Teoría de Galois

María Julia Redondo
Instituto de Matemática - UNS
Av. Alem 1253, Bahía Blanca

Abstract

La búsqueda de fórmulas que permitan hallar las raíces de los polinomios fue un problema central del álgebra durante siglos. Scipione del Ferro (1465-1526), Tartaglia (1499-1557), Cardano (1501-1576) mostraron cómo resolver ecuaciones de tercer grado, y Ferrari (1522-1565) encontró un método para calcular las raíces de la ecuaciones de cuarto grado. Galois fue el primero en investigar la estructura de los cuerpos y de los grupos, y mostró que existe una fuerte conexión entre estas dos estructuras. Para determinar si una ecuación algebraica se puede resolver por radicales hay que analizar la estructura del grupo de Galois asociado a dicha ecuación.

Evariste Galois nació en Francia el 25 de octubre de 1811, y murió en un duelo el 30 de mayo de 1832. Sus ideas han dado lugar a una de las teorías más importantes del álgebra: la Teoría de Galois.

Los objetivos de este curso son: definir el grupo de Galois de un polinomio; mostrar cuándo una ecuación es resoluble por radicales; dar aplicaciones de la teoría de Galois: construcciones con regla y compás.

1 La vida de Evariste Galois.

Evariste Galois nació en Francia el 25 de octubre de 1811. Sus padres, Nicholas Gabriel Galois y Adelaide Marie Demante, se preocuparon por transmitirle sus conocimientos de filosofía, literatura y religión. Hasta los 12 años de edad, Galois sólo recibió educación de parte de su madre, quien le enseñó latín, griego y religión. El 6 de octubre de 1823 ingresó en el Liceo Louis-le-Grand, sus calificaciones eran correctas, pero en 1826 tuvo que repetir de año porque su trabajo en retórica no era suficiente para el nivel standard. Fue en febrero de 1827 cuando comenzó a tomar sus primeras clases de matemática con M. Vernier. Sus profesores

lo calificaban como: *singular, extraño, original y cerrado.* El informe de M. Vernier decía: *Inteligente, progresando, pero sin métodos suficientes.*

En 1828 intenta ingresar en la Escuela Politécnica de Paris, pero fracasa. Por cuestiones académicas Galois tenía un gran interés por entrar en esta escuela, pero también le interesaba el fuerte movimiento político que existía entre sus estudiantes. Galois, siguiendo el ejemplo de sus padres, era un ardiente republicano.

En abril de 1829 publica su primer trabajo sobre fracciones continuas en Annales de Mathématiques. En mayo de ese mismo año presenta dos artículos a la Academia de Ciencias sobre la solución de ecuaciones algebraicas, y Cauchy fue el referee seleccionado para decidir sobre estos artículos.

En julio de 1829 Galois sufre el suicidio de su padre, y semanas después vuelve a fracasar en su intento de ingresar en la Escuela Politécnica. En diciembre de ese mismo año termina sus estudios en el Liceo Louis-le-Grand, con los siguientes informes:
En matemática,
Oscuro al expresar sus ideas, inteligente, interesante espíritu de investigación.
En literatura,
Es el único estudiante que ha dado respuestas pobres, no sabe absolutamente nada. Me habían informado que este estudiante tenía una capacidad extraordinaria para las matemáticas. Esto me asombra pues, después de haberlo examinado, creo que tiene muy poca inteligencia.

Galois siguió trabajando en la teoría de ecuaciones. Después de descubrir que sus trabajos incluían resultados ya demostrados por Abel, y siguiendo los consejos de Cauchy, redactó un nuevo artículo sobre las condiciones para que una ecuación sea resoluble por radicales. Este trabajo fue enviado en febrero de 1830 a Fourier, secretario de la Academia de Ciencias, para optar al Gran Premio de matemática. Pero Fourier murió en abril de 1830 y el trabajo nunca fue considerado para el premio.

En diciembre de 1830 fue expulsado de la Escuela Normal por publicar en la Gazette des Écoles una crítica al director M. Guigniault por mantener a los estudiantes encerrados en la escuela para impedir que participaran de los acontecimientos políticos de la época. Decide ingresar al ejército, más tarde es detenido y pasa casi un año en la cárcel. A pedido de Poisson, el 17 de enero de 1831 le envía una tercera versión de su trabajo sobre las soluciones de ecuaciones, y la respuesta fue: *Tus argumentos no son suficientemente claros ni están suficientemente desarrollados como para que pueda juzgar su rigor*, y le recomienda que escriba sus resultados en forma más completa y detallada.

En marzo de 1832, por una epidemia de cólera, los prisioneros de Paris, incluido Galois, son trasladados a la pensión Sieur Faultrier. Aparentemente allí Galois se

enamora de Stephanie-Felice du Motel. Al recobrar su libertad intercambia cartas con Stephanie, y su nombre aparece varias veces en los márgenes de los manuscritos de Galois. El 30 de mayo de 1832 Galois muere en un duelo con Perscheux d'Herbinville, las razones del duelo no son claras, aunque ciertamente relacionadas con Stephanie.

La noche anterior al duelo Galois escribió una nota en el margen de su manuscrito que decía:

Falta algo para completar la demostración. No tengo tiempo.

Tal vez fue esta nota la que dio origen a la leyenda que dice que Galois pasó toda la noche anterior al duelo escribiendo todos sus conocimientos sobre la teoría de grupos.

El hermano de Galois y su amigo Chevalier enviaron sus manuscritos a Gauss, Jacobi y otros, cumpliendo los deseos de Galois de conocer sus opiniones sobre su trabajo. Pero fue recién en septiembre de 1846 cuando Liouville anunció en la Academia que había encontrado en los trabajos de Galois una solución al siguiente problema *Dada una ecuación irreducible de grado primo, decidir si es o no resoluble por radicales.*

Liouville (1809-1882) publicó los trabajos de Galois en 1846, y esta teoría es la que hoy se conoce como **la teoría de Galois**.

2 Ecuaciones de segundo, tercer y cuarto grado.

Una ecuación algebraica de grado n en una incógnita es una ecuación de la forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

donde $a_{n-1}, \ldots, a_1, a_0$ son coeficientes conocidos. La ecuación de grado 1 se resuelve inmediatamente. La ecuación de grado 2 es también sencilla de resolver:

$$\begin{aligned} x^2 + ax + \tfrac{a^2}{4} &= -b + \tfrac{a^2}{4}, \\ (x + \tfrac{a}{2})^2 &= \tfrac{a^2}{4} - b, \\ x + \tfrac{a}{2} &= \pm\sqrt{\tfrac{a^2}{4} - b} \end{aligned}$$

de donde se obtiene la conocida fórmula para la solución de una ecuación de segundo grado:

$$x = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}.$$

El matemático italiano Scipione del Ferro (1465-1526) resolvió la ecuación general de grado 3, pero sus descubrimientos no fueron publicados. Otro matemático italiano, Tartaglia (1499-1557), encontró un método para resolver cualquier ecuación cúbica de la forma

$$x^3 + px + q = 0,$$

y sus resultados fueron publicados por Cardano (1501-1576) en su obra *Ars Magna*. Así, la fórmula para resolver cualquier ecuación cúbica recibe hoy el nombre de fórmula de Cardano, y se deduce de la siguiente manera. En primer lugar, la ecuación cúbica

$$x^3 + a_2x^2 + a_1x + a_0 = 0$$

se puede llevar a una de la forma

$$y^3 + py + q = 0$$

mediante la sustitución $y = x + \frac{a_2}{3}$. Ahora tomemos $y = u + v$ y transformemos nuestro problema en otro con dos incógnitas:

$$(u + v)^3 + p(u + v) + q = 0,$$

esto es,

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Supongamos que las incógnitas u, v satisfacen además la ecuación $3uv + p = 0$. Nuestro problema se reduce a encontrar u, v tales que

$$\begin{cases} u^3 + v^3 + q &= 0, \\ 3uv + p &= 0. \end{cases}$$

Conocidos $u^3 + v^3$ y u^3v^3, sabemos que u^3 y v^3 son las raíces de la ecuación de segundo grado

$$(z - u^3)(z - v^3) = z^2 + qz - \frac{p^3}{27} = 0.$$

Resolviendo esta ecuación de grado 2 en la forma usual, se tiene:

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \qquad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

y así llegamos a la fórmula de Cardano:

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

La ecuación de grado 4 fue resuelta por Ferrari (1522-1565), y su método consiste en lo siguiente. La ecuación

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

se puede escribir en la forma

$$(x^2 + \frac{ax}{2})^2 = (\frac{a^2}{4} - b)x^2 - cx - d.$$

Agreguemos al problema una nueva variable y, y sumemos a ambos miembros de la última ecuación la expresión $(x^2 + \frac{ax}{2})y + \frac{y^2}{4}$. El problema se reduce entonces a resolver la ecuación

$$(x^2 + \frac{ax}{2} + \frac{y}{2})^2 = (\frac{a^2}{4} - b + y)x^2 + (\frac{ay}{2} - c)x + (\frac{y^2}{4} - d) \qquad (*).$$

El objetivo es imponerle condiciones a la nueva variable y para que el segundo miembro de la expresión anterior se pueda escribir en la forma $(ex + f)^2$. Sabemos que la expresión de segundo grado $Ax^2 + Bx + C$ se escribe en la forma $(ex + f)^2$ si y sólo si $B^2 - 4AC = 0$ y, en este caso, $e = \sqrt{A}$ y $f = \sqrt{C}$. Entonces y debe ser solución de la ecuación:

$$(\frac{ay}{2} - c)^2 - 4(\frac{a^2}{4} - b + y)(\frac{y^2}{4} - d) = 0$$

que es una ecuación de grado 3 que ya sabemos resolver (usando la fórmula de Cardano). Sea y_0 una solución de esta ecuación, y calculemos e, f en función de y_0. La igualdad (*) se reduce a

$$(x^2 + \frac{ax}{2} + \frac{y_0}{2})^2 = (ex + f)^2,$$

de donde

$$x^2 + \frac{ax}{2} + \frac{y_0}{2} = ex + f \quad \text{ó} \quad x^2 + \frac{ax}{2} + \frac{y_0}{2} = -ex - f,$$

y las soluciones de estas dos ecuaciones de grado 2 nos dan las cuatro raíces de la ecuación de cuarto grado dada.

En 1770 el matemático francés Lagrange publicó un trabajo donde examinaba propiedades de las soluciones de las ecuaciones de segundo, tercer y cuarto grado que se conocían hasta entonces, y demostró que dichas propiedades no se verificaban para las ecuaciones de grado superior. Hasta este momento ningún matemático había dudado sobre la posibilidad de resolver las ecuaciones por el método de radicales, esto es, encontrar fórmulas que implicaran sólo operaciones de suma, resta,

multiplicación, división, potencia y radicación con exponentes enteros positivos, que permitieran expresar las soluciones en función de los coeficientes de la ecuación.

Lagrange encontró un método distinto para resolver las ecuaciones de grado 2, 3 y 4, que no dependía de un cambio de variables con ciertas condiciones, sino que era el final de una sucesión de razonamientos ordenados y profundos que utilizaban la teoría de los polinomios simétricos, la teoría de las permutaciones de las raíces y la teoría de las resolventes.

Fue el matemático noruego Abel (1802-1829) quien demostró en el año 1824 que no existe una expresión por radicales en función de los coeficientes de una ecuación general de grado n que sea solución de la ecuación, cuando $n \geq 5$.

Como es de esperar, hay muchas formas particulares de ecuaciones que sí son resolubles por radicales: las de la forma $x^n - a = 0$, las ecuaciones cíclicas, las ecuaciones abelianas, las ecuaciones de la forma $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$, con p un número primo. Estas últimas ecuaciones, llamadas ciclotómicas, fueron consideradas por Gauss en conexión con el problema de la construcción con regla y compás de polígonos regulares.

Fue el matemático francés Evariste Galois (1811-1832) quien resolvió el problema de encontrar condiciones necesarias y suficientes para la resolución de una ecuación por radicales.

El cálculo del próximo ejemplo será utilizado en la Sección 10 para mostrar que se puede construir un pentágono regular con regla y compás.

