bijectivă}\}$. Pe mulțimea S definim relația $\sqsubseteq$ astfel: pentru $f : X \rightarrow Y$ și $f' : X' \rightarrow Y'$ avem $f \sqsubseteq f' \Leftrightarrow X \subseteq X'$ și $f'|_X = f$ (i.e. $f'(x) = f(x), \forall x \in X$). Se verifică imediat că $\sqsubseteq$ este relație de ordine. Fie acum

$\mathcal{L} = \{f_i : X_i \rightarrow Y_i \mid i \in I\} \subseteq S$ cu $\mathcal{L}$ total ordonată. Arătăm că $\mathcal{L}$ este majorată în S . Fie $X = \bigcup_{i \in I} X_i$ și $Y = \bigcup_{i \in I} Y_i$. Funcția $f : X \rightarrow Y, f(x) = f_i(x)$ dacă $x \in X_i$ este bine definită, bijectivă și $f_i \sqsubseteq f, \forall i \in I$. Din lema lui Zorn rezultă că în S există un element maximal $f_0 : X_0 \rightarrow Y_0$. Cum f_0 este bijectivă, e de ajuns să demonstrăm că $X_0 = A$ sau $Y_0 = B$. Presupunem prin reducere la absurd că $X_0 \neq A$ sau $Y_0 \neq B$. Fie $a_0 \in A - X_0$ și $b_0 \in B - Y_0$. Atunci funcția $f' : X_0 \cup \{a_0\} \rightarrow Y_0 \cup \{b_0\}$, definită prin $f'(x) = \begin{cases} f_0(x), & x \in X_0 \\ b_0, & x = a_0 \end{cases}$ este bijectivă cu $f_0 \sqsubset f'$, contradicție cu maximalitatea lui f_0 . $\square$

Observație 1.

1. Dacă există $f : X \rightarrow Y$ injectivă, atunci există $g : Y \rightarrow X$ surjectivă,
$$g(y) = \begin{cases} f^{-1}(y), & y \in \text{Im} f \\ x_0, & y \notin \text{Im} f \end{cases} \quad \text{pentru un anumit } x_0 \in X \text{ fixat;}$$
2. În prezența axiomei alegerii, dacă $f : X \rightarrow Y$ este surjectivă, atunci există $g : Y \rightarrow X$ injectivă. Pentru orice $y \in Y$, $g(y)$ se definește ca fiind un reprezentant al mulțimii $f^{-1}(\{y\}) = \{x \in X \mid f(x) = y\}$.

Propoziție 2. Fie X, Y, Z mulțimi. Atunci avem:

1. $|X| \leq |Y| \Rightarrow |X| + |Z| \leq |Y| + |Z|$,
2. $|X| \leq |Y| \Rightarrow |X| \cdot |Z| \leq |Y| \cdot |Z|$,
3. $|X| \leq |Y| \Rightarrow |X|^{|Z|} \leq |Y|^{|Z|}$,
4. $|X| \leq |Y|$ și $Z \neq \emptyset \Rightarrow |Z|^{|X|} \leq |Z|^{|Y|}$,
5. $|X| + |Y| \leq |X| \cdot |Y|$ dacă $|X|, |Y| \geq 2$.

Demonstrație. 3) Fie $f : X \rightarrow Y$ injectivă. Definim $g : X^Z \rightarrow Y^Z, g(h) = f \circ h, \forall h \in X^Z$. Avem că g este injectivă.

4) Fie $f' : Y \rightarrow X$ surjectivă. Definim $g : Z^X \rightarrow Z^Y, g(h) = h \circ f', \forall h \in Z^X$. Avem g injectivă. $\square$

Curs 12: Mulțimi numărabile și nenumărabile, mulțimi infinite, mulțimi finite

Definiție 1.

- O mulțime este finită dacă este echipotentă cu un număr natural. Altfel spus X este finită dacă poate fi exprimată sub forma $\{x_1, \dots, x_n\}, n \in \mathbb{N}^*$.
- O mulțime care nu este finită este infinită.
- O mulțime X este numărabilă dacă este finită sau există o funcție bijectivă $f : \mathbb{N} \rightarrow X$.

Teorema 1. Fie A o mulțime. Următoarele afirmații sunt echivalente.

1. A este mulțime finită;
2. Există o funcție injectivă $f : \mathbb{N} \rightarrow A$;
3. Există $B \subsetneq A$ și $f : A \rightarrow B$ bijectivă.

Demonstrație. (Rezultatul este adevărat dacă acceptăm axioma alegerii)

1) $\Rightarrow$ 2). Fie A infinită. Deci $\exists a_0 \in A$. Avem $A - \{a_0\}$ infinită și astfel putem alege $a_1 \in A - \{a_0\}$. Mai mult $A - \{a_0, a_1\}$ este infinită și putem alege $a_2 \in A - \{a_0, a_1, a_2\}$. Știm că A poate fi bine ordonată (conform principiului lui Zermelo). Deci există $\leq$ pe A astfel încât $\forall S \subset (A, \leq), \exists \text{ minimum } S$. Astfel a_1 poate fi ales ca minimum $A - \{a_0\}$, a_2 ca minimum $A - \{a_0, a_1\}$ și, prin inducție, odată selectate $a_0, \dots, a_{n-1}$, selectăm pe a_n ca $a_n = \text{minimum } A - \{a_0, a_1, \dots, a_{n-1}\}$. Funcția $f : \mathbb{N} \rightarrow A$ definită prin $f(n) = a_n, \forall n \in \mathbb{N}$ este funcția cerută.

