Asupra rădăcinilor polinomului $X^3+pX+q\in\mathbb{Q}[X]$

Adrian REISNER[1]

I. Considerăm polinomul $P=X^3+pX+q\in\mathbb{Q}[X]$, având rădăcinile complexe α_1, α_2, α_3. Notăm, ca de obicei, cu ε rădăcina primitivă de ordin 3 a unităţii ($\varepsilon=-\frac{1}{2}+i\frac{\sqrt{3}}{2}=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$).

Propoziţia 1. *Pentru $\alpha,\beta\in\mathbb{C}$, următoarele afirmaţii sunt echivalente:*
(i) $3\alpha\beta=-p$ şi $P(\alpha+\beta)=0$;
(ii) α^3 şi p^3 sunt rădăcinile polinomului $Q=X^2+qX-\frac{p^3}{27}$.

Demonstraţie. Cum $P(\alpha+\beta)=\alpha^3+\beta^3+(3\alpha\beta+p)(\alpha+\beta)+q$, avem că

$$(i)\Leftrightarrow\left[\alpha^3+\beta^3+q=0,\ 3\alpha\beta=-p\right]\Leftrightarrow\left[\alpha^3+\beta^3=-q,\ \alpha^3\beta^3=-\frac{p^3}{27}\right]\Leftrightarrow(ii).$$

Consecinţa 1. *Dacă $\alpha,\beta\in\mathbb{C}$ satisfac (i) sau (ii), atunci rădăcinile polinomului P sunt $\alpha+\beta$, $\varepsilon\alpha+\varepsilon^2\beta$ şi $\varepsilon^2\alpha+\varepsilon\beta$.*

Demonstraţie. Dacă α şi β sunt rădăcinile cubice cu produs real ale celor două rădăcini ale polinomului Q, atunci perechile $\left(\varepsilon\alpha,\varepsilon^2\beta\right)$ şi $\left(\varepsilon^2\alpha,\varepsilon\beta\right)$ au aceleaşi proprietăţi, deci are loc (ii). Deducem că $P\left(\varepsilon\alpha+\varepsilon^2\beta\right)=P\left(\varepsilon^2\alpha+\varepsilon\beta\right)=0$, de unde concluzia.

Observaţie. Dacă $\Delta=q^2+\frac{4p^3}{27}$ este discriminantul polinomului Q atunci:

1) Dacă $\Delta>0$, atunci Q admite două rădăcini reale şi distincte, fie acestea A şi B. Notând cu $\alpha=\sqrt[3]{A}$, $\beta=\sqrt[3]{B}$ rădăcinile cubice reale, atunci $\alpha+\beta=\sqrt[3]{A}+\sqrt[3]{B}$ este unica rădăcină reală a lui P.

2) Dacă $\Delta=0$, atunci Q admite rădăcina reală dublă A. Notând $\alpha=\beta=\sqrt[3]{A}\in\mathbb{R}$, rădăcinile polinomului P vor fi $\alpha+\beta=2\sqrt[3]{A}$ şi $\varepsilon\alpha+\varepsilon^2\beta=\varepsilon^2\alpha+\varepsilon\beta=-\sqrt[3]{A}$ (rădăcină dublă), toate reale.

3) Dacă $\Delta<0$, atunci Q admite două rădăcini complexe conjugate A şi $\overline{A}$. Notând cu α una dintre rădăcinile cubice ale lui A şi cu β conjugatul lui α, rădăcinile lui P vor fi $\alpha+\overline{\alpha}$, $\varepsilon\alpha+\overline{\varepsilon\alpha}$ şi $\varepsilon^2\alpha+\overline{\varepsilon^2\alpha}$, toate reale.

II. În cele ce urmează, vom studia submulţimile lui $\mathbb{C}$ definite prin:

$$A_i=\mathbb{Q}(\alpha_i)=\{R(\alpha_i)\mid R\in\mathbb{Q}[X]\},\quad i=1,2,3;$$
$$A=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)=\{R(\alpha_1,\alpha_2,\alpha_3)\mid R\in\mathbb{Q}[X_1,X_2,X_3]\}.$$

Propoziţia 2. *În raport cu operaţiile de adunare şi înmulţire a numerelor complexe, A_i se structurează ca un corp comutativ. În plus, A_i este un $\mathbb{Q}$-spaţiu vectorial de dimensiune cel mult 3.*

