Rezultate privind morfismele de grupuri cu aplicații în problemele de concurs

Alexandru Daniel PÎRVUCEANU *

1 Introducere

În teoria grupurilor, morfismele sunt de o importanță aparte, deoarece ele ne oferă o serie de informații despre un anumit grup G. De aceea, determinarea morfismelor de la grupul pe care îl studiem la alte grupuri, a endomorfismelor sau a automorfismelor sale, este o problemă importantă.

Primul matematician care și-a propus să determine $\mathrm{Aut}(G)$ pentru un grup G dat a fost Hölder, care a și reușit acest lucru într-un caz particular, el demonstrând că $\mathrm{Aut}(S_n) \cong S_n$ pentru $n \in \mathbb{N}$, $n \geq 3$, $n \neq 6$. Până în prezent, nu există o soluție pentru problema generală pusă de Hölder, astfel dovedindu-se că această problemă extrem de veche este și extrem de dificilă. Totuși, interesul pentru ea și pentru determinarea morfismelor dintre două grupuri în general a generat un număr considerabil de rezultate referitoare la acestea.

În contextul pregătirii pentru concursurile de matematică, este extem de util să cunoaștem unele dintre aceste rezultate, deoarece numeroase probleme pot fi rezolvate mult mai ușor cu ajutorul lor. Așadar, acest articol își propune să prezinte o serie de astfel de teoreme și de propoziții, la un nivel accesibil unui elev de clasa a XII-a, urmând ca mai apoi să prezentăm și aplicații ale acestora.

2 Preliminarii

Pe tot parcursul acestei lucrări, grupurile multiplicative vor avea elementul neutru notat cu 1, iar cele aditive cu 0.

Pentru început, vom enunța câteva rezultate de teoria grupurilor. Mai apoi, vom prezenta câteva elemente de algebră liniară care nu sunt studiate în liceu. Peste tot vom încerca să menținem un caracter cât mai elementar și vom menționa de fiecare dată când particularizăm un rezultat pentru a ne atinge acest scop.

*Student, Facultatea de Matematică și Informatică, Universitatea din București, *pirvuceanualexandrudaniel@gmail.com*

Începem prin a enunța Teorema de structură a grupurilor abeliene finite, o teoremă a cărei demonstrație a durat aproape tot secolul al XIX-lea, fiind preocupați de ea mari matematicieni, precum Gauss (în anul 1801 a dat o formulare a acesteia în cadrul teoriei numerelor, conceptul de grup nefiind cunoscut atunci), Kronecker (în 1870 a demonstrat riguros teorema pe care o prezentăm mai jos) H.J.S. Smith sau Henri Poincaré (primul a extins teorema în anul 1861 pentru grupuri abeliene ce au o prezentare finită, iar cel de-al doilea a generalizat-o în anul 1900 chiar la grupuri abeliene finit generate; noi vom prezenta doar cazul grupurilor abeliene finite, cel pe care îl vom folosi în acest articol, însă cititorul interesat poate consulta [3] pentru mai multe detalii, precum și pentru demonstrațiile acestor teoreme):

Teorema 1. *Fie $(G, \cdot)$ un grup abelian finit. Atunci există în mod unic $n \in \mathbb{N}^*$ și $d_1, d_2, ..., d_n \in \mathbb{N}$ cu proprietatea că $d_1|d_2|...|d_n$ și $d_i \geq 2$, $\forall i = \overline{1,n}$, astfel încât*

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_n}.$$

Următoarele două propoziții își au rădăcinile în teoria categoriilor, prima dintre ele fiind un caz particular al proprietății de universalitate a coprodusului, iar cea de-a doua al proprietății de universalitate a produsului. Nu vom intra în mai multe amănunte, pentru a păstra caracterul elementar al expunerii noastre.