3) $\Rightarrow$ 1). Avem $\text{Im } f \subsetneq A$ deci $\exists x_0 \in A - \text{Im } f$. Deoarece $x_0 \notin \text{Im } f$ avem $x_0 \neq f(x_0)$. Fie $a_0 = x_0, a_1 = f(x_0), \dots, a_n = f^n(x_0) = f(a_{n-1})$. Avem $a_0 \neq a_1$. Presupunem că $\exists m, n \in \mathbb{N}, m \neq n$ astfel încât $a_m = a_n$, adică $f^m(x_0) = f^n(x_0)$. Deoarece f injectivă, urmează $x_0 = f^{|n-m|}(x_0)$ adică $x_0 = f(f^{|n-m|-1}(x_0)) \in \text{Im } f$, contradicție. Deci $a_m \neq a_n, \forall m, n \in \mathbb{N}, m \neq n$. Astfel A conține un șir infinit și, deci, este infinită. Evident funcția $f : \mathbb{N} \rightarrow A, f(n) = a_n$ este injectivă.

2) $\Rightarrow$ 3). Definim $\rho : A \rightarrow A - f(0)$ (unde $f : \mathbb{N} \rightarrow A$ este injectivă) prin
$$\rho(a) = \begin{cases} a, a \notin f(\mathbb{N}) \\ f(n+1), a = f(n) \end{cases}$$
. Arătăm că ρ este bijectivă. Fie $a, b \in A$ cu $\rho(a) = \rho(b)$. Dacă $a \in f(\mathbb{N})$ și $b \notin f(\mathbb{N})$ avem $\rho(b) = b \notin f(\mathbb{N})$ iar $\rho(a) \in f(\mathbb{N})$, contradicție cu $\rho(a) = \rho(b)$. Deci fie $a, b \in f(\mathbb{N})$, fie $a, b \notin f(\mathbb{N})$. Dacă $a, b \in f(\mathbb{N})$, atunci $a = f(k), b = f(l)$. Avem $\rho(a) = \rho(b) \Rightarrow f(k+1) = f(l+1) \xrightarrow{f \text{ inj.}} k+1 = l+1 \Rightarrow k = l \Rightarrow a = b$. Dacă $a, b \notin f(\mathbb{N})$ avem $a = \rho(a) = \rho(b) = b$. Deci ρ este injectivă.

Arătăm acum că ρ este surjectivă. Fie $a \in A - f(0)$. Dacă $a \notin f(\mathbb{N})$, evident $a = \rho(a)$. Dacă $a \in f(\mathbb{N})$, cum $a \neq f(0)$, avem $a = f(k), k \geq 1, k \in \mathbb{N}$. Deci $a = \rho(\underbrace{f(k-1)}_{\geq 0})$, deci ρ surjectivă. □

Observație 1. Echivalența 2) $\Leftrightarrow$ 3) se poate dovedi fără invocarea axiomei alegerii.

Teorema 2. Fie A o mulțime. Următoarele afirmații sunt echivalente:

1. A finită;
2. Orice funcție injectivă $f : A \rightarrow A$ este surjectivă;
3. Orice funcție surjectivă $f : A \rightarrow A$ este injectivă.

Demonstrație. (Rezultatul este adevărat dacă acceptăm axioma alegerii). Din teorema precedentă $1) \Leftrightarrow 2)$. Arătăm că $1) \Leftrightarrow 3)$. Fie A finită. Atunci, dacă $f : A \rightarrow A$ surjectivă, avem $\text{Im} f = A$. Presupunem $|A| = n$, $A = \{a_1, \dots, a_n\}$. Dacă $\exists i, j \in \{1, \dots, n\}, i \neq j$ cu $f(a_i) = f(a_j)$, atunci $|\text{Im} f| \leq n - 1$ contradicție cu $|\text{Im} f| = n$. Reciproc să presupunem că orice funcție surjectivă $\rho : A \rightarrow A$ este injectivă. Presupunem prin absurd că A ar fi infinită. Atunci $\exists f : \mathbb{N} \rightarrow A$ injectivă conform teoremei precedente.

$$\text{Definim } g : A \rightarrow A, g(a) = \begin{cases} a, a \notin f(\mathbb{N}) \\ f(n-1), a = f(n), n \geq 1 \\ f(0), a = f(0). \end{cases}$$

Avem că g este surjectivă, dar g nu este injectivă deoarece $g(f(1)) = g(f(0)) = f(0)$, o contradicție. $\square$

Propoziție 1. Fie A, B două mulțimi numărabile. Atunci $A \times B$ și $A + B$ sunt numărabile.

Demonstrație. Analizăm cazul când A și B sunt ambele infinite. Celelalte cazuri sunt triviale. Deci $|A| = |\mathbb{N}|$ și $|B| = |\mathbb{N}|$. Atunci $|A \times B| = |A| \cdot |B| = |\mathbb{N}| \cdot |\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Dar $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, $f(m, n) = \frac{(m+n)(m+n+1)}{2} + m, \forall m, n \in \mathbb{N}$ este bijectivă, deci $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Astfel $|A \times B| = |\mathbb{N}|$. Cum $|A + B| = |A| + |B| \leq |A| \cdot |B| \leq |\mathbb{N}|$ și $A + B$ infinită, deci $|\mathbb{N}| \leq |A + B|$, avem $|A + B| = |\mathbb{N}|$. $\square$

Propoziție 2. Fie A o mulțime infinită și C o mulțime numărabilă. Atunci $|A \cup C| = |A|$.

