GAZETA MATEMATICĂ

SERIA B

PUBLICAŢIE LUNARĂ PENTRU TINERET

Fondată în anul 1895

Anul CXIX nr. 3 **martie 2014**

ARTICOLE ŞI NOTE MATEMATICE

O PROPRIETATE A INELELOR CU UN NUMĂR IMPAR DE ELEMENTE

Ioan Băetu[1)]

Abstract. This article establishes some relations between the number of idempotent elements, the number of invertible elements and the number of nilpotent elements of a finite commutative ring with an odd number of elements.

Keywords: commutative finite ring, idempotent element, invertible element.

MSC : 13M99.

Problema 3 de la Olimpiada Judeţeană de Matematică din anul 2008, clasa a XII-a, autor *Mihai Piticari*, a fost următoarea:

Fie A un inel comutativ cu un număr impar de elemente. Dacă n este numărul soluţiilor ecuaţiei $x^2 = x$, $x \in A$, iar m este numărul elementelor inversabile ale inelului A, să se arate că n divide m.

În continuare vom prezenta o generalizare a acestui rezultat şi câteva consecinţe.

Peste tot, inelele le vom considera finite, cu un număr impar de elemente şi comutative. Fireşte, dacă A este un astfel de inel, nenul, iar n este ordinul elementului 1 în grupul aditiv $(A, +)$, rezultă n divide $\text{ord}(A)$, de unde $n \geq 3$. Mai mult, se ştie că subgrupul generat de elementul 1 în grupul aditiv $(A, +)$ este chiar un subinel al inelului A, izomorf cu $\mathbb{Z}_n$. Prin identificare putem presupune, făcând abstracţie de un izomorfism, că $\mathbb{Z}_n \subseteq A$ şi $\mathbb{Z}_n$ este un subinel al inelului A. În felul acesta $0 = \widehat{0} \in \mathbb{Z}_n$ este elementul nul iar $1 = \widehat{1} \in \mathbb{Z}_n$ este elementul unitate al inelului A.

Întrucât inelul A este comutativ, $U_2 = \{x \in A \mid x^2 = \widehat{1}\}$ este un subgrup al grupului multiplicativ $U(A)$ al elementelor inversabile ale inelului A.

[1)]Profesor, Colegiul Naţional „Mihai Eminescu“, Botoşani

Deoarece $\widehat{1} \neq -\widehat{1}$, rezultă $\text{ord}(U_2) \geq 2$. Fie p un divizor prim al $\text{ord}(U_2)$. Din teorema lui *Cauchy*, există $a \in U_2$ astfel încât $\text{ord}(a) = p$. Cum $a \in U_2$, rezultă $a^2 = \widehat{1}$, de unde p divide 2. Dar p este prim, deci $p = 2$. Aşadar 2 este singurul divizor prim al $\text{ord}(U_2)$, adică există $k \in \mathbb{N}^*$ pentru care $\text{ord}(U_2) = 2^k$. Să notăm

$$I_{a,b}(A) = \{x \in A \mid (x-a)(x-b) = \widehat{0}\}, \quad a, b \in A.$$

Propoziţia 1. *Dacă* $a^2 - b^2 \in U(A)$, *atunci* $\text{card}(I_{a,b}(A)) = \text{ord}(U_2)$.

Demonstraţie. Deoarece $a^2-b^2 = (a-b)(a+b)$ şi a^2-b^2 este inversabil, deducem că elementele $a-b$ şi $a+b$ sunt inversabile. Întrucât n este impar, rezultă $\widehat{2} \in U(\mathbb{Z}_n) \subseteq U(A)$. Fie

$$\alpha = 2(a-b)^{-1}, \quad \beta = -(a-b)^{-1}(a+b).$$

Pentru orice $x \in I_{a,b}(A)$, obţinem $x^2 = (a+b)x - ab$, de unde

$$\begin{aligned}(\alpha x + \beta)^2 &= \alpha^2 x^2 + 2\alpha\beta x + \beta^2 = \alpha^2\left((a+b)x - ab\right) + 2\alpha\beta x + \beta^2 = \\ &= \left(\alpha^2(a+b) + 2\alpha\beta\right)x + \beta^2 - ab\alpha^2 = \\ &= \left((a+b)\alpha + 2\beta\right)\alpha x + \beta^2 - ab\alpha^2.\end{aligned}$$

