UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

EL TEOREMA DE ABEL-RUFFINI

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A :

RICARDO RAMÍREZ LUNA

DIRECTOR DE TESIS:
DR. EMILIO ESTEBAN LLUIS PUEBLA

CIUDAD UNIVERSITARIA, CD. MX. **2017**

1. Datos del alumno.
Ramírez
Luna
Ricardo
54893940
Universidad Nacional Autónoma de México.
Facultad de Ciencias.
Matemáticas.
310268444

2. Datos del tutor
Dr.
Emilio Esteban
Lluis
Puebla

3. Datos de sinodal 1
Dra.
Eugenia
O'Reilly
Regueiro

4. Datos sinodal 2
Dr.
Rodolfo
San Agustín
Chi

5. Datos sinodal 3
Dr.
Alejandro
Alvarado
García

6. Datos sinodal 4
Dr.
Juan
Morales
Rodríguez

7. Datos del trabajo escrito.
El Teorema de Abel-Ruffini.
101p
2017

The Title

The Author

The Date

Contenido

Introducción.

El Teorema de Abel-Ruffini postula; en general, los polinomios de grado mayor o igual que 5 no pueden ser solubles por radicales. El teorema fue demostrado por Paolo Ruffini, en 1799. Abel, en 1824, probó que los polinomios de grado 5 no son ser solubles por radicales en general y, posteriormente, Galois resolvió el problema general de saber si un polinomio es soluble por radicales. En el primer capítulo se deducen las fórmulas generales ya que el Teorema de Abel-Ruffini se planteó buscando una fórmula general por medio de radicales para calcular las raíces de polinomios de quinto grado. Con estas fórmulas nosotros demostraremos que los polinomios de grado menor que 5 son solubles por radicales.

En el primer capítulo de este trabajo, se deducirán las fórmulas generales para calcular las raíces de polinomios de grado menor o igual que 4. En la primera parte, se muestra que la ecuación de segundo grado

$$ax^2 + bx + c = 0$$

con $a, b, c \in \mathbb{C}$, tiene soluciones:

$$x_1 = \frac{-b + \sqrt[2]{b^2 - 4ac}}{2a} \text{ y } x_2 = \frac{-b - \sqrt[2]{b^2 - 4ac}}{2a}$$

En la segunda parte del primer capítulo, se muestra que la ecuación

$$x^3 + ax^2 + bx + c = 0$$

con $a, b, c \in \mathbb{C}$, tiene soluciones

$$\begin{aligned} x_1 &= y + z - d \\ x_2 &= z\omega + y\omega^2 - d \\ x_3 &= z\omega^2 + y\omega - d \end{aligned}$$

con

$$\begin{aligned} y &= -\frac{1}{3}\frac{\alpha}{z} \\ z &= \sqrt[3]{\frac{-\beta}{2} \pm \sqrt[2]{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}} \end{aligned}$$

$$\begin{aligned} \omega &= e^{\frac{2\pi i}{3}} \\ d &= \frac{a}{3}. \end{aligned}$$

En la última parte del capítulo uno, se considera la ecuación

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

y se muestra que las raíces de los polinomios

$$\begin{aligned} x^2 + \frac{1}{2}bx + \frac{1}{2}\eta &= Ax + B \\ x^2 + \frac{1}{2}bx + \frac{1}{2}\eta &= -Ax - B. \end{aligned}$$

son las soluciones de $x^4 + ax^3 + bx^2 + cx + d = 0$.

Con η raíz de

$$y^3 - by^2 + (ac - 4d)y - b^2d + 4bd - c^2 = 0.$$

$$\begin{aligned} A^2 &= \frac{1}{4}a^2 - b + \eta \\ B^2 &= -d + \frac{1}{4}\eta^2 \end{aligned}$$

En el segundo capítulo de este trabajo, se hará una demostración del Teorema Fundamental de la Teoría de Galois. Este teorema establece una biyección entre los subgrupos de $Gal\,(K \rightarrowtail L)$ y los campos entre K y L si la extensión $K \rightarrowtail L$ es de Galois.

Nosotros ocuparemos la notación de [1] para extensiones de campos. Esto es, una extensión de campos la denotaremos $K \rightarrowtail L$.

En el capítulo 3, daremos una introducción de grupos solubles cuya finalidad, es probar que el grupo de permutaciones con 5 letras o más no

es soluble. En la segunda parte, mostraremos que si la extensión $K \rightarrowtail L$ es ciclotómica entonces, $Gal\,(K \rightarrowtail L)$ es un subgrupo de $\mathbb{Z}_n$. En la parte 3, demostraremos que si la extensión $K \rightarrowtail L$ es radical entonces el grupo $Gal\,(K \rightarrowtail L)$ es soluble. En la parte 4 del capítulo, construiremos una extensión radical por cada fórmula general, y para finalizar el capítulo haremos una demostración del Teorema de Abel-Ruffini.

En el apéndice se hará un panorama general de un artículo que presentará una demostración del Teorema de Abel-Ruffini con otras técnicas.

En este trabajo se supone un curso de Teoría de Campos, Teoría de Anillos, Teoría de Grupos y Álgebra lineal.

Por último, todas las observaciones de este trabajo han sido probadas por el autor de esta tesis.

Capítulo 1

Deducción de fórmulas generales.

Aunque en la demostración del Teorema de Abel-Ruffini, no son necesarias las fórmulas generales. Se incluyen, ya que dada la fórmula general para encontrar las raíces de polinomios de grado $2, 3$ y 4 por radicales podemos encontrar una extensión radical y así, los polinomios de grado $2, 3$ y 4 en general, son solubles por radicales. Esto es importante porque el Teorema de Abel-Ruffini surge de la pregunta: ¿Existe fórmula general para encontrar las raíces de polinomios de grado 5 por radicales?

La respuesta es negativa, la demostración es el propósito de esta tesis.

1.1 Polinomios de segundo grado.

Consideremos la ecuación de segundo grado

$$ax^2 + bx + c = 0$$

con $a, b, c \in \mathbb{C}$ con $a \neq 0$. Sumando el inverso aditivo de c, nos queda

$$ax^2 + bx = -c.$$

Luego, podemos completar el binomio cuadrado perfecto

$$(\sqrt[2]{a}x + \frac{b}{2\sqrt{a}})^2 = \frac{b^2}{4a} - c.$$

Sacando raíz cuadrada

$$\sqrt{(\sqrt{a}x + \frac{b}{2\sqrt{a}})^2} = \sqrt{\frac{b^2}{4a} - c}$$

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

Haciendo la suma de fracciones y separando la raíz en el cociente

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

Despejando x

$$\sqrt{a}x = -\frac{b}{2\sqrt{a}} \pm \frac{\sqrt{b^2 - 4ac}}{2\sqrt[2]{a}}$$

$$\begin{aligned} x &= (-\frac{b}{2\sqrt{a}} \pm \frac{\sqrt{b^2 - 4ac}}{2\sqrt{a}})\frac{1}{\sqrt{a}} \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

y así, obtenemos la fórmula general para calcular las raíces de cualquier polinomio de segundo grado. Estas son:

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ y } x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

Lo abreviaremos de la siguiente forma:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Ejemplo 1. Consideremos $x^2 - 4x + 3$.

Resolviendo la igualdad $x^2 - 4x + 3 = ax^2 + bx + c$, obtendremos los valores de a, b, c. Así

$$\begin{aligned} a &= 1 \\ b &= -4 \\ c &= 3 \end{aligned}$$

luego, sustituyendo en $x_{1,2} = \frac{-b \pm \sqrt[2]{b^2-4ac}}{2a}$, nos queda:

$$\begin{aligned} x_{1,2} &= \frac{4 \pm \sqrt[2]{16-4(1)(3)}}{2} \\ x_1 &= 1 \\ x_2 &= 3. \end{aligned}$$

Ejemplo 2. Consideremos $x^2 + 1$. Igualando $x^2 + 1 = ax^2 + bx + c$, obtenemos las valores de a, b, c. Estos son:

$$\begin{aligned} a &= 1 \\ b &= 0 \\ c &= 1. \end{aligned}$$

Luego, sustituyendo en la fórmula

$$\begin{aligned} x_{1,2} &= \frac{\pm\sqrt[2]{-4}}{2} \\ &= \pm\frac{2i}{2}. \end{aligned}$$

Entonces, las raíces son:

$$\begin{aligned} x_1 &= i \\ x_2 &= -i. \end{aligned}$$

1.2 Polinomios de tercer grado.

Notamos que cualquier polinomio de tercer grado

$$ax^3 + bx^2 + cx + d,$$

con $a, b, c, d \in \mathbb{C}$. Se tiene que $a \neq 0$ ya que el polinomio $ax^3 + bx^2 + cx + d$ es de tercer grado. Sustituyendo:

$$\alpha = \frac{b}{a}, \beta = \frac{c}{a}, \delta = \frac{d}{a}.$$

el polinomio $ax^3 + bx^2 + cx + d$ se reescribe $x^3 + \alpha x^2 + \beta x + \delta$.

Resolvamos la siguiente ecuación

$$x^3 + ax^2 + bx + d = 0.$$

Tomemos $d \in \mathbb{C}$, tal que sea raíz del polinomio $a - 3x$, y construyamos el polinomio

$$(x-d)^3 + a(x-d)^2 + b(x-d) + c.$$

Luego, si ξ es una raíz de $(x-d)^3 + a(x-d)^2 + b(x-d) + c$, obtenemos

$$(\xi - d)^3 + a\,(\xi - d)^2 + b\,(\xi - d) + c = 0.$$

entonces $\xi - d$ es raíz de $x^3 + ax^2 + bx + c$. Así, basta encontrar las raíces de $(x-d)^3 + a(x-d)^2 + b(x-d) + c$ para obtener las de $x^3 + ax^2 + bx + d$.

Calculemos las raíces de $(x-d)^3 + a(x-d)^2 + b(x-d) + c$.

Desarrollando y agrupando, se tiene

$$x^3 + (a - 3d)x^2 + (-2ad + 3d^2 + b)x + (-bd + c + ad^2 - d^3),$$

y como d es tal que $a - 3d = 0$, el término cuadrático se elimina, y nos queda un polinomio de tercer grado sin término cuadrático

$$x^3 + (b - \frac{1}{3}a^2)x + (-\frac{1}{3}ba + c + \frac{2}{27}a^3).$$

Si sustituimos

$$\alpha = b - \frac{1}{3}a^2, \beta = -\frac{1}{3}ba + c + \frac{2}{27}a^3,$$

el polinomio queda:

$$x^3 + \alpha x + \beta.$$

Entonces, basta encontrar las raíces de $x^3 + \alpha x + \beta$ para encontrar las de $x^3 + ax^2 + bx + c$.

Calculemos las raíces de $x^3 + \alpha x + \beta$.

Primero, tomemos $z = \sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$. Observamos que si $z = 0$, entonces $\alpha, \beta = 0$. Así, las 3 raíces de $x^3 + \alpha x + \beta$ son el cero, y por lo tanto, tenemos el problema resuelto.

Ahora, si $0 \neq z = \sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$. Haciendo la sustitución $x = y + z$ en $x^3 + \alpha x + \beta$, nos queda:

$$\begin{aligned}(y+z)^3 + \alpha(y+z) + \beta &= y^3 + 3y^2z + 3yz^2 + z^3 + \alpha y + \alpha z + \beta \\ &= y^3 + 3yz(y+z) + \alpha(y+z) + z^3 + \beta \\ &= y^3 + z^3 + (3yz + \alpha)(y+z) + \beta. \qquad (1)\end{aligned}$$

Observamos en (1), que si $3yz + \alpha = 0$, entonces $(3yz + \alpha)(y + z)$ se elimina. Luego, de $3yz + \alpha = 0$, obtenemos que $y = -\frac{1}{3}\frac{\alpha}{z}$ $z \neq 0$. Ahora, veamos por que $z = \sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$. Sustituyendo el valor de y en (1), obtenemos

$$(-\frac{1}{3}\frac{\alpha}{z})^3 + z^3 + \beta = -\frac{\alpha^3}{27z^3} + z^3 + \beta.$$

Luego, multiplicando por z^3

$$z^6 + \beta z^3 - \frac{\alpha^3}{27}.$$

Este es un polinomio de segundo grado en z^3. Aplicando la fórmula general para polinomios de segundo grado, se tiene:

$$\begin{aligned}z^3 &= \frac{-\beta \pm \sqrt{\beta^2 + \frac{4}{27}\alpha^3}}{2} = \frac{-\beta \pm \sqrt{\frac{4}{4}\beta^2 + \frac{4}{27}\alpha^3}}{2} = \\ &= \frac{-\beta \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}{2} = \frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}} \\ z &= \sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}.\end{aligned}$$

Entonces, como $y = -\frac{1}{3}\frac{\alpha}{z}$, obtenemos el valor de y, y por último $x = y + z$.

Resumiendo lo anterior, una raíz del polinomio

$$x^3 + ax^2 + bx + c$$

es:

$$x_1 = -\frac{1}{3\left(\sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}\right)} + \left(\sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}\right) - d,$$

con

$$\alpha = b - \frac{1}{3}a^2, \beta = -\frac{1}{3}ba + c + \frac{2}{27}a^3.$$

Luego, consideremos $\omega = e^{2\pi i/3}$. Sabemos que todas las otras raíces de z^3 son:

$$z$$
$$z\omega$$
$$z\omega^2.$$

Ahora, como

$$y = -\frac{1}{3}\frac{\alpha}{z},$$

con z raíz de z^3, sustituyendo $z\omega$, obtenemos

$$\begin{aligned} -\frac{1}{3}\frac{\alpha}{z\omega} &= y\left(\frac{1}{\omega}\right) \\ &= \omega^2 y. \end{aligned}$$

Haciendo lo mismo para $z\omega^2$, se obtiene

$$-\frac{1}{3}\frac{\alpha}{z\omega^2} = y\left(\frac{1}{\omega^2}\right) = y\omega.$$

Así, obtenemos todas las raíces de $x^3 + ax^2 + bx + c$. Estas son:

$$\begin{aligned} x_1 &= y + z - d \\ x_2 &= z\omega + y\omega^2 - d \\ x_3 &= z\omega^2 + y\omega - d \end{aligned}$$

Ejemplo 3. Consideremos $x^3 - 3x^2 + x - 3$. Resolviendo la igualdad

$$x^3 - 3x^2 + x - 3 = x^3 + ax^2 + bx + c,$$

tenemos que los valores de a, b, c son:

$$a = -3, b = 1, c = -3.$$

Recordando que

$$\alpha = b - \frac{1}{3}a^2, \beta = -\frac{1}{3}ba + c + \frac{2}{27}a^3,$$

y sustituyendo,

$$\begin{aligned} \alpha &= 1 - \frac{1}{3}(-3)^2 \\ \beta &= -\frac{1}{3}(1)(-3) + (-3) + \frac{2}{27}(-3)^3, \end{aligned}$$

obtenemos

$$\begin{aligned} \alpha &= -2 \\ \beta &= -4. \end{aligned}$$

Basta encontrar las soluciones de $x^3 - 2x - 4 = 0$.