Propoziția 1. ([6]) Fie G, G_1, G_2, ..., G_n ($n \in \mathbb{N}$, $n \geq 2$) grupuri abeliene. Pentru fiecare $i \in \{1, 2, ..., n\}$, considerăm morfismul de grupuri $\lambda_i : G_i \to G_1 \times G_2 \times ... \times G_n$, $\lambda_i(x_i) = (1..., 1, x_i, 1, ..., 1)$. Definim acum funcția $\phi : \mathrm{Hom}(G_1 \times G_2 \times ... \times G_n, G) \to \mathrm{Hom}(G_1, G) \times \mathrm{Hom}(G_2, G) \times ... \times \mathrm{Hom}(G_n, G)$, $\phi(f) = (f \circ \lambda_1, f \circ \lambda_2, ..., f \circ \lambda_n)$. Atunci, ϕ este bijectivă.

Demonstrație. • ϕ este injectivă.

Fie $f, g \in \mathrm{Hom}(G_1 \times G_2 \times ... \times G_n, G)$ astfel încât $\phi(f) = \phi(g)$. Rezultă că $f \circ \lambda_i = g \circ \lambda_i$, $\forall i = \overline{1,n}$.

Așadar, pentru orice $(x_1, x_2, ..., x_n) \in G_1 \times G_2 \times ... \times G_n$, putem scrie acum că $f(x_1, x_2, ..., x_n) = f(\lambda_1(x_1) \cdot \lambda_2(x_2) \cdot ... \cdot \lambda_n(x_n)) = f(\lambda_1(x_1)) \cdot f(\lambda_2(x_2)) \cdot ... \cdot f(\lambda_n(x_n)) = g(\lambda_1(x_1)) \cdot g(\lambda_2(x_2)) \cdot ... \cdot g(\lambda_n(x_n)) = g(\lambda_1(x_1) \cdot \lambda_2(x_2) \cdot ... \cdot \lambda_n(x_n)) = g(x_1, x_2, ..., x_n)$, deci $f = g$, adică ϕ este injectivă.

• ϕ este surjectivă.

Fie $f_i \in \mathrm{Hom}(G_i, G), \forall i = \overline{1,n}$. Considerăm acum funcția $f : G_1 \times G_2 \times ... \times G_n \to G$, $f(x_1, x_2, ..., x_n) = f_1(x_1) f_2(x_2) ... f_n(x_n)$. Se constată ușor că f este morfism de grupuri și că $f \circ \lambda_i = f_i$, $\forall i = \overline{1,n}$.

Așadar, $\phi(f) = (f \circ \lambda_1, f \circ \lambda_2, ..., f \circ \lambda_n) = (f_1, f_2, ..., f_n)$, deci, cum $f_1, f_2, ..., f_n$ au fost alese arbitrar, concluzionăm că ϕ este surjectivă.

Am arătat că ϕ este injectivă și surjectivă, deci putem spune acum că ϕ este bijectivă. □

Propoziția 2. ([7]) Fie G, G_1, G_2, ..., G_n ($n \in \mathbb{N}$, $n \geq 2$) grupuri. Pentru fiecare $i \in \{1, 2, ..., n\}$, considerăm morfismul de grupuri $\mu_i : G_1 \times G_2 \times ... \times G_n \to G_i$, $\mu_i(x_1, x_2, ..., x_n) = x_i$. Definim acum funcția $\phi : \text{Hom}(G, G_1 \times G_2 \times ... \times G_n) \to \text{Hom}(G, G_1) \times ... \times \text{Hom}(G, G_n)$, $\phi(f) = (\mu_1 \circ f, \mu_2 \circ f, ..., \mu_n \circ f)$. Atunci, ϕ este bijectivă.

Demonstrație. • ϕ este injectivă.

Fie $f, g \in \text{Hom}(G, G_1 \times G_2 \times ... \times G_n) \to \text{Hom}(G, G_1) \times ... \times \text{Hom}(G, G_n)$ astfel încât $\phi(f) = \phi(g)$. Rezultă că $\mu_i \circ f = \mu_i \circ g$, $\forall i = \overline{1, n}$.