Demonstrație. (Rezultatul este adevărat dacă acceptăm axioma alegerii). Fie A infinită. Deci există $f : \mathbb{N} \rightarrow A$ injectivă. Adică $f : \mathbb{N} \rightarrow f(\mathbb{N})$ este bijectivă, de unde $|f(\mathbb{N})| = |\mathbb{N}|$. Considerăm cazul în care C este reprezentat de B cu $A \cap B = \emptyset$ și B numărabilă.

Avem $A = (A - f(\mathbb{N})) \cup f(\mathbb{N})$. Deci $A \cup B = (A - f(\mathbb{N})) \cup f(\mathbb{N}) \cup B = (A - f(\mathbb{N})) \cup \underbrace{(f(\mathbb{N}) \cup B)}_{\text{numărabilă}}$. Știm că $\exists \rho : f(\mathbb{N}) \rightarrow f(\mathbb{N}) \cup B$ bijectivă deoarece atât $f(\mathbb{N})$ cât și $f(\mathbb{N}) \cup B$ sunt

numărabile infinite. Definim funcția $g : A \rightarrow A \cup B$ prin $g(a) = \begin{cases} \rho(a), a \in f(\mathbb{N}) \\ a, a \in A - f(\mathbb{N}) \end{cases}$. Avem

că g este bijectivă și $|A| = |A \cup B|$. Într-adevăr g este evident surjectivă. Dacă $x, y \in A$ cu $g(x) = g(y)$ atunci fie $x, y \in f(\mathbb{N})$, fie $x, y \in A - f(\mathbb{N})$. Dacă am avea $x \in f(\mathbb{N})$ și $y \in A - f(\mathbb{N})$, atunci am obține $\rho(x) = y \in A - f(\mathbb{N})$. Dar $\rho(x) \in f(\mathbb{N}) \cup B$, o contradicție. Am demonstrat că g este injectivă conform injectivității lui ρ .

Deoarece $A \cap B = \emptyset \Rightarrow |A \cup B| = |A + B|$. Astfel $|A + B| = |A|$. Fie acum C o mulțime arbitrară numărabilă. Avem $|A \cup C| \leq |A + C| = |A|$. Evident, deoarece $A \subseteq A \cup C$ avem $|A| \leq |A \cup C|$, de unde conform teoremei Cantor-Bernstein, avem $|A| = |A \cup C|$. $\square$

Notăm $|\mathbb{N}| = \chi_0$ și $|\mathcal{P}(\mathbb{N})| = 2^{\chi_0} = c$. Conform teoremei lui Cantor $\chi_0 < c$.

Ipoteza continuului. Între χ_0 și c nu există un alt cardinal.

Propoziție 3. Pentru orice mulțime A avem $|A| + 1 = |A|$ dacă și numai dacă A este infinită.

Demonstrație. Fie $B = A \cup \{x_0\}$ unde $x_0 \notin A$. Avem $|B| = |A| + 1$.

Funcția $i : A \rightarrow B, i(a) = a, \forall a \in A$ este injectivă deci $|A| \leq |B|$.

Presupunem $|A| = |B|$, deci $\exists f : B \rightarrow A$ bijectivă. Funcția $f|_A : A \rightarrow A$ definită prin $f|_A(a) = f(a), \forall a \in A$ este injectivă dar $f(x_0) \notin f|_A(A)$, deoarece, din injectivitatea lui f , avem $f(x_0) \neq f(a), \forall a \in A$, deci $f|_A$ nu este surjectivă, de unde avem că A este infinită.

Reciproc, dacă A este infinită, există $g : A \rightarrow A$ care este injectivă, dar nu este surjectivă. Deci $\exists a_0 \in A, a_0 \notin g(A) = \text{Img}$.

$$\text{Fie } f : B \rightarrow A, f(x) = \begin{cases} g(x), x \in A \\ a_0, x = x_0 \end{cases}.$$

Avem că f este injectivă, deci $|B| \leq |A|$. În final $|A| = |B|$ conform teoremei lui Cantor - Bernstein. $\square$

Propoziție 4. *Au loc relațiile:*

1. $n + \chi_0 = \chi_0$;
2. $\chi_0 + \chi_0 = \chi_0$;
3. $c + c = c$;
4. $n + c = \chi_0 + c = c$;
5. $c \cdot c = c$;
6. $n \cdot c = \chi_0 \cdot c = c$;
7. $c^n = c, \forall n > 0, n \in \mathbb{N}$;
8. $n^{\chi_0} = \chi_0^{\chi_0} = c^{\chi_0} = c, \forall n > 1, n \in \mathbb{N}$;
9. $c^c = 2^c$.

Demonstrație. 1) și 2) din faptul că reuniunea (disjunctă) a două mulțimi numărabile este numărabilă.

$$3) c + c = 2^{\chi_0} + 2^{\chi_0} = 2 \cdot 2^{\chi_0} = 2^{\chi_0+1} = 2^{\chi_0} = c.$$

4) $c \leq n + c \leq \chi_0 + c \leq c + c$. Dar $c = c + c$ și rezultă concluzia din teorema lui Cantor-Bernstein.

$$5) c \cdot c = 2^{\chi_0} \cdot 2^{\chi_0} = 2^{\chi_0+\chi_0} = 2^{\chi_0} = c.$$

6) $c \leq n \cdot c \leq \chi_0 \cdot c \leq c \cdot c = c$. Deci rezultatul se obține din teorema lui Cantor-Bernstein.

7) $c^2 = c$, deci $c^n = c^{n-1} \cdot c = c$, conform principiului inducției matematice.

