The power function in Group Theory

ROBERT, ROGOZSAN[a], GHEORGHE, BOROICA[b]

[a]*Gheorghe Şincai National College, Baia Mare, Romania*
[b]*Gheorghe Şincai National College, Baia Mare, Romania*

Email addresses: robertrogozsan@gmail.com (ROBERT, ROGOZSAN), ghitaboroica64@gmail.com (GHEORGHE, BOROICA)

Abstract

In this article we will present some special properties and applications regarding the power function over a group. First we will give an equivalent condition for the power function to be a bijection over a group G, then we will present some problems which can easily be solved by using the properties we will prove at the beginning of the paper.

Keywords: *group, power function, lemma, bijection.*

Scopul acestui articol este de a prezenta câteva proprietăţi interesante ale funcţiei $f(x) = x^p$ peste un grup G, unde p este un număr natural nenul. Vom structura articolul pe două părţi, prima parte fiind compusă dintr-o serie de rezultate remarcabile, iar a doua parte fiind alcătuită din probleme care pot fi rezolvate natural cu ajutorul lemei de mai jos. Pentru a familiariza cititorul cu notaţiile folosite în continuare, vom nota cu $Z(G)$ centrul grupului G, adică mulţimea $\{y \in G \mid xy = yx, \forall x \in G\}$, şi vom accepta cunoscut faptul că $Z(G)$ e subgrup al lui G. De asemenea, vom prezenta fără demonstraţie Teorema lui Cauchy, de care vom avea nevoie pentru a motiva proprietăţile de mai jos.

Teoremă. *(Teorema lui Cauchy) Fie G un grup de ordin n. Fie p un număr prim astfel încât $p|n$. Atunci numărul soluţiilor ecuaţiei $x^p = e$ în G este un multiplu nenul al lui p. În particular rezultă că în G există cel puţin un element de ordin p.*

Lemă. *Fie G un grup finit de ordin n. Atunci funcţia $f : G \to G, f(x) = x^p$ este bijectivă dacă şi numai dacă $(n, p) = 1$.*

Demonstraţie.
„⇒” Presupunem prin absurd că $(n, p) = d > 1$, atunci există q număr prim cu $q|d$. Din Teorema lui Cauchy vom avea că există $a \in G$ cu $ord(a) = q$. Aşadar $q|p$ şi deci vom avea $f(a) = a^p = (a^q)^{\frac{p}{q}} = e^{\frac{p}{q}} = e = f(e)$ şi cum f e injectivă $\Rightarrow a = e$, fals. Deci $(n, p) = 1$.
„⇐” Cum G e finit, e suficient să arătam că f e injectivă. Cum $(n, p) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ cu $un + vp = 1$. Din $f(a) = f(b) \Rightarrow a^p = b^p \Rightarrow a^{vp} = b^{vp} \Rightarrow a^{1-un} = b^{1-un}$ şi cum $x^n = e, \forall x \in G$ va rezulta $a = b$, adică f e injectivă, deci bijectivă. □

Observaţie. O formă mai puternică a lemei de mai sus a fost enunţată de Sorin Rădulescu şi Ion Savu: Fie G un grup cu proprietatea că există $n \in \mathbb{N}^*, n$ minim cu $x^n = e, \forall x \in G$ (se spune că G e de exponent n) şi fie funcţia $f : G \to G, f(x) = x^p$. Atunci următoarele afirmaţii sunt echivalente:

