Curs 7

II.3 Grupuri

II.3.1 Definiţie. Exemple

Definiţia II.3.1.1. *Un grup G este o mulţime, împreună cu o operaţie binară pe G, notată $\cdot : G \times G \longrightarrow G$, $(x, y) \longrightarrow x \cdot y$, astfel încât:*

(G1) *(Asociativitate)* $(x \cdot y) \cdot z = x \cdot (y \cdot z), (\forall)x, y, z \in G$;

(G2) *(Element neutru)* $(\exists)e \in G$ *astfel încât* $x \cdot e = e \cdot x = x$ $(\forall)x \in G$;

(G3) *(Inversabilitate)* $(\forall)x \in G(\exists)x^{-1} \in G$ *astfel încât* $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Dacă în plus are loc:

(G4) *(Comutativitate)* $x \cdot y = y \cdot x, (\forall)x, y \in G$,

spunem că G este abelian sau comutativ.

Exemplul II.3.1.2. *(i)* $(\mathbb{Z}, +)$ *şi* $(\mathbb{Z}_n, +)$ *sunt grupuri abeliene.*

(ii) $(\mathbb{Z}, \cdot)$ *şi* $(\mathbb{Z}_n, \cdot)$ *sunt doar monoizi. Dar pentru orice monoid M, mulţimea elementelor inversabile formează un grup, notat $U(M)$. În particular, avem: $U(\mathbb{Z}) = \{-1, 1\}$, grup multiplicativ cu 2 elemente, $U(\mathbb{Z}_n) = \{\hat{k} \in \mathbb{Z}_n \mid (k, n) = 1\}$ grup cu $\phi(n)$ elemente.*

Merită reamintită aici metoda de determinare al inversului unui element $\hat{k} \in U(\mathbb{Z}_n)$. Acesta se bazează pe următoarele observaţii: fiind date două numere întregi $a, b \in \mathbb{Z}^*$, cel mai mare divizor comun al acestora este $(a, b) = d \Leftrightarrow (\exists)k, l \in \mathbb{Z}$, $ak + bl = d$. De asemenea, $(a, b) = (a, b-a)$. De exemplu, să determinăm inversul lui $\hat{3}$ în $U(\mathbb{Z}_{47})$. Avem $(3, 47) = 1$, obţinut prin algoritmul lui Euclid astfel:

$$\begin{aligned} 47 &= 3 \cdot 15 + 2 \\ 3 &= 2 \cdot 1 + 2 \end{aligned}$$

de unde rezultă că

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (47 - 3 \cdot 15) \cdot 1 \\ &= 3 - 47 \cdot 1 + 3 \cdot 15 \cdot 1 \\ &= 3 \cdot 16 - 47 \cdot 1 \end{aligned}$$

Trecând la clase de resturi modulo 47*, obţinem*

$$\begin{aligned} \hat{1} &= \hat{3} \cdot \hat{16} - \hat{0} \cdot \hat{1} \\ &= \hat{3} \cdot \hat{16} \end{aligned}$$

Deci $(\hat{3})^{-1} = \hat{16}$.

(iii) $(\mathcal{M}_n(\mathbb{R}), +)$ *este grup abelian, dar* $(\mathcal{M}_n, (\mathbb{R}), \cdot)$ *este doar monoid. De fapt,* $U(\mathcal{M}_n(\mathbb{R})) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid detA \neq 0\}$ *(şi se notează de obicei cu* GL_n*, grupul general liniar de ordin* n*).*

(iv) Fie X *o mulţime şi* $(X^X, \circ)$ *monoidul funcţiilor definite pe* X *cu valori tot în mulţimea* X*. Atunci* $U(X^X) = \{f : X \to X \mid f$ *bijecţie* $\}$*. Acest grup se mai notează şi cu* S_X*. Reamintim că o funcţie bijectivă se mai numeşte şi permutare. Avem deci* $(S_X, \circ, \mathbf{1}_X)$ *grupul permutărilor mulţimii* X *(grup necomutativ dacă* $|X| > 2$*). Dacă* X *este finită,* $|X| = n$*, atunci* S_X *se mai notează şi* S_n *şi* $|S_n| = n!$*.*
Cazul $n = 3$*: putem considera* $X = \{1, 2, 3\}$*; vom reprezenta o funcţie bijectivă* $f : X \to X$ *printr-un tabel* $\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$*. Se obţine astfel*

