Matemática Universitária Nº 16, julho de 1994, 60-66

Sobre Solubilidade por Radicais Reais

Carlos Gustavo Tamm de Araujo Moreira

Introdução

Em um artigo publicado na Matemática Universitária nº 12 entitulado "Um teorema sobre solubilidade de equações polinomiais por radicais reais" ([3]) foi provado que se um polinômio $f(x) \in \mathbf{Q}[x]$ tem todas as suas raízes reais e solúveis por radicais reais então $|\,\mathrm{Gal}(f)\,|$ é uma potência de 2, e vale a recíproca. Nesse caso podemos concluir que as raízes de f são solúveis por raízes quadradas. Em particular deduzimos que se p e q são inteiros e $\cos\left(\frac{p\pi}{q}\right)$ é solúvel por radicais reais, então $\cos\left(\frac{p\pi}{q}\right)$ é solúvel por raízes quadradas, caso em que q se fatora como produto de uma potência de 2 por primos de Fermat (da forma $2^{2^k}+1$) distintos.

No artigo citado foi sugerida a definição de solubilidade por radicais reais para números complexos que será usada neste artigo: dizemos que $z = a + bi$ ($a \in \mathbf{R}$ e $b \in \mathbf{R}$) é solúvel por radicais reais se suas partes real e imaginária a e b o forem. Isso equivale a dizer que uma extensão $K \mid \mathbf{Q}$ é solúvel por radicais reais se houver uma torre radical $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n \subset L_{n+1}$, com $K \subset L_{n+1} = L_n(i)$, $L_n \subset \mathbf{R}$ (portanto $L_n = L_{n+1} \cap \mathbf{R}$), e $L_{k+1} = L_k(\alpha_k)$, com $P_{\alpha_k \mid L_k} = X^{p_k} - \alpha_k^{p_k}$, $\alpha_k^{p_k} \in L_k$ e p_k primo. Neste artigo provaremos que se $K \mid \mathbf{Q}$ é uma extensão normal solúvel por radicais reais (não supomos $K \subset \mathbf{R}$) e p é um primo que divide $[K : \mathbf{Q}]$ então $p = 2$ ou p é primo de Fermat.

O resultado principal do artigo anterior pode ser encontrado num livro de Tschebotarör e Schwerdtfeger [4], e como um problema de uma lista de exercícios do Prof. W. D. Geyer, na qual também se encontra o seguinte problema, relacionado com solubilidade por radicais reais: Se $f(x) \in \mathbf{Q}[x]$ é um polinômio

irredutível de grau ímpar com uma raiz real α solúvel por radicais reais então α é a única raiz real de f. Neste artigo apresentaremos também uma prova desse resultado. A demonstração do 1° resultado será baseada num lemà que afirma que se $K \mid \mathbf{Q}$ está contido em uma torre radical $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n$ $(K \subset L_n)$ e $K \mid \mathbf{Q}$ é normal então L_n contém as raízes p-ésimas da unidade para todo primo p que divida $[K : \mathbf{Q}]$, resultado que continua válido se substituímos $\mathbf{Q}$ por um corpo qualquer. Deste lema seguirá também o resultado central do artigo anterior, o que torna este artigo independente do outro.

Seção I: Solubilidade por radicais reais e extensões normais

Lema. *Suponha que* $K \mid \mathbf{Q}$ *seja normal e que exista uma torre radical* $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n$, *com* $L_{k+1} = L_k(\alpha_k)$, *com* $P_{\alpha_k \mid L_k} = X^{p_k} - \alpha_k^{p_k}$, p_k *primo para* $k = 0,1, \ldots, n-1$, *com* $K \subset L_n$. *Então, para qualquer primo p que divida* $[K : \mathbf{Q}]$ *temos* $e^{2\pi i/p} \in L_n$.

Demonstração. Seja p um primo que divida $[K : \mathbf{Q}]$. Tome $H < \mathrm{Gal}(K \mid \mathbf{Q})$ com $|H| = p$ (tal H existe pelo 1° teorema de Sylow. Veja [2], pág. 159). Seja $M = \mathrm{Fix}(H)$. Temos assim $K \mid M$ normal de grau p. Considere os corpos $N_i = L_i \cdot M$, $0 \le i \le n$. Seja r tal que $K \not\subset N_r$ mas $K \subset N_{r+1}$, e seja $\gamma \in K \setminus M$. Temos $K = M(\gamma)$, pois $[K : M]$ é primo, e portanto não há corpos entre M e K.