a) $(n, p) = 1$

b) f e injectivă

c) f e surjectivă

ISSN

d) f e bijectivă

Demonstrație.
„a) $\Rightarrow$ b)" Cum $(n,p)=1 \Rightarrow \exists u,v \in \mathbb{Z}$ cu $un+vp=1$.
Din $f(a)=f(b) \Rightarrow a^p=b^p \Rightarrow a^{vp}=b^{vp} \Rightarrow a^{1-un}=b^{1-un}$ şi cum $x^n=e, \forall x \in G$ va rezulta $a=b$, adică f e injectivă
„b) $\Rightarrow$ a)" Presupunem că $(n,p)=d>1$, deci $n=d\cdot m$, cu $m \in \mathbb{N}^*$. Cum $x^n=(x^m)^d=e, \forall x \in G \Rightarrow \exists u \in G$ cu $u^d=e$. Dacă am avea $x^m=e, \forall x \in G$ ar rezulta o contradicţie între m şi minimalitatea lui n, aşadar $\exists x_0 \in G$ cu $x_0^m \neq e$, dar cum $(x_0^m)^d=e=e^d$ va rezulta $f(x_0^m)=f(e)$, contradicţie cu injectivitatea lui f. Deci $(n,p)=1$
„b) $\Rightarrow$ d)" Cum b) $\Rightarrow$ a) $\Rightarrow (n,p)=1$. Fie $u,v \in \mathbb{Z}$ cu $un+vp=1$ şi funcţia $g\colon G \to G, g(x)=x^v$. Avem $f(g(x))=g(f(x))=x^{vp}=x^{1-un}=x$, deci $f\circ g=g\circ f=1_G$, adică f e bijectivă, cu $g=f^{-1}$.
„d) $\Rightarrow$ c)" Clar.
„c) $\Rightarrow$ a)" Presupunem că $(n,p)=d>1$ şi fie q un divizor prim al lui d.
Cum funcţia f e surjectivă, vom avea că $\forall y \in G, \exists x \in G$ cu $f(x)=x^p=(x^{\frac{p}{q}})^q=g(x^{\frac{p}{q}})$, unde $g\colon G \to G, g(x)=x^q$, deci şi g e surjectivă.
Dacă am avea $x^q \neq e, \forall x \in G$, cum $e=x^n=(x^q)^{\frac{n}{q}}$ ar rezulta, conform surjectivităţii lui g, că $x^{\frac{n}{q}}=e, \forall x \in G$, adică o contradicţie între $\frac{n}{q}$ şi minimalitatea lui n, aşadar $\exists x_0 \in G$ cu $x_0^q=e$.
Fie y un element astfel încât $ord(y)=\max\{ord(z) \mid q|ord(z), z \in G\}$. Fie $t=ord(y)$.
Cum f e surjectivă, $\exists z \in G$ cu $z^p=y$, deci $ord(z^p)=t$. Fie $s=ord(z)$. Atunci avem că $t=\frac{s}{(s,p)}$. Cum q divide pe p,t şi s avem că q divide şi pe (p,s), deci $s=t\cdot(p,s) \geq t\cdot q>t$, contradicţie cu maximalitatea lui t. Deci $(n,p)=1$. □

Propoziţia 1. *Dacă într-un grup finit G avem $x^p=e, \forall x \in G$, unde p e număr prim, atunci $\exists k \in \mathbb{N}$ cu $ord(x)=p^k$.*

Demonstrație.
Presupunem prin absurd că $ord(G)$ nu are forma p^k, cu $k \in \mathbb{N}$. Atunci $\exists q$-prim, diferit de p, cu $q|ord(G)$.
Din Teorema lui Cauchy $\Rightarrow \exists x \in G$ cu $ord(x)=q$. Cum $x^p=e=x^q$ va rezulta că $x^{(p,q)}=e$, iar din $(p,q)=1$ rezultă $x=e$, fals.
Deci $ord(G)=p^k$, cu $k \in \mathbb{N}$. □

Propoziţia 2. *Fie G un grup. Dacă funcţia $f\colon G \to G, f(x)=x^p$ este un morfism surjectiv atunci $x^{p-1} \in Z(G), \forall x \in G$.*

Demonstrație.
Fie $x,y \in G$. Atunci $\exists! z \in G$ cu $xz=y$, deci $x^{p-1}y=x^{p-1}(xz)=x^pz$. Cum f e surjectivă $\Rightarrow \exists u \in G$ cu $u^p=z$. Deci, cum f e morfism vom avea $x^{p-1}y=x^pz=x^pu^p=(xu)^p=x(ux)^{p-1}u=x(ux)^p(ux)^{-1}u=xu^px^px^{-1}u^{-1}u=xzx^px^{-1}=yx^{p-1}$, deci vom avea că $x^{p-1} \in Z(G), \forall x \in G$. □

Consecinţă. *Fie G un grup de ordin n. Dacă funcţia $f\colon G \to G, f(x)=x^p$ e un morfism surjectiv (deci, automorfism al lui G) şi $(n,p-1)=1$, atunci G e abelian.*

Demonstrație.
Fie $x \in G$. Din propoziţia anterioară rezultă că $x^{p-1} \in Z(G)$. Cum $x^n=e \in Z(G)$ şi cum $Z(G)$-grup, va rezulta că $x^{(n,p-1)}=x^1=x \in Z(G)$, iar cum pe x l-am ales arbitrar $\Rightarrow Z(G)=G$, adică G e abelian. □

Problema 1. Fie G un grup finit cu proprietatea că $x^p=e, \forall x \in G$ şi $y^2z^2=z^2y^2, \forall y,z \in G$, unde p e un număr prim impar. Demonstraţi că G e abelian.

