MATEMÁTICA UNIVERSITÁRIA
no. 20/21 – junho/dezembro 1996 – pp. 60-61

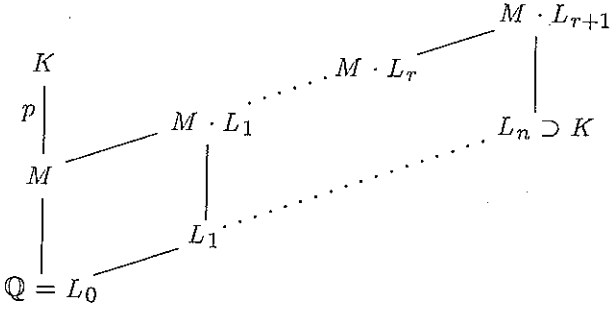
Sobre solubilidade por radicais reais

Carlos Gustavo Tamm de Araujo Moreira

Errata: *Apresentamos uma versão corrigida do Lema da Seção I do artigo "Sobre Solubilidade por Radicais Reais", publicado na RMU n° 16, página 61 do referido artigo.*

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

Demonstração: Seja p um primo que divida $[K : \mathbb{Q}]$. Tome $H < \mathrm{Gal}(K|\mathbb{Q})$ com $|H| = p$ (tal H existe pelo 1° teorema de Sylow. Veja [2], pág. 159). Seja $M = \mathrm{Fix}(H)$. Temos assim $K|M$ normal de grau p. Considere os corpos $N_i = L_i \cdot M$, $0 \leq i \leq n$. 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 $P_{\gamma|M} = (X - \gamma_1)(X - \gamma_2)\ldots(X - \gamma_p)$ onde $\gamma_1 := \gamma$. Temos $\gamma_i \in N_{r+1} \setminus N_r$, $1 \leq i \leq p$, pois se $\gamma_i \in N_r$, $M(\gamma_i) \subset N_r \Rightarrow K \subset N_r$, absurdo. Suponhamos que $X^{p_r} - \alpha_r^{p_r}$ seja irredutível sobre N_r. Então $[N_{r+1} : N_r] = p_r$, que é primo, donde não há corpos entre N_r e N_{r+1}. Definimos uma relação de equivalência em $\{\gamma_1, \gamma_2, \ldots, \gamma_p\}$ 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 $p \Rightarrow p_r = p$. Como $N_{r+1} = N_r(\gamma)$ e os conjugados γ_i de γ pertencem a $K \subset N_{r+1}$, temos que $N_{r+1}|N_r$ é normal. Assim, os conjugados de α_r sobre N_r têm que estar em $N_{r+1} \Rightarrow \alpha_r,\ e^{2\pi i/p} \cdot \alpha_r \in N_{r+1} \Rightarrow e^{2\pi i/p} = (e^{2\pi i/p}\alpha_r)/\alpha_r \in N_{r+1} \subset L_n$.

Suponhamos agora que $X^{p_r} - \alpha_r^{p_r}$ seja redutível sobre N_r. Nesse caso $X^{p_r} - \alpha_r^{p_r}$ deve ter raiz em N_r, pois p_r é primo (veja [1], pág. 125), ou seja, existe k primo com p_r com $\alpha_r \cdot e^{2k\pi i/p_r} \in N_r$, e nesse caso $e^{2\pi i/p_r} \in N_{r+1}$, e de fato, $N_{r+1} = N_r(e^{2\pi i/p_r})$, donde $[N_{r+1} : N_r]|(p_r - 1)$, pois, definindo em $(\mathbb{Z}/p_r\mathbb{Z})^*$ a relação de equivalência $k_1 \sim k_2$ se $e^{2k_1\pi i/p_r}$ e $e^{2k_2\pi i/p_r}$ são conjugados sobre N_r cada classe de equivalência terá $[N_{r+1} : N_r]$ elementos. Por outro lado, $[N_r(\gamma) : N_r] = p$ (pois, como antes, deve dividir p), donde $p|[N_{r+1} : N_r] \Rightarrow p_r \equiv 1(\text{mod } p)$. Basta portanto provar o lema no caso $K = Q(e^{2\pi i/q})$, com $q \equiv 1(\text{mod } p)$. Supondo por absurdo que $e^{2\pi i/p} \notin L_n$, podemos supor que q é o menor primo congruente a 1 módulo p tal que exista uma tal torre com $e^{2\pi i/p} \notin L_n$. Na notação anterior teríamos $\alpha_r \cdot e^{2k\pi i/p_r} \in N_r = L_r \cdot M \subset L_r(e^{2\pi i/q})$, e $P_{\alpha_r \cdot e^{2k\pi i/p_r}|L_r} = X^{p_r} - \alpha_r^{p_r}$, donde $p_r \leq [N_r : L_r] \leq [L_r(e^{2\pi i/q}) : L_r] \leq q - 1$, $p_r \equiv 1(\text{mod } p)$ e $\mathbb{Q}(e^{2\pi i/p_r})$ está contido numa torre fortemente radical com $e^{2\pi i/p} \notin L_n$, absurdo. □