Seja $P_{\gamma \mid M} = (X - \gamma_1)(X - \gamma_2) \ldots (X - \gamma_p)$ onde $\gamma_1 := \gamma$. Temos $\gamma_i \in N_{r+1} \setminus N_r$, $1 \le i \le p$, pois se $\gamma_i \in N_r$, $M(\gamma_i) \subset N_r \Rightarrow K \subset N_r$, absurdo. Portanto, $N_{r+1} = N_r(\gamma_i)$, $1 \le i \le p$, pois $[N_{r+1} : N_r] = p_r$, que é primo, donde não há corpos

entre N_r e N_{r+1} (a afirmação $[N_{r+1} : N_r] = p_r$ vale pois $N_{r+1} = N_r(\alpha_r)$ onde α_r satisfaz à equação $X^{p_r} - \alpha_r^{p_r} = 0$, $\alpha_r^{p_r} \in L_r \subset N_r$, $N_{r+1} \neq N_r$, usando aqui o fato de que um polinômio do tipo $X^q - \alpha$ com q primo ou é irredutível ou tem raiz (veja [1], pág. 125)). Definimos uma relação de equivalência em $\{\gamma_1, \gamma_2 \dots, \gamma_{p_r}\}$ por $\gamma_i \equiv \gamma_j \Leftrightarrow \gamma_i$ é conjugado a γ_j sobre N_r. As classes de equivalência têm $[N_{r+1} : N_r] = p_r$ elementos cada. Portanto, p_r divide $p \Leftrightarrow p_r = p$. Como $N_{r+1} = N_r(\gamma)$ e os conjugados γ_i de γ pertencem a $K \subset N_{r+1}$, temos que $N_{r+1} \mid N_r$ é normal. Assim, os conjugados de α_r sobre N_r têm que estar em $N_{r+1} \Rightarrow \alpha_r, e^{2\pi i/p} \cdot \alpha_r \in N_{r+1} \Rightarrow e^{2\pi i/p} = (e^{2\pi i/p}\alpha_r)/\alpha_r \in N_{r+1} \subset L_n$.

Teorema I.1. *Se $K \mid \mathbf{Q}$ é normal e existe uma torre radical $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbf{R}$ tal que $K \subset L_n$ então $[K : \mathbf{Q}]$ é uma potência de 2.*

Demonstração: Suponha que exista um primo ímpar p que divida $[K : \mathbf{Q}]$. Então, pelo lema, devemos ter $e^{2\pi i/p} \in L_n \subset \mathbf{R}$, absurdo.

Corolário I.1. *Se p e q são inteiros e $mdc(p,q) = 1$ então $\cos\left(\frac{2\pi p}{q}\right)$ é solúvel por radicais reais se e só se q é produto de uma potência de 2 por primos de Fermat distintos.*

Demonstração: $\mathbf{Q}(\cos(\frac{2\pi \cdot p}{q})) = \mathbf{Q}(\xi) \cap \mathbf{R}$, onde $\xi = e^{2\pi i/p}$ é uma raiz q-ésima primitiva da unidade (pois $\mathbf{Q}(\xi) = \mathbf{Q}(\xi^p)$ e $\cos(\frac{2\pi \cdot p}{q}) = \frac{1}{2}(\xi^p + \xi^{-p})$), ou seja, $\mathbf{Q}(\cos(\frac{2\pi p}{q})) = \mathrm{Fix}(\sigma)$ onde $\sigma \in \mathrm{Gal}(\mathbf{Q}(\xi) \mid \mathbf{Q})$ é a conjugação complexa, e $(\sigma) = \{id, \sigma\}$. Como $\mathrm{Gal}(\mathbf{Q}(\xi) \mid \mathbf{Q}) \approx (\mathbf{Z}/q\mathbf{Z})^*$ é abeliano, toda subextensão de $\mathbf{Q}(\xi) \mid \mathbf{Q}$ é normal $\Rightarrow \mathbf{Q}(\cos(\frac{2\pi \cdot p}{q})) \mid \mathbf{Q}$ é normal e está contida em $\mathbf{R}$. Se for solúvel por radicais reais, devemos ter $[\mathbf{Q}(\cos(\frac{2\pi \cdot p}{q})) : \mathbf{Q}]$ potência de $2 \Rightarrow [\mathbf{Q}(\xi) : \mathbf{Q}]$ é potência de $2 \Leftrightarrow \varphi(q)$ é potência de 2, onde φ é a função de Euler, o que equivale a q ser produto de uma potência de 2 por primos de Fermat distintos (ver capítulo 10 de [1]). Para a recíproca, ver capítulo 10 de [1].

