Ordinul elementelor grupului $GL_n(\mathbb{Z})$

Adrian REISNER[1]

În *RecMat 2/2005*, **Gabriel Dospinescu** a propus problema

L94. *Fie $A \in \mathcal{M}_n(\mathbb{C})$ o matrice cu elemente întregi, inversabilă şi astfel încât mulţimea $\left\{A^k \mid k \in \mathbb{N}\right\}$ este finită. Să se demonstreze că această mulţime are cel mult 3^{n^2} elemente. Rămâne rezultatul adevărat dacă suprimăm condiţia ca elementele matricei să fie întregi?*

Soluţia autorului a fost publicată în numărul 2/2006 al revistei. Propunem în continuare o abordare oarecum diferită a problemei, care permite o mai bună privire asupra laticei subgrupurilor lui $GL_n(\mathbb{Z})$.

Notăm cu $GL_n(\mathbb{Z})$ mulţimea matricelor inversabile cu elemente întregi, pentru care inversa are tot elemente întregi. Evident că $M \in GL_n(\mathbb{Z})$ dacă şi numai dacă $M \in \mathcal{M}_n(Z)$ şi $\det M = \pm 1$. Dacă G este un subgrup finit al grupului $GL_n(\mathbb{Z})$, iar $p \geq 3$ este prim, considerăm aplicaţia $\varphi : G \to GL_n(\mathbb{Z})$, care asociază unei matrice $M \in G$ acea matrice care are ca elemente redusele modulo p ale elementelor lui M.

Propoziţie. *Aplicaţia φ este un monomorfism de grupuri.*

Demonstraţie. Se observă uşor că φ este bine definită, în sensul că $\varphi(M)$ este matrice inversabilă în $\mathcal{M}_n(\mathbb{Z}_p)$, precum şi faptul că φ este morfism de grupuri. Vom arăta că φ este injectivă demonstrând că nucleul său $\operatorname{Ker}\varphi$ este $\{I_n\}$. Fie $M \in \operatorname{Ker}\varphi$, deci $M \equiv I_n \pmod{p}$; există atunci o matrice $N \in \mathcal{M}_n(\mathbb{Z})$ astfel încât $M = I_n + pN$. Grupul G fiind finit, rezultă că M este de ordin finit $m \geq 1$: $M^m = I_n$. Din această egalitate deducem că polinomul $P = (1 + pX)^m - 1$ este polinom anulator pentru matricea N. Dacă $\zeta_0, \zeta_1, \ldots, \zeta_{m-1}$ sunt rădăcinile de ordin m ale unităţii, rădăcinile lui P vor fi $\lambda_j = \dfrac{1}{p}\left(\zeta_j - 1\right)$, $j = \overline{0, m-1}$ şi acestea sunt numere distincte; rezultă că N este diagonalizabilă. În plus, cum $p \geq 3$, avem că $|\lambda_j| < 1$, prin urmare $\lim\limits_{k\to\infty} N^k = O_n$. Matricea N fiind cu elemente întregi, există k suficient de mare pentru care $N^k = O_n$, deci N este nilpotentă. O matrice diagonalizabilă şi nilpotentă este nulă şi deducem că $M = I_n + pO_n = I_n$, ceea ce încheie demonstraţia.

Consecinţa 1. *Ordinul oricărui subgrup finit al grupului $GL_n(\mathbb{Z})$ este majorat de 3^{n^2}, iar $GL_n(\mathbb{Z})$ conţine un număr finit de subgrupuri finite neizomorfe.*

Demonstraţie. Cardinalul unui subgrup G este majorat, conform propoziţiei precedente, de cardinalul lui $GL_n(\mathbb{Z}_3)$, care este 3^{n^2} (deoarece aplicaţia φ este injectivă). A doua afirmaţie rezultă imediat, deoarece $GL_n(\mathbb{Z}_3)$ are un număr finit de subgrupuri neizomorfe, fiind el însuşi grup finit.

Consecinţa 2. *Ordinul oricărui element al grupului $GL_n(\mathbb{Z})$ este sau infinit, sau majorat de 3^{n^2}.*

[1] Cercetător, Centrul de Calcul E.N.S.T., Paris

Demonstraţie. Concluzia rezultă din faptul că ordinul oricărui element al subgrupului divide ordinul grupului.

Din Consecinţa 2 urmează imediat prima parte a problemei **L94**.

Proprietatea nu mai are loc dacă A nu are elemente întregi. De exemplu, un subgrup $G \in GL_2(\mathbb{R})$ care este *de torsiune* ($\forall x \in G$, $\exists q \in \mathbb{N}^*$ cu $x^q = I_2$) poate să fie infinit; acest fapt aduce o îmbunătăţire soluţiei problemei **L94** dată în nr. 2/2006, unde se consideră un contraexemplu bazat pe o matrice cu elemente complexe nereale.

Fie G subgrupul lui $GL_2(\mathbb{R})$ format din matricele de forma

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \theta \in \{2r\pi \mid r \in \mathbb{Q}\}.$$

Dacă $\theta = \dfrac{p}{q}$, cu $p, q \in \mathbb{Z}$, $q \geq 1$, evident că

$$[R(\theta)]^q = \begin{pmatrix} \cos 2p\pi & -\sin 2p\pi \\ \sin 2p\pi & \cos 2p\pi \end{pmatrix} = I_2,$$

deci G este grup de torsiune. Pe de altă parte, G este de ordin infinit, izomorf cu grupul $(\mathbb{Q}/\mathbb{Z}, +)$; izomorfismul asociază matricei $R(\theta)$, cu $\theta = 2r\pi$, clasa din $\mathbb{Q}/\mathbb{Z}$ a părţii fracţionare a lui r (verificările se fac uşor).

Recreaţii ... matematice

Puncte coliniare

Ora de matematică la o clasă cu profil sportiv. Un elev de cl. a IX-a are de rezolvat la tablă o problemă simplă de *coliniaritate*, dar ...

– Ce sunt punctele coliniare? intervine profesorul, decis să-l ajute.

– !?!??

– Bine! S-o luăm altfel ... Tu eşti fotbalist. Ce înseamnă *coechiper*?

– Din aceeaşi echipă, de ce râdeţi de mine d-le profesor?

– Atunci, ce-ar putea să însemne *coliniar*?

– Din echipa adversă!...

Vreţi să vă ghicesc numărul ales?

Alegeţi un număr de două cifre pe care-l doriţi. Înmulţiţi prima cifră cu 5, adunaţi 3, dublaţi rezultatul, adăugaţi a doua cifră şi spuneţi-mi rezultatul. Vă voi indica pe loc numărul ales.

(*Explicaţii găsiţi la pagina 28.*)