Demonstrație.
Problema pare inatacabilă cu tehnici elementare, dar folosind **Propoziţia 1.** vom avea că $ord(G)=p^k$ şi cum p-impar $\Rightarrow (ord(G),2)=1$, deci funcţia $f\colon G \to G, f(x)=x^2$ este bijectivă.
Ipoteza se scrie $f(y)f(z)=f(z)f(y), \forall y,z \in G$, iar notând $f(y)$ cu u şi $f(z)$ cu v, vom avea că $uv=vu, \forall u,v \in \text{Im } f$, iar cum $\text{Im } f=G$ va rezulta că G e abelian. □

Problema 2. Fie G un grup comutativ de ordin impar. Arătaţi că produsul elementelor sale este egal cu e.

Demonstraţie.
Cum $(ord(G), 2) = 1$ vom avea că funcţia $f\colon G \to G, f(x) = x^2$ este bijectivă, aşadar $G = \text{Im } f = \{x^2 \mid x \in G\}$ şi cum G e abelian vom avea că $\prod\limits_{x\in G} x = \prod\limits_{x\in G} x^2 = (\prod\limits_{x\in G} x)^2$, deci $\prod\limits_{x\in G} = e$. □

Problema 3. Fie grupul G şi $n \in \mathbb{N}_{\geq 2}$ astfel încât funcţia $f\colon G \to G, f(x) = x^{n+1}$ este un automorfism al lui G. Demonstraţi că:

a) funcţia $g\colon G \to G, g(x) = x^n$ este un endomorfism a lui G;

b) dacă g e injectivă sau surjectivă, atunci G e abelian.

Gheorghe Andrei, OJM 1994

Demonstraţie.
Din **Propoziţia2.** şi ipoteză $\Rightarrow x^n \in Z(G), \forall x \in G$.

a) Din ipoteză $\Rightarrow (xy)^{n+1} = x^{n+1}y^{n+1}, \forall x, y \in G$, adică $x(yx)^n y = xx^n y^n y, \forall x, y \in G$, de unde $(yx)^n = x^n y^n = y^n x^n, \forall x, y \in G$, deci g e morfism.

b) Dacă g e injectivă, atunci din $(xy)^n = x^n y^n = y^n x^n = (yx)^n, \Rightarrow xy = yx, \forall x, y \in G$, deci G e abelian.
Dacă g e surjectivă, atunci $\forall y \in G, \exists z \in G$ cu $y = z^n \Rightarrow xy = xz^n = z^n x = yx, \forall x, y \in G$, deci G e abelian.

□

Problema 4. Fie G un grup comutativ cu n elemente. Pentru fiecare $k \in \mathbb{Z}$ definim $G_k = \{x^k \mid x \in G\}$. Dacă $a, b \in \mathbb{Z}$ şi $(a, b) = d$, arătaţi că $G_aG_b = G$ dacă şi numai dacă $(d, n) = 1$, unde $G_aG_b = \{u \cdot v \mid u \in G_a$ şi $v \in G_b\}$.

Dana Heuberger, Concursul „Nicolae Coculescu", 2010

Demonstraţie.
Universal demonstrăm următoarea: $G_aG_b = G_d$.
Fie $g \in G_aG_b$. Avem că $\exists (x, y) \in G^2$ cu $g = x^a \cdot y^b$, deci, cum $d|a$ şi $d|b$ vom avea $g = (x^{\frac{a}{d}})^d \cdot (y^{\frac{b}{d}})^d$ şi cum G-comutativ va rezulta că $g = (x^{\frac{a}{d}} \cdot y^{\frac{b}{d}})^d$ deci $g \in G_d, \forall g \in G_aG_b$, adică $G_aG_b \subset G_d$.
Ramâne să arătăm că $G_aG_b \supset G_d$.
Din $(a, b) = d \Rightarrow \exists s, t \in \mathbb{Z}$ cu $sa + tb = d$. Fie $h \in G_d$, atunci $\exists z \in G$ cu $h = z^d$, deci $h = z^{sa+tb} = (z^s)^a \cdot (z^t)^b$, aşadar h are forma $x^a \cdot y^b$, cu $x, y \in G$ $(x = z^s, y = z^t)$, deci $h \in G_aG_b, \forall h \in G_d$, adică $G_aG_b \supset G_d$, deci $G_aG_b = G_d$.
Revenim la problemă:
Ţinând cont de lemă, vom avea că funcţia $f\colon G \to G, f(x) = x^d$ e bijectivă (Im $f = G$) dacă şi numai dacă $(d, n) = 1$ iar cum $G_aG_b = G_d = \text{Im } f$ va rezulta $G_aG_b = G \Leftrightarrow (d, n) = 1$. □

Problema 5. Fie G un grup cu $ord(G) = 6k + 1, k \in \mathbb{N}$. Aflaţi numărul soluţiilor ecuaţiei $x^3 = y^2$ în G^2.