Considerăm acum $x \in G$ arbitrar. Avem $f(x) = (y_1, y_2, ..., y_n)$ și $g(x) = (z_1, z_2, ..., z_n)$, unde $y_i, z_i \in G_i, \forall i = \overline{1, n}$. În baza celor de mai sus, putem scrie că $y_i = \mu_i(f(x)) = (\mu_i \circ f)(x) = (\mu_i \circ g)(x) = \mu_i(g(x)) = z_i, \forall i = \overline{1, n}$, deci $f(x) = g(x)$. Cum x a fost ales arbitrar, obținem că $f = g$, așadar, ϕ este injectivă.

• ϕ este surjectivă.

Fie $f_i \in \text{Hom}(G, G_i)$, $\forall i = \overline{1, n}$. Considerăm funcția $f : G \to G_1 \times G_2 \times ... \times G_n$, $f(x) = (f_1(x), f_2(x), ..., f_n(x))$.

Este ușor de văzut că f este morfism de grupuri și că $\mu_i \circ f = f_i$, $\forall i = \overline{1, n}$.

Putem scrie acum că $\phi(f) = (\mu_1 \circ f, \mu_2 \circ f, ..., \mu_n \circ f) = (f_1, f_2, ..., f_n)$, iar cum $f_1, f_2, ..., f_n$ au fost alese arbitrar, concluzionăm că ϕ este surjectivă.

Așadar, am arătat că ϕ este bijectivă. □

Așa cum am anunțat la începutul acestei secțiuni, acum vom enunța câteva rezultate elementare de algebră liniară. Recomandăm cititorului interesat să consulte lucrarea [2] pentru o mai bună aprofundare a acestora. În cele ce urmează, $\mathbb{K}$ va fi un corp comutativ.

Definiția 1. Un **spațiu vectorial** peste corpul $\mathbb{K}$ (pe scurt, un $\mathbb{K}$- spațiu vectorial) este un grup abelian $(V, +)$ împreună cu o operație externă $\mathbb{K} \times V \to V$, $(a, x) \mapsto ax$, numită **înmulțire cu scalari**, care verifică următoarele condiții pentru orice $a, b \in \mathbb{K}$ și $x, y \in V$:

1. $a(x + y) = ax + ay$;
2. $(a + b)x = ax + bx$;
3. $(ab)x = a(bx)$;
4. $1x = x$.

Definiția 2. Fie V un $\mathbb{K}$-spațiu vectorial. O submulțime $\{x_1, x_2, ..., x_n\}$ ($n \in \mathbb{N}^*$) a lui V se numește:

• **liniar independentă**, dacă, pentru orice $a_1, a_2, ..., a_n \in \mathbb{K}$, are loc implicația

$$a_1x_1 + a_2x_2 + ...a_nx_n = 0 \implies a_1 = a_2 = ... = a_n = 0.$$

• **sistem de generatori**, dacă, pentru orice $x \in V$, există $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{K}$ astfel încât $x = \alpha_1x_1 + \alpha_2x_2 + ... + \alpha_nx_n$.

• **bază**, dacă este liniar independentă și sistem de generatori.

Teorema 2. *Orice $\mathbb{K}$- spațiu vectorial admite o bază și oricare două baze ale acestuia au același cardinal.*

Definiția 3. Fie V un $\mathbb{K}$-spațiu vectorial. Cardinalul comun al tuturor bazelor lui V se numește **dimensiunea** lui V și se notează $\dim_{\mathbb{K}}(V)$. Dacă acest cardinal este finit, atunci spunem că V este un spațiu **finit dimensional**, iar în caz contrar că este **infinit dimensional**.

Definiția 4. Fie V și W două $\mathbb{K}$-spații vectoriale. Atunci:

• o funcție $f : V \to W$ cu proprietatea că $f(ax + by) = af(x) + bf(y)$, $\forall a, b \in \mathbb{K}, x, y \in V$ se numește **aplicație liniară** sau **morfism de spații vectoriale**. Dacă f este bijectivă, atunci f se numește **izomorfism liniar**.

• o aplicație liniară $g : V \to V$ se numește **endomorfism**. Dacă g este bijectivă, atunci g se numește **automorfism**.

Definiția 5. Fie V un $\mathbb{K}$-spațiu vectorial de dimensiune n ($n \in \mathbb{N}^*$), $B = \{e_1, e_2, ..., e_n\}$ o bază a sa și f un endomorfism.

