Câteva proprietăţi ale subgrupurilor finite din $GL_n(\mathbb{Z})$

Gabriel DOSPINESCU[1]

Cu ocazia aniversării a 110 ani de apariţie neîntreruptă a Gazetei Matematice

1. Introducere: lema lui Serre. Ceea ce veţi citi în continuare este o încercare timidă de a expune o colecţie de rezultate referitoare la subgrupurile finite din $GL_n(\mathbb{Z})$. Se prea poate ca demonstraţiile care urmează să fie cunoscute; autorul le-a găsit "aproape" singur şi crede că merită să fie prezentate. Articole (mai serioase) despre proprietăţile acestor subgrupuri s-au scris multe şi, cu siguranţă, se vor mai scrie, căci problemele referitoare la ele sunt dificile şi multe dintre ele îşi aşteaptă de ani buni rezolvările. Îl invităm pe cititorul interesat de rezultate mai profunde să citească articolele din bibliografie, mult mai tehnice şi mai specializate. Se pare că în [**3**] ar fi o descriere superbă a aceloraşi (sau chiar a mai multor) rezultate, însă, din păcate, nu am avut acces la acest articol, aşa că nu putem decât să-l recomandăm "orbeşte" cititorilor interesaţi de asemenea aspecte.

Iată, mai întâi, ce rezultate vom demonstra (sau doar aminti). Vom deduce forma simplă a teoremei *Jordan-Zassenhaus* (cu ajutorul lemei lui Serre, de care am luat cunoştinţă din [**7**]) relativ la finitudinea claselor de izomorfism ale subgrupurilor finite ale lui $GL_n(\mathbb{Z})$, apoi vom demonstra că orice subgrup finit din $GL_n(\mathbb{Z})$ are cel mult $(2n)!$ elemente şi că există 9 clase de izomorfism pentru subgrupurile lui $GL_2(\mathbb{Z})$.

Vom începe cu *lema lui Serre*, un rezultat de o frumuseţe deosebită, care permite o primă majorare a ordinului subgrupurilor finite din $GL_n(\mathbb{Z})$; utilitatea acesteia ne permite să o numim "teoremă". Toate grupurile despre care va fi vorba în continuare au cel puţin două elemente.

Teorema 1 (Lema lui Serre). *Fie $G \subset GL_n(\mathbb{Z})$ un grup finit şi $p > 2$ un număr prim. Considerăm aplicaţia $\varphi : GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}_p)$ care asociază fiecărei matrici A matricea claselor de resturi modulo p ale elementelor din A. Atunci restricţia acestei aplicaţii la G este injectivă.*

Demonstraţie. Desigur, φ este bine definită şi este un morfism între grupurile $GL_n(\mathbb{Z})$ şi $GL_n(\mathbb{Z}_p)$ (aşa cum se verifică imediat). Să presupunem că restricţia aplicaţiei φ la G nu este injectivă, deci există $A \in G$, $A \neq I_n$ astfel încât $\varphi(A) = \varphi(I_n)$. Asta înseamnă că putem scrie $A = I_n + pB$, unde $B \in M_n(\mathbb{Z})$. Fie $\lambda_1, \lambda_2, \ldots, \lambda_n$ valorile proprii ale matricii B; se ştie atunci că A are valorile proprii $1 + p\lambda_i$, $1 \leq i \leq n$. Acum să privim cu atenţie sumele $S_k = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$ (pentru k număr natural): toate vor fi numere întregi (cel mai simplu argument este teorema fundamentală a polinoamelor simetrice, căci toate aceste sume sunt polinoame cu coeficienti întregi în sumele simetrice fundamentale ale numerelor $\lambda_1, \lambda_2, \ldots, \lambda_n$, iar aceste sume simetrice sunt - modulo un semn plus sau minus - coeficienţii polinomului caracteristic al matricii $B \in M_n(\mathbb{Z})$, deci întregi). Însă, G fiind finit, putem scrie $A^{|G|} = I_n$, deci trebuie să avem $(1 + p\lambda_i)^n = 1$, pentru fiecare $1 \leq i \leq n$, iar de aici obţinem imediat că $|\lambda_i| < 1, \forall 1 \leq i \leq n$. Or, aceasta înseamnă că şirul de numere întregi $(S_k)_{k \geq 1}$ tinde