Demonstraţie. Faptul că A_i este un inel integru, unitar şi $\mathbb{Q}$-spaţiu vectorial se verifică imediat. Dacă $R\in\mathbb{Q}[X]$, din teorema împărţirii cu rest rezultă că $R(X)=P(X)C(X)+\lambda+\mu X+\nu X^2$ şi, cum $P(\alpha_i)=0$, deducem că

$$A_i=\left\{\lambda+\mu\alpha_i+\nu\alpha_i^2\mid\lambda,\mu,\nu\in\mathbb{Q}\right\},$$

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

prin urmare $\left\{1, \alpha_i, \alpha_i^2\right\}$ constituie un sistem de generatori pentru $\mathbb{Q}$-spaţiul vectorial A_i; astfel , $\dim_{\mathbb{Q}} A_i \leq 3$. În sfârşit, pentru orice $a \in A_i \setminus \{0\}$, aplicaţiile liniare $A_i \to A_i$ definite prin $x \mapsto ax$ şi $x \mapsto xa$ sunt injective (A_i fiind integru), deci surjective (A_i fiind spaţiu vectorial de dimensiune finită) şi atunci există $a', a'' \in A_i$ pentru care $aa' = a''a = 1$. Urmează uşor că $a' = a''$, deci A_i este corp.

Propoziţia 3. *Mulţimea A se structurează canonic drept corp comutativ şi ca $\mathbb{Q}$-spaţiu vectorial de dimensiune cel mult* 6.

Demonstraţie. Cum $\alpha_1+\alpha_2+\alpha_3 = 0$, deducem că $A = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1)(\alpha_2)$. Dar α_2 este rădăcină a polinomului $\dfrac{P(X)}{X-\alpha_1} = X^2 + \alpha X + \left(\alpha_1^2 + p\right) \in A_1[X]$, prin urmare A va fi un A_1-spaţiu vectorial de dimensiune cel mult 2. Rezultă că $\dim_{\mathbb{Q}} A = \dim_{A_1} A \cdot \dim_{\mathbb{Q}} A_1 \leq 6$. Faptul că orice element nenul al lui A este inversabil se demonstrează ca în Propoziţia 2.

III. Automorfismele algebrei A.

Să observăm că orice endomorfism al spaţiului vectorial A cu proprietăţile că $u(1) = 1$, $u(xy) = u(x)\,u(y)$, $\forall x, y \in A$ este în mod necesar bijectiv: dacă $u(x) = 0$, cu $x \neq 0$, atunci $1 = u(1) = u\left(xx^{-1}\right) = u(x)\,u\left(x^{-1}\right) = 0$, contradicţie, deci u este injectiv, iar surjectivitatea urmează din faptul că $\dim A$ este finită.

Un astfel de endomorfism (de algebre) u va fi numit *automorfism*, iar mulţimea tuturor acestor automorfisme o vom nota $\operatorname{Aut} A$. În raport cu compunerea funcţiilor, $\operatorname{Aut} A$ se structurează în mod evident ca grup abelian.

Propoziţia 4. *În cazul în care P este un polinom reductibil peste $\mathbb{Q}$, atunci $\dim A \in \{1, 2\}$; mai mult există doi indici distincţi i, j astfel încât $A = A_i = A_j$. Dacă $\dim A = 1$, atunci $|\operatorname{Aut} A| = 1$, iar dacă $\dim A = 2$, atunci $|\operatorname{Aut} A| = 2$.*

Demonstraţie. Cum P este reductibil peste $\mathbb{Q}$, atunci toate cele trei rădăcini sunt raţionale şi atunci $A = A_1 = A_2 = A_3 = \mathbb{Q}$, iar $\dim_{\mathbb{Q}} A = 1$, sau o singură rădăcină, să zicem α_1, este raţională, caz în care $A_1 = \mathbb{Q}$, $A = A_2 = A_3$ este A_1-spaţiu vectorial de dimensiune 2, deci $\dim_{\mathbb{Q}} A = 2$.

Pentru orice $u \in \operatorname{Aut} A$ şi $x \in A$, avem că $u(x^n) = [u(x)]^n$, deci $u(R(x)) = R(u(x))$, $\forall R \in \mathbb{Q}[X]$. În particular, $P(u(\alpha_i)) = u(P(\alpha_i)) = u(0) = 0$, deci $\forall i \in \{1, 2, 3\}$, $\exists j \in \{1, 2, 3\}$ a. î. $u(\alpha_i) = \alpha_j$; altfel spus, un automorfism u realizează o permutare a rădăcinilor.

