Boletín de Matemáticas
Vol. XVII Nº 1,2,3 (1983)

SOBRE UN EJEMPLO DE ARTIN

Luis E. Giraldo Montes

Si x es trascendente sobre el campo K el grupo G de los automorfismos de $K(x)$ que dejan fijo a K esta constituído por los automorfismos $\sigma_{a,b,c,d}$ donde $\sigma_{a,b,c,d}(x) = \frac{ax+b}{cx+d}$ con $ad-bc \neq 0$. G es isomorfo al grupo proyectivo lineal de grado 2 sobre K,

$$PLG_2(K) = GL_2(K)/\{kI_2 \mid k \in K^*\} ,$$

ya que la aplicación

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longrightarrow \sigma_{a,b,c,d}$$

es un epimorfismo del grupo general lineal de grado 2 sobre K en G cuyo núcleo es precisamente el subgrupo de $GL_2(K)$ formado por las matri-

ces escalares no nulas. Usando el Teorema de Artin-Kronecker el cual nos dice que si L es un cuerpo cualquiera y T un grupo *finito* de automorfismos de L entonces L es extensión galoisiana del campo fijo L^T de T y el grado de L sobre L^T es $[L:L^T] = \theta(T)$ (el orden de T), vemos que si un grupo finito H se sumerge en $PLG_2(K)$ podemos realizar a H como un grupo de Galois.

En efecto, como T es subgrupo de $Gal(L/L^T)$ (el grupo de Galois de L sobre L^T) y $\theta(Gal(L/L^T)) = [L:L^T] = \theta(T)$ tenemos $T = Gal(L/L^T)$: todo lo anterior se hace en [2] como una disgresión en el transcurso de la demostración del Teorema de Luroth sobre Extensiones Trascendentes (ver [3]).

El ejemplo usual clásico debido a Artin (ver [1]), que ilustra la situación anterior es el siguiente: El subgrupo S de G generado por

$$x \xrightarrow{X} \frac{1}{x} \quad , \quad x \xrightarrow{Y} \frac{1}{1-x}$$

es isomorfo al grupo simétrico S_3 y un elemento y de $K(x)$ que genera al campo fijo de S sobre K (es decir, $K(y) = K(x)^S$) es

$$y = \frac{(x^2-x-1)^3}{x^2(x-1)^2}$$

por lo tanto $S_3 \approx Gal(K(x)|K(y))$.

Las dos preguntas naturales son:

(1) Es cierto que $y \in K(x)^S$?

(2) En caso afirmativo, cómo hizo Artin para encontrar tal y?

La veneración que yo siento por Artin me impidió tratar de responder la primera pregunta, abordando directamente la segunda: Para ello recordemos que una manera de producir elementos en L^T si $T = \{t_1,\ldots,t_m\}$ es considerar funciones simétricas de los elementos $t_1(\ell),\ldots,t_m(\ell)$ para $\ell \in L$. En particular, las funciones simétricas elementales de dichos elementos

$$\sigma_1(\ell) = t_1(\ell)+\ldots+t_m(\ell) = \text{Traza de } \ell.$$

$$\vdots$$

$$\sigma_i(\ell) = \sum_{1\le j_1<\ldots<j_i\le m} t_{j_1}(\ell)t_{j_2}(\ell)\ldots t_{j_i}(\ell)$$

$$\vdots$$

$$\sigma_m(\ell) = t_1(\ell)t_2(\ell)\ldots t_m(\ell) = N(\ell) = \text{Norma de } \ell.$$

pertenecen a L^T para cada $\ell \in L$.

Si L como extensión de K tiene un elemento primitivo λ (o sea $L = K(\lambda)$) y queremos en-

contrar un ℓ que genere a L^T sobre K, se acostumbra tomar $\ell = r$ y tratar con $\sigma_1(r)$ y $\sigma_m(r)$ que son las más sencillas. Si no funcionan se consideran funciones simétricas más complicadas.

Ilustremos lo anterior con un ejemplo sencillo.

PROBLEMA: Determinar el grupo de Galois de $f(x) = x^4 - 10x^2 + 1$ sobre los racionales $\mathbb{Q}$ e ilustrar la correspondencia galoisiana exhibiendo cada campo intermedio entre $\mathbb{Q}$ y el campo de descomposición L de $f(x)$ como una extensión simple de $\mathbb{Q}$.