Obs.: Vale a recíproca do Teorema I.1. Na verdade, se $K \mid \mathbf{Q}$ for normal e $[K : Q]$ for potência de 2 então os elementos de K são solúveis por raízes

quadradas (e construtíveis com régua e compasso). Ver Capítulo 10 de [1].

Teorema I.2. *Se* $K|Q$ *é normal e existe uma torre radical* $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n \subset L_{n+1}$ *com* $L_n \subset \mathbf{R}$ *e* $L_{n+1} = L_n(i)$ $(L_n = L_{n+1} \cap \mathbf{R})$, *tal que* $K \subset L_{n+1}$ *então* $p \mid [K : \mathbf{Q}] \Rightarrow p = 2$ *ou* $p = 2^{2^r} + 1$ *para algum* $r \in \mathbf{N}$.

Demonstração: Pelo lema, dado $p \mid [K : \mathbf{Q}]$, devemos ter $e^{2\pi i/p} \in L_{n+1} \Rightarrow \cos(\frac{2\pi}{p}) = \frac{1}{2}(e^{2\pi i/p} + (e^{2\pi i/p})^{-1}) \in L_n = L_{n+1} \cap \mathbf{R}$ donde $\cos\left(\frac{2\pi}{p}\right)$ é solúvel por radicais reais, e pelo Corolário I.1, $p = 2$ ou p é primo de Fermat.

Seção II: Solubilidade por radicais reais e polinômios de grau ímpar

Teorema II.1. *Seja* $f(x) \in \mathbf{Q}[x]$ *um polinômio irredutível de grau ímpar que tenha uma raiz real* α *solúvel por radicais reais. Então* α *é a única raiz real de* $f(x)$.

Demonstração: Suponha que exista uma torre radical $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbf{R}$, com $L_{k+1} = L_k(\alpha_k)$, $P_{\alpha_k | L_k} = X^{p_k} - \alpha_k^{p_k}$, p_k primo, com $\alpha \in L_n$. Suponha que α tenha um conjugado real $\beta \neq \alpha$. Então existe um isomorfismo σ: $\mathbf{Q}(\alpha) \to \mathbf{Q}(\beta)$. Considere os corpos $M_k = \mathbf{Q}(\alpha) \cdot L_k$. Tentaremos estender o homomorfismo σ:$\mathbf{Q}(\alpha) = M_0 \to \mathbf{C}$ a homomorfismos σ:$M_k \to \mathbf{C}$ que tenham a propriedade

(*) $\quad \sigma \mid L_k = Id$

((*) implica em particular que $\sigma(M_k) \subset \mathbf{R}$). Suponha que $M_k \subsetneq M_{k+1}$. Então $M_{k+1} = M_k(\alpha_k)$, $P_{\alpha_k | M_k} = X^{p_k} - \alpha_k^{p_k}$, como antes. Se σ está definido em M_k satisfazendo (*), ou seja, $\sigma \mid_{L_k} = Id$, então podemos estendê-lo a M_{k+1} levando α_k em α_k (pois $P^{\sigma}_{\alpha_k | M_k} = P_{\alpha_k | M_k}$) e teremos $\sigma \mid_{M_{k+1}}$ satisfazendo (*). Suponha agora que $M_{k+1} = M_k$ e que p_k é impar. Então $\alpha_k \in M_k$, e como $\sigma(M_k) \subset \mathbf{R}$ e $\sigma(\alpha_k)$ é raiz de $P^{\sigma}_{\alpha_k | L_k} = X^{p_k} - \alpha_k^{p_k}$ devemos ter necessariamente $\sigma(\alpha_k) = \alpha_k$ pois α_k é a única raiz real de $X^{p_k} - \alpha_k^{p_k} \Rightarrow \sigma \mid_{L_{k+1}} = Id \Rightarrow \sigma \mid_{M_{k+1}}$ satisfaz (*). Assim, só não podemos garantir a existência de uma extensão de σ a M_{k+1} satisfazendo (*) se