Recordemos que

$$\begin{aligned} y &= -\frac{1}{3}\frac{\alpha}{z} \\ z &= \sqrt[3]{\frac{-\beta}{2} \pm \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}. \end{aligned}$$

Entonces,

$$\begin{aligned} z &= \sqrt[3]{\frac{-(-4)}{2} + \sqrt{\frac{(-4)^2}{4} + \frac{(-2)^3}{27}}} \\ &= \sqrt[3]{2 + \sqrt{4 - \frac{8}{27}}} \\ &= \sqrt[3]{2 + \sqrt{\frac{100}{27}}} \\ &= \sqrt[3]{2 + \frac{10}{\sqrt{27}}}, \end{aligned}$$

y así, y es:

$$y = -\frac{1}{3}\frac{(-2)}{\sqrt[3]{2+\frac{10}{\sqrt{27}}}}.$$

Como $x = y + z$, tenemos:

$$\begin{aligned} x &= -\frac{1}{3}\frac{(-2)}{\sqrt[3]{2+\frac{10}{\sqrt{27}}}} + \sqrt[3]{2+\frac{10}{\sqrt{27}}} \\ &= 2. \end{aligned}$$

Por lo tanto, una raíz del polinomio $x^3 - 2x - 4$, es 2. Pero el polinomio original antes de sustituir $x - d$ es $x^3 - 3x^2 + x - 3$. Sabemos que $d = \frac{a}{3}$ y $a = -3$. En consecuencia, $d = -1$. Así, si $x = 2$ es raíz de $x^3 - 2x - 4$, entonces $2 - (-1) = 3$ es raíz de $x^3 - 3x^2 + x - 3$.

Haciendo una división, obtenemos

$$\frac{x^3 - 3x^2 + x - 3}{x - 3} = x^2 + 1.$$

En el **Ejemplo 2** obtuvimos las raíces de $x^2 + 1$. Estas son:

$$\begin{aligned} x_1 &= i \\ x_2 &= -i. \end{aligned}$$

Entonces, las raíces del polinomio $x^3 - 3x^2 + x - 3$ son:

$$\begin{aligned} x_1 &= 3 \\ x_2 &= i \\ x_3 &= -i. \end{aligned}$$

1.3 Polinomios de cuarto grado.

A continuación, obtendremos la fórmula general para calcular las raíces de polinomios de cuarto grado. Lo haremos considerando variables auxiliares.

Consideremos el polinomio $ax^4 + bx^3 + cx^2 + dx + e$, con $a, b, c, d, e \in \mathbb{C}$. Como $a \neq 0$, podemos multiplicar por $\frac{1}{a}$. Entonces,

$$\frac{1}{a}(ax^4 + bx^3 + cx^2 + dx + e)$$
$$x^4 + \frac{b}{a}x^3 + \frac{c}{a}x^2 + \frac{d}{a}x + \frac{e}{a}.$$

Sustituyendo,

$$\begin{aligned} \alpha &= \frac{b}{a} \\ \beta &= \frac{c}{a} \\ \gamma &= \frac{d}{a} \\ \delta &= \frac{e}{a}. \end{aligned}$$

El polinomio

$$ax^4 + bx^3 + cx^2 + dx + e$$

se trasforma en el polinomio

$$x^4 + \alpha x^3 + \beta x^2 + \gamma x + \delta.$$

Así, es suficiente considerar el polinomio mónico

$$x^4 + ax^3 + bx^2 + cx + d.$$

Resolvamos la ecuación $x^4 + ax^3 + bx^2 + cx + d = 0$. Consideremos η tal que

$$\eta^3 - b\eta^2 + (ac - 4d)\eta - b^2d + 4bd - c^2 = 0. \tag{1}$$

En otras palabras, η es raíz del polinomio

$$y^3 - by^2 + (ac - 4d)y - a^2d + 4bd - c^2.$$

Como ya tenemos la fórmula general para encontrar las raíces de polinomios de tercer grado, resulta sencillo encontrar η.

Por otro lado, tenemos:

$$\begin{aligned}
x^4 + ax^3 &= -bx^2 - cx - d \\
x^2 + ax^3 + \frac{1}{4}a^2x^2 &= -bx - cx - d + \frac{1}{4}a^2x^2 \\
(x^2 + \frac{1}{2}ax)^2 &= (\frac{1}{4}a^2 - b)x^2 - cx - d \\
(x^2 + \frac{1}{2}ax)^2 + (x^2 + \frac{1}{2}ax)\eta + \frac{1}{4}\eta^2 &= (\frac{1}{4}a^2 - b)x^2 - cx - d + (x^2 + \frac{1}{2}ax)\eta + \frac{1}{4}\eta \\
(x^2 + \frac{1}{2}ax + \frac{1}{2}\eta)^2 &= (\frac{1}{4}a^2 - b + \eta)x^2 + ... + \qquad (2) \\
&\quad +(-c + \frac{1}{2}a\eta)x + (-d + \frac{1}{4}\eta^2).
\end{aligned}$$

Observemos que

$$(-c + \frac{1}{2}a\eta)^2 = 4(\frac{1}{4}a^2 - b + \eta)(-d + \frac{1}{4}\eta^2), \qquad (3)$$

o equivalentemente,

$$(-c + \frac{1}{2}a\eta)^2 - 4(\frac{1}{4}a^2 - b + \eta)(-d + \frac{1}{4}\eta^2) = 0.$$

Desarrollando el lado izquierdo de la ecuación anterior

$$(-c + \frac{1}{2}a\eta)^2 - 4(\frac{1}{4}a^2 - b + \eta)(-d + \frac{1}{4}\eta^2) =$$

$$\begin{aligned}
&= c^2 - a\eta + \frac{1}{4}a^2\eta^2 - \left(-\frac{1}{4}a^2d + \frac{1}{16}a^2\eta^2 + bd - \frac{1}{4}b\eta^2 - \eta d + \frac{1}{4}\eta^3\right) \\
&= c^2 - a\eta + \frac{1}{4}a^2\eta^2 + a^2d - \frac{1}{4}a^2\eta^2 - 4bd + b\eta^2 + 4\eta d - \eta^3 \\
&= -\left[\eta^3 - b\eta^2 + (a - 4d)\,\eta + 4bd - a^2d - c^2\right],
\end{aligned}$$

y así, por la ecuación (1),

$$(-c + \frac{1}{2}a\eta)^2 - 4(\frac{1}{4}a^2 - b + \eta)(-d + \frac{1}{4}\eta^2) = 0.$$

Ahora, encontraremos números complejos A, B que cumplan

$$\begin{aligned} A^2 &= \frac{1}{4}a^2 - b + \eta \quad (4)\\ B^2 &= -d + \frac{1}{4}\eta^2 \quad (5)\\ 2AB &= -c + \frac{1}{2}a\eta. \quad (6) \end{aligned}$$

Para ello, sean A_1 y B_1 tales que

$$\begin{aligned} A_1^2 &= \frac{1}{4}a^2 - b + \eta\\ B_1^2 &= -d + \frac{1}{4}\eta^2. \end{aligned}$$

Por la ecuación (3), se cumple

$$4(A_1B_1)^2 = (-c + \frac{1}{2}a\eta).$$

Sacando raíz, obtenemos

$$2A_1B_1 = \pm(-c + \frac{1}{2}a\eta).$$

Entonces, consideremos los siguientes casos:

Caso (1) . Si $2A_1B_1 = -c + \frac{1}{2}a\eta$, tomamos $A = A_1, B = B_1$.

Caso (2). Si $2A_1B_1 = -(-c + \frac{1}{2}a\eta)$, tomamos $A = -A_1, B = B_1$.

Es claro que en los dos casos, A y B satisfacen (4), (5) y (6).

Así, tenemos complejos A, B que cumplen:

$$\begin{aligned} A^2 &= \frac{1}{4}a^2 - b + \eta\\ B^2 &= -d + \frac{1}{4}\eta^2\\ 2AB &= -c + \frac{1}{2}a\eta. \end{aligned}$$

Sumando $A^2, B^2, 2AB$ obtenemos

$$A^2 + 2AB + B^2 = (\frac{1}{4}a^2 - b + \eta)x^2 + (-c + \frac{1}{2}a\eta)x + (-d + \frac{1}{4}\eta^2).$$

Luego, factorizando del lado izquierdo la ecuación anterior,

$$(Ax+B)^2 = (\frac{1}{4}a^2 - b + \eta)x^2 + (-c + \frac{1}{2}a\eta)x + (-d + \frac{1}{4}\eta^2),$$

y sustituyendo en la ecuación (2), tenemos:

$$(x^2 + \frac{1}{2}ax + \frac{1}{2}\eta)^2 = (Ax+B)^2.$$

La ecuación anterior es equivalente a la ecuación original

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

Entonces, resolviendo las ecuaciones

$$\begin{aligned} x^2 + \frac{1}{2}ax + \frac{1}{2}\eta &= Ax + B \\ x^2 + \frac{1}{2}ax + \frac{1}{2}\eta &= -Ax - B, \end{aligned}$$

obtendremos las raíces de $x^4 + ax^3 + bx^2 + cx + d$. Por lo tanto, las raíces del polinomio $x^4 + ax^3 + bx^2 + cx + d$, son las soluciones de las ecuaciones

$$\begin{aligned} x^2 + (\frac{1}{2}a - A)x + (\frac{1}{2}\eta - B) &= 0 \\ x^2 + (\frac{1}{2}a + A)x + (\frac{1}{2}\eta + B) &= 0. \end{aligned}$$

Ejemplo 5. Sea $x^4 + 4x^3 + x + 1$. Calculemos los valores de a, b, c y d; resolvamos la siguiente ecuación

$$x^4 + 4x^3 + x + 1 = x^4 + ax^3 + bx^2 + cx + d.$$

Entonces

$$\begin{aligned} a &= 4 \\ b &= 0 \\ c &= 1 \\ d &= 1. \end{aligned}$$

Ahora, para calcular η, sustiruyamos los valores de a, b, c y d en

$$\eta^3 - b\eta^2 + (ac - 4d)\eta - a^2 d + 4bd - c^2 = 0,$$

nos queda

$$\eta^3 - 17 = 0.$$

Luego, $\eta = \sqrt[3]{17}$. Recordando que

$$\begin{aligned} A^2 &= \frac{1}{4}a^2 - b + \eta \\ B^2 &= -d + \frac{1}{4}\eta^2 \\ 2AB &= -c + \frac{1}{2}a\eta, \end{aligned}$$

los valores de A, B son:

$$\begin{aligned} A &= \sqrt{4 + \sqrt[3]{17}} \\ B &= \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}. \end{aligned}$$

Entonces, obtenemos las ecuaciones:

$$\begin{aligned} x^2 + (2 - 4\sqrt{4 + \sqrt[3]{17}})x + (\frac{1}{2}\sqrt[3]{17} - \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}) &= 0 \\ x^2 + (2 + \sqrt{4 + \sqrt[3]{17}})x + (\frac{1}{2}\sqrt[3]{17} + \sqrt{-1 + \frac{1}{4}\sqrt[3]{17^2}}) &= 0, \end{aligned}$$

y ocupando la fórmula general de segundo grado, obtenemos:

$$
\begin{aligned}
x_1 &= \frac{-(2-4\sqrt{4+\sqrt[3]{17}})+\sqrt[2]{\left(2-4\sqrt{4+\sqrt[3]{17}}\right)^2-4\left(\frac{1}{2}\sqrt[3]{17}-\sqrt{-1+\frac{1}{4}\sqrt[3]{17^2}}\right)}}{2}\\
x_2 &= \frac{-(2-4\sqrt{4+\sqrt[3]{17}})-\sqrt[2]{\left(2-4\sqrt{4+\sqrt[3]{17}}\right)^2-4\left(\frac{1}{2}\sqrt[3]{17}-\sqrt{-1+\frac{1}{4}\sqrt[3]{17^2}}\right)}}{2}\\
x_3 &= \frac{-(2+4\sqrt{4+\sqrt[3]{17}})+\sqrt[2]{\left(2-4\sqrt{4+\sqrt[3]{17}}\right)^2-4\left(\frac{1}{2}\sqrt[3]{17}+\sqrt{-1+\frac{1}{4}\sqrt[3]{17^2}}\right)}}{2}\\
x_4 &= \frac{-(2+4\sqrt{4+\sqrt[3]{17}})-\sqrt[2]{\left(2-4\sqrt{4+\sqrt[3]{17}}\right)^2-4\left(\frac{1}{2}\sqrt[3]{17}+\sqrt{-1+\frac{1}{4}\sqrt[3]{17^2}}\right)}}{2}
\end{aligned}
$$

Capítulo 2

Teoría de Galois.

Consideremos una extensión de campos $K \rightarrowtail L$. Definimos

$Gal(K \rightarrowtail L) = \{f : L \to L |\ f$ es isomorfismo y si $x \in K$, entonces $f(x) = x\}$.

Esto es, el conjunto de automorfismos de L que dejan fijo a K.

