O NOUĂ SOLUŢIE A UNEI PROBLEME DIN VECHEA GAZETĂ MATEMATICĂ

Marcel Ţena[1)]

Profesorului D. M. Bătineţu-Giurgiu,
vechi colaborator al Gazetei Matematice,
la împlinirea vârstei de 80 de ani.

Abstract. A new solution for an 110 year old problem of this revue is presented, using some higher algebra considerations

Keywords: minimal polynomial, Galois extension

MSC : 12F10

Problema 1106 din Gazeta Matematică volumul XI (1906) are următorul enunţ:

Să se găsească forma generală a ecuaţiilor algebrice cu coeficienţi raţionali şi ireductibile ale căror rădăcini să se exprime raţional în raport cu una sau mai multe din rădăcinile ecuaţiei $x^5 - 1 = 0$.

A.G. Ioachimescu

Soluţie. Deoarece rădăcinile ecuaţiei $x^5 - 1 = 0$ sunt $1, \zeta, \zeta^2, \zeta^3, \zeta^4$, unde $\zeta = \cos\dfrac{2\pi}{5} + \mathrm{i}\sin\dfrac{2\pi}{5}$ şi pentru că orice funcţie raţională de aceste rădăcini este un element al corpului ciclotomic $\mathbb{Q}(\zeta)$, rezultă că rădăcinile ecuaţiilor pe care le căutăm sunt elemente din acest corp. Să căutăm, aşadar, polinoamele ireductibile monice din inelul $\mathbb{Q}[X]$, având rădăcinile în corpul $\mathbb{Q}(\zeta)$.

Acestea sunt *polinoamele minimale ale elementelor din* $\mathbb{Q}(\zeta)$.

Într-adevăr, orice polinom minimal al unui element $\alpha \in \mathbb{Q}(\zeta)$ este ireductibil în $\mathbb{Q}[X]$ şi, având o rădăcină $\alpha \in \mathbb{Q}(\zeta)$, are toate rădăcinile în $\mathbb{Q}(\zeta)$,

[1)]Prof. dr., Colegiul Naţional „Sf. Sava“, Bucureşti.

căci extinderea ciclotomică $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ este normală. Reciproc, dacă un polinom ireductibil din $\mathbb{Q}[X]$ are toate rădăcinile în corpul $\mathbb{Q}(\zeta)$, el este polinomul minimal pentru oricare din rădăcinile sale.

Fie $f \in \mathbb{Q}[X]$ polinomul minimal al elementului $\alpha \in \mathbb{Q}(\zeta)$. Avem extinderile de corpuri $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$. Cum $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(5) = 4$, rezultă, din relaţia gradelor, că $\mathrm{grad}(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ este un divizor al lui 4, adică vom avea $\mathrm{grad}(f) \in \{1, 2, 4\}$.

Considerăm, aşadar, următoarele trei cazuri:

1) $\mathrm{grad}(f) = 1$. Atunci $f = X - a$, cu $a \in \mathbb{Q}$.

2) $\mathrm{grad}(f) = 2$. Atunci extinderea $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ are gradul 2.

Dar $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ este o extindere *Galois* cu grupul lui *Galois* ciclic, izomorf cu $U(\mathbb{Z}_5) = \mathbb{Z}_5^*$, deci un grup ciclic de ordinul 4.

Acest grup are un singur subgrup propriu, prin urmare între $\mathbb{Q}$ şi $\mathbb{Q}(\zeta)$ există un singur subcorp intermediar propriu datorită teoremei fundamentale din teoria lui *Galois* şi acest subcorp este:

$$\mathbb{Q}\left(\zeta + \zeta^{-1}\right) = \mathbb{Q}(2\mathrm{Re}\zeta) = \mathbb{Q}\left(2\cos\frac{2\pi}{5}\right) = \mathbb{Q}\left(\frac{\sqrt{5}-1}{2}\right) = \mathbb{Q}\left(\sqrt{5}\right).$$

Prin urmare, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{5}\right)$, deci $\alpha \in \mathbb{Q}\left(\sqrt{5}\right)$, adică $\alpha = u + v\sqrt{5}$, cu $u, v \in \mathbb{Q}$, $v \neq 0$. Atunci, polinomul minimal al lui α este:

$$\begin{aligned} f &= \left(X - u - v\sqrt{5}\right)\left(X - u + v\sqrt{5}\right) = \\ &= X^2 - 2uX + u^2 - 5v^2, \quad u \in \mathbb{Q}, \quad v \in \mathbb{Q}^*. \end{aligned} \tag{1}$$

Prin urmare, polinoamele f căutate, de gradul 2, au forma (1).

3) $\mathrm{grad}(f) = 4$.

