2. Exemple de grupuri

2.1. **Produs direct de grupuri.** [1]

Teorema 2.1. *Fie* $(G_i, \cdot)$*,* $i \in I$*, o familie de grupuri. Pe mulţimea produs cartezian*

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I} \mid \forall i \in I, g_i \in G_i\}$$

definim operaţia $\cdot$ *dată de*

$$(g_i)_{i \in I}(h_i)_{i \in I} = (g_i h_i)_{i \in I}.$$

Atunci

(1) $(\prod_{i \in I} G_i, \cdot)$ *este un grup;*
(2) *pentru fiecare* $k \in I$*, proiecţia canonică*

$$p_k : \prod_{i \in I} G_i \to G_k,\ p_k((g_i)_{i \in I}) = g_k,$$

este un morfism de grupuri surjectiv;
(3) $(\prod_{i \in I} G_i, \cdot)$ *este comutativ dacă şi numai dacă* $\forall i \in I$ *grupul* G_i *este comutativ.*

Demonstraţie.

□

Definiţia 2.2. Grupul construit în teorema anterioară se numeşte *produsul direct al familiei de grupuri* $(G_i)_{i \in I}$.

Notaţia 2.3. Dacă $I = \{1, 2, \ldots, n\}$, atunci notăm

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n.$$

Exemplul 2.4. 1) Dacă $I = \{1, 2\}$, atunci

[1] 29 februarie 2020

- $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$;
- $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$;
- $p_1 : G_1 \times G_2 \to G_1$, $p_1(g_1, g_2) = g_1$.

2) Dacă $G_1 = G_2 = (\mathbb{Z}_2, +)$, atunci grupul $G_1 \times G_2$ este un grup cu 4 elemente.

$G_1 \times G_2 = \ldots$

Tabla operaţiei este:

Definiţia 2.5. Un grup $K = \{e, a, b, c\}$ izomorf cu $(\mathbb{Z}_2 \times Z_2, \cdot)$ se numeşte *grupul lui Klein.*

2.2. **Grupuri generate de o mulţime.**

Definiţia 2.6. Fie $(G, \cdot)$ un grup şi $S \subseteq G$. Spunem că G este *generat de* S dacă orice element din G este un produs de elemente din S sau inverse de elemente din S. Dacă G este generat de S, atunci spunem că S este o *mulţime de generatori* pentru G.

Notaţia 2.7. 1) Notăm $G = \langle S \rangle$ dacă G este generat de submulţimea $S \subseteq G$.

2) Dacă $S = \{x_1, \ldots, x_n\}$, notăm $G = \langle x_1, \ldots, x_n \rangle$.

Definiţia 2.8. Spunem că grupul G este *ciclic* dacă există $x \in G$ astfel încât $G = \langle x \rangle$. In aceste condiţii vom spune că x este un *generator* pentru G.

Observaţia 2.9. Grupul $(G, +)$ este ciclic, generat de x dacă şi numai dacă $G = \{x^n \in n \in \mathbb{Z}\}$.

Exemplul 2.10. 1) $(\mathbb{Q}^*_+, \cdot)$ este generat de mulţimea

$$X = \{p \in \mathbb{N} \mid p \text{ este prim}\}.$$

2) $(\mathbb{Z}, +)$:

- $\mathbb{Z}$ este ciclic, generat de 1, deci $\mathbb{Z} = \langle 1 \rangle$;
- Dacă $m, n \in \mathbb{Z}^*$ sunt relativ prime, atunci $\mathbb{Z} = \langle m, n \rangle$.

3) $(\mathbb{Q}, +)$:

$$\mathbb{Q} = \left\langle \{\frac{1}{n} \mid n \in \mathbb{N}^*\} \right\rangle = \left\langle \{\frac{1}{p^\alpha} \mid p \text{ este prim şi } \alpha \in \mathbb{N}\} \right\rangle$$

4) $\mathbb{Z}_n = \langle \widehat{1} \rangle$.