EJEMPLO 2.1. *Calculemos las soluciones de la ecuación* $x^4+x^3+x^2+x+1=0$. *Como* $x = 0$ *no es solución, podemos dividir la ecuación anterior por* x^2, *y así obtenemos*

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0.$$

Sea $y = x + \frac{1}{x}$, *entonces* $y^2 = x^2 + \frac{1}{x^2} + 2$, *y la ecuación anterior se reduce a*

$$y^2 + y - 1 = 0.$$

Entonces

$$x + \frac{1}{x} = -\frac{1}{2} + \frac{\sqrt{5}}{2} \quad \acute{o} \quad x + \frac{1}{x} = -\frac{1}{2} - \frac{\sqrt{5}}{2},$$

y estas ecuaciones son equivalentes a

$$x^2 + \frac{1}{2}(1 - \sqrt{5})x + 1 = 0 \quad \acute{o} \quad x^2 + \frac{1}{2}(1 + \sqrt{5})x + 1 = 0.$$

Luego, las cuatro soluciones de la ecuación dada son

$$\frac{1}{4}(-1 + \sqrt{5}) \pm \frac{i}{2}\sqrt{\frac{5 + \sqrt{5}}{2}}, \quad \frac{1}{4}(-1 - \sqrt{5}) \pm \frac{i}{2}\sqrt{\frac{5 - \sqrt{5}}{2}}.$$

3 Polinomios.

Sea K un cuerpo. Recordemos algunas definiciones y propiedades del anillo de polinomios $K[x]$.

Un polinomio no constante $f(x)$ se dice **irreducible** si no se puede escribir como producto de dos polinomios de grado mayor o igual que 1. Si $f(x)$ no es irreducible, entonces $f(x) = g(x)h(x)$ con $1 \leq \operatorname{gr} g(x), \operatorname{gr} h(x) \leq \operatorname{gr} f(x)$, y diremos que el polinomio $g(x)$ **divide** a $f(x)$, o que $g(x)$ es un **factor** de $f(x)$.

- Algoritmo de división: dados dos polinomios $f(x), g(x) \in K[x]$ con $g(x) \neq 0$, existen únicos $q(x), r(x) \in K[x]$ tales que $f(x) = q(x)g(x) + r(x)$ y $r(x) = 0$ ó $\operatorname{gr} r(x) < \operatorname{gr} g(x)$.

- Factorización única: todo polinomio no constante se escribe como producto de una constante por polinomios irreducibles mónicos, y esta factorización es única salvo el orden de los factores.

- Criterio de irreducibilidad de Eisenstein: si A es un dominio de factorización única, K su cuerpo de cocientes, $f(x) = a_n x^n + \cdots + a_0 \in A[x]$, $n \geq 1$, y existe un primo $p \in A$ tal que $p \nmid a_n$, $p \mid a_i$ para $i = 0, 1, \ldots, n-1$ y $p^2 \nmid a_0$, entonces $f(x)$ es irreducible en $K[x]$.

EJEMPLO 3.1. *El polinomio* $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ *es irreducible en* $\mathbb{Q}[x]$*, cualquiera sea el primo* p*. En efecto, el polinomio*

$$f(x+1) = x^{p-1} + \tbinom{p}{1} x^{p-2} + \cdots + \tbinom{p}{p-2} x + p$$

verifica las condiciones del criterio de Eisenstein.

Un elemento $a \in K$ se dice una raíz del polinomio no nulo $f(x) \in K[x]$ si $f(a) = 0$. Como el resto de dividir a $f(x)$ por $x - a$ es $f(a)$, tenemos que las siguientes condiciones son equivalentes:

- a es raíz de $f(x)$,

- $f(a) = 0$,

- $x - a$ divide a $f(x)$.

Una raíz a del polinomio $f(x)$ se dice una raíz múltiple si existe un natural $m > 1$ tal que $(x-a)^m$ divide a $f(x)$. Si además $(x-a)^{m+1}$ no divide a $f(x)$, se dice que m es el orden de multiplicidad de la raíz a. Como $K[x]$ es un dominio de factorización única, todo polinomio $f(x)$ en $K[x]$ tiene a lo sumo $\operatorname{gr} f(x)$ raíces.

- Un polinomio no constante no tiene raíces múltiples si y sólo si él y su derivado son polinomios coprimos.
- Si $f(x)$ es un polinomio irreducible, $f(x)$ no tiene raíces múltiples si y sólo si $f'(x) \neq 0$.
- Si $\operatorname{car} K = p > 0$, $f'(x) = 0$ si y sólo si $f(x)$ es un polinomio en x^p.
- Un polinomio $f(x)$ irreducible en $K[x]$ tiene raíces múltiples si y sólo si $\operatorname{car} K = p > 0$, $f(x) = h(x^{p^s})$, con $s > 0$, $h(x)$ irreducible sin raíces múltiples, y todas las raíces de $f(x)$ tienen multiplicidad p^s.

4 Extensiones de cuerpos. Cuerpos de raíces.

Un cuerpo E que contiene a un cuerpo K se dice una **extensión** de K. Como E tiene una estructura natural de K-espacio vectorial, llamamos **grado** de E sobre K, y notamos $[E : K]$, a la dimensión de E como K-espacio vectorial. La extensión $K \subset E$ se dice **finita** si su grado es finito.

Si F es una extensión de K y E es una extensión de F entonces E es una extensión de K y $[E : K] = [E : F][F : K]$.

Si E es una extensión de K y $\{c_1, \ldots, c_n\}$ es un subconjunto no vacío de E, se nota $K(c_1, \ldots, c_n)$ al subcuerpo de E generado por K y por $c_1, \ldots, c_n$. Se puede describir al cuerpo $K(c_1, \ldots, c_n)$:

$$K(c_1, \ldots, c_n) = \{\frac{f(c_1, \ldots, c_n)}{g(c_1, \ldots, c_n)} : f, g \in K[x_1, \ldots, x_n], g(c_1, \ldots, c_n) \neq 0\}.$$

Sea E una extensión de K. Un elemento $u \in E$ se dice **algebraico** sobre K si existe un polinomio $f(x) \in K[x]$ tal que $f(u) = 0$. Los elementos que no son algebraicos se dicen **trascendentes**.

EJEMPLO 4.1.

i) El cuerpo $\mathbb{C}$ de números complejos es una extensión de $\mathbb{R}$ de grado 2.

ii) El cuerpo $\mathbb{R}$ es una extensión de $\mathbb{Q}$ de grado infinito (π es un número trascendente).

iii) El cuerpo $\mathbb{Q}(i) = \{a + bi \in \mathbb{C},\ a, b \in \mathbb{Q}\}$ es una extensión de grado 2 de $\mathbb{Q}$.

PROPOSICION 4.2. *Sea E una extensión de K, y sea $u \in E$ algebraico sobre K. Entonces existe un único polinomio mónico irreducible $p(x) \in K[x]$ tal que $p(u) = 0$. Además, el cuerpo $K(u)$ es isomorfo a $K[x]/(p(x))$ y $[K(u) : K] = \operatorname{gr} p(x)$.*

Demostración. Sea $u \in E$ algebraico sobre K y sea I el conjunto de todos los polinomios no nulos $f(x) \in K[x]$ tales que $f(u) = 0$. El conjunto $T = \{\operatorname{gr} f(x),\ f(x) \in I\}$ es un subconjunto no vacío de $\mathbb{N}$, y por lo tanto, tiene primer elemento n. Sea $p(x) \in I$ un polinomio mónico de grado n. El polinomio $p(x)$ es irreducible pues si no lo fuera existirían $g(x), h(x) \in K[x]$ tales que $f(x) = g(x)h(x)$, con $0 < \operatorname{gr} g(x), \operatorname{gr} h(x) < \operatorname{gr} f(x) = n$. Como $0 = f(u) = g(u)h(u)$ implica $g(u) = 0$ ó $h(u) = 0$, existiría en I un polinomio de grado estrictamente menor que n, que es una contradicción pues n es el primer elemento del conjunto T. Veamos que $p(x)$ es único. Sea $f(x) \in I$, mónico e irreducible. Por el algoritmo de la división, existen $q(x), r(x) \in K[x]$ tales que $f(x) = q(x)p(x) + r(x)$ con $r(x) = 0$ ó $0 \leq \operatorname{gr} r(x) < \operatorname{gr} p(x) = n$. Si fuera $r(x) \neq 0$, como $r(u) = f(u) - q(u)p(u) = 0$, tendríamos que $r(x) \in I$, contradicción pues $\operatorname{gr} r(x) < n$. Luego $r(x) = 0$ y $f(x) = q(x)p(x)$. Pero $p(x)$ y $f(x)$ irreducibles mónicos implica que $q(x) = 1$, y por lo tanto $f(x) = p(x)$.
Veamos que $K[x]/(p(x)) \simeq K(u)$. Consideremos la aplicación $\phi : K[x] \to E$ definida por $\phi(f(x)) = f(u)$. La aplicación ϕ es un morfismo de anillos y su núcleo es el conjunto de todos los polinomios en $K[x]$ que se anulan en u, es decir, $\operatorname{Nu} \phi = I \cup \{0\}$. Además, si $f(x) \in I$ vimos que $p(x)$ divide a $f(x)$. Luego $\operatorname{Nu} \phi$ es el ideal generado por $p(x)$, y por lo tanto,

$$K[x]/(p(x)) \simeq K[u] = \{f(u) : f(x) \in K[x]\}.$$

Como $p(x)$ es irreducible, $K[u]$ es un subcuerpo de E. En efecto, sea $w = f(u)$, $f(x) \in K[x]$, $w \neq 0$. Como $p(x)$ es irreducible y $f(u) \neq 0$, el máximo común divisor de $f(x)$ y $p(x)$ es 1, esto es, existen $a(x), b(x) \in K[x]$ tales que $1 = a(x)f(x) + b(x)p(x)$. Aplicando ϕ a la igualdad anterior se tiene que $1 = a(u)w$. Por lo tanto $K[u]$ es un subcuerpo de E, generado por K y por u, es decir, $K[u] = K(u)$ y $[K(u) : K] = \operatorname{gr} p(x)$. □

Sea K un cuerpo y $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$. Una extensión F de K se dice un **cuerpo de raíces** de $f(x)$ sobre K si existen elementos $c_1, \ldots, c_n \in F$ tales que

- $f(x) = a_n(x - c_1) \cdots (x - c_n)$, y
- $F = K(c_1, \ldots, c_n)$.

Es decir, un **cuerpo de raíces** de un polinomio $f(x) \in K[x]$ es una extensión minimal del cuerpo K que contiene a todas las raíces del polinomio $f(x)$. Los próximos teoremas nos aseguran la existencia y unicidad (a menos de isomorfismos) del cuerpo de raíces de un polinomio $f(x) \in K[x]$.

TEOREMA 4.3. *Si $f(x) \in K[x]$ es un polinomio de grado $n \geq 1$, existe una extensión F de K tal que $f(x) = a(x - c_1) \cdots (x - c_n)$, $a \in K$, $c_1, \ldots, c_n \in F$.*

Demostración. La existencia se muestra por inducción en el grado del polinomio. Si $f(x) \in K[x]$ tiene grado 1, $F = K$ satisface el teorema. Sea $\operatorname{gr} f(x) = n$ y supongamos que el teorema es válido para todo polinomio no constante de grado menor que n.
Si $f(x)$ es irreducible, $F_1 = K[x]/(f(x))$ es un cuerpo que contiene a K (identificando $k \in K$ con la clase de equivalencia $\overline{k}$ de $K[x]/(f(x))$ que contiene a k), y por lo tanto es una extensión de K. Si $c_1 = \overline{x} \in F_1$ es la clase de equivalencia de $K[x]/(f(x))$ que contiene al polinomio x, entonces $f(\overline{x}) = \overline{f(x)} = 0$. Luego $f(x) = a(x - c_1)g(x)$ en $F_1[x]$. Por hipótesis inductiva, existe una extensión F_2 de F_1 tal que $g(x) = (x - c_2) \cdots (x - c_n)$, $c_2, \ldots, c_n \in F_2$. Entonces F_2 es la extensión de K buscada.
Si $f(x)$ no es irreducible, $f(x) = g(x)h(x)$, con $1 \leq \operatorname{gr} g(x), \operatorname{gr} h(x) < n$. Por hipótesis inductiva, existe una extensión F_1 de K tal que $g(x) = a(x - c_1) \cdots (x - c_r)$, $c_1, \ldots, c_r \in F_1$. Como $K[x] \subset F_1[x]$, podemos aplicar la hipótesis inductiva en el polinomio $h(x) \in F_1[x]$. Entonces existe una extensión F_2 de F_1, y por lo tanto extensión de K, que satisface el teorema. □

Por el teorema anterior $K(c_1, \ldots, c_n)$, es decir, el subcuerpo de F generado por K y por $c_1, \ldots, c_n$, es un cuerpo de raíces de $f(x)$.