Deoarece $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ şi $\zeta^5 = 1$ avem $\zeta^4 = -(1 + \zeta + \zeta^2 + \zeta^3)$ şi $\zeta^{-1} = \zeta^4$. Mulţimea $B = \{1, \zeta, \zeta^2, \zeta^3\}$ este o bază a extinderii ciclotomice $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$, deci orice element $\alpha \in \mathbb{Q}(\zeta)$ are o scriere unică

$$\alpha = a + b\zeta + c\zeta^2 + d\zeta^3, \; a, b, c, d \in \mathbb{Q}. \tag{2}$$

Să vedem cum arată elementele subcorpului $\mathbb{Q}(\sqrt{5})$ în scrierea (2). Deoarece $\zeta + \zeta^{-1} = 2\cos\frac{2\pi}{5} = 2 \cdot \frac{\sqrt{5}-1}{4} = \frac{\sqrt{5}-1}{2}$, rezultă

$$\sqrt{5} = 1 + 2\zeta + 2\zeta^{-1} = 1 + 2\zeta + 2\zeta^4 = 1 + 2\zeta + 2(-1 - \zeta - \zeta^2 - \zeta^3) = -1 - 2\zeta^2 - 2\zeta^3,$$

deci $\alpha \in \mathbb{Q}(\sqrt{5}) \Leftrightarrow \alpha = u + v\sqrt{5} = u + v(-1 - 2\zeta^2 - 2\zeta^3) = a + c\zeta^2 + c\zeta^3$, cu $a, c \in \mathbb{Q}$. Aşadar, un element α scris sub forma (2) este în subcorpul $\mathbb{Q}(\sqrt{5})$ dacă şi numai dacă $b = 0$ şi $c = d$. Negând, un element $\alpha \in \mathbb{Q}(\zeta) \backslash \mathbb{Q}(\sqrt{5})$ dacă şi numai dacă $b \neq 0$ sau $c \neq d$ şi acestea sunt elementele al căror polinom minimal este ireductibil de gradul 4. Să vedem cum arată efectiv un astfel de polinom ireductibil de gradul 4.

Notăm cu G grupul *Galois* al extinderii $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$. Un automorfism $\sigma \in G$ invariază mulţimea rădăcinilor primitive de grad 5 ale unităţii şi atunci este determinat de valoarea $\sigma(\zeta) \in \{\zeta, \zeta^2, \zeta^3, \zeta^4\}$.

Prin urmare, $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, unde

$\sigma_1(\zeta) = \zeta$ $(\sigma_1 = 1_{\mathbb{Q}(\zeta)})$; $\sigma_2(\zeta) = \zeta^2$; $\sigma_3(\zeta) = \zeta^3$; $\sigma_4(\zeta) = \zeta^4$.

Conjugatele unui element $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3 \in \mathbb{Q}(\zeta)$, cu $b \neq 0$ sau $c \neq d$ sunt:

$$\begin{aligned}
&\alpha_1 = \sigma_1(\alpha) = \alpha = a + b\zeta + c\zeta^2 + d\zeta^3;\\
&\alpha_2 = \sigma_2(\alpha) = a + b\zeta^2 + c\zeta^4 + d\zeta^6 = a + b\zeta^2 - c(1 + \zeta + \zeta^2 + \zeta^3) + d\zeta =\\
&\quad = (a - c) + (d - c)\zeta + (b - c)\zeta^2 - c\zeta^3;\\
&\alpha_3 = \sigma_3(\alpha) = a + b\zeta^3 + c\zeta^6 + d\zeta^9 = a + b\zeta^3 + c\zeta + d\zeta^4 =\\
&\quad = a + b\zeta^3 + c\zeta - d(1 + \zeta + \zeta^2 + \zeta^3) = (a - d) + (c - d)\zeta - d\zeta^2 + (b - d)\zeta^3;\\
&\alpha_4 = \sigma_4(\alpha) = a + b\zeta^4 + c\zeta^8 + d\zeta^{12} = a - b(1 + \zeta + \zeta^2 + \zeta^3) + c\zeta^3 + d\zeta^2 =\\
&\quad = (a - b) - b\zeta + (d - b)\zeta^2 + (c - b)\zeta^3.
\end{aligned}$$

Atunci, polinomul minimal $f \in \mathbb{Q}[X]$ al lui α, descompus în factori liniari, în inelul $\mathbb{C}[X]$, este:

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4) = \prod_{i=1}^{4}(X - \sigma_i(\alpha)). \tag{3}$$

Comentarii. Prima soluţie a problemei a fost dată în G. M. vol. XIV (2/1908) de studenţii *N. Praporgescu* şi *D. Georgescu.*

Traian Lalescu dă o altă soluţie în G.M.vol.XIV(3/1908), bazată pe teoria lui *Galois*, indicând şi o generalizare, punând în locul lui 5 un număr prim p oarecare.

Prin metoda sa, *Traian Lalescu* obţine că polinoamele ireductibile de gradul 2 sunt de forma :

$$f = (X-a)^2+c(X-a)-c^2 = X^2-(2a-c)X+a^2-ac-c^2,\ a, c \in \mathbb{Q}, c \neq 0. \tag{4}$$

Punând $a = u + v$, $c = 2v$ ($\Leftrightarrow u = a - \dfrac{c}{2}$, $v = \dfrac{c}{2}$), obţinem

$f = X^2 - 2uX + u^2 - 5v^2$, adică formele (1) şi (4) sunt echivalente.

De asemenea *Traian Lalescu* obţine, prin metoda sa, faptul că elementele α din (2) al căror polinom minimal este de gradul 2 sunt cele cu $b = 0$ şi $c = d$.

Bibliografie

[1] A. G. Ioachimescu, *Problema 1106*, G.M. vol. XI (1906).
[2] T. Lalescu, *O problemă de algebră*, G. M. vol.XIV (1908), 3.