Matemática Universitária Nº 12, dezembro de 1990, 87–93

Um Teorema sobre Solubilidade de Equações Polinomiais por Radicais Reais(*)

Carlos Gustavo Tamm de Araujo Moreira

IMPA
Estr. Dona Castorina 110
22460 Rio de Janeiro - RJ

1. Introdução.

Um dos problemas mais antigos da Álgebra é a busca de soluções de equações polinomiais que possam ser expressas por combinações finitas de radicais. Esse problema só foi resolvido no século XIX por Évariste Galois, que construiu uma teoria que permite, dado um polinômio com coeficientes racionais, decidir se ele tem ou não raízes solúveis por radicais, hoje conhecida como teoria de Galois.

(*) Após a redação desse artigo o Professor Derek Hacon comunicou-me que o teorema principal já havia sido demonstrado por Hölder (ver [3], pág. 346–348), com enunciado e demonstração um pouco diferentes dos aqui apresentados. Apesar disso, continua sendo interessante a publicação do artigo, tendo em vista que os autores mais modernos têm feito a Teoria de Galois sobre um corpo qualquer, ganhando em generalidade mas perdendo às vezes resultados relevantes (como o do presente trabalho), relativos especificamente a $\mathbf{Q}$ ou a $\mathbf{R}$.

Deixo aqui meus agradecimentos ao prof. Derek por ter-me avisado da existência desse resultado e ao professor Karl Otto Stöhr, por ter-me ajudado a compreender o teorema, que está em alemão no livro de Tschebotarëw (ver [3], e por me haver estimulado a publicar o presente artigo, com argumentos como o citado acima.

Um dos principais resultados dessa teoria é o seguinte: Dado $f(x) \in \mathbf{Q}[x]$ irredutível, as raízes de f são exprimíveis por radicais $\Leftrightarrow$ Gal(f) é um grupo solúvel, onde Gal(f) é o grupo dos automorfismos de $\mathbf{Q}$(raízes de f) que fixam $\mathbf{Q}$ (Gal(f) = Aut($\mathbf{Q}$(raízes de$f|\mathbf{Q}$)).

Um dos corolários desse teorema é que (como já se sabia no século XVI) polinômios do 1º, 2º, 3ºe 4ºgraus são sempre solúveis por radicais, havendo até fórmulas explícitas para as raízes dessas equações. No entanto, nem sempre essas fórmulas são satisfatórias, no seguinte sentido: existem, por exemplo, equações do 3º grau com todas as 3 raízes reais cujas expressões por radicais dadas pela fórmula envolvem números imaginários. É o caso da equação $x^3 - 3x + 1 = 0$. A fórmula para as soluções de $x^3 + px + q = 0$ é

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

que nesse caso nos dá

$$\begin{aligned} x &= \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - 1}} + \sqrt[3]{-\frac{1}{2} - \sqrt{\frac{1}{4} - 1}} \\ &= \sqrt[3]{-\frac{1}{2} + i\frac{\sqrt{3}}{2}} + \sqrt[3]{-\frac{1}{2} + i\frac{\sqrt{3}}{2}}, \end{aligned}$$

expressão que envolve números complexos, enquanto seria de se esperar uma expressão que só envolvesse números reais.

Surge então uma pergunta natural: Dado um polinômio $f(x) \in \mathbf{Q}[x]$ que tenha todas as raízes reais, solúvel por radicais, em que condições pode-se garantir que seja solúvel por radicais reais, no sentido de existir uma extensão radical K de $\mathbf{Q}$, $K \subset \mathbf{R}$, com $\mathbf{Q}$ (raízes de f) $\subset K$?

O objetivo deste trabalho é dar uma resposta a essa pergunta.

2. O teorema e algumas conseqüências.

Teorema. *Seja $f \in \mathbf{Q}[x]$ irredutível. Então f é solúvel por radicais reais $\Leftrightarrow$ $|\text{Gal}(f)| = 2^K$, para algum $K \in \mathbf{N}$, e nesse caso as raízes se escrevem usando só raízes quadradas.*

DEMONSTRAÇÃO:
($\Leftarrow$) Seja $L = \mathbf{Q}$(raízes de$f$), e seja $G = \mathrm{Aut}(L/\mathbf{Q}) = \mathrm{Gal}(f)$.

