

# Curs 7

## II.3 Grupuri

### II.3.1 Definiție. Exemple

**Definiția II.3.1.1.** *Un grup  $G$  este o mulțime, împreună cu o operație binară pe  $G$ , notată  $\cdot : G \times G \rightarrow G$ ,  $(x, y) \rightarrow x \cdot y$ , 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)  $(\mathbb{Z}, +)$  și  $(\mathbb{Z}_n, +)$  sunt grupuri abeliene.*

*(ii)  $(\mathbb{Z}, \cdot)$  și  $(\mathbb{Z}_n, \cdot)$  sunt doar monoizi. Dar pentru orice monoid  $M$ , mulțimea 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 observații: 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  $(3, 47) = 1$ , obținut 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, obținem

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

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,  $U(\mathcal{M}_n(\mathbb{R})) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det A \neq 0\}$  (și se notează de obicei cu  $GL_n$ , grupul general liniar de ordin  $n$ ).

(iv) Fie  $X$  o mulțime și  $(X^X, \circ)$  monoidul funcțiilor definite pe  $X$  cu valori tot în mulțimea  $X$ . Atunci  $U(X^X) = \{f : X \rightarrow X \mid f \text{ bijectivă}\}$ . Acest grup se mai notează și cu  $S_X$ . Reamintim că o funcție bijectivă se mai numește și permutare. Avem deci  $(S_X, \circ, \mathbf{1}_X)$  grupul permutărilor mulțimii  $X$  (grup necomutativ dacă  $|X| > 2$ ). Dacă  $X$  este finită,  $|X| = n$ , atunci  $S_X$  se mai notează și  $S_n$  și  $|S_n| = n!$ .

Cazul  $n = 3$ : putem considera  $X = \{1, 2, 3\}$ ; vom reprezenta o funcție bijectivă  $f : X \rightarrow X$  printr-un tabel  $\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$ . Se obține 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  $\mathbf{1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ ,  $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$  și  $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ , atunci avem:  $f^2 = g^3 = \mathbf{1}$ ,  $g^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ ,  $fg = g^2f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ,  $gf = fg^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ .

(v) Grupul diedral  $D_n$  (grupul simetriilor poligonului regulat cu  $n$  laturi). Vom prezenta doar cazul  $n = 4$ : considerăm un pătrat împărțit în 4 părți egale: 

2	1
3	4

. Asupra acestui pătrat vom efectua următoarele transformări:

- *rotații 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 față de axele de simetrie:*

$$S_{\uparrow} : \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 4 & 3 \\ \hline \end{array}, S_{-} : \begin{array}{|c|c|} \hline 3 & 4 \\ \hline 2 & 1 \\ \hline \end{array}, S_{/} : \begin{array}{|c|c|} \hline 4 & 1 \\ \hline 3 & 2 \\ \hline \end{array}, S_{\setminus} : \begin{array}{|c|c|} \hline 2 & 3 \\ \hline 1 & 4 \\ \hline \end{array}$$

Fie  $\mathcal{D}_4 = \{R_0, R_{90}, R_{180}, R_{270}, S_{\uparrow}, S_{-}, S_{/}, S_{\setminus}\}$ . Atunci mulțimea  $\mathcal{D}_4$  este închisă la operația de compunere a funcțiilor (exercițiu: scrieți tabla!). De exemplu,  $R_{90} \circ S_{\uparrow} = S_{\setminus}$ ,  $S_{\uparrow} \circ R_{90} = S_{/}$ . Cum operația de compunere a transformărilor (funcțiilor) este asociativă și fiecare transformare este inversabilă (de exemplu, fiecare simetrie este propria sa inversă), rezultă că  $\mathcal{D}_4$  este un grup necomutativ cu elementul neutru  $R_0$ .

**Definiția II.3.1.3.** O submulțime  $H$  a unui grup  $G$  se numește subgrup dacă:

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

(SG2)  $e \in H$

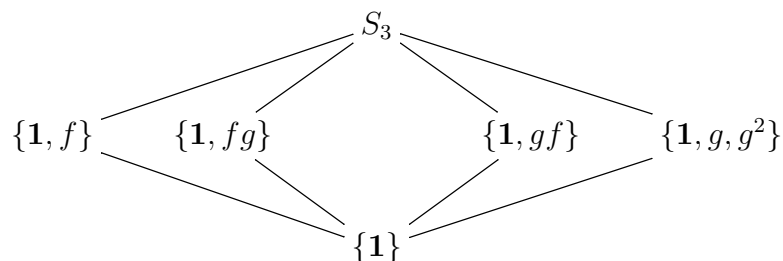
(SG3)  $(\forall)x \in H \Rightarrow x^{-1} \in H$

(condiția (SG2) nu e necesară; rezultă din (SG1) și (SG3)).

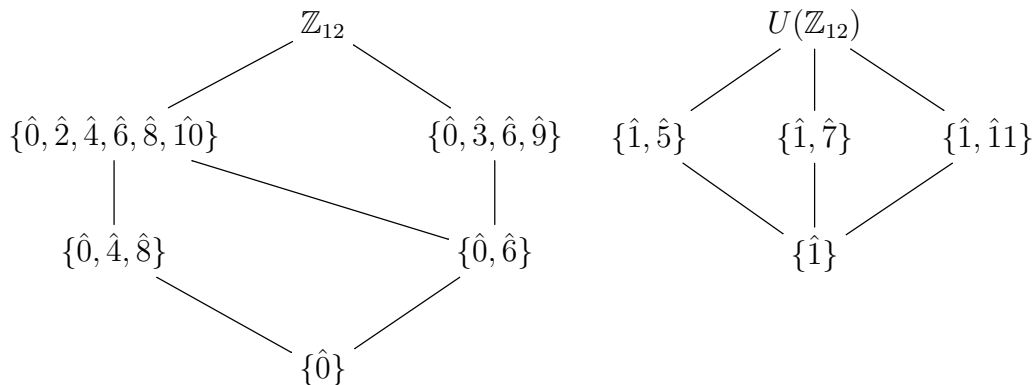
În particular, orice subgrup  $H$  este grup cu operația indusă, cu același element neutru.

