Coordonator
DANA HEUBERGER

Dana Heuberger Vasile Pop

MATEMATICĂ DE EXCELENŢĂ

pentru concursuri, olimpiade şi centre de excelenţă

Clasa a XII-a

Volumul I: ALGEBRĂ

Ediţia a II-a, revizuită

ÎNVĂŢARE DE EXCELENŢĂ®
supersucces

PARALELA 45
EDITURA

CUPRINS

TESTE INIȚIALE

TESTUL I.1

I.1.1. Fie $n\in\mathbb{N}$ și $A\in\mathcal{M}_{2n+1}(\mathbb{R})$, $A\neq O_{2n+1}$. Arătați că dacă există matricea $B\in\mathcal{M}_{2n+1}(\mathbb{R})$ inversabilă, astfel încât $A\cdot B+B\cdot A=O_{2n+1}$, atunci funcția $f:\mathbb{R}\to\mathbb{R}$, $f(x)=\det(x\cdot I_{2n+1}-A)$ este impară.

I.1.2. Arătați că nu există matrice $A,B,C\in\mathcal{M}_3(\mathbb{R})$, astfel încât

$$A\cdot B=B\cdot C=C\cdot A=\begin{pmatrix}1&2&3\\4&5&6\\7&8&10\end{pmatrix}.$$

I.1.3. Arătați că pentru orice $n\geq 3$ există o permutare σ a mulțimii $\{1,2,\ldots,n\}$, astfel încât pentru orice i,j,k, $1\leq i<j<k\leq n$ să avem $\sigma(i)+\sigma(k)\neq 2\sigma(j)$.

Vasile Pop,
Concursul „Argument”, ediția I, 2009

I.1.4. Fie $A\in\mathcal{M}_2(\mathbb{C})$, astfel încât există $n\in\mathbb{N}^*$ pentru care $\operatorname{tr}\left(A^n\right)=\operatorname{tr}\left(A^{n+1}\right)=0$.

Arătați că $A^2=O_2$.

Sorin Rădulescu, Mihai Piticari,
Concursul „Arhimede” 2006

TESTUL I.2

I.2.1. Pentru $a\in\mathbb{R}$ considerăm matricea $X_a=\begin{pmatrix}a&1\\-1&a\end{pmatrix}$ și notăm:

$$(X_a)^n=\begin{pmatrix}a_n&b_n\\-b_n&a_n\end{pmatrix},\ n\in\mathbb{N}^*.$$

Arătați că există $a\in\mathbb{R}$ pentru care $b_1<a_1, b_2<a_2,\ldots,b_{2009}<a_{2009}$ și $b_{2010}>a_{2010}$.

Vasile Pop

I.2.2. Fie $A\in\mathcal{M}_n(\mathbb{C})$, astfel încât $A^{2013}=A^{2015}$, unde $n\in\mathbb{N}^*$. Demonstrați că matricea $B=A^3-14\cdot A^2+56\cdot A-64\cdot I_n$ este inversabilă.

Dana Heuberger

I.2.3. Arătați că există o matrice $A\in\mathcal{M}_n(\mathbb{R})$ cu proprietatea că toți minorii săi, de orice ordin, sunt numere iraționale strict pozitive.

Ion Savu,
Concursul „Nicolae Păun" 2006

I.2.4. a) Arătați că există $X,Y\in\mathcal{M}_2(\mathbb{R})$, astfel încât $\det(XY+YX)>0$ și $\det\left(X^2+Y^2\right)<0$.

b) Arătați că pentru orice $X,Y\in\mathcal{M}_2(\mathbb{R})$, astfel încât $\det(XY+YX)\le 0$ avem $\det\left(X^2+Y^2\right)\ge 0$.