[1] Student, École Normale Supérieure, Paris

la zero, deci trebuie ca toţi termenii săi să fie nuli (de la un rang încolo). O simplă aplicare a formulelor lui *Newton* ne va duce la concluzia că e necesar, pentru asta, ca toţi λ_i să fie egali cu 0; dar atunci toate valorile proprii ale matricii A sunt egale cu 1, deci (teorema *Cayley-Hamilton*) ea este "rădăcină" a polinomului $(X-1)^n$. Cum am văzut, mai este rădăcină şi pentru $X^{|G|}-1$, deci va fi rădăcină pentru cel mai mare divizor comun al acestor polinoame, care este $X-1$: adică $A=I_n$ (alt argument ar fi că identitatea este singura matrice unipotentă diagonalizabilă, iar matricea A are aceste două proprietăţi: este unipotentă - căci tocmai am arătat că toate valorile sale proprii sunt egale cu 1 - şi diagonalizabilă, deoarece polinomul său minimal nu are decât rădăcini simple, fiind un divizor al lui $X^{|G|}-1$) şi teorema 1 este demonstrată.

Să examinăm puţin consecinţele acestei teoreme; obţinem imediat că $\varphi(G)$ (imaginea lui G prin morfismul φ) este un subgrup cu $|G|$ elemente din $GL_n(\mathbb{Z}_p)$. Însă $GL_n(\mathbb{Z}_p)$ are exact $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$ elemente (lăsăm cititorului ca exerciţiu demonstraţia acestui rezultat clasic). Rezultă atunci, din teorema lui *Lagrange*, că $|G|$ divide pe $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$, pentru orice subgrup finit $G\subset GL_n(\mathbb{Z})$ şi orice $p>2$ prim. În particular, există un număr finit de ordine posibile ale matricilor din $GL_n(\mathbb{Z})$ (participanţii la olimpiade - şi nu numai ei - trebuie să-şi fi amintit celebra problemă: orice matrice din $GL_2(\mathbb{Z})$ are ordinul 1, 2, 3, 4, sau 6; încercaţi să demonstraţi aceasta pentru $n=3$!; mai mult, curajoşii se pot gândi la o variantă mult mai generală: mulţimile ordinelor posibile ale matricilor din $GL_{2k}(\mathbb{Z})$ şi $GL_{2k+1}(\mathbb{Z})$ coincid, pentru orice $k\geq 1$ natural). De asemenea, mai rezultă (tot ca un caz particular) că ordinul oricărei matrici din $GL_n(\mathbb{Z})$ divide pe $(3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$ (această problemă a fost propusă de autor în RecMat, pe vremea când nu cunoştea lema lui *Serre*; de altfel, am reuşit să demonstrăm că ordinul oricărei matrici din $GL_n(\mathbb{Z})$ este mai mic decât $A^{\sqrt{n\ln n}}$, unde A este o constantă pozitivă ce nu depinde de n, dar nu despre asta ne-am propus să vorbim aici). Tot din lema lui *Serre* mai putem deduce şi varianta simplă a teoremei lui *Jordan-Zassenhaus*, căci am obţinut că orice subgrup finit al lui $GL_n(\mathbb{Z})$ are cel mult $(3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$ elemente, deci, cu siguranţă, există un număr finit de clase de izomorfism în $GL_n(\mathbb{Z})$. Desigur, de aici şi până la demonstrarea teoremei lui *Jordan-Zassenhaus* (care afirmă finitudinea numărului claselor de conjugare ale subgrupurilor finite ale lui $GL_n(\mathbb{Z})$) mai e mult de muncă, şi, oricum, nu vom face asta aici; recomandăm excelentul articol [**7**].