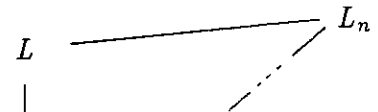
Como $|G| = 2^k$, G é um 2-grupo, e por [1], exemplo 2, pág. 206, temos que G é solúvel $\Rightarrow \exists \{e\} = G_o \triangleleft G_1 \triangleleft \ldots \triangleleft G_k = G$, onde $|G_i| = 2^i$ e logo $(G_{i+1} : G_i) = 2$. Isso nos dá a seguinte extensão de corpos:

$$\begin{array}{c} L_k = L \subset \mathbf{R} \\ | \\ \vdots \\ | \\ L_1 \\ | \\ \mathbf{Q} = L_o \end{array}$$

onde $L_i = \mathrm{Fix}(G_{k-i})$. Temos que $[L_{i+1} : L_i] = 2 \Rightarrow \begin{array}{c} L_{i+1} \\ | \\ L_i \end{array}$ é normal. Como $[L_{i+1} : L_i] = 2$, $\exists \alpha_{i+1} \in L_{i+1}$, $L_{i+1} = L_i(\alpha_{i+1})$, com $\alpha_{i+1}^2 \in L_i$, o que decorre da fórmula da equação do 2º grau.

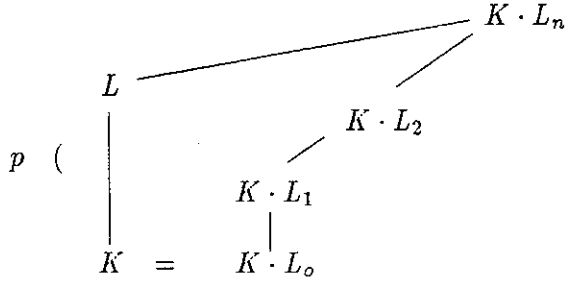
Essas observações implicam que $L/\mathbf{Q}$ é uma extensão radical, e, como $L \subset \mathbf{R}$, $L_i \subset \mathbf{R}$, $\forall i$, f é solúvel por radicais reais, pois $\alpha_i \in \mathbf{R}, \forall i$, e $L_i = L_{i-1}(\alpha_i)$, com $\alpha_i^2 \in L_{i-1}$.

($\Rightarrow$) Se f é solúvel por radicais reais, f é solúvel por radicais $\Rightarrow$ $\exists$ extensões de corpos; todos contidos em $\mathbf{R}$, da seguinte forma:



onde $L = \mathbf{Q}$(raízes de$f$); $\exists n_i$ primos, α_i tais que $L_i = L_{i-1}(\alpha_i)$ e $\alpha_i^{n_i} \in L_{i-1}$. Se $|\mathrm{Gal}(f)| = [L : Q]$ não é uma potência de 2, existe p primo, $p \neq 2$ tal que $p|[L : \mathbf{Q}] = |\mathrm{Gal}(f)|$, donde, pelo 1º teorema

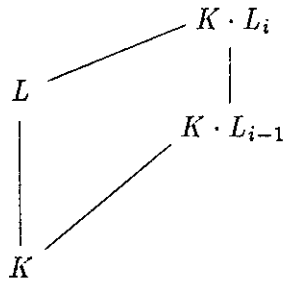
de Sylow ([1], pág. 159), existe subgrupo H de $G = \mathrm{Gal}(f)$ com $|H| = p$. Seja $K = \mathrm{Fix}(H)$. Temos que $[L : K] = p$. Temos a seguinte extensão de corpos:



Temos que $K \cdot L_i = K \cdot L_{i-1}(\alpha_i)$; $\alpha_i^{n_i} \in L_{i-1} \subset K \cdot L_{i-1}$. Como $L \subset K \cdot L_n$ mas $L \not\subset K \cdot L_o$, $\exists i \in \{1, 2, \ldots, n\}$ tal que $L \subset K \cdot L_i$ mas $L \not\subset K \cdot L_{i-1}$.

Seja agora β_1 tal que $L = K(\beta_1)$. Como $L/\mathbf{Q}$ é normal, L/K também é normal. Assim, $P_{\beta_1|K} = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_p)$, onde $\beta_1, \ldots, \beta_p \in L$, e, como $\mathrm{Car}(\mathbf{Q}) = 0$, $\mathrm{Car}(K) = 0 \Rightarrow P_{\beta_1|K}$ é separável, por ser irredutível $\Rightarrow \beta_i \neq \beta_j$, $i \neq j$.