$M_{k+1} = M_k$ e $p_k = 2$, caso em que temos $M_k = L_k(\alpha) = M_{k+1} \supset L_{k+1}$ e $[L_{k+1} : L_k] = 2 \Rightarrow [L_k(\alpha) : L_k]$ é par. Como certamente não podemos estender σ a L_n satisfazendo (*) (senão $\sigma \mid_{L_n} = Id \Rightarrow \sigma(\alpha) = \alpha$), para cada β existe um k com $[L_k(\alpha) : L_k]$ par tal que é possível estender o homomorfismo $\sigma : \mathbf{Q}(\alpha) \to \mathbf{Q}(\beta)$ que leva α em β a $\mathbf{Q}(\alpha) \cdot L_k$ com $\sigma \mid_{L_k} = Id$. Seja k_0 o menor k tal que existe β conjugado real de α para o qual acontece o fenômeno acima. Então $[L_{k_0}(\alpha) : L_{k_0}]$ é par. Por outro lado, α é conjugado a β sobre L_{k_0} para todo conjugado real β de α, donde $\{$ raízes reais de $P_{\alpha \mid L_{k_0}}$ $\} = \{$ raízes reais de $P_{\alpha \mid \mathbf{Q}}$ $\}$, que têm um número ímpar de elementos donde o grau de $P_{\alpha \mid L_{k_0}}$ seria ímpar, absurdo.

Obs.: O Teorema I.1 pode ser obtido como consequência do II.1. De fato, se $K \mid \mathbf{Q}$ é uma extensão normal, real e solúvel por radicais reais com $[K : \mathbf{Q}] \neq 2^n$, $\forall n$, então, se $H < \mathrm{Gal}(K \mid \mathbf{Q})$ é um 2-Sylow, $\mathrm{Fix}(H) \mid \mathbf{Q}$ é real, de grau ímpar e solúvel por radicais reais, absurdo, pois dado $\alpha \in \mathrm{Fix}(H) \setminus \mathbf{Q}$ temos $P_{\alpha \mid \mathbf{Q}}$ irredutível de grau ímpar, mas as raízes de $P_{\alpha \mid \mathbf{Q}}$ estão todas em K (pois $K \mid \mathbf{Q}$ é normal), e portanto são reais, contradizendo o Teorema II.1.

Seção III: Exemplos

Exemplo III.1: Mostraremos que o grupo de Galois não determina a solubilidade por radicais reais para extensões normais complexas (ao contrário de extensões normais reais, caso em que a ordem do grupo de Galois já determina se a extensão é solúvel por radicais reais ou não).

Considere os corpos $K_1 = \mathbf{Q}(\sqrt[3]{2},\ e^{2\pi i/3})$ e $K_2 = \mathbf{Q}(\cos(\frac{\theta}{3}), \cos(\frac{\theta+2\pi}{3}))$ onde θ é tal que $\cos\theta = \frac{3}{5}$ e $\mathrm{sen}\,\theta = \frac{4}{5}$. Temos $K_1 \mid \mathbf{Q}$ e $K_2 \mid \mathbf{Q}$ normais (são os fechos normais de $\mathbf{Q}(\sqrt[3]{2})$ e $\mathbf{Q}(\cos(\frac{\theta}{3}))$, respectivamente). Temos claramente K_1 solúvel por radicais reais. Por outro lado, $K_2 \subset \mathbf{R}$. Se provarmos que $[K_2 : \mathbf{R}] = 6$ concluiremos que K_2 não é solúvel por radicais reais, pelo Teorema I.1. Entretanto, nesse caso teremos $\mathrm{Gal}(K_1 \mid \mathbf{Q}) \approx \mathrm{Gal}(K_2 \mid \mathbf{Q}) \approx S_3$ (são ambos fechos normais de extensões de grau 3 não normais). Para isso, note que $\cos(\frac{\theta+2\pi}{3}) = -\frac{1}{2}\cos(\frac{\theta}{3}) + \frac{\sqrt{3}}{2}\mathrm{sen}(\frac{\theta}{3})$ donde $\mathbf{Q}(\cos(\frac{\theta}{3}), \cos(\frac{\theta+2\pi}{3})) = \mathbf{Q}(\cos(\frac{\theta}{3}), \sqrt{3}\ \mathrm{sen}(\frac{\theta}{3}))$. Por outro lado, como $\mathrm{sen}(3x) = \mathrm{sen}\,x(4\cos^2 x - 1)$, $\frac{4}{5} =$

$\operatorname{sen}(\theta) = \operatorname{sen}(\frac{\theta}{3})(4\cos^2(\frac{\theta}{3}) - 1) \Rightarrow \operatorname{sen}(\frac{\theta}{3}) = \frac{4}{5(4\cos^2(\frac{\theta}{3})-1)} \in \mathbf{Q}(\cos(\frac{\theta}{3}))$ donde