Dacă exprimăm vectorii $f(e_1), f(e_2), ..., f(e_n)$ în baza B, adică pentru fiecare $j \in \{1, 2, ..., n\}$ scriem $f(e_j) = \sum_{i=1}^{n} a_{ij}e_i$ pentru $a_{ij} \in \mathbb{K}$, obținem matricea $M_B(f) := (a_{ij})_{1 \leq i,j, \leq n}$, numită **matricea lui f în baza B**.

Teorema 3. *În contextul Definiției 5, aplicația $\phi : \mathrm{End}(V) \to \mathcal{M}_n(\mathbb{K})$, $\phi(f) = M_B(f)$ este un izomorfism de spații vectoriale, unde prin $\mathrm{End}(V)$ am notat mulțimea endomorfismelor $\mathbb{K}$-spațiului vectorial V.*

Observație. Această ultimă teoremă ne spune că un endomorfism al unui spațiu vectorial se poate identifica cu matricea lui într-o anumită bază. Rezultă imediat acum că avem un izomorfism între $\mathrm{Aut}(V)$ (mulțimea automorfismelor spațiului vectorial V) și $\mathrm{GL}_n(\mathbb{K})$ (mulțimea matricelor inversabile cu n linii și n coloane ce au elemente din $\mathbb{K}$), deci vom identifica automorfismele unui $\mathbb{K}$-spațiu vectorial de dimensiune n cu matricele inversabile de dimensiune $n \times n$ ce se pot forma cu elemente din $\mathbb{K}$. În final, mai spunem că există un rezultat similar și pentru aplicații liniare între două $\mathbb{K}$-spații vectoriale finit dimensionale diferite, dar acesta nu este folositor scopului articolului nostru.

Propoziția 3. Fie $n \in \mathbb{N}, n \geq 2$ și $A \in \mathcal{M}_n(\mathbb{K})$. Pentru fiecare $i \in \{1, 2, ..., n\}$, notăm cu c_i a i-a coloană a lui A. Atunci, A este inversabilă $\iff$ mulțimea $\{c_1, c_2, ..., c_n\}$ este liniar independentă.

Observație. Propoziția de mai sus este o consecință imediată a unei teoreme a lui Kronecker privind rangul unei matrice. Nu am enunțat acea teoremă pentru a evita să introducem noțiunea de subspațiu vectorial, însă cititorul interesat o poate consulta în [2].

3 Aplicații

Suntem pregătiți acum să vedem cum putem folosi în probleme rezultatele pe care le-am prezentat. Pentru început, ne vom îndrepta atenția asupra unor exerciții care apar în [6] și [7].

Aplicația 1. Determinați cardinalul mulțimii $\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3 \times S_3)$.

Soluție. Folosind Propoziția 2, avem o bijecție între $\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3 \times S_3)$ și $\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3) \times \mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3)$, deci $|\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3 \times S_3)| =$

$= |\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3)|^2$. Așadar, am redus problema noastră la a număra morfismele de la $\mathbb{Z}_2 \times \mathbb{Z}_2$ la S_3 (ceea ce este mult mai simplu).

Fie $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to S_3$ un morfism de grupuri netrivial. Atunci, $|\mathrm{Ker}(f)| < 4$. Cum S_3 nu are subgrupuri de ordin 4 (dacă ar avea, din Teorema lui Lagrange ar rezulta că $4|6$, ceea ce este absurd), f nu poate fi injectiv, deci $|\mathrm{Ker}(f)| > 1$. Așadar, $|\mathrm{Ker}(f)| = 2$ ($\mathrm{Ker}(f)$ este subgrup al lui $\mathbb{Z}_2 \times \mathbb{Z}_2$, deci ordinul lui trebuie să fie divizor al lui 4).