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Notând $\mathbf{1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$*,* $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *şi* $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$*, atunci avem:* $f^2 = g^3 = \mathbf{1}$*,* $g^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$*,* $fg = g^2 f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$*,* $gf = fg^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

(v) Grupul diedral D_n *(grupul simetriilor poligonului regulat cu* n *laturi). Vom prezenta doar cazul* $n = 4$*: considerăm un pătrat împărţit în 4 părţi egale:* $\begin{array}{|c|c|} \hline 2 & 1 \\ \hline 3 & 4 \\ \hline \end{array}$*. Asupra acestui pătrat vom efectua următoarele transformări:*

- *Rotaţii în sens trigonometric în jurul centrului pătratului:* $R_0 : \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 & 4 \\ \hline \end{array}$, $R_{90} : \begin{array}{|c|c|}\hline 1 & 4 \\ \hline 2 & 3 \\ \hline \end{array}$, $R_{180} : \begin{array}{|c|c|}\hline 4 & 3 \\ \hline 1 & 2 \\ \hline \end{array}$, $R_{270} : \begin{array}{|c|c|}\hline 3 & 2 \\ \hline 4 & 1 \\ \hline \end{array}$.
- *Reflexii faţă de axele de simetrie:* $S_| : \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline \end{array}$, $S_- : \begin{array}{|c|c|}\hline 3 & 4 \\ \hline 2 & 1 \\ \hline \end{array}$, $S_/ : \begin{array}{|c|c|}\hline 4 & 1 \\ \hline 3 & 2 \\ \hline \end{array}$, $S_\backslash : \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 & 4 \\ \hline \end{array}$

Fie $\mathcal{D}_4 = \{R_0,\ R_{90},\ R_{180},\ R_{270},\ S_|,\ S_-,\ S_/,\ S_\backslash\}$. *Atunci mulţimea* $\mathcal{D}_4$ *este închisă la operaţia de compunere a funcţiilor (exerciţiu: scrieţi tabla!). De exemplu,* $R_{90} \circ S_| = S_\backslash$, $S_| \circ R_{90} = S_/$. *Cum operaţia de compunere a transformărilor (funcţiilor) este asociativă şi fiecare transformare este inversabilă (de exemplu, fiecare simetrie este propria sa inversă), rezultă că* $\mathcal{D}_4$ *este un grup necomutativ cu elementul neutru* R_0.

Definiţia II.3.1.3. *O submulţime* H *a unui grup* G *se numeşte* subgrup *dacă:*

(SG1) $(\forall)x, y \in H \Rightarrow x \cdot y \in H$

(SG2) $e \in H$

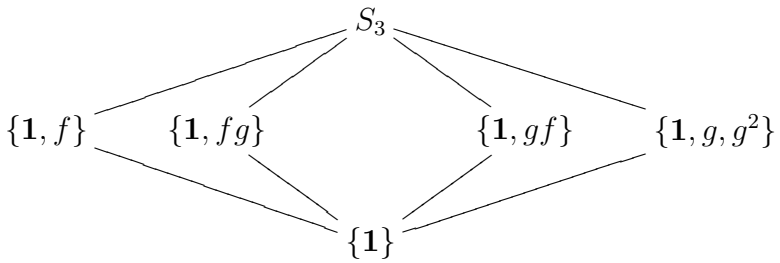
(SG3) $(\forall)x \in H \Rightarrow x^{-1} \in H$

(condiţia (SG2) nu e necesară; rezultă din (SG1) şi (SG3)).

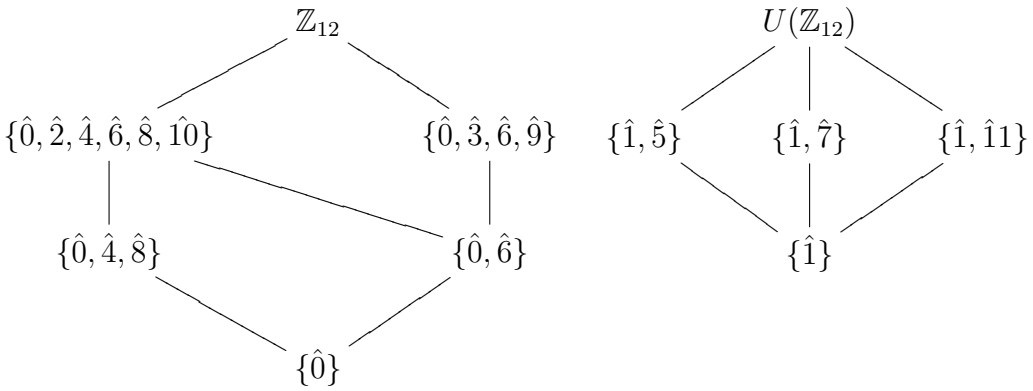
În particular, orice subgrup H este grup cu operaţia indusă, cu acelaşi element neutru.

