Boletín de Matemáticas
Vol. XIX Nº 3 (1985)

ALGUNOS CRITERIOS PARA DETERMINAR POLINOMIOS NO SOLUBLES POR RADICALES

Ivan Castro Ch.

En alguna ocasión tuvimos que enfrentarnos con el siguiente ejercicio: hallar la solución general de la ecuación diferencial

$$y^{(5)} + 5y^{(4)} + 10y^{(3)} + 10y^{(2)} - 4y' - 5y = 0$$

Al tomar la ecuación de índices $f(z) = 0$ con

$$f(z) = z^5 + 5z^4 + 10z^3 + 10z^2 - 4z - 5$$

fracasamos en los intentos por hallar sus raíces. Algún tiempo después comprendimos que era imposible encontrar fórmulas en las cuales aparecieran como únicas operaciones la suma, la resta, la multiplicación, la división y la elevación

a exponentes racionales que, relacionando los coeficientes de $f(z)$, permitieran expresar las raíces de este polinomio, ya que $f(z) = (z+1)^5 - 9(z+1) + 3$ y el polinomio $f(z) = z^5 - 9z + 3$ no es soluble por radicales.

Situaciones similares se presentan más a menudo de lo que usualmente creemos; por esta razón es importante que conozcamos unos criterios que nos permitan determinar si ciertos polinomios son o nó solubles por radicales. El propósito de este artículo es difundir algunos de ellos. Recordemos que un grupo G con módulo e, es soluble, si existen $G_0 = G \supseteq G_1 \supseteq \ldots \supseteq G_s \supseteq G_{s+1} = \{e\}$ una secuencia finita de subgrupos de G tales que

1) $G_n \triangleq G_{n-1}$ (G_n es subgrupo normal de G_{n-1}) $\forall n \in I_{s+1}$ (1)

2) G_{n-1}/G_n es abeliano $\forall n \in I_{s+1}$.

La secuencia $\{G_n\}_{0 \leq n \leq s+1}$ también se denomina una secuencia soluble de G.

Algunas de las propiedades importantes de los grupos solubles son:

---

(1) Notamos $I_n = \{1,2,\ldots,n\}$ y S_n el n-ésimo grupo simétrico.

PROPOSICION 1. Todo grupo abeliano es soluble.

PROPOSICION 2. Todo isomorfismo envía secuencias solubles en secuencias solubles.

PROPOSICION 3. Si $f(z)$ es un polinomio sobre un cuerpo K, E su cuerpo de descomposición (c.d.d.) y $G(E;K)$ el grupo de automorfismos de E que dejan fijo a K, entonces: $f(z)$ es soluble por radicales, si y sólo si, $G(E;K)$ es soluble.

PROPOSICION 4. Si G es un grupo finito y $H \triangleq G$ entonces: G es soluble, si y sólo si, H y G/H son solubles.

Se pueden encontrar las demostraciones de estas propiedades en los textos [2] y [3].

DEFINICION 1. Sea G un subgrupo de S_n. Definimos la relación δ sobre I_n de la siguiente manera: Sean $X,Y \in I_n$, entonces $X\delta Y$ si y sólo si existe $\sigma \in G$ tal que $\sigma(X) = Y$.

LEMA 1. La relación presentada en la definición 1 es de equivalencia.

demostración. 1) Como $id \in G$ entonces $X\delta X$ $\forall X \in I_n$ y por lo tanto δ es reflexiva.
2) Sean $X,Y \in I_n$ tales que $X\delta Y$. Existe $\sigma \in G$ tal que $\sigma(X) = Y$. Como G es un grupo, $\sigma^{-1} \in G$; además $X = \sigma^{-1}(Y)$. De donde $Y\ \delta\ X$.

3) Sean $X,Y,Z \in I_n$ tales que $X\delta Y$ y $Y\delta Z$. Existen σ y τ en G tales que $\sigma(X) = Y$ y $\tau(Y) = Z$. Como G es un grupo $\tau\circ\sigma \in G$; además $(\tau\circ\sigma)(X) = Z$. De donde $X\delta Z$.

Notación. Si $X \in I_n$ notaremos $[X]_G = \{Y \in I_n \mid X\delta Y\}$

DEFINICION 2. Si $X \in I_n$, $[X]_G$ se denomina la clase transitiva de X determinada por G.

DEFINICION 3. Un subgrupo G de S_n es transitivo si $\forall X,Y \in I_n$ existe $\sigma \in G$ tal que $\sigma(X) = Y$.

