Universidad Nacional Autónoma de México

Posgrado en Ciencias Matemáticas
Facultad de Ciencias

SOBRE ALGUNOS RESULTADOS DE LA TEORÍA DE GALOIS

T E S I N A

QUE PARA OBTENER EL GRADO ACADÉMICO DE:

MAESTRO EN CIENCIAS

PRESENTA:

MANUEL GERARDO ZORRILLA NORIEGA

DIRECTOR DE LA TESINA:
DR. JUAN MORALES RODRÍGUEZ

MÉXICO, D.F.
JUNIO, 2010

Índice general

Introducción

Este trabajo está dividido en tres capítulos: resultados teóricos, problemas y ejemplos. Para su lectura, se supone familiaridad con los resultados que se cubren en un curso básico de teoría de Galois (hasta el teorema fundamental de la teoría de Galois y el teorema de Steinitz). Los criterios usados para incluir artículos fueron su importancia teórica y su valor ilustrativo (aparte de las razones estéticas).

Varios de los resultados que se presentan aquí fueron enunciados o propuestos como problemas durante un curso de álgebra que estudié en la maestría. Ésta fue mi motivación principal para realizar esta tesina.

Concretamente, se tocarán los temas del gran teorema de Galois, el teorema del elemento primitivo, el teorema llamado del *casus irreducibilis* y una consecuencia suya (que no existe una fórmula general en términos de radicales reales para obtener una raíz cúbica de un número complejo). Se harán algunas observaciones sobre las funciones simétricas que permitirán demostrar que todo grupo finito es el grupo de Galois de algún polinomio, y se abordará el problema de, dado un subgrupo H de S_4, exhibir un polinomio con coeficientes racionales cuyo grupo de Galois sea H. Se darán finalmente algunos ejemplos, incluyendo una extensión de campos finita pero no simple y un polinomio que no es soluble por radicales pero cuyo grupo de Galois es soluble.

La notación y las convenciones que se manejan a lo largo de este trabajo coinciden, en general, con las usadas en [Rot1] (con excepción de la definición de normalidad de una extensión). Repasemos las que no son usuales. Si E, F son campos, $E : F$ denota una extensión de campos, $[E : F]$ su grado, $\mathrm{Gal}(E : F)$ su grupo de Galois, y, si H es un conjunto de automorfismos de E, E^H el campo fijo de H. Diremos que $E : F$ es *normal* si y sólo si cada vez que un polinomio en $F[x]$ irreducible tiene una raíz en E, tiene todas sus raíces en E (sabemos[1] que, en presencia de finitud de $E : F$,

[1] Véase [St, Teorema 9.9].

esto es equivalente a que $E : F$ sea campo de descomposición de algún polinomio en $F[x]$). Diremos que $E : F$ es *de Galois* si y sólo si es finita, normal y separable (sabemos[2] que esto, en presencia de finitud de $E : F$, es equivalente a que $E^{\mathrm{Gal}(E:F)} = F$). Se tiene[3] que la extensión $E : F$ es de Galois si y sólo si es campo de descomposición de algún pollinomio separable en $F[x]$. Lo demás es razonablemente estándar.

[2]Véase [Rot1, Teorema 81] ó [St, Teorema 11.12 y 11.14].
[3]Véase [Rot1, Teorema 81]

Capítulo 1

Teoría General

1.1. El Gran Teorema de Galois

En la mayor parte de los cursos básicos sobre teoría de Galois, se estudia que, en campos de caractrística 0, un polinomio soluble por radicales tiene por fuerza un grupo de Galois soluble, y así se puede dar una ecuación polinomial de grado 5 que no es soluble por radicales. Probaremos la afirmación recíproca, es decir, que en un campo de característica 0 todo polinomio cuyo grupo de Galois es un grupo soluble es soluble por radicales, que es lo que se conoce como el gran teorema de Galois. Seguiremos a [Rot1, pp 90-95], y requerimos cierta familiaridad con el tema de solubilidad de grupos, que se puede revisar en [Al] o en [Rot1, Ap. B].

Necesitamos algunos resultados previos.

Lema 1.1 (Irracionalidades Accesorias)**.** *Sea $E : F$ un campo de descomposición de $f(x) \in F[x]$ con $G = \mathrm{Gal}(E : F)$. Si $F^* : F$ es una extensión y $E^* : F^*$ es un campo de descomposición de $f(x) \in F^*[x]$ que contiene a E, entonces la restricción $\sigma \mapsto \sigma \restriction_E$ es un homomorfismo inyectivo*

$$\mathrm{Gal}(E^* : F^*) \to \mathrm{Gal}(E : F).$$

Demostración. Tenemos, por hipótesis, que

$$E = F(\alpha_1, \ldots, \alpha_n)$$

y que

$$E^* = F^*(\alpha_1, \ldots, \alpha_n),$$

donde $\alpha_1, \ldots, \alpha_n$ son las raíces de $f(x)$. Si $\sigma \in \mathrm{Gal}(E^* : F^*)$, entonces σ permuta las α_i's y deja fijo a F^*, y por tanto a F; así, $\sigma \restriction_E \in \mathrm{Gal}(E : F)$. La inyectividad se observa. □

Definición 1.2. *Si $E : F$ es una extensión de Galois y $\alpha \in E^{\#} = E \backslash \{0\}$, definimos su* ***norma*** *$N(\alpha)$ como*

$$N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(E:F)} \sigma(\alpha).$$

Las siguientes son propiedades fundamentales de la norma, de demostración fácil. En (i) y en (iv), $G = \mathrm{Gal}(E : F)$.

(i) Si $\alpha \in E^{\#}$, entonces $N(\alpha) \in F^{\#}$ (pues $N(\alpha) \in E^G = F$).

(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$, con lo que $N : E^{\#} \to F^{\#}$ es un homomorfismo.

(iii) Si $\alpha \in F^{\#}$, entonces $N(\alpha) = \alpha^{[E:F]}$.

(iv) Si $\sigma \in G$ y $\alpha \in E^{\#}$, entonces $N(\sigma(\alpha)) = N(\alpha)$.

El siguiente resultado debe su nombre a que fue el nonagésimo teorema de una exposición de Hilbert sobre teoría algebraica de números, en 1897.

Lema 1.3 (Teorema 90 de Hilbert)**.** *Sea $E : F$ una extensión de Galois con $G = \mathrm{Gal}(E : F)$ cíclico de orden n; sea σ un generador de G. Entonces $N(\alpha) = 1$ si y sólo si hay $\beta \in E^{\#}$ tal que*

$$\alpha = \beta\sigma(\beta)^{-1}.$$

Demostración. Si $\alpha = \beta\sigma(\beta)^{-1}$, entonces

$$\begin{aligned} N(\alpha) &= N(\beta\sigma(\beta)^{-1}) \\ &= N(\beta)N(\sigma(\beta)^{-1}) \\ &= N(\beta)N(\sigma(\beta^{-1})) \\ &= N(\beta)N(\beta)^{-1} \\ &= 1 \end{aligned}$$

Para demostrar la afirmación recíproca, definimos las siguientes "normas

parciales":

$$\begin{aligned}
\delta_0 &= \alpha, \\
\delta_1 &= \alpha\sigma(\alpha), \\
\delta_2 &= \alpha\sigma(\alpha)\sigma^2(\alpha), \\
&\vdots \\
\delta_{n-1} &= \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = N(\alpha) = 1
\end{aligned}$$

Es fácil ver que

$$\alpha\sigma(\delta_i) = \delta_{i+1}$$

para cada $i = 1, \ldots, n-2$. Como los caracteres $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ son distintos, son independientes[1]. Hay entonces $\gamma \in E$ tal que

$$\delta_0\gamma + \delta_1\sigma(\gamma) + \cdots + \delta_i\sigma^i(\gamma) + \cdots + \delta_{n-2}\sigma^{n-2}(\gamma) + \sigma^{n-1}(\gamma) \neq 0;$$

llamemos β a esta suma. Usando que $\sigma^n = 1$ y lo que se observó de las normas parciales, se verifica que

$$\begin{aligned}
\sigma(\beta) &= \sigma(\delta_0\gamma + \delta_1\sigma(\gamma) + \cdots + \delta_i\sigma^i(\gamma) + \cdots + \delta_{n-2}\sigma^{n-2}(\gamma) + \sigma^{n-1}(\gamma)) \\
&= \alpha^{-1}[\delta_1\sigma(\gamma) + \cdots + \delta_i\sigma^i(\gamma) + \cdots + \delta_{n-1}\sigma^{n-1}(\gamma)] + \sigma^n(\gamma) \\
&= \alpha^{-1}(\beta - \delta_0\gamma) + \gamma \\
&= \alpha^{-1}(\beta - \delta_0\gamma) + \alpha^{-1}\delta_0\gamma \\
&= \alpha^{-1}\beta.
\end{aligned}$$