Notăm $x := (\widehat{1}, \widehat{0})$ și $y := (\widehat{0}, \widehat{1})$. Atunci, $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{1, x, y, x+y\}$. Presupunem că $\mathrm{Ker}(f) = \{1, x\}$. Rezultă că $f(x+y) = f(y)$, iar $f(y)$ este un element de ordin 2 din S_3. Cum S_3 are 3 elemente de ordinul 2, concluzionăm că sunt 3 feluri în care putem alege f în acest caz. Analog se obțin 3 funcții f și dacă $\mathrm{Ker}(f) = \{1, y\}$ sau $\mathrm{Ker}(f) = \{1, x+y\}$.

Așadar, $|\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3)| = 10$, iar acum, ținând cont de cele de mai sus, putem concluziona că $|\mathrm{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, S_3 \times S_3)| = 100$. □

Aplicația 2. Fie G un grup abelian finit și fie $n \in \mathbb{N}$, $n \geq 2$. Determinați cardinalul mulțimilor $\mathrm{Hom}(G, \mathbb{Z}_n)$ și $\mathrm{Hom}(G, \mathbb{Z})$.

Soluție. Vom folosi câteva rezultate elementare de teoria grupurilor, care apar și în [5]: $|\mathrm{Hom}(\mathbb{Z}_k, \mathbb{Z}_l)| = (k, l)$, $\forall k, l \in \mathbb{N}, k, l \geq 2$, unde prin (k, l) am notat cel mai mare divizor comun al numerelor naturale k și l, iar $|\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z})| = 1$, $\forall m \in \mathbb{N}$, $m \geq 2$.

De asemenea, vom mai utliza faptul că, dacă H, K și L sunt trei grupuri astfel încât $H \cong K$, atunci $|\mathrm{Hom}(H, L)| = |\mathrm{Hom}(K, L)|$ (dacă $f : K \to H$ este un izomorfism de grupuri, atunci $\phi : \mathrm{Hom}(H, L) \to \mathrm{Hom}(K, L)$, $\phi(g) = g \circ f$ este bijectivă).

Conform Teoremei 1, există (în mod unic) $k \in \mathbb{N}^*$ și $d_1, d_2, ..., d_k \in \mathbb{N}$ cu $d_1|d_2|...|d_k$ și $d_i \geq 2$, $\forall i = \overline{1, k}$, astfel încât $G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_k}$.

Putem scrie acum că:

$$|\mathrm{Hom}(G, \mathbb{Z}_n)| = |\mathrm{Hom}(\mathbb{Z}_{d_1}, \mathbb{Z}_n) \times \mathrm{Hom}(\mathbb{Z}_{d_2}, \mathbb{Z}_n) \times ... \times \mathrm{Hom}(\mathbb{Z}_{d_k}, \mathbb{Z}_n)|,$$

deoarece $|\mathrm{Hom}(G, \mathbb{Z}_n)| = |\mathrm{Hom}(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_k}, \mathbb{Z}_n)|$, iar Propoziția 1

implică $|\operatorname{Hom}(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_k}, \mathbb{Z}_n)| = |\operatorname{Hom}(\mathbb{Z}_{d_1}, \mathbb{Z}_n) \times \operatorname{Hom}(\mathbb{Z}_{d_2}, \mathbb{Z}_n) \times ... \times \operatorname{Hom}(\mathbb{Z}_{d_k}, \mathbb{Z}_n)|$.

Așadar, $|\operatorname{Hom}(G, \mathbb{Z}_n)| = \prod_{i=1}^{k}(d_i, n)$.

Printr-un raționament analog, găsim că:

$$|\operatorname{Hom}(G, \mathbb{Z})| = |\operatorname{Hom}(\mathbb{Z}_{d_1}, \mathbb{Z}) \times \operatorname{Hom}(\mathbb{Z}_{d_2}, \mathbb{Z}) \times ... \times \operatorname{Hom}(\mathbb{Z}_{d_k}, \mathbb{Z})|,$$

deci $|\operatorname{Hom}(G, \mathbb{Z})| = 1$. □

Aplicația 3. (**C.O:4985**, *G.M.-B 11/2008*) Fie G un grup abelian finit cu n elemente cu proprietatea că numărul endomorfismelor sale este n. Să se arate că G este izomorf cu $\mathbb{Z}_n$.