Vasile Pop,
Concursul „Argument" 2013

SOLUȚIILE TESTELOR INIȚIALE

TESTUL I.1

R.I.1.1. Din $AB=-BA$ rezultă că $A=-BAB^{-1}$. Pentru orice $x\in\mathbb{R}$, avem:
$f(-x)=\det(-x\cdot I_{2n+1}-A)=-\det(x\cdot I_{2n+1}+A)=-\det\left(xB\cdot B^{-1}-BAB^{-1}\right)=$
$=-\det\left(B\cdot(x\cdot I_{2n+1}-A)\cdot B^{-1}\right)=-\det(B)\cdot\det(x\cdot I_{2n+1}-A)\cdot\det\left(B^{-1}\right)=$
$=-\det\left(B\cdot B^{-1}\right)\cdot\det(x\cdot I_{2n+1}-A)=-\det(x\cdot I_{2n+1}-A)=-f(x)$, deci f este impară.

R.I.1.2. Presupunând că există matrice ca în enunț, trecând la determinanți obținem $\det(A\cdot B)=\det(B\cdot C)=\det(C\cdot A)=-3$. Prin înmulțirea acestor relații rezultă:
$\det\left(A^2\right)\cdot\det\left(B^2\right)\cdot\det\left(C^2\right)=-27$, adică $\left(\det(A)\cdot\det(B)\cdot\det(C)\right)^2=-27$, fals.

R.I.1.3. Demonstrăm mai întâi afirmația pentru numere de forma 2^p, prin inducție după $p\ge 2$. Pentru $p=2$, avem permutarea $\sigma_2=\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}$.

Dacă $\sigma_{2^p}=\begin{pmatrix}1&2&\dots&2^p\\ \sigma_1&\sigma_2&\dots&\sigma_{2^p}\end{pmatrix}$, atunci definim

$$\sigma_{2^{p+1}}=\begin{pmatrix}1&2&\dots&2^p&2^p+1&2^{p+2}&\dots&2^{p+1}\\ 2\sigma_1-1&2\sigma_2-1&\dots&2\sigma_{2^p}-1&2\sigma_1&2\sigma_2&\dots&2\sigma_{2^p}\end{pmatrix}.$$

Avem: $2\sigma_i-1+2\sigma_k-1=2(2\sigma_j-1)\Leftrightarrow\sigma_i+\sigma_k=2\sigma_j$, fals.

$2\sigma_i + 2\sigma_k = 2\cdot 2\sigma_j \Leftrightarrow \sigma_i + \sigma_k = 2\sigma_j$, fals

şi $2\sigma_i - 1 + 2\sigma_k \neq 2(2\sigma_j - 1)$ şi $2\sigma_i - 1 + 2\sigma_k \neq 2\cdot 2\sigma_j$.

Aşadar $\sigma_{2^{p+1}}$ are proprietatea din enunţ.

Pentru n între 2^{p-1} şi 2^p, folosim permutarea $\sigma_{2^p} = \begin{pmatrix} 1 & 2 & \dots & 2^p \\ \sigma_1 & \sigma_2 & \dots & \sigma_{2^p} \end{pmatrix}$ şi formăm permutarea $\sigma_n = \begin{pmatrix} 1 & 2 & \dots & n \\ x_1 & x_2 & \dots & x_n \end{pmatrix}$ în care $x_1, x_2, \dots, x_n$ sunt numerele $1, 2, \dots, n$ alese în ordinea în care apar în σ_{2^p}.

R.I.1.4. Pentru $k \in \mathbb{N}$ notăm $t_k = \operatorname{tr}(A^k)$. Fie $\Delta = \det(A)$.

Din relaţia Cayley–Hamilton obţinem că $\forall\, k \in \mathbb{N}$, $A^{k+2} - t_1 \cdot A^{k+1} + \Delta \cdot A^k = O_2$.

Calculând urmele matricelor din egalitatea precedentă, rezultă că

$$\forall\, k \in \mathbb{N},\ t_{k+2} - t_1 \cdot t_{k+1} + \Delta \cdot t_k = 0 \qquad (1)$$

Din relaţia (1) obţinem prin inducţie că $\forall\, k \in \mathbb{N},\ k \geq n,\ t_k = 0$. (2)

Din relaţia Cayley–Hamilton avem $A^{2n} - t_n \cdot A^n + \Delta^n \cdot I_2 = O_2$, deci $A^{2n} = -\Delta^n \cdot I_2$.