2. Majorări pentru ordinele subgrupurilor finite ale lui $GL_n(Z)$. Şi iată că ne apropiem de un punct sensibil al acestei note, anume de obţinerea unei majorări bune pentru ordinul oricărui subgrup finit din $GL_n(\mathbb{Z})$; am obţinut deja că cel mai mare divizor comun al numerelor

$$(p^n-1)(p^n-p)\cdots(p^n-p^{n-1}), p>2, \quad p \text{ prim}$$

este un astfel de majorant. *Minkowski* a demonstrat şi un rezultat asemănător pentru $p=2$, anume că ordinul oricărui subgrup finit din $GL_n(\mathbb{Z})$ divide pe $2^{n^2}(2^n-1)(2^n-2)\cdots(2^n-2^{n-1})$. Din păcate această majorare este oricum, dar nu uşoară şi este departe de a fi cea mai bună. Vom încerca să dăm un rezultat mai "simplu" (în sensul că formula e mai simplă) care este, şi el, departe de valoarea optimală conjecturată.

Teorema 2. *Orice subgrup din $GL_n(\mathbb{Z})$ are cel mult $(2n)!$ elemente; de fapt,*

ordinul oricărui subgrup din $GL_n(\mathbb{Z})$ *divide pe* $(2n)!$.

Menţionăm că o majorare bună pentru ordinul maxim al subgrupurilor din $GL_n(\mathbb{Z})$ este, după câte ştim noi, o problemă deschisă şi foarte dificilă. Cititorul va fi observat o minorare aproape evidentă: există subgrupuri cu $2^n \cdot n!$ elemente (gândiţi-vă, de exemplu, la matricile ce au exact un 1 sau -1 pe fiecare linie şi pe fiecare coloană, în rest zerouri!). Cel mai bun rezultat obţinut până în prezent pare să fie o majorare de forma $C^n \cdot (n!)^{1+\varepsilon}$, unde C este o constantă care depinde de ε, nu şi de n, însă aceasta necesită un efort considerabil, pe care nu-l vom face aici. Invităm cititorul să găsească mai multe detalii în [**5**], unde există chiar şi o menţiune referitoare la faptul că $2^n \cdot n!$ este valoarea maximă a ordinului unui subgrup finit din $GL_n(\mathbb{Z})$ pentru toţi $n \notin \{2, 4, 6, 7, 8, 9, 10\}$ (afirmaţie atribuită acolo lui *W. Feit*).

Să revenim acum la Teorema 2, a cărei origine nu o ştim - ştim doar că a apărut în [**7**] fără menţiuni suplimentare şi fără... demonstraţie. Demonstraţia (cel puţin cea pe care am găsit-o noi) cere răbdare din partea cititorului, precum şi nişte rezultate ajutătoare, pe care le vom numi tot teoreme, datorită frumuseţii şi utilităţii lor.

Teorema 3. *Fie* $G \subset GL_n(Z)$ *un subgrup finit. Atunci, pentru orice* $k \in \mathbb{N}^*$, $|G|$ *este un divizor al numărului*

$$\sum_{g \in G} (\mathrm{tr}(g))^k.$$

Demonstraţie. Înainte de toate, să spunem că nici măcar nu e nevoie să presupunem că elementele matricilor sunt numere complexe; acestea pot fi dintr-un corp comutativ oarecare a cărui caracteristică este număr prim cu $|G|$. Demonstrăm mai întâi afirmaţia pentru $k = 1$. Să considerăm matricea

$$M = \frac{1}{|G|} \sum_{g \in G} g$$

pentru care, clar, avem

$$M^2 = \frac{1}{|G|^2} \sum_{g \in G} \sum_{h \in G} gh = M,$$

deoarece, pentru fiecare $g \in G$, avem (G fiind grup) $\{gh \mid h \in G\} = G$. Egalitatea $M^2 = M$ implică faptul că toate valorile proprii ale matricii M sunt 0 sau 1, deci $\mathrm{tr}(M)$ (care este urma matricii M, deci suma valorilor proprii) este un număr întreg; or, folosind proprietăţile urmei, avem

$$\mathrm{tr}(M) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(g),$$

deci demonstraţia pentru $k = 1$ este încheiată (totodată am rezolvat şi o problemă mai veche de la concursul *Putnam*: dacă $\sum_{g \in G} \mathrm{tr}(g) = 0$, G fiind un grup finit de matrici pătratice, atunci $\sum_{g \in G} g = 0$; într-adevăr, egalitatea $\sum_{g \in G} \mathrm{tr}(g) = 0$ implică faptul că suma valorilor proprii ale matricii M - definită ca mai sus - este 0, deci toate valorile proprii sunt 0; atunci M este idempotentă şi nilpotentă, deci este matricea nulă).