LEMA 2. Sean G un grupo transitivo y H un subgrupo normal de G, entonces

$$\forall X,Z \in I_n,\ \#[X]_H = \#[Z]_H .$$

Demostración. Sean $X,Z \in I_n$. Como G es transitivo, existe $\sigma \in G$ tal que $\sigma(X) = Z$. Si $u \in [X]_H$, existe $\tau \in H$ tal que $\tau(X) = u$. Luego $(\tau\sigma^{-1})(Z) = u$. Por lo tanto $(\sigma\tau\sigma^{-1})(Z) = \sigma(u)$. Pero como $H \trianglelefteq G$, $\sigma\tau\sigma^{-1} \in H$. Luego $\sigma(u) \in [Z]_H$, por consiguiente $\#[X]_H \leq \#[Z]_H$.

En forma similar podemos demostrar que $\#[Z]_H \leq \#[X]_H$. De lo anterior se desprende que $\#[Z]_H = \#[X]_H$ que era lo que querîamos demostrar.

LEMA 3. Sean $p > 0$ primo y G un subgrupo transitivo de S_p. Si $H \trianglelefteq G$ y $\#H \geq 2$, entonces H también es transitivo.

Demostración. Sean $[X_1]_H, \ldots, [X_n]_H$ las distintas clases transitivas determinadas por H. Entonces $[X_i]_H \cap [X_j]_H = \phi$, $\forall i \neq j$, y $\bigcup_{i=1}^{n} [X_i]_H = I_p$. Luego $\sum_{i=1}^{n} \#[X_i]_H = p$. Pero por el Lema 2 tenemos que $\#[X_i]_H = \#[X_j]_H$, $\forall i, j \in I_n$. De donde $n\#[X_1]_H = p$. Como p es primo, entonces $n = 1$ ó $\#[X_1]_H = 1$.

Por hipótesis tenemos que $\#H \geq 2$; esto es, existen $x \in I_p$ y $\sigma, \tau \in H$ tales que $\sigma(X) \neq \tau(X)$. Es claro que $\sigma(X)$ y $\tau(X)$ están en $[X]_H$. De donde $\#[X]_H \geq 2$, y por lo tanto $\#[X_1] \geq 2$. Luego $\#[X_1]_H \neq 1$. Lo anterior nos permite afirmar que $n = 1$, lo cual significa que $[X_1]_H = I_p$. Así si $Z, W \in I_p$ entonces $Z \delta X_1$ y $W \delta X_1$. Por consiguiente, $Z \delta W$; es decir, existe $\mu \in H$ tal que $\mu(Z) = W$, luego H es transitivo.

DEFINICION 4. Una permutación $\sigma \in S_q$ es lineal, si existen $b, c \in \mathbb{Z}$ tales que

$$\sigma(x) \equiv bx+c \bmod q \quad \forall x \in I_q.$$

DEFINICION 5. Un subgrupo G de S_q es lineal, si $\forall \sigma \in G$, σ es lineal.

LEMA 4. Si q es primo y $\sigma \in S_q$ es tal que $\sigma \neq id$ y $\sigma(x) \equiv bx+c \bmod q$ para algunos b y c en $\mathbb{Z}$ y $\forall x \in I_q$, entonces $\sigma(x) \neq x$, $\forall x \in I_q$, si y sólo si $b \equiv 1 \bmod q$.

Demostración. $\Leftarrow$) Supongamos que exista $t_o \in I_q$ tal que $\sigma(t_o) = t_o$, entonces $t_o \equiv bt_o + c \bmod q$ Luego $q \mid t_o(b-1)+c$, pero como $q \mid b-1$, entonces $q \mid c$, por lo tanto $\sigma(t) \equiv bt \bmod q$, $\forall t \in I_q$ por ser $b \equiv 1 \bmod q$, entonces $bt \equiv t \bmod q$ $\forall t \in I_q$. De donde $\sigma(t) \equiv t \bmod q$, $\forall t \in I_q$ y por consiguiente $q \mid \sigma(t)-t$ $\forall t \in I_q$. Esto es imposible, si $\sigma(t) \neq t$ para algún $t \in I_q$, ya que $0<|\phi(t) - t| < q$. Por tal razón $\sigma(t) = t$, $\forall t \in I_q$, pero esto implica que $\sigma = id$, lo cual es una contradicción.

$\Rightarrow$) Como q es primo $(\mathbb{Z}_q; +, \cdot)$ es un cuerpo. Si $b \not\equiv 1 \bmod q$, entonces, $[b-1] \neq [0]$. Luego la ecuación $[b-1][x] = -[c]$ tiene una única solución en $\mathbb{Z}_q$ (esta es $[x] = -[b-1]^{-1}[c]$). De donde la congruencia $bx+c \equiv x \bmod q$ tiene solución en Z_q. Por lo tanto existe $x' \in I_q$ tal que $bx'+c \equiv x' \bmod q$. Luego $\sigma(x') \equiv x' \bmod q$. Entonces $q \mid \sigma(x') - x'$. Pero es imposible ya que $0<|\sigma(x') - x'| < q$.

