Revista MateInfo.Ro ISSN 2065 - 6432 octombrie 2009

GRUPURI

probleme propuse cu indicații şi răspunsuri

Grupuri numerice

1. Într–un grup aditiv G notăm $nx = x + x + \ldots + x$ (n termeni), pentru $n \in \mathbb{N}^*$, $x \in G$. Să se arate că în grupul $(\mathbb{Z}, +)$ ecuația $nx = a$ nu ar e totdeaunae soluție ($n \in \mathbb{N}^*$, $a \in \mathbb{Z}$), pe când în grupul $(\mathbb{Q}, +)$ aceeaşi ecuație cu $a \in \mathbb{Q}$ are totdeauna soluție

2. Să se arate că în grupul $(\mathbb{Z}, +)$ ecuația $2x = 0$ are o singură soluție, pe când în grupul $(\mathbb{Q}^*, \cdot)$ ecuația $x^2 = 1$ are două soluții..

3. Se consideră mulțimea $G = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a^2 - 3b^2 = 1\}$ şi operația $(a, b)*(c, d) = (ac + 3bd, ad + bc)$. Să se arate că $(G, *)$ este grup abelian infinit.

4. Se consideră mulțimea $G = \{a + b\sqrt{37} \mid a, b \in \mathbb{Q}, a^2 - 37b^2 = 1\}$. Să se demonstreze că mulțimea G este infinită.

5. Fie $\mathbb{Q}$ grupul aditiv al numerelor raționale şi pentru orice $n \in \mathbb{N}^*$, $H_n = \left\{\frac{m}{n!} \,\middle|\, m \in \mathbb{Z}\right\}$. Să se arate că :

a) $H_n \subset H_{n+1}$.

b) $\bigcup_{n\geq 1} H_n = \mathbb{Q}$.

6. Fie mulțimea $Q_0 = \left\{\frac{m}{n} \,\middle|\, m, n \in \mathbb{Z}, m \text{ şi } n \text{ sunt impare}\right\}$ şi $G = Q_0 \times \mathbb{Z}$. Pe G se defineşte legea de compoziție

$$(q_1, k_1) * (q_2, k_2) = (q_1q_2, k_1 + k_2), \forall q_1, q_2 \in Q_0, \forall k_1, k_2 \in \mathbb{Z}.$$

a) Să se arate că $(G, *)$ este un grup abelian.

b) Să se calculeze $(1, 1)*(1, 2)* \ldots *(1, n)$, n $\mathbb{N}^*$.

7. Fie G un grup cu cel puțin trei elemente şi e elementul neutru. Spunem că G are proprietatea “ p” dacă $\forall x, y \in G - \{e\}$ $\exists z$ (care depinde de x şi y) astfel încât $xy = z^2$. Să se arate că grupul $(\mathbb{R}_+^*, \cdot)$ are proprietatea « p », dar grupul $(\mathbb{R}^*, \cdot)$ nu are această proprietate.

8. Să se arate că există $z \in \mathbb{C}$ astfel încât $|z| = 1$, dar $z^n \neq 1$, oricare ar fi $n \in \mathbb{N}^*$.

Grupuri de matrice

9. Se consideră mulțimea $P = \{A \in M_2(\mathbb{R}) \mid AA^t = I_2\}$, unde A^t este transpusa matricei A. Să se arate că înmulțirea matricelor determină pe mulțimea P o structură de grup necomutativ.

10. Se consideră mulțimea $G = \left\{ X = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a, b \in \mathbb{R}, a > 0 \right\}$.

a) Să se găsească două matrice $C, D \in G$ pentru care $CD \neq DC$.

b) Să se arate că dacă $A \in G$, atunci $I_2 - A + A^2 \in G$.

11. Se consideră matricea $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ şi mulțimea $M = \{X \in M_2(\mathbb{R}) \mid AX = XA\}$.

a) Să se arate că $G = \{X \in M \mid \det X \neq 0\}$ este grup în raport cu înmulțirea matricelor.

b) Să se rezolve în G ecuația $X^2 = I_2$.