Dacă $\Delta \neq 0$, obţinem că $t_{2n} = -2\Delta^n \neq 0$, contradicţie cu (2).

Aşadar $\Delta = 0$, deci $A^{2n} = O_2$. Rezultă că $A^2 = O_2$. (Este o proprietate cunoscută.)

TESTUL I.2

R.I.2.1. Avem $X_a = \sqrt{1+a^2} \cdot \begin{pmatrix} \frac{a}{\sqrt{1+a^2}} & \frac{1}{\sqrt{1+a^2}} \\ \frac{-1}{\sqrt{1+a^2}} & \frac{a}{\sqrt{1+a^2}} \end{pmatrix} = \sqrt{1+a^2} \cdot \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$, unde

$t \in [0, 2\pi)$ este astfel încât $\cos t = \frac{a}{\sqrt{1+a^2}}$, $\sin t = \frac{1}{\sqrt{1+a^2}}$.

Atunci, $X_a^n = \sqrt{1+a^2}^n \cdot \begin{pmatrix} \cos nt & \sin nt \\ -\sin nt & \cos nt \end{pmatrix}$ şi condiţiile din problemă devin:

$\cos(k\cdot t) > \sin(k\cdot t)$, $k = \overline{1, 2009}$ şi $\cos(2010\cdot t) < \sin(2010\cdot t)$.

Alegem $t \in [0, 2\pi)$ astfel ca $2009\cdot t < \frac{\pi}{4}$ şi $2010\cdot t > \frac{\pi}{4}$, deci $t \in \left(\frac{\pi}{4\cdot 2010}, \frac{\pi}{4\cdot 2009}\right)$

De exemplu, luăm $t = \frac{\pi}{8038}$ şi relaţiile anterioare sunt verificate.

Avem $\cos t, \sin t \in (0,1)$ şi căutăm o soluţie $a>0$.

$$\frac{a^2}{1+a^2}=\cos^2 t \Leftrightarrow a^2\left(1-\cos^2 t\right)=\cos^2 t \Leftrightarrow a^2=\operatorname{ctg}^2 t \overset{a>0}{\Leftrightarrow} a=\operatorname{ctg} t.$$

Această valoare pentru a verifică inegalităţile din problemă.

R.I.2.2. Fie polinomul $f(X)=X^{2013}\left(X^2-1\right)$. Notăm cu m_A polinomul minimal şi cu p_A polinomul caracteristic al matricei A. Deoarece $f(A)=O_n$, rezultă că $m_A \mid f$. Atunci m_A şi p_A au aceiaşi factori ireductibili, care aparţin mulţimii $\{X, X-1, X+1\}$ şi, în consecinţă, există $\alpha, \beta, \gamma \in \mathbb{N}$, cu $\alpha+\beta+\gamma=n$, astfel încât

$$\forall x \in \mathbb{C},\ p_A(x)=x^{\alpha}\cdot(x-1)^{\beta}\cdot(x+1)^{\gamma}=\det\left(x\cdot I_n-A\right).$$

Atunci $p_A\left(2^k\right)=\det\left(2^k\cdot I_n-A\right)\neq 0,\ \forall k\in\mathbb{N}^*$.

Deoarece $B=A^3-14A^2+56A-64I_n=-(2I_n-A)(4I_n-A)(8I_n-A)$ rezultă că $\det(B)=(-1)^n\cdot p_A\left(2^1\right)\cdot p_A\left(2^2\right)\cdot p_A\left(2^3\right)\neq 0$, deci matricea B este inversabilă.

R.I.2.3. Pentru orice $n\in\mathbb{N},\ n\geq 2$, vom construi o matrice $B_n\in\mathcal{M}_n(\mathbb{Z})$ care are toţi minorii strict pozitivi. Rezultă că matricea $A_n=\sqrt[n]{2}\cdot B_n$ este o soluţie a problemei.

Pentru $n=2$, alegem matricea $A_2=\begin{pmatrix}2 & 1\\ 3 & 4\end{pmatrix}$.