Acelaşi argument nu funcţionează însă pentru $k \geq 2$ (din păcate); şi totuşi... O clipă de graţie în algebra liniară a permis introducerea noţiunii de *produs tensorial* a două matrici. Astfel, dacă $A \in M_n(K)$ şi $B \in M_p(K)$, produsul lor tensorial este definit prin

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \in M_{np}(K).$$

O proprietate fundamentală a produsului tensorial (uşor de verificat) este că

$$(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD), \quad \forall A, C \in M_n(K), \quad \forall B, D \in M_p(K);$$

această egalitate ne permite să definim un subgrup $G' \subset GL_{n^2}(\mathbb{Z})$ prin $G' = \{g \otimes g \mid g \in G\}$ (relaţia de mai sus, precum şi faptul că $\det(A \otimes B) = (\det A)^p \cdot (\det B)^n$, pentru A, B ca mai sus, folosesc ca să arătăm că G' este subgrup al lui $GL_{n^2}(\mathbb{Z})$). Acest subgrup are, evident, tot $|G|$ elemente, deci îi putem aplica rezultatul deja demonstrat pentru a deduce că

$$|G| \sum_{g \in G} \operatorname{tr}(g \otimes g) = \sum_{g \in G} (\operatorname{tr}(g))^2$$

(dacă mai folosim şi formula foarte simplă $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \cdot \operatorname{tr}(B)$). Cititorul a înţeles acum modul în care va demonstra afirmaţia pentru orice $k \in \mathbb{N}^*$ (vom mai spune doar că pentru $k = 3$ trebuie considerat $G'' = \{(g \otimes g) \otimes g \mid g \in G\}$).

Acum putem începe să demonstrăm Teorema 2. Să notăm $x_1 > x_2 > \dots > x_q$ elementele mulţimii $\{\operatorname{tr}(g) \mid g \in G\}$ şi să observăm că avem $q \geq 2$ şi $x_1 = n$. Nefiind evidente (dar interesante şi în sine) vom demonstra aceste proprietăţi. În primul rând, am văzut că, dacă $A \in G$, atunci $A^{|G|} = I_n$, deci valorile proprii ale lui A sunt rădăcini ale unităţii, în particular ele au modulul 1. E clar atunci că avem $|\operatorname{tr}(A)| \leq n$, pentru orice $A \in G$; cum $I_n \in G$, se cheamă că $x_1 = n$. Dar, să mai observăm, dacă $A \in G - \{I_n\}$ (şi existenţa unei asemenea matrici e asigurată de presupunerea făcută încă de la început), nu putem avea $\operatorname{tr}(A) = n$, căci atunci toate valorile proprii ale matricii A ar fi egale cu 1, ceea ce este imposibil (cititorul nu a uitat argumentul final din demonstraţia teoremei 1); deci $q \geq 2$. În plus, dacă notăm cu $a_1, a_2, \dots, a_q$ numărul apariţiilor numerelor $x_1, x_2, \dots, x_q$ respectiv în mulţimea urmelor matricilor din G, teorema 3 afirmă că

$$|G| | a_1 x_1^k + a_2 x_2^k + \dots + a_q x_q^k, \quad \forall k \geq 1.$$

Desigur, mai avem şi $|G| = a_1 + a_2 + \dots + a_q$, precum şi $a_1 = 1$ (este suficient să fi înţeles argumentele din acest paragraf pentru a ne convinge şi de acest lucru, precum şi de faptul că, dacă $x_q = -n$, atunci şi $a_q = 1$; toate aceste observaţii se vor dovedi esenţiale în studiul subgrupurilor finite ale lui $GL_2(\mathbb{Z})$). Iar avem nevoie de un rezultat ajutător.