12. Se consideră matricele $U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $V = \begin{pmatrix} \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{pmatrix}$, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ şi mulțimea

$G = \{I_2, V, V^2, U, VU, V^2U\}$.

a) Să se verifice că $U^2 = V^3 = I_2$.

b) Să se arate că $(G, .)$ este un grup necomutativ.

13. Se consideră matricele $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $C = A \cdot B$ şi mulțimea
$G = \{X \in M_2(\mathbb{C}) \mid \det(X) = 1\}$.

a) Să se verifice că $A^4 = B^6 = I_2$.

b) Să se arate că $(G, \cdot)$ este grup.

c) Să se demonstreze că $C^n \neq I_2$, pentru orice $n \in \mathbb{N}^*$.

14. Să se arate că ecuația $X^2 = I_2$ are o infinitate de soluții în $M_2(\mathbb{Z})$.

15. Se consideră matricele $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ şi $B = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$, cu $t \in \mathbb{R}$.

a) Să se arate că dacă matricea $X \in M_2(\mathbb{R})$ verifică relația $AX = XA$, atunci există $a, b \in \mathbb{R}$ astfel ca $X = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

b) Să se demonstreze că $B^n = \begin{pmatrix} \cos nt & -\sin nt \\ \sin nt & \cos nt \end{pmatrix}$, pentru orice $n \in \mathbb{N}^*$.

c) Să se rezolve în mulțimea $M_2(\mathbb{R})$ ecuația $X^2 = A$.

16. Se consideră mulțimea $G = \left\{ \begin{pmatrix} x & iy \\ iy & x \end{pmatrix} \middle| x, y \in \mathbb{R}, x^2 + y^2 \neq 0 \right\}$. Să se arate că $(G, \cdot)$ este grup abelian.

17. În mulțimea $M_2(\mathbb{C})$ se consideră submulțimea $H = \left\{ A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \middle| z, w \in \mathbb{C}, |z| + |w| > 0 \right\}$. Să se arate că H este un grup necomutativ în raport cu înmulțirea obişnuită a matricelor.

18. Fie mulțimea

$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\}$.

Să se arate că G împreună cu înmulțirea matricelor este un grup necomutativ.

19. Se consideră matricele $A = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ şi $M_x = \frac{x}{3} A + \frac{1}{3x^2} B$, $x \in \mathbb{R}^*$.

a) Să se calculeze produsul AB.

b) Să se arate că $M_x M_y = M_{xy}$, $\forall x, y \in \mathbb{R}^*$.

c) Să se arate că $\det(M_x) \neq 0$, $\forall x \in \mathbb{R}^*$.

20. În mulțimea $M_2(\mathbb{R})$ se consideră submulțimea $G = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z}, a^2 - 2b^2 = 1 \right\}$. Să se arate că mulțimea G conține o infinitate de elemente.

Grupuri de permutări

21. Să se calculeze :

a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$; b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$; c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^2$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}^3$;

d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}^{100}$; e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 6 & 4 & 7 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 7 & 4 & 5 & 6 \end{pmatrix}^{-1}$.

22. Considerăm că ordinea inițială a literelor este cea alfabetică. Să se determine număul de inversiuni din cuvintele:

a) logaritm ; b) algoritm.

23. Să se arate că orice transpoziție are un număr impar de inversiuni.

27. Fie $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ și $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Să se arate că $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

28. Fie permutările $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\beta =$,$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, elemente ale grupului $(S_4, \cdot)$.

a) Să se verifice că γ este soluție a ecuației $\alpha x = x\beta$.

b) Să se arate că $\alpha^4 = \beta^4$.

c) Să se determine o soluție a ecuației $x\beta^3 = \alpha^3 x$ în S_4.

29. Fie permutarea $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in S_5$ și mulțimea $A = \{\sigma^n \mid n \in \mathbb{N}^*\}$.

a) Să se determine numărul inversiunilor lui σ.

b) Să se determine numărul elementelor mulțimii A.

c) Fie $\tau \in S_5$ astfel încât $\tau\sigma^2 = \sigma^2\tau$. Să se arate că $\tau\sigma = \sigma\tau$.