Temos agora as seguintes extensões de corpos:



Temos que $K \cdot L_i = K \cdot L_{i-1}(\alpha_i)$, onde $\alpha_i \in L_i$, e $\exists n_i$ primo tal que $\alpha_i^{n_i} \in L_{i-1} \subset K \cdot L_{i-1}$. Assim, $P_{\alpha_i|K \cdot L_{i-1}} \mid X^{n_i} - \alpha_i^{n_i}$.

Ao mesmo tempo temos que, como $K \cdot L_i \not\subset K \cdot L_{i-1}$, $\alpha_i \notin K \cdot L_{i-1}$ e como $\alpha_i \in L_i \subset \mathbf{R}$, $X^{n_i} - \alpha_i^{n_i}$ não tem raiz em $K \cdot L_{i-1}$, pois $K \cdot L_{i-1} \subset \mathbf{R}$ e $\alpha_i \notin K \cdot L_{i-1}$ é a única raiz real de $X^{n_i} - \alpha_i^{n_i}$.

Desta forma, como n_i é primo, $X^{n_i} - \alpha_i^{n_i}$ é irredutível sobre $K \cdot L_{i-1}[X]$. De fato, $X^{n_i} - \alpha_i^{n_i} = \prod_{k=0}^{n_i-1} (X - \xi^k \alpha_i)$, onde ξ é raiz n_i-ésima primitiva da unidade. Assim, se $f | X^{n_i} - \alpha_i^{n_i}$, f deve ser da

forma $c(X-\xi^{r_1}\alpha_i)(X-\xi^{r_2}\alpha_i)\dots(X-\xi^{r_m}\alpha_i) \Rightarrow$ se $f \in K\cdot L_{i-1}[X]$, teremos $\xi^{n_1+\dots+n_m}\alpha_i^m \in K\cdot L_{i-1} \Rightarrow \alpha_i^m \in K\cdot L_{i-1}$. Se $m < n_i$, como n_i é primo, $\exists a,b \in \mathbf{Z}$, $an_i + bm = 1 \Rightarrow \alpha_i = \alpha_i^{an_i+bm} = (\alpha_i^{n_i})^a(\alpha_i^m)^b \in K\cdot L_{i-1}$, contradição. Assim, $m = n_i \Rightarrow f = c(X^{n_i} - \alpha_i^{n_i})$ ou $m = 0$. Assim $X^{n_i} - \alpha_i^{n_i}$ é, de fato, irredutível.

Assim, $X^{n_i} - \alpha_i^{n_i} = P_{\alpha_i|K\cdot L_{i-1}} \Rightarrow [K\cdot L_i : K\cdot L_{i-1}] = n_i$, que é primo. Assim, não existe corpo propriamente contido entre $K\cdot L_{i-1}$ e $K\cdot L_i$, donde, como $L \subset K\cdot L_i$ mas $L \not\subset K\cdot L_{i-1}$, e $L = K(\beta_j)$, para cada $j \in \{1,2,\dots,p\}$ temos que $K\cdot L_i = K\cdot L_{i-1}(\beta_j)$, para cada $j \in \{1,2,\dots,p\}$. Como todos os conjugados de β_1 estão em L, todos os conjugados de β_1 estão em $K\cdot L_i \Rightarrow K\cdot L_i/K\cdot L_{i-1}$ é uma extensão normal.

Daí segue que, como $K\cdot L_i = K\cdot L_{i-1}(\alpha_i)$ e $P_{\alpha_i|K\cdot L_{i-1}} = X^{n_i} - \alpha_i^{n_i}$, temos que todas as raízes de $X^{n_i} - \alpha_i^{n_i}$ estão em $K\cdot L_i \Rightarrow \xi\cdot\alpha_i \in K\cdot L_i \subset \mathbf{R} \Rightarrow \xi \in \mathbf{R} \Rightarrow n_i = 2$.

Como $P_{\beta_j|K\cdot L_{i-1}} \mid P_{\beta_j|K} = (X-\beta_1)\dots(X-\beta_p)$, e $\partial P_{\beta_j|K\cdot L_{i-1}} = [K\cdot L_i : K\cdot L_{i-1}] = n_i = 2$, temos que $\forall j \in \{1,2,\dots,p\}$, $\exists r_j \in \{1,2,\dots,p\}$ tal que $P_{\beta_j|K\cdot L_{i-1}} = (X-\beta_j)(X-\beta_{r_j})$. Claramente $r_{r_j} = j$. Como $P_{\beta_j|K\cdot L_{i-1}}$ é irredutível, $\forall i,j$, temos que $P_{\beta_i|K\cdot L_{i-1}} = P_{\beta_j|K\cdot L_{i-1}} \Leftrightarrow i \in \{j, r_j\} \Leftrightarrow j \in \{i, r_i\}$.