Solución: Como $f(x)$ es bicuadrático sus raíces son las raíces cuadradas de las raíces de $v^2 - 10v + 1$ o sea $\pm\sqrt{5\pm2\sqrt{6}}$ y ya que $(5+2\sqrt{6})\cdot(5-2\sqrt{6}) = 1$, las raíces de $f(x)$ son r, $-r$, r^{-1} y $-r^{-1}$ si hacemos $r = 5+2\sqrt{6}$. Luego $L = \mathbb{Q}(r)$ y como $f(x)$ es irreducible sobre $\mathbb{Q}$ tenemos

$$\theta(Gal(f(x)|\mathbb{Q})) = [L:\mathbb{Q}] = 4.$$

Por lo tanto $Gal(x^4-10x^2+1/\mathbb{Q})$ es cíclico o el cuarto grupo de Klein V.

A continuación lo describimos como grupo

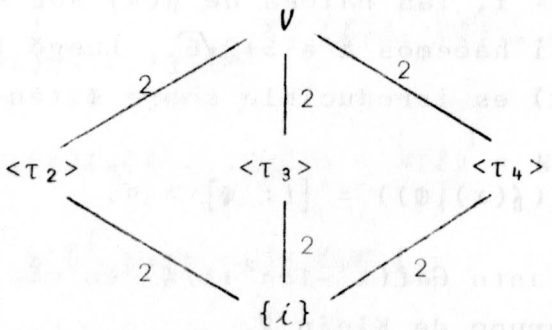
de permutaciones de las cuatro raíces para averiguar con cual alternativa nos quedamos:

Raíces R	r	$-r$	r^{-1}	$-r^{-1}$
$\tau_1(R)$	r	$-r$	r^{-1}	$-r^{-1}$
$\tau_2(R)$	r^{-1}	$-r^{-1}$	r	$-r$
$\tau_3(R)$	$-r$	r	$-r^{-1}$	r^{-1}
$\tau_4(R)$	$-r^{-1}$	r^{-1}	$-r$	r

o sea

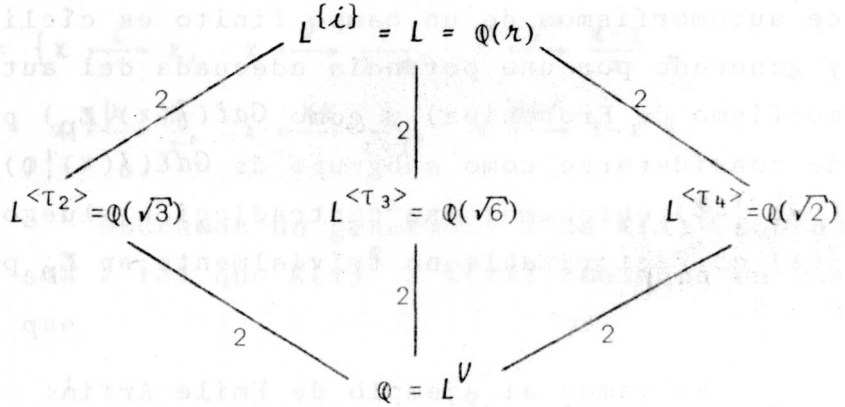
$$\tau_1 = id$$
$$\tau_2 = (r, r^{-1})(-r, -r^{-1})$$
$$\tau_3 = (r, -r)(r^{-1}, -r^{-1})$$
$$\tau_4 = (r, -r^{-1})(-r, r^{-1})$$

Por lo tanto $Gal(x^4-10x^2+1|\mathbb{Q})$ es V y su diagrama de subgrupos con índices es



De acuerdo al Teorema Fundamental de la Teoría

de Galois el diagrama de campos intermedios con grados entre $\mathbb{Q}$ y $L = \mathbb{Q}(r)$ es



Como $<\tau_2> = \{L, \tau_2\}$, en $L^{<\tau_2>}$ están $r\tau_2(r) = 1$ y $\sigma_1(r) = r + r^{-1} = \sqrt{5+2\sqrt{6}} + \sqrt{5-2\sqrt{6}} = \rho$, $\rho^2 = 12$, $\rho = 2\sqrt{3}$ luego $L^{<\tau_2>} = \mathbb{Q}(\sqrt{3})$.

En forma similar se puede observar que $L^{<\tau_3>} = \mathbb{Q}(\sqrt{6})$ y $L^{<\tau_4>} = \mathbb{Q}(\sqrt{2})$.