Exemplul II.3.1.4. *(i)* $\{0\}$ *este subgrup în* $(\mathbb{Z}, +)$. *La rândul său,* $\mathbb{Z}$ *este subgrup de exemplu în* $(\mathbb{Q}, +)$.

(ii) Subgrupurile lui S_3*:*



(iii) Subgrupurile grupurilor $(\mathbb{Z}_{12},\ +)$ *şi* $(U(\mathbb{Z}_{12}),\ +)$ *(unde* $U(\mathbb{Z}_{12} = \{\hat{1},\ \hat{5},\ \hat{7},\ \hat{11}\}$*):*



Ordinul unui grup G este numărul de elemente al mulţimii G (posibil ∞). Ordinul unui element $x \in G$ este cel mai mic număr natural n astfel încât $x^n = e$ (sau ∞ dacă nu există asemenea n). Dacă $x \in G$, atunci $< x >= \{e,\ x,\ x^2,\ x^3, \ldots\}$ este subgrup (numit subgrupul ciclic generat de x) de ordin n egal cu ordinul lui x.

Teorema II.3.1.5. *(Lagrange) Fie* G *un grup finit şi* $H \subseteq G$ *un subgrup. Atunci* $|H| \mid |G|$.

Corolarul II.3.1.6. *Fie* G *un grup finit de ordin* $|G| = n$ *şi* $x \in G$. *Atunci* $x^n = e$.

Exemplul II.3.1.7. *Fie* p *un număr prim. Atunci* $U(\mathbb{Z}_p) = \{\hat{1}, \hat{2}, ..., \hat{p-1}\}$ *şi din Corolar rezultă* $\hat{k}^{p-1} = \hat{1}, \forall \hat{k} \in U(\mathbb{Z}_p)$. *În particular, pentru orice* $x \in \mathbb{Z}$ *prim cu* p, *avem* $x^{p-1} \equiv 1 (mod\ p)$ *(teorema lui Fermat).*

Aplicaţie*: test parţial pentru detectarea numerelor prime:*

- *Alegem* x *număr natural nedivizibil cu* p;
- *Dacă* $x^{p-1} \not\equiv (mod\ p)$, *atunci* p *nu e prim.*

Testăm $p = 35$. *Alegem* $x = 2$. *Avem* $2^{34} \equiv 9 (mod\ 35)$, *deci* p *nu e prim. Testăm acum* $p = 341 = 11 \cdot 31$. *Alegem* $x = 2$. *Atunci* $2^{340} \equiv 1 (mod\ 341)$, *deci rezultatul nu este suficient. Alegem şi* $x = 3$. *Atunci* $3^{340} \equiv 56 (mod\ 341)$, *deci* 341 *nu e prim.*

II.3.2 Grupuri ciclice în criptografie. Protocolul Diffie-Hellman (1976)

Este o metodă prin care două părţi pot comunica prin mesaje secrete pe un canal public de comunicaţie, fără să fie nevoie de o terţă parte sau schimb off-line; se bazează pe conceptul de cheie publică privată:

(i) Se fac publice următoarele elemente: un număr prim mare p şi un număr g primitiv modulo p (adică mulţimea resturilor modulo p ale numerelor $g, g^2, \ldots, g^{p-1}$ coincide cu $\{1, 2, 3, ..., p-1\}$).

(ii) Utilizatorii Alice şi Bob doresc să stabilească o cheie secretă.

(iii) Alice alege o valoare aleatoare $x \in \mathbb{Z}_p$, calculează $a \equiv g^x (mod\ p)$ şi trimite rezultatul lui Bob pe canalul public.

(iv) Analog Bob alege $y \in \mathbb{Z}_p$, calculează $b \equiv g^y (mod\ p)$ şi trimite rezultatul lui Alice.