30. Fie $\sigma \in S_n$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix}$. Să se determine cel mai mic număr natural k astfel încât $\sigma^k = e$, unde e este permutarea identică.

31. Se dau permutările $\sigma, \tau \in S_9$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 8 & 9 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 9 & 5 & 6 & 7 & 8 \end{pmatrix}$. Să se găsească cel mai mic număr natural n astfel încât $(\tau\sigma)^n = e$, unde e este permutarea identică.

32. Dacă $\sigma \in S_n$, notăm cu $m(\sigma)$ numărul inversiunilor permutării σ. Să se demonstreze egalitatea:

$$\sum_{\sigma \in S_n} m(\sigma) = n! \, \frac{C_n^2}{2} .$$

33. Să se arate că pentru orice $k \in \mathbb{N}$, $0 \le k \le C_n^2$, există în S_n o permutare care are exact k inversiuni

34. (*Grupul altern A_n*). Mulțimea permutărilor pare de grad n este grup față de compunerea permutărilor.

$$\mathbb{Z}_n$$

35. Se defineşte şirul lui *Fibonacci* astfel : $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$, dacă $n \in \mathbb{N}$, $n \ge 2$. Săse arate că

a) dacă n se divide cu 4, atunci a_n se divide cu 3 ;

b) dacă n se divide cu 5, atunci a_n se divide cu 5 ;

c) dacă n se divide cu 8, atunci a_n se divide cu 7.

36. Se consideră mulțimea $G = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_3 \right\}$.

a) Să se determine numărul elementelor mulțimii G.

b) Să se arate că $AB \in G$, pentru orice $A, B \in G$.

c) Să se determine numărul matricelor din mulțimea G care au determinantul nul.

37. Se consideră mulțimile $H = \{a^2 \mid a \in \mathbb{Z}_7\}$ şi $G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_7, a \ne \hat{0} \text{ sau } b \ne \hat{0} \right\}$

a) Să se determine elementele mulțimii H.

b) Fie $x, y \in H$ astfel încât $x + y = \hat{0}$. Să se arate că $x = y = \hat{0}$.

c) Să se arate că G este grup abelian în raport cu operația de înmulțire a matricelor.

38. Fie $I_2 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$, $T = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$ şi $S = \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$ matrice cu elemente din $\mathbb{Z}_2$.

a) Să se arate că $T^3 = S^2 = I_2$.

b) $G = \{I_2, T, T^2, S, ST, ST^2\}$ este un grup necomutativ în raport cu înmulțirea matricelor.

39. (*Grupul diedral D_n*). Fie $A = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}$ şi $B = \begin{pmatrix} \widehat{-1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}$ matrice din $M_2(\mathbb{Z}_n)$.

a) Să se verifice că $A^n = B^2 = I_2$.

b) Să se arate că $D_{2n} = \{I_2, A, A^2, \ldots, A^{n-1}, B, AB, A^2B, \ldots, A^{n-1}B\}$ împreună cu operația obişnuită de înmulțire a matricelor este un grup necomutativ

40. Să se demonstreze teorema lui *Wilson* : Dacă p este un număr prim, atunci $(p - 1)! + 1$ se divide cu p.

41. Să se demonstreze teorema lui *Fermat* : Dacă p este un număr prim şi $a \in \mathbb{Z}$, atunci $a^p - a$ se divide cu p. ∗

42. Să se arate că $2^{32} + 1$ se divide cu 641.

Indicații şi răspunsuri

Grupuri numerice

1. Ecuația $2x = 1$ nu are soluții în $\mathbb{Z}$.

2. $S = \{0\}$; $S = \{-1, 1\}$.

3. Elementul neutru este $(1, 0)$, simetricul lui (a, b) este $(a, -b)$. Din $(2, 1) \in G$ şi $\underbrace{(2,1) * \dots * (2,1)}_{n\ factori} \neq (1, 0)$, ($n \in \mathbb{N}$), rezultă că G este mulțime infinită.