NOTA: $f(x)$ tiene la interesante propiedad de ser irreducible sobre $\mathbb{Q}$ pero $\overline{f}(x) \in \mathbb{Z}_p[x]$ es reducible para cada primo p. En efecto, si $p = 2$ ó $p = 3$, $\overline{f}(x) = (x^2+1)^2$. Para $p \geq 5$ como $f'(x) = 4x^3 - 20x = 4x(x^2-5) = 0$ si y sólo si $x = 0$ ó $x^2 = 5$ y cuando reemplazamos x^2 por 5 en $f(x)$ obtenemos $-24 \neq 0$, $f(0) = 1$ vemos que $\overline{f}(x)$

es separable sobre $\mathbb{Z}_p$ para $p \geq 5$. Si $\overline{f}(x)$ fuera irreducible en $\mathbb{Z}_p$, $Gal(\overline{f}(x)|\mathbb{Z}_p)$ sería cíclico de orden 4 a lo menos (recordar que todo grupo de automorfismos de un campo finito es cíclico y generado por una potencia adecuada del automorfismo de Frobenius) y como $Gal(\overline{f}(x)|\mathbb{Z}_p)$ puede considerarse como subgrupo de $Gal(f(x)|\mathbb{Q})$ (ver [4]) obtenemos una contradicción, luego $\overline{f}(x)$ es factorizable no trivialmente en $\mathbb{Z}_p$ para $p \geq 5$.

Volvamos al ejemplo de Emile Artin:

Para ver que $S = \langle X, Y \rangle \cong S_3$ basta mostrar que $\theta(X) = 2$, $\theta(Y) = 3$ y $XY = Y^2X$ (ya que ésta es la presentación de S_3). Verifiquémoslo:

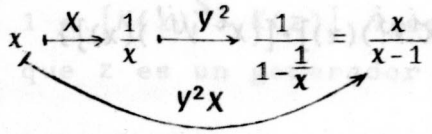
$$x \xrightarrow{X} \frac{1}{x} \xrightarrow{X} \frac{1}{\frac{1}{x}} = x \qquad \text{luego } \theta(X) = 2$$

$$x \xrightarrow{y} \frac{1}{1-x} \xrightarrow{y} \frac{1}{1-\frac{1}{1-x}} = 1-\frac{1}{x} \xrightarrow{y} 1-\frac{1}{\frac{1}{1-x}} = x$$

y^3 luego $\theta(Y) = 3$

$$x \xrightarrow{y} \frac{1}{1-x} \xrightarrow{X} \frac{1}{1-\frac{1}{x}} = \frac{x}{x-1}$$

XY



Por tanto $XY = Y^2X$

$$S = \{x \xrightarrow{i} x,\ x \xrightarrow{y} \frac{1}{1-x},\ x \xrightarrow{y^2} \frac{x-1}{x},$$
$$x \xrightarrow{X} \frac{1}{x},\ x \xrightarrow{XY} \frac{x}{x-1},\ x \xrightarrow{XY^2} 1-x\ \}$$

Buscamos un generador z de $K(x)^S$ sobre K (o sea z tal que $K(x)^S = K(z)$) teniendo en cuenta que

$$6 = \theta(S) = [K(x) : K(x)^S] = [K(x) : K(z)]$$
$$= gr(Irr(x, K(z))),$$

y nuestro mecanismo de producción de elementos en $K(x)^S$:

$$\sigma_6(x) = \prod_{i=0}^{1} \prod_{j=0}^{2} (X^iY^j)(x) = x \cdot \frac{1}{1-x} \cdot \frac{x-1}{x} \cdot \frac{1}{x} \cdot \frac{x}{x-1} \cdot (1-x) = 1$$

$$\sigma_1(x) = \sum_{i=0}^{1} \sum_{j=0}^{2} (X^iY^j)(x) = x + \frac{1}{1-x} + \frac{x-1}{x} + \frac{1}{x} + \frac{x}{x-1} + 1-x = 3$$

Observamos que ninguna de las dos funciones simétricas más sencillas nos sirvió, luego no queda más remedio que considerar funciones simétricas mas complicadas:

$$\sigma_2(x) = \sum_{i,i'=0}^{1} \sum_{j,j'=0}^{2} \{[(x^i y^j)(x)] \cdot [(x^{i'} y^{j'})(x)]\}$$

$$(i,j) \neq (i',j')$$

$$= 1 + \frac{x}{1-x} + x - 1 + \frac{x^2}{x-1} + x(1-x) + \frac{1}{x(1-x)} + \frac{x-1}{x^2} +$$

$$+ \frac{1}{x-1} + \frac{1-x}{x} + \frac{-1}{x} + \frac{-x}{(1-x)^2} + 1 + 1 + \frac{-(1-x)^2}{x} + (-x)$$

$$= \frac{-x^5+3x^5-5x^3+3x-1}{x^2(1-x)^2}$$

Si tomamos $z = -\sigma_2(x)$ tenemos $z \in K(x)^S$ luego $K(z)$ es subcampo de $K(x)^S$ así