OBSERVACION. Sea E un cuerpo de descomposición de un polinomio $f(z)$ sobre un cuerpo F. En los cursos de Teoría de Cuerpos aprendemos que si

$d_1,\ldots,d_m$ son las raíces de $f(z)$ en E y $\sigma \in G(E;K)$, entonces σ envía raíces de $f(z)$ en raíces de $f(z)$ por lo tanto existe $\sigma_f \in S_m$ tal que $\sigma(d_i) = d_{\sigma_f(i)}$, $\forall i \in I_m$.

Notación. Notaremos $H_f = \{\sigma_f \mid \sigma \in G(E;K)\}$.

TEOREMA. Sea $f(z)$ un polinomio irreducible de grado q primo sobre un cuerpo F, de característica cero. $f(z)$ es soluble, si y sôlo si, previa una conveniente numeración de las raíces de $f(z)$, H_f es un grupo de permutaciones lineales môdulo q y $\forall c \in I_q$, existe $\sigma_c \in H_f$ tal que $\sigma_c(x) \equiv x+c \bmod q$, $\forall x \in I_q$.

Demostración. $\Rightarrow$) Sean E un c.d.d. de $f(z)$ sobre F. Como $f(z)$ es soluble entonces $G(E;F)$ es soluble, luego existe una secuencia soluble: $G_o = G(E;F) \supset \ldots \supset G_\delta \supset G_{\delta+1} = \{id\}$. Como $G_\delta \simeq G_\delta/\{id\}$ y $G_\delta/G_{\delta+1}$ es abeliano, entonces, G_δ es abeliano. Si G_δ no es cíclico, escogemos $\sigma \in G_\delta - \{id\}$ y extendemos esta cadena agregando el subgrupo $\langle\sigma\rangle$ entre G_δ y $G_{\delta+1}$, y esta nueva cadena descendente de subgrupos, sigue siendo una secuencia soluble. De tal forma que podemos suponer sin pérdida de generalidad que G_δ es un grupo cíclico.

Sean $d_1,d_2,\ldots,d_q$ las raíces de $f(z)$ en E

y $\varphi \in G(E;F)$.

En la observación anterior vimos que, existe $\varphi_\delta \in S_q$ tal que

$$\varphi(d_i) = d_{\varphi_\delta(i)} \qquad \forall i \in I_q.$$

$H_\delta = \{\varphi_\delta \in S_q \mid \varphi \in G(E;F)\}$. Es fácil ver que $H_\delta \leqslant S_q$ además si

$$\mathcal{H}: G(E;F) \longrightarrow H_\delta$$
$$\varphi \longmapsto \mathcal{H}(\varphi) = \varphi_\delta$$

entonces $\mathcal{H}$ es un isomorfismo.

Como siempre que tomemos dos raíces de $f(z)$ en E, es posible encontrar un elemento de $G(E;F)$ que envía la una en la otra, entonces H_δ es un grupo transitivo. Además H_δ es soluble y si $\bar{G}_n = \mathcal{H}(G_n)$ $\forall n = 0,\ldots,s+1$, entonces por la Proposición 2 podemos decir que $\{\bar{G}_n\}_{0\leqslant n\leqslant s+1}$ es una secuencia soluble de H_δ.

Veamos que $\bar{G}_s$ es transitivo. En efecto; como $\bar{G}_1 \triangleq H_\delta$, $\#\bar{G}_1 \geqslant \#\bar{G}_s \geqslant 2$ y H_δ es transitivo, aplicando el Lema 3 podemos afirmar que $\bar{G}_1$ es transitivo.

Sea $n \in I_{s-1}$. Supongamos que $\bar{G}_n$ es transitivo. Como $\bar{G}_{n+1} \triangleq \bar{G}_n$ y $\#\bar{G}_{n+1} \geqslant \#\bar{G}_s \geqslant 2$, nue

vamente el Lema 3 nos permite concluir que $\bar{G}_{n+1}$ es transitivo.

De lo anterior se desprende que $\bar{G}_n$ es transitivo $\forall n \in I_\delta$. De donde $\bar{G}_\delta$ es transitivo. Luego $\forall i, j \in I_q$, existe $\varphi_\beta \in \bar{G}_\delta$ tal que $\varphi_\beta(i) = j$. Por lo tanto $\forall i, j \in I_q$ existe $\varphi \in G_\delta$ tal que $\varphi(d_i) = d_j$. En particular $\forall j \in I_q$, existe $\varphi \in G_\delta$ tal que $\varphi(d_1) = d_j$. Como G_δ es cíclico, existe $\tau \in G_\delta$ tal que $G_\delta = \langle \tau \rangle$.