EJEMPLO 4.4.

1) *$\mathbb{Q}(\sqrt{a^2 - 4b})$ es un cuerpo de raíces del polinomio $x^2 + ax + b \in \mathbb{Q}[x]$.*

2) *Si ω es una raíz del polinomio $f(x) = \frac{x^p - 1}{x - 1} \in \mathbb{Q}[x]$, entonces $\mathbb{Q}(\omega)$ es un cuerpo de raíces de $f(x)$.*

3) *Si F es un cuerpo de característica $p > 0$, y b es una raíz del polinomio $f(x) = x^p - x - a \in F[x]$, entonces todas las raíces de $f(x)$ son $b, b+1, b+2, \ldots, b+p-1$. Luego $F(b)$ es un cuerpo de raíces de $f(x)$ sobre F.*

TEOREMA 4.5. *Sea $\varphi : K \to K_1$ un isomorfismo de cuerpos, $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, $f_1(x) = \sum_{i=0}^{n} \varphi(a_i) x^i \in K_1[x]$. Sean F, F_1 cuerpos de raíces de $f(x), f_1(x)$ respectivamente. Entonces existe un isomorfismo $\psi : F \to F_1$ que extiende a φ y que aplica raíces de $f(x)$ en raíces de $f_1(x)$.*

Demostración. Por inducción sobre n. Si $n = 1$, $F = K$, $F_1 = K_1$ y $\psi = \varphi$. Sea $n > 1$ y supongamos que el teorema es cierto para cualquier polinomio de grado $n-1$.

Sean $c_1, \ldots, c_n$ las raíces de $f(x)$ en F y $d_1, \ldots, d_n$ las raíces de $f_1(x)$ en F_1. Sea $g(x)$ un factor irreducible de $f(x)$, $g_1(x)$ el factor irreducible correspondiente de $f_1(x)$. Supongamos que c_1 y d_1 son raíces de $g(x), g_1(x)$ respectivamente. Entonces, por la Proposición 4.2, sabemos que $K(c_1) \simeq K[x]/(g(x))$ y que $K_1(d_1) \simeq K_1[x]/(g_1(x))$. El isomorfismo $\varphi : K \to K_1$ induce naturalmente un isomorfismo entre $K[x]/(g(x))$ y $K_1[x]/(g_1(x))$. Por composición, obtenemos un isomorfismo $\psi_1 : K(c_1) \to K_1(d_1)$ que extiende a φ y tal que $\psi_1(c_1) = d_1$. Sean $f(x) = (x - c_1)h(x)$, $f_1(x) = (x - d_1)h_1(x)$. Como $h_1(x)$ es el polinomio en $K_1(d_1)[x]$ correspondiente al polinomio $h(x)$ en $K(c_1)[x]$ vía el isomorfismo $\psi_1 : K(c_1) \to K_1(d_1)$, y F, F_1 son los cuerpos de raíces de $h(x), h_1(x)$ respectivamente, por hipótesis inductiva sabemos que existe un isomorfismo $\psi : F \to F_1$ que extiende a ψ_1 y que aplica raíces de $h(x)$ en raíces de $h_1(x)$. Luego ψ es el isomorfismo buscado. □

En particular, si $K = K_1$ y $\varphi = id_K$, el teorema anterior nos dice que el cuerpo de raíces de un polinomio $f(x)$ es único a menos de isomorfismos, y estos isomorfismos producen una permutación de las raíces del polinomio.

Dado un cuerpo F, se llama **cuerpo primo** de F al menor subcuerpo de F que contiene al 1. Si F es un cuerpo de característica cero, esto es, la aplicación $h : \mathbb{Z} \to F$ definida por $h(n) = n.1_F$ es un monomorfismo de anillos, entonces su cuerpo primo es isomorfo a $\mathbb{Q}$. Si la aplicación $h : \mathbb{Z} \to F$ definida por $h(n) = n.1_F$ no es un monomorfismo, su núcleo es un ideal primo de $\mathbb{Z}$, $\operatorname{Nu} h = p\mathbb{Z}$. En este caso se dice que F es un cuerpo de característica p, y su cuerpo primo es isomorfo a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

En particular, si F es un cuerpo finito con q elementos, la aplicación $h : \mathbb{Z} \to F$ no puede ser un monomorfismo. Si $\mathbb{F}_p$ es el cuerpo primo de F, F es una extensión de $\mathbb{F}_p$. Si $[F : \mathbb{F}_p] = n$ entonces F tiene p^n elementos.

TEOREMA 4.6. *Si F es un cuerpo finito con p^n elementos entonces F es el cuerpo de raíces del polinomio $x^{p^n} - x$ sobre el subcuerpo primo de F.*

Demostración. Sea F un cuerpo finito con p^n elementos, y sea $\mathbb{F}_p$ el cuerpo primo de F. El grupo multiplicativo $F^* = F \setminus \{0\}$ tiene orden $p^n - 1$, entonces $a^{p^n-1} = 1$ cualquiera sea $a \in F^*$. Entonces todo elemento de F es raíz del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$. Por otro lado, como el polinomio derivado de $x^{p^n} - x$ es -1, el polinomio $x^{p^n} - x$ tiene p^n raíces distintas, y éstas generan al cuerpo F. Luego F es el cuerpo de raíces del polinomio $x^{p^n} - x$. □

5 Grupos de Galois.

Galois descubrió que el problema de decidir si las soluciones de una ecuación se pueden expresar en términos de sumas, productos y raíces n-ésimas de los coeficientes de la ecuación, se podía resolver comparando el cuerpo generado por los coeficientes con el cuerpo generado por las soluciones de la ecuación. Galois consideraba permutaciones de las raíces que dejaban fijo el cuerpo generado por los coeficientes.

Sea $\mathrm{Aut}(F)$ el grupo de todos los automorfismos de F, esto es, funciones biyectivas de F en F que preservan la adición y la multiplicación.

Sea F una extensión del cuerpo K. El **grupo de Galois** de F sobre K se define como el grupo de los automorfismos de F que dejan fijo al cuerpo K, es decir,

$$\mathrm{Gal}(F/K) = \{\phi \in \mathrm{Aut}(F) : \phi(a) = a \text{ para todo } a \in K\}.$$

EJEMPLO 5.1. *El grupo de Galois* $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ *es cíclico de orden* 2. *En efecto, sea* $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ *un automorfismo que deja fijo al cuerpo* $\mathbb{Q}$, $\sigma \neq id$. *Entonces* $\sigma(a + bi) = a + b\sigma(i)$, *y* $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$. *Como* $\sigma \neq id$, *tenemos que* $\sigma(i) = -i$, *y es claro que* $\sigma^2 = id$.

Si F es el cuerpo de raíces del polinomio $f(x) \in K[x]$, el grupo de Galois $\mathrm{Gal}(F/K)$, llamado también el grupo de Galois de $f(x)$ sobre K, se puede identificar con un subgrupo del grupo S_n. En efecto, si $f(x) = (x - c_1) \cdots (x - c_n) \in F[x]$ y $\sigma \in \mathrm{Gal}(F/K)$, como σ es un morfismo que deja fijos los elementos de K, $\sigma(f(a)) = f(\sigma(a))$, para todo $a \in F$. En particular, σ aplica raíces en raíces, y por lo tanto, define una permutación de $\{c_1, \ldots, c_n\}$.

Si F es una extensión de un cuerpo K y H es un subgrupo de $\mathrm{Gal}(F/K)$, se llama **cuerpo fijo** de H, y se nota F^H, al conjunto de elementos de F que quedan fijos por H, esto es,

$$F^H = \{a \in F : \sigma(a) = a \text{ para todo } \sigma \in H\}.$$

Es fácil probar que F^H es un subcuerpo de F que contiene a K.

PROPOSICION 5.2. *Sea* F *una extensión finita de un cuerpo* K. *Entonces:*

(i) $|\mathrm{Gal}(F/K)| \leq [F : K]$.

(ii) Si H *es un subgrupo de* $\mathrm{Gal}(F/K)$ *entonces* $[F : F^H] \leq |H|$.

(iii) Si el cuerpo fijo de $\mathrm{Gal}(F/K)$ *es* K *entonces* $|\mathrm{Gal}(F/K)| = [F : K]$.

Para demostrar la proposición anterior usaremos el siguiente resultado.

LEMA 5.3. *Sean $\{\sigma_1, \ldots, \sigma_r\}$ un conjunto de r automorfismos distintos de F. Entonces el conjunto dado es linealmente independiente sobre F, es decir, no existen $a_1, \ldots, a_r \in F$ no todos nulos tales que $a_1\sigma_1 + \cdots + a_r\sigma_r = 0$.*

Demostración. Lo demostraremos por inducción sobre r. Si $r = 1$ es inmediato pues $\sigma_1 \neq 0$. Supongamos que el lema es cierto para cualquier conjunto de $r-1$ automorfismos, y supongamos que existen $a_1, \ldots, a_r \in F$ no todos nulos tales que $a_1\sigma_1 + \cdots + a_r\sigma_r = 0$. Por la hipótesis inductiva sabemos que ningún a_i puede ser cero. Como $\sigma_1 \neq \sigma_r$, existe $b \in F$ tal que $\sigma_1(b) \neq \sigma_r(b)$. Para todo $x \in F$, $0 = (a_1\sigma_1 + \cdots + a_r\sigma_r)(bx) = (a_1\sigma_1(b)\sigma_1 + \cdots + a_r\sigma_r(b)\sigma_r)(x)$. Si restamos miembro a miembro las igualdades

$$\begin{aligned} a_1\sigma_1(b)\sigma_1 + a_2\sigma_2(b)\sigma_2 + \cdots + a_r\sigma_r(b)\sigma_r &= 0 \\ a_1\sigma_r(b)\sigma_1 + a_2\sigma_r(b)\sigma_2 + \cdots + a_r\sigma_r(b)\sigma_r &= 0 \end{aligned}$$

tenemos que

$$a_1(\sigma_1(b) - \sigma_r(b))\sigma_1 + \cdots + a_{r-1}(\sigma_{r-1}(b) - \sigma_r(b))\sigma_{r-1} = 0$$

y esta igualdad contradice la hipótesis inductiva. □

Demostración. De la Proposición 5.2.

(i) Veamos que $|\operatorname{Gal}(F/K)| \leq [F : K]$. Sea $n = [F : K]$ y sea $\{a_1, \ldots, a_n\}$ una base de F sobre K. Sea $\{\sigma_1, \ldots, \sigma_r\}$ un conjunto de r K-automorfismos distintos de F, y supongamos que $r > n$. Entonces el sistema homogéneo de n ecuaciones con r incógnitas

$$\begin{cases} \sigma_1(a_1)x_1 + \cdots + \sigma_r(a_1)x_r &= 0 \\ \cdots & \\ \sigma_1(a_n)x_1 + \cdots + \sigma_r(a_n)x_r &= 0 \end{cases}$$

admite solución no trivial $(b_1, \ldots, b_r)$. Si $a \in F$, a se escribe como $a = \lambda_1 a_1 + \cdots + \lambda_n a_n$, con $\lambda_i \in K$, y luego $\sigma_i(a) = \lambda_1\sigma_i(a_1) + \cdots + \lambda_n\sigma_i(a_n)$. Entonces $(b_1, \ldots, b_r)$ es también solución de la ecuación

$$\sigma_1(a)x_1 + \cdots + \sigma_r(a)x_r = 0$$

y esto para todo $a \in F$. El lema anterior nos dice entonces que los automorfismos no pueden ser todos distintos. Contradicción que provino de suponer que $r > n$.