8) $c = 2^{\chi_0} \leq n^{\chi_0} \leq \chi_0^{\chi_0} \leq c^{\chi_0} = (2^{\chi_0})^{\chi_0} = 2^{\chi_0 \cdot \chi_0} = 2^{\chi_0} = c$. Am folosit teorema lui Cantor-Bernstein și faptul că produsul cartezian a două mulțimi numărabile este numărabil, adică $\chi_0 \cdot \chi_0 = \chi_0$ ($|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$).

$$9) c^c = (2^{\chi_0})^c = 2^{\chi_0 \cdot c} \stackrel{6)}{=} 2^c. \quad \square$$

Propoziție 5. *Următoarele mulțimi sunt numărabile: $\mathbb{Z}, \mathbb{Q}$.*

Demonstrație. 1. Funcția $f : \mathbb{Z} \rightarrow \mathbb{N}, f(x) = \begin{cases} 2x, x \geq 0 \\ -2x - 1, x < 0 \end{cases}$ este bijectivă.

2. Deoarece $\mathbb{N} \subseteq \mathbb{Q}$ avem $\chi_0 \leq |\mathbb{Q}|$. Fie $\mathbb{Z}^* = \mathbb{Z} - \{0\}$.

Funcția $g : \mathbb{Z} \rightarrow \mathbb{Z}^*, g(x) = \begin{cases} x+1, & x \geq 0 \\ x, & x < 0 \end{cases}$ este bijectivă, deci $|\mathbb{Z}^*| = \chi_0$ și apoi $|\mathbb{Z} \times \mathbb{Z}^*| = \chi_0$. Funcția $f : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}, f(x, y) = \frac{x}{y}, \forall (x, y) \in \mathbb{Z} \times \mathbb{Z}^*$ este surjectivă deci $\underbrace{|\mathbb{Z} \times \mathbb{Z}^*|}_{\chi_0} \geq |\mathbb{Q}|$. În concluzie, $|\mathbb{Q}| = \chi_0$.

□

Propoziție 6. *Următoarele mulțimi au cardinalul egal cu c :*

1. $(0, 1) \subsetneq \mathbb{R}$;
2. Orice interval real: $[a, b), (a, b), (a, b], [a, b]$ cu $a, b \in \mathbb{R}$;
3. $\mathbb{R}$;
4. $\mathbb{R} - \mathbb{Q}$;
5. $\mathbb{C}$.

Demonstrație. 1) Arătăm că nu există o funcție $f : \mathbb{N} \rightarrow (0, 1)$ care să fie surjectivă. Fie $f : \mathbb{N} \rightarrow (0, 1)$. Fiecare număr real $f(n)$ poate fi scris sub forma $f(n) = 0, a_{n1}a_{n2} \dots a_{nn} \dots$

Fie $b = 0, b_1b_2 \dots b_n \dots \in (0, 1)$ unde pentru orice n avem că b_n este o cifră diferită de 0, 9 și de a_{nn} . Atunci $b \notin \text{Im}f$, deci f nu este surjectivă. Deci $\chi_0 < |(0, 1)|$.

Fie acum funcția $\rho : \{0, 1, 2, \dots, 9\}^{\mathbb{N}} \rightarrow (0, 1), \rho(f) = 0, f_1f_2 \dots f_n \dots$ unde $f(n) := f_n$. Această funcție este surjectivă, deci $|(0, 1)| \leq |\{0, 1, 2, \dots, 9\}^{\mathbb{N}}| = 10^{\chi_0} = c$. Din ipoteza continuului avem $|(0, 1)| = c$.

2) Deoarece $|A \cup C| = |A|$ oricând A este infinită și C numărabilă avem $|[a, b]| = |[a, b]| = |(a, b]| = |(a, b)|$. Fie $f : [0, 1] \rightarrow [a, b], f(x) = a + (b - a)x, \forall x \in [0, 1]$. Avem că f bijectivă, deci obținem $|[a, b]| = |[0, 1]| = c$.

3) Funcția $f : \mathbb{R} \rightarrow (0, 1), f(x) = \frac{1}{2} + \frac{1}{\pi} \arctg(x)$ este continuă, strict crescătoare ($f'(x) = \frac{1}{\pi} \cdot \frac{1}{1+x^2} > 0$), $\lim_{x \rightarrow -\infty} f(x) = 0, \lim_{x \rightarrow \infty} f(x) = 1$, deci f bijectivă. Astfel $|\mathbb{R}| = |(0, 1)| = c$.

4) Dacă mulțimea infinită $\mathbb{R} - \mathbb{Q}$ ar fi numărabilă, am avea că $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$ este numărabilă, deci $\mathbb{R} - \mathbb{Q}$ este nenumărabilă ($\chi_0 < |\mathbb{R} - \mathbb{Q}|$). Cum $|\mathbb{R} - \mathbb{Q}| \leq c$, avem concluzia.

5) $|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = c \cdot c = c$. □

Teorema 3. *Fie $\emptyset \neq A \subseteq (\mathbb{R}, \leq)$ unde $\leq$ este relația de ordine uzuală pe $\mathbb{R}$. Dacă A este bine ordonată, atunci A este finită sau numărabilă.*

Demonstrație. (Se utilizează axioma alegerii) Dacă A este finită, rezultă concluzia, deci tratăm cazul A infinită.