Marian Andronache

Soluție. Vom prezenta, în esență, soluția primită de autorul acestui articol în [4]. Conform Teoremei 1, există (în mod unic) $k \in \mathbb{N}^*$ și $d_1, d_2, ..., d_k \in \mathbb{N}$ astfel încât $d_i \geq 2, \forall i = \overline{1,k}$, $d_1|d_2|...|d_k$ și

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times ... \times \mathbb{Z}_{d_k}. \tag{1}$$

Folosind faptul că $|\operatorname{Hom}(\mathbb{Z}_m, \mathbb{Z}_l)| = (m, l), \forall k, l \in \mathbb{N}, k, l \geq 2$ [5], Propoziția 1 și Propoziția 2, putem scrie acum că

$$|\operatorname{End}(G)| = |\operatorname{Hom}(G, G)| = |\prod_{1 \leq i,j \leq k} \operatorname{Hom}(\mathbb{Z}_{d_i}, \mathbb{Z}_{d_j})| = \prod_{1 \leq i,j \leq k} (d_i, d_j).$$

Cum $d_i|d_j$ pentru orice $j \geq i$, avem

$$|\operatorname{End}(G)| = d_1^{2k-1} d_2^{2k-3} ... d_k. \tag{2}$$

Din (1) și (2) avem $n = |\operatorname{End}(G)| \iff d_1 d_2 ... d_k = d_1^{2k-1} d_2^{2k-3} ... d_k$, egalitate care are loc, evident, dacă și numai dacă $k = 1$, ceea ce implică $n = d_1$, iar acum din (1) avem $G \cong \mathbb{Z}_{d_1} = \mathbb{Z}_n$. □

Aplicația 4. (**27600**, *G.M.-B 10/2018*) Fie $n \in \mathbb{N}$, $n \geq 2$ și $(G, \cdot)$ un grup abelian finit de ordin n, cu proprietatea că, pentru orice $a \in G$, numărul endomorfismelor f ale lui G cu $f(a) = a$ este egal cu $n + 1 - \operatorname{ord}(a)$, unde $\operatorname{ord}(a)$ este ordinul lui a în grupul $(G, \cdot)$. Să se arate că n este număr prim.

Marian Andronache

Soluție. Vom prezenta, în esență, soluția oficială din *G.M.-B 4/2019*.

Dacă în ipoteză luăm $a = 1$, obținem că G are n endomorfisme. Conform Aplicației 3, avem că $G \cong \mathbb{Z}_n$.

Fie acum m și s două numere naturale cu $n = ms$ și fie f un endomorfism al lui $\mathbb{Z}_n$. Dacă notăm $f(\widehat{1}) =: \widehat{k}$, atunci $f(\widehat{m}) = \widehat{m} \iff \widehat{km} = \widehat{m} \iff n|m(k-1) \iff s|k-1 \iff k = st+1, t = \overline{0, m-1}$ (deoarece lucrăm modulo n, considerăm că $0 \leq k < n$). Deci, există exact m endomorfisme care invariază $\widehat{m}$. Cum $\text{ord}(\widehat{m}) = s$, rezultă că $n + 1 - s = m \iff ms - m - s + 1 = 0 \iff (m-1)(s-1) = 0 \iff m = 1$ sau $s = 1$, deci n este prim. □

Aplicația 5. (*Lista scurtă a O.N.M. 2018*) Fie p un număr prim, iar G un grup finit comutativ, cu elementul neutru e, având proprietatea că $x^p = e$, pentru orice $x \in G$. Notăm cu $\text{Aut}(G)$ grupul tuturor automorfismelor lui G. Dacă G are cel puțin 3 elemente, să se arate că:

a) $|G| = p^n$, unde n este cel mai mic număr de generatori ai lui G;

b) $|Aut(G)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$.

Ioan Băetu

Soluție. a) Vom înzestra grupul G cu o structură de $\mathbb{Z}_p$-spațiu vectorial.

Într-adevăr, dacă pentru orice $\widehat{k} \in \mathbb{Z}_p$ și $x \in G$ definim $\widehat{k} \cdot x = x^k$, atunci G devine un $\mathbb{Z}_p$-spațiu vectorial cu această înmulțire cu scalari (verificarea celor 4 axiome îi este lăsată cititorului).