Así, $\alpha = \beta\sigma(\beta)^{-1}$, como se quería probar. □

Corolario 1.4. *Sea $E : F$ una extensión de Galois de grado primo p. Si F tiene una raíz p-ésima primitiva de la unidad, entonces $E = F(\beta)$, donde $\beta^p \in F$ (así que $E : F$ es una extensión pura).*

Demostración. Si ω es una raíz p-ésima primitiva de la unidad, entonces $N(\omega) = \omega^p = 1$, por estar $\omega \in F$. Llamemos $G = \mathrm{Gal}(E : F)$. Como $E : F$ es de Galois, se tiene que $|G| = [E : F] = p$, así que $G \cong \mathbb{Z}_p$, que es cíclico; sea σ un generador. El teorema 90 de Hilbert da $\beta \in E$ tal que $\omega = \beta\sigma(\beta)^{-1}$ y por tanto $\sigma(\beta) = \beta\omega^{-1}$. Se sigue que $\sigma(\beta^p) = (\beta\omega^{-1})^p = \beta^p$, así que $\beta^p \in E^G = F$ por generar σ a G y ser $E : F$ de Galois. Si ocurriera que $\beta \in F$, tendríamos que $\omega = \beta\sigma(\beta)^{-1} = \beta\beta^{-1} = 1$, así que $\beta \notin F$ y $F(\beta) \neq F$. Por lo tanto, tenemos que $F \subsetneq F(\beta) \subseteq E$, y como $[E : F] = p$, $E = F(\beta)$. □

[1] Véase [Rot1, Lema 76].

Teorema 1.5 (Gran Teorema de Galois)**.** *Sea F un campo de característica 0, y sea $E : F$ una extensión de Galois. Entonces $G = \mathrm{Gal}(E : F)$ es un grupo soluble si y sólo si E está incluido en una extensión radical de F.*

Por lo tanto, si F es un campo de característica 0, el grupo de Galois de $f(x) \in F[x]$ es soluble si y sólo si $f(x)$ es soluble por radicales.

Demostración. La segunda afirmación se sigue de la primera, en virtud de que los campos de característica 0 son perfectos. Probemos pues la primera afirmación.

En virtud de lo señalado al principio del capítulo, basta que demostremos la necesidad. Sabemos que, como G es finito y soluble, tiene una serie subnormal en la cual todos los factores son de orden primo. Por lo tanto, y como podemos suponer que G no es trivial, G tiene un subgrupo H normal de índice primo, digamos p. Como F tiene característica 0, el polinomio $x^p - 1 \in F[x]$ no tiene raíces repetidas, por lo que existe ω raíz p-ésima primitiva de la unidad.

Supongamos primero que $\omega \in F$. Procedemos por inducción sobre $[E : F]$. Consideremos el campo intermedio E^H. Por supuesto, la extensión $E : E^H$ es también de Galois. Además, como $\mathrm{Gal}(E : E^H) \leq \mathrm{Gal}(E : F) = G$ y G es soluble, tenemos que $\mathrm{Gal}(E : E^H)$ también lo es. Como $[E : E^H] < [E : F]$ (pues $H \neq G$), la hipótesis de inducción da una torre radical

$$E^H \subseteq R_1 \subseteq \cdots \subseteq R_m$$

con $E \subseteq R_m$. Ahora, como $H \trianglelefteq G$, $E^H : F$ es de Galois, y $[E^H : F] = [G : H] = p$. Estamos suponiendo que $\omega \in F$, así que el corolario 1.4 da $\beta \in E^H$ tal que $E^H = F(\beta)$ con $\beta^p \in F$; es decir, la extensión $E^H : F$ es pura. Así, podemos extender la torre radical hacia la izqierda añadendo $F \subseteq E^H$, exhibiendo a $R_m : F$ como extensión radical.

Supongamos ahora que $\omega \notin F$. Definimos $F^* = F(\omega)$ y $E^* = E(\omega)$. Se tiene que la extensión $E^* : F^*$ es de Galois. En efecto, si $E : F$ es un campo de descomposición de $f(x) \in F[x]$, entonces $E^* : F^*$ es un campo de descomposición de $f(x) \in F^*[x]$ (que por supuesto es separable). Llamemos $G^* = \mathrm{Gal}(E^* : F^*)$. Por el lema que se probó sobre irracionalidades accesorias, hay un monomorfismo $G^* \to G$, de manera que G^* es soluble, por ser isomorfo a un subgrupo de un grupo soluble. Como $\omega \in F^*$, el caso anterior da una torre radical

$$F^* \subseteq S_1 \subseteq \cdots \subseteq S_n$$

con $E \subseteq E^* \subseteq S_n$. Pero $F^* = F(\omega)$, así que la extensión $F^* : F$ es pura y por lo tanto podemos extender la torre radical hacia la izqierda añadendo $F \subseteq F^*$, exhibiendo a $S_n : F$ como extensión radical. □

Posteriormente, en la sección 3.3, daremos un ejemplo que hace ver que no es posible eliminar la hipótesis de que la característica sea 0 sin perder el resultado.

Corolario 1.6. *Si F es un campo de característica 0, entonces todo polinomio en $F[x]$ de grado $n \leq 4$ es soluble por radicales.*

Demostración. El grupo de Galois de tal polinomio es un subgrupo de S_4, que sabemos que es soluble (y todo subgrupo de un grupo soluble es soluble). □

1.2. El Teorema del Elemento Primitivo

La versión más conocida del teorema del elemento primitivo dice que toda extensión de campos finita y separable es simple, es decir, que si $E : F$ es una extensión de campos con $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, donde para cada $i \in \{1, \ldots, n\}$ α_i es algebraico sobre F y separable, entonces hay $\beta \in E$ tal que $E = F(\beta)$. Debilitaremos estas hipótesis. Con precisión, probaremos[2] que se puede permitir que una de las α_i no sea separable.

Teorema 1.7 (Teorema del Elemento Primitivo)**.** *Sea $F : K$ una extensión de campos finita tal que $F = K(u, v_1, v_2, \ldots, v_n)$ con $v_1, v_2, ..., v_n$ separables. Entonces $F : K$ es una extensión simple.*

Demostración. Tratemos primero el caso en el que K es un campo finito. Si esto ocurre, tenemos, como la extensión $F : K$ es finita, que F es también finito. Se conoce que entonces $(F\backslash\{0\}, \cdot)$ es un grupo cíclico; digamos que $F\backslash\{0\} = \langle w \rangle$. Entonces, como $F = \langle w \rangle \cup \{0\}$, tenemos que $F = K(w)$.

Supongamos pues que K es infinito. Demostraremos por inducción sobre n que $F : K$ es simple.

En caso de que $n = 1$, tenemos que $F = K(u, v_1)$. Sean $p(x), q(x) \in K[x]$ los polinomios mínimos sobre K de u y de v_1, respectivamente. Sea $\Sigma : F$ un campo de descomposición de $p(x)q(x)$ sobre F. Tenemos, por supuesto, que $K \subseteq F \subseteq \Sigma$. Sean $u = u_1, u_2, \ldots, u_r$ las diferentes raíces de $p(x)$ y $v_1, v_2, \ldots, v_s$ las diferentes raíces de $q(x)$. Notemos que $r \leq \partial(p)$, y que la hipótesis de que v_1 es separable y el hecho de que $q(x)$ es irreducible sobre K aseguran que $s = \partial(q)$. Ahora, para cada $i = 1, \ldots, r$, $j = 2, \ldots, s$, tenemos que $v_1 - v_j \neq 0$, así que hay $\lambda_{ij} \in \Sigma$ tal que

$$\lambda_{ij}(v_1 - v_j) = u_i - u.$$

[2]Seguiremos a [Z, Cap. 8, §7, Teorema 95].