Fie $x_0 \in A$ astfel încât x_0 nu este cel mai mare element al lui A (dacă acesta există îl notăm cu M). Atunci $\{y \in A \mid x_0 < y\} \neq \emptyset$. Fie $m(x_0) = \text{minimum } \{y \in A \mid x_0 < y\}$. Deci $x_0 < m(x_0)$, de unde avem că $\exists q(x_0) \in \mathbb{Q}$ astfel încât $x_0 < q(x_0) < m(x_0)$. Folosind axioma alegerii, alegem din mulțimea $\{q(x_0) \mid x_0 < q(x_0) < m(x_0) \text{ și } q(x_0) \in \mathbb{Q}\}$ exact un element $\bar{q}(x_0)$. Astfel putem defini $\rho : A \setminus \{M\} \rightarrow \mathbb{Q}, \rho(a) = \bar{q}(a)$. Fie $a, b \in A \setminus \{M\}, a \neq b$ (presupunem $a < b$). Atunci $a < \bar{q}(a) < m(a) \leq b < \bar{q}(b) < m(b)$, deci $\bar{q}(a) < \bar{q}(b)$ adică $\rho(a) \neq \rho(b)$ de unde ρ este injectivă. Urmează $|A \setminus \{M\}| \leq \chi_0$, deci $|A| = |A \setminus \{M\}| \leq \chi_0$. □

Alte proprietăți ale operațiilor cu cardinali.

Considerăm A o mulțime infinită și presupunem adevărată axioma alegerii. Atunci

1. $|A \times \mathbb{N}| = |A|$;
2. Dacă $|A| \leq |B|$, avem $|A| + |B| = |B|$;
3. $|A \times A| = |A|$;
4. $|A^n| = |A|$;
5. $|A^A| = |2^A| = 2^{|A|}$.

Curs 13: Ordinali

Reamintim definiția unui ordinal.

Definiție 1. O mulțime α se numește ordinal dacă:

1. $(\forall x)(x \in \alpha \rightarrow x \subseteq \alpha)$;
2.
 - $(\forall x, y, z \in \alpha)((x \in y \wedge y \in z) \rightarrow (x \in z))$;
 - $(\forall x, y \in \alpha)(x \in y \rightarrow y \notin x)$;
 - $(\forall \beta)\{(\beta \subseteq \alpha \wedge \beta \neq \emptyset) \rightarrow \exists x[x \in \beta \wedge \forall y(y \in \beta \rightarrow (x = y \vee x \in y))]\}$.

Definiție 2. Fie $(A, \leq)$ o mulțime ordonată. O submulțime $S \subseteq A$ se numește segment inițial al lui A dacă are proprietatea că, dacă $x \in S$, toate elementele mai mici decât x aparțin lui S ,

$$\forall x[x \in S \rightarrow \forall y((y \in A \wedge y \leq x) \rightarrow y \in S)].$$

Am demonstrat că într-o mulțime bine ordonată $(A, \leq)$ pentru orice segment inițial S al lui A avem $S = A$ sau $\exists a \in A$ cu $S = \{x \in A \mid x \leq a\}$.

Definiție 3. Fie $(A, \leq)$ și $(B, \leq)$ mulțimi ordonate. O funcție $f : A \rightarrow B$ se numește morfism de ordine dacă $\forall x, y \in A$ din $x \leq y$ rezultă $f(x) \leq f(y)$. Morfismul f se numește izomorfism de ordine dacă f este bijectivă și f^{-1} este tot morfism de ordine. Mulțimile $(A, \leq)$ și $(B, \leq)$ se numesc izomorfe dacă există măcar un izomorfism de ordine $f : A \rightarrow B$.

Propoziție 1. Dacă $(A, \leq)$ și $(B, \leq)$ sunt mulțimi total ordonate, atunci orice morfism de ordine bijectiv $f : A \rightarrow B$ este izomorfism de ordine.

Propoziție 2. Fie $(A, \leq)$ și $(B, \leq)$ mulțimi bine ordonate. Atunci are loc exact una din situațiile:

1. A izomorf cu B ;
2. A izomorf cu un segment inițial al lui B ;
3. B izomorf cu un segment inițial al lui A .

Teorema 1. Fie $(A, \leq)$ o mulțime bine ordonată. Atunci există un unic ordinal $(\alpha, \preceq)$ izomorf cu $(A, \leq)$, unde pe ordinalul α am definit relația $\preceq$ prin $u \preceq v$ dacă $u \in v$ sau $u = v$ (relația $\preceq$ este o relație de bună ordonare).

Pentru o mulțime bine ordonată $(A, \leq)$, ordinalul $(\alpha, \preceq)$ care este izomorf cu $(A, \leq)$ se notează $\overline{(A, \leq)}$.

Propoziție 3. Fie $(A, \leq)$ și $(A', \leq')$ mulțimi bine ordonate. Avem că există un izomorfism între $(A, \leq)$ și $(A', \leq')$ dacă și numai dacă există un izomorfism între $\overline{(A', \leq')}$ și $\overline{(A, \leq)}$.

Definiție 4. Fie $\alpha = \overline{A}$ și $\beta = \overline{B}$ două ordinale.

- a) Spunem că $\alpha \sqsubset \beta$ dacă există $b \in B$ astfel încât A să fie izomorf cu $S_b = \{y \in B \mid y \leq b\}$.
- b) Spunem că $\alpha \sqsubseteq \beta$ dacă $\alpha \sqsubset \beta$ sau $\alpha = \beta$.

Teorema 2.

1. Dacă $\mathcal{O}$ este o mulțime a cărei elemente sunt ordinale atunci $(\mathcal{O}, \sqsubseteq)$ este mulțime bine ordonată.
2. Dacă α și β sunt ordinale, atunci $\alpha \sqsubseteq \beta \Leftrightarrow \alpha \preceq \beta \Leftrightarrow \alpha \subseteq \beta$.