Dar $(a+b)\alpha + 2\beta = 2(a-b)^{-1}(a+b) - 2(a-b)^{-1}(a+b) = \widehat{0}$ şi $\beta^2 - ab\alpha^2 = (a-b)^{-2}(a+b)^2 - 4ab(a-b)^{-2} = (a-b)^{-2}\left((a+b)^2 - 4ab\right) = = (a-b)^{-2}(a-b)^2 = \widehat{1}$, de unde $(\alpha x + \beta)^2 = \widehat{1}$, $\forall x \in I_{a,b}(A)$. Prin urmare, $\alpha x + \beta \in U_2, \forall x \in I_{a,b}(A)$.

Deoarece α este inversabil, funcţia $\phi : I_{a,b}(A) \to U_2$, $\phi(x) = \alpha x + \beta$ este injectivă. Arătăm că ϕ este surjectivă. Într-adevăr, pentru orice $t \in U_2$, există $x = \alpha^{-1}(t-\beta) \in A$ astfel încât $\phi(x) = t$. Mai rămâne să probăm că $x = \alpha^{-1}(t-\beta) \in I_{a,b}(A)$. Avem

$$\begin{aligned}(x-a)(x-b) &= x^2 - (a+b)x + ab = \alpha^{-2}(t-\beta)^2 - (a+b)\alpha^{-1}(t-\beta) + ab = \\ &= \alpha^{-2}(\widehat{1} - 2\beta t + \beta^2) - \alpha^{-2}(a+b)(\alpha t - \alpha\beta) + ab = \\ &= \alpha^{-2}\left(\widehat{1} - 2\beta t + \beta^2 - \alpha t(a+b) + \alpha\beta(a+b)\right) + ab = \\ &= \alpha^{-2}\left(\widehat{1} - t\left(2\beta + (a+b)\alpha\right) + \beta\left(\beta + (a+b)\alpha\right)\right) + ab.\end{aligned}$$

Dar $2\beta + (a+b)\alpha = \widehat{0}$, de unde $\beta + (a+b)\alpha = -\beta$. Atunci

$$\begin{aligned}(x-a)(x-b) &= \alpha^{-2}(\widehat{1} - \beta^2) + ab = \widehat{2}^{-2}(a-b)^2(\widehat{1} - (a-b)^{-2}(a+b)^2) + ab = \\ &= \widehat{2}^{-2}[(a-b)^2 - (a+b)^2] + ab = -ab + ab = \widehat{0},\end{aligned}$$

adică $x \in I_{a,b}(A)$. Astfel, aplicaţia ϕ este surjectivă, deci bijectivă. Rezultă $\text{card}(I_{a,b}(A)) = \text{ord}(U_2)$, ceea ce încheie demonstraţia. □

Întrucât U_2 este un subgrup al grupului multiplicativ $U(A)$, conform teoremei lui *Lagrange*, $\text{ord}(U_2)$ divide $\text{ord}(U(A))$. Aşadar avem:

Consecinţă. *Dacă* $a, b \in A$ *astfel încât* $a^2 - b^2 \in U(A)$, *atunci* $\mathrm{card}(I_{a,b}(A))$ *divide* $\mathrm{ord}(U(A))$.

Păstrând notaţia de mai sus, în virtutea propoziţiei **1**) reiese că numărul elementelor mulţimii $I_{a,b}(A)$ nu depinde de alegerea elementelor a şi b. Cum $\widehat{0}^2 - \widehat{1}^2 = -\widehat{1} \in U(A)$, găsim $\mathrm{card}(I_{a,b}(A)) = \mathrm{card}(I_{\widehat{0},\widehat{1}}(A))$, unde

$$I_{\widehat{0},\widehat{1}}(A) = \{x \in A \mid x(x-\widehat{1}) = \widehat{0}\} = \{x \in A \mid x^2 = x\} \overset{\text{not}}{=} I(A)$$

reprezintă mulţimea elementelor idempotente ale inelului A. Notând cu m numărul elementelor idempotente ale inelului A, obţinem $m \geq 2$ şi m divide $\mathrm{ord}(U(A))$. Aşadar $2 \leq m \leq \mathrm{ord}(U(A))$.