Dacă $\dim A = 1$, deci când $A = \mathbb{Q}$, atunci pentru orice $x \in A$ avem că $u(x) = u(x \cdot 1) = xu(1) = x$, deci $\operatorname{Aut} A = \{1_A\}$. Dacă $\dim A = 2$, fie $\alpha_i \in \mathbb{Q}$, $\alpha_2, \alpha_3 \notin \mathbb{Q}$, $\alpha_2 \neq \alpha_3$. Pentru $u \in \operatorname{Aut} A$ vom avea că $u(\alpha_1) = \alpha_1$. Dacă $u(\alpha_2) = \alpha_2$, $u(\alpha_3) = \alpha_3$, iar $x = y + z\alpha_2$, $y, z \in \mathbb{Q}$, este un element al lui A, atunci $u(x) = y + zu(\alpha_2) = x$, deci $u = 1_A$. Dacă $u(\alpha_2) = \alpha_3$, $u(\alpha_3) = \alpha_2$, atunci $u(x) = y + z\alpha_3$. Trebuie să avem $u(xx') = u(x)\,u(x')$, $\forall x, x' \in A$, ceea ce revine la $u\left(\alpha_2^2\right) = [u(\alpha_2)]^2$, iar această egalitate este realizată: am văzut în demonstraţia Propoziţiei 3 că α_2, α_3 sunt rădăcinile polinomului $X^2+\alpha_1 X+\left(\alpha_1^2+p\right) \in A_1[X]$, deci $\alpha_2^2 = -\alpha_1\alpha_2 - \alpha_1^2 - p$, prin urmare $u\left(\alpha_2^2\right) = -\alpha_1\alpha_3 - \alpha_1^2 - p = \alpha_3^2 = [u(\alpha_2)]^2$. Astfel, în acest caz avem că $\operatorname{Aut} A = \{1_A, u\}$.

Propoziţia 5. *Dacă P este ireductibil peste $\mathbb{Q}$, atunci:*

a) $\dim A \in \{3, 6\}$;

b) Dacă $\dim A = 6$ *şi* $u \in \operatorname{Aut} A$*, atunci există* $\sigma \in S_3$ *astfel încât* $u(\alpha_i) = \alpha_{\sigma(i)}$*,* $\forall i \in \{1,2,3\}$*, iar* $|\operatorname{Aut} A| = |S_3| = 6$*;*

c) Dacă $\dim A = 3$*, atunci* $|\operatorname{Aut} A| = 3$ *şi singurele elemente invariante pentru orice automorfism sunt elementele lui* $\mathbb{Q}$*.*

Demonstraţie. *a)* P fiind ireductibil, admite trei rădăcini distincte iraţionale (o eventuală rădăcină dublă ar anula P şi P', deci $(P, P') \in \mathbb{Q}[X]$ ar divide P, care astfel nu ar fi ireductibil). Cum α_i nu este rădăcină a unui polinom din $\mathbb{Q}[X]$ de grad ≤ 2, atunci $\left\{1, \alpha_i, \alpha_i^2\right\}$ este sistem liniar independent şi astfel $\dim_{\mathbb{Q}} A = 3$. Dacă $\alpha_2 \in A_1$, atunci $\alpha_3 = \alpha_1 - \alpha_2 \in A_1$, deci $A = A_1 = A_2 = A_3$ şi $\dim_{\mathbb{Q}} A = 3$. Dacă $\alpha_2 \notin A_1$, atunci $\dim_{A_1} A = 2$, deci $\dim_{\mathbb{Q}} A = \dim_{A_1} A \cdot \dim_{\mathbb{Q}} A_1 = 6$.