Como K es infinito, hay $\lambda \in K$ tal que $\lambda \neq \lambda_{ij}$ para $i = 1, \ldots, r$, $j = 2, \ldots, s$. Sea

$$w = u + \lambda v_1.$$

Demostraremos que

$$K(u, v_1) = K(w).$$

Es claro que $K(w) \subseteq K(u, v_1)$, así que basta probar que $K(u, v_1) \subseteq K(w)$. Como

$$u = w - \lambda v_1,$$

sucede que

$$p(w - \lambda v_1) = 0.$$

Sea

$$g(x) = p(w - \lambda x) \in K(w)[x].$$

Tenemos que v_1 es una raíz común de $g(x)$ y de $q(x)$. Haremos ver que v_1 es la única raíz común de $g(x)$ y de $q(x)$. En efecto, si v_j fuese raíz de $g(x)$ para alguna $j \geq 2$, tendríamos que

$$w - \lambda v_j = u_i$$

para alguna $i \in \{1, \ldots, r\}$, y como $w = u + \lambda v_1$, ocurriría que

$$u + \lambda v_1 - \lambda v_j = u_i$$

y por tanto que

$$\lambda(v_1 - v_j) = u_i - u,$$

de donde $\lambda = \lambda_{ij}$, contradiciendo la elección de λ. Así, el único factor lineal mónico común de $g(x), q(x) \in K(w)[x]$ es el polinomio $x - v_1$. Sea $d(x) \in K(w)[x]$ el máximo común divisor de $g(x)$ y de $q(x)$. Tenemos que $x - v_1 | d(x)$. Además, ya observamos que $q(x)$ no tiene raíces repetidas, así que $d(x) = x - v_1$. Por lo tannto, $v_1 \in K(w)$, y como $u = w - \lambda v_1$, $u \in K(w)$. Hemos probado que $K(u, v_1) \subseteq K(w)$.

Para dar el paso inductivo, supongamos que hay $\theta \in K(u, v_1, v_2, \ldots, v_{n-1})$ tal que

$$K(u, v_1, v_2, \ldots, v_{n-1}) = K(\theta).$$

Entonces, como por hipótesis v_n es separable, lo discutido en el caso base asegura que

$$K(u, v_1, v_2, \ldots, v_{n-1}, v_n) = K(\theta, v_n) = K(w)$$

para alguna $w \in F$. □

Notemos que esta demostración es independiente del teorema fundamental de la teoría de Galois. En muchos textos[3], se prueba el teorema fundamental y después, usando también el teorema de Steinitz (que asegura que cualquier extensión de campos finita es simple si y sólo si tiene una cantidad finita de campos intermedios), el teorema del elemento primitivo.

En la sección 3.2 mostraremos con un ejemplo que se necesita la hipótesis de separabilidad.

1.3. Casus Irreducibilis

Sea $f(x) \in \mathbb{Q}[x]$ un polinomio cúbico. Recordemos que el discriminante D de $f(x)$ se define como $D = [(u-v)(u-w)(v-w)]^2$, donde $u, v, w \in \mathbb{C}$ son las raíces de $f(x)$. Se observa que si $E \subseteq \mathbb{C}$ es campo de descomposición de $f(x)$ sobre $\mathbb{Q}$ y G es el grupo de Galois de $f(x)$, entonces $D \in E^G = \mathbb{Q}$. Tampoco es difícil hacer ver[4] que

(i) $D = 0$ si y sólo si $f(x)$ tiene raíces repetidas,

(ii) $D > 0$ si y sólo si u, v, w son distintas y reales, y

(iii) $D < 0$ si y sólo si u, v, w son distintas y exactamente una de ellas es real.

Es conocido[5] que la fórmula general para hallar las raíces de $f(x) = x^3 + qx + r$, que aquí llamaremos *de Cardano*, involucra a $\sqrt{R}$, donde $R = \frac{r^2}{4} + \frac{q^3}{27}$. Así, cuando R es negativa, cada raíz de $f(x)$ involucra números complejos. Como el discriminante $D = -108R$ (véase [Rot1, Teo 100(ii)]), hay raíces reales dadas en términos de números complejos cada vez que $D > 0$. Este fenómeno inquietaba bastante a los matemáticos del siglo XVI, que trataron de reescribir la fórmula de Cardano a fin de obtener fórmulas específicas para cada problema en las que no aparecieran números imaginarios, que no se habían inventado. El siguiente teorema muestra que tales intentos de reescritura estaban condenados al fracaso. Seguiremos a [Rot1, Teorema 102].

Teorema 1.8 (Casus Irreducibilis)**.** *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio cúbico irreducible con raíces reales u, v, w. Sea $E = \mathbb{Q}(u, v, w)$ un campo de descomposición de $f(x)$, y sea*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

[3] Véase, por ejemplo, [Rot1, Corolario 88].
[4] Véase [Rot1, Teorema 104].
[5] Véase, por ejemplo, [Rot1, pp 44-47].

una torre radical con $E \subseteq K_t$. Entonces K_t no es un subcampo de $\mathbb{R}$.

Demostración. Supongamos que $K_t \subseteq \mathbb{R}$. Dado que las raíces u, v, w son reales, tenemos que $D \geq 0$ (de hecho, por ser $f(x)$ irreducible sobre el campo perfecto $\mathbb{Q}$, la desigualdad es estricta), así que $\sqrt{D}$ es real. Sin pérdida de generalidad podemos suponer que el primer elemento que se adjunta a $\mathbb{Q}$ es $\sqrt{D}$, de modo que

$$K_1 = K_0(\sqrt{D}).$$

No es difícil ver (descomponiendo en factores primos el tipo de cada extensión pura de las que conforman la torre radical) que podemos suponer que cada extensión $K_{i+1} : K_i$, para $i = 1, \ldots, t-1$, es pura de tipo primo. Como $f(x)$ es irreducible sobre K_0 y se descompone sobre K_t (pues $E \subseteq K_t$), hay una primera $j \geq 0$ tal que $f(x)$ es irreducible sobre K_j y no lo es sobre K_{j+1}. Digamos que $K_{j+1} = K_j(\alpha)$, donde α es raíz de $x^p - c \in K_j[x]$ para algún primo p, de forma que

$$[K_{j+1} : K_j] = [K_j(\alpha) : K_j] \leq p.$$

Ahora, es cierto que el polinomio cúbico $f(x) \in K_j[x]$ tiene una raíz en K_{j+1}, digamos u. Ocurre entonces que

$$K_j \subseteq K_j(u) \subseteq K_{j+1}.$$

Pero $f(x)$ es un polinomio cúbico irreducible sobre K_j, por lo que se tiene que

$$3 = [K_j(u) : K_j] | [K_{j+1} : K_j] \leq p,$$

así que p es un primo impar. Observemos aquí que $f(x)$ es irreducible sobre K_1, es decir que $j \geq 1$. En efecto, si $j = 0$, tendríamos que $p = 2$ (pues $K_1 = K_0(\sqrt{D})$. Verifiquemos que el poliomio $x^p - c \in K_j[x]$ es irreducible. En efecto, sabemos, por [Rot1, Corolario 72], que tal polinomio es irreducible sobre K_j o c tiene una raíz p-ésima en K_j. Supongamos que se da el segundo caso. Tenemos que α es una raíz p-ésima real de $c \in \mathbb{R}$ (¡recordemos que $K_t \subseteq \mathbb{R}$!), así que es la única (por ser p impar). Así, $\alpha \in K_j$ y por tanto $K_j = K_{j+1}$, contradiciendo que $3 | [K_{j+1} : K_j]$. Por lo tanto,

$$3 | [K_{j+1} : K_j] = [K_j(\alpha) : K_j] = p.$$

Entonces, $p = 3$.

Como el polinomio cúbico $f(x)$ es irreducible sobre K_j, $u \notin K_j$. Como además K_{j+1} contiene a u y a $\sqrt{D}$, ocurre que

$$K_j \subsetneq K_j(u, \sqrt{D}) \subseteq K_{j+1}.$$

Ahora, el corolario 101 de [Rot1] asegura que $K_j(u, \sqrt{D})$ es campo de descomposición de $f(x)$ sobre K_j. Pero $K_{j+1} : K_j$ no tiene campos intermedios (pues su grado es 3), así que $K_j(u, \sqrt{D}) = K_{j+1}$.

Por lo tanto, la extensión $K_{j+1} : K_j$ es normal. Ya argumentamos que el polinomio $x^3 - c \in K_j[x]$ es irreducible y tiene una raíz, a saber α, en K_{j+1}, así que tiene todas ahí. Explícitamente, $\zeta\alpha, \zeta^2\alpha \in K_{j+1}$, donde ζ es una raíz cúbica primitiva de la unidad. Por supuesto, $\alpha \neq 0$ (de otro modo $K_j = K_{j+1}$). Pero esto implica que $\zeta = \frac{\zeta\alpha}{\alpha} \in K_{j+1} \subseteq K_t \subseteq \mathbb{R}$, cosa que contradice el hecho de que $\zeta \in \mathbb{C}\backslash\mathbb{R}$. □

Corolario 1.9. *Existen polinomios con coeficientes racionales solubles por radicales tales que su campo de descomposición sobre $\mathbb{Q}$ no es una extensión radical.*

Demostración. Considérese cualquier polinomio cúbico cuyo discriminante sea positivo. Como sus tres raíces son reales, su campo de descomposición es subcampo de $\mathbb{R}$, así que si $E : \mathbb{Q}$ fuese una extensión radical, se contradiría el teorema anterior. □

En la sección 3.1 exhibiremos un ejemplo que ilustre lo afirmado en el corolario anterior sin apelar al teorema del *casus irreducibilis*.