Definiţia 2.11. Fie G un grup, $S \subseteq G$ şi R o mulţime de posibile egalităţi între elemente obţinute prin operarea cu elemente din S. Spunem că S este *prezentat* de mulţimea de generatori S împreună cu relaţiile S dacă $G = \langle S \rangle$, elementele lui S satisfac relaţiile din R şi toate celelalte relaţii care au loc în G pot fi deduse folosindu-le pe cele din R.

Notaţia 2.12. Notăm $G = \langle S \mid R \rangle$ faptul că G este prezentat de mulţimea S şi de relaţiile R.

Exemplul 2.13. 1) $\mathbb{Z} = \langle a \mid \varnothing \rangle$.

2) Dacă G este un grup ciclic de ordin n, atunci $G = \{1, g, g^2, \ldots, g^{n-1}\} = \langle g \mid g^n = 1 \rangle$.

3) Grupul lui Klein este prezentat ca

$$K = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle.$$

- $a^2 = 1 \Rightarrow a = a^{-1}$ şi $b^2 = 1 \Rightarrow b = b^{-1}$;
- $(ab)^2 = 1 \Rightarrow ab = ba$;
- orice produs de a, b, a^{-1}, b^{-1} va fi de forma $a^k b^j$, $k, j \in \{1, 2\}$;
- $K = \{1, a, b, ab\}$ şi se constată că tabla operaţiei este chiar tabla grupului lui Klein.

4) Grupul $\langle a, b \mid a^3 = b^3 = (ab)^3 = 1 \rangle$ este infinit pentru că elementul ab^2 are ordinul infinit.

2.3. **Grupuri diedrale.**

Definiţia 2.14. Fie $P = A_1A_2\dots A_n$ ($n \geq 3$) un poligon regulat cu n-laturi. Notăm cu O centrul de simetrie al lui P. Prin *simetrie* a poligonului P înţelegem o transformare a lui P în P realizată prin unul din următoarele moduri:

a) o rotaţie în jurul centrului de simetrie;
b) o simetrie faţă de o axă de simetrie a lui P.

Exemplul 2.15.

Teorema 2.16. *Fie P un poligon regulat cu n laturi. Atunci:*

(1) *mulţimea simetriilor lui P este, în raport cu compunerea funcţiilor, un grup cu $2n$ elemente.*
(2) *orice simetrie poate fi obţinută ca o compunere de rotaţii cu $\frac{2\pi}{n}$ şi simetrii în raport cu axa de simetrie care trece prin A_1.*

Definiţia 2.17. Grupul simetriilor unui poligon regulat cu n laturi se numeşte *grupul diedral* de grad n şi se notează cu D_n.

Teorema 2.18. *Fie P un poligon regulat cu n laturi. Notăm cu*

- *r rotaţia cu $\frac{2\pi}{n}$ înjurul centrului de simetrie a lui P şi*
- *s simetria faţă de axa de simetrie care trece prin A_1.*

Atunci

(1) $D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ rs = sr^{n-1}\rangle$;
(2) *pentru orice* $k \in \{0, \dots, n-1\}$ *avem* $r^k s = sr^{n-k}$.
(3)

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\} = \{1, r, r^2, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$$

are $2n$ *elemente;*

Observaţia 2.19. In grupul diedral D_n avem $\mathrm{ord}(r) = n$ şi $\mathrm{ord}(s) = \mathrm{ord}(sr) = \dots = \mathrm{ord}(sr^{n-1}) = 2$.

Exemplul 2.20. 1) n=3

2) n=4

Exerciţiul 2.21. Construţi tabla operaţiei pentru D_6.

Grupul cuaternionilor. Fie $Q = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Pe această mulţime definim o operaţie de înmulţire care respectă următoarele reguli:

- $\forall x \in Q$, $1 \cdot x = x$;

- are loc regula semnelor;
- $i^2 = j^2 = k^2 = -1$;
- $ij = k$, $jk = i$, $ki = j$;
- $ji = -k$, $kj = -i$, $ik = -j$.

In acest mod se obţine un grup, numit *grupul cuaternionilor*.