Soluţie.
Cum $(ord(G), 2) = (ord(G), 3) = 1$, funcţiile $f, g\colon G \to G, f(x) = x^3, g(x) = x^2$ vor fi bijective. Aşadar pentru orice $x_a \in G, \exists!(y_a, a) \in G^2$ cu $x_a^3 = y_a^2 = a$, deci numărul soluţiilor ecuaţiei $x^3 = y^2$ in G^2 este chiar $ord(G)$. □

Problema 6. Fie grupul G şi funcţia $f\colon G \to G, f(x) = x^3$. Arătaţi că dacă f e un endomorfism injectiv sau surjectiv al lui G, atunci G e abelian.

Demonstrație.
Din f-morfism $\Rightarrow (xy)^3 = x^3y^3$, deci $(yx)^2 = x^2y^2, \forall x, y \in G$
Dacă f e surjectivă, atunci din **Propoziția2.** vom avea că $t^2 \in Z(G), \forall t \in G$, deci vom avea $(yx)^2 = y^2x^2$ de unde va rezulta $xy = yx$, deci G e abelian.
Dacă f e injectivă, o serie de calcule ne dă că $(yx)^2 = x^2y^2 \Rightarrow (yx)^4 = (x^2y^2)^2 = y^4x^4 \Rightarrow (yx)^3yx = y^4x^4 \Rightarrow y^3x^3yx = y^4x^4 \Rightarrow x^3y = yx^3$, deci $x^3 \in Z(G), \forall x \in G$. Atunci avem $(xy)^3 = x^3y^3 = y^3x^3 = (yx)^3$ și din injectivitatea lui f iese că $xy = yx$, deci G e abelian. □

Problema 7. Fie G un grup de ordin p, cu $p \in \mathbb{N}_{\geq 3}$ astfel încât există $n \in \mathbb{Z}$ pentru care funcțiile $f, g\colon G \to G, f(x) = x^n$ și $g(x) = x^{n+2}$ sunt endomorfisme surjective ale lui G. Demonstrați că

a) Dacă p este impar, atunci G e abelian;

b) Dacă p e par, $p \neq 2^k (k \in \mathbb{N})$, atunci $|Z(G)| \geq 3$

Dana Heuberger

Demonstrație.
Din **Propoziția2.** și ipoteză vom avea că x^{n-1} și $x^{n+1} \in Z(G), \forall x \in G$.
Fie $d = (n-1, n+1)$, atunci $d \in \{1, 2\}$. Cum $Z(G)$ e grup $\Rightarrow x^{(n-1,n+1)} = x^d \in Z(G), \forall x \in G$

a) Cum $d \in \{1, 2\}$ și p-impar $\Rightarrow (d, p) = 1 \Rightarrow$ funcția $f\colon G \to G, f(x) = x^2$ e bijectivă, deci notând pe x^2 cu y vom avea că $y \in Z(G), \forall y \in$ Im $f = G$, deci $Z(G) = G$, adică G e abelian.

b) Din $2|p$ și Teorema lui Cauchy $\Rightarrow \exists a \in G$ cu $ord(a) = 2$. Din $p \neq 2^k \Rightarrow \exists q$-prim impar cu $q|p$, și din nou, din Teorema lui Cauchy $\Rightarrow \exists b \in G$ cu $ord(b) = q$.
Dacă n-par $\Rightarrow d = 1 \Rightarrow Z(G) = G \Rightarrow |Z(G)| \geq 3$.
Dacă n-impar $\Rightarrow d = 2 \Rightarrow x^2 \in Z(G), \forall x \in G$, deci și $b^2 \in Z(G)$, iar cum $b^q = e \in Z(G)$ și $Z(G)$ e grup $\Rightarrow b^{(2,q)} = b \in Z(G)$.
Demonstrăm că și $a \in Z(G)$: din f-morfism $\Rightarrow (ax)^n = a^nx^n = ax^n$, iar din g-morfism $\Rightarrow (ax)^{n+2} = a^{n+2}x^{n+2} = ax^{n+2}$, iar cum $(ax)^{n+2} = (ax)^2(ax)^n$, folosind relațiile de mai sus va rezulta $axaxax^n = ax^{n+2}$, deci $xaxa = x^2$, de unde $axa = x$, și cum a este propriul său invers $\Rightarrow ax = xa, \forall x \in G$, adică $a \in Z(G)$.
Așadar $\{e, a, b\} \subset Z(G)$ și cum $e \neq a \neq b \neq e \Rightarrow |Z(G)| \geq 3$.

□

References

[1] Dana Heuberger, Vasile Pop, Matematică de excelență, pentru concursuri, olimpiade și centre de excelență. Editura Paralela 45, Pitești, România, 2014.

[2] Lucian-Georges Lăduncă, BORNE PENTRU MATEMATICIENI, Algebră-Analiză, Clasele IX-XII, Editura TAIDA, Iași, România, 2010.