Corolario 1.10. *Si $E : F$ es radical y K es un campo intermedio, $K : F$ no necesariamente es radical.*

Demostración. Directo del corolario anterior. □

Precisemos ahora en qué sentido habla el teorema del *casus irreducibilis* de una situación irreducible. Convengamos primero en decir que, para $F \subseteq \mathbb{R}$ un subcampo, $x \in \mathbb{R}$ es *expresable por radicales reales a partir de F* si y sólo si hay una expresión formal E en la cual sólo intervienen elementos de F, operaciones de campo y radicales reales (es decir, radicales en los cuales no ocurre que el índice sea par y el radicando negativo) tal que se verifica que $x = E$. Recordemos[6] la formula de Cardano. Sea $f(x) = x^3 + qx + r \in \mathbb{Q}[x]$. Si $R = \frac{r^2}{4} + \frac{q^3}{27}$, $A \in \mathbb{C}$ es tal que $A^3 = -\frac{r}{2} + \sqrt{R}$ (donde si $R < 0$, entendemos por $\sqrt{R}$ una de las dos raíces cuadradas imaginarias puras de R), y $B \in \mathbb{C}$ es tal que $AB = -\frac{q}{3}$, entonces las raíces de $f(x)$ son $A + B$, $\omega A + \omega^2 B$, $\omega^2 A + \omega B$, donde ω es una raíz cúbica primitiva de la unidad. Observemos que $B^3 = -\frac{q^3}{27A^3} = -\frac{r}{2} - \sqrt{R}$. Además, si $R \geq 0$ y A es la raíz cúbica real de $-\frac{r}{2} + \sqrt{R}$, la igualdad $AB = -\frac{q}{3}$ obliga a B a ser la raíz cúbica real de

[6] Véase, por ejemplo, [Rot1, pp 44-47].

$-\frac{r}{2}-\sqrt{R}$, mientras que si $R<0$, tenemos que $(\bar{A})^3=\overline{A^3}=\overline{-\frac{r}{2}+\sqrt{R}}=-\frac{r}{2}-\sqrt{R}=B^3$, así que $B\in\{\bar{A},\bar{A}\omega,\bar{A}\omega^2\}$. Si $B=\bar{A}\omega$, tendríamos que $-\frac{q}{3}=AB=A\bar{A}\omega=|A|^2\omega\in\mathbb{C}\backslash\mathbb{R}$, pero $q\in\mathbb{Q}$. Por lo tanto, $B\neq\bar{A}\omega$. Análogamente, $B\neq\bar{A}\omega^2$. Así, $B=\bar{A}$. Probemos ahora un lema.

Lema 1.11. *Sean $f(x)=x^3+qx+r\in\mathbb{Q}[x]$ irreducible y con todas sus raíces reales, $R=\frac{r^2}{4}+\frac{q^3}{27}$, $A\in\mathbb{C}$ tal que $A^3=-\frac{r}{2}+\sqrt{R}$, y $B\in\mathbb{C}$ tal que $AB=-\frac{q}{3}$. Digamos que $A=a+bi$, con $a,b\in\mathbb{R}$. Entonces a no es expresable por radicales reales a partir de $\mathbb{Q}$.*

Demostración. Supongamos que sí lo es. Como $\mathbb{Q}$ es perfecto, $f(x)$ no tiene raíces repetidas, así que $D>0$. Tenemos entonces que $R<0$ y por tanto, en vista de lo ya discutido, que $B=\bar{A}$ y entonces $u=A+B=A+\bar{A}=2a$ es una raíz de $f(x)$. Nuestra definición de expresabilidad por radicales reales nos dice que hay

$$\mathbb{Q}=K_0\subseteq K_1\subseteq\cdots\subseteq K_t$$

torre radical con $K_t\subset\mathbb{R}$ tal que $u\in K_t$. Ahora, $g(x)=\frac{f(x)}{x-u}\in K_t[x]$ es un polinomio cuadrático. Sus dos raíces, v,w, son reales (pues son raíces de $f(x)$). Pero v,w se pueden obtener con la fórmula general para resolver ecuaciones cuadráticas, lo que hace ver que son expresables por radicales reales a partir de K_t (escribiendo sólo un radical, por cierto). Es decir, hay

$$\mathbb{Q}=K_0\subseteq K_1\subseteq\cdots\subseteq K_{t+1}$$

torre radical con $K_{t+1}\subset\mathbb{R}$ tal que $u,v,w\in K_{t+1}$, cosa que contradice el teorema del *casus irreducibilis*. □

Si $w=a+bi\in\mathbb{C}$, es conocido que las raíces cuadradas de w son $z=x+yi$, donde $x=\pm\sqrt{\frac{a}{2}+\frac{1}{2}\sqrt{a^2+b^2}}$, $y=\pm\sqrt{-\frac{a}{2}+\frac{1}{2}\sqrt{a^2+b^2}}$, con $\operatorname{sgn}(xy)=\operatorname{sgn}(b)$. Es decir, hay una fórmula general para obtener las raíces cuadradas de un número complejo arbitrario, donde las partes real e imaginaria de cada solución están expresadas por radicales reales (pues $|\frac{a}{2}|\leq\frac{1}{2}\sqrt{a^2+b^2}$) a partir del campo que se obtiene adjuntando a $\mathbb{Q}$ las partes real e imaginaria del número complejo dado. Probaremos ahora que éste no es el caso con las raíces cúbicas.

Proposición 1.12. *No existe una fórmula general que proporcione una raíz cúbica de un número complejo arbitrario, donde las partes real e imaginaria de la solución estén expresadas por radicales reales a partir del campo que se obtiene adjuntando a $\mathbb{Q}$ las partes real e imaginaria del número complejo dado.*

Demostración. Supongamos que sí la hay. Tomemos cualquier polinomio $f(x) = x^3 + qx + r \in \mathbb{Q}[x]$ irreducible y con todas sus raíces reales. Sea R como en el enunciado del lema anterior. Tenemos que $R < 0$. Consideremos el número complejo

$$\zeta = -\frac{r}{2} + i\sqrt{-R},$$

cuyas partes real e imaginaria son expresables por radicales reales (pues $-R > 0$) a partir de $\mathbb{Q}$. Aplicando la fórmula que estamos suponiendo que existe, obtenemos una raíz cúbica de ζ cuyas partes real e imaginaria son expresables por radicales reales a partir de $\mathbb{Q}$, en particular su parte real, cosa que el lema anterior asegura que no puede suceder. □

Capítulo 2

Problemas

2.1. Funciones Simétricas

Sean K un campo, $E = K(x_1, x_2, \ldots, x_n)$. Para $\sigma \in S_n$ llamemos $\hat{\sigma}$ al automorfismo de E que resulta al aplicar σ a los subíndices de las indeterminadas que aparecen en un elemento de E. Hagamos $G = \{\hat{\sigma} | \sigma \in S_n\}$. Sea $F = E^G$ (los elementos de F se conocen como *funciones simétricas*). Es fácil ver que $E : F$ es un campo de descomposición del polinomio

$$f(t) = \prod (t - x_i) \in F[t],$$

que es separable por no tener raíces repetidas. Además, como las distintas raíces de $f(t)$ son $\{x_1, x_2 \ldots, x_n\}$, $\mathrm{Gal}(E : F) \leq G$, y por supuesto $G \leq \mathrm{Gal}(E : E^G) = \mathrm{Gal}(E : F)$, por lo que $\mathrm{Gal}(E : F) = G \cong S_n$, de donde $[E : F] = n!$.

Para $i = 1, \ldots, n$, denotemos como a_i a la suma de todos los posibles productos de i diferentes indeterminadas, tomadas del conjunto $\{x_1, x_2, \ldots, x_n\}$ (así, $a_1 = x_1 + x_2 + \cdots + x_n$, $a_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$,...,$a_n = x_1x_2 \cdots x_n$). Tenemos entonces que

$$f(t) = (t - x_1)(t - x_2) \cdots (t - x_n) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \cdots + (-1)^n a_n.$$

Tradicionalmente, a a_i se le llama la i-ésima *función simétrica elemental* en n indeterminadas, para cada $i = 1, \ldots, n$.

Probaremos, siguiendo a [Ar1, Cap. II, Sec. G], la siguiente

Proposición 2.1. *Sea K un campo. Toda función simétrica en n indeterminadas con coeficientes en K se puede escribir como una función racional con coeficientes en K evaluada en las funciones simétricas elementales.*

Demostración. Sean $E, F, f(t), a_1, a_2, \ldots, a_n$ como arriba. Definimos $S = K(a_1, a_2, \ldots, a_n)$. Ya observamos que $f(t) \in S[t]$, y en general es claro que $S \subseteq F \subseteq E$.