Presupunem că pentru $k\in\mathbb{N},\ k\geq 2$ am construit matricea $A_k\in\mathcal{M}_k(\mathbb{Z})$ cu proprietatea din enunţ.

Alegem matricea $B_{k+1}\in\mathcal{M}_{k+1}(\mathbb{R})$, $B_{k+1}=\begin{pmatrix} & & x\\ & B_k & x^3\\ & & \vdots\\ x & x^3 & \ldots\ x^{3^k}\end{pmatrix}$.

Arătăm că există $x\in\mathbb{R}$ astfel încât toţi minorii lui B_{k+1} să fie strict pozitivi. Dacă alegem un minor al lui B_k, atunci acesta este strict pozitiv. Dacă alegem un minor care conţine elemente ale ultimei linii şi / sau ale ultimei coloane, atunci acesta este o funcţie polinomială de grad impar cu coeficienţi reali şi cu coeficientul dominant strict pozitiv. Limita acestui minor când x tinde spre $+\infty$ este egală cu $+\infty$. În consecinţă, există $a_k\in\mathbb{R}$, astfel încât pentru orice $x\in(a_k,+\infty)$ minorul respectiv este strict pozitiv. Alegând M cea mai mare dintre constantele $a_k\in\mathbb{R}$ care apar pentru fiecare dintre minorii lui B_{k+1} care conţin şi puteri ale lui x, obţinem că pentru orice $x>M$, matricea B_{k+1} are toţi minorii strict pozitivi. Din primul principiu de inducţie rezultă concluzia.

R.I.2.4. a) Fie matricele $X=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ şi $Y=\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$.

Avem $\det(XY+YX)=20>0$ şi $\det\left(X^2+Y^2\right)=-12<0$.

b) Ştim că

$$\forall\, M,N\in\mathcal{M}_2(\mathbb{C}),\ \det(M+N)+\det(M-N)=2\left(\det(M)+\det(N)\right) \qquad (1)$$

Presupunem că $\det\left(X^2+Y^2\right)<0$.

Avem: $0\le\left(\det(X+Y)\right)^2=\det\left((X+Y)^2\right)=\det\left(X^2+Y^2+XY+YX\right)$ şi

$$0\le\left(\det(X-Y)\right)^2=\det\left((X-Y)^2\right)=\det\left(X^2+Y^2-(XY+YX)\right).$$

Notând cu $M=X^2+Y^2$, $N=XY+YX$ şi adunând egalităţile precedente, obţinem:

$0\le\det(M+N)+\det(M-N)\overset{(1)}{=}2\left(\det(M)+\det(N)\right)<0$, fals.

Aşadar $\det\left(X^2+Y^2\right)\ge 0$.

CAPITOLUL 1. ORDINUL UNUI ELEMENT AL UNUI GRUP

Conceptul modern de grup abstract s-a dezvoltat începând cu secolul al XIX-lea, pornind de la cercetările matematicianului francez Évariste Galois, care a dat un criteriu pentru existența soluțiilor unei anume ecuații polinomiale în termeni de grup de simetrie al rădăcinilor polinomului. Elementele grupului lui Galois corespund unor anumite permutări ale rădăcinilor polinomului. Noțiunile legate de grupuri și de structurile algebrice s-au îmbogățit datorită aplicabilității lor în domenii dintre cele mai variate, atât matematice, cât și nematematice (în teoria relativității restrânse din fizică, în fenomene de simetrie din chimia moleculară, în teoria numerelor, în geometria clasică, în cea hiperbolică și în cea proiectivă, printre altele) și au ajuns să ajute la dezvoltarea domeniilor respective. Aceasta, datorită faptului că o organizare coerentă a proprietăților unor legi de compoziție interne (operații algebrice), fără să ținem seama de caracteristicile specifice ale operațiilor și de natura concretă a mulțimilor pe care sunt definite, permite utilizarea lor într-o manieră flexibilă și evidențierea acelor proprietăți general valabile care le valorifică potențialul și particularitățile.

În teoria grupurilor, un rol important îl joacă ordinul unui element al unui grup și proprietățile pe care acesta le generează. Le vom evidenția în continuare pe cele mai importante.