În continuare ne propunem să studiem unele proprietăţi ale inelului A în cazurile $m = 2$ respectiv $m = \mathrm{ord}(U(A))$.

Propoziţia 2. *Fie* A *un inel cu* $\widehat{0} \in A$ *unicul element nilpotent şi* $a, b \in A$ *astfel încât* $a^2 - b^2 \in U(A)$. *Atunci următoarele afirmaţii sunt echivalente*:

i) A *este corp.*

ii) *Singurele soluţii ale ecuaţiei* $(x-a)(x-b) = \widehat{0}$, $x \in A$, *sunt* $x = a$ şi $x = b$.

Demonstraţie. Fie A un corp şi $x \in A$ astfel încât $(x-a)(x-b) = \widehat{0}$. Cum A nu are divizori ai lui zero, rezultă $x = a$ sau $x = b$.

Reciproc, să presupunem că $x \in A$ şi $(x-a)(x-b) = \widehat{0}$ implică $x = a$ sau $x = b$. Atunci $I_{a,b}(A) = \{a, b\}$, de unde $\mathrm{card}(I(A)) = 2$. Dar $\widehat{0}, \widehat{1} \in I(A)$, deci $I(A) = \{\widehat{0}, \widehat{1}\}$.

Fie acum $y \in A \backslash \{\widehat{0}\}$. Conform ipotezei, rezultă $y^r \in A \backslash \{\widehat{0}\}, \forall r \in \mathbb{N}^*$ şi, cum $A \backslash \{\widehat{0}\}$ este o mulţime finită, există $p, q \in \mathbb{N}^*$ cu $p < q$ şi $y^p = y^q$. Înmulţind succesiv cu y^{q-p}, ultima egalitate conduce la $y^{kq-(k-1)p} = y^q$, $\forall k \in \mathbb{N}^*$. Alegem $k \in \mathbb{N}^*$ astfel încât $t = kq - (k-1)p > 2q$. Înmulţind acum egalitatea $y^q = y^t$cu y^{t-2q}, găsim $y^{t-q} = y^{2(t-q)}$. Notând cu $z = y^{t-q}$, obţinem $z^2 = z$, de unde $z \in I(A)$. Dar $z \neq \widehat{0}$, deci $z = \widehat{1}$. Prin urmare $y^{t-q} = \widehat{1}$, adică y este inversabil, $\forall y \in A \backslash \{\widehat{0}\}$.

Propoziţia 3. *Dacă numărul elementelor idempotente ale inelului* A *coincide cu numărul elementelor inversabile, atunci inelul* A *nu are elemente nilpotente nenule.*

Demonstraţie. Cum $U_2 \subseteq U(A)$ şi $\mathrm{ord}(U_2) = \mathrm{card}(I(A)) = \mathrm{ord}(U(A))$, rezultă $U(A) = U_2$.

Notăm cu n caracteristica inelului A. Din $\widehat{2} \in U(\mathbb{Z}_n) \subseteq U(A)$, găsim $\widehat{2}^2 = \widehat{1}$. Astfel $\widehat{3} = \widehat{0}$, de unde $n = 3$.

Să presupunem acum că există un element $x \in A \backslash \{\widehat{0}\}$ şi un număr $k \in \mathbb{N}$, $k \geq 2$, astfel încât $x^k = \widehat{0}$. Fie p cel mai mic număr din $\mathbb{N}^*$pentru care $x^p = \widehat{0}$. Atunci $p \geq 2$ şi $x^{p-1} \neq \widehat{0}$. Fie $y = x^{p-1}$. Din $y^2 = x^{2p-2} = x^p x^{p-2} = \widehat{0}$

rezultă $(\widehat{1}-y)^3=\widehat{1}-y^3=\widehat{1}$, de unde $\widehat{1}-y\in U(A)$. Dar $U(A)=U_2$, deci $(\widehat{1}-y)^2=\widehat{1}$. Astfel $\widehat{1}-y=(\widehat{1}-y)^3(\widehat{1}-y)^{-2}=\widehat{1}$, adică $y=\widehat{0}$, contradicţie. În definitiv, inelul A nu are elemente nilpotente nenule. □