b) Dacă $\dim_{\mathbb{Q}} A = 6$, o bază a lui A fiind $\left\{1, \alpha_1, \alpha_1^2, \alpha_2, \alpha_1\alpha_2, \alpha_1^2\alpha_2\right\}$ (v. Propoziţia 3), înseamnă că un automorfism u este bine determinat prin cunoaşterea elementelor $u(\alpha_1)$ şi $u(\alpha_2)$, pentru că u realizează şi aici o permutare a rădăcinilor lui P (v. Propoziţia 4). Din comportarea lui u faţă de bază, rezultă că

$$u(1) = 1,\ u\left(\alpha_1^2\right) = \left[u(\alpha_1)\right]^2,\ u(\alpha_1\alpha_2) = u(\alpha_1)\,u(\alpha_2),\ u\left(\alpha_1^2\alpha_2\right) = \left[u(\alpha_1)\right]^2 u(\alpha_2);$$

aceste condiţii sunt suficiente pentru a demonstra că u este automorfism al lui A. Mai întâi, să arătăm că u este automorfism al lui A_1: o bază a acestui spaţiu fiind $\left\{1, \alpha_1, \alpha_1^2\right\}$, ar fi destul să arătăm că $u\left(\alpha_1^3\right) = \left[u(\alpha_1)\right]^3$ şi $u\left(\alpha_1^4\right) = \left[u(\alpha_1)\right]^4$. Într-adevăr, avem:

$$u\left(\alpha_1^3\right) = u\left(-p\alpha_1 - q\right) = -pu(\alpha_1) - q = \left[u(\alpha_1)\right]^3;$$
$$u\left(\alpha_1^4\right) = u\left(-p\alpha_1^2 - q\alpha_1\right) = -p\left[u(\alpha_1)\right]^2 - qu(\alpha_1) = \left[u(\alpha_1)\right]^4.$$

Fie acum $x = y + z\alpha_2$, $x' = y' + z'\alpha_2$, cu $y, z, y', z' \in A_1$; trebuie să verificăm că $u(xx') = u(x)\,u(x')$. Cum această proprietate are loc dacă $x \in A_2$ sau $x' = \alpha_2$, rămâne să justificăm că $u\left(\alpha_2^2\right) = \left[u(\alpha_2)\right]^2$. Avem:

$$\alpha_2^2 = -\alpha_1\alpha_2 - \alpha_1^2 - p \Rightarrow u\left(\alpha_2^2\right) = -\alpha_2\alpha_3 - \alpha_2^2 - p = \alpha_3^2 = \left[u(\alpha_2)\right]^2,$$

dat fiind că α_3 este rădăcină pentru $\dfrac{P(X)}{X - \alpha_2} = X^2 + \alpha X + \left(\alpha_2^2 + p\right)$ caz în care permutatrea asociată lui u este $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Obţinem astfel toate automorfismele lui A ca fiind asociate câte unei permutări din S_3, deci $|\operatorname{Aut} A| = |S_3| = 6$.

c) Conform celor demonstrate la *a)*, dacă $\dim A = 3$, atunci $A = A_1 = A_2 = A_3$, baze a lui A fiind $\left\{1, \alpha_i, \alpha_i^2\right\}$, $i = 1, 2, 3$. Fie $u \in \operatorname{Aut} A$. Dacă există i astfel încât $u(\alpha_i) = \alpha_i$, atunci u invariază toate elementele unei baze, deci $u = 1_A$. Dacă $u \neq 1_A$, avem că $u(\alpha_1) = \alpha_2$ şi $u\left(\alpha_1^2\right) = \alpha_2^2$ sau $u(\alpha_1) = \alpha_3$ şi $u\left(\alpha_1^2\right) = \alpha_3^2$. Aceste automorfisme u sunt astfel unic determinate, deci $|\operatorname{Aut} A| = 3$ (automorfismele sunt asociate ciclurilor de lungime 3 din S_3).

Căutăm acum elementele invariante pentru orice automorfism. Dacă $x = x_1 + x_2\alpha_1 + x_3\alpha_1^2 \in A$, atunci pentru $u \neq 1_A$ avem că $u(x) = x_1 + x_2\alpha_2 + x_3\alpha_2^2$ şi $u^2(x) = x_1 + x_2\alpha_3 + x_3\alpha_3^2$. Egalitatea $x = u(x) = u^2(x)$ conduce, după calcule, la $x_2 + x_3(\alpha_2 + \alpha_1) = 0$, $x_2 + x_3(\alpha_3 + \alpha_1) = 0$. Dacă x_2 şi x_3 nu sunt ambele nule, atunci $\alpha_2 + \alpha_1 = \alpha_3 + \alpha_1$, deci $\alpha_2 = \alpha_3$, absurd. Rezultă că singurele elemente invariante pentru orice automorfism sunt elementele lui $\mathbb{Q}$.