Considerăm cunoscute noțiunile fundamentale studiate în liceu (grup, subgrup, morfisme de grupuri). În cele ce urmează, G este o mulțime nevidă, care are structură de grup în raport cu o lege de compoziție notată multiplicativ. Ordinul grupului G, notat cu $\operatorname{ord}(G)$ sau cu $|G|$, este egal cu numărul elementelor grupului G, dacă G are un număr finit de elemente și este egal cu $+\infty$, dacă G are o infinitate de elemente.

1.1. Propoziție. Fie $(G,\cdot)$ un grup și X o submulțime nevidă a sa.

Notăm $\langle X\rangle = \bigcap\{H \mid X \subseteq H, H \text{ subgrup al lui } G\}$.

Atunci, $(\langle X\rangle,\cdot)$ este un subgrup al lui G (numit *subgrupul generat* de mulțimea X).

1.2. Observație.

a) $\langle X\rangle$ este cel mai mic subgrup (în raport cu relația de ordine „$\subseteq$") al lui G, care conține mulțimea X.

b) $\langle X\rangle = \left\{\alpha \in G \mid \exists n \in \mathbb{N}^*, \exists x_1, x_2, \ldots, x_n \in X, \exists k_1, k_2, \ldots, k_n \in \mathbb{Z}, \alpha = x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}\right\}$,

adică subgrupul generat de X este mulțimea tuturor produselor finite de puteri întregi ale elementelor mulțimii.

c) Dacă $x \in G$, atunci subgrupul generat de elementul x este $\langle x\rangle = \left\{x^k \mid k \in \mathbb{Z}\right\}$.

1.3. Definiţie. Grupul $(G,\cdot)$ se numeşte *finit generat* dacă există $n\in\mathbb{N}^*$ şi $a_1,a_2,\ldots,a_n\in G$, astfel încât $\langle\{a_1,a_2,\ldots,a_n\}\rangle \overset{not}{=} \langle a_1,a_2,\ldots,a_n\rangle = G$.

În acest caz, elementele $a_1,a_2,\ldots,a_n$ se numesc *generatori* ai grupului G.

1.4. Exemplu. Mulţimea S_n e *generată* de mulţimea transpoziţiilor sale.

Adică, orice permutare din S_n este un produs finit de transpoziţii.

Deoarece $(i,j)=(1,i)(1,j)(1,i)$, $\forall\, i,j\in\{1,2,\ldots,n\}$ cu $i\neq j$, permutările din mulţimea $G_1=\{(1,2),(1,3),\ldots,(1,n)\}$ generează S_n. Spunem că mulţimea G_1 este un *sistem de generatori* pentru S_n.

Alte sisteme de generatori pentru S_n sunt:

$$G_2=\{(1,2),(2,3),\ldots,(n-1,n)\} \quad \text{şi} \quad G_3=\{(1,2),(1,2,\ldots,n)\}.$$

1.5. Definiţie. Grupul $(G,\cdot)$ se numeşte grup *ciclic* dacă există $x\in G$, astfel încât $\langle x\rangle = G$. În acest caz, elementul x se numeşte *generator* al grupului G.

1.6. Observaţie. Dacă $(G,\cdot)$ este un grup ciclic de ordinul n, $a\in G$, este un generator al grupului şi $k\in\mathbb{Z}$, atunci a^k este un generator al lui G dacă şi numai dacă $(n,k)=1$.

1.7. Exemplu. Generatorii grupului ciclic $(\mathbb{Z}_6,+)$ sunt $\hat{1}$ şi $\hat{5}$.

1.8. Observaţie. Orice grup ciclic este comutativ.

1.9. Exemple de grupuri ciclice: $(\mathbb{Z},+)$, $(\mathbb{Z}_n,+)$, $(\mathcal{U}_n,\cdot)$, unde $\mathcal{U}_n$ este grupul rădăcinilor de ordinul n ale unităţii.

1.10. Definiţie. Fie grupul $(G,\cdot)$, cu elementul neutru $e\in G$.

Elementul $x\in G$ este *de ordin finit* dacă există $m\in\mathbb{N}^*$, astfel încât $x^m=e$.