(v) Alice calculează $b^x \equiv (g^y)^x \equiv (g^x)^y \equiv a^y (mod\ p)$.

(vi) Bob obţine acelaşi rezultat.

(vii) $K = b^x = a^y$ este cheia privată care o vor utiliza în viitor.

Dacă un al treilea utilizator Eve urmăreşte comunicarea, atunci află p, g, a, b, deci are de rezolvat sistemul

$$\begin{aligned} g^x &\equiv a(mod\ p) \\ g^y &\equiv b(mod\ p) \end{aligned}$$

pentru a descoperi cheia privată $k = a^y = b^x$. În practică, aceast lucru este foarte dificil.

Exemplul II.3.2.1. *Fie $p = 7$, $g = 3$.*

- *Alice alege cheia $x = 1$, iar Bob alege $y = 2$.*
- *Alice calculează cheia sa publică $a \equiv g^x (mod\ p)$, $a = 3$ şi o trimite lui Bob.*
- *Bob calculează cheia sa publică $b \equiv g^y (mod\ p)$, $b = 2$ şi o trimite lui Alice.*
- *Alice calculează $K \equiv b^x (mod\ p)$, $K = 2$*
- *Bob calculează $k \equiv a^y (mod\ p)$, $K = 2$*

Deci $K = 2$ este cheia secretăpe care o vor folosi în viitor pentru a comunica mesaje private.

II.4 Inele. Corpuri

II.4.1 Definiţie. Exemple

Definiţia II.4.1.1. *Un inel R este o mulţime, împreună cu două operaţii binare, notate $+ : R \times R \longrightarrow R$, $\cdot : R \times R \longrightarrow R$, astfel încât:*

(R1) $(R, +)$ *este grup abelian.*

(R2) *(R,·) este monoid.*

(R3) *(Distributivitate)* $x \cdot (y + z) = x \cdot y + x \cdot z, (\forall)x, y, z \in \mathbb{R}$, $(x + y) \cdot z = x \cdot z + y \cdot z, (\forall)x, y, z \in \mathbb{R}$

Proprietaţi suplimentare

(i) Inel comutativ: $x \cdot y = y \cdot x, (\forall)x, y \in R$.

(ii) Inel boolean: $x \cdot x = x, (\forall)x \in R$.

(iii) Inel integru: $(\forall)x, y \in R \setminus \{0\}$, $x \cdot y \neq 0$ (avem voie să simplificăm la dreapta sau la stânga).

(iv) Corp: $(\forall)x \in R \setminus \{0\}$, x este inversabil în raport cu operaţia $\cdot$.

Exemplul II.4.1.2. *(i)* $(\mathbb{Z}, +, \cdot)$ *este un inel comutativ integru.*

(ii) $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ *este un inel necomutativ şi cu divizori ai lui zero.*

(iii) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ *(p prim) sunt corpuri comutative.*

(iv) Există şi corpuri necomutative: corpul cuaternionilor $\mathbb{H}$ (după numele matematicianului W.R. Hamilton), având drept elemente tupluri de forma $q = (a, b, c, d)$ cu $a, b, c, d \in \mathbb{R}$, cu operaţia aditivă - adunarea pe componente. Pentru operaţia multiplicativă, notăm $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$, $k = (0, 0, 0, 1)$. Atunci orice $q \in \mathbb{H}$, $q = (a, b, c, d)$ se mai scrie $q = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$. Definim operaţia multiplicativă prin:

$$\begin{aligned} 1 \cdot 1 &= 1 \\ 1 \cdot i = i \cdot 1 &= i \\ 1 \cdot j = j \cdot 1 &= j \\ 1 \cdot k = k \cdot 1 &= k \\ i^2 = j^2 = k^2 &= -1 \\ i \cdot j = -j \cdot i &= k \\ j \cdot k = -k \cdot j &= i \\ k \cdot i = -i \cdot k &= j \end{aligned}$$

şi extindem prin liniaritate la toate elementele lui $\mathbb{H}$. Se obţine astfel pe $\mathbb{H}$ o structură de inel necomutativ, în care orice element $q \in \mathbb{H} \setminus \{0\}$ este inversabil, cu inversul: $q^{-1} = \frac{1}{a^2+b^2+c^2+d^2}(a \cdot 1 - b \cdot i - c \cdot j - d \cdot k)$, deci un corp necomutativ.