$$gr(Irr(x,K(z))) = [K(x):K(z)]$$

$$= [K(x):K(x)^S][K(x)^S:K(z)]$$

$$= 6[K(x)^S:K(z)] ,$$

(ya que por el teorema de Artin-Kronecker $[K(x):K(x)^S] = \theta(S) = 6$) o sea $gr(Irr(x,K(z))) \geq 6$. Pero de la expresión $z = \frac{x^6-3x^5+5x^3-3x+1}{x^2(1-x)^2}$ se deduce que x es raíz del polinomio

$$g(\delta) = (\delta^6-3\delta^5-z\delta^4+(2z+5)\delta^3-z\delta^2-3\delta+1) \in K(z)[\delta]$$

luego de necesidad $g(\delta) = Irr(x,K(z))$ y

$1 = [K(x)^S : K(z)]$ ó sea $K(x)^S = K(z)$ y tenemos que z es un generador de $K(x)^S$ sobre K .

Como (según Artin) $y = \frac{(x^2-x-1)^3}{x^2(x-1)^2}$ es también generador, entonces $K(z) = K(y)$ de donde $gr(Irr(y, K(z))) = 1$ lo que induce a sospechar que z y y deben coincidir. Para tratar de verificarlo calculamos $(x^2-x-1)^3$ y obtenemos

$$(x^2-x-1)^3 = x^6-3x^5+5x^3-3x - 1.$$

O sea que las expresiones de z y y solo difieren por el signo del término constante de sus numeradores!

Esto me hizo revisar las operaciones para encontrar el error aritmético que yo había cometido. Al no encontrar el error busqué la respuesta a la pregunta $¿y \in K(x)^S$? Como $S = \langle X, Y \rangle$ bastará ver que y es invariante tanto por X como por Y

$$y = \frac{(x^3-x-1)^3}{x^2(x-1)^2} \xrightarrow{X} \frac{\left(\left(\frac{1}{x}\right)^2-\frac{1}{x}-1\right)^3}{\left(\frac{1}{x}\right)^2\left(\frac{1}{x}-1\right)^2} = \frac{(-x^2-x+1)^3}{x^2(1-x)^2} \neq y$$

Por ende $y \notin K(x)^S$. Pero como fácilmente se verifica que $\frac{(x^2-x+1)^3}{x^2(x-1)^2}$ es invariante bajo X ello lleva a pensar que hay un error de sig

no en mis apuntes y que el Y que Artin pensó es en realidad $\frac{(x^2-x+1)^3}{x^2(x-1)^2} = \omega$.

Aplicamos Y a este ω:

$$\omega \xrightarrow{Y} \frac{((\frac{1}{1-x})^2 - \frac{1}{1-x} + 1)^3}{(\frac{1}{1-x})^2(\frac{1}{1-x} - 1)^2} = \omega$$

Luego $K(\omega) = K(x)^S$ y es cierto lo del error de signo en mis apuntes. A continuación verifiqué que z es invariante bajo X y bajo Y de donde $K(\omega) = K(x)^S = K(z)$ lo que confirma que z es también generador.

Como $(x^2-x+1)^3 = x^6-3x^5+6x^4-7x^3+6x^2-3x+1$ tenemos $z \neq \omega$ y continúa sin respuesta la segunda pregunta natural. Surge otra pregunta interesante:

Como $K(\omega) = K(z)$ tenemos que $\omega \in K(z)$ luego existen $a_0,\ldots,a_n$, $b_0,\ldots,b_m$ en K tales que

$$\omega = \frac{a_0+a_1z+\ldots+a_nz^n}{b_0+b_1z+\ldots+b_mz^m} \quad (a_n \neq 0 \neq b_m)$$

La pregunta es cómo hallar los a_i y los b_j.

Usando las primeras ideas de la demostración del Teorema de Luroth simplificamos conven

ciéndonos $\omega = \dfrac{a_0+a_1 z}{b_0+b_1 z}$ $(a_1 \neq 0 \neq b_1)$ y luego por tanteo vemos que $\omega = z + 6$ vislumbrando así la respuesta a la segunda pregunta natural.

*

BIBLIOGRAFIA

[1] Artin, Emile, *Galois Theory.*

[2] Gentile, Enzo R., Notas de clase del curso de Algebra III, Universidad de Buenos Aires, 1982.

[3] Jacobson, Nathan, *Lectures in Abstract Algebra*, Vol. III.

[4] Van der Waerden, *Modern Algebra.*

* * *