În acest caz, cel mai mic exponent $k\in\mathbb{N}^*$, astfel încât $x^k=e$ se numeşte *ordinul* elementului x.

Elementul $x\in G$ este *de ordin infinit* dacă x nu este de ordin finit, adică dacă

$$\forall\, m\in\mathbb{N}^*,\ x^m\neq e.$$

1.11. Notaţie. Ordinul elementului x al grupului $(G,\cdot)$ se notează cu $\text{ord}(x)$.

1.12. Exemplu. $\hat{3}$ are ordinul 4 în grupul $(\mathbb{Z}_{12},+)$, $\hat{3}$ are ordinul 6 în grupul $(\mathbb{Z}_7^*,\cdot)$, iar 3 are ordinul infinit în grupul $(\mathbb{Z},+)$.

1.13. Teoremă. Fie grupul $(G,\cdot)$ şi $x\in G$.

a) Dacă $\text{ord}(x)=n\in\mathbb{N}^*$, atunci elementele $e, x, \ldots, x^{n-1}$ sunt distincte două câte două şi $\forall\, k\in\mathbb{Z},\ x^k=x^{k(\text{mod } n)}$.

b) $\text{ord}(x)=+\infty \Leftrightarrow \forall\, k_1,k_2\in\mathbb{Z},\ k_1\neq k_2$, avem $x^{k_1}\neq x^{k_2}$.

1.14. Consecinţă. Fie grupul $(G,\cdot)$.

Dacă $x\in G$ şi $\text{ord}(x)=n\in\mathbb{N}^*$, atunci $\text{ord}(\langle x\rangle)=n$ şi $\langle x\rangle=\{e,x,\ldots,x^{n-1}\}$.

1.15. Exemplu. Fie $k\in\{2,\ldots,n\}$ şi ciclul de lungime k, $c=(i_1,i_2,\ldots,i_k)\in S_n$. Atunci, $\text{ord}(c)=k$.

1.16. Observaţie. Considerăm, formal, că orice punct fix al unei permutări reprezintă un ciclu de lungime 1 şi că acesta are ordinul 1. Cu această convenţie, pentru orice $\sigma\in S_n$ există $t\in\mathbb{N}^*$ şi ciclurile disjuncte $c_1,c_2,\ldots,c_t$, astfel încât $\sigma=c_1\cdot c_2\cdot\ldots\cdot c_t$ şi $\text{ord}(c_1)+\text{ord}(c_2)+\ldots+\text{ord}(c_t)=n$.

1.17. Observaţie. Ştim că permutarea $\sigma\in S_n$ se poate descompune în mod unic (făcând abstracţie de ordinea factorilor) într-un produs de cicluri disjuncte. Ordinul permutării σ este cel mai mic multiplu comun al ordinelor ciclurilor componente.

1.18. Exemplu. Fie $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&2&7&9&6&8&1&5&4\end{pmatrix}=(137)(2)(49)(568)$

$\text{ord}(137)+\text{ord}(2)+\text{ord}(49)+\text{ord}(568)=9$ şi $\text{ord}(\sigma)=[3,1,2,3]=6$.

1.19. Observaţie (Cauchy).

Pentru $k_1,k_2,\ldots,k_n\in\mathbb{N}$, determinăm numărul permutărilor din S_n care se pot descompune într-un produs de tipul $(k_1,k_2,\ldots,k_n)$, adică numărul acelor permutări care au k_1 cicluri de lungime 1, k_2 cicluri de lungime 2, ..., k_n cicluri de lungime n şi toate aceste cicluri să fie disjuncte. Procedăm astfel:

a) Scriem toate n-uplurile $(m_1,m_2,\ldots,m_n)$ cu $m_1,m_2,\ldots,m_n\in\mathbb{N}$, $m_1\le m_2\le\ldots\le m_n$ şi $m_1+m_2+\ldots+m_n=n$ (numite, formal, *partiţiile* lui n).

b) Calculăm $k_1=m_n-m_{n-1}$, $k_2=m_{n-1}-m_{n-2}$, ..., $k_{n-1}=m_2-m_1$, $k_n=m_1$ şi obţinem n-uplul $(k_1,k_2,\ldots,k_n)$. Deoarece avem $n=\sum_{i=1}^{n} i\cdot k_i$, în S_n vor exista permutări care să aibă *tipul de descompunere* $(k_1,k_2,\ldots,k_n)$.