Conform Teoremei 2, G va admite o bază, care va fi finită, căci mulțimea G este finită. Fie aceasta $B = \{e_1, e_2, ..., e_n\} \subset G$, unde $n \in \mathbb{N}$ va fi, dacă ținem cont de definiția unei baze, cel mai mic număr de generatori ai lui G.

Atunci, pentru orice $x \in G$, $\exists! \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{Z}_p$ astfel încât $x = \prod_{i=1}^{n} \alpha_i \cdot e_i$, adică funcția $f : \mathbb{Z}_p^n \to G$, $f(\alpha_1, \alpha_2, ..., \alpha_n) = \prod_{i=1}^{n} \alpha_i \cdot e_i$, este bijectivă.

De aici, obținem că $|G| = p^n$.

b) Să remarcăm că $\text{Aut}(G) = \text{Aut}_{\mathbb{Z}_p}(G)$, unde prin $\text{Aut}_{\mathbb{Z}_p}(G)$ am notat grupul automorfismelor $\mathbb{Z}_p$-spațiului vectorial G (această egalitate se demonstrează ușor prin dublă incluziune). Folosind observația Teoremei 3, deducem că trebuie să determinăm cardinalul lui $\text{GL}_n(\mathbb{Z}_p)$. Fie $A \in \text{GL}_n(\mathbb{Z}_p)$. Vom construi matricea A inductiv. Notăm cu c_i a i-a coloană a lui A, $\forall i \in \overline{1, n}$. c_1 poate să fie orice vector nenul din $\mathbb{Z}_p^n$, deci poate fi aleasă în $p^n - 1$ feluri.

Presupunem acum că avem primele k coloane construite (acestea trebuie să fie liniar independente, conform Propoziției 3), unde $2 \leq k \leq n-1$. Vrem să construim c_{k+1}. Aceasta nu trebuie să fie un element al mulțimii $\{a_1c_1 + a_2c_2 + ... + a_kc_k | a_i \in \mathbb{Z}_p, \forall i = \overline{1, k}\}$, mulțime care are p^k elemente (fiecare a_i poate lua k valori, iar pentru fiecare dintre aceste valori obținem un element diferit al mulțimii). Așadar, deducem că c_{k+1} poate fi aleasă în $p^n - p^k$ moduri.

În concluzie, $|\text{GL}_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$, deci am obținut concluzia dorită.

□

Observație. Un grup abelian G în care toate elementele au ordinul $p \in \mathbb{N}^*$ se numește **p-grup abelian elementar**. Să observăm că p este obligatoriu un număr prim (dacă presupunem că p nu este prim, atunci există $m, n \in \mathbb{N}^*$, $m, n \geq 2$, astfel încât $p = mn$. Pentru orice $x \in G \setminus \{1\}$, vom avea că $\text{ord}(x^m) = n < p$, contradicție.). Așadar, Aplicația 5 ne-a cerut să determinăm cardinalul unui p-grup abelian elementar finit și să numărăm automorfismele sale. Acesta este un rezultat important (și cunoscut) în teoria grupurilor, care merită reținut.

Aplicația 6. ([1]) Să se arate că există un grup care nu este izomorf cu $\text{Aut}(G)$ pentru niciun grup G.

Soluție. Fie $n \in \mathbb{N}^*$ arbitrar. Vom arăta că $\mathbb{Z}_{2n+1} \ncong \text{Aut}(G)$ pentru orice grup G. Într-adevăr, să presupunem că există un grup G astfel încât $\text{Aut}(G) \cong \mathbb{Z}_{2n+1}$. Notăm cu $\text{Inn}(G)$ grupul automorfismelor interioare ale lui G. Acesta este un subgrup al lui $\text{Aut}(G)$, care, din presupunerea făcută, este ciclic. Astfel, $\text{Inn}(G)$ este un grup ciclic, iar cum $G/\text{Z}(G) \cong \text{Inn}(G)$, obținem că grupul $G/\text{Z}(G)$ este ciclic. Dar este bine cunoscut faptul că, dacă $G/\text{Z}(G)$ este ciclic, atunci G este abelian.