Operații cu ordinali

- o Adunarea. Fie $(A, \leq)$ și $(B, \leq)$ două mulțimi bine ordonate. Pe $A + B$ definim relația $\leq$ prin:

$$(0, a_1) \leq (0, a_2) \text{ dacă } a_1 \leq a_2;$$

$$(1, b_1) \leq (1, b_2) \text{ dacă } b_1 \leq b_2;$$

$$(0, a) \leq (1, b) \text{ pentru orice } a \in A \text{ și } b \in B.$$

Atunci $(A + B, \leq)$ este bine ordonată și $\overline{A + B} : \stackrel{\text{def.}}{=} \overline{A + B}$. Această definiție este corectă (nu depinde de reprezentării aleși pentru clasele de echivalență modulo a relației de izomorfism). Adunarea are proprietăți:

$$1) \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \text{ pentru orice ordinali } \alpha, \beta, \gamma;$$

$$2) \alpha \sqsubseteq \beta \Leftrightarrow \exists \gamma \neq 0 \text{ cu } \beta = \alpha + \gamma;$$

$$3) \alpha \sqsubseteq \beta \text{ și } \alpha' \sqsubseteq \beta' \text{ implică } \alpha + \alpha' \sqsubseteq \beta + \beta';$$

$$4) \text{ Dacă } \alpha \sqsubset \beta, \text{ atunci pentru orice ordinal } \gamma \text{ avem}$$

$$\gamma + \alpha \sqsubset \gamma + \beta,$$

$$\alpha + \gamma \sqsubseteq \beta + \gamma;$$

$$5) \alpha \cup \{\alpha\} = \alpha + 1 \text{ pentru orice ordinal } \alpha;$$

$$6) \gamma + \alpha = \gamma + \beta \Rightarrow \alpha = \beta;$$

$$7) \gamma + \alpha \sqsubset \gamma + \beta \Rightarrow \alpha \sqsubset \beta;$$

$$\alpha + \gamma \sqsubset \beta + \gamma \Rightarrow \alpha \sqsubset \beta.$$

- o Înmulțirea ordinalilor.

Fie $(A_1, \leq)$ și $(B_1, \leq)$ două mulțimi bine ordonate. Pe produsul cartezian $A \times B$ definim relația $\leq$ prin: $(a, b) \leq (a', b')$ dacă avem $a < a'$ sau $(a = a' \text{ și } b \leq b')$. Avem că $(A \times B, \leq)$ este bine ordonată și $\overline{A \cdot B} : \stackrel{\text{def.}}{=} \overline{A \times B}$.

Înmulțirea ordinalilor are următoarele proprietăți:

$$1) \alpha(\beta\gamma) = (\alpha\beta)\gamma, \text{ pentru orice ordinali } \alpha, \beta, \gamma;$$

$$2) \alpha(\beta + \gamma) = \alpha\gamma + \alpha\beta, \text{ pentru orice ordinali } \alpha, \beta, \gamma;$$

$$3) \alpha \sqsubset \beta \text{ și } \gamma \neq 0 \Rightarrow \gamma\alpha \sqsubset \gamma\beta, \text{ pentru orice ordinali } \alpha, \beta, \gamma;$$

$$4) \alpha \sqsubseteq \beta \Rightarrow \alpha\gamma \sqsubseteq \beta\gamma, \text{ pentru orice ordinali } \alpha, \beta, \gamma;$$

$$5) \gamma\alpha \sqsubset \gamma\beta \Rightarrow \alpha \sqsubset \beta, \text{ pentru orice ordinali } \alpha, \beta, \gamma;$$

$$6) \gamma\alpha = \gamma\beta \Rightarrow \alpha = \beta, \forall \alpha, \beta, \gamma \text{ ordinali.}$$

Curs 14: Elemente de combinatorică

Fie A, B două mulțimi și $M \subseteq A \times B$.

Regula produsului pentru determinarea cardinalului mulțimii M

Dacă pentru constituirea unei perechi carteziene $(x, y) \in M$, elementul x poate fi ales în p moduri diferite și, indiferent de modul în care ar fi fost ales x , elementul y poate fi ales în q moduri diferite, atunci

$$|M| = p \cdot q.$$

Observație 1. Inductiv, dacă $M \subset A_1 \times \dots \times A_n$ și pentru constituirea unei n -uple $(x_1, \dots, x_n)$, x_i poate fi ales independent în p_i moduri $\forall i \in \{1, \dots, n\}$, atunci $|M| = p_1 \dots p_n$.

Definiție 5. Fie $X = \{x_1, \dots, x_n\}$.

- (a) Un șir de lungimea k din X în care fiecare element apare cel mult o dată se numește k -aranjament de n elemente. Numărul k -aranjamentelor de n elemente se notează A_n^k .
- (b) Un șir de lungime n de elemente din X în care fiecare element apare exact o dată se numește permutare de n elemente. Numărul permutărilor de n elemente se notează cu P_n .
- (c) O submulțime cu k elemente a lui X ($k \leq n$) se numește k -combinare cu n elemente. Numărul k -combinărilor cu n elemente se notează C_n^k .

Teorema 3. Pentru $k \leq n$ au loc relațiile:

1. $A_n^k = \frac{n!}{(n-k)!}$;
2. $P_n = n!$;
3. $C_n^k = \frac{n!}{k!(n-k)!}$.

Demonstrație.