(ii) Sea H un subgrupo de $\mathrm{Gal}(F/K)$ y supongamos que $m = |H| < [F : F^H] = r$. Sea $H = \{\sigma_1 = id, \sigma_2, \ldots, \sigma_m\}$ y sean $a_1, \ldots, a_{m+1}$ elementos de F linealmente independientes sobre F^H. El sistema homogéneo de m ecuaciones con $m+1$ incógnitas

$$\begin{cases} \sigma_1(a_1)x_1 + \cdots + \sigma_1(a_{m+1})x_{m+1} & = 0 \\ \cdots & \\ \sigma_m(a_1)x_1 + \cdots + \sigma_m(a_{m+1})x_{m+1} & = 0 \end{cases}$$

admite solución no trivial $(b_1, \ldots, b_{m+1})$. Como $\sigma_1 = id$, los elementos b_i no pueden pertencer todos al cuerpo F^H pues, en ese caso, la primer ecuación sería una contradicción a la independencia lineal de los elementos $a_1, \ldots, a_{m+1}$ sobre F^H. Sin pérdida de generalidad, podemos elegir una solución no trivial $(b_1, \ldots, b_s, 0, \ldots, 0)$ tal que s sea mínimo, esto es, que cualquier solución no trivial del sistema tenga por lo menos s coordenadas no nulas. Si fuera $s = 1$, tendríamos que $\sigma_1(a_1)b_1 = 0$, y por lo tanto, $a_1 = 0$ pues $b_1 \neq 0$ y $\sigma_1 = id$. Luego $s > 1$. Además podemos suponer que $b_s = 1$, pues $b_s^{-1}(b_1, \ldots, b_s, 0, \ldots, 0)$ es también solución del sistema. Entonces tenemos que

$$\sigma_i(a_1)b_1 + \cdots + \sigma_i(a_{s-1})b_{s-1} + \sigma_i(a_s) = 0 \qquad (*)$$

para todo $i = 1, \ldots, m$. Sabemos que $b_1, \ldots, b_{s-1}$ no pueden pertenecer todos al cuerpo F^H. Supongamos que $b_1 \notin F^H$. Como F^H es el cuerpo fijo de H, existe $\sigma_k \in H$ tal que $\sigma_k(b_1) \neq b_1$. Si aplicamos σ_k a las expresiones (*) tenemos que

$$(\sigma_k\sigma_i)(a_1)\sigma_k(b_1) + \cdots + (\sigma_k\sigma_i)(a_{s-1})\sigma_k(b_{s-1}) + (\sigma_k\sigma_i)(a_s) = 0$$

para todo $i = 1, \ldots, m$. Como $\{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_m\} = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$, tenemos que

$$\sigma_i(a_1)\sigma_k(b_1) + \cdots + \sigma_i(a_{s-1})\sigma_k(b_{s-1}) + \sigma_i(a_s) = 0 \qquad (**)$$

para todo $i = 1, \ldots, m$. Si restamos (**) a (*) tenemos que

$$\sigma_i(a_1)(b_1 - \sigma_k(b_1)) + \cdots + \sigma_i(a_{s-1})(b_{s-1} - \sigma_k(b_{s-1})) = 0$$

para todo $i = 1, \ldots, m$. Pero esto contradice la minimalidad de s.

(iii) Inmediato de (i) y (ii). □

EJEMPLO 5.4.

1) *Sea* $f(x) = x^2 - 5 \in \mathbb{Q}[x]$. *El cuerpo de raíces de* $f(x)$ *es* $\mathbb{Q}(\sqrt{5})$ *y el grupo de Galois* $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ *es cíclico de orden* 2, *generado por el automorfismo* $\sigma : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5})$, $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$.

2) *Sea* $f(x) = x^3 - 5 \in \mathbb{Q}[x]$. *El cuerpo de raíces de* $f(x)$ *es* $\mathbb{Q}(\sqrt[3]{5}, \omega)$, *con* $\omega = \frac{-1+\sqrt{3}i}{2}$, *y el grupo de Galois* $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5}, \omega)/\mathbb{Q})$ *es el grupo simétrico* S_3, *generado por los automorfismos* $\sigma, \tau : \mathbb{Q}(\sqrt[3]{5}, \omega) \to \mathbb{Q}(\sqrt[3]{5}, \omega)$, $\sigma(a + b\sqrt[3]{5} + c\omega) = a + b\sqrt[3]{5}\omega + c\omega$, $\tau(a + b\sqrt[3]{5} + c\omega) = a + b\sqrt[3]{5} + c\omega^2$, *con* $\sigma^3 = id = \tau^2$, $\sigma\tau = \tau\sigma^2$.

3) *Sea* $f(x) = x^4 - 5 \in \mathbb{Q}[x]$. *El cuerpo de raíces de* $f(x)$ *es* $\mathbb{Q}(i, \sqrt[4]{5})$ *y el grupo de Galois* $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{5})/\mathbb{Q})$ *es el grupo dihedral de orden* 8, *generado por los automorfismos* $\sigma, \tau : \mathbb{Q}(i, \sqrt[4]{5}) \to \mathbb{Q}(i, \sqrt[4]{5})$, $\sigma(a + bi + c\sqrt[4]{5}) = a + bi + c\sqrt[4]{5}i$, $\tau(a + bi + c\sqrt[4]{5}) = a - bi + c\sqrt[4]{5}$, *con* $\sigma^4 = 1 = \tau^2$ *y* $\sigma\tau = \tau\sigma^3$.

Si F es un cuerpo de característica p, la función $\phi : F \to F$ definida por $\phi(x) = x^p$ es un morfismo de anillos. Además, como F es un cuerpo y $\phi \neq 0$, ϕ es un monomorfismo. Si F es finito, ϕ resulta un isomorfismo de cuerpos, y recibe el nombre de **automorfismo de Frobenius**.

Una potencia apropiada del automorfismo de Frobenius nos permite demostrar que el grupo de Galois de cualquier cuerpo finito es cíclico.

PROPOSICION 5.5. *Si* K *es un cuerpo finito,* F *una extensión de* K *y* $[F : K] = m$, *entonces* $\mathrm{Gal}(F/K)$ *es un grupo cíclico de orden* m.

Demostración. Por la Proposición 5.2 sabemos que $|\mathrm{Gal}(F/K)| \leq m$. Sea p^n el número de elementos del cuerpo K. Entonces F tiene p^{nm} elementos, y todo elemento de F es raíz del polinomio $x^{p^{nm}} - x$. Sea $\theta : F \to F$ definido por $\theta(x) = x^{p^n}$, es decir, θ es la composición n-veces del automorfismo de Frobenius. Luego θ es un automorfismo, y de orden m. En efecto, supongamos que existe d con $1 < d \leq m$ tal que $\theta^d = id$. Entonces todo elemento de F sería raíz del polinomio $x^{p^{nd}} - x$, que tiene p^{nd} raíces distintas. Luego $p^{nd} = p^{nm}$ y por lo tanto $d = m$. Entonces $\mathrm{Gal}(F/K)$ es un grupo de orden m que admite a θ como generador. □

6 El teorema fundamental de la teoría de Galois.

El problema de decidir si las soluciones de una ecuación $f(x) = 0$, con $f(x) \in K[x]$, se pueden resolver por radicales, es decir, si se pueden obtener a partir de operaciones

de suma, producto y radicación de elementos del cuerpo K, es equivalente a decidir si el cuerpo de raíces de $f(x)$ se puede obtener a partir de K a través de una sucesión de extensiones que se obtienen adjuntando raíces de polinomios $x^n - a$. Si queremos encontrar una condición necesaria y suficiente para nuestro problema en términos del grupo de Galois $\mathrm{Gal}(F/K)$ de $f(x)$ sobre K, es necesario conocer la relación que existe entre los cuerpos que viven entre K y F y los subgrupos de $\mathrm{Gal}(F/K)$.

Un polinomio no constante $f(x)$ se dice **separable** si todos sus factores irreducibles tienen sólo raíces simples. En particular, si K es un cuerpo de característica cero, todo polinomio no constante en $K[x]$ es separable.

Una extensión F de un cuerpo K se dice **algebraica** si todo elemento de F es algebraico sobre K.

Una extensión algebraica F de un cuerpo K se dice **normal** si todo polinomio irreducible en $K[x]$ que tiene una raíz en F tiene todas sus raíces en F.

EJEMPLO 6.1.

1) $\mathbb{C}$ *es una extensión algebraica de* $\mathbb{R}$ *pero no es una extensión algebraica de* $\mathbb{Q}$.

2) $\mathbb{Q}(\sqrt[3]{2})$ *es una extensión algebraica de* $\mathbb{Q}$ *pero no es una extensión normal.*

3) $\mathbb{Q}(\sqrt{2}, i)$ *es una extensión normal de* $\mathbb{Q}$.

4) Toda extensión finita de un cuerpo K es algebraica. En efecto, si F es una extensión de K de grado n y $a \in F$, el conjunto $\{1, a, \ldots, a^n\}$ es linealmente dependiente sobre K, y por lo tanto, a es raíz de un polinomio en $K[x]$ de grado menor o igual a n.

LEMA 6.2. *Si F es el cuerpo de raíces de un polinomio separable $f(x) \in K[x]$ entonces el cuerpo fijo de su grupo de Galois* $\mathrm{Gal}(F/K)$ *es K.*

Demostración. Lo demostraremos por inducción en el número de raíces del polinomio $f(x)$ que están en F y no están en K. Si todas las raíces de $f(x)$ están en K, entonces $F = K$, $\mathrm{Gal}(F/K) = \{id\}$ y $F^{\mathrm{Gal}(F/K)} = K$.

Supongamos que $f(x)$ tiene $m > 0$ raíces en F que no están en K. Sea $f(x) = p_1(x)p_2(x)\cdots p_r(x)$ una factorización de $f(x)$ en producto de polinomios irreducibles en $K[x]$. Como $f(x)$ tiene raíces en $F \setminus K$, los $p_i(x)$ no pueden ser todos de grado 1. Supongamos que $\mathrm{gr}\, p_1(x) = s > 1$ y sea $u_1 \in F$ una raíz de $p_1(x)$. Entonces $[K(u_1) : K] = \mathrm{gr}\, p_1(x) = s$. Por hipótesis inductiva, como $f(x)$ es un polinomio separable en $K(u_1)[x]$ y F es su cuerpo de raíces, el cuerpo fijo del grupo de Galois $\mathrm{Gal}(F/K(u_1))$ es $K(u_1)$. Por hipótesis, las raíces $u_1, \ldots, u_s$ de $p_1(x)$ son distintas dos a dos. Por la Proposición 4.2 sabemos que $K(u_i) \simeq K[x]/(p_1(x))$ para todo

$i = 1, \ldots, s$. Entonces existen isomorfismos $\sigma_1, \ldots, \sigma_s$ tales que $\sigma_i : K(u_1) \to K(u_i)$ deja fijo al cuerpo K y $\sigma_i(u_1) = u_i$, para todo $i = 1, \ldots, s$. Por el Teorema 4.5, para cada i existe un automorfismo $\varphi_i : F \to F$ que extiende a σ_i y que permuta las raíces de $f(x)$. Por lo tanto $\varphi_i \in \mathrm{Gal}(F/K)$.

Sea $w \in F^{\mathrm{Gal}(F/K)}$. Como $K \subset K(u_1)$ tenemos que $\mathrm{Gal}(F/K(u_1)) \subset \mathrm{Gal}(F/K)$, y por lo tanto, $F^{\mathrm{Gal}(F/K)} \subset F^{\mathrm{Gal}(F/K(u_1))}$. Luego $w \in F^{\mathrm{Gal}(F/K(u_1))} = K(u_1)$, esto es, $w = a_{s-1}u_1^{s-1} + \cdots + a_1u_1 + a_0$, con todos los $a_i \in K$. Aplicando φ_i a la igualdad anterior tenemos que

$$w = \varphi_i(w) = a_{s-1}u_i^{s-1} + \cdots + a_1u_i + a_0$$

para todo $i = 1, \ldots, s$. Entonces el polinomio

$$a_{s-1}x^{s-1} + \cdots + a_1x + (a_0 - w)$$

tiene s raíces distintas $u_1, u_2, \ldots, u_s$, y por lo tanto, todos sus coeficientes son nulos. Luego $w = a_0 \in K$ y $F^{\mathrm{Gal}(F/K)} = K$. □

TEOREMA 6.3. *Sea F el cuerpo de raíces de un polinomio $f(x) \in K[x]$, $f(x)$ separable,* $\mathrm{Gal}(F/K)$ *su grupo de Galois.*

(a) Existe una correspondencia biunívoca entre subgrupos de $\mathrm{Gal}(F/K)$ *y subcuerpos de F que contienen a K:*

(i) Si $K \subset E \subset F$, el subgrupo correspondiente es $\mathrm{Gal}(F/E)$*, formado por todos los automorfismos de F que dejan fijo al cuerpo E;*

(ii) Si H es un subgrupo de $\mathrm{Gal}(F/K)$*, el cuerpo correspondiente F^H está formado por todos los elementos de F que son dejados fijos por los automorfismos en H;*

(iii) Si E_1, E_2 son subcuerpos asociados a los subgrupos H_1, H_2 respectivamente, entonces $E_1 \subset E_2$ si y sólo si $H_1 \supset H_2$.