**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  $(\mathbb{Z}_{12}, +)$  și  $(U(\mathbb{Z}_{12}), \cdot)$  (unde  $U(\mathbb{Z}_{12}) = \{\hat{1}, \hat{5}, \hat{7}, \hat{11}\}$ ):



Ordinul unui grup  $G$  este numărul de elemente al mulțimii  $G$  (posibil  $\infty$ ). Ordinul unui element  $x \in G$  este cel mai mic număr natural  $n$  astfel încât  $x^n = e$  (sau  $\infty$  dacă nu există asemenea  $n$ ). Dacă  $x \in G$ , atunci  $\langle x \rangle = \{e, x, x^2, x^3, \dots\}$  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 și  $H \subseteq G$  un subgrup. Atunci  $|H| \mid |G|$ .

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

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

**Aplicație:** test parțial pentru detectarea numerelor prime:

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

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

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

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

- (i) Se fac publice următoarele elemente: un număr prim mare  $p$  și un număr  $g$  primitiv modulo  $p$  (adică mulțimea resturilor modulo  $p$  ale numerelor  $g, g^2, \dots, g^{p-1}$  coincide cu  $\{1, 2, 3, \dots, p-1\}$ ).
- (ii) Utilizatorii Alice și Bob doresc să stabilească o cheie secretă.
- (iii) Alice alege o valoare aleatoare  $x \in \mathbb{Z}_p$ , calculează  $a \equiv g^x \pmod{p}$  și trimite rezultatul lui Bob pe canalul public.
- (iv) Analog Bob alege  $y \in \mathbb{Z}_p$ , calculează  $b \equiv g^y \pmod{p}$  și trimite rezultatul lui Alice.
- (v) Alice calculează  $b^x \equiv (g^y)^x \equiv (g^x)^y \equiv a^y \pmod{p}$ .
- (vi) Bob obține același rezultat.
- (vii)  $K = b^x = a^y$  este cheia privată care o vor utiliza în viitor.

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

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

pentru a descoperi cheia privată  $k = a^y = b^x$ . În practică, acest 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  $a \equiv g^x \pmod{p}$ ,  $a = 3$  și o trimite lui Bob.
- Bob calculează cheia sa publică  $b \equiv g^y \pmod{p}$ ,  $b = 2$  și o trimite lui Alice.
- Alice calculează  $K \equiv b^x \pmod{p}$ ,  $K = 2$
- Bob calculează  $k \equiv a^y \pmod{p}$ ,  $K = 2$

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

## II.4 Inele. Corpuri

### II.4.1 Definiție. Exemple

**Definiția II.4.1.1.** *Un inel  $R$  este o mulțime, împreună cu două operații binare, notate  $+$  :  $R \times R \rightarrow R$ ,  $\cdot$  :  $R \times R \rightarrow R$ , astfel încât:*

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

(R2)  $(R, \cdot)$  este monoid.

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

Proprietăți 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 operația  $\cdot$ .

**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 și 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 și 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 operația aditivă - adunarea pe componente. Pentru operația 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 operația multiplicativă prin:

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

și extindem prin liniaritate la toate elementele lui  $\mathbb{H}$ . Se obține 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  $\mathbb{k}$  este comutativ și există  $p, n \in \mathbb{N}$  cu  $p$  prim astfel încât  $|\mathbb{k}| = p^n$ . Mai mult, oricare două corpuri finite cu același număr de elemente sunt izomorfe (izomorfism de corpuri: bijecție care păstrează cele două operații, elementele simetrizabile și inversabilitatea în raport cu operațiile).

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

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

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

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

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

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

Pentru adunarea și multiplicarea modulo  $P$ , avem de exemplu

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

și

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

**Exercițiul II.4.1.5.** Scrieți tabla înmulțirii în  $(\mathbb{Z}_2)^3$  folosind corespondența de mai sus și verificați că orice string diferit de 000 este inversabil.

Fie acum  $\mathbb{k}$  un corp și  $\mathbb{k}[X] = \{a_0 + a_1X + \dots + a_nX^n \mid a_0, a_1, a_n \in \mathbb{k}, n \in \mathbb{N}\}$  inelul polinoamelor cu coeficienți în  $\mathbb{k}$ .

**Proprietăți:**

- (i)  $\mathbb{k}[X]$  inel integru.
- (ii) (Teorema împărțirii cu rest)  $(\forall)P, Q \in \mathbb{k}[X], Q \neq 0$ , există în mod unic două polinoame  $C, R \in \mathbb{k}[X]$ , astfel încât  $\text{grad}R < \text{grad}Q$  și  $P = Q \cdot C + R$ .
- (iii) (Teorema lui Bezout) Fie  $P \in \mathbb{k}[X]$ ,  $a \in \mathbb{k}$ . Atunci  $P(a) = 0 \Leftrightarrow X - a \mid P$ .
- (iv)  $P \in \mathbb{k}[X]$ ,  $\text{grad}P = n \implies P$  are cel mult  $n$  rădăcini.

**Consecința II.4.1.6.** Orice funcție  $f : \mathbb{k} \rightarrow \mathbb{k}$ , unde  $\mathbb{k}$  este un corp finit, este polinomială (soluție: polinomul de interpolare Lagrange).

## II.4.2 Aplicație în criptografie. Secret Sharing

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

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

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

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

<sup>1</sup>A. Shamir, 1979.



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

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

și

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