Considerăm funcția $f : G \to G, f(x) = x^{-1}$. Se verifică ușor că f este un automorfism al lui G (este esențial faptul că G este abelian). Mai mult, avem $f \circ f = \text{Id}_G$, deci, dacă $f \neq \text{Id}_G$, atunci $\text{Aut}(G)$ are un element de ordinul 2, ceea ce este absurd (ar însemna că $\mathbb{Z}_{2n+1}$ are un element de ordinul 2, ceea ce ar contrazice teorema lui Lagrange). Așadar, $f = \text{Id}_G$, ceea ce implică $x^2 = 1, \forall x \in G$.

Acum, putem înzestra G cu o structură de $\mathbb{Z}_2$- spațiu vectorial exact cum am făcut în Aplicația 5. Distingem două cazuri:

Cazul I. $\dim_{\mathbb{Z}_2}(G) = 1$. În acest caz, $G \cong \mathbb{Z}_2$ ca spații vectoriale, deci, în particular, și ca grupuri. Obținem $\text{Aut}(G) \cong \text{Aut}(\mathbb{Z}_2)$, de unde $|\text{Aut}(G)| = 1 < 2n + 1$, contradicție.

Cazul II. $\dim_{\mathbb{Z}_2}(G) \geq 2$. Fie $\{e_i | i \in I\}$, unde I este o mulțime cu cel puțin două elemente, o bază a lui G. Definim $\phi : G \to G$, $\phi(e_1) = e_2$, $\phi(e_2) = e_1$, $\phi(e_i) = e_i$, $\forall i \geq 3$. Lăsăm cititorului verificarea faptului că funcția ϕ este corect definită și că este un automorfism al $\mathbb{Z}_2$-spațiului vectorial G [1] al cărui ordin este 2. Așadar, și grupul $\text{Aut}(G)$ are un element de ordinul 2 (deoarece $\text{Aut}(G) = \text{Aut}_{\mathbb{Z}_2}(G)$, așa cum am remarcat în rezolvarea punctului b) al Aplicației 5), contradicție.

Așadar, $\mathbb{Z}_{2n+1} \ncong \text{Aut}(G)$ pentru orice grup G, deci am găsit un grup (chiar o clasă de grupuri, aceea a grupurilor ciclice de ordin impar) cu proprietatea cerută. □

În final, invităm cititorul să descopere și alte probleme în care pot fi folosite rezultatele teoretice prezentate de noi. De asemenea, autorul dorește să

[1] Nu este nevoie să facem această verificare dacă știm proprietatea de universalitate a spațiilor vectoriale, dar recomandăm cititorilor nefamiliari cu spațiile vectoriale să o facă.

îi mulțumească domnului prof. univ. dr. Gigel Militaru, ale cărui sugestii l-au ajutat să își îmbunătățească lucrarea.

Bibliografie

[1] C. Băețica, C. Boboc, S. Dăscălescu, G. Mincu, *Probleme de algebră*, Ed. Universității din București, 2008.

[2] T. Dumitrescu, *Algebra* , Ed. Universității din București, 2006.

[3] L. Fuchs, *Abelian Groups*, Springer International Publishing, 2015, pg. 80-85.

[4] Y. Sharifi [ysharifi], postat în *Finite abelian group with exactly n endomorphisms*, Art of Problem Solving, `https://artofproblemsolving.com/community/u354682h1930305p13267571`.

[5] Y.Sharifi, *Group homomorphism - cyclic groups*, `https://ysharifi.wordpress.com/2019/09/24/group-homomorphism-cyclic-groups/`

[6] Y. Sharifi, *Group homomorphism - direct product(1)*, `https://ysharifi.wordpress.com/2019/09/26/group-homomorphism-direct-product-1/` .

[7] Y. Sharifi, *Group homomorphism - direct product (2)*, `https://ysharifi.wordpress.com/2019/09/26/group-homomorphism-direct-product-2/`.

[8] Colecția revistei *Gazeta Matematică*.