1. Fie $x_{i_1}x_{i_2}\dots x_{i_k}$ un k -aranjament de n elemente din X . Atunci x_{i_1} poate fi ales în n moduri. Independent de alegerea lui x_{i_1} , x_{i_2} poate fi ales în $n-1$ moduri pentru că x_{i_2} poate fi oricare dintre $x_1, \dots, x_n$ mai puțin x_{i_1} . Continuând procesul de alegere x_{i_k} poate fi ales în $n-(k-1) = n-k+1$ moduri, deoarece poate lua orice valoare dintre $x_1, \dots, x_n$ mai puțin valorile luate deja de $x_{i_1}, \dots, x_{i_{k-1}}$.

Așadar, conform regulii produsului, vom obține că:

$$A_n^k = n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}.$$

2. $P_n = A_n^n = n!$.
3. Fie $A(X, k)$ mulțimea k -aranjamentelor din X și $C(X, k)$ mulțimea k -combinărilor din X . Definim funcția:

$$\rho : A(X, k) \rightarrow C(X, k)$$

prin $\rho(x_{i_1}x_{i_2}\dots x_{i_k}) = \{x_{i_1}, \dots, x_{i_k}\}$ oricare ar fi $x_{i_1}, \dots, x_{i_k}$ un k -aranjament din X . Evident ρ este surjectivă. Mai mult, $\forall A \in C(X, k)$, $|f^{-1}(\{A\})| = k!$ pentru că $f^{-1}(\{A\})$ conține exact toate k -aranjamentele care se pot forma din cele k -elemente ale lui A , în total $P_k = k!$ astfel de k -aranjamente.

Se verifică imediat că $A(X, k) = \bigcup_{A \in C(X, k)} f^{-1}(\{A\})$.

Evident, dacă $A, B \in C(X, k)$ cu $A \neq B$ avem $f^{-1}(\{A\}) \cap f^{-1}(\{B\}) = \emptyset$.

Deci $|A(X, k)| = \sum_{A \in C(X, k)} |f^{-1}(\{A\})| = \sum_{A \in C(X, k)} k! = C_n^k \cdot k!$.

Deci $C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$.

□

Proprietăți:

1. $C_n^k = C_n^{n-k}$;
2. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$;
3. $\sum_{h=0}^k C_m^h C_n^{k-h} = C_{m+n}^k$;
4. $C_n^k = \frac{n}{k} C_{n-1}^{k-1}$.

Relațiile (1), (2) și (4) se verifică direct. Pentru (3) se folosește relația

$$(1+x)^{m+n} = (1+x)^m(1+x)^n$$

și formula de mai jos:

$$(1+x)^n = \sum_{k=0}^n C_n^k x^k \quad (*).$$

Demonstrație. Procedăm prin inducție după n . Fie $P(n) : (1+x)^n = \sum_{k=0}^n C_n^k x^k$.

Evident $P(1)$ este adevărată deoarece $1+x = C_1^0 + C_1^1 x$. Presupunem afirmația

$$(1+x)^n = \sum_{k=0}^n C_n^k x^k$$

adevărată și arătăm că $(1+x)^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k x^k$ este adevărată. Într-adevăr

$$(1+x)^{n+1} = (1+x)^n(1+x) = \sum_{k=0}^n C_n^k x^k (1+x) = \sum_{k=0}^n C_n^k x^k + \sum_{k=0}^n C_n^k x^{k+1} =$$

$$C_n^0 + C_n^1 x + \dots + C_n^n x^n + C_n^0 x + C_n^1 x^2 + \dots + C_n^n x^{n+1} =$$

$$C_n^0 + x(C_n^0 + C_n^1) + x^2(C_n^1 + C_n^2) + \dots + x^n(C_n^n + C_n^{n-1}) + C_n^n x^{n+1} =$$

$$C_{n+1}^0 + C_{n+1}^1 x + C_{n+1}^2 x^2 + \dots + C_{n+1}^n x^n + C_{n+1}^{n+1} x^{n+1}$$

deoarece $C_{n+1}^k = C_n^k + C_n^{k-1}$.

□

Observație 2.

$$(x + y)^n = x^n \left(1 + \frac{y}{x}\right)^n \stackrel{(*)}{=} x^n \sum_{k=0}^n C_n^k \left(\frac{y}{x}\right)^k = \sum_{k=0}^n C_n^k x^{n-k} y^k \quad (\text{Binomul lui Newton}).$$

Teorema 4 (Principiul includerii și excluderii). *Fie $A_1, \dots, A_n$ mulțimi finite. Avem*

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \dots \\ &+ (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| + \dots + (-1)^{n+1} \left| \bigcap_{i=1}^n A_i \right|. \end{aligned}$$

Demonstrație. Procedăm prin inducție după n . Pentru $n = 2$ avem:

$$|A_1 \cup A_2| = |A_1| + |A_2 - A_1|$$

și

$$|A_2| = |A_2 - A_1| + |A_1 \cap A_2|.$$

Am folosit că, dacă $A \cap B = \emptyset$, atunci $|A \cup B| = |A + B| = |A| + |B|$.