Teorema II.4.1.3. *Orice corp finit $\Bbbk$ este comutativ şi există $p, n \in \mathbb{N}$ cu p prim astfel încât $|\Bbbk| = p^n$. Mai mult, oricare două corpuri finite cu acelaşi număr de elemente sunt izomorfe (izomorfism de corpuri: bijecţie care păstrează cele două operaţii, elementele simetrizabile şi inversabilitatea în raport cu operaţiile).*

Un corp finit cu p^n elemente se mai numeste şi corp Galois şi se notează $GF(p^n)$ sau $\mathbb{F}_{p^n}$.

Construcţia unui corp Galois cu p^n elemente: fie $P \in \mathbb{Z}_p[X]$ un polinom ireductibil de grad n; atunci mulţimea resturilor la împărţirea cu P formează corpul dorit în raport cu adunarea şi înmulţirea polinoamelor modulo P.

Pentru $p = 2$, asociind fiecărui polinom $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in \mathbb{Z}_2[X]$ secvenţa coeficienţilor săi $(a_0, a_1, \ldots, a_{n-1}) \in (\mathbb{Z}_2)^n$, obţinem o structură de corp pe mulţimea stringurilor binare de lungime n.

Exemplul II.4.1.4. *Corpul $GF(2^3)$ (realizat pe mulţimea $(\mathbb{Z}_2)^3$).*

Căutăm un polinom de grad 3 ireductibil din $\mathbb{Z}_2[X]$; din cele 8 polinoame existente, se verifică uşor că doar X^3+X+1 şi X^3+X^2+1 sunt ireductibile. Alegem de exemplu $P = X^3 + X + 1$. Atunci resturile la împărţirea cu P sunt:

$0 \longleftrightarrow 000$
$1 \longleftrightarrow 001$
$X \longleftrightarrow 010$
$X + 1 \longleftrightarrow 011$
$X^2 \longleftrightarrow 100$
$X^2 + 1 \longleftrightarrow 101$
$X^2 + X \longleftrightarrow 110$
$X^2 + X + 1 \longleftrightarrow 111$

Pentru adunarea şi multiplicarea modulo P, avem de exemplu

$$\begin{aligned}(X^2 + 1) + (X^2 + X + 1) &= 2X^2 + X + 2 \\ &= X (mod\ P)\end{aligned}$$

şi

$$\begin{aligned}(X^2 + 1)(X^2 + X + 1) &= X^4 + X^3 + X^2 + X^2 + X + 1 \\ &= X^4 + 2X^2 \\ &= X^4 \\ &= X^2 + X (mod\ P)\end{aligned}$$

Exerciţiul II.4.1.5. *Scrieţi tabla înmulţirii în* $(\mathbb{Z}_2)^3$ *folosind corespondenţa de mai sus şi verificaţi că orice string diferit de* 000 *este inversabil.*

Fie acum *Bbbk* un corp şi $\Bbbk[X] = \{a_0 + a_1X + \ldots + a_nX^n \mid a_0, a_1, a_n \in \Bbbk, n \in \mathbb{N}\}$ inelul polinoamelor cu coeficienţi în $\Bbbk$.
Proprietăţi:

(i) $\Bbbk[X]$ inel integru.

(ii) (Teorema împărţirii cu rest) $(\forall)P, Q \in \Bbbk[X], Q \neq 0$, există în mod unic două polinoame $C, R \in \Bbbk[X]$, astfel încât $gradR < gradQ$ şi $P = Q \cdot C + R$.

(iii) (Teorema lui Bezout) Fie $P \in \Bbbk[X]$, $a \in \Bbbk$. Atunci $P(a) = 0 \Leftrightarrow X - a \mid P$.

(iv) $P \in \Bbbk[X]$, $gradP = n \Longrightarrow P$ are cel mult n rădăcini.