$\sqrt{3} \in \mathbf{Q}(\cos(\frac{\theta}{3}), \cos(\frac{\theta+2\pi}{3})) \Rightarrow 2[K_2 : \mathbf{Q}]$ é par. Além disso, como

$\cos(3x) = 4\cos^3 x - 3\cos x$, $4\cos^3(\frac{\theta}{3}) - 3\cos(\frac{\theta}{3}) = \cos\theta = \frac{3}{5} \Rightarrow 20\cos^3(\frac{\theta}{3}) - 3 = 0$.

O polinômio $20x^3 - 15x - 3$ é irredutível sobre $\mathbf{Q}$ pelo critério de Eisenstein e tem como raízes $\cos(\frac{\theta}{3})$, $\cos(\frac{\theta+2\pi}{3})$ e $\cos(\frac{\theta+4\pi}{3})$ donde $[\mathbf{Q}(\cos(\frac{\theta}{3})) : \mathbf{Q}] = 3 \Rightarrow$ $[K_2 : \mathbf{Q}] = 6$, e $\operatorname{Gal}(K_2 \mid \mathbf{Q}) = S_3$.

Nesse caso temos $K_1 \not\subset \mathbf{R}$ e $K_2 \subset \mathbf{R}$, o que pode incomodar o leitor. Faremos uma pequena modificação do exemplo para que nenhum dos corpos esteja contido em $\mathbf{R}$: Sejam $\overline{K} = K_1(i)$ e $\overline{K}_2 = K_2(i)$. Temos $\operatorname{Gal}(\overline{K}_1)$ gerado pelos homomorfismos a e b, definidos por:

$$a: (\sqrt[3]{2} \to \xi\sqrt[3]{2}, \quad \xi \to \xi, \quad i \to -i)$$

e

$$b: (\sqrt[3]{2} \to \sqrt[3]{2}, \quad \xi \to \xi^2, \quad i \to -i)$$

onde $\xi = e^{2\pi i/3}$. Temos $\operatorname{ord}(a) = 6$, $\operatorname{ord}(b) = 2$ e $b \cdot a = a^5 \cdot b$ (ambos são iguais a $(\sqrt[3]{2} \to \xi^2\sqrt[3]{2}, \quad \xi \to \xi^2, \quad i \to -i)$). Já em $\overline{K}_2$, se $\alpha = \cos(\frac{\theta}{3})$, $\alpha_2 = \cos(\frac{\theta+2\pi}{3})$ e $\alpha_3 = \cos(\frac{\theta+4\pi}{3})$ são os conjugados de $\cos(\frac{\theta}{3})$, temos $\operatorname{Gal}(\overline{K}_2)$ gerado por $\sigma : \left(\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3\\ \alpha_2 & \alpha_3 & \alpha_1\end{pmatrix}, i \to -i\right)$ e $\tau : \left(\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3\\ \alpha_2 & \alpha_1 & \alpha_3\end{pmatrix}, i \to i\right)$ que são tais que $\operatorname{ord}(\sigma) = 6$, $\operatorname{ord}(\tau) = 2$ e $\tau \circ \sigma = \sigma^5 \circ \tau$ (ambos são iguais a $\left(\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3\\ \alpha_1 & \alpha_3 & \alpha_2\end{pmatrix}, i \to -i\right)$). Pela Teoria de grupos gerados por dois elementos (ver [2], p. 114), $\operatorname{Gal}(\overline{K}_1)$ e $\operatorname{Gal}(\overline{K}_2)$ são isomorfos (na verdade isomorfos a $S_3 \times \mathbf{Z}_2 = \langle \sigma_1, \sigma_2 \rangle$ onde $\sigma_1 = \left(\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \bar{1}\right)$ e $\sigma_2 = \left(\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \bar{0}\right)$ satisfazem $\operatorname{ord}(\sigma_1) = 6$, $\operatorname{ord}(\sigma_2) = 2$ e $\sigma_2\sigma_1 = \sigma_1^5\sigma_2$).