Sean $j \in I_q$ y $\varphi \in G_\delta$ tales que $\varphi(d_1) = d_j$; existe $k \in \mathbb{Z}_+$ tal que $\varphi = \tau^k$, así

$$\{k \in \mathbb{Z}_+ \mid \tau^k(d_1) = d_j\} \neq \phi$$

Sea $k_j = \min\{k \in \mathbb{Z}_+ \mid \tau^k(d_1) = d_j\}$.

Si $\tau^\ell(d_1) = \tau^r(d_1)$ con $1 \leq \ell < r \leq k_j$ entonces

$$\tau^{\ell + k_j - r}(d_1) = \tau^{k_j}(d_1)$$

con $0 < \ell + k_j - r \leq k_j$, lo cual es una contradicción. Luego

$$\forall j \in I_q \quad \tau^\ell(d_1) \neq \tau^h(d_1) \text{ si } 1 \leq \ell < h \leq k_j$$

Por otra parte, si $k_j \geq q+1$, y como $\tau^\ell(d_1)$ es una raíz de $\beta(z)$ $\forall \ell \in I_{k_j}$, entonces $\beta(z)$ tiene más de q raíces, lo cual es imposible ya que el

grado de δ es q. Por lo tanto $1 \leq k_j \leq q$ $\forall j \in I_q$.

En un cuerpo de característica cero un polinomio irreducible tiene todas sus raíces simples, de lo anterior se desprende que

$$\{k_1, k_2, \ldots, k_q\} = I_q$$

y por consiguiente $\{\tau(d_1), \tau^2(d_1), \ldots, \tau^q(d_1)\}$ es el conjunto de raíces de $\delta(z)$. Sean

$$\tau(d_1) = c_1,\ \tau^2(d_1) = c_2, \ldots, \tau^q(d_1) = c_q$$

Sin pérdida de generalidad podemos suponer que $c_1 = d_2$, $c_2 = d_3, \ldots, c_{q-1} = d_q$ y $c_q = d_1$ (ya que desde el principio hubiéramos podido escogerlas de esta forma). Entonces

$$\tau_\delta(1) = 2,\ \tau_\delta(2) = 3, \ldots, \tau_\delta(q-1) = q \text{ y } \tau_\delta(q) = 1$$

Por lo tanto $\tau_\delta = (1, 2, 3, \ldots, q)$.

Por otra parte, como τ genera a G_δ entonces $\bar{G}_\delta$ es generado por τ_δ; es decir $\bar{G}_\delta = \langle(1, 2, \ldots, q)\rangle$. Además es claro que $\tau_\delta(x) \equiv x+1 \bmod q$ $\forall x \in I_q$. Por otra parte

$$\tau_\delta^2(1) = 3,\ \tau_\delta^2(2) = 4, \ldots, \tau_\delta^2(q-2) = q, \tau_\delta^2(q-1) = 1$$

y

$$\tau_\delta^2(q) = 2$$

esto es $\tau_{\delta}^{2}(x) \equiv x+2 \bmod q \quad \forall x \in I_q$ y en general $\forall m \in \mathbb{Z}_+$, $\tau_{\delta}^{m}(x) \equiv x+m \bmod q \quad \forall x \in I_q$. De donde, todos los elementos de $\bar{G}_{\delta}$ son permutaciones lineales de la forma $\sigma_m(x) \equiv x+m \bmod q \quad \forall x \in I_q$ y $\bar{G}_{\delta} = \{\sigma_1, \sigma_2, \ldots, \sigma_{q-1}, \sigma_q = id\}$. Como $\#\bar{G}_{\delta} = q$ (primo) entonces todos los elementos de $\bar{G}_{\delta}$ distintos de id son de orden q y por lo tanto generan a $\bar{G}_{\delta}$.

Si existiera $k \in I_{q-1}$ tal que σ_k no fuera un ciclo de orden q, entonces, σ_k sería un producto de ciclos disyuntos; luego, si i está en uno de estos ciclos y j está en otro, ninguna potencia de σ_k envía a i en j, lo cual es falso ya que $\bar{G}_{\delta}$ es transitivo. Por lo tanto, todos los elementos de $\bar{G}_{\delta}$ son ciclos de orden q.

Veamos por inducción que $\bar{G}_{\delta-n}$ es un grupo de permutaciones lineales $\forall n \in I_{\delta}$ y que todos los ciclos de orden q de $\bar{G}_{\delta-n}$ son los que están en $\bar{G}_{\delta}$.