Observaţia 2.22. Din tabla operaţiei putem deduce toate proprietăţie necesare, cu excepţia asociativităţii. Pentru demonstrarea asociativităţii vom identifica un model, i.e. o mulţime şi operaţie despre care ştim deja că este asociativă şi care furnizează aceeaşi tabla a operaţiei.

In $(GL_2(\mathbb{C}), \cdot)$ considerăm matricile:

$$I_2, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Atunci $\mathfrak{Q} = \{\pm I_2, \pm I, \pm J, \pm K\}$ împreună cu înmulţirea matricilor este un grup care are aceeaşi tablă a operaţiei ca şi Q, deci $(Q, \cdot)$ este un grup izomorf cu $(\mathfrak{Q}, \cdot)$.

2.4. **Grupul permutărilor unei mulţimi.** Fie X o mulţime. Notăm cu

$$\mathcal{F}(X) = X^X = \{f : X \to X \mid f \text{ este funcţie}\}.$$

Atunci $(X^X, \circ)$ este un monoid. Elementele inversabile în acest monoid sunt

$$S_X = U(X^X) = \{f : X \to X \mid f \text{ este funcţie bijectivă}\}.$$

Rezultă că $(S_X, \circ)$ este un grup.

Definiţia 2.23. 1) Grupul $(S_X, \circ)$ se numeşte *grupul permutărilor mulţimii* X sau *grupul simetric asociat lui* X.

2) Dacă $X = \{1, \dots, n\}$, atunci notăm $S(X) = S_n$ şi grupul permutărilor mulţimii X se numeşte *grupul permutărilor de grad* n .

Observaţia 2.24. $|S_n| = n!$.

Teorema 2.25. *Fie X şi Y mulţimi. Următoarele afirmaţii sunt echivalente:*

(1) *X şi Y au acelaşi cardinal (i.e. există o funcţie bijectivă $\alpha : X \to Y$;*
(2) *grupurile $(S_X, \circ)$ şi $(S_Y, \circ)$ sunt izomorfe.*

Demonstraţie. (1)$\Rightarrow$(2)

□

Observaţia 2.26. Demonstraţia pentru (2)⇒(1) necesită cunoştinte suplimentare.

Notaţia 2.27. **(reprezentarea permutărilor de grad n)** Fie $n \geq 1$ un număr natural. Atunci permutările $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ din S_n vor fi reprezentate ca

$$\sigma = \begin{pmatrix} 1 & \ldots & i & \ldots & n \\ \sigma(1) & \ldots & \sigma(i) & \ldots & \sigma(n) \end{pmatrix}.$$

Observaţia 2.28. (Compunerea pernutărilor)

Dacă

$$\sigma = \begin{pmatrix} 1 & \ldots & i & \ldots & n \\ \sigma(1) & \ldots & \sigma(i) & \ldots & \sigma(n) \end{pmatrix}$$

şi

$$\tau = \begin{pmatrix} 1 & \ldots & i & \ldots & n \\ \tau(1) & \ldots & \tau(i) & \ldots & \tau(n) \end{pmatrix}$$

atunci

$$\sigma\tau \overset{not}{=} \sigma \circ \tau = \begin{pmatrix} 1 & \ldots & i & \ldots & n \\ \sigma\tau(1) & \ldots & \sigma\tau(i) & \ldots & \sigma\tau(n) \end{pmatrix}.$$

Exemplul 2.29.

Definiţia 2.30. Spunem că o permutare $\sigma \in S_n$ este un *ciclu de lungime* k dacă există $a_1, \ldots, a_k \in \{1, \ldots, n\}$ astfel încât

- $\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$ şi
- $\forall i \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$ avem $\sigma(i) = i$.

Un ciclu de lungime 2 se numeşte *transpoziţie*.

Notaţia 2.31. Notăm cu $(a_1, \ldots, a_k)$ ciclul descris în definiţia anterioară.

Observaţia 2.32.

$$(a_1, \ldots, a_k) = (a_2, \ldots, a_k, a_1) = (a_3, \ldots, a_k, a_1, a_2) = \cdots.$$

Exemplul 2.33.