Exemplo III.2: Veremos agora que não há outras restrições sobre os fatores do grau de uma extensão normal solúvel por radicais reais além da que dá o Teorema I.2. De fato, se $q_1, q_2, \ldots, q_n$ são iguais a 2 ou a primos de Fermat (não

necessariamente distintos), e $p_1 = 2$,$p_2 = 3$, p_3 , ... , p_n são os primeiros números primos então $\mathbf{Q}(\sqrt[q_1]{p_1}, \sqrt[q_2]{p_2}, \ldots, \sqrt[q_n]{p_n}, \xi_{q_1}, \xi_{q_2}, \ldots, \xi_{q_n})$ onde $\xi_{q_i} = e^{2\pi i/q_i}$ é uma extensão normal cujo grau é múltiplo de $q_1 q_2 \ldots q_n$ (é o fecho normal de $\mathbf{Q}(\sqrt[q_1]{p_1} \ldots, \sqrt[q_n]{p_n}) =: L$, que satisfaz $[L : \mathbf{Q}] = q_1 q_2 \ldots q_n$). Essa extensão é solúvel por radicais reais, pois é gerada por elementos solúveis por radicais reais.

Obs.: Provaremos que efetivamente $[L : \mathbf{Q}] = q_1 q_2 \ldots q_n$: Sejam $L_0 = \mathbf{Q}$, $L_i = L_{i-1}(\sqrt[q_i]{p_i})$, $1 \le i \le n$ (e portanto $L_n = L$). Basta provar que $[L_{i+1} : L_i] = q_i$, ou que $P_{\sqrt[q_i]{p_i} \mid L_{i-1}} = X^{q_i} - p_i$. Para isso basta provar que $\sqrt[q_i]{p_i} \notin L_{i-1}$, para $1 \le i \le n$ (veja [1], p. 125). Se não, seja k o menor índice tal que existe $\sqrt[q_k]{p_k} \in L_{k-1}$. Seja j o menor índice tal que existam r_1 , r_2 , ... , $r_{k-1} \in \mathbf{Z}$ com $\sqrt[q_k]{p_1^{r_1} p_2^{r_2} \cdots p_{k-1}^{r_{k-1}} p_k} \in L_j$ (temos então $j \le k-1$). Não podemos ter $q_j \ne q_k$, senão $x = \sqrt[q_k]{p_1^{r_1} p_2^{r_2} \cdots p_{k-1}^{r_{k-1}} p_k}$ é tal que $x \notin L_{j-1} \Rightarrow [L_{j-1}(x) : L_{j-1}] = q_k$, mas $L_{j-1} \subset L_j$, e $[L_j : L_{j-1}] = q_j \Rightarrow q_k \mid q_j \Rightarrow q_k = q_j =: q$. Nesse caso temos $x \in L_{i-1}(\sqrt[q]{p_j}) \Rightarrow$ existem α_l , α_{l+1} , ... , α_{q-1} com $\alpha_l \ne 0$ $(l \ge 0)$ tais que $X = \alpha_l \sqrt[q]{p_j}^{\,l} + \alpha_{l+1} \sqrt[q]{p_j}^{\,l+1} + \cdots + \alpha_{q-1} \sqrt[q]{p_j}^{\,q-1} \Rightarrow y = x \cdot \sqrt[q]{p_j}^{\,-l} = \alpha_l + \alpha_{l+1} \sqrt[q]{p_j} + \cdots + \alpha_{q-1} \sqrt[q]{p_j}^{\,q-l-1}$ é tal que $y^q \in \mathbf{Q} \subset L_{j-1}$ e $Tr_{L_j \mid L_{j-1}}(y) = q \cdot \alpha_l \ne 0 \Rightarrow y \in L_{j-1}$ (para provarmos isso, observemos que se $y \notin L_{j-1}$, como $y^q \in L_{j-1}$ teríamos $P_{y \mid L_{j-1}} = X^q - y^q$, donde $Tr_{L_j \mid L_{j-1}}(y) = 0$). Mas $y \in L_{j-1}$ contradiz a minimalidade de j, absurdo.

Referências

[1] Endler, Otto, *Teoria dos Corpos*, Monografias de Matemática nº 44, IMPA.

[2] Garcia, Arnaldo e Lequain, Yves, *Álgebra, um curso de introdução*, Projeto Euclides, IMPA, 1988.

[3] Moreira, Carlos Gustavo, Um teorema sobre solubilidade de equações polinomiais por radicais reais, *Revista Matemática Universitária nº 12, 1990.*

[4] Tschebotaröw, N. e Schwerdtfeger, H., *Grundzüge der Galois chen Theorie*, P. Noordhoff, N.V., 1950.

IMPA
Estrada Dona Castorina, 110
22460-320, Rio de Janeiro - RJ