Assim, dividimos $\{1,2,\dots,p\}$ em classes de equivalência do tipo $\{j, r_j\}$, $r_j \neq j$, (pois $K\cdot L_i/K\cdot L_{i-1}$ é separável), absurdo, pois p é um número ímpar. ∎

COROLÁRIO 1: Se $f \in \mathbf{Q}[x]$ é irredutível, de grau que não é potência de 2, com $\{\text{raízes de} f\} \subset \mathbf{R}$, então a equação $f(x) = 0$ não é solúvel por radicais reais.

DEMONSTRAÇÃO: Basta ver que $\partial f \mid |\mathrm{Gal}(f)|$. ∎

COROLÁRIO 2: Seja $f \in \mathbf{Q}[x]$ com todas as raízes reais. Então todas as raízes de f são exprimíveis por radicais reais $\Leftrightarrow$ todas as raízes de f são construtíveis com régua e compasso.

DEMONSTRAÇÃO: Basta provar para cada fator irredutível de f. Podemos supor, pois, f irredutível. Nesse caso, f é solúvel por radicais reais $\Leftrightarrow \exists k$, $|\mathrm{Gal}(f)| = 2^k \Leftrightarrow$ todas as raízes de f são construtíveis com régua e compasso (ver [2], teoremas (10.7) e (10.8)).

COROLÁRIO 3: $\cos\left(\frac{2\pi}{n}\right)$ é exprimível por radicais reais $\Leftrightarrow$ o polígono regular de n lados é construtível com régua e compasso

$\Leftrightarrow n = 2^k \cdot P_1 \cdot P_2 \ldots P_r$, onde $k \in \mathbf{N}$ e $P_1, \ldots, P_r$ são primos de Fermat distintos (da forma $2^{2^n}+1$).

DEMONSTRAÇÃO: Para a segunda equivalência, ver [2], (10.9) e (10.10).

($\Leftarrow$ da 1ª equivalência): Nesse caso $|\mathrm{Gal}(\phi_n)|$ é potência de $2 \Rightarrow$ como $\mathbf{Q}(\text{raízes de } \phi_n) = \mathbf{Q}\left(e^{\frac{2\pi i}{n}}\right)$, e $\cos\frac{2\pi}{m} = \frac{1}{2}\left(e^{\frac{2\pi i}{n}} + e^{\frac{-2\pi i}{n}}\right)$, temos a seguinte extensão de corpos:

$$\begin{array}{c} \mathbf{Q}(e^{2\pi i/n}) \\ | \\ \mathbf{Q}\left(\cos\dfrac{2\pi}{n}\right) \\ | \\ \mathbf{Q} \end{array}$$

Como $[\mathbf{Q}\left(e^{\frac{2\pi i}{n}}\right) : \mathbf{Q}]$ é potência de 2, $[\mathbf{Q}\left(\cos\frac{2\pi}{n}\right) \cdot \mathbf{Q}]$ também é $\Rightarrow$ (pelo teorema e por $\mathbf{Q}\left(\cos\frac{2\pi}{n}\right) \subset \mathbf{R}$) $\cos\frac{2\pi}{n}$ é exprimível por radicais reais.

($\Rightarrow$ da 1ª equivalência):

LEMA: $\exists$ polinômios P_n e Q_n de $\mathbf{Q}[x]$ tais que $\cos nx = P_n(\cos x)$ e $\operatorname{sen} nx = \operatorname{sen} x\, Q_n(\cos x)$, $\partial P_n \leq n, \partial Q_n \leq n-1$.

DEMONSTRAÇÃO: Vale para $n = 0$ e $n = 1$. Por indução, $\cos(n+1)x = \cos(nx + x) = \cos nx \cos x - \operatorname{sen} nx \operatorname{sen} x = \cos x\, P_n(\cos x) - \operatorname{sen}^2 x\, Q_n(x) = P_{n+1}(\cos x)$, onde $P_{n+1}(y) = yP_n(y) - (1-y^2)Q_n(y) \Rightarrow \partial P_{n+1} \leq n+1$

$$\begin{aligned} \operatorname{sen}(n+1)x = \operatorname{sen}(nx+x) &= \operatorname{sen} nx \cos x + \operatorname{sen} x \cos nx \\ &= \operatorname{sen} x\, Q_{n+1}(\cos x) \end{aligned}$$

onde $Q_{n+1}(y) = yQ_n(y) + P_n(y) \Rightarrow \partial Q_n \leq n$.