Deci $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ (*). Acum să presupunem că afirmația din enunț este adevărată pentru un anumit n și arătăm că ea este adevărată pentru $n + 1$. Avem:

$$\begin{aligned} \left| \bigcup_{i=1}^{n+1} A_i \right| &= \left| \bigcup_{i=1}^n A_i \cup A_{n+1} \right| \stackrel{(*)}{=} \left| \bigcup_{i=1}^n A_i \right| + |A_{n+1}| - \left| \left(\bigcup_{i=1}^n A_i \right) \cap A_{n+1} \right| = \\ &\sum_{i=1}^{n+1} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n+1} \left| \bigcap_{i=1}^n A_i \right| - \left| \bigcup_{i=1}^n (A_i \cap A_{n+1}) \right| = \\ &\sum_{i=1}^{n+1} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n+1} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n+2} \left| \bigcap_{i=1}^{n+1} A_i \right|. \end{aligned}$$

□

Teorema 5. *Fie A și B două mulțimi cu $|A| = m$ și $|B| = n$. Atunci:*

1. $|B^A| = |\{f : A \rightarrow B \mid f \text{ funcție}\}| = n^m$;
2. $|\{f : A \rightarrow B \mid f \text{ funcție bijectivă}\}| = \begin{cases} m!, m = n \\ 0, m \neq n \end{cases}$;
3. $|\{f : A \rightarrow B \mid f \text{ funcție injectivă}\}| = \begin{cases} A_n^m, m \leq n \\ 0, m > n \end{cases}$;
4. $|\{f : A \rightarrow B \mid f \text{ funcție surjectivă}\}| = \begin{cases} \sum_{k=0}^{n-1} (-1)^k C_n^k (n-k)^m, m \geq n \\ 0, m < n \end{cases}$.

Demonstrație.

1. Procedăm prin inducție după m . Dacă $m = 1$, evident numărul funcțiilor de la A la B este n . Într-adevăr $A = \{x_0\}$, iar $f(x_0)$ poate fi ales în n moduri. Presupunem $|B^A| = n^{|A|}$ pentru orice mulțime A cu $|A| \leq m-1$. Fie $|A| = m$. Atunci $A = A' \cup \{z_0\}$ unde $|A'| = m-1$ și $z_0 \in A, z_0 \notin A'$.

Oricărei funcții $f : A \rightarrow B$ i se asociază în mod unic $f|_{A'} : A' \rightarrow B$, $f|_{A'}(a) = f(a), \forall a \in A'$. Pentru fiecare funcție $g : A' \rightarrow B$ putem construi n funcții distincte $g^b : A \rightarrow B, b \in B$ definite prin $g^b(a) = \begin{cases} g(a), a \in A' \\ b, a = z_0 \end{cases}$.

Conform ipotezei inductive $|B^{A'}| = n^{m-1}$ și deci $|B^A| = n \cdot n^{m-1} = n^m$.

2. Dacă $n \neq m$ evident nu există funcții bijective de la A la B . Analizăm cazul $n = m$. Procedăm prin inducție după m . Pentru $m = 1$, afirmația este trivială. Presupunem adevărată afirmația pentru $|A| = |B| = m-1$. Fie acum A și B două mulțimi cu $|A| = |B| = m$. Fie $x_0 \in A$ și $A' = A - \{x_0\}$. O funcție bijectivă $f : A \rightarrow B$ este complet determinată de funcția bijectivă $f|_{A'} : A' \rightarrow B - \{f(x_0)\}$, $f|_{A'}(a) = f(a), \forall a \in A'$ și de valoarea $f(x_0)$. Conform ipotezei inductive și a regulii produsului, deoarece $f(x_0)$ poate fi ales în m moduri, iar $f|_{A'}$ poate fi ales în $(m-1)!$ moduri, avem că f poate fi ales în $m(m-1)! = m!$ moduri.
3. Pentru orice funcție injectivă $f : A \rightarrow B$, funcția $g : A \rightarrow \text{Im}f, g(a) = f(a), \forall a \in A$ este bijectivă. Așadar funcția f este unic determinată de g și de $\text{Im}f$. $\text{Im}f$ poate fi aleasă în C_n^m moduri (fiind o submulțime cu m elemente a unei mulțimi cu n elemente) iar g în $m!$ moduri. Conform regulii produsului, f poate fi aleasă în $m! \cdot C_n^m = A_n^m$ moduri în cazul $n \geq m$. Dacă $n < m$ evident nu există nici o injecție de la A la B .
4. Fie $A = \{x_1, \dots, x_m\}, B = \{y_1, \dots, y_n\}$. Fie $S_{m,n} = \{f : A \rightarrow B \mid f \text{ surjectivă}\}$. Fie $A_i = \{f \in B^A \mid y_i \notin \text{Im}f\}, i \in \{1, \dots, n\}$. Atunci $|S_{m,n}| = |B^A| - |\bigcup_{i=1}^n A_i| = n^m - |\bigcup_{i=1}^n A_i|$. Dar $A_i = \{f : A \rightarrow B - \{y_i\} \mid f \text{ funcție}\}$. Mai mult, pentru $k \in \{1, 2, \dots, n\}, 1 \leq i_1 < i_2 < \dots < i_k \leq n$, avem $A_{i_1} \cap \dots \cap A_{i_k} = \{f : A \rightarrow B - \{y_{i_1}, y_{i_2}, \dots, y_{i_k}\} \mid f \text{ funcție}\}$. Așadar $|A_i| = (n-1)^m, \dots, |A_{i_1} \cap \dots \cap A_{i_k}| = (n-k)^m$. Conform principiului includerii și excluderii obținem

$$\begin{aligned} |S_{m,n}| &= n^m - \sum_{i=1}^m |A_i| + \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| - \dots + \\ &+ (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| + \dots + (-1)^n |A_1 \cap \dots \cap A_n| = \\ &= n^m - C_n^1(n-1)^m + C_n^2(n-2)^m - \dots + (-1)^k C_n^k(n-k)^m + \dots + (-1)^{n-1} C_n^{n-1}. \end{aligned}$$

□