4. Se demonstrează că G înzestrat cu înmulțirea obişnuită a numerelor reale este un grup abelian. El conține elementul $73 + 12\sqrt{37}$, deci şi toate puterile lui naturale, aşadar G este mulțime infinită.

5. a) $\dfrac{m}{n!} = \dfrac{m(n+1)}{(n+1)!} \in H_{n+1}$. b) $\dfrac{m}{n} = \dfrac{m(n-1)!}{n!} \in H_n$.

6. a) Produsul a două numere impare este un număr impar, deci legea de compoziție este bine definită.Se verifică simplu asociativitatea şi comutativitatea operației, elemental neutru este $(1, 0)$, simetricul elementului (q, k) este elementul $\left(\frac{1}{q}, -k\right)$. b) $(1, 1)*(1, 2)* \dots *(1, n) = \left(1, \frac{n(n+1)}{2}\right)$, $n \in \mathbb{N}^*$.

7. În grupul $(\mathbb{R}_+^*, \cdot)$ putem să extragem rădăcina pătrată, pe când în grupul $(\mathbb{R}^*, \cdot)$ acest lucru nu este posibil: este suficient să luăm $x = 1$, $y = -1$.

8. $|z| = 1 \Leftrightarrow z = \cos \alpha + i\sin \alpha$, $\alpha \in \{0, 2\pi)$; $z^n = 1 \Leftrightarrow z = \cos \dfrac{2k\pi}{n} + i \sin \dfrac{2k\pi}{n}$, $n \in \mathbb{N}^*$, $0 \le k \le n-1$. Este suficient să luăm α astfel încât $\dfrac{\alpha}{\pi} \notin \mathbb{Q}$, de exemplu $\alpha = \pi^2$.

Grupuri de matrice

9. $AA^t = BB^t = I_2 \Rightarrow AB(AB)^t = A(BB^t)A^t = AI_2A^t = I_2$, deci înmulțirea este lege de compoziție internă pe P. Elementul neutru este $I_2 \in P$, matricele din P sunt inversabile, deoarece $\det(AA^t) = (\det A)^2 = 1 \neq 0$, inversa unei matrice din P este o matrice din P : $AA^t = I_2 \Rightarrow A^t = A^{-1} \Rightarrow A^{-1}(A^{-1})^t = A^{-1}(A^t)^t = A^{-1}A = I_2$.

10. a) $C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $D = \begin{pmatrix} 2 & -3 \\ 0 & 1 \end{pmatrix}$, $CD = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}$, $DC = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$; b) $I_2 - A + A^2 = \begin{pmatrix} 1-a+a^2 & ab \\ 0 & 1 \end{pmatrix} \in G$, deoarece $1 - a + a^2 > 0$, $\forall a \in \mathbb{R}$.

11. a) $X, Y \in M \Rightarrow XY \in M$: $AXY = (AX)Y = X(AY) = XYA$. Elementele mulțimii G sunt de forma $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$, $a, b \in \mathbb{R}$, $a \neq 0$. Elementul neutru este $I_2 \in G$, matricea inversă $X^{-1} = \begin{pmatrix} \frac{1}{a} & 0 \\ \frac{-b}{a^2} & \frac{1}{a} \end{pmatrix} \in G$.

b) $X^2 = I_2$, $X \in G \Rightarrow X = \pm I_2$.

12. calcul direct.

13. a) $A^2 = B^3 = -I_2$, deci $A^4 = B^6 = I_2$;

c) Se demonstrează prin inducție egalitatea $C^n = \begin{pmatrix} (-1)^n & (-1)^{n-1}n \\ 0 & (-1)^n \end{pmatrix}$, deci $C^n \neq I_2$, $\forall n \in \mathbb{N}^*$.

14. $X = \begin{pmatrix} a & 1+a \\ 1-a & -a \end{pmatrix}$, $a \in \mathbb{Z}$.

15. a) calcul direct; b) inducție după n ; c) $X = \pm\frac{\sqrt{2}}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

16. $\begin{pmatrix} x & iy \\ iy & x \end{pmatrix}\begin{pmatrix} z & it \\ it & z \end{pmatrix} = \begin{pmatrix} xz-yt & i(xt+yz) \\ i(xt+yz) & xz-yt \end{pmatrix}$, $(xz- yt)^2 + (xt + yz)^2 = (x^2 + y^2)(z^2 + t^2)$.