En efecto, sea $\delta \in \bar{G}_{\delta-1}$, como $\bar{G}_{\delta} \triangleq \bar{G}_{\delta-1}$, entonces $\delta\tau_{\delta}\delta^{-1} \in \bar{G}_{\delta}$. Luego existe $p \in I_q$ tal que $\delta\tau_{\delta}\delta^{-1} = \tau_{\delta}^{p}$. Por lo tanto

$$(\delta\tau\ \delta^{-1})(x) \equiv x+p \bmod q \quad \forall x \in I_q$$

Calculando esta ecuación en $\delta(x)$ obtenemos

$$(\delta\tau_{\delta})(x) \equiv \delta(x)+p \bmod q \quad \forall x \in I_q.$$

Pero si $x \neq q$ entonces $\delta(x+1) \equiv \delta(x)+p \bmod q$. Luego $\delta(2) \equiv \delta(1)+p \bmod q$, $\delta(3) \equiv \delta(2)+p \bmod q$ y por lo tanto $\delta(3) \equiv \delta(1)+2p \bmod q$. $\delta(4) \equiv \delta(3)+p \bmod q$. Entonces $\delta(4) \equiv \delta(1)+3p \bmod q$ y en general $\delta(x) \equiv \delta(1)+(x-1)p \bmod q \quad \forall x \in I_{q-1}$. Esto es $\delta(x) \equiv px+(\delta(1)-p) \bmod q \quad \forall x \in I_{q-1}$. Si $x = q$ se tiene que $\delta(\tau_\delta(q)) \equiv \delta(q)+p \bmod q$ reemplazando $\tau_\delta(q)$ por 1, $\delta(1) \equiv \delta(q)+p \bmod q$. Luego $\delta(q) \equiv pq+(\delta(1)-p) \bmod q$. Por consiguiente $\delta(x) \equiv px+(\delta(1)-p) \bmod q \quad \forall x \in I_q$. Lo cual quiere decir, que δ es una permutación lineal. Si δ fuera un ciclo de orden q, entonces, $\delta(x) \neq x \quad \forall x \in I_q$. Aplicando el Lema 4, tenemos que $p \equiv 1 \bmod q$ entonces, $\delta(x) \equiv \tau_\delta^{\delta(1)-p}(x) \bmod q \quad \forall x \in I_q$, de donde $\delta = \tau_\delta^{\delta(1)-p}$, por lo tanto $\delta \in \bar{G}_\delta = \langle \tau_\delta \rangle$. Es decir, hemos probado que los únicos ciclos de orden q que pertenecen a $\bar{G}_{\delta-1}$ son precisamente los que están en $\bar{G}_\delta$. Supongamos que para $n \geq 1$ $(n < \delta)$ se tenga que $\bar{G}_{\delta-n}$ es un grupo de permutaciones lineales y que los únicos ciclos de orden q que pertenecen a $\bar{G}_{\delta-n}$ son los de $\bar{G}_\delta$. Sea $\rho \in \bar{G}_{\delta-n-1}$. Como $\bar{G}_{\delta-n} \triangleq \bar{G}_{\delta-n-1}$ entonces $\forall \psi \in \bar{G}_{\delta-n}$, $\rho^{-1}\psi\rho \in \bar{G}_{\delta-n}$.

En particular tomando $\psi = \tau_\delta$ tenemos que $\rho^{-1}\tau_\delta\rho \in \bar{G}_{\delta-n}$, pero

$$\rho^{-1}\tau_\delta\rho = \rho^{-1}(1,2,\ldots,q)\rho$$
$$= (\rho(1),\rho(2),\ldots,\rho(q)),$$

luego $\rho^{-1}\tau_\delta\rho$ es un ciclo de orden q, por hipótesis de inducción tenemos que $\rho^{-1}\tau_\delta\rho \in \bar{G}_\delta$.

En forma similar a como lo hicimos con δ, podemos probar que ρ es una permutación lineal y además que si fuese un ciclo de orden q entonces $\rho \in \bar{G}_\delta$.

De lo anterior se desprende que $\bar{G}_{\delta-n}$ es un grupo de permutaciones lineales $\forall n \in I_\delta$ y que todos los ciclos de orden q de $\bar{G}_{\delta-n}$ son los que están en $\bar{G}_\delta$.

En particular, $\bar{G}_o = H_\delta$ es un grupo de permutaciones lineales y los ciclos de orden q de H_δ son los que están en $\bar{G}_\delta$, es decir todas las permutaciones lineales de la forma σ_c, en donde $c \in I_q$ y $\sigma_c(x) \equiv x+c \bmod q \quad \forall x \in I_q$.