Teorema 4. *Fie $a_1, a_2, \dots, a_q, x_1, x_2, \dots, x_q$ şi m numere întregi astfel încât*

$$m \mid a_1 x_1^k + a_2 x_2^k + \dots + a_q x_q^k, \quad \forall k \in \mathbb{N}^*.$$

Atunci avem şi

$$m \mid a_1 (x_1 - x_2) \cdots (x_1 - x_q).$$

Demonstraţie. Să considerăm seria formală

$$f(z) = \frac{a_1}{1 - x_1 z} + \frac{a_2}{1 - x_2 z} + \dots + \frac{a_q}{1 - x_q z}$$

şi să observăm că

$$f(z) = \sum_{i=1}^{q} a_i + \left(\sum_{i=1}^{q} a_i x_i\right) z + \left(\sum_{i=1}^{q} a_i x_i^2\right) z^2 + \cdots,$$

deci, folosind ipoteza, rezultă existenţa unor numere întregi $b_0, b_1, b_2, \ldots$ astfel încât $f(z) = m \cdot \sum_{j\geq 0} b_j z^j$. Pe de altă parte, putem scrie şi

$$f(z) = \frac{\sum a_1(1-x_2z)\cdots(1-x_qz)}{(1-x_1z)(1-x_2z)\cdots(1-x_qz)}.$$

Asta ne arată că seria formală (de fapt, polinomul) de la numărător poate fi scris în forma

$$\sum a_1(1-x_2z)\cdots(1-x_qz) = m(1-x_1z)(1-x_2z)\cdots(1-x_qz)\sum_{j\geq 0} b_j z^j,$$

deci are toţi coeficienţii divizibili cu m, de unde obţinem că $m \mid \sum_{i=1}^{q} a_i S_t^{(i)}$, unde $S_t^{(i)}$ este a t-a sumă simetrică fundamentală în $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_q$, ceea ce implică şi

$$m | x_1^{q-1} \sum_{i=1}^{q} a_i - x_1^{q-2} \sum_{i=1}^{q} a_i S_1^{(i)} + \cdots + (-1)^{q-1} \sum_{i=1}^{q} a_i S_{q-1}^{(i)}$$

sau

$$m | \sum_{i=1}^{q} a_i (x_1^{q-1} - x_1^{q-2} S_1^{(i)} + \cdots + (-1)^{q-1} S_{q-1}^{(i)}).$$

Cum, pentru $i > 1$, avem $(x_1 - x_1)\cdots(x_1 - x_{i-1})(x_1 - x_{i+1})\cdots(x_1 - x_q) = 0$, adică

$$x_1^{q-1} - x_1^{q-2} S_1^{(i)} + \cdots + (-1)^{q-1} S_{q-1}^{(i)} = 0,$$

ne rămâne doar că

$$m \mid a_1(x_1^{q-1} - x_1^{q-2} S_1^{(1)} + \cdots + (-1)^{q-1} S_{q-1}^{(1)}) = a_1(x_1 - x_2)\cdots(x_1 - x_q),$$

ceea ce trebuia demonstrat.

Iar asta încheie şi demonstraţia teoremei 2: din teoremele 3 şi 4 şi faptul că $a_1 = 1$, rezultă că $|G|$ divide $(x_1 - x_2)\cdots(x_1 - x_q)$, care este produsul a $q-1$ numere naturale diferite şi cel mult egale cu $2n$ (deoarece urma oricărei matrici din G este un număr întreg cuprins între $-n$ şi n), deci divide şi pe $(2n)!$.

Bibliografie

1. **G. P. Dresden** - *There are only nine finite groups of fractional linear transforms with integer coefficients*, Mathematics Magazine, June 2004, 211-218.
2. **R. A. Horn, Ch. R. Johnson** - *Analiză matricială*, Fundaţia Theta, Bucureşti, 2001.
3. **J. Kuzmanovich, A. Pavlichenkov** - *Finite groups of matrices whose entries are integers*, American Mathematical Monthly, February 2002.
4. **T. J. Laffey** - *Lectures in integer matrices.*
5. **D. N. Rockmore, Ki-Seng Tan** - *A note on the order of finite subgroups of* $GL_n(\mathbb{Z})$, Commutative Algebra, 2/1999.
6. **Ken-Ichi Tahara** - *On the finite subgroups of* $GL_3(\mathbb{Z})$, Nagoya Math. Journal.
7. **Nicolas Tossel** - *Reseaux et théorèmes de finitude*, Revue des mathèmatiques speciales, 1-2/2005.