Para lograr nuestro objetivo (es decir, obtener que $S = F$), basta hacer ver que $[E : S] \leq n!$. Consideremos pues la siguiente torre de campos:

$$S = S_n \subseteq S_{n-1} \subseteq S_{n-2} \subseteq \cdots \subseteq S_2 \subseteq S_1 \subseteq S_0 = E$$

donde para $i = 1, 2, \ldots, n$, $S_{i-1} = S(x_i, x_{i+1}, \ldots, x_n) = S_i(x_i)$. Basta probar que, para cada $i = 1, \ldots, n$, $[S_{i-1} : S_i] \leq i$, y para ello basta ver que el generador x_i de S_{i-1} sobre S_i es raíz de un polinomio de grado i con coeficientes en S_i. Construyamos tales polinomios. Sean $F_n(t) = f(t)$ y

$$F_i(t)\frac{f(t)}{(t - x_{i+1})(t - x_{i+2}) \cdots (t - x_n)} = \frac{F_{i+i}(t)}{t - x_{i+1}}$$

para $i = 1, \ldots, n-1$. Se tiene que, para $i = 1, \ldots, n$, $F_i(t)$ es un polinomio mónico en t de grado i y cuyos coeficientes son polinomios con coeficientes enteros evaluados en $a_1, a_2, \ldots, a_n$ y en $x_{i+1}, x_{i+2}, \ldots, x_n$. En efecto, si para $i = 1, \ldots, n-1$, llamamos b_i a la i-ésima función simétrica elemental en $n-1$ indeterminadas, tenemos que

$$\begin{aligned} F_{n-1}(t) &= (t - x_1)(t - x_2) \cdots (t - x_{n-1}) \\ &= t^{n-1} - b_1 t^{n-2} + b_2 t^{n-3} - \cdots + (-1)^{n-1} b_{n-1}, \end{aligned}$$

de donde se observa que $b_1 = a_1 - x_n$ y que, para $i = 2, \ldots, n-1$, $b_i = a_i - x_n b_{i-i}$. Si ahora llamamos, para $i = 1, \ldots, n-2$, c_i a la i-ésima función simétrica elemental en $n-2$ indeterminadas, tenemos que

$$\begin{aligned} F_{n-2}(t) &= (t - x_1)(t - x_2) \cdots (t - x_{n-2}) \\ &= t^{n-2} - c_1 t^{n-3} + c_2 t^{n-4} - \cdots + (-1)^{n-2} c_{n-2}, \end{aligned}$$

de donde se observa que $c_1 = b_1 - x_{n-1}$ y que, para $i = 2, \ldots, n-2$, $c_i = b_i - x_{n-1} c_{i-i}$. Así proseguimos hasta llegar a

$$F_1(t) = t - x_1 = t - [a_1 - (x_2 + \cdots + x_n)].$$

Por lo tanto, $F_i(t) \in S_i(t)$. Además, es claro que x_i es raíz de $F_i(t)$. □

Ahora, usando un poco de teoría de Galois, es fácil deducir que $S = F$. En efecto, consideremos a $f(t) \in S[t]$. Observemos que $E : S$ es un campo de descomposición de $f(t)$, así que es una extensión de Galois. Ahora, $G \leq$

$\mathrm{Gal}(E : F) \leq \mathrm{Gal}(E : S)$ y, como arriba, $\mathrm{Gal}(E : S) \leq G$, por lo que $\mathrm{Gal}(E : S) = G$. Entonces, $S = E^G = F$.

Es cierto que sobre un campo K, cualquier polinomio simétrico en las indeterminadas $x_1, x_2, \ldots, x_n$ puede ser escrito como un *polinomio* con coeficientes en K evaluado en las funciones simétricas elementales $a_1, a_2, \ldots, a_n$. Véanse, a tal efecto, las referencias citadas en [St, Teorema 18.8] o la demostración dada en [Rom, Teorema 6.2.2].

2.2. Un Problema Inverso

Se sabe[1] que dado un polinomio $p(x) \in \mathbb{Q}[x]$, se puede calcular su grupo de Galois. Tiene sentido plantear el problema inverso, es decir, si dado un grupo finito G, habrá un polinomio $p(x)$ tal que su grupo de Galois sea (isomorfo a) G.

Si el campo de base F no se especifica, la respuesta es afirmativa. En efecto, dado un grupo G, digamos de orden n, consideramos un polinomio $p(x)$ separable de grado n, digamos con coeficientes en F, tal que su grupo de Galois sea S_n (véase la sección 2.1). Sea $E : F$ un campo de descomposición de $p(x)$. El teorema de Cayley asegura la existencia de $H \leq S_n$ tal que $G \cong H$. Consideremos E^H. El teorema fundamental de la teoría de Galois garantiza que $\mathrm{Gal}(E : E^H) = H$. Así, basta ver a $p(x)$ como un polinomio con coeficientes en E^H para obtener que el grupo de Galois de $p(x)$ sobre E^H es H, y por tanto isomorfo a G.

Hemos probado la siguiente

Proposición 2.2. *Todo grupo finito G es el grupo de Galois de algún polinomio.*

Sin embargo, si se requiere que el campo de base sea $\mathbb{Q}$, el problema se vuelve mucho más difícil, tanto que aún no se conoce una solución general. En 1954 el matemático ruso Šafarevich probó[2] que tal polinomio $p(x)$ existe si G es soluble. En este caso, el problema se transforma en uno equivalente, pero de teoría de números.

Se puede consultar algunos resultados parciales en este sentido (por ejemplo, el caso $G = S_p$ con p primo, o el hecho de que si G es abeliano y

[1] Véase el algoritmo dado en [St, Sec. 22.4] o los procedimientos descritos en [G, Sec. 4.9].

[2] Véase [Sa].

finito entonces hay una extensión $E : \mathbb{Q}$ tal que $\mathrm{Gal}(E : \mathbb{Q}) \cong G$) en [Rom, Sec. 10.5].

Supongamos que nos enfrentamos al siguiente problema: Dado $H \leq S_4$, hallar $f(x) \in \mathbb{Q}[x]$ tal que el grupo de Galois de $f(x)$ sea (isomorfo a) H. En lo que resta de esta sección, para $f(x) \in \mathbb{Q}[x]$, denotaremos como $\mathrm{Gal}(f)$ al grupo de Galois de $f(x)$ sobre $\mathbb{Q}$.

Determinemos en primer lugar todos los subgrupos H de S_4, módulo isomorfismo. La teoría de grupos necesaria para seguir esta discusión es elemental y puede consultarse en cualquier texto básico de álgebra abstracta o en [Rot1, Ap. B]. Como $|S_4| = 24$, los posibles órdenes para H son 24, 12, 8, 6, 4, 3, 2 y 1. Los casos $|H| = 24$ y $|H| = 1$ son triviales. Si $|H| = 12$, se tiene que $[G : H] = 2$ y por tanto que $H \trianglelefteq G$. Como los únicos subgrupos normales de S_4 son A_4 y V (el 4-grupo de Klein), $H = A_4$. Si $|H| = 8$, H es un 2-subgrupo de Sylow de S_4. Los teoremas de Sylow aseguran que dos cualesquiera de estos H's son conjugados, así que H es único módulo isomorfismo. Como $D_{2(4)}$, el grupo diédrico de orden 8, es subgrupo de S_4, tenemos que $H \cong D_{2(4)}$. Por cierto, los teoremas de Sylow también garantizan que la cantidad de subgrupos de S_4 de orden 8 es un número congruente con 1 módulo 2 (es decir impar) que divide a 24. Por lo tanto, hay 1 ó 3. Si hubiera uno, sería normal en S_4, pero $|A_4| \neq 8 \neq |V|$, así que hay 3. Si $|H| = 6$, $H \cong \mathbb{Z}_6$ ó $H \cong S_3$, pero en S_4 no hay elementos de orden 6, así que $H \cong S_3$. Por cierto, es fácil ver que H tiene que ser una de las 4 copias de S_3 que son subgrupos de S_4 (los grupos de permutaciones que dejan fijo al 1, al 2, al 3 ó al 4, respectivamente). Si $|H| = 4$, $H \cong V$ ó $H \cong \mathbb{Z}_4$. Si $|H| = 3$, $H \cong \mathbb{Z}_3 \cong A_3$. Si $|H| = 2$, $H \cong \mathbb{Z}_2$. Tenemos entonces que H es isomorfo a S_4, A_4, $D_{2(4)}$, S_3, V, $\mathbb{Z}_4$, A_3, $\mathbb{Z}_2$ ó 1.