17. $A = \begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix}$, $B = \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} \Rightarrow AB = \begin{pmatrix} z_1z_2 - w_1\overline{w_2} & z_1w_2 + w_1\overline{z_2} \\ -\overline{z_1}\overline{w_2} - \overline{w_1}z_2 & \overline{z_1}\overline{z_2} - \overline{w_1}w_2 \end{pmatrix}$; $\det(AB) = \det(A)\det(B) = 0 \Rightarrow$
$\Rightarrow \det(A) = 0$ sau $\det(B) = 0$.Dar $\det(A) = 0 \Leftrightarrow z = w = 0$. Rezultă că produsul a două matrice din H este o matrice din H. Avem şi $A^{-1} = \frac{1}{\det(A)}\begin{pmatrix} \bar{z} & -w \\ \bar{w} & z \end{pmatrix} \in$ H. Grupul H este necomutativ: $A = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \Rightarrow AB \neq BA$.

18. Produsul a două matrice din G este o matrice din G, înmulțirea matricelor este asociativă în $M_2(\mathbb{C})$, deci şi în G, elementul neutru este $I_2 \in G$, inversa oricărei matrice din G este o matrice din G (verificare !).

19. a) $AB = O_3$. b) calcul direct. c) $M_xM_{\frac{1}{x}} = I_3 \Rightarrow \det(M_x) \neq 0$.

20. Mulțimea G este un grup abelian cu înmulțirea obişnuită a matricelor şi conține toate puterile naturale ale matricei $\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$, care sunt distincte, deci G este infinită.

Grupuri de permutări

21. a) $\begin{pmatrix} 1\,2\,3\,4 \\ 3\,1\,2\,4 \end{pmatrix}$; b) $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,5\,1\,2\,4 \end{pmatrix}$; c) $\begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix}$; $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix}$; d) $\sigma^3 = e \Rightarrow \sigma^{100} = \sigma^{99}\sigma = \sigma$;

e) $\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 4\,2\,6\,7\,1\,3\,5 \end{pmatrix}$.

22. a) logaritm $\rightarrow \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 4\,6\,2\,1\,7\,3\,8\,5 \end{pmatrix}$ are 11 inversiuni; b) algoritm $\rightarrow \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 1\,4\,2\,6\,7\,3\,8\,5 \end{pmatrix}$ are 7 inversiuni .

23. Fie $\tau_{kl} \in S_n$, $k < l$, transpoziția $\tau_{kl}(i) = \begin{cases} l. \text{ dacă } i = k, \\ k, \text{dacă } i = l, \\ i, \text{dacă } i \neq k \text{ şi } i \neq l. \end{cases}$ Atunci $m(\tau_{kl}) = 2(l-k) - 1$.

28. a) $\alpha\gamma = \gamma\beta = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,2\,3 \end{pmatrix}$; b) $\alpha^4 = \beta^4 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix} = e$; c) $\alpha(x\beta^3)\beta = \alpha(\alpha^3x)\beta \Rightarrow \alpha x\beta^4 = \alpha^4x\beta \Rightarrow \alpha x = x\beta$.

Putem lua $x = \gamma$.

29. a) $m(\sigma) = 4$; b) $A = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = e\}$ are 5 elemente; c) $\tau\sigma^2 = \sigma^2\tau \Rightarrow \tau\sigma^4 = \sigma^2\tau\sigma^2 = \sigma^2\sigma^2\tau = \sigma^4\tau \Rightarrow$
$\Rightarrow \sigma(\tau\sigma^4)\sigma = \sigma(\sigma^4\tau)\sigma \Rightarrow \sigma\tau = \tau\sigma$.

30. $\sigma^m = \begin{pmatrix} 1 & 2 & \dots & n-m & n-m+1 & \dots & n \\ m+1 & m+2 & \dots & n & 1 & \dots & m \end{pmatrix}$, $1 \leq m \leq n-1$, deci n este k minim cu proprietatea cerută.