(b) $[F : F^H] = |H|$ y $[F^H : K] = [\mathrm{Gal}(F/K) : H]$, para cualquier subgrupo H de $\mathrm{Gal}(F/K)$.

(c) H es un subgrupo normal de $\mathrm{Gal}(F/K)$ *si y sólo si F^H es una extensión normal de K. En este caso,* $\mathrm{Gal}(F^H/K) \simeq \mathrm{Gal}(F/K)/\mathrm{Gal}(F/F^H)$.

Demostración.

1. Si $K \subset E \subset F$ entonces $\mathrm{Gal}(F/E)$ es un subgrupo de $\mathrm{Gal}(F/K)$.

2. Si H es un subgrupo de $\mathrm{Gal}(F/K)$ entonces F^H es un subcuerpo de F que contiene a K.

3. Si $K \subset E_1 \subset E_2 \subset F$ entonces

$$\mathrm{Gal}(F/K) \supset \mathrm{Gal}(F/E_1) \supset \mathrm{Gal}(F/E_2) \supset \mathrm{Gal}(F/F) = \{1\}.$$

4. Si $H_1 \subset H_2 \subset \mathrm{Gal}(F/K)$ entonces

$$F \supset F^{H_1} \supset F^{H_2} \supset F^{\mathrm{Gal}(F/K)} = K.$$

5. Si H es un subgrupo de $\mathrm{Gal}(F/K)$, la Proposición 5.2(i)(ii) nos dice que $|\,\mathrm{Gal}(F/F^H)| \leq [F : F^H]$ y que $[F : F^H] \leq |H|$. Entonces

$$[F : F^H] \leq |H| \leq |\,\mathrm{Gal}(F/F^H)| \leq [F : F^H]$$

y por lo tanto $H = \mathrm{Gal}(F/F^H)$.

6. Si $K \subset E \subset F$, como $f(x)$ es un polinomio separable en $E[x]$ y F es su cuerpo de raíces, el lema anterior nos dice que $F^{\mathrm{Gal}(F/E)} = E$.

7. Si H es un subgrupo de $\mathrm{Gal}(F/K)$, ya vimos que $[F : F^H] = |\,\mathrm{Gal}(F/F^H)| = |H|$. Además, como $[F : F^H][F^H : K] = [F : K] = [F : F^{\mathrm{Gal}(F/K)}] = |\,\mathrm{Gal}(F/K)| = [\mathrm{Gal}(F/K) : H]|H|$, se tiene que $[F^H : K] = [\mathrm{Gal}(F/K) : H]$.

8. Sea H un subgrupo de $\mathrm{Gal}(F/K)$ tal que F^H es una extensión normal de K. Sea $\Phi : \mathrm{Gal}(F/K) \to \mathrm{Gal}(F^H/K)$ la aplicación definida por $\Phi(\sigma) = \sigma/_{F^H}$. Veamos que la definición es buena, esto es, si $\sigma : F \to F$ es un automorfismo que deja fijo al cuerpo K y $w \in F^H$, hay que ver que $\sigma(w) \in F^H$. Como cada w es algebraico sobre K, la Proposición 4.2 nos dice que existe un polinomio irreducible $p(x) \in K[x]$ que tiene a w como raíz. Además, como F^H es una extensión normal de K, $p(x)$ tiene todas sus raíces en F^H. Entonces $p(\sigma(w)) = \sigma(p(w)) = 0$ implica que $\sigma(w) \in F^H$. Entonces $\sigma/_{F^H} : F^H \to F^H$ es un automorfismo que deja fijo al cuerpo K. Es claro que Φ es un morfismo de grupos y su núcleo es

$$\mathrm{Nu}\,\Phi = \{\sigma \in \mathrm{Gal}(F/K) : \Phi(\sigma) = id\} = \mathrm{Gal}(F/F^H) = H.$$

Entonces H es un subgrupo normal de $\mathrm{Gal}(F/K)$. Además

$$|\,\mathrm{Gal}(F^H/K)| \leq [F^H : K] = [\mathrm{Gal}(F/K) : H] = |\,\mathrm{Im}\,\Phi| \leq |\,\mathrm{Gal}(F^H/K)|$$

y por lo tanto, Φ es sobreyectiva y $\mathrm{Gal}(F^H/K) \simeq \mathrm{Gal}(F/K)/\,\mathrm{Gal}(F/F^H)$.

9. Si H es un subgrupo normal de $\mathrm{Gal}(F/K)$, la aplicación $\Phi : \mathrm{Gal}(F/K) \to \mathrm{Gal}(F^H/K)$ definida por $\Phi(\sigma) = \sigma/_{F^H}$ es buena, esto es, si $\sigma : F \to F$ es un automorfismo que deja fijo al cuerpo K y $w \in F^H$, hay que ver que $\sigma(w) \in F^H$. Pero como $\sigma H = H\sigma$, $h\sigma(w) = \sigma h'(w) = \sigma(w)$, y por lo tanto $\sigma(w) \in F^H$. Es claro que Φ es un morfismo de grupos. Sea $G' = \mathrm{Im}\,\Phi$ y sea $E = F^H$. Entonces

$$\begin{aligned} E^{G'} &= \{w \in F^H : \Phi(\sigma)(w) = w \text{ para todo } \sigma \in \mathrm{Gal}(F/K)\} \\ &= \{w \in F^H : \sigma(w) = w \text{ para todo } \sigma \in \mathrm{Gal}(F/K)\} \\ &= K. \end{aligned}$$

Sea $g(x)$ mónico irreducible en $K[x]$, $u \in E$ una raíz de $g(x)$. Veamos que todas las raíces de $g(x)$ están en E. Sea $\{u, u_2, \ldots, u_r\}$ el conjunto de todos los elementos distintos del conjunto $\{\sigma(u), \sigma \in G'\}$. Como G' es un grupo, si $\tau \in G'$, $\tau(u_i) = \tau\sigma(u) = u_j$. Entonces todo automorfismo de G' permuta los elementos $u, u_2, \ldots, u_r$. Sea $h(x) = (x-u)(x-u_2)\cdots(x-u_r) \in E[x]$. Si $\tau \in G'$, como $\tau(h(x)) = h(x)$ resulta que $h(x) \in E^{G'}[x] = K[x]$. Como $g(x) \in K[x]$ y $g(u) = 0$, tenemos que $g(u_i) = g(\sigma(u)) = \sigma(g(u)) = 0$, esto es, $u, u_2, \ldots, u_r$ son raíces distintas de $g(x)$. Luego $h(x)$ divide a $g(x)$, pero como $g(x)$ es irreducible y mónico, $g(x) = h(x)$ y $g(x)$ tiene todas sus raíces en E, y por lo tanto $E = F^H$ es una extensión normal de K. □

EJEMPLO 6.4. *Volviendo al Ejemplo 5.4, describiremos la correspondencia entre subgrupos y cuerpos intermedios.*

1) Si $f(x) = x^2 - 5 \in \mathbb{Q}[x]$, $\mathbb{Q}(\sqrt{5})$ *es su cuerpo de raíces y* $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ *es cíclico de orden 2, generado por el automorfismo* $\sigma : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5})$, $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$. *Los subgrupos de* $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$, *ordenados por la relación inclusión, forman el reticulado*

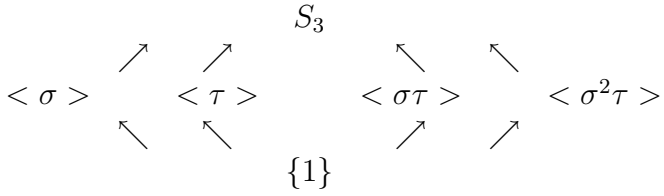
$$\{1\} \to \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$$

que corresponde al reticulado de cuerpos intermedios

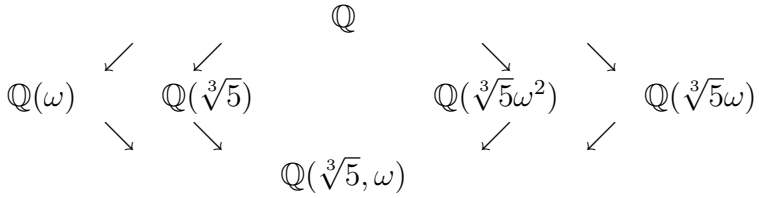
$$\mathbb{Q}(\sqrt{5}) \leftarrow \mathbb{Q}.$$

2) Si $f(x) = x^3 - 5 \in \mathbb{Q}[x]$, $\mathbb{Q}(\sqrt[3]{5}, \omega)$ *es su cuerpo de raíces y* $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5}, \omega)/\mathbb{Q})$ *es el grupo simétrico* S_3, *generado por los automorfismos* $\sigma, \tau : \mathbb{Q}(\sqrt[3]{5}, \omega) \to \mathbb{Q}(\sqrt[3]{5}, \omega)$, $\sigma(a + b\sqrt[3]{5} + c\omega) = a + b\sqrt[3]{5}\omega + c\omega$, $\tau(a + b\sqrt[3]{5} + c\omega) = a + b\sqrt[3]{5} + c\omega^2$, *con* $\sigma^3 = id = \tau^2$, $\sigma\tau = \tau\sigma^2$.

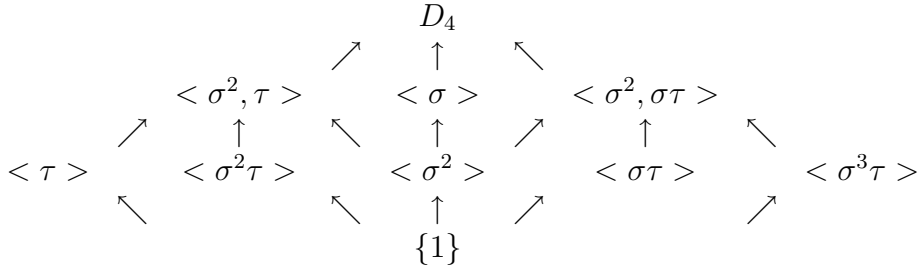
Los subgrupos de $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5},\omega)/\mathbb{Q})$*, ordenados por la relación inclusión, forman el reticulado*



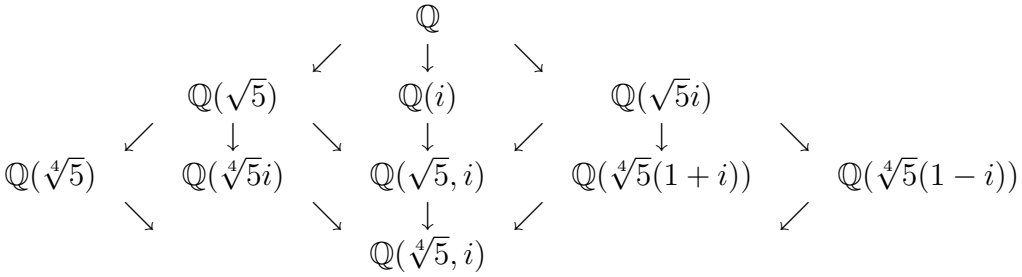
que corresponde al reticulado de cuerpos intermedios



3) Si $f(x)=x^4-5\in\mathbb{Q}[x]$*,* $\mathbb{Q}(i,\sqrt[4]{5})$ *es el cuerpo de raíces y su grupo de Galois* $\mathrm{Gal}(\mathbb{Q}(i,\sqrt[4]{5})/\mathbb{Q})$ *es el grupo dihedral de orden* 8*, generado por los automorfismos* $\sigma,\tau:\mathbb{Q}(i,\sqrt[4]{5})\to\mathbb{Q}(i,\sqrt[4]{5})$*,* $\sigma(a+bi+c\sqrt[4]{5})=a+bi+c\sqrt[4]{5}i$*,* $\tau(a+bi+c\sqrt[4]{5})=a-bi+c\sqrt[4]{5}$*, con* $\sigma^4=1=\tau^2$ *y* $\sigma\tau=\tau\sigma^3$*. Los subgrupos de* $\mathrm{Gal}(\mathbb{Q}(i,\sqrt[4]{5})/\mathbb{Q})$*, ordenados por la relación inclusión, forman el reticulado*



que corresponde al reticulado de cuerpos intermedios



7 Polinomios irreducibles: un criterio para determinarlos.

Si F es el cuerpo de raíces de un polinomio $f(x) \in K[x]$, su grupo de Galois $\mathrm{Gal}(F/K)$ nos permite decidir si el polinomio dado es irreducible o no.