Numărul tuturor permutărilor din S_n de tipul $(k_1,k_2,\ldots,k_n)$ este:

$$\frac{n!}{k_1!\cdot k_2!\cdot\ldots\cdot k_n!\cdot 1^{k_1}\cdot 2^{k_2}\cdot\ldots\cdot n^{k_n}}.$$

1.20. Exemplu. Pentru mulţimea S_4, partiţiile lui $n=4$ sunt:
$(0,0,0,4),(0,0,2,2),(0,0,1,3),(0,1,1,2),(1,1,1,1)$.
De exemplu, pentru $(m_1,m_2,m_3,m_4)=(0,0,2,2)$ obţinem:
$k_1=m_4-m_3=0$, $k_2=m_3-m_2=2$, $k_3=m_2-m_1=0$ şi $k_4=m_1=0$.
Tipul de descompunere este $(0,2,0,0)$, deci permutările trebuie să fie produsul a două transpoziţii disjuncte.
Permutările de acest tip sunt: $(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$.

1.21. Propoziţie. Fie grupul $(G,\cdot)$ cu n elemente şi $x\in G$. Atunci, $\text{ord}(x)\mid n$.

1.22. Propoziţie. Fie grupul $(G,\cdot)$.
Dacă $x\in G$, $\text{ord}(x)=m\in\mathbb{N}^*$ şi pentru $k\in\mathbb{Z}$ avem $x^k=e$, atunci $m\mid k$.

Demonstraţie: Conform teoremei împărţirii cu rest, $\exists!\, q,r\in\mathbb{Z}$, $0\le r<\text{ord}(x)$, astfel încât $k=\text{ord}(x)\cdot q+r$. Avem $x^m=e$ şi m este minim cu această proprietate.
Atunci, $e=x^k=x^{mq+r}=\left(x^m\right)^q\cdot x^r=x^r$.
Cum m este minim, obţinem $r=0$, deci $m\mid k$.

1.23. Propoziţie. Fie $(M,\cdot)$ un monoid cu elementul neutru $e\in M$ şi fie $p,q\in\mathbb{N}^*$ distincte. $a\in M$ este o soluţie comună a ecuaţiilor $x^p=e$ şi $x^q=e \Leftrightarrow a^{(p,q)}=e$.

Demonstraţie: „$\Rightarrow$” Fie $(p,q)=d$ şi $h,k\in\mathbb{Z}$, astfel încât $ph+qk=d$.
Avem: $a^{(p,q)}=a^d=a^{ph}\cdot a^{qk}=\left(a^p\right)^h\cdot\left(a^q\right)^k=e$.
Implicaţia „$\Leftarrow$” este evidentă.

1.24. Observaţie. Grupul finit $(G,\cdot)$ de ordinul $n\in\mathbb{N}^*$ este ciclic $\Leftrightarrow$ G are un element ordinul n.

1.25. Propoziţie. Orice două grupuri ciclice de acelaşi ordin sunt izomorfe.
Dacă G este un grup ciclic de ordinul n, atunci $(G,\cdot)\simeq(\mathbb{Z}_n,+)$.

1.26. Propoziţie. Orice subgrup al unui grup ciclic este ciclic.

Demonstraţie: Fie $(G,\cdot)$ un grup ciclic.
I. Dacă $\text{ord}(G)=+\infty$ şi $G=\langle a\rangle$, atunci grupul G este izomorf cu $(\mathbb{Z},+)$ (un izomorfism este $f:G\to\mathbb{Z}$, $f\left(a^k\right)=k$, $\forall\, k\in\mathbb{Z}$). Deoarece subgrupurile lui $\mathbb{Z}$ sunt de forma $n\mathbb{Z}=\langle n\rangle$, cu $n\in\mathbb{Z}$, rezultă că şi subgrupurile lui G sunt ciclice, pe baza următorului rezultat cunoscut:

Lemă. Dacă grupurile $(G,\cdot)$ şi $(G',\cdot)$ sunt izomorfe şi $f:G\to G'$ este un izomorfism, atunci: H este subgrup al lui $G \Leftrightarrow f(H)$ este subgrup al lui G'.