$\Leftarrow$) El conjunto N de todas las permutaciones lineales de la forma $\sigma_c(x) \equiv x+c \bmod q \quad \forall x \in I_q$ donde $c \in I_q$, es un subgrupo de S_q. Además, en forma similar a como lo hicimos al iniciar la demostración, podemos ver que

$$N = \langle(1,2,\ldots,q)\rangle = \langle\sigma_1\rangle.$$

Si $\gamma \in H_\delta$, entonces $\gamma^{-1}\sigma_1\gamma = \gamma^{-1}(1,2,\ldots,q)\gamma = (\gamma(1),\gamma(2),\ldots,\gamma(q))$.

Luego $\gamma^{-1}\sigma_1\gamma$ no deja ningún elemento fijo. Pero por el lema 4 tenemos que las únicas permutaciones lineales que no dejan ningún elemento fijo son precisamente las de N. Luego $\gamma^{-1}\sigma_1\gamma \in N$.

Pero como N es un subgrupo de H_{δ} entonces

$$\gamma^{-1}\sigma_1^k\gamma = (\gamma^{-1}\sigma_1\gamma)^k \in N \qquad \forall k \in \mathbb{Z}$$

De donde, $\forall \gamma \in H_{\delta}$, $\forall \mu \in N$, $\gamma^{-1}\mu\gamma \in N$, es decir $N \trianglelefteq H_{\delta}$.

Para demostrar que $\delta(z)$ es soluble, basta probar que $G(E;F)$ es soluble. Pero como $G(E;F)$ es isomorfo a H_{δ} entonces nos limitaremos a demostrar que H_{δ} es soluble; la proposición 4 nos garantiza que esto puede lograrse, si demostramos que N y H_{δ}/N son solubles.

En efecto, sean τ y $\mu \in H_{\delta}$. Existen $a,b,c,d \in \mathbb{Z}$ tales que $\tau(x) \equiv bx+c \bmod q$ y $\mu(x) \equiv ax+d \bmod q$ $\forall x \in I_q$.

Supongamos que $\tau N = \mu N$. Como $N \trianglelefteq H_{\delta}$, tenemos que $\tau N = N\tau$ y $\mu N = N\mu$. Luego $N\tau = N\mu$. Sea $\sigma \in N$ tal que $\sigma(x) \equiv x+c \bmod q$. Como $N \leqslant H_{\delta}$, $\sigma^{-1} \in N$. Luego existe $h \in \mathbb{Z}$ tal que $\sigma^{-1}(x) \equiv x+h \bmod q$ $\forall x \in I_q$. Pero $x = \sigma(\sigma^{-1}(x)) \equiv (x+h)+c \bmod q$. Luego $h \equiv -c \bmod q$ y por lo tanto $\sigma^{-1}(x) \equiv x-c \bmod q$. Como $\sigma^{-1}\tau \in N\tau$, entonces

$\sigma^{-1}\tau \in N\mu$. Luego existe $\theta \in N$ tal que $\sigma^{-1}\tau = \theta\mu$

Sea $\theta(x) \equiv x+\beta \bmod q \quad \forall x \in I_q$. Entonces $(\theta\mu)(x) \equiv \mu(x)+\beta \bmod q \equiv ax+d+\beta \bmod q \quad \forall x \in I_q$ y $(\sigma^{-1}\tau)(x) \equiv \tau(x)-c \bmod q \equiv bx \bmod q \quad \forall x \in I_q$. Luego $bx \equiv ax+d+\beta \bmod q \quad \forall x \in I_q$.

En particular si $x = q$, entonces $0 \equiv d+\beta \bmod q$. Por lo tanto $bx \equiv ax \bmod q \quad \forall x \in I_q$. Si tomamos $x = 1$, obtenemos $b \equiv a \bmod q$.

Lo anterior nos permite construir la siguiente función:

$$\Gamma : H_\beta/N \longrightarrow \mathbb{Z}_q$$
$$\tau N \longmapsto \Gamma(\tau N) = [b],$$

si y sólo si $\tau(x) \equiv bx+c \bmod q$, para algún $c \in \mathbb{Z}$.

Veamos que Γ es un homomorfismo. En efecto sean τN y μN en H_β/N con $\tau(x) \equiv bx+c \bmod q$ y $\mu(x) \equiv ax+d \bmod q \quad \forall x \in I_q$. $\Gamma(\tau N\mu N) = \Gamma(\tau\mu N)$. Pero $(\tau\mu)(x) \equiv bax+bd+c \bmod q \quad \forall x \in I_q$. Por lo tanto $\Gamma(\tau\mu N) = [ba] = [b][a] = \Gamma(\tau N)\Gamma(\mu N)$.