Sea $f(x) \in \mathbb{Q}[x]$ cuártico, y sea $X = \{1, 2, 3, 4\}$. Es un hecho básico[3] que si $f(x)$ es irreducible sobre $\mathbb{Q}$ entonces $\mathrm{Gal}(f)$ es transitivo (es decir que actúa transitivamente sobre el conjunto de raíces de $f(x)$, o equivalentemente que, visto como subgrupo de S_4, actúa sobre X de manera transitiva). Dado un subgrupo transitivo de S_4, digamos H, se tiene una única H-órbita, a saber, todo X. Entonces $|X| = 4$ es un índice en H (el índice en H de un cierto estabilizador), de donde 4 divide a $|H|$, por lo que H es isomorfo a S_4, A_4, $D_{2(4)}$, V ó $\mathbb{Z}_4$ (y es fácil verificar que cada uno de éstos es transitivo).

Empleando razonamientos análogos se observa también que, si $f(x) \in$

[3] Véase, por ejemplo, [Rot2, Proposición 4.13].

$\mathbb{Q}[x]$ es cúbico e irreducible, entonces 3 divide a $|\mathrm{Gal}(f)|$, por lo que $\mathrm{Gal}(f)$ es isomorfo a S_3 ó a A_3.

Enunciemos algunos resultados que nos serán útiles.

Recordemos[4] primero que el discriminante de $x^3 + qx + r \in \mathbb{Q}[x]$ es $-4q^3 - 27r^2$.

Los siguientes criterios para $f(x) \in \mathbb{Q}[x]$ cúbico irreducible con discriminante D y $G = \mathrm{Gal}(f)$ están probados en [Rot1, Teorema 104].

(i) Si D no es un cuadrado en $\mathbb{Q}$, entonces $G \cong S_3$.

(ii) Si D es un cuadrado en $\mathbb{Q}$, entonces $G \cong A_3$.

Para $f(x) \in \mathbb{Q}[x]$ cuártico con raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, definimos

$$\begin{aligned} u &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ v &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ w &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3), \end{aligned}$$

y llamamos *ecuación cúbica resolvente* de $f(x)$ a $(x-u)(x-v)(x-w)$. Con estas convenciones, la ecuación cúbica resolvente de $x^4+qx^2+rx+s \in \mathbb{Q}[x]$ es $x^3 - 2qx^2 + (q^2 - 4s)x + r^2$ (según [Rot1, Teorema 105]).

Los siguientes criterios para $f(x) \in \mathbb{Q}[x]$ cuártico irreducible con ecuación cúbica resolvente $g(x)$, $m = |\mathrm{Gal}(g)|$ y $G = \mathrm{Gal}(f)$ están probados en [Rot1, Teorema 106].

(i) Si $m = 6$, entonces $G \cong S_4$.

(ii) Si $m = 3$, entonces $G \cong A_4$.

(iii) Si $m = 1$, entonces $G \cong V$.

El caso especial del polinomio cuártico $x^4 + bx^2 + c$ está explorado en [Rom], en donde el teorema 6.4.3 asegura que, si tal polinomio es irreducible sobre $\mathbb{Q}$ y si se tiene que ni c ni $c(b^2 - 4c)$ son cuadrados en $\mathbb{Q}$, entonces $\mathrm{Gal}(f) \cong D_{2(4)}$.

Demos ahora los polinomios en $\mathbb{Q}[x]$ pedidos.

Si $f(x) = x$, $\mathrm{Gal}(f) \cong 1$, trivialmente.

Si $f(x) = x^2 + 1$, $\mathrm{Gal}(f) = \{1, \sigma\} \cong \mathbb{Z}_2$, donde σ es la conjugación compleja (restringida apropiadamente).

Sea $f(x) = x^3 - 3x + 1$. Como el polinomio cúbico $f(x)$ no tiene raíces racionales, es irreducible sobre $\mathbb{Q}$. Su discriminante es $-4(-3)^3 - 27(1)^2 = 81 = 9^2$, así que $\sqrt{D} \in \mathbb{Q}$ y por tanto $\mathrm{Gal}(f) \cong A_3$.

[4] Véase [Rot1, Teorema 100(ii)].

Si $f(x) = x^3 - 2$, que es irreducible sobre $\mathbb{Q}$ (por no tener raíces racionales o por el criterio de Eisenstein) y cuyo discrminante es -108, tenemos que $\mathrm{Gal}(f) \cong S_3$.

Si $f(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$, el quinto polinomio ciclotómico, es un hecho muy conocido[5] que $\mathrm{Gal}(f) = (\mathbb{Q}(\zeta) : \mathbb{Q}) \cong \mathbb{Z}_5^{\#} \cong \mathbb{Z}_4$, donde ζ es una raíz quinta primitiva de la unidad.

Sea $f(x) = x^4 - 10x^2 + 1$. Se tiene que $f(x)$ es irreducible sobre $\mathbb{Q}$. En efecto, no tiene raíces racionales, y no es difícil ver que no hay $a, b, c \in \mathbb{Q}$ tales que $x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + c)$. La ecuación cúbica resolvente es

$$x^3 + 20x + 96x = x(x + 8)(x + 12),$$

que se descompone sobre $\mathbb{Q}$, por lo que $m = 1$. Así, $\mathrm{Gal}(f) \cong V$.

Sea $f(x) = x^4 + 2x^2 + 2$. Por el criterio de Eisenstein, $f(x)$ es irreducible sobre $\mathbb{Q}$. Como ni 2 ni -8 son cuadrados en $\mathbb{Q}$, tenemos inmediatamente que $\mathrm{Gal}(f) \cong D_{2(4)}$.

Sea $f(x) = x^4 + 8x + 12$. Verifiquemos que $f(x)$ es irreducible sobre $\mathbb{Q}$. Es fácil ver que $f(x)$ no tiene raíces racionales. Si $x^4 + qx^3 + rx + s \in \mathbb{Q}[x]$ tuviera un factor cuadrático $x^2 + kx + l \in \mathbb{Q}[x]$, el método de Descartes para resolver ecuaciones cuárticas asegura[6] que k^2 sería raíz de $x^3 + 2qx^2 + (q^2 - 4s)x - r^2$. Por supuesto, si $k \in \mathbb{Q}$, entonces $k^2 \in \mathbb{Q}$. Haciendo $q = 0$, $r = 8$, y $s = 12$, se sigue que, si $f(x)$ no fuese irreducible sobre $\mathbb{Q}$,

$$h(x) = x^3 - 48x - 64$$

tampoco lo sería (pues tendría una raíz en $\mathbb{Q}$). Pero $h(x)$ es irreducible sobre $\mathbb{Q}$, pues reduciéndolo módulo 5 obtenemos $x^3 + 2x + 1$, y este polinomio es irreducible sobre $\mathbb{Z}_5$, ya que no tiene raíces. Ahora, la ecuación cúbica resolvente de $f(x)$ es

$$g(x) = x^3 - 48x + 64.$$

Otra vez, para ver que $g(x)$ es irreducible sobre $\mathbb{Q}$, reduzcámoslo módulo 5. Resulta $x^3 + 2x - 1$, y este polinomio es irreducible sobre $\mathbb{Z}_5$, pues no tiene raíces. El discriminante de $g(x)$ es $331776 = 576^2$, así que $\mathrm{Gal}(g) \cong A_3$ y por tanto $m = 3$. Entonces, $\mathrm{Gal}(f) \cong A_4$.

Sea $f(x) = x^4 - 4x + 2$, que por el criterio de Eisenstein es irreducible sobre $\mathbb{Q}$. La ecuación cúbica resolvente es

$$g(x) = x^3 - 8x + 16.$$

[5] Véase, por ejemplo, [Rot1, Ejemplo 27].

[6] Véase [Rot1, pp 48-49].

Para ver que $g(x)$ es irreducible sobre $\mathbb{Q}$, reduzcámoslo módulo 5. Obtenemos x^3+2x+1, y en el párrafo anterior hicimos ver que este polinomio es irreducible sobre $\mathbb{Z}_5$. El discriminante de $g(x)$ es -4864, así que $\mathrm{Gal}(g) \cong S_3$ y por tanto $m = 6$. Entonces, $\mathrm{Gal}(f) \cong S_4$.

Se recomienda la lectura de Conrad, K., *Galois Groups of Cubics and Quartics*, así como de Spearman, B. & Williams, K., *Quartic Trinomials with Galois Groups A_4 and V_4* (donde V_4 es V).