Desigur, interesează un exemplu de inel de caracteristică 3 ce verifică condiţiile propoziţiei **3**. Un astfel de exemplu este inelul $\mathbb{Z}_3\times\mathbb{Z}_3$, în care avem patru elemente idempotente: $(\widehat{0},\widehat{0})$, $(\widehat{0},\widehat{1})$, $(\widehat{1},\widehat{0})$, $(\widehat{1},\widehat{1})$ şi patru elemente inversabile: $(\widehat{1},\widehat{1})$, $(\widehat{1},\widehat{2})$, $(\widehat{2},\widehat{1})$, $(\widehat{2},\widehat{2})$. Un exemplu mai general este următorul.

Propoziţia 4. *Fie A un inel cu 9 elemente astfel încât $\widehat{1}+\widehat{1}+\widehat{1}=\widehat{0}$. Dacă A nu este corp şi $\widehat{0}\in A$ este unicul element nilpotent al inelului A, atunci numărul elementelor inversabile ale inelului A coincide cu numărul elementelor idempotente.*

Demonstraţie. Din ipoteză rezultă că A este un inel de caracteristică 3, deci $\mathbb{Z}_3\subseteq A$. Fie $\alpha\in A\backslash\mathbb{Z}_3$ un element neinversabil. Procedând ca în propoziţia **2**, rezultă că există un număr $k\in\mathbb{N}^*$ astfel încât $\alpha^k=\alpha^{2k}$.

Fie $\beta=\alpha^k$. Atunci β nu este inversabil şi $\beta^2=\beta$. Cum $\beta\neq\widehat{0}$, rezultă $\beta\in A\backslash\mathbb{Z}_3$. Fie $\mathbb{Z}_3[\beta]=\{x+y\beta\mid x,y\in\mathbb{Z}_3\}\subseteq A$. Arătăm că aplicaţia $\phi:\mathbb{Z}_3\times\mathbb{Z}_3\to\mathbb{Z}_3[\beta]$, $\phi(x,y)=x+y\beta$ este injectivă. Într-adevăr, din $\phi(x_1,y_1)=\phi(x_2,y_2)$, cu $x_1,y_1,x_2,y_2\in\mathbb{Z}_3$, obţinem $x_1+y_1\beta=x_2+y_2\beta$, de unde $(y_1-y_2)\beta=x_2-x_1$.

Dacă $y_1\neq y_2$, atunci $\beta=(y_1-y_2)^{-1}(x_2-x_1)\in\mathbb{Z}_3$, contradicţie. Deci $y_1=y_2$ şi totodată $x_1=x_2$, adică ϕ este injectivă. Conform modului ei de definire, aplicaţia ϕ este şi surjectivă, deci bijectivă. Din $\mathbb{Z}_3[\beta]\subseteq A$ şi $\mathrm{card}(\mathbb{Z}_3[\beta])=\mathrm{card}(\mathbb{Z}_3\times\mathbb{Z}_3)=9=\mathrm{card}(A)$ găsim $\mathbb{Z}_3[\beta]=A$.

Astfel, pentru orice $z\in A$ putem scrie $z=x+y\beta$, cu $x,y\in\mathbb{Z}_3$, de unde $z^3=x^3+y^3\beta^3=x+y\beta=z$. Fireşte, pentru orice $z\in U(A)$ rezultă $z^2=z^3z^{-1}=zz^{-1}=\widehat{1}$, de unde $U(A)\subseteq U_2$. Dar $U_2\subseteq U(A)$, deci $U_2=U(A)$. Atunci $\mathrm{card}(I(A))=\mathrm{ord}(U_2)=\mathrm{ord}(U(A))$.

BIBLIOGRAFIE

[1] *Olimpiada de matematică 2008 – 2012*, Biblioteca Societăţii de Ştiinţe Matematice, Bucureşti.