De lo anterior se desprende que Γ es un homomorfismo. Γ es uno a uno ya que si $\tau(x) \equiv bx+c \bmod q \quad \forall x \in I_q$ y $\Gamma(\tau N) = [1]$. Entonces $[b] = [1]$, por consiguiente $b \equiv 1 \bmod q$. De donde $\tau \in N$, lo cual implica que $\tau N = N$. Lo anterior

nos permite concluir que H_f/N es isomorfo a un subgrupo del grupo multiplicativo de los elementos invertibles de $\mathbb{Z}_q$ con el producto, pero como $(\mathbb{Z}_q;\cdot)$ es conmutativo, entonces H_f/N es abeliano y por lo tanto soluble (Proposición 4).

Por otra parte; como N es cíclico, entonces es abeliano y así soluble.

COROLARIO 1. Sea $f(z)$ un polinomio de grado q primo, irreducible y soluble sobre un cuerpo F de característica cero. Entonces la única permutación de H_f que deja por lo menos dos elementos fijos, es la idéntica.

Demostración. Por el teorema anterior tenemos que, previa una conveniente numeración de las raíces de $f(z)$, H_f es un grupo de permutaciones lineales módulo q y en H_f están todas las permutaciones lineales de la forma $\sigma(x) \equiv x+c \bmod q$ $\forall c \in I_q$. Sea $\sigma \in H_f$, existen $b,c \in \mathbb{Z}$ tales que $\sigma(x) \equiv bx+c \bmod q$ $\forall x \in I_q$. Si podemos encontrar $d \in I_q$ tal que $\sigma(d) = d$, entonces por el Lema 4, tenemos que $b \not\equiv 1 \bmod q$. En este caso la ecuación

$$x \equiv bx+c \bmod q$$

tiene una única solución en el cuerpo $\mathbb{Z}_q$ y esta es

$$[x] = [c]\,([1]-[b])^{-1}\,.$$

Es decir, cualquier permutación en H_f distinta de la idéntica, deja fijo a lo más un elemento y por lo tanto, la única permutación de H_f que deja más de un elemento fijo es la idéntica.

COROLARIO 2. Sea $f(z)$ un polinomio de grado q primo impar, irreducible y soluble sobre un subcuerpo F de $\mathbb{R}$. Entonces, $f(z)$ tiene una única raíz real o todas sus raíces son reales.

Demostración. Sea E un c.d.d. de $f(z)$ sobre F. Sabemos por el Corolario 1 que la única permutación de H_f que deja fijos por lo menos dos elementos, es la idéntica.

Por otra parte, como q es impar, $f(z)$ tiene por lo menos una raíz real. Si tuviese dos o más, el automorfismo $\sigma \in G(E;F)$ tal que $\sigma(z) = \bar{z}$ dejaría fijas a por lo menos dos raíces de $f(z)$; luego la permutación $\sigma_f \in H_f$, deja por lo menos dos elementos fijos, lo cual implica por el corolario anterior, que σ_f es la permutación idéntica. De esto se desprende que $\sigma = id$ y por lo tanto, todas las raíces de $f(z)$ son reales.

COROLARIO 3. Sea $f(z)$ un polinomio de grado $q \geq 5$ primo, irreducible sobre un subcuerpo F de $\mathbb{R}$. Si $f(x)$ tiene exactamente n raíces reales, con $2 < n < q$, entonces no es soluble por radicales sobre F.

Demostración. Si $f(z)$ fuese soluble por radicales sobre F, entonces tendría una raíz real, o, todas sus raíces serían reales, lo cual es una contradicción.

OBSERVACION. Con el fin de tener suficiente claridad sobre el porqué se tomó $n > 2$ y nó $n \geq 2$, vale la pena recordarle al lector, que todo polinomio de grado impar sobre un subcuerpo de $\mathbb{R}$ que tenga por lo menos dos raíces reales, tiene por lo menos tres raíces reales.

EJERCICIO 1. Sean q primo $q \geq 5$ y $a, b \in \mathbb{Z}$ tales que $1 < b < a^{q-1} - 1$, si $f(z) = z^q - az + b$ es irreducible sobre $\mathbb{Q}$, entonces no es soluble por radicales.

Desarrollo. Como $f(0) = b > 0$, $f(1) = 1 - a + b < 0$ y $f(b) = b^q - ab + b = b(b^{q-1} - a + 1) > 0$ y $f(z)$ es una función contínua, entonces por el teorema de Bolzano su gráfica corta por lo menos dos veces al eje real; es decir $f(z)$ tiene por lo menos dos raíces reales, lo cual implica que $f(z)$ tiene por lo menos tres raíces reales.