Ejemplo 1. Tomemos la extensión de campos $\mathbb{R} \rightarrowtail \mathbb{C}$. Sea

$$f \in Gal(\mathbb{R} \rightarrowtail \mathbb{C}).$$

Entonces, $f : \mathbb{C} \to \mathbb{C}$ es isomorfismo tal que, si $x \in \mathbb{R}$, entonces $f(x) = x$. Ahora, si $x \in \mathbb{C}$, sabemos que $x = a + bi$ con $a, b \in \mathbb{R}$. Aplicando f a x tenemos

$$f(x) = f(a + bi) = f(a) + f(b)f(i) = a + bf(i),$$

ya que f es homomorfismo de campos y $a, b \in \mathbb{R}$. Para saber qué homomorfismo es f, basta saber el valor de $f(i)$. Calculemos $f(i)$. Sabemos que

$$\begin{aligned} i^2 &= -1 \\ (f\,(i))^2 &= f(i^2) = f(i)f(i) = f(-1) = -1 \end{aligned}$$

Entonces, $f(i)$ es un complejo cuyo cuadrado es -1. Por lo tanto, el valor de $f(i)$ es $\pm i$, y se tiene que $f(a+bi) = a \pm bi$, es decir, f es la identidad o la función conjugar. Luego, $Gal(\mathbb{R} \rightarrowtail \mathbb{C}) = \{id_L, c\}$, con c la función conjugar.

Ejemplo 2. Tomemos la extensión de campos $\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2})$. Calculemos $Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}))$.

Tomemos $f \in Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt{2}))$ y $x \in \mathbb{Q}(\sqrt{2})$. Por definición de $\mathbb{Q}(\sqrt[2]{2})$, $x = a + b\sqrt[2]{2}$, con $a, b \in \mathbb{Q}$. Aplicando f a x, obtenemos:

$$\begin{aligned} f(x) &= f(a + b\sqrt{2}) \\ &= f(a) + f(b)f(\sqrt{2}) \\ &= a + bf(\sqrt{2}). \end{aligned}$$

Así, basta encontrar el valor de $f(\sqrt{2})$. Sabemos que

$$\begin{aligned} 2 &= f(2) \\ &= f(\sqrt{2})f(\sqrt{2}). \end{aligned}$$

Por lo tanto, $f(\sqrt{2})$ es un elemento de $\mathbb{Q}(\sqrt{2})$, tal que al elevarlo al cuadrado es 2. Luego $f(\sqrt{2}) = \pm\sqrt{2}$. Entonces, f tiene dos posibilidades

$$\begin{aligned} f(a + b\sqrt{2}) &= a + b\sqrt{2} \\ &= a - b\sqrt{2}. \end{aligned}$$

Por lo tanto $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id_{\mathbb{Q}(\sqrt{2})}, c\}$.

Una observación de **Ejemplo 1** y **Ejemplo 2** es

$$\begin{aligned} 2 &= |Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[2]{2}))| \\ &= [\mathbb{Q}(\sqrt[2]{2}) : \mathbb{Q}] \end{aligned}$$

y

$$\begin{aligned} 2 &= |Gal(\mathbb{R} \rightarrowtail \mathbb{C})| \\ &= [\mathbb{R} : \mathbb{Q}] \end{aligned}$$

Podríamos plantearnos la siguiente pregunta: ¿Coincide el grado de la extensión con el orden del grupo $Gal\,(K \rightarrowtail L)$?

La respuesta es no, como el siguiente ejemplo lo muestra.

Ejemplo 3. Sea $\alpha = \sqrt[3]{2} \in \mathbb{R}$ y consideremos la extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2})$. Tomemos $f \in Gal(\ \mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2}))$. Los elementos de $\mathbb{Q}(\sqrt[3]{2})$ son de la forma $a + b\sqrt[3]{2} + c\sqrt[3]{2^2}$ pero para saber que automorfismo es f basta con considerar $a + b\sqrt[3]{2}$.

Como f es automorfismo, tenemos:

$$\begin{aligned} f(a+b\sqrt[3]{2}) &= f(a)+f(b)f(\sqrt[3]{2}) \\ &= a+bf(\sqrt[3]{2}). \end{aligned}$$

Basta encontrar el valor de $f\left(\sqrt[3]{2}\right)$. Para saber el valor de $f\left(\sqrt[3]{2}\right)$, se tiene que

$$\begin{aligned} 2 &= \alpha^3 \\ &= f(\alpha^3) \\ &= f(\alpha)f(\alpha)f(\alpha) \\ &= f(\alpha)^3. \end{aligned}$$

Por lo tanto, $f(\alpha)$ es un elemento de $\mathbb{Q}(\sqrt[3]{2})$ tal que al elevarlo al cubo nos da 2. Sabemos que las otras dos raíces de $\sqrt[3]{2}$ son complejas por lo que no están en $\mathbb{Q}(\sqrt[3]{2})$. Así, $f(\alpha)=\alpha$. Se sigue que f es el homomorfismo identidad. Luego, $Gal\,(K \rightarrowtail L)$ solo consta del homomorfismo identidad. Así

$$Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2})) = \{id_{\mathbb{Q}(\sqrt[3]{2})}\}.$$

Por lo que

$$|Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2}))| = 1$$

y

$$[\mathbb{Q} : \mathbb{Q}(\sqrt[3]{2})] = 3.$$

ya que el polinomio mínimo de $\sqrt[3]{2}$ es x^3-2.

En consecuencia

$$|Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2})| < [\mathbb{Q} : \mathbb{Q}(\sqrt[3]{2})].$$

Por lo tanto, el grado de la extensión no coincide con el orden del grupo de automorfismos. Mostraremos que el grado de la extensión, será cota para el orden del grupo de automorfismos, si el grado de la extensión es finita.

Proposición 2.1. Sea $K \rightarrowtail L$ una extensión de campos. Entonces, $Gal(K \rightarrowtail L)$ es un grupo bajo la composición.

Demostración: Mostremos que $Gal(K \rightarrowtail L)$ es cerrado bajo la composición. Sean $g, f \in Gal\,(K \rightarrowtail L)$. Sabemos que la composición de isomorfismos es isomorfismo. Sólo falta ver que $f \circ g$ deja fijo a K. Sea $x \in K$, entonces

$$g(x) = f(x) = x.$$

Así

$$(f \circ g)(x) = f(g(x)) = f(x) = x.$$

Entonces, $f \circ g : L \to L$ es un isomorfismo que deja fijo a K. Luego

$$f \circ g \in Gal(K \rightarrowtail L).$$

El elemento indentidad de $Gal\,(K \rightarrowtail L)$ es $id_L : L \to L$ dada por $id\,(x) = x$.

La composición de funciones es asociativa, entonces, como los elementos de $Gal(K \rightarrowtail L)$ son funciones, $Gal(K \rightarrowtail L)$ es asociativo bajo la composición.

Como f es un automorfismo, existe f^{-1} y es isomorfismo de campos. Solo falta ver que f^{-1} deja fijo a K, tomemos $x \in K$. Como $f \in Gal\,(K \rightarrowtail L)$, $f(x) = x$. Así,

$$x = f^{-1}(f(x)) = f^{-1}(x),$$

es decir, f^{-1} es un isomorfismo que deja fijo a K.

Luego, $Gal(K \rightarrowtail L)$ es un grupo.♦

Continuaremos con dos definiciones, pero primero, daremos un ejemplo en un caso particular.

En **Ejemplo 1,** demostramos que $Gal(\mathbb{R} \rightarrowtail \mathbb{C}) = \{id_{\mathbb{C}}, c\}$. Consideremos los subgrupos $G_1 = \{id\}$, y $G_2 = \{id_{\mathbb{C}}, c\}$ de $Gal(\mathbb{R} \rightarrowtail \mathbb{C})$. Vamos a construir el campo fijo de G_1 y G_2 respectivamente. Definimos los campos fijos (se demostrará que son campos en **Lema 2.3**) de G_1 y G_2 como los elementos de $\mathbb{C}$ que quedan fijos bajo todos los homomorfismos de G_1 y G_2, respectivamente. Utilizamos la siguiente notación:

$$\mathbb{C}^{G_1} = \{\alpha \in \mathbb{C} \mid \ f(\alpha) = \alpha \text{ para todo } f \in G_1\}$$

$$\mathbb{C}^{G_2} = \{\alpha \in \mathbb{C} \mid f(\alpha) = \alpha \text{ para todo } f \in G_2\}.$$

Observemos que $\mathbb{C}^{G_1} = \mathbb{C}$. La contención $\mathbb{C}^{G_1} \subset \mathbb{C}$ es por definición de $\mathbb{C}^{G_1}$.

Por otro lado, si $x \in \mathbb{C}$, entonces, como la identidad en $\mathbb{C}$ deja fijo a todo $\mathbb{C}$, en particular, deja fijo a x; además, ya que la identidad es el único elemento de G_1, tenemos que $x \in \mathbb{C}^{G_1}$. Por lo tanto, $\mathbb{C}$ es el campo fijo de G_1.

Calculemos ahora $\mathbb{C}^{G_2}$. Como $G_2 = \{id_{\mathbb{C}}, c\}$, encontremos el subconjunto de complejos que queden fijos bajo la identidad y la conjugación. Esto es,

los complejos tales que $c(a+bi) = a+bi$. Entonces, como $c(a+bi) = a-bi$, tenemos que encontrar los números que cumplen $a+bi = a-bi$. Se sigue que $bi = -bi$. El único complejo que cumple esta ecuación es $b = 0$. Por lo tanto, los complejos que cumplen esta propiedad, son aquellos de la forma $a + 0i = a$. En consecuencia, el campo fijo de G_2 son los reales.

Así, dado un subgrupo del grupo de automorfismos, podemos encontrar un campo asociado al grupo. Ahora, veamos que a un campo entre los complejos y los reales, le podemos asociar un subgrupo del grupo de autormorfismos.

Consideremos K tal que $\mathbb{R} \subset K \subset \mathbb{C}$. Podemos tomar dos subgrupos asociados a K; el primero, $Gal(\mathbb{R} \rightarrowtail K)$, es un grupo por **Proposición 2.1**, pero para nuestro propósito no es muy útil, ya que no necesariamente es un subgrupo de $Gal(\mathbb{R} \rightarrowtail \mathbb{C})$. En consecuencia, consideraremos $Gal(K \rightarrowtail \mathbb{C})$.

Como K tiene dos posibilidades ($K = \mathbb{R}$ ó $K = \mathbb{C}$), consideraremos primero $K = \mathbb{R}$. Notamos que $Gal(K \rightarrowtail \mathbb{C}) = Gal(\mathbb{R} \rightarrowtail \mathbb{C})$, por lo que $Gal(\mathbb{R} \rightarrowtail \mathbb{C}) = \{id_{\mathbb{C}}, c\}$, que es un subgrupo de $Gal(\mathbb{R} \rightarrowtail \mathbb{C})$. Ahora, consideremos $K = \mathbb{C}$. Entonces $Gal(\mathbb{C} \rightarrowtail \mathbb{C})$ son los automorfismos que dejan fijo a $\mathbb{C}$. Por lo tanto, $Gal(\mathbb{C} \rightarrowtail \mathbb{C}) = \{id_{\mathbb{C}}\}$, que también es un subgrupo de $Gal(\mathbb{R} \rightarrowtail \mathbb{C})$.

De lo anterior vimos cómo relacionar subgrupos de $Gal(\mathbb{R} \rightarrowtail \mathbb{C})$ con campos entre $\mathbb{C}$ y $\mathbb{R}$, y también, dado un campo intermedio entre $\mathbb{C}$ y $\mathbb{R}$, le asociamos un subgrupo de $Gal(\mathbb{R} \rightarrowtail \mathbb{C})$.

En el ejemplo anterior, calculamos cuál es el campo fijo de un subgrupo de $Gal\,(\mathbb{R} \rightarrowtail \mathbb{C})$, así como también, dado un campo entre $\mathbb{C}$ y $\mathbb{R}$, calculamos el grupo asociado al campo intermedio. Definamos, en general, el grupo asociado a un campo intermedio y el campo fijo de un subgrupo de $Gal\,(K \rightarrowtail L)$.

Definición 2.2. Sea $K \rightarrowtail L$ una extensión de campos y G un subgrupo de $Gal(K \rightarrowtail L)$. **El campo fijo de** G es el conjunto de todos los elementos de L que quedan fijos bajo todo elemento de G. Lo denotaremos con L^G. Esto es

$$L^G = \{a \in L | f(a) = a \text{ para todo elemento } f \text{ en } G\}.$$

Hasta este momento no tenemos nada que nos asegure que, en efecto, el conjunto $L^G = \{a \in L|\ f(a) = a$ para todo elemento f en $G\}$ sea un campo.

Necesitamos el siguiente lema para que nuestra definición tenga sentido.

Lema 2.3. Sea G un subgrupo de $Gal(K \rightarrowtail L)$. L^G es un campo entre L y K.

Demostración: Como $L^G = \{a \in L |\ f(a) = a$ para todo elemento f en $G\}$, se tiene que $L^G \subset L$; también $K \subset L^G$. En efecto, como G es un subconjuto de $Gal(K \rightarrowtail L)$ y $Gal(K \rightarrowtail L)$ son todos los isomorfismos de L que dejan fijo a K, se tiene que todos los elementos de G dejan fijo a K.

Sólo falta mostrar que es un campo. Sean $x, y \in L^G$. Tenemos que para todo elemento $f \in G$, se cumple que

$$f(x+y) = f(x) + f(y) = x + y,$$

ya que

$$\begin{aligned} f(x) &= x \\ f(y) &= y. \end{aligned}$$

Así,

$$x + y \in L^G.$$

Por otro lado, para todo elemento $f \in G$, se cumple que

$$\begin{aligned} f(x) &= x \\ f(y) &= y. \end{aligned}$$

Se sigue que

$$f(xy) = f(x)f(y) = xy,$$

por lo que $xy \in L^G$, es decir, L^G es cerrado bajo sumas y productos. Luego, L^G es un campo.♦

Lema 2.5. Consideremos $K \rightarrowtail L$ una extensión de campos y M un campo tal que $K \subset M \subset L$. Entonces, $Gal(M \rightarrowtail L)$ es un subgrupo de $Gal(K \rightarrowtail L)$.