Capítulo 3

Ejemplos

3.1. Solubilidad por Radicales

Recordemos que si F es un campo, decimos que $f(x) \in F[x]$ es soluble por radicales si y sólo si hay una extensión radical $E : F$ tal que $f(x)$ se descompone sobre E. No es evidente, por supuesto, que esto implique que el campo de descomposición de f sobre F sea una extensión radical de F. Daremos[1] un ejemplo que hace ver que efectivamente no lo implica. En otras palabras, exhibiremos un polinomio soluble por radicales cuyo campo de descomposición no es una extensión radical.

Sean $F = \mathbb{Q}$ y $f(x) = x^3 - 3x + 1$, y sea $K : \mathbb{Q}$ un campo de descomposición de $f(x)$ sobre $\mathbb{Q}$. Como todo polinomio cúbico con coeficientes en $\mathbb{Q}$, $f(x)$ es soluble por radicales. Probaremos que K no es una extensión radical de $\mathbb{Q}$. Determinemos el grado de $K : \mathbb{Q}$. En la sección 2.2 se demostró que, si G es el grpo de Galois de $f(x)$ sobre $\mathbb{Q}$, $G \cong A_3$. Como $\mathbb{Q}$ es perfecto, $[K : \mathbb{Q}] = |G| = 3$. Ahora, supongamos que K es una extensión radical de $\mathbb{Q}$. Entonces hay una torre de campos

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$$

en donde $F_i : F_{i-1}$ es una extensión pura para cada $i \in \{1, \ldots, r\}$. Como $[K : \mathbb{Q}]$ es primo, hay una y sólo una inclusión propia en la cadena. Asi, $K = \mathbb{Q}(b)$ con $b \in K \backslash \mathbb{Q}$ y $b^n = u \in \mathbb{Q}$ para algún entero positivo n. El polinomio mínimo $p(x)$ de b sobre $\mathbb{Q}$ se descompone sobre K, por ser $K : \mathbb{Q}$ normal. Sea $b' \in K$ otra raíz de $p(x)$. Entonces $b^n = u = (b')^n$, así que $\mu = b'/b$ es

[1] Seguiremos a [M, Ejemplo 16.13].

una raíz n-ésima de la unidad. En el grupo de raíces n-ésimas de la unidad, digamos que μ tiene orden m. Entonces μ es una raíz m-ésima primitiva de la unidad. Sabemos[2] que entonces $[\mathbb{Q}(\mu) : \mathbb{Q}] = \varphi(m)$. Como $\mathbb{Q}(\mu) \subseteq K$, tenemos que $\varphi(m)$ es 1 ó 3. Pero se tiene que, para todo entero positivo m, $\varphi(m) \neq 3$. En efecto, $\varphi(1) = 1$ y, para $\beta \geq 1$, $\varphi(2^\beta) = 2^{\beta-1}(2-1) = 2^{\beta-1} \neq 3$, así que podemos suponer que m no es una potencia de 2. Digamos que $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ con $p_1, p_2, \ldots, p_s$ primos distintos y $s, \alpha_1, \alpha_2, \ldots, \alpha_s$ enteros positivos. Entonces $\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s})$. Sea p un primo impar que divida a m. Así, si $\varphi(m) = 3$, $\varphi(p^\alpha)$ dividiría a 3, para algún entero positivo α. Ahora, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Pero, por supuesto, $p-1$, siendo par, no divide a 3. Así, $[\mathbb{Q}(\mu) : \mathbb{Q}] = \phi(m) = 1$, y entonces $\mu \in \mathbb{Q}$. Ahora, las únicas raíces de la unidad racionales son ± 1, por lo que $\mu = \pm 1$. Tenemos entonces que $b' = \pm b$. Podemos ahora asegurar que $p(x)$ tiene a lo más 2 raíces distintas. Como $\mathbb{Q}$ es perfecto y $p(x)$ es irreducible sobre $\mathbb{Q}$, tenemos que $\partial(p) \leq 2$, así que $[\mathbb{Q}(b) : \mathbb{Q}] \leq 2 < 3 = [K : \mathbb{Q}]$, cosa que contradice la igualdad $K = \mathbb{Q}(b)$. Por lo tanto, K no es una extensión radical de $\mathbb{Q}$.

3.2. Una Extensión de Campos Finita pero no Simple

Como los campos finitos y los de característica cero son perfectos, y por tanto toda extensión finita de uno de ellos es separable, en virtud del teorema del elemento primitivo el ejemplo tendrá que ser sobre un campo infinito de característica positiva.[3]

Sea $E = \mathbb{Z}_2(x, y)$, el campo de funciones racionales en dos indeterminadas con coeficientes en $\mathbb{Z}_2$. Un elemento típico de E sería, digamos,

$$\frac{x^2 + xy + x^5}{y^5 + y^3 x^2}$$

(en el cual todos los coeficientes son 1). Como campo base tomemos a $F = \mathbb{Z}_2(x^2, y^2)$, el subcampo de E formado por aquellos elementos de E en los cuales todas las potencias de las indetermnadas son pares. Como $E = \mathbb{Z}_2(x, y) = \mathbb{Z}_2(x^2, y^2, x, y) = F(x, y)$, y tanto x como y son algebraicos sobre F, es claro que $E : F$ es finita.

[2] Véase [M, Corolario 7.8].

[3] Seguiremos a [Ar2, Cap. VII, pág. 144].

Calculemos primero $[E : F]$. Consideremos cualquier $\theta \in E$. Escribamos

$$\theta = \frac{\phi(x,y)}{\psi(x,y)}$$

con $\psi(x,y) \neq 0$. Dado que la característica es 2, el cuadrado de un polinomio es simplemente la suma de los cuadrados de sus términos, así que

$$\theta = \frac{\phi(x,y)}{\psi(x,y)} = \frac{\phi(x,y)\psi(x,y)}{\psi^2(x,y)} = \frac{\phi(x,y)\psi(x,y)}{\psi_1(x^2,y^2)}$$

con $\psi_1(x^2,y^2) \in F$. Escribamos al polinomio del numerador como

$$\phi(x,y)\psi(x,y) = g_1(x^2,y^2) + g_2(x^2,y^2)x + g_3(x^2,y^2)y + g_4(x^2,y^2)xy$$

para ciertos polinomios $g_i(x^2,y^2) \in F$ para $i = 1,2,3,4$. Es decir, cualquier $\theta \in E$ se puede poner en la forma

$$\theta = a_1 + a_2x + a_3y + a_4xy$$

con $a_i \in F$ para $i = 1,2,3,4$. Entonces, $\mathscr{B} = \{1, x, y, xy\}$ genera al F-espacio vectoral E. Verifiquemos que $\mathscr{B}$ es linealmente independiente. Si en $\theta = a_1 + a_2x + a_3y + a_4xy$ tenemos que $\theta = 0$, podemos limpiar denominadores para obtener la igualdad entre polinomios

$$f_1(x^2,y^2) + f_2(x^2,y^2)x + f_3(x^2,y^2)y + f_4(x^2,y^2)xy = 0$$

y de ahí, comparando coeficientes, se sigue que $a_i = 0$ para cada $i = 1,2,3,4$. Por lo tanto, $\mathscr{B}$ es una base y $[E : F] = 4$.

Probemos ahora que $E : F$ no es simple. Supongamos que lo es, digamos $E = F(\alpha)$. Pero $\alpha^2 \in F$, así que $4 = [E : F] = [F(\alpha) : F] \leq 2$, cosa que es una contradicción.

Nótese que es fácil adaptar este razonamiento para obtener que, para p primo, la extensión $\mathbb{Z}_p(x,y) : \mathbb{Z}_p(x^p,y^p)$ es finita pero no simple.

Sigamos estudiando el caso $p = 2$. El teorema de Steinitz asegura que hay una cantidad infinita de campos intermedios entre E y F. Sea cualquier $\alpha \in E$. Como $\alpha^2 \in F$, tenemos, como arriba, que $[F(\alpha) : F] \leq 2$. Ahora, ya sabemos que podemos escribir

$$\alpha = a_1 + a_2x + a_3y + a_4xy$$

con $a_i \in F$ para $i = 1,2,3,4$. Por supuesto, alguno de a_2, a_3, a_4 es distinto de cero si y sólo si $\alpha \notin F$, y esto equivale a que $[F(\alpha) : F] = 2$. Supongamos

que ése es el caso. Tenemos que cualquier elemento $\xi \in F(\alpha)$ tiene la forma $A + B\alpha$, con $A, B \in F$. Entonces,

$$\xi = A + B\alpha = C + Ba_2x + Ba_3y + Ba_4xy$$

para $C \in F$, donde para esta α específica, a_2, a_3, a_4 están fijos. Observemos que la proporción $Ba_2 : Ba_3 : Ba_4$ es constante para todo el campo $F(\alpha)$. Así, para obtener una cantidad infinita de campos basta tomar una cantidad infinita de proporciones $a_2 : a_3 : a_4$. Por ejemplo, consideremos el conjunto de valores $\alpha = x + y^{2n+1}$, donde $n \in \mathbb{N}$. Tenemos un campo diferente para cada valor de n con $a_2 = 1, a_3 = 2n, a_4 = 0$.