Consecinţa II.4.1.6. *Orice funcţie* $f : \Bbbk \longrightarrow \Bbbk$*, unde* $\Bbbk$ *este un corp finit, este polinomială (soluţie: polinomul de interpolare Lagrange).*

II.4.2 Aplicaţie în criptografie. Secret Sharing

Este metoda de a distribui un secret la un grup de participanţi, fiecărui participant fiindu-i atribuită câte o parte a secretului[1]. Secretul poate fi reconstituit doar prin combinarea a cel puţin un număr fixat de participanţi. Ideea: aşa cum două puncte din plan determină în mod unic o dreaptă(deci o funcţie de gradul I), 3 puncte determină o parabolă(o funcţie de gradul II), etc., k puncte în plan vor determina în mod unic un polinom de grad $k-1$. Fie n numărul participanţilor, $k < n$ şi S mesajul secret(un element dintr-un corp finit $\Bbbk$). Alegem la întâmplare $k-1$ elemente $a_1, a_2, a_3, ..., a_{k-1} \in \Bbbk$ şi luăm $a_0 = S$. Construim polinomul

$$P(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}$$

şi calculăm $(i, P(i))$ pentru $i = \overline{1,n}$ (deci corpul $\Bbbk$ va avea mai mult de n elemente). Fiecărui participant i se atribuie o pereche $(i, P(i))$ de elemente din corpul $\Bbbk$ (cunoscut de toţi). Fiind dat orice grup de k participanţi se poate reconstitui polinomul şi afla mesajul secret $S = a_0$.

Exemplul II.4.2.1. *Fie* $n = 5$*,* $k = 3$*,* $P = \hat{2}X^2 + \hat{7}X + \hat{10} \in \Bbbk = \mathbb{Z}_{11}$*. Secretul este* $S = \hat{10}$*. Mesajele participanţilor sunt:* $P(\hat{1}) = \hat{8}$*,* $P(\hat{2}) = \hat{10}$*,*

[1] A. Shamir, 1979.

$P(\hat{3}) = \hat{5}$, $f(\hat{4}) = \hat{4}$, $P(\hat{7}) = \hat{7}$. *Alegem grupul de participanţi* $(1, 2, 4)$. *Atunci polinomul reconstruit este:*

$$P(X) = \hat{8} \cdot \frac{(X-\hat{2})(X-\hat{4})}{(\hat{1}-\hat{2})(\hat{1}-\hat{4})} + \hat{10} \cdot \frac{(X-\hat{1})(X-\hat{4})}{(\hat{2}-\hat{1})(\hat{2}-\hat{4})} + \hat{4} \cdot \frac{(X-\hat{1})(X-\hat{2})}{(\hat{4}-\hat{1})(\hat{4}-\hat{1})}$$

şi

$$\begin{aligned} S &= P(0) \\ &= \hat{8} \cdot \hat{2} \cdot \hat{4} \cdot \hat{10}^{-1} \cdot \hat{8}^{-1} + \hat{10} \cdot \hat{1} \cdot \hat{4} \cdot \hat{1}^{-1} \cdot \hat{9}^{-1} + \hat{4} \cdot \hat{1} \cdot \hat{2} \cdot \hat{3}^{-1} \cdot \hat{2}^{-1} \\ &= \hat{8} \cdot \hat{2} \cdot \hat{4} \cdot \hat{10} \cdot \hat{7} + \hat{10} \cdot \hat{1} \cdot \hat{4} \cdot \hat{1} \cdot \hat{5} + \hat{4} \cdot \hat{1} \cdot \hat{2} \cdot \hat{4} \cdot \hat{6} \\ &= \hat{3} + \hat{2} + \hat{5} \\ &= \hat{10} \end{aligned}$$

II.5 Latici şi algebre Booleene

II.5.1 Latici

Laticile pot fi definite în două moduri: fie ca mulţimi cu anumite structuri de ordine, fie ca algebre (mulţimi cu operaţii), însă cele două definiţii sunt echivalente:

Definiţia II.5.1.1. *O* latice *este un poset* $(L, \leq)$ *cu proprietatea că pentru orice* $x, y \in L$, *există* $\sup\{x, y\}$ *şi* $\inf\{x, y\}$.

Reamintim că pentru o submulţime $X \subseteq L$ se defineşte marginea sa superioară - sau supremum - prin:

$$a = \sup X \iff \begin{cases} (\forall)x \in X, x \leq a \\ (\forall)b \in L \text{ astfel încât } x \leq b, (\forall)x \in X \Longrightarrow a \leq b \end{cases}$$

Analog definim marginea inferioara sau infimum:

$$a = \inf X \iff \begin{cases} (\forall)x \in X, a \leq x \\ (\forall)b \in L \text{ astfel încât } b \leq x, (\forall)x \in X \Longrightarrow b \leq a \end{cases}$$

Definiţia II.5.1.2. *O* latice *este o mulţime* L *împreună cu două operaţii binare* $\wedge : L \times L \longrightarrow L$, $\vee : L \times L \longrightarrow L$ *astfel încât*