Por otra parte $f'(z) = qz^{q-1} - a$ tiene sólo dos raíces reales; esto es, $f(z)$ tiene a lo más dos puntos críticos y por tal razón corta al eje real en el mejor de los casos en tres puntos distintos.

De las observaciones anteriores se desprende que $f(z)$ tiene exactamente tres raíces reales, lo cual implica, según el corolario 3, que $f(z)$ no es soluble por radicales.

EJEMPLO 1. Si p es primo, el polinomio $f(z) = z^q - p^2z + p$ no es soluble por radicales sobre $\mathbb{Q}$, para todo primo $q \geq 5$.

Desarrollo. $f(z)$ es irreducible sobre $\mathbb{Q}$ (criterio de Eisenstein), además $1 < p < p^2 - 1 < p^{q-1}$. Luego $f(z)$ no es soluble por radicales.

EJERCICIO 2. Sean q primo $q \geq 5$ y $a, b \in \mathbb{Z}$ tales que $1 < b < a-1 < b^{q-1}$, si $f(z) = z^q - az^2 + b$ es irreducible sobre $\mathbb{Q}$, entonces no es soluble por radicales.

Desarrollo. Similar al anterior, como puede comprobar el lector.

EJEMPLO 2. Si p es primo, el polinomio $f(z) = z^q - p^2z^2 + p$ no es soluble por radicales sobre $\mathbb{Q}$, para todo primo $q \geq 5$.

Desarrollo. Consecuencia inmediata del ejercicio 2 y del criterio de Eisenstein.

EJERCICIO 3. Sean $q \geq 5$ y $f(z) = z^q + a_{q-1}z^{q-1} + \ldots + a_3z^3 + a_o$ un polinomio irreducible sobre $\mathbb{Q}$; si $f(z)$ tiene más de una raíz real, entonces no es soluble por radicales sobre $\mathbb{Q}$.

Desarrollo. Si $f(z)$ tiene más de una raíz real entonces tiene por lo menos tres raíces reales porque q es impar.

Por otra parte, como

$$f'(z) = z^2(qz^{q-3}+a_{q-1}(q-1)z^{q-4}+\ldots+3a_3)$$

la ecuación $f'(z) = 0$ tiene, en el mejor de los casis, $q-2$ raíces distintas. Por lo tanto hay a lo más $q-2$ puntos críticos, lo cual implica que no se pueden presentar más de $q-1$ cortes con el eje real; es decir no es posible que todas las raíces de $f(z)$ sean reales (recuerde que $f(z)$ no tiene raíces múltiples ya que es irreducible sobre $\mathbb{Q}$). De donde, por el corolario 3 podemos concluír que $f(z)$ no es soluble por radicales sobre $\mathbb{Q}$.

EJEMPLO 3. Sean $q \geq 5$ primo y $p \geq 3$ primo, entonces el polinomio $f(z) = z^q+pz^4-p^2z^3+p$ no es soluble por radicales sobre $\mathbb{Q}$.

Desarrollo. $f(z)$ es irreducible sobre $\mathbb{Q}$, por el criterio de Eisenstein. Por otra parte $f(0) = p > 0$, $f(1) = 1+2p-p^2 < 0$ porque $1+2p-p^2 < p+2p-p^2 \leq 3p-p^2 \leq p^2-p^2 \leq 0$ y $f(p) = p^q+p > 0$. Luego $f(z)$ tiene más de una raíz real. Aplicando el ejercicio 3 tenemos que $f(z)$ no es soluble por radicales sobre $\mathbb{Q}$.

OBSERVACION. Como hemos visto, el criterio que se demostró en el Corolario 3, nos permite construir muchos ejemplos de polinomios no solubles. Sería conveniente que el lector presentara otros ejemplos.

En general $\forall n \in \mathbb{Z}_+$, $n \geq 5$ siempre es posible encontrar, polinomios de grado n que no sean solubles por radicales.

*

BIBLIOGRAFIA

[1] Artin, E., *La Teoría de Galois*. Editorial Vicens-vives. Barcelona, 1970. pp.74-77.

[2] Warner, S., *Classical Modern Algebra*. Prentice-Hall. New Jersey, 1971. Cap.VIII.

[3] Caycedo, F., *Temas de Teoría de Grupos*. Depto. de Mat. y Est. U.Nal. Bogotá.

[4] Dean, R.A., *Elements of Abstract Algebra*. Wiley International Edition. Cap. IX y X.

* *

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
BOGOTA. D.E.