Demostración: Mostremos que

$$Gal(M \rightarrowtail L) \subset Gal(K \rightarrowtail L).$$

Sea $f \in Gal(M \rightarrowtail L)$. Sabemos que $f : L \longrightarrow L$ es un isomorfismo que deja fijo a M, y como $K \subset M$, entonces también deja fijo a K. Por lo tanto, $f \in Gal(K \rightarrowtail L)$.

Mostremos que $Gal(M \rightarrowtail L)$ es subgrupo de $Gal(K \rightarrowtail L)$. Sean

$$f, g \in Gal(M \rightarrowtail L).$$

Sabemos que $f \circ g$ es un isomorfismo de L en L. Falta probar que deja fijo a M. En efecto, si $x \in M$

$$(f \circ g)(x) = f(g(x)) = f(x) = x$$

ya que $f, g \in Gal(M \rightarrowtail L)$. Luego, $(f \circ g)$ es un isomorfismo de L en L que deja fijo a cualquier elemento de M. Se sigue que $f \circ g \in Gal(M \rightarrowtail L)$.

Falta mostrar que dado $f \in Gal(M \rightarrowtail L)$, entonces $f^{-1} \in Gal(M \rightarrowtail L)$. Sea $f \in Gal(M \rightarrowtail L)$. Sabemos que f^{-1} existe, es isomorfismo y es único. Veamos que f^{-1} deja fijo a M. Sea $x \in M$, tenemos que, $f(x) = x$ ya que $f \in Gal(M \rightarrowtail L)$. Entonces

$$x = f^{-1}(f(x)) = f^{-1}(x)$$

es decir, $x = f^{-1}(x)$. Luego f^{-1} deja fijo a M. En consecuencia, $f^{-1} \in Gal(M \rightarrowtail L)$.

Por lo tanto $Gal(M \rightarrowtail L)$ es un subgrupo de $Gal(K \rightarrowtail L)$.♦

Definición 2.4. Sea $K \rightarrowtail L$ una extensión de campos y M un campo tal que $K \subset M \subset L$. Definimos $S(M) = Gal(M \rightarrowtail L)$ como el subgrupo de $Gal(K \rightarrowtail L)$ asociado al campo M.

Notemos que, en general, dado un subgrupo G de $Gal(K \rightarrowtail L)$, le podemos asignar un campo entre K y L, a saber, el campo fijo de G.

También, dado un campo entre L y K, le podemos asociar un subgrupo de $Gal(K \rightarrowtail L)$. Así, podemos construir dos funciones; la primera, que a cada subgrupo de $Gal(K \rightarrowtail L)$ le asocie un campo entre L y K; la otra función será la que asigne a cada campo intemedio un subgrupo de $Gal(K \rightarrowtail L)$. A dichas funciones las llamaremos F y S respectivamente. Construyámoslas formalmente.

Denotemos

$$\begin{aligned} Sub_{K \rightarrowtail L} &= \{\text{subgrupos de } Gal(M \rightarrowtail L)\} \\ Cam_{K \rightarrowtail L} &= \{\text{ campos entre } L \text{ y } K\}. \end{aligned}$$

Así,

$$\begin{aligned} F &: Sub_{K \rightarrowtail L} \longrightarrow Cam_{K \rightarrowtail L} \\ S &: Cam_{K \rightarrowtail L} \longrightarrow Sub_{K \rightarrowtail L} \end{aligned}$$

Estas funciones se definen por:

Si G es un subgrupo de $Gal\,(K \rightarrowtail L)$

$$F\,(G) = L^G.$$

Si M es un campo tal que $K \subset M \subset L$

$$S\,(M) = Gal\,(M \rightarrow L)\,.$$

Mostremos que F y S estan bien definidas.

Para F, de **Proposición 2.1,** dado un subgrupo G de

$$Gal(K \rightarrow L),$$

F le asigna L^G, que es un campo tal que $K \subset L^G \subset L$. Luego, F está definida de los subgrupos de $Gal(K \rightarrowtail L)$, a los campos entre K y L . Veamos que, si $G_1, G_2 \in Sub_{K \rightarrow L}$ tales que $G_1 = G_2$, entonces, $F(G_1) = F(G_2)$.

Por definición, $F(G_1) = L^{G_1}$ y $F(G_2) = L^{G_2}$. Entonces, lo que queremos demostrar es: $L^{G_1} = L^{G_2}$, si $G_1 = G_2$. Supongamos que $G_1 = G_2$. Por definición,

$$\begin{aligned} L^{G_1} &= \{a \in L | f\,(a) = a \text{ para todo } f \in G_1\} \\ L^{G_2} &= \{a \in L | f\,(a) = a \text{ para todo } f \in G_2\}. \end{aligned}$$

Si $x \in L^{G_1}$, x cumple que $x \in L$ y $f\,(x) = x$, para todo $f \in G_1 = G_2$. Por lo tanto, $x \in L$ y $f\,(x) = x$ para todo $f \in G_2$, es decir $x \in L^{G_2}$. La otra contención es análoga a la anterior. Entonces, $L^{G_1} = L^{G_2}$. En consecuencia, F está bien definida.

Mostremos que S está bien definida. Por **Lema 2.5**, dado un campo entre L y K, le podemos asignar un subgrupo de

$$Gal(K \rightarrowtail L).$$

Así, S está definida de los campos entre L y K a los subgrupos de

$$Gal(K \rightarrowtail L).$$

Demostremos que S es función, es decir, que si M_1, M_2 son campos iguales, se tiene que $S(M_1) = S(M_2)$. En efecto, por definición,

$$\begin{aligned} S(M_1) &= Gal(M_1 \rightarrowtail L) \\ S(M_2) &= Gal(M_2 \rightarrowtail L). \end{aligned}$$

Entonces, si $f \in S(M_1) = Gal(M_1 \rightarrowtail L)$, f es un isomorfismo de L en L que deja fijo a M_1. Pero, como $M_1 = M_2$, entonces, f es un isomorfismo de L en L que deja fijo a M_2. Por lo tanto, $f \in S(M_2) = Gal(M_2 \rightarrowtail L)$. La otra contención es análoga a la anterior. Se sigue que S, es función.♦

Ahora nos preguntamos si F y S son inversas una de la otra; la respuesta es negativa. En **Ejemplo 3,** vimos que $Gal(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2})) = \{id_{\mathbb{Q}(\sqrt[3]{2})}\}$. Se sigue que

$$S(\mathbb{Q}) = Gal\left(\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2})\right) = \{id_{\mathbb{Q}(\sqrt[3]{2})}\}.$$

Entonces

$$F \circ S(\mathbb{Q}) = F\left(\{id_{\mathbb{Q}(\sqrt[3]{2})}\}\right) = \mathbb{Q}(\sqrt[3]{2}).$$

Por lo tanto,

$$F \circ S(\mathbb{Q}) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}.$$

Luego,

$$F \circ S \neq Id_{C_{\mathbb{Q} \rightarrowtail \mathbb{Q}(\sqrt[3]{2})}}.$$

Sería deseable que las funciones F y S fueran inversa una de la otra, pero por lo anterior, no sucede. Al final de esta sección daremos condiciones para que F y S sean inversas.

Proposición 2.6. Las funciones $F : Sub_{K \rightarrowtail L} \longrightarrow Cam_{K \rightarrowtail L}$ y $S : Cam_{K \rightarrowtail L} \longrightarrow Sub_{K \rightarrowtail L}$ satisfacen:

a) Si M_1, M_2 son campos entre L y K, y $M_1 \subset M_2$, entonces

$$S(M_1) \supset S(M_2).$$

b) Para $M = K$, se satisface que $S(M) = Gal(K \rightarrowtail L)$.

c) Para el campo $M = L$, $S(L) = \{id_L\}$.

d) Si H_1 y H_2 son subgrupos de $Gal(K \rightarrowtail L)$, y $H_1 \subset H_2$, entonces $F(H_1) \supset F(H_2)$.

e) Si H es un subgrupo de $Gal(K \rightarrowtail L)$, entonces $H \subset S(F(H))$.

f) Si M es un campo entre L y K, entonces $M \subset F(S(M))$.

Demostración:

a) Sean M_1 y M_2 campos entre L y K, tales que $M_1 \subset M_2$. Por definición $S(M_1) = Gal(M_1 \rightarrowtail L)$ y $S(M_2) = Gal(M_2 \rightarrowtail L)$. Sea

$$f \in S(M_2) = Gal(M_2 \rightarrowtail L).$$

Entonces, f es un isomorfismo de L en L que deja fijo a M_2. Como $M_1 \subset M_2$, si f deja fijo a M_2, en particular dejará fijo a M_1, es decir, f es un isomorfismo de L en L que deja fijo a M_1. Por lo tanto $f \in S(M_1) = Gal(M_1 \rightarrowtail L)$. Luego $S(M_1) \supset S(M_2)$.

b) Sea $M = K$. Por definición

$$\begin{aligned} S(M) &= S(K) \\ &= Gal(M \rightarrowtail L) \\ &= Gal(K \rightarrowtail L). \end{aligned}$$

Por lo tanto $S(M) = Gal(K \rightarrowtail L)$.

c) Sea $M = L$. Entonces $S(M) = S(L) = Gal(L \rightarrowtail L)$. Luego, como $S(M)$ son todos los isomorfismos de L en L que dejan fijo a todo $M = L$, $S(M) = \{id_L\}$.

d) Sean H_1, H_2 subgrupos de $Gal(K \rightarrowtail L)$ tales que $H_1 \subset H_2$. Mostremos que $F(H_1) \supset F(H_2)$. Si $a \in F(H_2) = L^{H_2}$, entonces $f(a) = a$ para todo $f \in H_2$, ya que L^{H_2} es el campo fijo de H_2. Entonces, como $f \in H_1 \subset H_2$, se tiene que $f(a) = a$ para todo $f \in H_1$. Por lo tanto, a permanece fijo bajo todos los elementos de H_2, es decir, $a \in L^{H_2} = F(H_2)$. Luego $F(H_1) \supset F(H_2)$.

e) Sea H un subgrupo de $Gal(K \rightarrowtail L)$. Se tiene que

$$S(F(H)) = S(L^H) = Gal(L^H \rightarrowtail L) = \{f : L \to L| \quad f|_{L^H} = id\}.$$

Por definición

$$L^H = \{a \in L | f(a) = a \text{ para todo } f \in H\}.$$

Entonces, si $f \in H$, $f\lfloor_{L^H} = id$, ya que, L^H son todos los elementos de L que quedan fijos bajo cualquier elemento de H. Se sigue que $f \in S(F(H))$. Así, obtenemos que $H \subset S(F(H))$.

f) Sea M un campo entre L y K. Procedamos como en el inciso anterior. Calculemos $F(S(M))$.

$$F(S(M)) = F(Gal(M \to L)) = L^{Gal(M \rightarrowtail L)}.$$

Se tiene que

$$Gal(M \rightarrowtail L) = \{f : L \to L | f \text{ es isomorfismo, y si } x \in M,\, f(x) = x\}.$$

Entonces, si $x \in M$, dado cualquier $f \in Gal(M \rightarrowtail L)$, se cumple que $f(x) = x$. Por lo tanto, $x \in L^{Gal(M \rightarrowtail L)} = F(S(M))$. Luego, $M \subset F(S(M))$.♦

Para continuar, necesitamos definir que significa que un conjunto de automorfismos de un campo sea linealmente independiente.

Definición 2.7. Sea K un campo y $\{f_1, ..., f_n\}$ un conjunto de automorfismos distintos de K. Diremos que $\{f_1, ..., f_n\}$ es linealmente independiente si para todo $x \in K$ y $a_1, ..a_n \in K$ tal que

$$a_1 f_1(x) + ... + a_n f_n(x) = 0,$$

entonces $a_1, .., a_n = 0$.

Observación: Si f es un automorfismo de algún campo K, entonces $f(1) = 1$. En efecto, $f(1) \neq 0$ ya que si $f(1) = 0$, tendríamos que

$$f(x) = f(x) f(1) = f(x) \cdot 0 = 0.$$

en consecuencia f es la función cero. Luego

$$f(1) \cdot f(1) = f(1)$$

Entonces, como f es un automorfismo de K, tenemos que $0 \neq f(1) \in K$, así, $f(1)$ tiene inverso. Multiplicando la igualdad anterior por $f(1)^{-1}$, obtenemos

$$\begin{aligned} f(1) \cdot f(1) f(1)^{-1} &= f(1) \cdot f(1)^{-1} \\ f(1) &= 1. \end{aligned}$$

Teorema 2.8. Sea K un campo. Cualquier conjunto finito de automorfismos de K es linealmente independiente.

Demostración: Por inducción sobre el número de automorfismos.

Si $n = 1$, sólo tenemos un automorfismo. Supongamos que $af(x) = 0$ para todo $x \in K$ y demostremos que $a = 0$. Sabemos que, para $x = 1$, se tiene

$$af(1) = 0.$$

Entonces, por la observación anterior, sustituyendo $f(1) = 1$ en la igualdad $af(1) = 0$, obtenemos

$$a \cdot 1 = 0,$$

y como K es un campo, en particular es un domino entero. Luego $a = 0$.

Mostremos que es válido para $n \geq 2$. Supongamos que el teorema es cierto para m menor que n. Sea $\{f_1, ..., f_n\}$ un conjunto de n automorfismos de K. Demostraremos que $\{f_1, ..., f_n\}$ es linealmente independiente.