(L1) *(Asociativitate)* $x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ $(\forall)x, y, z \in L$

(L2) *(Comutativitate)* $x \wedge y = y \wedge x,\ x \vee y = y \vee x\ (\forall)x, y \in L$

(L3) *(Idempotenţă)* $x \wedge x = x,\ x \vee x = x\ (\forall)x \in L$

(L4) *(Absorbţie)* $x \vee (x \wedge z) = x,\ x \wedge (x \vee z) = x\ (\forall)x, z \in L$

Propoziţia II.5.1.3. *Cele două definiţii sunt echivalente.*

Demonstraţie. Def.II.5.1.1⇒ Def.II.5.1.2: notăm $x \vee y = \mathsf{sup}\{x, y\}$ şi $x \wedge y = \mathsf{inf}\{x, y\},\ (\forall)x, y \in L$.

Def.II.5.1.2⇒ Def.II.5.1.1: relaţia de ordine este $x \leq y \iff x \wedge y = x\ (\forall)x, y \in L$ □

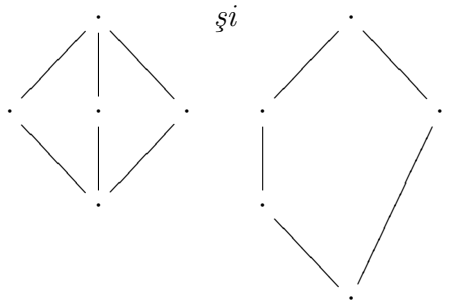
Exemplul II.5.1.4. *(i)* $(\mathcal{P}(X), \cup, \cap)$ *este o latice.*

(ii) Fie X o mulţime. Atunci mulţimile fuzzy peste X formează o latice (reamintim că o mulţime fuzzy peste X este dată printr-o funcţie $f : X \longrightarrow [0, 1]$). Pe mulţimea $Fuzzy_X = \{f : X \longrightarrow [0, 1]\}$ punem relaţia de ordine $f \leq g \iff (\forall)x \in X,\ f(x) \leq g(x)$. Atunci $\mathsf{sup}\{f, g\}(x) = \mathsf{max}(f(x), g(x))$ şi $\mathsf{inf}\{f, g\}(x) = \mathsf{min}(f(x), g(x)),\ (\forall)x \in X$.

(iii) Fie G un grup abelian cu operaţia notată aditiv. Atunci mulţimea subgrupurilor sale formează o latice în raport cu incluziunea, cu $\mathsf{inf}\{H_1, H_2\} = H_1 \cap H_2$ şi $\mathsf{sup}\{H_1, H_2\} = H_1 + H_2 = \{h_1 + h_2 \mid h_1 \in H_1,\ h_2 \in H_2\}$

(iv) Nu orice poset este o latice: fie de exemplu, mulţimea $\{1, 2, 3, 12, 18, 36\}$ ordonată prin divizibilitate. Atunci perechea $(2, 3)$ nu are margine superioară, iar perechea $(12, 18)$ nu are margine inferioară.

(v) Mulţimea numerelor întregi (Z) cu $x \wedge y = \mathsf{cmmdc}(x, y)$ şi $x \vee y = \mathsf{cmmmc}(x, y)$ este o latice.

(vi) Exemple de latici finite:  *şi* *sunt (sin-*

gurele!) latici cu 5 elemente.

II.5.2 Algebre Boole

Definiţia II.5.2.1. *O* algebră Boole *este o mulţime B împreună cu: două operaţii binare $\wedge : B \times B \longrightarrow B$, $\vee : B \times B \longrightarrow B$, o operaţia unară $(-)' : B \times B \longrightarrow B$ şi două constante (operaţii nulare) notate $0, 1 \in B$, astfel încât:*

(B1) *(Asociativitate)* $x \vee (y \vee z) = (x \vee y) \vee z,\ x \wedge (y \wedge z) = (x \wedge y) \wedge z\ (\forall)x, y, z \in B$

(B2) *(Comutativitate)* $x \wedge y = y \wedge x,\ x \vee y = y \vee x\ (\forall)x, y \in B$

(B3) *(Idempotenţă)* $x \wedge x = x,\ x \vee x = x\ (\forall)x \in B$

(B4) *(Absorbţie)* $x \vee (x \wedge z) = x,\ x \wedge (x \vee z) = x\ (\forall)x, z \in B$