II. Dacă $\text{ord}(G)=n\in\mathbb{N}^*$ şi $G=\langle a\rangle$, subgrupurile improprii ale lui G fiind evident ciclice, alegem un subgrup propriu H al lui G, $H=\left\{a^{k_1},a^{k_2},...,a^{k_t}\right\}$, cu $k_1<k_2<...<k_t$ numere naturale nenule. Demonstrăm, prin inducţie după m, că $H=\left\langle a^{k_1}\right\rangle$, deci că $\forall\, m\in\{1,2,...,t\}$, $a^{k_m}\in\left\langle a^{k_1}\right\rangle$.

Pentru $m=2$, avem $a^{k_1},a^{k_2}\in H$. Cum H este un subgrup al lui G, obţinem $\left(a^{k_1}\right)^{-1}\cdot a^{k_2}\in H$, deci $a^{k_2-k_1}\in H$. Din $k_2-k_1<k_2$ rezultă $k_2-k_1=k_1$, deci $k_2=2\cdot k_1$ şi $a^{k_2}\in\left\langle a^{k_1}\right\rangle$.

Fie $s\in\{2,...,t\}$. Presupunem că avem $k_{s-1}=(s-1)\cdot k_1$ şi demonstrăm că şi $k_s=s\cdot k_1$.

Avem: $k_s-k_1>k_s-k_2>...>k_s-k_{s-1}$ şi $a^{k_s-k_1},a^{k_s-k_2},...,a^{k_s-k_{s-1}}\in H$, iar $k_s-k_1,k_s-k_2,...,k_s-k_{s-1}\in\{k_1,k_2,...,k_{s-1}\}$, deci $k_s-k_{s-1}=k_1$.

Folosind ipoteza de inducţie obţinem $k_s=s\cdot k_1$ şi $a^{k_s}=\left(a^{k_1}\right)^s\in\left\langle a^{k_1}\right\rangle$, aşadar H este ciclic, generat de a^{k_1}.

1.27. Propoziţie. Dacă $x,y\in G$, atunci

a) $\text{ord}(x)=\text{ord}\left(x^{-1}\right)$.

b) $\text{ord}(x\cdot y)=\text{ord}(y\cdot x)$.

Demonstraţie:

a) I. Dacă $\text{ord}(x)=n\in\mathbb{N}^*$, avem $x^n=e$ şi $\left(x^{-1}\right)^n=\left(x^n\right)^{-1}=e^{-1}=e$.

Fie $\text{ord}\left(x^{-1}\right)=k$. Din Propoziţia 1.22. rezultă $k\mid n$. Cum $e=\left(x^{-1}\right)^k=\left(x^k\right)^{-1}$, rezultă că $x^k=e$. Dar $\text{ord}(x)=n$, deci $n\mid k$. Aşadar $n=k$.

II. Dacă $\text{ord}(x)=+\infty$, să presupunem că $\text{ord}\left(x^{-1}\right)=k\in\mathbb{N}^*$. Atunci, din cazul anterior rezultă că $\text{ord}(x)=\text{ord}\left(x^{-1}\right)=k$, fals. Aşadar $\text{ord}\left(x^{-1}\right)=+\infty$.

b) I. Dacă $\text{ord}(x\cdot y)=k\in\mathbb{N}^*$, avem $(x\cdot y)^k=e\Leftrightarrow x\cdot(y\cdot x)^{k-1}\cdot y=e\Leftrightarrow$ $\Leftrightarrow(y\cdot x)^k\cdot y=y\Leftrightarrow(y\cdot x)^k=e$, aşadar $\text{ord}(y\cdot x)=k'\in\mathbb{N}^*$ şi $k'\mid k$.