Supongamos que $\{f_1, ..., f_n\}$ es linealmente dependendiente, es decir, existe

$$a_1 f_1(x) + ... + a_n f_n(x) = 0$$

tal que, algún $a_i \neq 0$. La primera observación importante es que todos los $a_j \neq 0$, ya que de lo contrario, si algún $a_j = 0$ con j menor que n, eliminado $a_j f_j$ de $a_1 f_1(x) + ... + a_n f_n(x) = 0$, tendríamos una combinación lineal de menos de n elementos, con algún $a_i \neq 0$, que contradice nuestra hipótesis de inducción. Entonces, todos los escalares de $a_1 f_1(x) + ... + a_n f_n(x) = 0$ son distintos de cero. Por otro lado, como los f_i son distintos, en particular $f_1 \neq f_n$, por lo que, existe $a \in K$ tal que $f_1(a) \neq f_n(a)$. Como la ecuación $a_1 f_1(x) + ... + a_n f_n(x) = 0$ es válida para todo $x \in K$, en particular lo es para ax. Luego, sustituyendo, nos queda

$$a_1 f_1(ax) + ... + a_n f_n(ax) = 0.$$

Como los f_i son automorfismos de K, tenemos

$$a_1 f_1(a) f_1(x) + ... + a_n f_n(a) f_n(x) = 0.$$

Por otro lado, multiplicando a $a_1 f_1(x) + ... + a_n f_n(x)$ por $f_1(a)$, se obtiene

$$a_1 f_1(a) f_1(x) + ... + a_n f_1(a) f_n(x) = 0.$$

Entonces, restando $a_1 f_1(a) f_1(x) + ... + a_n f_1(a) f_n(x)$ a $a_1 f_1(a) f_1(x) + ... + a_n f_n(a) f_n(x)$, nos queda

$$a_1 f_1(a) f_1(x) + ... + a_n f_n(a) f_n(x) -$$

$$+ (a_1 f_1(a) f_1(x) + ... + a_n f_1(a) f_n(x)) = 0$$

$$a_2[f_2(a) - f_1(a)]f_2(x) + ...+$$
$$+a_n[f_n(a) - f_1(a)]f_n(x) = 0.$$

Observemos que en la última ecuación, el coficiente $a_n[f_n(a) - f_1(a)] \neq 0$, ya que $a_n \neq 0$ y $f_1(a) \neq f_n(a)$. Así, obtuvimos una combinación lineal no trivial de menos de n automorfismos, lo cual contradice nuestra hipótesis de inducción. Luego, el conjunto $\{f_1, ..., f_n\}$ es linealmente independiente.♦

Corolario 2.9. Sea $K \rightarrowtail L$ una extensión finita. Entonces

$$|Gal(K \rightarrowtail L)| \leq [L : K].$$

Demostración: Procedamos por contradicción. Supongamos que

$$|Gal(K \rightarrowtail L)| > [L : K].$$

Como la extensión $K \rightarrowtail L$ es finita, existe un natural, tal que

$$n = [L : K].$$

Tomemos $a_1, ...a_n \in L$ una base de L sobre K. Por la suposición, sabemos que $Gal(K \rightarrowtail L)$ tiene al menos $n + 1$ elementos, digamos

$$f_1, ..., f_{n+1} \in Gal(K \rightarrowtail L).$$

Consideremos el siguiente sistema con coeficientes en L:

$$f_1(a_1)x_1 + ... + f_{n+1}(a_1)x_{n+1} = 0$$

$$\vdots$$

$$f_1(a_n)x_1 + ... + f_{n+1}(a_n)x_{n+1} = 0.$$

Notamos que tenemos más variables que ecuaciones, por lo que nuestro sistema tiene una solución no trivial. Sea $(b_1, .., b_{n+1})$ una solución no trivial del sistema, entonces algún $b_i \neq 0$. Luego, para cualquier ecuación de nuestro sistema, se tiene

$$f_1(a_j)b_1 + ... + f_{n+1}(a_j)b_{n+1} = 0, \tag{1}$$

con $1 \leq j \leq n$ y algún $b_i \neq 0$.

Por otro lado, como $\{a_1, ..., a_n\}$ es una base de L sobre K, se tiene que para todo $x \in L$ existen $\eta_1, ..., \eta_n \in K$ tales que

$$x = \eta_1 a_1 +, ..., +\eta_n a_n \in K,$$

y como los f_i son automorfismos de L que dejan fijo K, y $\eta_1, ..., \eta_n \in K$, $f_i(\eta_j) = \eta_j$. Entonces, para todo $x \in L$ se cumple que

$$\begin{aligned} f_i(x) &= f_i(\eta_1 a_1 + ... + \eta_n a_n) \\ &= f_i(\eta_1 a_1) + ... + f_i(\eta_n a_n) \\ &= \eta_1 f_i(a_1) + ... + \eta_n f_i(a_n). \end{aligned} \tag{2}$$

Sustituyendo (2) en (1)

$$\begin{aligned} b_1 f_1(x) + ... + b_{n+1} f_{n+1}(x) &= b_1(\eta_1 f_1(a_1) + ... + \eta_n f_1(a_n)) + ... + \\ &\quad + b_{n+1}(\eta_1 f_n(a_1) + ... + \eta_n f_n(a_n)) \\ &= \eta_1(b_1 f_1(a_1) + ... + b_{n+1} f_{n+1}(a_1)) + ... + \\ &\quad + \eta_n(b_1 f_1(a_1) + ... + b_{n+1} f_{n+1}(a_n)), \end{aligned}$$

y recordando que $f_1(a_j) b_1 + ... + f_{n+1}(a_j) b_{n+1} = 0$ con $1 \leq j \leq n$. Se sigue que

$$\eta_1(b_1 f_1(a_1) + ... + b_{n+1} f_{n+1}(a_1)) + ... +$$
$$+\eta_n(b_1 f_1(a_1) + ... + b_{n+1} f_{n+1}(a_n)) = 0$$

luego

$$b_1 f_1(x) + ... + b_{n+1} f_{n+1}(x) = 0.$$

Observamos que, como $(b_1, .., b_{n+1})$ es una solución no trivial, algún $b_i \neq 0$. Por lo tanto, tenemos una combinación lineal de los elementos de $\{f_1, ..., f_{n+1}\}$ no trivial igual a cero. Luego, $\{f_1, ..., f_{n+1}\}$ no es linealmente independiente, esto contradice el teorema anterior. La contradicción surge de suponer $|Gal(K \rightarrowtail L)| > [L : K]$. Se sigue que

$$|Gal(K \rightarrowtail L)| \leq [L : K].$$

♦

Definición 2.10. Diremos que una extensión $K \rightarrowtail L$ es **normal** si, dado un polinomio irreducible $f(x)$ en $K[x]$ tal que $f(x)$ tiene una raíz en L, implica que todas las raíces de $f(x)$ están en L.

Nótese que, en general, dado un polinomio $f(x) \in K[x]$, con K un campo, no necesariamente se puede factorizar en polinomios de grado 1 en $K[x]$. Por ejemplo, si consideramos x^2+1, este polinomio tiene coeficientes reales, es decir $x^2+1 \in \mathbb{R}[x]$, pero, no lo podemos ver como producto de elementos lineales de $\mathbb{R}[x]$, pues sus raíces son i,$-i$. Así, si consideramos $\mathbb{R}(i)[x]$ tenemos que x^2+1 se puede factorizar en producto de polinomios lineales, a saber, $(x-i)(x+1) = x^2+1 \in \mathbb{R}(i)[x]$. Entonces, llamaremos $\mathbb{R}(i)[x]$ el campo de descomposición del polinomio x^2+1. Definamos, en general, qué es un campo de descomposición.

Definición 2.11. Sea K un campo y $f(x) \in K[x]$. Diremos que la extensión $K \rightarrowtail L$ es un **campo de descomposición** de $f(x)$ sobre K, si:

(1) $f(x)$ se descompone en factores lineales en $L[x]$.
(2) Si M es otra extensión de K, tal que, $f(x)$ se factoriza en factores lineales en $M[x]$ y $M \subset L$, entonces $M = L$.
Equivalentemente
$L = K(a_1, ..., a_n)$ donde cada a_i es raíz de $f(x)$.

Supondremos las siguientes proposiciones:
Proposición 2.12. Consideremos K un campo y $f(x) \in K[x]$. Existe campo de descomposición de $f(x)$ sobre K y es único salvo isomorfismos.
Ver demostración en [11] página 95.

Proposición 2.13. Una extensión $K \rightarrowtail L$ es normal y finita si, y sólo si, L es campo de descomposición de algún polinomio en $K[x]$.

Ver demostración en [11] página 97.
Definición 2.14. Consideremos $f(x)$ un polinomio irreducible en $K[x]$ y L su campo de descomposición. Diremos que $f(x)$ es **separable** si no tiene raíces multiples en L e **inseparable** si no es separable.

Definición 2.15. Consideremos $K \rightarrowtail L$ es una extensión de campos y $\alpha \in L$. Decimos que α es **algebraico** sobre K, si existe un polinomio $f(x) \in K[x]$ tal que α es raíz de $f(x)$.

Definición 2.16. Sea K un campo y α algebraico sobre K. El **polinomio mínimo** $m(x) \in K[x]$ de α es el polinomio mínimo irreducible de grado menor del cual α es raíz. Lo denotaremos

$$m(x) = Irr(\alpha, K).$$

Definición 2.17. Sea $K \rightarrowtail L$ es una extensión de campos $\alpha \in L$ algebraico. Diremos que α es **separable** si $Irr(\alpha, K)$ es separable.

Definición 2.18. Si $K \rightarrowtail L$ es una extensión tal que, para todo α en L, α es separable, diremos que la extensión $K \rightarrowtail L$ es **separable.**

El siguiente resultado de Teoría de Campos, puede ser consultado en [11] página 100.

Teorema 2.19. Sea K un campo y $f(x) \in K[x]$ irreducible. Si la característica de K es cero, entonces $f(x)$ es separable sobre K.

Definición 2.20. Consideremos $K \rightarrowtail L$ una extensión finita. $K \rightarrowtail L$ es una **extensión de Galois** si $K \rightarrowtail L$ es normal y separable.

Ejemplos:

(1) Consideremos el campo $\mathbb{Q}$. Sabemos que $x^2 - 2$ es irreducible sobre $\mathbb{Q}$, ya que sus raíces de $x^2 - 2$ son $\pm\sqrt[2]{2}$, que no son racionales. $\mathbb{Q}\left(\sqrt[2]{2}\right)$ es campo de descomposición de $x^2 - 2$ sobre $\mathbb{Q}$, ya que $x^2 - 2$ se factoriza $\left(x - \sqrt[2]{2}\right)\left(x + \sqrt[2]{2}\right)$ en $\mathbb{Q}\left(\sqrt[2]{2}\right)$.

(2) Consideremos la extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}\left(\sqrt[3]{2}\right)$. Esta extensión no es campo de descomposición, ya que $x^3 - 2 \in \mathbb{Q}$ tiene una raíz $\sqrt[3]{2} \in \mathbb{Q}\left(\sqrt[3]{2}\right)$, pero las otras dos raíces de $x^3 - 2$ son complejas. Luego, no se factoriza en producto de factores lineales en $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

(3) Consideramos el polinomio $x^2 - \overline{2} \in \mathbb{Z}_3$. Este polinomio es irreducible en $\mathbb{Z}_3$, ya que ningún elemento de $\mathbb{Z}_3$ es raíz de $x^2 - \overline{2}$. Entonces, tomemos α tal que $\alpha^2 = \overline{2}$. Tenemos el conjunto $\mathbb{Z}_3(\alpha) = \{a + b\alpha | a, b \in \mathbb{Z}_3\}$. Claramente contiene a $\mathbb{Z}_3$ y es un campo con las siguientes operaciones:

$$\begin{aligned} (a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha \\ (a + b\alpha)(c + d\alpha) &= (ac + 2bd) + (ad + cb)\alpha. \end{aligned}$$

Calculando los elementos de $\mathbb{Z}_3(\alpha)$, nos queda

$$\mathbb{Z}_3(\alpha) = \left\{\overline{0}, \overline{1}, \alpha, \overline{2}\alpha, \overline{1}+\alpha, \overline{1}+2\alpha, \overline{2}+\alpha, \overline{2}+\overline{2}\alpha\right\}.$$

Como este campo es finito, pondremos su tabla de multiplicar

$(\mathbb{Z}_3(\alpha), \cdot)$	$\overline{1}$	$\overline{2}$	α	$\overline{2}\alpha$
$\overline{1}$	$\overline{1}$	$\overline{2}$	α	$\overline{2}\alpha$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2}\alpha$	α
α	α	$\overline{2}\alpha$	$\overline{2}$	$\overline{1}$
$\overline{2}\alpha$	$\overline{2}\alpha$	α	$\overline{1}$	$\overline{2}$
$\overline{1}+\alpha$	$\overline{1}+\alpha$	$\overline{2}+\overline{2}\alpha$	$\overline{2}+\alpha$	$\overline{1}+\overline{2}\alpha$
$\overline{1}+\overline{2}\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{2}+\alpha$	$\overline{1}+\alpha$	$\overline{2}+\overline{2}\alpha$
$\overline{2}+\alpha$	$\overline{2}+\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{2}+\overline{2}\alpha$	$\overline{1}+\alpha$
$\overline{2}+\overline{2}\alpha$	$\overline{2}+\overline{2}\alpha$	$\overline{1}+\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{2}+\alpha$

$(\mathbb{Z}_3(\alpha), \cdot)$	$\overline{1}+\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{2}+\alpha$	$\overline{2}+\overline{2}\alpha$
$\overline{1}$	$\overline{1}+\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{2}+\alpha$	$\overline{2}+\overline{2}\alpha$
$\overline{2}$	$\overline{2}+\overline{2}\alpha$	$\overline{2}+\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{1}+\alpha$
α	$\overline{2}+\alpha$	$\overline{1}+\alpha$	$\overline{2}+\overline{2}\alpha$	$\overline{1}+\overline{2}\alpha$
$\overline{2}\alpha$	$\overline{1}+\overline{2}\alpha$	$\overline{2}+\overline{2}\alpha$	$\overline{1}+\alpha$	$\overline{2}+\alpha$
$\overline{1}+\alpha$	$\overline{2}\alpha$	$\overline{2}$	$\overline{1}$	α
$\overline{1}+\overline{2}\alpha$	$\overline{2}$	α	$\overline{2}\alpha$	$\overline{1}$
$\overline{2}+\alpha$	$\overline{1}$	$\overline{2}\alpha$	α	$\overline{2}$
$\overline{2}+\overline{2}\alpha$	α	$\overline{1}$	$\overline{2}$	$\overline{2}\alpha$

En la tabla anterior, se observa que $x^2-\overline{2} = (x-\alpha)\left(x-\overline{2}\alpha\right)$, por lo que $\mathbb{Z}_3(\alpha)$ es el **campo de descomposición** de $x^2-\overline{2}$ sobre $\mathbb{Z}_3$. Por otro lado, $x^2-\overline{2}$ es irreducible sobre $\mathbb{Z}_3$ y como en su campo de descomposición no tiene raíces múltiples, tenemos que $x^2-\overline{2}$ es un polinomio separable.