3.3. Un Polinomio no Soluble por Radicales con Grupo de Galois Soluble

De entrada, el gran teorema de Galois nos orienta a buscar el ejemplo en un campo de característica positiva.

Probemos primero un lema, tomado de [Rot2, Lema 4.55].

Lema 3.1. *Si p es primo y $k = \mathbb{Z}(t)$, el campo de funciones racionales sobre el campo $\mathbb{Z}_p$, entonces $f(x) = x^p - x - t$ no tiene raíces en k.*

Demostración. Si hubiera una raíz α de $f(x)$ en k, habrían $g(t), h(t) \in \mathbb{Z}_p[t]$ con $\alpha = \frac{g(t)}{h(t)}$; podemos suponer que $(g, h) = 1$. Como α es raíz de $f(x)$, tenemos que $\left(\frac{g(t)}{h(t)}\right)^p - \left(\frac{g(t)}{h(t)}\right) = t$; limpiando denominadores obtenemos la ecuación en $\mathbb{Z}_p[t]$

$$g^p - h^{p-1}g = th^p.$$

Así, $g|th^p$. Como $(g, h) = 1$, tenemos que $g|t$, por lo que $g(t) = at$ ó $g(t)$ es constante, digamos $g(t) = b$, donde $a, b \in \mathbb{Z}_p$. De la ecuación desplegada se sigue también que $h|g^p$, pero el hecho de que $(g, h) = 1$ obliga a h a ser constante. Tenemos ahora, sin pérdida de generalidad, que $\alpha = at$ o que $\alpha = b$. En el primer caso, es decir, si $\alpha = at$, como el (pequeño) teorema de Fermat da que $a^p = a$ en $\mathbb{Z}_p$, ocurre que

$$\begin{aligned} 0 &= \alpha^p - \alpha - t \\ &= (at)^p - (at) - t \\ &= a^p t^p - at - t \\ &= at^p - at - t \\ &= t(at^{p-1} - a - 1). \end{aligned}$$

Se sigue que $at^{p-1} - a - 1 = 0$. De aquí, $a \neq 0$, pero entonces se contradice la trascendencia de t sobre $\mathbb{Z}_p$. En el segundo caso, es decir, si $\alpha = b \in \mathbb{Z}_p$, tenemos, por el teorema de Fermat, que $0 = f(\alpha) = f(b) = b^p - b - t = -t \neq 0$. Con esto se tiene que $\alpha \notin k$. □

Sean p un primo, $k = \mathbb{Z}_p(t)$, $f(x) = x^p - x - t \in k[t]$. Probaremos que el grupo de Galois de $f(x)$ sobre k es isomorfo a $\mathbb{Z}_p$ (que por supuesto es soluble), pero que $f(x)$ no es soluble por radicales. Seguiremos a [Rot2, Proposición 4.56].

Hagamos ver primero que el grupo de Galois de $f(x)$ sobre k es de orden p. Sea α una raíz de $f(x)$ y sea $E = k(\alpha)$. Por el teorema de Fermat, en $\mathbb{Z}_p$ ocurre, para cualquier i, que $i^p = i$, así que para $i = 0, \ldots, p-1$ se tiene que

$$(\alpha + i)^p - (\alpha + i) - t = \alpha^p - \alpha - t = 0,$$

es decir, $\alpha + i$ es raíz de $f(x)$. Como $f(x)$ es de grado p, ésas son todas sus raíces, y por tanto $E = k(\alpha)$ es un campo de descomposición de $f(x)$ sobre k, y como todas son distintas, el polinomio es separable. Verifiquemos ahora que es irreducible sobre k. Supongamos que $f(x) = u(x)v(x)$, con

$$u(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in k[x]$$

y $0 < d < \partial(f) = p$. Tenemos que $u(x)$ es el producto de d factores de la forma $x - (\alpha + i)$. Sabemos que $-c_{d-1}$ es la suma de las raíces, así que $-c_{d-1} = d\alpha + j$, para alguna $j \in \mathbb{Z}_p \subseteq k$. Por lo tanto, $d\alpha \in k$. Como $0 < d < p$, tenemos que $d \neq 0$ en k, obligando a que $\alpha \in k$, cosa que contradice el lema 3.1. Como $f(x)$ es un polinomio irreducible de grado p, sabemos que $[E : k] = [k(\alpha) : k] = p$, y como $f(x)$ es separable, tenemos que $|\mathrm{Gal}(E : k)| = [E : k] = p$. Así, el grupo de Galois de $f(x)$ sobre k es $\mathrm{Gal}(E : k) \cong \mathbb{Z}_p$.

Probemos ahora que $f(x)$ no es soluble por radicales. Si lo fuera, habría una torre radical

$$k = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_r$$

con $E \subseteq B_r$. Como ya antes lo hemos hecho, podemos suponer que para $i = 1, \ldots, r$ la extensión $B_i : B_{i-1}$ es pura de tipo primo; digamos que $B_i = B_{i-1}(u_i)$, donde $u_i^{q_i} \in B_{i-1}$ con q_i primo. Como $\alpha \in B_r \backslash B_0$ (por el lema 3.1), hay $j \in \{1, \ldots, r\}$ tal que $\alpha \in B_j \backslash B_{j-1}$. Escribamos, para aligerar la notación, $B = K(u)$, donde $u^q = b \in K$ con q primo, $\alpha, u \in B \backslash K$. Es un hecho conocido[4] que como el polinomio $x^q - b \in K[x]$ no se descompone

[4]Véase, por ejemplo, [Rot2, Proposición 3.126] ó [Rot1, Corolario 71].

sobre K (pues $u \notin K$), es irreducible sobre K. Por tanto, $[B : K] = q$. Entonces, $B : K$ no tiene campos intermedios. Tenemos que

$$K \subsetneq K(\alpha) \subseteq B,$$

por lo que $B = K(\alpha)$. Ahora, de manera exactamente análoga a como se hizo ver que $f(x)$ es irreducible sobre k, también se tiene que lo es sobre K (arriba usamos que $\alpha \notin k$ y ahora que $\alpha \notin K$). Entonces, α es raíz del polinomio irreducible $f(x) \in K[x]$, de manera que $q = [B : K] = [K(\alpha) : K] = p$. Ahora, como $K(\alpha) : K$ es claramente campo de descomposición del polinomio separable $f(x) \in K[x]$, y $B = K(\alpha)$, la extensión $B : K$ es de Galois, y en particular separable. Por lo tanto, $u \in B$ es un elemento separable. Pero el polinomio irreducible de u sobre K es, como sabemos, $x^q - b = x^p - b = (x - u)^p$, que tiene raíces repetidas. La contradicción proviene de la suposición de que $f(x)$ es soluble por radicales; por lo tanto, no lo es.

Este ejemplo hace ver, por supuesto, que en el enunciado del gran teorema de Galois no se puede omitir la hipótesis de que la característica del campo sea 0. Cabe señalar que la definición de solubilidad por radicales se puede extender, debilitándola, a campos de característica arbitraria para que no sea necesario imponer tal hipótesis. Véase el enunciado explícito de la definición extendida en [M, Cap. 16, Problema 2], o bien la demostración presentada en [Rom, Sec. 12.3].

Bibliografía

[Al] Alperin, J.L., Bell, R.B., *Groups and Representations*, New York: Springer, 1995.

[Ar1] Artin, E., *Galois Theory - Lectures Delivered at the University of Notre Dame*, 2nd ed., London: University of Notre Dame, 1944.

[Ar2] Artin, E., *Modern Higher Algebra - Galois Theory*, New York: Courant Institute of Mathematical Sciences, 1947.

[G] Gaal, L., *Classical Galois Theory with Examples*, New York: Chelsea Publishing Company, 1998.

[M] Morandi, P., *Field and Galois Theory*, New York: Springer, 1996.

[Rom] Roman, S., *Field Theory*, New York: Springer, 1995.

[Rot1] Rotman, J., *Galois Theory*, 2nd ed., New York: Springer, 1998.

[Rot2] Rotman, J., *Advanced Modern Algebra*, New Jersey: Prentice Hall, 2002.

[Sa] Šafarevič, I. R., On extensions of fields of algebraic numbers solvable in radicals, *Dokl. Akad. Nauk SSSR* (N.S.), **95**, 225-227 (1954).

[St] Stewart, I., *Galois Theory*, 3rd ed., London: Chapman & Hall, 2004.

[Z] Zappa, G., Permutti, R., *Gruppi, Corpi, Equazioni*, Milano: Feltrinelli, 1963.