31. $\tau\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,3\,4\,5\,9\,1\,6\,7\,8 \end{pmatrix}$, $(\tau\sigma)^2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 3\,4\,5\,9\,8\,2\,1\,6\,7 \end{pmatrix}$, $(\tau\sigma)^3 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 4\,5\,9\,8\,7\,3\,2\,1\,6 \end{pmatrix}$, $(\tau\sigma)^4 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 5\,9\,8\,7\,6\,4\,3\,2\,1 \end{pmatrix}$,

$(\tau\sigma)^5 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 9\,8\,7\,6\,1\,5\,4\,3\,2 \end{pmatrix}$, $(\tau\sigma)^6 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 8\,7\,6\,1\,2\,9\,5\,4\,3 \end{pmatrix}$, $(\tau\sigma)^7 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 7\,6\,1\,2\,3\,8\,9\,5\,4 \end{pmatrix}$, $(\tau\sigma)^8 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 6\,1\,2\,3\,4\,7\,8\,9\,5 \end{pmatrix}$,

$(\tau\sigma)^9 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 1\,2\,3\,4\,5\,6\,7\,8\,9 \end{pmatrix} = e$.

32. Fie $\sigma \in S_n$ o permutare oarecare şi $\widetilde{\sigma} = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(n) & \sigma(n-1) & \dots & \sigma(1) \end{pmatrix}$ permutarea obținută prin scrierea îin ordine inversă a elementelor din linia de jos. Orice pereche de indici (i, j) este inversiune în exact una dina ceste două permutări. Rezultă că numărul de inversiuni din cele două permutări este egal cu numărul perechilor de indici, deci este C_n^2 .Deoarece permutările din S_n pot fi distribuite în $\dfrac{n!}{2}$ submulțimi de tipul $\{\sigma, \widetilde{\sigma}\}$ şi numărul de inversiuni dintr-o astfel de submulțime este egal cu C_n^2 , se obține egalitatea din enunț.

33. O transpoziție (i, j) se numeşte *adiacentă* dacă $j = i + 1$. O transpoziție adiacentă compusă cu o permutare îi schimbă acesteia numărul de inversiuni cu o unitate. Prin transpoziții adiacente plecând de la permutarea identică (0 inversiuni), se obține permutarea $\begin{pmatrix} 1 & 2 & \dots n \\ n & n-1 & \dots 1 \end{pmatrix}$, care are numărul maxim de inversiuni. Este clar acum că la un anumit pas se obține o permutare cu k inversiuni.

34. Fie $\varepsilon : S_n \to \{-1, 1\}$, definită prin $\varepsilon(\sigma) = (-1)^{m(\sigma)}$. Atunci $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$, deci compunerea a două permutări pare este o permutare pară, permutarea identică este pară, inversa unei permutări pare este pară. Prin compunerea cu o transpoziție se schimbă paritatea unei permutări, astfel că există tot atâtea permutări pare câte sunt impare. Rezultă că numărul permutărilor pare este egal cu $\dfrac{n!}{2}$.

$\mathbb{Z}_n$

35. a) Şirul corespunzător în $\mathbb{Z}_3$ este periodic cu perioada principală 8 : $\hat{0}, \hat{1}, \hat{1}, \hat{2}, \hat{0}, \hat{2}, \hat{2}, \hat{1}, \hat{0}, \hat{1}, \ldots$, dar $\widehat{a_4} = \hat{0}$.

b) Şirul corespunzător în $\mathbb{Z}_5$ este periodic cu perioada principală 20 :
$\hat{0}, \hat{1}, \hat{1}, \hat{2}, \hat{3}, \hat{0}, \hat{3}, \hat{3}, \hat{1}, \hat{4}, \hat{0}, \hat{4}, \hat{4}, \hat{3}, \hat{2}, \hat{0}, \hat{2}, \hat{2}, \hat{4}, \hat{1}, \hat{0}, \hat{1}, \hat{1}, \ldots$ dar $\widehat{a_5} = \widehat{a_{10}} = \widehat{a_{15}} = \hat{0}$.

c) Şirul corespunzător în $\mathbb{Z}_7$ este periodic cu perioada principală 16 :

$\hat{0}, \hat{1}, \hat{1}, \hat{2}, \hat{3}, \hat{5}, \hat{1}, \hat{6}, \hat{0}, \hat{6}, \hat{6}, \hat{5}, \hat{4}, \hat{2}, \hat{6}, \hat{1}, \hat{0}, \hat{1}, \ldots$ dar $\widehat{a_8} = \hat{0}$.