TEOREMA 7.1. *Sea $f(x) \in K[x]$ un polinomio no constante sin raíces múltiples, F su cuerpo de raíces y $\mathrm{Gal}(F/K)$ su grupo de Galois. Entonces $f(x)$ es irreducible si y sólo si para todo par de raíces $\alpha, \beta \in F$ de $f(x)$, existe $\phi \in \mathrm{Gal}(F/K)$ tal que $\phi(\alpha) = \beta$.*

Demostración. Supongamos que $f(x)$ es un polinomio irreducible y sin raíces múltiples, F el cuerpo de raíces de $f(x)$, $\alpha, \beta \in F$ dos raíces de $f(x)$. Como $f(x)$ es irreducible, la Proposición 4.2 nos dice que $K(\alpha) \simeq K[x]/(f(x))$ y $K(\beta) \simeq K[x]/(f(x))$. Entonces existe un K-isomorfismo $\varphi : K(\alpha) \to K(\beta)$ tal que $\varphi(\alpha) = \beta$. Por el Teorema 4.5, φ que se puede extender a un K-automorfismo ϕ de F, esto es, $\phi \in \mathrm{Gal}(F/K)$.
Recíprocamente, sea $g(x)$ un factor irreducible de $f(x)$. Sea α una raíz de $g(x)$ y β una raíz cualquiera de $f(x)$. Por hipótesis, existe $\phi \in \mathrm{Gal}(F/K)$ tal que $\phi(\alpha) = \beta$. Como $g(x)$ tiene coeficientes en K, tenemos que

$$g(\beta) = g(\phi(\alpha)) = \phi(g(\alpha)) = \phi(0) = 0,$$

esto es, toda raíz de $f(x)$ es raíz de $g(x)$. Luego $f = g$ y f es irreducible. □

8 Grupos resolubles.

Recordemos que un grupo G se dice **resoluble** si existe una cadena de subgrupos

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = 1$$

tal que, para todo $i = 1, 2, \ldots, s$, G_i es un subgrupo normal de G_{i-1} y G_{i-1}/G_i es abeliano.

EJEMPLO 8.1.

(i) Todo grupo abeliano es resoluble.

(ii) Todo subgrupo de un grupo resoluble es resoluble (se demuestra usando que si G_i es normal en G_{i-1} entonces $G_i \cap H$ es normal en $G_{i-1} \cap H$, y que

$$(G_{i-1} \cap H)/(G_i \cap H) \simeq (G_{i-1} \cap H)/(G_i \cap G_{i-1} \cap H) \simeq G_i.(G_{i-1} \cap H)/G_i$$

y este último es un subgrupo de G_{i-1}/G_i que es abeliano).

(iii) Todo cociente de un grupo resoluble es resoluble. Sea G resoluble,

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = 1$$

una cadena con cocientes abelianos. Si $G' = G/H$, tomemos $\Phi : G \to G/H$ el epimorfismo canónico, y sean $G'_i = \Phi(G_i)$. Como Φ induce epimorfismos canónicos $G_{i-1}/G_i \to G'_{i-1}/G'_i$, los cocientes de la cadena $G' = G'_0 \supset G'_1 \supset \cdots \supset G'_s = 1$ son abelianos.

(iv) El grupo dihedral D_n es resoluble pues $D_n \supset (a) \supset 1$ es una cadena que cumple las condiciones de la definición, siendo a un elemento de orden n.

(v) Los grupos simétricos S_2, S_3, S_4 son resolubles. En efecto, S_2 es abeliano y las cadenas $S_3 \supset A_3 \supset 1$ y $S_4 \supset A_4 \supset K \supset 1$ son cadenas que verifican las condiciones de la definición de grupo resoluble, siendo K el grupo de Klein.

Veremos que el grupo S_n no es resoluble si $n > 4$.

LEMA 8.2. *Sea G un subgrupo de S_n, $n > 4$, que contiene a todos los 3-ciclos, y sea H un subgrupo normal de G tal que G/H es abeliano. Entonces H también contiene a todos los 3-ciclos.*

Demostración. Sea $\phi : G \to G/H$ el epimorfismo canónico, y sean $x = (ijk)$, $y = (krs)$ dos elementos en G tales que i, j, k, r, s son distintos dos a dos. Como G/H es abeliano, $\phi(x^{-1}y^{-1}xy) = 1$, y por lo tanto, $x^{-1}y^{-1}xy \in H$. Pero $x^{-1}y^{-1}xy = (kji)(srk)(ijk)(krs) = (kjs)$. □

TEOREMA 8.3. *El grupo S_n no es resoluble si $n > 4$.*

Demostración. Si existiera una cadena de subgrupos en las condiciones de la definición de resolubilidad, como S_n contiene a todos los 3-ciclos, lo mismo sucede con todos los subgrupos de la cadena. Luego esta no puede terminar en el grupo trivial. □

9 Criterio de resolubilidad por radicales.

El teorema fundamental de la teoría de Galois establece una correspondencia entre cuerpos y sus grupos de Galois. Esta relación se puede aplicar al problema de resolver ecuaciones algebraicas por radicales. Una ecuación $f(x) = 0$, con $f(x) \in K[x]$, se dice resoluble por radicales si sus soluciones se pueden expresar mediante una fórmula que involucre un número finito de operaciones $+, ., \sqrt[m]{}$ aplicadas a elementos del cuerpo K. Es claro que la extracción de raíces n-ésimas es la única operación que nos lleva a trabajar con extensiones del cuerpo K, y que nuestro problema se puede plantear en términos de extensiones sucesivas obtenidas por adjunciones de raíces de polinomios $x^n - a$ para elementos a convenientes.

Una extensión F de un cuerpo K se dice una **extensión por radicales** si existen cuerpos intermedios

$$F = F_r \supset F_{r-1} \supset \cdots \supset F_0 = K$$

tales que $F_i = F_{i-1}[u_i]$, con u_i una raíz del polinomio $x^{n_i} - a_i \in F_{i-1}[x]$. Esto es, $F = F(u_1, \ldots, u_r)$ y $u_i^{n_i} \in F(u_1, \ldots, u_{i-1})$.

Un polinomio $f(x) \in K[x]$ se dice **resoluble por radicales** si su cuerpo de raíces está contenido en una extensión por radicales de K.

Vimos en la introducción que todo polinomio de grado menor o igual que 4 es resoluble por radicales. Pero esto no es cierto si el cuerpo no es de característica cero. Por ejemplo, el polinomio $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ no es resoluble por radicales. En efecto, $f(x)$ no tiene raíces en $\mathbb{F}_2[x]$, y por lo tanto, $f(x)$ es irreducible en $\mathbb{F}_2[x]$. Sea $E = \mathbb{F}_2(\alpha) \simeq \mathbb{F}_2[x]/(f(x))$ el cuerpo de raíces de $f(x)$ sobre $\mathbb{F}_2$. Como $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$, el grupo $\mathrm{Gal}(\mathbb{F}_2(\alpha)/\mathbb{F}_2)$ es cíclico de orden 2. Por lo tanto, si $f(x)$ fuera resoluble por radicales, existiría una extensión $\mathbb{F}_2(\sqrt{m})$ con $m \in \mathbb{F}_2$ tal que $\alpha \in \mathbb{F}_2(\sqrt{m})$. Esto significa que existen $a, b \in \mathbb{F}_2$ tales que $\alpha = a + b\sqrt{m}$. Pero no existen $a, b, m \in \mathbb{F}_2$ tales que $a + b\sqrt{m}$ sea raíz de $f(x)$.

Recordemos que si K es un cuerpo de característica cero, ningún polinomio irreducible en $K[x]$ tiene raíces múltiples.

PROPOSICION 9.1. *Si K es un cuerpo de característica cero y F es el cuerpo de raíces de $x^n - 1$ sobre K, entonces* $\mathrm{Gal}(F/K)$ *es abeliano.*

Demostración. El polinomio $x^n - 1$ es coprimo con su derivado, luego tiene n raíces simples en F. Si A es el conjunto de las raíces, A tiene estructura de grupo con el producto de F. Entonces A es un grupo abeliano finito de orden n, y por lo tanto se descompone en producto directo de subgrupos cíclicos, $A = \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{m_s}\mathbb{Z}$.

Si r es el mínimo de los múltiplos comunes de $p_1^{m_1}, \ldots, p_s^{m_s}$, entonces r divide a n y todo elemento de A satisface la ecuación $x^r = 1$. Pero el polinomio $x^r - 1$ tiene a lo sumo r raíces en F, entonces $r \geq n$. Luego $r = n$ y A es cíclico. Sea ϵ un generador de A y sea $U(\mathbb{Z}/n\mathbb{Z})$ el grupo de las unidades de $\mathbb{Z}/n\mathbb{Z}$. Si $\sigma \in \mathrm{Gal}(F/K)$, entonces $\sigma(\epsilon) = \epsilon^{m_\sigma}$, para algún $m_\sigma \in \mathbb{Z}$, $1 \leq m_\sigma < n$. La aplicación $\Gamma : \mathrm{Gal}(F/K) \to U(\mathbb{Z}/n\mathbb{Z})$ definida por $\Gamma(\sigma) = \overline{m_\sigma}$ es un monomorfismo de grupos. Luego $\mathrm{Gal}(F/K)$ es un grupo abeliano. □

Observemos que la demostración anterior prueba la existencia de raíces primitivas.

PROPOSICION 9.2. *Si K es un cuerpo de característica cero que contiene todas las raíces n-ésimas de la unidad y a es un elemento de K, entonces el grupo de Galois del polinomio $x^n - a$ sobre K es un grupo cíclico cuyo orden es un divisor de n.*

Demostración. Sea F un cuerpo de raíces de $x^n - a$ y sea $\alpha \in F$ con $\alpha^n = a$. Si $A = \{1, \epsilon, \ldots, \epsilon^{n-1}\}$ es el conjunto de raíces del polinomio $x^n - 1$, entonces $\alpha, \alpha\epsilon, \ldots, \alpha\epsilon^{n-1}$ son todas las raíces de $x^n - a$ en F. Entonces $F = K(\alpha)$. Si $\sigma \in \mathrm{Gal}(F/K)$, entonces $\sigma(\alpha) = \alpha\epsilon^{m_\sigma}$, para algún $m_\sigma \in \mathbb{Z}$, $0 \leq m_\sigma < n$. La aplicación $\Gamma : \mathrm{Gal}(F/K) \to A$ definida por $\Gamma(\sigma) = \epsilon^{m_\sigma}$ es un monomorfismo de grupos. Luego $\mathrm{Gal}(F/K)$ es un grupo cíclico cuyo orden es un divisor de n. □

PROPOSICION 9.3. *Si K es un cuerpo de característica cero que contiene todas las raíces p-ésimas de la unidad, p primo, y F es una extensión de K tal que $[F : K] = |\mathrm{Gal}(F/K)| = p$, entonces $F = K(u)$ para algún $u \in F$ tal que $u^p \in K$.*

Demostración. Sea F una extensión de K tal que $[F : K] = |\mathrm{Gal}(F/K)| = p$. Como p es primo, $\mathrm{Gal}(F/K)$ es cíclico. Sea σ un generador de $\mathrm{Gal}(F/K)$ y sean $1, \epsilon, \ldots, \epsilon^{p-1}$ las raíces p-ésimas de la unidad. Miremos a σ como K-transformación lineal de F en F. Por el Lema 5.3 sabemos que el polinomio minimal de σ no puede tener grado menor que p. Como $\sigma^p = id$, el polinomio minimal de la transformación lineal σ es $x^p - 1$. Entonces ϵ es un autovalor, y por lo tanto existe un autovector $u \in F$ tal que $\sigma(u) = \epsilon u$, $u \notin K$. Como $K \subset K(u) \subset F$, si $s = [K(u) : K]$, entonces $s > 1$ y s divide a $[F : K] = p$. Luego $[K(u) : K] = p$ y $K(u) = F$. Sea $h(x) \in K[x]$ el polinomio irreducible mónico de grado p que tiene a u como raíz. Como $\sigma^i(u) = \epsilon^i u$ y $h(\sigma^i(u)) = \sigma^i(h(u)) = 0$, tenemos que $K(u)$ es el cuerpo de raíces del polinomio $h(x)$. Además $\sigma^i(u^p) = \sigma^i(u)^p = u^p$, para todo $i = 0, \ldots, p-1$. Entonces $u^p \in K(u)^{\mathrm{Gal}(K(u)/K)} = K$. □

TEOREMA 9.4. *Si K es un cuerpo de característica cero, un polinomio $f(x) \in K[x]$ es resoluble por radicales si y sólo si su grupo de Galois es resoluble.*

Demostraremos este teorema usando el Teorema Fundamental de la teoría de Galois que establece una correspondencia entre subgrupos y cuerpos intermedios. Observemos que, como K es un cuerpo de característica cero, todo polinomio irreducible tiene sólo raíces simples, y por lo tanto, todo polinomio no constante en $K[x]$ es separable.