Assim, como $\cos\left(n \cdot \frac{2\pi}{n}\right) = 1$, $\cos\left(\frac{2\pi}{n}\right)$ é raiz de $(P_n(x) - 1)$. Para cada $k \in \{0, 1, \ldots, n-1\}$, $\cos\left(\frac{2k\pi}{n}\right)$ é raiz de $(P_n(x) - 1)$.

$\cos\left(\frac{2k\pi}{n}\right) = \cos\left(\frac{2\ell k}{n}\right)$, $k \neq \ell$, $\{l, \ell\} \subset \{0, 1, \ldots, n-1\} \Leftrightarrow k + \ell = n$. Nesse caso, provaremos que $\cos\left(\frac{2k\pi}{n}\right)$ é raiz dupla de $P_n(x) - 1$.

$P_n(\cos x) = \cos nx \Rightarrow -P_n'(\cos x)\operatorname{sen} x = -n \operatorname{sen} nx$. Temos que se $x = \frac{2k\pi}{n}$, $k \neq 0$, $k \neq \frac{n}{2}$ então $\operatorname{sen} x \neq 0$ e $\operatorname{sen} nx = 0 \Rightarrow P_n'(\cos x) = 0$. Como $P_n(\cos x) - 1 = 0$, $\cos x$ é raiz de $P_n - 1$ e de $P_n' = (P_n - 1)' \Rightarrow \cos x$ é (pelo menos) raiz dupla de $P_n - 1 \Rightarrow \left(x - \cos\frac{2k\pi}{n}\right)\left(x - \cos\frac{2\ell\pi}{n}\right) \mid (P_n - 1)$, se $k + \ell = n, k \neq \ell$, $\{k, \ell\} \subset \{0, 1, \ldots, n-1\} \Rightarrow \Pi_{k=1}^{n}\left(x - \cos\left(\frac{2k\pi}{n}\right)\right) \mid (P_n - 1)$, e $\partial(P_n - 1) = n \Rightarrow$ os dois polinômios diferem por um fator constante $\Rightarrow$ todas as raízes de $P_n - 1$ são reais, e a aplicação do corolário 2 encerra a demonstração.

Podemos aplicar o corolário 2 pois, como $\cos\frac{2k\pi}{n} = P_k\left(\cos\left(\frac{2\pi}{n}\right)\right)$, se $\cos\left(\frac{2\pi}{n}\right)$ é exprimível por radicais reais então $\cos\left(\frac{2k\pi}{n}\right)$ também o é, $\forall k$. Assim, todas as raízes de $P_n(x) - 1$ são exprimíveis por radicais reais.

OBSERVAÇÃO: Claramente o seguinte resultado vale: se $\operatorname{mdc}(p, q) = 1$ então $\cos\left(\frac{p\pi}{q}\right)$ é exprimível por radicais reais $\Leftrightarrow$ o polígono de q lados é construtível com régua e compasso (basta ver que p é invertível módulo q e usar o corolário 3).

EXEMPLO 1: $\cos 40°$ não se exprime por radicais reais ($40° = \frac{2\pi}{9}$).

EXEMPLO 2:

$$\cos\frac{2\pi}{17} = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}+\sqrt{170-26\sqrt{17}}-4\sqrt{34+2\sqrt{17}}}}{16}$$

observe que só usamos raízes quadradas.

OBSERVAÇÃO: Podemos estender o conceito de solubilidade por radicais reais para números complexos da seguinte forma: $a + bi$ é exprimível por radicais reais se e só se a e b o são.

BIBLIOGRAFIA

1. Garcia, Arnaldo e Lequain, Yves, "Álgebra: um curso de introdução," Projeto Euclides, IMPA, 1988.
2. Endler, Otto, "Teoria dos Corpos," Monografias de Matemática nº 44, IMPA.
3. Tschebotarëw, N. e Schwerdtfeger, H., "Grundzüge der Galois'schen Theorie," P. Noordhoff, N.V., 1950.