Definiţia 2.34. Spunem că două cicluri $(a_1, \dots, a_k)$ şi $(b_1, \dots, b_\ell)$ din S_n sunt *disjuncte* dacă $\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_\ell\} = \varnothing$.

Propoziţia 2.35. *Fie $n \in \mathbb{N}^*$ şi $\gamma, \delta \in S_n$. Sunt adevărate afirmaţiile:*
(i) *Dacă γ este un ciclu de lungime k, atunci* $\operatorname{ord}(\gamma) = k$.
(ii) *Dacă γ şi δ sunt cicluri disjuncte, atunci $\gamma\delta = \delta\gamma$.*
(iii) *Orice ciclu este un produs de transpoziţii, mai precis:*

$$(a_1, \dots, a_k) = (a_k, a_{k-1})(a_{k-1}, a_{k-1}) \dots (a_2, a_1).$$

Teorema 2.36. *Orice permutare se descompune intr-un produs de cicluri disjuncte. Mai mult, dacă facem abstracţie de ordinea factorilor, această descompunere este unică.*

Procedura de descompunere a unei permutări $\sigma \in S_n$ este următoarea:
(1) Alegem cel mai mic $i \in \{1, \dots, n\}$ astfel încât $\sigma(i) \neq i$ şi construim ciclul $\gamma_1 = (i, \sigma(i), \sigma^2(i), \dots)$.
(2) Descompunem $\sigma = \gamma_1\sigma_1$, unde

$$\sigma_1(j) = \begin{cases} \sigma(j), & \text{dacă } j \notin \{i, \sigma(i), \sigma^2(i), \dots\} \\ j, & \text{dacă } j \in \{i, \sigma(i), \sigma^2(i), \dots\}. \end{cases}$$

(3) Se repetă paşii (1) şi (2) pentru σ_1 şi se obţine o permutare σ_2 ş.a.m.d.

Exemplul 2.37.

Observaţia 2.38. Putem folosi descompunerea unei permutări în produs de cicluri disjuncte ca să calculăm ordinul permutării.

Mai precis, dacă $\sigma = \gamma_1 \dots \gamma_\ell$ este descopunerea lui σ în produs de cicluri disjuncte şi k_u reprezintă lungimea ciclului γ_u, atunci

$$\operatorname{ord}(\sigma) = [k_1, \dots, k_\ell].$$

Corolarul 2.39. *Orice permutare este un produs de transpoziţii.*

Observaţia 2.40. Descompunerea în produs de transpoziţii nu este unică.

Definiţia 2.41. Fie $\sigma \in S_n$. Spunem că o pereche (i, j) cu $1 \leq i < j \leq n$ determină o *inversiune* pentru σ dacă $\sigma(i) > \sigma(j)$. Notăm cu $Inv(\sigma)$ numărul inversiunilor lui σ. Numărul $\epsilon(\sigma) = (-1)^{Inv(\sigma)}$ s.n. *signatura* permutării σ.

Propoziţia 2.42. *a) Dacă $\sigma \in S_n$, atunci $\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$.*
b) $\epsilon : S_n \to \{1, -1\}$ este un morfism de grupuri.

Corolarul 2.43. *Fie $\sigma \in S_n$.*

(i) *Dacă $\sigma = \tau_1\tau_2 \dots \tau_k$, atunci $\epsilon(\sigma) = (-1)^k$.*

(ii) *Dacă se consideră două (sau mai multe) descompuneri ale unei permutări σ în ale lui produse de transpoziţii*

$$\sigma = \tau_1 \dots \tau_k = \rho_1 \dots \rho_\ell,$$

atunci numerele k şi ℓ au aceeaşi paritate.

2.5. **Teorema lui Cayley.**

Definiţia 2.44. Spunem că grupul G *se scufundă în* grupul H dacă există un morfism injectiv $G \to H$.

Teorema 2.45. (Teorema lui Cayley) *Orice grup se scufundă într-un grup de permutări.*

Demonstraţie.

$\square$

Exemplul 2.46.

2.6. **O aplicaţie: 15-puzzle.**