Nuestro objetivo es demostrar que el cuerpo de raíces F de $f(x)$ está contenido en una extensión radical F_s de K si y sólo si el grupo de Galois $\mathrm{Gal}(F/K)$ es resoluble. Hay que tener en cuenta que la definición de resoluble involucra subgrupos normales, y estos, por el Teorema Fundamental, se corresponden con extensiones normales. Ahora bien, las extensiones radicales no necesariamente son normales, y recíprocamente, no toda extensión normal es radical. Necesitamos entonces los siguientes lemas.

LEMA 9.5. *Sea F una extensión finita de un cuerpo K de característica cero. Las siguientes condiciones son equivalentes:*

(i) *F es una extensión normal de K;*

(ii) *F es el cuerpo de raíces de un polinomio separable en $K[x]$;*

(iii) *El cuerpo fijo de $\mathrm{Gal}(F/K)$ es K.*

Demostración.

$(i) \Rightarrow (ii)$ Sea $\{a_1, \ldots, a_n\}$ una base de F sobre K, y sea $f_i(x) \in K[x]$ el polinomio irreducible que tiene a a_i como raíz. Sea $f(x) = f_1(x)f_2(x)\cdots f_n(x)$. Como F es una extensión normal de K, F contiene a todas las raíces del polinomio $f(x)$. Pero $F = K(a_1, \ldots, a_n)$, luego F es el cuerpo de raíces de $f(x)$. Como K es un cuerpo de característica cero, $f(x)$ es separable.

$(ii) \Rightarrow (iii)$ Es inmediato por el Lema 6.2.

$(iii) \Rightarrow (i)$ Sea $g(x) \in K[x]$ irreducible, mónico, $u \in F$ una raíz de $g(x)$. Veamos que todas las raíces de $g(x)$ están en F. Sean $u, \sigma_2(u), \ldots, \sigma_r(u)$ todos los elementos distintos del conjunto $\{\sigma(u) : \sigma \in \mathrm{Gal}(F/K)\}$. Entonces

$$h(x) = (x-u)(x-\sigma_1(u))\cdots(x-\sigma_r(u)) \in F^{\mathrm{Gal}(F/K)}[x] = K[x].$$

Además, $g(\sigma_j(u)) = \sigma_j(g(u)) = 0$, y por lo tanto $h(x)$ divide a $g(x)$. Pero $g(x)$ es irreducible mónico, luego $g(x) = h(x)$ y $g(x)$ tiene todas su raíces en F. $\square$

LEMA 9.6. *Sea K un cuerpo de característica cero. Si $K \subset F \subset F(\alpha)$ con F una extensión normal de K y $\alpha^m \in F$, existe un cuerpo E tal que*

(a) E es una extensión normal de $F(\alpha)$;

(b) E es una extensión normal de K;

(c) E es una extensión radical de F;

(d) $\mathrm{Gal}(E/F)$ es resoluble;

(e) Si $\mathrm{Gal}(F/K)$ es resoluble, entonces $\mathrm{Gal}(E/K)$ es resoluble.

Demostración. Por hipótesis existe $a \in F$ tal que $\alpha^m = a$. Sean $a_1 = a, a_2, \ldots, a_k$ todos los elementos distintos del conjunto $\{\sigma(a) : \sigma \in \mathrm{Gal}(F/K)\}$. Sea ϵ una raíz primitiva de la unidad de orden m y sea α_i tal que $\alpha_i^m = a_i$. Sea $E = F(\epsilon, \alpha, \alpha_2, \ldots, \alpha_k)$. Tenemos entonces una cadena

$$F \subset F(\epsilon) \subset F(\epsilon, \alpha) \subset F(\epsilon, \alpha, \alpha_2) \subset \cdots \subset F(\epsilon, \alpha, \ldots, \alpha_{k-1}) \subset E \qquad (*)$$

tal que cada extensión se obtiene a partir de la anterior adjuntando todas las raíces de un polinomio separable: $x^m - 1,\ x^m - a,\ x^m - a_2,\ \ldots, x^m - a_k$ respectivamente. Para probar (b) basta observar que E es el cuerpo de raíces del polinomio separable $p(x) = (x^m - a)(x^m - a_2)\cdots(x^m - a_k)$ cuyos coeficientes están en el cuerpo fijo de $\mathrm{Gal}(F/K)$ que es K. Las condiciones (a) y (c) son inmediatas. Aplicando el Teorema Fundamental 6.3 a la cadena de extensiones (*) y usando las Proposiciones 9.1 y 9.2, se tiene (d). Además si $\mathrm{Gal}(F/K)$ es resoluble, entonces $\mathrm{Gal}(E/K)$ también lo es. □

LEMA 9.7. *Si F es una extensión radical de un cuerpo K de característica cero, existe una extensión E de F tal que E es una extensión normal radical de K y $\mathrm{Gal}(E/K)$ es resoluble.*

Demostración. Sea $F = K(\alpha_1, \ldots, \alpha_k)$ con $\alpha_i^{m_i} \in K$. Por el lema anterior, dada $K \subset K(\alpha_1)$ existe E_1 una extensión de $K(\alpha_1)$ que es una extensión radical normal de K y tal que $\mathrm{Gal}(E_1/K)$ es resoluble. Apliquemos ahora el lema anterior a la cadena $K \subset E_1 \subset E_1(\alpha_2)$. Obtenemos una extensión E_2 de $E_1(\alpha_2)$ que es una extensión radical normal de K cuyo grupo de Galois $\mathrm{Gal}(E_2/K)$ es resoluble. Si continuamos con este proceso, obtenemos una extensión radical normal E_k de K que contiene a F y cuyo grupo de Galois sobre K es resoluble. □

Demostración. Del Teorema 9.4.

Supongamos que $f(x)$ es resoluble por radicales, y sea F el cuerpo de raíces de $f(x)$. Por el Lema 9.7 sabemos que existe una extensión normal radical E de K que contiene a F y tal que $\mathrm{Gal}(E/K)$ es resoluble. Como F es una extensión normal de K, el Teorema Fundamental 6.3 nos dice que $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F)$. Por lo tanto $\mathrm{Gal}(F/K)$ es resoluble.

Recíprocamente supongamos que el grupo de Galois de $f(x)$ es resoluble. Sea $n = \mathrm{gr}\, f(x)$, y sea K' una extensión del cuerpo K que contiene a todas las raíces $n!$-ésimas de la unidad. Sea F' un cuerpo de raíces de $f(x)$ sobre K'. Si $a_1, \ldots, a_m$ son las raíces de $f(x)$ en F', $F = K(a_1, \ldots, a_m)$ es el cuerpo de raíces de $f(x)$ sobre K, $F \subset F'$. Si $\sigma \in \mathrm{Gal}(F'/K')$, σ permuta las raíces $a_1, \ldots, a_m$, entonces $\sigma/_F : F \to F$ es un automorfismo que deja fijo al cuerpo K. Más aún, la aplicación $\Phi : \mathrm{Gal}(F'/K') \to \mathrm{Gal}(F/K)$ definida por $\Phi(\sigma) = \sigma/_F$ es un monomorfismo de grupos. Entonces $G' = \mathrm{Gal}(F'/K')$ es resoluble. Sea

$$G' = G'_0 \supset G'_1 \supset \cdots \supset G'_s = 1$$

una cadena con cocientes abelianos. Más aún, toda cadena se puede refinar, y por lo tanto, sin pérdida de generalidad, podemos suponer que los cocientes son cíclicos de orden primo. Si $F'_i = F'^{G'_i}$, por el Teorema Fundamental 6.3 existe una cadena de extensiones

$$K' = F'_0 \subset F'_1 \subset \cdots \subset F'_s = F'$$

tales que F'_i es una extensión normal de F'_{i-1} y $\mathrm{Gal}(F'_i/F'_{i-1})$ es cíclico de orden p. Además, como F'_{i-1} contiene todas las raíces p-ésimas de la unidad para p cualquier divisor de $n!$, la Proposición 9.3 nos dice que $F'_i = F'_{i-1}[u_i]$ con $u_i^p \in F'_{i-1}$. Por lo tanto $f(x)$ es resoluble por radicales. □

TEOREMA 9.8. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio irreducible de grado primo p. Si $f(x)$ tiene exactamente dos raíces no reales en el cuerpo $\mathbb{C}$ de los números complejos, entonces su grupo de Galois es S_p.*

Demostración. Como $f(x)$ es un polinomio irreducible en $\mathbb{Q}[x]$, no tiene raíces múltiples, y por hipótesis, tiene $p-2$ raíces reales y 2 raíces complejas, que son conjugadas. Sea F el cuerpo de raíces de $f(x)$, y sea $\mathrm{Gal}(F/\mathbb{Q})$ su grupo de Galois. La conjugación define un automorfismo de $\mathbb{C}$, que restringido a F nos da un elemento de $\mathrm{Gal}(F/\mathbb{Q})$ que deja fijas todas las raíces reales. Por lo tanto $\mathrm{Gal}(F/\mathbb{Q})$ contiene una trasposición.
Por otro lado, sea $u \in F$ una raíz de $f(x)$. Como $f(x)$ es irreducible, la Proposición 4.2 nos dice que $\mathbb{Q}(u) \simeq \mathbb{Q}[x]/(f(x))$ y que $[\mathbb{Q}(u) : \mathbb{Q}] = \mathrm{gr}\, f(x)$. Pero $\mathbb{Q} \subset \mathbb{Q}(u) \subset F$ implica que p divide a $[F : \mathbb{Q}]$, es decir, al orden de $\mathrm{Gal}(F/\mathbb{Q})$. Entonces $\mathrm{Gal}(F/\mathbb{Q})$

es un subgrupo de S_p que contiene una trasposición y un elemento de orden p. Luego $\mathrm{Gal}(F/\mathbb{Q}) = S_p$. □

TEOREMA 9.9. *Existen polinomios de grado* 5 *con coeficientes racionales que no son resolubles por radicales.*

Demostración. Vimos que S_n no es un grupo resoluble si $n \geq 5$. Por el teorema anterior, si $f(x)$ es un polinomio irreducible en $\mathbb{Q}[x]$ de grado 5 que tiene exactamente dos raíces no reales en el cuerpo $\mathbb{C}$, su grupo de Galois sobre $\mathbb{Q}$ es S_5. Por lo tanto, el polinomio dado no será resoluble por radicales. □

EJEMPLO 9.10. *Sea p primo, $p \geq 5$, y sea*

$$f(x) = (x^2 + 2)(x - 2)(x - 4) \cdots (x - 2(p - 2)) - 2 \in \mathbb{Q}[x].$$

Por el criterio de Eisenstein, $f(x)$ es irreducible: $4 \mid a_i$ para todo $i = 1, \ldots, p - 1$, $2 \mid a_0$ y $4 \nmid a_0$. Además, $f(x)$ tiene exactamente dos raíces no reales, luego $f(x)$ no es resoluble por radicales.