(B5) *(Distributivitate)* $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\ (\forall)x, y, z \in B$

(B6) *(Top şi bottom)(primul şi ultimul element)* $x \vee 1 = 1,\ x \wedge 1 = x,\ x \vee 0 = x,\ x \wedge 0 = 0 (\forall)x \in B$

(B7) *(Complementaritate)* $x \wedge x' = 0,\ x \vee x' = 1 (\forall)x \in B$

Deci o algebră Boole este o latice cu proprietăţi suplimentare. Dar atenţie: nu orice latice este şi algebră Boole. Fie de exemplu $Fuzzy_X$ mulţimea mulţimilor fuzzy peste X, ca mai devreme, cu 0 funcţia constantă $X \longrightarrow [0, 1],\ x \longrightarrow 0$ şi 1 funcţia constantă $X \longrightarrow [0, 1],\ x \longrightarrow 1$ şi complementarea dată de $f'(x) = 1 - f(x)$ (atenţie: nu este vorba despre derivata funcţiei f!). Atunci $Fuzzy_X$ nu este o algebră Boole, căci de exemplu relaţia $f \vee f' = 1$ este falsă ($\mathsf{max}(f(x), 1 - f(x))$ nu este întotdeauna egal cu 1 pentru oricare x).

Corolarul II.5.2.2. *În orice algebră Boole au loc relaţiiile:*

(i) $(x')' = x$

(ii) $(x \vee y)' = x' \wedge y'$

(iii) $(x \wedge y)' = x' \vee y'$

Demonstraţie. (i) Să remarcăm mai întâi că x' e unicul element cu proprietatea (B7): dacă există x_1 şi x_2, atunci

$$\begin{aligned} x_1' &= x_1' \wedge 1 \\ &= x_1' \wedge (x \vee x_2') \\ &= (x_1' \wedge x) \vee (x_1' \wedge x_2') \\ &= 0 \vee (x_1' \wedge x_2') \\ &= x_1' \wedge x_2' \end{aligned}$$

şi analog $x_2' = x_1' \wedge x_2'$, deci $x_1' = x_2'$. Acum afirmaţia (i) rezultă imediat.

(ii) Este suficient să arătăm că $(x' \wedge y') \vee (x \vee y) = 1$ şi $(x' \wedge y') \wedge (x \vee y) = 0$. Dar

$$\begin{aligned} (x' \wedge y') \vee (x \vee y) &= [(x' \wedge y') \vee x] \vee y \\ &= [(x' \wedge x) \vee (y' \vee x)] \vee y \\ &= [0 \vee (y' \vee x)] \vee y \\ &= (y' \vee x) \vee y \\ &= (y' \vee y) \vee x \\ &= 1 \vee x \\ &= 1 \end{aligned}$$

şi analog $(x' \wedge y') \wedge (x \vee y) = 0$.

(iii) La fel. □

Exemplul II.5.2.3. *(i)* $(\mathcal{P}(X), \cup, \cap, (-)^c, \emptyset, X)$ *este o algebră booleană.*

(ii) $(\{true, false\}, or, and, not, false, true)$ *este o algebră booleană (se obţine din exemplul precedent pentru* X *o mulţime cu un singur element).*

Observaţia II.5.2.4. *Orice algebră booleană este şi inel boolean şi reciproc: dacă* $(B, \vee, \wedge, (-)', 0, 1)$ *e algebră booleană, atunci* $x + y = (x \wedge y') \vee (x' \wedge y)$ *şi* $x \cdot y = x \wedge y$ *determină* $(B, +, \cdot)$ *inel boolean (*$+$ *este echivalentul diferenţei simetrice sau* XOR*); reciproc, dacă* $(B, +, \cdot)$ *este inel boolean, atunci* $x \vee y = x + y + x \cdot y$ *şi* $x \wedge y = x \cdot y$ *conduc la o algebra booleană cu* $x' = 1 - x$.

Teorema II.5.2.5. *(M. Stone) Fie* B *o algebră booleană finită. Atunci există o mulţime* X *astfel încât* $B \cong \mathcal{P}(X)$ *(izomorfism de algebre Boole: bijecţie care păstrează* $\vee$, $\wedge$, 0, 1 *(rezultă că păstrează şi* $(-)'$ *)).*