36. a) G are $3\cdot 3 = 9$ elemente. b) Suma şi produsul a două elemente din $\mathbb{Z}_3$ este un element din $\mathbb{Z}_3$. c) $a^2 = b^2 =$

$= \hat{0} \Rightarrow a = b = \hat{0}$; $a^2 = b^2 = \hat{1} \Rightarrow a, b \in \{\hat{1}, \hat{2}\}$; $a^2 = b^2 = \hat{2}$, imposibil. Rezultă că sunt 5 matrice în G care au determinantul nul.

37. a) $H = \{\hat{0}, \hat{1}, \hat{2}, \hat{4}\}$;b) verificare cu tabla adunării; c) $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$, unde $c = (\det A)^{-1}\cdot a$,
$d = -(\det A)^{-1}\cdot d$.

39. a) $A^k = \begin{pmatrix} \hat{1} & \hat{k} \\ \hat{0} & \hat{1} \end{pmatrix}$; b) $BA = A^{n-1}B$, deci produsul a două matrice din D_n este o matrice din D_n . Avem $(A^k)^{-1} = A^{n-k}$ şi

$(A^kB)^{-1} = B^{-1}A^{n-k} = BA^{n-k} = A^{n-1}BA^{n-k-1} = \ldots = A^{(n-k)(n-1)}B = A^kB$.

40. Se calculează produsul elementelor din grupul abelian $\mathbb{Z}_p^*$, înmulțind fiecare factor cu inversul său. Dacă $x = x^{-1}$, $x \in \mathbb{Z}_p^*$, atunci $x^2 = \hat{1}$, deci $x = \hat{1}$ sau $x = -\hat{1}$. Rezultă $\hat{1}\cdot\hat{2}\cdot\hat{3}\cdot\ldots\widehat{p-1} = \hat{1}\cdot\widehat{(-1)} = -\hat{1}$.

41. Fie $a \in \mathbb{Z}_p^*$ şi $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ definită prin $f(x) = ax$. Funcţia f este injectivă, deci este şi surjectivă, deoarece $\mathbb{Z}_p^*$ este mulţime finită. Rezultă $\mathbb{Z}_p^* = \{x_1, x_2, \ldots, x_{p-1}\} = \{ax_1, ax_2, \ldots, ax_{p-1}\}$, deci $ax_1 \cdot ax_2 \cdot \ldots \cdot ax_{p-1} = a^{p-1}x_1x_2 \ldots x_{p-1} = x_1x_2 \ldots x_{p-1}$, de unde $a^{p-1} = \hat{1}$, aşadar $a^p = a$. Dacă $a = \hat{0} \in \mathbb{Z}_p$, atunci egalitatea $a^p = a$ este evident adevărată. Luând acum $a \in \mathbb{Z}$, se obţine $\hat{a}^p = \hat{a} \in \mathbb{Z}_p$, deci $a^p - a$ se divide cu p.

42. Numărul $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$ este prim, deci $(\mathbb{Z}_{641}^*, \cdot)$ este grup abelian. Avem $\widehat{2^7} \cdot \hat{5} = -\hat{1}$, deci $\left(\widehat{2^7} \cdot \hat{5}\right)^4 = \left(-\hat{1}\right)^4 = \hat{1}$, de unde $\widehat{2^{28}} \cdot \widehat{5^4} = \widehat{2^{28}} \cdot \left(-\widehat{2^4}\right) = -\widehat{2^{32}} = \hat{1}$.

Prof. Corneliu Mănescu-Avram