El Teorema 9.4 no es válido si quitamos la hipótesis sobre la característica del cuerpo K. Pero si modificamos la definición de resoluble por radicales admitiendo extensiones que se obtienen adjuntando raíces de polinomios de la forma $x^p - x - a$, y nos restringimos a resolver polinomios separables, el teorema es válido en característica p.

10 Construcciones con regla y compás.

Muchos problemas de la geometría plana pueden resolverse con construcciones que sólo utilizan regla y compás. Por ejemplo se pueden construir polígonos regulares de 3, 4, 5, 6, 8, 10 lados, pero no se puede construir un polígono regular de 7, 9, 11 lados. La teoría de Galois nos permite decidir cuándo es posible realizar una construcción con regla y compás.

Fijado un conjunto de puntos M, las construcciones básicas permitidas son:

- Dados dos puntos en M, trazar (con la regla) la recta que pasa por ellos.
- Dado un punto P y un segmento AB, con $A, B, P \in M$, trazar (con el compás) la circunferencia de centro P y radio AB.

Un punto P se dice **construible** con regla y compás a partir de un conjunto M si existe una sucesión de puntos $P_0, P_1, \ldots, P_m = P$ tales que P_i se obtiene a partir del conjunto $M \cup \{P_0, P_1, \ldots, P_{i-1}\}$ como intersección de dos rectas, como intersección de una recta y una circunferencia, o como intersección de dos circunferencias.

Por ejemplo, con regla y compás se puede:

- Dada un recta L y un punto $P \notin L$, hallar una recta perpendicular a L que pase por P.
- Dado un segmento hallar su punto medio.
- Dibujar ángulos de 45^o y de 60^o.
- Dados dos segmento de longitud a y b, con $a > b > 0$, dibujar segmentos de longitud $a + b$, $a - b$, ab, $\frac{a}{b}$.
- Dado un segmento de longitud a hallar un segmento de longitud $\sqrt{a}$.

El problema de hallar intersecciones entre dos rectas, entre una recta y una circunferencia o entre dos circunferencias se reduce al problema de resolver ecuaciones de primer o segundo grado. Por lo tanto cualquier construcción con regla y compás de un punto P a partir de un conjunto M es equivalente a la construcción sucesiva de extensiones de cuerpos de grado 2, es decir, si K es un subcuerpo de $\mathbb{R}$ generado por las coordenadas de los puntos en M, las coordenadas del punto P pertenecen a un cuerpo F para el cual existe una sucesión de extensiones

$$K \subset F_1 \subset F_2 \subset \cdots \subset F_m = F$$

con $[F_i : F_{i-1}] = 2$. Por lo tanto, $[F : K] = 2^m$.

Para decidir si un problema geométrico se puede resolver mediante construcciones con regla y compás, hay que encontrar una ecuación algebraica equivalente al problema dado, determinar el factor irreducible que corresponde a la solución del problema, y determinar si esa ecuación irreducible se puede resolver utilizando raíces cuadradas. La teoría de Galois nos dice que si esto sucede, el orden del grupo de Galois correspondiente es una potencia de 2.

Gauss demostró que un polígono regular con un número primo p de lados se puede construir con regla y compás si $p = 2^{2^n} + 1$; la teoría de Galois nos dice que esta condición también es suficiente.

Este método nos permite demostrar que no es posible, con regla y compás, dividir un ángulo arbitrario en tres partes iguales, duplicar un cubo o construir un cuadrado de igual área que la de un círculo de radio dado.

- Si queremos dividir un ángulo α en tres ángulos iguales, necesitamos conocer $\cos\frac{\alpha}{3}$. Usando la fórmula trigonométrica

$$\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}$$

tenemos que $\cos\frac{\alpha}{3}$ es raíz del polinomio $4x^3 - 3x - \cos\alpha$. Así resulta que α es trisecable con regla y compás si y sólo si el polinomio $4x^3 - 3x - \cos\alpha$ es reducible en el cuerpo $\mathbb{Q}(\cos\alpha)$.

- Para dibujar un cubo cuyo volumen sea el doble del de uno dado necesitamos hallar una raíz del polinomio $x^3 - 2$. Pero este polinomio es irreducible en $\mathbb{Q}[x]$, y por lo tanto $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

- Para construir un cuadrado de igual área que la de un círculo de radio r, se necesita considerar las raíces de la ecuación $x^2 - \pi = 0$. Si la construcción fuera posible con regla y compás, existiría una extensión F de $\mathbb{Q}$ de grado 2^s y tal que $\sqrt{\pi} \in F$. Pero esto es imposible porque π es trascendente sobre $\mathbb{Q}$.

En el próximo ejemplo veremos cómo construir, con regla y compás, un péntagono regular. Como las raíces quintas de la unidad son los vértices de un pentágono regular inscripto en una circunferencia de radio 1, bastará con dibujar sobre dicha circunferencia el arco correspondiente a una raíz primitiva de la unidad de orden 5. En el Ejemplo 2.1 vimos que $\omega = \frac{1}{4}(-1+\sqrt{5}) + i\frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$ es raíz del polinomio $p(x) = x^4 + x^3 + x^2 + x + 1$.

EJEMPLO 10.1. *Veamos cómo construir un pentágono regular. Fijemos una escala que determine una unidad de medida. Dibujemos un triángulo rectángulo cuyos lados midan* 1 *y* 2 *unidades respectivamente. Entonces la hipotenusa es un segmento que mide* $\sqrt{5}$ *unidades. Construimos ahora un segmento que mida* $\sqrt{5}-1$ *unidades, y tomamos la cuarta parte de este segmento. Así conseguimos un segmento* U *que mide* $\frac{1}{4}(\sqrt{5}-1)$*. Dibujemos una circunferencia de radio 1, y traslademos el segmento* U *de manera tal que uno de sus extremos coincida con el centro* O *de la circunferencia. Sea* $U = \overline{OP}$*. Tracemos una recta* L *perpendicular a* $\overline{OP}$ *que pase por* P*, y sea* Q *un punto de intersección de la circunferncia con la recta* L*. Si dibujamos el plano complejo con origen* O *y eje real la recta que contiene al segmento* $\overline{OP}$*, el punto* Q *corresponde al número complejo*

$$\frac{1}{4}(\sqrt{5}-1) + i\frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$$

que es una raíz primitiva de la unidad de orden 5*.*

11 Ejercicios.

1. Demostrar el criterio de irreducibilidad de Eisenstein.

2. Mostrar que $x^p - x - 1$ es irreducible sobre $\mathbb{Q}[x]$, cualquiera sea p primo.

3. Si R es un dominio de integridad que contiene a un cuerpo K, y $\dim_K R$ es finita, entonces R es un cuerpo. En particular, si F es una extensión del cuerpo K, S un conjunto de F, $K[S]$ el subanillo generado por K y por S y $\dim_K K[S]$ finita, entonces $K[S] = K(S)$.

4. Si F es una extensión de K y E es una extensión de F entonces E es una extensión de K y $[E : K] = [E : F][F : K]$.

5. Sea K un cuerpo, $K(u)$, $K(v)$ extensiones de K de grados m y n respectivamente. Si m y n son coprimos, entonces $[K(u, v) : K] = mn$.

6. Calcular $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ y hallar $u \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ tal que $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

7. Hallar un cuerpo de raíces de

   (a) $x^5 - 2$ sobre $\mathbb{Q}$;

   (b) $x^4 + 9$ sobre $\mathbb{Q}$;

   (c) $x^4 + 7$ sobre $\mathbb{Q}$;

   (d) $x^3 - 11$ sobre $\mathbb{Q}$;

   (e) $x^4 + x^2 + 1$ sobre $\mathbb{Q}$;

   (f) $x^p - 1$ sobre $\mathbb{Q}$, para p primo;

   (g) $(x^3 + x + 1)(x^2 + x + 1)$ sobre $\mathbb{F}_2$;

   (h) $x^6 + 6$ sobre $\mathbb{F}_7$;

   (i) $x^5 - 1$ sobre $\mathbb{F}_{11}$.

8. Sea F una extensión de K de grado 2. Mostrar que F es el cuerpo de raíces de algún polinomio en $K[x]$.

9. Sea $K(u)$ una extensión de K de grado impar. Mostrar que $K(u^2) = K(u)$.

10. Hallar un elemento $u \in \mathbb{Q}(\sqrt{2}, i)$ tal que $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, i)$.

11. Hallar el grupo de Galois del polinomio

    (a) $x^4 + 9$ sobre $\mathbb{Q}$;

(b) $x^4 + 6$ sobre $\mathbb{F}_7$;

(c) $x^3 - 2$ sobre $\mathbb{F}_5$, $\mathbb{F}_7$ y $\mathbb{F}_{11}$.

12. Sea F el cuerpo de raíces del polinomio $x^4+1 \in \mathbb{C}[x]$. Mostrar que $[F : \mathbb{C}] = 4$ y calcular $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{2}))$, $\mathrm{Gal}(F/\mathbb{Q}(i))$ y $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{2}i))$.

13. Sea F el cuerpo de raíces de un polinomio separable sobre K. Probar que si $\mathrm{Gal}(F/K)$ es cíclico, entonces para cada divisor d de $[F : K]$ existe una única extensión E de K contenida en F tal que $[E : K] = d$.

14. Hallar el orden del grupo de Galois del polinomio $x^5 - 3$ sobre $\mathbb{Q}$.

15. Sea F el cuerpo de raíces de un polinomio irreducible $f(x) \in \mathbb{Q}[x]$. Si $[F : \mathbb{Q}]$ es impar, mostrar que todas las raíces de $f(x)$ son reales.

16. Describir explícitamente la correspondencia entre subgrupos del grupo de Galois y subcuerpos del cuerpo de raíces para:

    (a) $x^4 + 9 \in \mathbb{Q}[x]$;

    (b) $(x^2 - 2)(x^2 + 1) \in \mathbb{Q}[x]$;

    (c) $x^3 + x + 1 \in \mathbb{F}_2[x]$;

    (d) $x^4 - 5 \in \mathbb{Q}(i)[x]$.

17. Mostrar que el polinomio $x^5 - 4x + 2 \in \mathbb{Q}[x]$ es irreducible, hallar su grupo de Galois y explicar por qué no es resoluble sobre $\mathbb{Q}$.

18. Mostrar cómo realizar con regla y compás las siguientes construcciones.

    (a) Dada un recta L y un punto $P \notin L$, hallar una recta perpendicular a L que pase por P.

    (b) Dado un segmento hallar su punto medio.

    (c) Dibujar ángulos de 45^o y de 60^o.

    (d) Dados dos segmento de longitud a y b, con $a > b$, dibujar segmentos de longitud $a + b$, $a - b$, ab, $\frac{a}{b}$.

    (e) Dado un segmento de longitud a hallar un segmento de longitud $\sqrt{a}$.

19. Sea $\varphi(n)$ el número de raíces primitivas de la unidad de orden n, es decir, el cardinal del conjunto $\{k \in \mathbb{N} : 1 \leq k < n \text{ y } (k, n) = 1\}$. Mostrar que un polígono regular de n-lados se puede construir con regla y compás si y sólo si $\varphi(n)$ es una potencia de 2. Los primos impares p tales que $\varphi(p)$ es una potencia de 2 son los llamados **primos de Fermat**.

20. Mostrar que es posible construir un polígono regular de 7 lados utilizando regla, compás y un trisector de ángulos.

Referencias.

[1] Mathematics. Its content, methods and meaning. Edited by A. D. Aleksandrov, A. N. Kolmogorov and M. A. Lavrentiev. Translated from the Russian by Tamas Bartha, Kurt Hirsch and S. H. Gould. Translation edited by Gould. Dover Publications, Inc., Mineola, NY, 1999.

[2] Artin, Emil. Galois theory. Edited and supplemented with a section on applications by Arthur N. Milgram. Second edition, with additions and revisions. Fifth reprinting. Notre Dame Mathematical Lectures, No. 2 University of Notre Dame Press, South Bend, Ind., 1959.

[3] Gaal, Lisl. Classical Galois theory with examples. Markham Publishing Co., Chicago, Ill. 1971.

[4] Gastaminza, María Luisa. Extensiones algebraicas, teoría de Galois. Departamento de Matemática, Universidad Nacional del Sur, 1991.

[5] Milne, James S. Fields and Galois Theory. http://www.jmilne.org/math/, 2003.