(4) Consideremos la extensión finita $\mathbb{Q} \rightarrowtail \mathbb{Q}\left(\sqrt[2]{2}\right)$. Por **Ejemplo 1**, sabemos que $\mathbb{Q}\left(\sqrt[2]{2}\right)$ es campo de descomposición de x^2-2. Así, por **Proposición 2.13**, la extensión $\mathbb{Q} \rightarrowtail \mathbb{Q}\left(\sqrt[2]{2}\right)$ es normal.

(5) La extensión $\mathbb{R} \rightarrow \mathbb{C}$ es finita, ya que el grado de la extensión es 2. También, $\mathbb{R} \rightarrowtail \mathbb{C}$ es normal por el teorema fundamental del álgebra. Además, $\mathbb{R} \rightarrowtail \mathbb{C}$ es separable ya que cualquier polinomio con coeficientes en

un campo de característica cero es separable. Luego, la extensión $\mathbb{R} \rightarrowtail \mathbb{C}$ es de Galois.

Teorema 2.20. Sea G un grupo de n automorfismos de un campo L. Si L^G es el campo fijo de G, entonces:

$$[L : L^G] = |G| = n.$$

Demostración: Primero mostremos que $[L : L^G] \leq n = |G|$. Procederemos por contradicción. Supongamos que $[L : L^G] > n$. Entonces, existen al menos $v_1, ..., v_{n+1} \in L$ tales que $v_1, ..., v_{n+1}$ forman una base del espacio vectorial L sobre L^G.

Escribamos $G = \{f_1, ..., f_n\}$ y consideremos el siguiente sistema:

$$f_1(v_1)\, x_1 + ... + f_1(v_{n+1})\, x_{n+1} = 0$$

$$\vdots$$

$$f_n(v_1)\, x_1 + ... + f_n(v_{n+1})\, x_{n+1} = 0.$$

Nótese que el número de ecuaciones es menor que el número de incógnitas, por lo que, el sistema tiene una solución no trivial $(a_1, ..., a_{n+1})$, con algún $a_i \neq 0$, $1 \leq i \leq n+1, a_i \in L$. Consideremos el conjunto de soluciones del sistema anterior. Para cada $(a_1, .., a_{n+1})$ solución no trivial del sistema, contemos las entradas distintas de cero. Formemos el conjunto A cada número natural del conteo. Así, como A es un subconjunto de los naturales, por el principio del buen orden tiene primer elemento, sea r el mínimo de A. Entonces, r resulta ser el menor número de entradas distintas de cero. Sea

$$(a_1, .., a_{r,}0, ..., 0)$$

solución con r entradas distintas de cero.

Por otro lado, como el conjunto de soluciones no triviales del sistema forma un espacio vectorial sobre el campo L y $a_r \in L$, multiplicando la solución $(a_1, .., a_r, 0, ..., 0)$ por $a_r^{-1} \in L$, nos queda

$$\left(a_1 \cdot a_r^{-1}, ..., 1, 0..., 0\right),$$

que sigue siendo solución. Así, definiendo $b_i = a_i \cdot a_r^{-1}$, $1 \leq i \leq r$, la solución se reescribe $(b_1, ..., b_{r-1}, 1, 0, ..., 0)$.

Ahora, como G es un grupo, algún $f_j \in G$ es el elemento neutro, digamos $f_1 \in G$.

Una observación es que, en $(b_1, ..., b_{r-1}, 1, 0, ..., 0)$, algún $b_i \in L - L^G$, con $1 \leq i \leq r-1$. En efecto, si suponemos lo contrario, sustituyendo la solución $(b_1, ..., b_{r-1}, 1, 0, ..., 0)$ en la primera ecuación, obtenemos

$$f_1(v_1) b_1 + ... + f_1(v_{n+1}) b_{n+1} = 0,$$

y como f_1 es el elemento neutro de G, nos queda

$$v_1 b_1 +, ..., + v_{n+1} b_{n+1} = 0,$$

y así, tenemos una combinación lineal de los elementos de $\{v_1, ..., v_{n+1}\}$ con $b_i \in L^G$ y algún $b_i \neq 0$, lo que contradice que $\{v_1, ..., v_{n+1},\}$ sea base. Luego, algún $b_j \in L - L^G$.

Otra observación importante es que debe existir algún $f_i \in G$ tal que $f_i(b_j) \neq b_j$, ya que si suponemos lo contrario, para todo $f_i \in G$, $f_i(b_j) = b_j$ lo que implica que $b_j \in L^G$, contradiciendo nuestra observación anterior. Denotemos $\sigma = f_i$.

Mostremos que $r \geq 2$. En efecto, si suponemos que $r = 1$, en la primera ecuación del sistema, se tendría lo siguiente

$$f_1(v_1) b_1 = 0$$

con $b_1 \neq 0$. Por lo que tendríamos que $f_1(v_1) = 0$, y como f_1 es el elemento neutro de G, lo que implicaría que $v_1 = 0$ contradiciendo que $\{v_1, ..., v_{n+1}\}$ sea linealmente independiente. Por lo tanto $r \geq 2$.

Como $(b_1, ..., b_{r-1}, 1, 0, ..., 0)$ es solución del sistema, se tienen ecuaciones

$$f_i(v_1) b_1 + f_i(v_2) b_2 + ... + f_i(v_r) = 0,$$

$1 \leq i \leq n$. Entonces, aplicando el morfismo σ tal que $\sigma(a_1) \neq a_1$ a $f_i(v_1) b_1 + f_i(v_2) b_2 + ... + f_i(v_r)$, nos queda

$$\sigma(f_i(v_1)) \sigma(b_1) + ... + \sigma(f_i(v_{r-1})) \sigma(b_{r-1}) + \sigma(f_i(v_r)) = 0,$$

$1 \leq i \leq n$.

Otra observación es que $G = \{\sigma f_i | f_i \in G\}$. La contención $\subset$ se da, ya que G es cerrado bajo la composición. Para $\supset$. Si $f_j \in G$, entonces, como

G es un grupo, $\sigma^{-1} \in G$, y también, $\sigma^{-1} f_j$ por lo que $f_j = \sigma\sigma^{-1} f_j$, y así $f_j \in \{\sigma f_i | f_i \in G\}$.

De la observación anterior, tenemos que $\sigma f_i = f_j$ para alguna $1 \leq j \leq n$. Entonces, sustituyendo en

$$\sigma\left(f_i\left(v_1\right)\right)\sigma\left(b_1\right) + ... + \sigma\left(f_i\left(v_{r-1}\right)\right)\sigma\left(b_{r-1}\right) + \sigma\left(f_i\left(v_r\right)\right) = 0,$$

tenemos

$$f_j\left(v_1\right)\sigma\left(b_1\right) + ... + f_j\left(v_{r-1}\right)\sigma\left(b_{r-1}\right) + f_j\left(v_r\right) = 0,$$

y como tenemos que las ecuaciones $f_i\left(v_1\right)b_1 + f_i\left(v_2\right)b_2 + ... + f_i\left(v_r\right) = 0$ son válidas para $1 \leq i \leq n$, para la ecuación j, se tiene

$$f_j\left(v_1\right)b_1 + f_j\left(v_2\right)b_2 + ... + f_j\left(v_r\right) = 0.$$

Si sustraemos $f_j\left(v_1\right)\sigma\left(b_1\right) + ... + f_j\left(v_{r-1}\right)\sigma\left(b_{r-1}\right) + f_j\left(v_r\right)$ de $f_j\left(v_1\right)b_1 + f_j\left(v_2\right)b_2 + ... + f_j\left(v_r\right)$, obtenemos

$$f_j\left(v_1\right)\left[\sigma\left(b_1\right) - b_1\right] + ... + f_j\left(v_{r-1}\right)\left[\sigma\left(b_{r-1}\right) - b_{r-1}\right] = 0,$$

y como σ es tal que $\sigma\left(b_1\right) \neq b_1$, tenemos otra solución no trivial, ya que $\sigma\left(b_1\right) - b_1 \neq 0$. Esto contradice la minimalidad de r, ya que obtuvimos una solución no trivial del sistema con menos de r elementos distintos de cero. Se sigue que $[L : L^G] \leq n = |G|$.

Falta demostrar la igualdad. Por **Corolario 2.9**, tenemos

$$|Gal\left(K \rightarrowtail L\right)| \leq [L : K].$$

Ahora, como G es un grupo de automorfismos de L, $G \subset Gal\left(K \rightarrowtail L\right)$, así,

$$n = |G| \leq |Gal\left(K \rightarrowtail L\right)|.$$

Se sigue que

$$n = |G| \leq |Gal\left(K \rightarrowtail L\right) \leq [L : K].$$

Luego

$$|G| = [L : L^G].$$

♦

Corolario 2.22. Sea L un campo y G un grupo finito de automorfismos de L. Entonces $Gal\left(L^G \rightarrowtail L\right) = G$.

Demostración: En **Teorema 2.21** obtuvimos que

$$[L : L^G] = |G|.$$

Además, sabemos que $G \subset Gal\left(L^G \rightarrowtail L\right)$. Entonces

$$|G| \leq |Gal\left(L^G \rightarrowtail L\right)|.$$

Por **Corolario 2.9**,

$$|Gal\left(L^G \rightarrowtail L\right)| \leq [L : L^G].$$

Luego

$$|G| \leq |Gal\left(L^G \rightarrowtail L\right)| \leq [L : L^G] = |G|$$

$$|G| = |Gal\left(L^G \rightarrowtail L\right).$$

Entonces, como G es un subgrupo finito de $Gal\left(L^G \rightarrowtail L\right)$ del mismo orden de $Gal\left(L^G \rightarrowtail L\right)$, concluimos que $G = Gal\left(L^G \rightarrowtail L\right)$.♦

Corolario 2.23. La función F es inyectiva para grupos finitos y cualquier campo L.

Demostración: Sean G_1, G_2 subgrupos finitos de $Gal\,(L)$ tales que

$$L^{G_1} = L^{G_2}.$$

Por **Corolario 2.22**, se tiene

$$G_1 = Gal\left(L^{G_1} \rightarrowtail L\right)$$

$$G_2 = Gal\left(L^{G_2} \rightarrowtail L\right),$$

y como $L^{G_1} = L^{G_2}$ obtenemos $G_1 = G_2$. Luego, F es inyectiva.♦

El siguiente resultado de Teoría de Campos, que puede ser consultado en [11] página 67.

Teorema 2.24. Sean $\psi : K \to L$ un isomorfismo de campos,

$$\begin{array}{rcl} K & \rightarrowtail & K\,(\alpha) \\ L & \rightarrowtail & L\,(\beta) \end{array}$$

extensiones algebraicas simples,

$$\begin{aligned} m_{\alpha}(x) &= Irr(\alpha, K) \\ m_{\beta}(x) &= Irr(\beta, L) \end{aligned}$$

los mónicos irreducibles correspondientes, y

$$\widehat{\psi} : K[x] \to L[x]$$

el morfismo inducido por ψ. Si $\widehat{\psi}(m_{\alpha}(x)) = m_{\beta}(x)$, entonces existe un isomorfismo de campos $\phi : K(\alpha) \to L(\beta)$ tal que $\phi|_K = \psi$ y más aún $\phi(\alpha) = \beta$.

Teorema 2.25. Consideremos $K \rightarrowtail L$ una extensión de campos finita y $G = Gal(K \rightarrowtail L)$. Las siguientes afirmaciones son equivalentes

(1) $K \rightarrowtail L$ es de Galois.
(2) L es campo de descomposición de algún polinomio $f(x)$ en $K[x]$.
(3) K es el campo fijo de G.

Demostración:(1) implica (2). Como la extensión $K \rightarrowtail L$ es finita, existen $a_1, ..., a_n \in L$ tales que $K(a_1, ..., a_n) = L$, con a_i algebraico sobre K. Para cada a_i consideremos

$$g_i(x) = Irr(a_i, K).$$

Como la extensión $K \rightarrowtail L$ es separable, cada g_i es separable. Luego, g_i se descompone en L, ya que a_i es raíz de g_i y la extensión $K \rightarrowtail L$ es normal. Consideremos

$$h(x) = g_1(x) \cdots g_n(x) \in K.$$

Así, $h(x)$ es separable, ya que cada factor g_i es separable; también, $h(x)$ se descompone en L, ya que cada g_i se descompone factores lineales en L, y como cada $a_1, ..., a_n \in L$ es raíz de $h(x)$, L es campo de descomposición del polinomio separable $h(x)$.

(2) implica (3). Sea $p(x)$ un polinomio separable con coeficientes en K tal que L es campo de descomposición. Mostraremos que $K = L^G$ por inducción sobre el numero de raíces de $p(x)$ en $L - K$.

Si $n = 0$, tenemos que el número de raíces de $p(x)$ en $L - K$ es cero, entonces, $p(x)$ se factoriza en K. Así, K es campo de descomposición de $p(x)$. Luego $L = K$. Entonces

$$\begin{aligned} Gal(K \rightarrowtail L) &= Gal(L \rightarrowtail L) \\ &= \{id_L\} \end{aligned}$$

Por lo tanto $L^G = K$.

Si $n \geq 1$, nuestra hipótesis de inducción es: si $g(x)$ es un polinomio en $M[x]$ con menos de n raíces en $L - M$, entonces $L^{Gal(M \rightarrowtail L)} = M$. ($M$ es un campo entre K y L). Lo que demostraremos es: si $p(x) \in K[x]$ es un polinomio con n raíces en $L - K$, entonces $L^{Gal(K \rightarrowtail L)} = K$.

Sea $p(x) \in K[x]$ un polinomio con n raíces en $L - K$. Consideremos una factorización de $p(x)$ en polinomios irreducibles de $K[x]$,

$$p(x) = p_1(x) \cdots p_m(x).$$

Observamos que alguno de los $p_i(x)$ debe tener grado mayor que uno, ya que de lo contrario, se tendría que, $p(x)$ se descompe en factores lineales en $K[x]$. Así, obtenemos una contradicción, ya que $p(x)$ tiene raíces en $L - K$. Entonces, sin perdida de generalidad, podemos suponer que el grado de $p_1(x)$ es mayor que 1. Sean $a_1, ..., a_r$ las raíces de $p(x)$. Son distintas ya que $p(x)$ es un polinomio separable. Luego, como cada a_i es raíz de $p(x)$ y L es campo de descomposición de $p(x)$, $a_i \in L$, mas aún, $a_i \in L - K$, ya que $p_1(x)$ es irreducible sobre K.

Sabemos que $K \subset K(a_1)$. Entonces, como $p(x) \in K[x]$, $p(x) \in K(a_1)$. Luego, como L es campo de descomposición de $p(x)$ y $a_1 \in K(a_1)$ es una raíz, tenemos que $p(x)$ tiene menos de n raíces en $L - K(a_1)$. Usando la hipótesis de inducción, obtenemos

$$K(a_1) = L^{Gal(K(a_1) \rightarrowtail L)}.$$

Observación (1): Como las a_i son raíces del mismo polinomio irreducible $p_1(x)$ en K, por **Teorema 2.24**, existen isomorfismos

$$\delta_i : K(a_1) \rightarrow K(a_i),$$

tales que $\delta_i|_K = id$ y $\delta_i(a_1) = a_i$.

Como L es campo de descomposición de $p(x)$ visto como polinomio de $K(a_1)$, se sigue cada extensión es isomorfa. Luego, existen isomorfismos

$f_i : L \rightarrowtail L$ tales que $f_i|_{K(a_1)} = \delta_i$. Entonces, $f_i \in Gal\,(K \rightarrowtail L)$, ya que

$$\begin{aligned} f_i|_{K(a_1)} &= \delta_i \\ \delta_i|_K &= id \\ f_i|_K &= id. \end{aligned}$$

Ahora, mostremos que K es el campo fijo de G, es decir, $K = L^G$. La contención $K \subset L^G$, se tiene por definición de L^G.

Para la contención $K \supset L^G$, sea $y \in L^G$. Primero mostremos que $y \in K\,(a_1)$. En efecto, se tiene que $Gal\,(K\,(a_1) \rightarrowtail L) \subset Gal\,(K \rightarrowtail L)$, por la **Proposición 2.6**. Entonces, si x queda fijo bajo todos los elementos de $Gal\,(K \rightarrowtail L)$, también quedará fijo bajo todos los elementos de $Gal\,(K\,(a_1) \rightarrowtail L)$. Luego, $y \in L^{Gal(K(a_1) \rightarrowtail L)}$. Entonces, por hipótesis de inducción

$$L^{Gal(K(a_1) \rightarrowtail L)} = K\,(a_1)\,,$$

se sigue que $y \in K\,(a_1)$.

Veamos a $K\,(a_1)$ como espacio vectorial sobre K. Como $1, a_1, ..., a^{s-1}$ es una base del espacio vectorial anterior, existen escalares en K tales que

$$y = \kappa_1 + \kappa_2 a_1 + ... + \kappa_s a^{s-1}.$$

Luego, aplicando cada f_i a y, con $f_i, 1 \leq i \leq s$, las funciones de observación (1), obtenemos

$$f_i\,(y) = f_i(\kappa_1) + f_i(\kappa_2) f_i\,(a_1) + ... + f_i(\kappa_s) f_i\,(a_1)^{s-1}\,,$$

pero como $f_i \in Gal\,(K \rightarrowtail L)$, $\kappa_j \in K$, $1 \leq j \leq s$, y $f_i\,(a_1) = a_i$, se sigue que

$$f_i\,(y) = \kappa_1 + k_2(a_i) + ... + k_s(a_i)^{s-1},$$

y como $y \in L^{Gal(K \rightarrowtail L)}$, obtenemos

$$y = \kappa_1 + k_2(a_i) + ... + k_s(a_i)^{s-1}.$$

Luego

$$0 = \kappa_1 - y + k_2(a_i) + ... + k_s(a_i)^{s-1}$$

para $1 \leq i \leq s$. Consideremos el siguiente polinomio

$$h\,(x) = \kappa_1 - y + k_2(x) + ... + k_s(x)^{s-1}.$$

Por construcción, se sabe que tiene s raíces. Pero el grado de $h\,(x)$ es a lo más $s - 1$, se sigue que todos los coeficientes deben de ser cero. Así

$$h\,(x) = 0.$$

Por lo tanto,

$$\kappa_1 = y,$$

y como $\kappa_1 \in K$, entonces $y \in K$. Luego,

$$K = L^{Gal(K \rightarrowtail L)}.$$

K es el campo fijo de $Gal\,(K \rightarrowtail L)$.

(3) implica (1). Para mostrar que la extensión finita $K \rightarrowtail L$ es de Galois, necesitamos mostrar lo siguiente:

(i) $K \rightarrowtail L$ es separable

(ii) $K \rightarrowtail L$ es normal.

(i) Sea $x \in L$ cualquier elemento y escribamos a $G = \{f_1, ..., f_n\}$. Supongamos sin pérdida de generalidad que $f_1 = id_L$.

Construyamos el siguiente conjunto

$$M = \{f_i\,(a)\,|f_i \in Gal\,(K \rightarrowtail L)\}.$$

Sean $a_1, ..., a_t$ los elementos distintos de M con $a = a_1$.

Observemos que, dado $a_i \in M$, existe un l tal que $1 \leq l \leq t$ y $f_l\,(a) = a_i$. En efecto, para cualquier f_j, $1 \leq l \leq t$, se cumple que

$$f_j\,(a_i) = f_j\,(f_l\,(a)),$$

y como $Gal\,(K \rightarrowtail L) = G$ es un grupo, y $f_i f_l \in G$, existe un s tal que $1 \leq s \leq n$ y $f_i f_l = f_s$. Así obtenemos

$$f_j\,(a_i) = f_s\,(a),$$

es decir, los elementos de M sólo son permutados por los elementos de $G = Gal\,(K \rightarrowtail L)$.

Así, si consideramos

$$p\,(x) = (x - a_1)\,...\,(x - a_t)$$

y

$$f_i : L[x] \rightarrow L[x],$$

tenemos que

$$f_i\,(p\,(x)) = (x - f_i\,(a_1)\,...\,(x - f_i\,(a_t))).$$

Como los elementos de M son permutados por los elementos de $G = Gal\,(K \rightarrow L)$, se tiene que

$$f_i\left(p\left(x\right)\right) = p\left(x\right).$$

Por hipótesis, K es el campo fijo de G y $f_i\left(p\left(x\right)\right) = p\left(x\right)$ para todo $f_i \in G$. Se sigue que $p\left(x\right) \in K[x]$. Entonces, como $a_1 = a$, construimos un polinomio $p\left(x\right)$ que tiene como raíz a. Este polinomio es separable, ya que todas las raíces son distintas. Sólo falta mostrar que $p\left(x\right) = Irr\left(a, K\right)$. En efecto, sea $h\left(x\right) \in K[x]$ cualquier polinomio que tenga como raíz a, entonces

$$0 = f_i\left(h\left(a\right)\right) = h\left(f_i\left(a\right)\right) = h\left(a_i\right),$$

ya que K es el campo fijo de G. Se sigue que cada a_i, con $1 \leq i \leq t$, es raíz de $h\left(x\right)$. Luego, si consideramos en particular $h\left(x\right) = Irr\left(a, K\right)$, se tiene que $p\left(x\right) | h\left(x\right)$, y como $p\left(x\right)$ es irreducible mónico, obtenemos que $p\left(x\right) = h\left(x\right) = Irr\left(a, K\right)$. Por lo tanto, $Irr\left(a, K\right)$ es separable. Luego, la extensión $K \rightarrowtail L$ es separable.

(ii) Sea $a \in L$. Construyamos $p\left(x\right)$ de igual manera que en (i).

Sea $f\left(x\right) \in K[x]$ un polinomio irreducible tal que a sea raíz. Por la observación anterior, si a es raíz de $f\left(x\right)$, entonces todas las a_i con $1 \leq i \leq t$ son raíces de $f\left(x\right)$. Entonces $p\left(x\right) | f\left(x\right)$; también, como $f\left(x\right)$ es irreducible sobre $K[x]$ y a es raíz, se sigue que $f\left(x\right) | p\left(x\right)$. Luego, existe un $d \in K - \{0\}$ tal que

$$f\left(x\right) = d(p\left(x\right)).$$

Entonces, si $p\left(x\right)$ se descompone en factores lineales de L, $f\left(x\right)$ también se descompone en factores lineales en L. Asi $f\left(x\right)$ tiene todas sus raíces en L. Por lo tanto, la extensión $K \rightarrowtail L$, es separable.

Luego, por (i) y (ii), la extensión $K \rightarrow L$ es de Galois.♦

Lema 2.26. Consideremos $K \rightarrowtail M$ una extensión finita. Las siguientes afirmaciones son equivalentes:

(1) La extensión $K \rightarrowtail M$ es normal.

(2) Sea L una extensión de M tal que $K \rightarrowtail L$ es normal. Entonces, cualquier monomorfismo $f : M \rightarrow L$ que deja fijo a K cumple que

$$f\left(M\right) = M.$$

Demostración: (1) implica (2). Sea $f : M \rightarrow L$ un monomorfismo tal que $f|_K = id$. Mostremos que $f\left(M\right) = M$.

Sea $a \in M$. Consideremos $p(x) = Irr(a, K)$. Se tiene que

$$0 = p(a) = f(p(a)) = p(f(a)),$$

ya que los coeficientes de $p(x)$ están en K y $f|_K = id_K$. Por lo que

$$f(a) \in L$$

es una raíz de $p(x)$. Entonces, como la extensión $K \to M$ es normal, obtenemos $f(a) \in M$. Por lo tanto $f(M) \subset M$. Falta mostrar la otra contención, para esto, notamos que $f : M \to f(M)$ es lineal e inyectiva. Por el teorema de la dimensión de espacios vectoriales, se sigue

$$\dim(M) = \dim(f(M)) + \dim(N(f)).$$

Luego, como f es inyectiva, la dimensión del núcleo es cero. Entonces,

$$\dim(M) = \dim(f(M)),$$

y como M es una espacio de dimensión finita, la dimensión de $f(M)$ es finita. Además, como $f(M) \subset M$, obtenemos que $f(M) = M$.

(2) implica (1). Sea $a \in M$. Tomemos $p(x)$ tal que a sea raíz. Tenemos que la extensión $K \rightarrowtail L$ es normal, y como $M \subset L$, se sigue que $a \in L$ y $p(x)$ se descompone en factores lineales en L. Así, si consideramos $b \in L$ cualquier raíz de $p(x)$, por **Teorema 2.24,** existe un isomorfismo

$$f : K(a) \to K(b)$$

tal que $f(a) = b$ y $f|_K = id$. También, como $K \rightarrowtail L$ es normal y finita, por **Proposición 2.13**, tenemos que es campo de descomposición de algún polinomio $h(x) \in K$. Entonces, si consideramos a $h(x) \in K[a]$ ó $h(x) \in K[b]$, L es campo de descomposición de $h(x)$ visto como polinomio en $K[a]$ o $K[b]$. Luego, existe un isomorfismo

$$\delta : L \to L$$

tal que $\delta|_{K[a]} = f$. Se sigue que $\delta(a) = b$. Entonces, como $\delta|_M : M \to L$ es un monomorfismo tal que $(\delta|_M)|_K = id$, por hipótesis

$$\delta|_M(M) = M$$

y como $a \in M$, se sigue que $b = \delta|_M(a) \in M$. Por lo tanto, $b \in M$, y como b es una raíz cualquiera de $p(x)$, todas las raíces de $p(x)$ están en M.♦

Lema 2.27. Sea $K \rightarrowtail L$ una extensión. Si M es un campo entre K y L, y $f \in Gal\left(K \rightarrowtail L\right)$. Entonces

$$S\left(f\left(M\right)\right) = fS\left(M\right)f^{-1}.$$

Demostración: Primero mostremos que $S\left(f\left(M\right)\right) \supset fS\left(M\right)f^{-1}$. Sabemos que

$$fS\left(M\right)f^{-1} = \left\{f\gamma f^{-1} | \gamma \in S\left(M\right) = Gal\left(M \rightarrowtail L\right)\right\}.$$

Para esta contención, mostremos que cualquier elemento $x\prime$ de $f\left(M\right)$ permanece fijo bajo cualquier elemento $f\gamma f^{-1}$. Así obtendremos que $f\gamma f^{-1} \in Gal\left(f\left(M\right) \rightarrow L\right)$. En efecto, sea $x\prime \in f\left(M\right)$. Entonces existe algún $x \in M$ tal que $f\left(x\right) = x\prime$. Sea $f\gamma f^{-1} \in fS\left(M\right)f^{-1}$. Se sigue que

$$\left(f\gamma f^{-1}\right)\left(x\prime\right) = \left(f\gamma f^{-1}\right)\left(f\left(x\right)\right),$$

ya que $f\left(x\right) = x\prime$. Entonces, como $fS\left(M\right)f^{-1}$ es un grupo, en particular, es asociativo. Obtenemos

$$\begin{aligned}\left(f\gamma f^{-1}\right)\left(x'\right) &= \left(f\gamma f^{-1}f\right)\left(x\right)\\ &= f\gamma\left(x\right).\end{aligned}$$

Sabemos que $x \in M$ y $\gamma \in Gal\left(M \rightarrowtail L\right)$. Entonces, $\gamma\left(x\right) = x$. Sustituyendo,

$$\begin{aligned}\left(f\gamma f^{-1}\right)\left(x'\right) &= \left(f\gamma f^{\cdot 1}f\right)\left(x\right)\\ &= f\gamma\left(x\right)\\ &= f\left(x\right),\end{aligned}$$

y como $f\left(x\right) = x\prime$, se tiene que $\left(f\gamma f^{-1}\right)\left(x\prime\right) = x\prime$. Luego $x\prime \in f\left(M\right)$ permanece fijo bajo todo elemento de $fS\left(M\right)f^{-1}$. Se sigue que

$$fS\left(M\right)f^{-1} \subset Gal\left(f\left(M\right) \rightarrow L\right) = S\left(f\left(M\right)\right).$$

Para la contención $S\left(f\left(M\right)\right) \subset fS\left(M\right)f^{-1}$ ocuparemos $fS\left(M\right)f^{-1} \subset S\left(f\left(M\right)\right)$. Sustituyamos f^{-1} en el lugar de f. En consecuencia

$$f^{-1}S\left(M\right)f \subset S\left(f^{-1}\left(M\right)\right).$$

Consideremos $S(f(M))$ en lugar de $S(M)$. Obtenemos

$$f^{-1}S(f(M))f \subset S\left(ff^{-1}(M)\right).$$

Luego

$$f^{-1}S(f(M))f \subset S(M).$$

Entonces

$$S(f(M)) \subset fS(M)f^{-1}.$$

Por lo tanto

$$S(f(M)) = fS(M)f^{-1}.$$

♦

Para poder demostrar el Teorema fundamental de la Teoría de Galois tenemos que suponer el siguiente teorema que puede ser consultado en [11] página 95

Teorema 2.28. Sean $\phi : K \longrightarrow K\prime$ un isomorfismo de campos y $f(x) \in K[x]$ un polinomio. Sea L un campo de descomposición de f sobre K y sea $L\prime$ un campo de descomposición de $\phi(f)$ sobre $K\prime$. Entonces, existe un isomorfismo $\psi : L \longrightarrow L\prime$.

Teorema 2.29 (Teorema fundamental de la teoría de Galois).
Consideremos una extensión $K \rightarrowtail L$ de Galois y $G = Gal(K \rightarrowtail L)$. Entonces:

(1) $|Gal(K \rightarrowtail L)| = [L : K]$
(2) Las funciones F y S son inversas una de la otra.
(3) Si M es un campo entre L y K, entonces:
(i) $S(M) = |Gal(M \rightarrow L)| = [L : K]$
(ii) $[M : K] = \frac{|G|}{|S(M)|}$
(4) Si M es un campo entre L y K. Entonces, $M \rightarrowtail L$ es normal si, y sólo si, $Gal(M \rightarrowtail L)$ es un subgrupo normal de $Gal(K \rightarrowtail L)$
(5) Si $M \rightarrow L$ es normal, se tiene que el grupo de Galois $Gal(M \rightarrowtail L)$ es isomorfo al grupo cociente $Gal(K \rightarrowtail L)/Gal(M \rightarrowtail L)$.

Demostración: (1) Por **Teorema 2.21**, se tiene que

$$[L : L^{Gal(K \rightarrowtail L)}] = |Gal(K \rightarrowtail L)|.$$

Luego, como la extensión $K \rightarrowtail L$ es de Galois, por **Teorema 2.25**, tenemos que el campo fijo de $Gal(K \rightarrowtail L)$ es K. Sustituyendo, obtenemos

$$[L : K] = |Gal(K \rightarrowtail L)|$$

(2) Mostremos que F y S son inversas.

Demostremos que

$$F : Sub_{K \rightarrowtail L} \rightarrow Cam_{K \rightarrowtail L}$$

es suprayectiva.

Sea $M \in Sub_{K \rightarrowtail L}$. Sabemos que $K \rightarrowtail L$ es de Galois, por **Teorema 2.25**, L es campo de descomposición de algún polinomio $f(x) \in K[x]$. Pero como $K \subset M$, se sigue que $f(x) \in M[x]$. Así, L es campo de descomposición de $f(x)$ en $M[x]$, entonces, por el mismo teorema, la extensión $M \rightarrow L$ es de Galois y $M = L^{Gal(M \rightarrowtail L)}$. Por definición de F,

$$F(Gal(M \rightarrowtail L)) = M.$$

Luego, F es suprayectiva.

Ahora, ya podemos probar que son inversas una de la otra. Mostremos que

$$H = (SF)(H)$$

con $H \in Sub_{K \rightarrowtail L}$, y

$$M = (FS(M))$$

con $M \in Cam_{K \rightarrowtail L}$.

Primero demostremos que $H = (SF)(H)$. Sea $H \in Sub_{K \rightarrowtail L}$. por **Corolario 2.22,**

$$H = Gal\left(L^H \rightarrowtail L\right).$$

Por definición de F,

$$F(H) = L^H.$$

Entonces, sustituyendo $F(H) = L^H$ en $H = Gal\left(L^H \rightarrowtail L\right)$, obtenemos

$$\begin{aligned} H &= Gal(F(H) \rightarrowtail L) \\ &= S(F(H)) \\ &= (SF)(H). \end{aligned}$$

Ahora, mostremos que $M = (FS(M))$. Sea M un campo entre K y L. Cuando demostramos que F es suprayectiva, lo que observamos fue que

$M = L^{Gal(M \rightarrowtail L)}$. Por definición,

$$\begin{aligned} M &= L^{Gal(M \rightarrowtail L)} \\ &= F\left(Gal\left(M \rightarrowtail L\right)\right) \\ &= F\left(S\left(M\right)\right) \\ &= \left(FS\right)\left(M\right). \end{aligned}$$

Luego, F y S son inversa una de la otra.

(3) (i) Sea M un campo entre K y L. Cuando demostramos que F es suprayectiva, se observó que $M \rightarrowtail L$ es de Galois. Entonces, por la parte (1) de este teorema,

$$[L : M] = |Gal\left(M \rightarrowtail L\right)|,$$

y por definición, $S\left(M\right) = Gal\left(M \rightarrowtail L\right)$. Luego

$$\begin{aligned} [L : M] &= |Gal\left(M \rightarrowtail L\right)| \\ & \quad S\left(M\right). \end{aligned}$$

(ii) Por teorema de Teoría de Campos,

$$[M : K] \cdot [L : M] = [L : K].$$

Despejando a $[M : K]$

$$[M : K] = \frac{[L : K]}{[L : M]}.$$

Por (3) (i)

$$|S\left(M\right)| = [L : M].$$

Luego, por (1),

$$[L : K] = |Gal\left(K \rightarrowtail L\right)|.$$

Entonces, como

$$G = Gal\left(K \rightarrowtail L\right),$$

se sigue que

$$[M : K] = \frac{|G|}{|S\left(M\right)|}$$

(4) Sea M un campo entre K y L tal que la extensión $K \rightarrowtail M$ es normal. Probemos que $S\left(M\right)$ es normal en $G = Gal\left(K \rightarrowtail L\right)$, es decir, que para cualquier $f \in G$

$$fS\left(M\right)f^{\cdot 1} = S\left(M\right).$$

Por el **Lema 2.27**,

$$fS(M)f^{-1} = S(f(M)).$$

Para demostrar $fS(M)f^{.1} = S(M)$, es suficiente mostrar que $f(M) = M$.

Sabemos que $f : L \to L$ es un isomorfismo que deja fijo a K. Ahora, como las extensiones $K \to L$ y $K \to M$ son normales y $f : |_M : M \to L$ es un monomorfismo que deja fijo a K, por **Teorema 2.26,**

$$f(M) = M.$$

Entonces, sustituyendo en $fS(M)f^{-1} = S(f(M))$, obtenemos

$$fS(M)f^{-1} = S(M).$$

Luego, $S(M)$ es normal en G.

Supongamos que $S(M)$ es normal en $G = Gal(K \rightarrowtail L)$. Mostremos que dado cualquier monomorfismo $f : M \to L$ tal que $f|_K = id$, cumple que $f(M) = M$.

Como $K \rightarrowtail L$ es normal, también $K \rightarrowtail M$ es normal. Luego, como la extensión $K \rightarrowtail L$ es de Galois, entonces L es campo de descomposición de algún polinomio $h(x)$ en K.

Ahora, $K \subset M$ implica que $h(x) \in M[x]$. Así, L es campo de descomposición de $f(x)$ sobre $M(x)$.

Aplicando f a $h(x)$

$$f(h(x)) = h(x),$$

ya que $f|_K = id$. Entonces, $h(x) \in f(M)[x]$. Así, L también es campo de descomposición de $h(x)$ sobre $f(M)[x]$. Luego, por **teorema 2.28**, existe un isomorfismo

$$\delta : L \to L$$

tal que

$$\delta|_M = f.$$

Por lo tanto, $\delta \in G = Gal(K \rightarrowtail L)$, ya que $\delta|_M = f$ y $f|_K = id$. Además, como $S(M)$ es normal en G,

$$\delta S(M)\delta^{-1} = S(M),$$

y por **Lema 2.27,**

$$\delta S(M)\delta^{-1} = S(\delta(M)).$$

Juntando las dos igualdades, obtenemos

$$S(M) = S(\delta(M)),$$

y por el inciso (2), S es inyectiva. En consecuencia

$$M = \delta(M),$$

pero como $\delta|_M = f$,

$$M = f(M)$$

entonces, por **Lema 2.26**, como f es arbitrario y la extensión $K \rightarrowtail L$ es finita y nomal, la extensión $K \rightarrowtail M$ es normal.

(5) Sea M un campo entre K y L tal que $K \rightarrowtail M$ sea normal. Para demostrar que $Gal(M \rightarrowtail L) \cong Gal(K \rightarrowtail L)/Gal(M \rightarrowtail L)$, construiremos un homomorfismo

$$\phi : Gal(K \rightarrowtail L) \rightarrow Gal(K \rightarrowtail M)$$

que sea suprayectivo, con núcleo $Gal(M \rightarrowtail L)$. Así, por el primer teorema de isomorfismo de grupos, se tendrá

$$Gal(M \rightarrowtail L) \cong\!\!\!\!\cong Gal(K \rightarrowtail L)/Gal(M \rightarrowtail L).$$

Definamos

$$\phi : Gal(K \rightarrowtail L) \rightarrow Gal(K \rightarrowtail M)$$

$$\phi(f) = f|_M.$$

Veamos que está bien definida. Como $f|_M : M \rightarrow L$ es un monomorfismo que deja fijo a K y las extensiónes $K \rightarrowtail L$ y $K \rightarrowtail M$ son normales, por **Lema 2.26**, $f(M) = M$. Entonces, $f(M) = M$ y $f|_K = id$. Se sigue que $f|_M \in Gal(K \rightarrowtail M)$. Luego, ϕ está bien definida.

Mostremos que ϕ es homomorfismo de grupos. Sean

$$f, g \in Gal(K \rightarrowtail L).$$

Entonces

$$\phi(f \circ g) = f \circ g|_M = f|_M \circ g|_M = \phi(f) \circ \phi(g).$$

Luego, ϕ es un homomorfismo de grupos.

Observemos que ϕ es suprayectivo . Sea $f \in Gal(K \rightarrowtail M)$. Como la extensión $K \rightarrow L$ es de Galois, L es campo de descomposición del algún polinomio $h(x)$ en $K[x]$. Entonces, como $K \subset M$, se sigue que $h(x) \in M[x]$. Así, L es campo de descomposición del polinomio $h(x)$ sobre $M[x]$. Notemos que $f|_K = id$ implica $f(h(x)) = h(x)$. Luego, por la unicidad del campo de descomposición, existe $\delta : L \rightarrow L$ tal que $\delta|_M = f$. Como $K \subset M$, se sigue que $\delta|_K = f|_K = id$, es decir,

$$\delta \in Gal(K \rightarrowtail L)$$

y

$$\phi(\delta) = \delta|_M = f.$$

Por lo tanto, ϕ es suprayectiva.

Por último, calculemos el núcleo de ϕ:

$$\begin{aligned} \ker(\phi) &= \{f \in Gal(K \rightarrowtail L) \mid \ f|_M = id\} \\ &= \{f : L \rightarrow L \text{ es isomorfismo} \mid \ f|_M = id\} \\ &= Gal(M \rightarrowtail L). \end{aligned}$$

Entonces, ϕ es un homomorfismo suprayectivo con núcleo $Gal(M \rightarrow L)$. Luego, por el primer teorema de isomorfismo de grupos

$$Gal(M \rightarrowtail L) \cong Gal(K \rightarrowtail L)/Gal(M \rightarrowtail L).$$

♦

Capítulo 3

Solubilidad por radicales.

3.1 Grupos solubles.

Definición 3.1. Un grupo G es **soluble** si existe una cadena finita de subgrupos

$$e = G_0 \subset G_1 \subset ... \subset G_n = G$$

tal que cada $G_i \lhd G_{i+1}$, $0 \leq i \leq n-1$ y los cocientes G_{i+1}/G_i son abelianos.

Definición 3.2. Consideremos G un grupo. Si $a, b \in G$, definimos el **conmutador** de a, b

$$aba^{-1}b^{-1}.$$

Utilizaremos la notación $[a, b] = aba^{-1}b^{-1}$

Denotaremos con $[G, G]$ el subgrupo de G generado por los conmutadores $[a, b]$ y sus inversos con $a, b \in G$. Observamos que $([a, b])^{-1} = [b, a]$

El grupo $[G, G]$ se llama el **subgrupo conmutador** de G.

Lema 3.3. Sea G un grupo. Entonces,

(1) $[G, G]$ es un subgrupo normal de G.
(2) El grupo cociente $G/[G, G]$ es abeliano.
(3) Si M es un subgrupo normal de G, tal que G/M es abeliano, entonces $[G, G] \subset M$.

Demostración:

1) Si $x \in [G, G]$, por definición, es un producto finito de la forma

$$x = [a_1, b_1] \cdots [a_n, b_n].$$

Procederemos por inducción sobre el número de factores en el producto. Si $n = 1$, tenemos $x = [a, b]$ con $a, b \in G$. Sea $g \in G$. Entonces

$$\begin{aligned} g[a,b]g^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= gag^{-1}gbg^{-1}ga^{-1}g^{-1}b^{-1}g^{-1} \\ &= [gag^{-1}, gbg^{-1}] \in [G, G]. \end{aligned}$$

Por lo tanto $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G, G]$. En otras palabras, al conjugar el conmutador de a y b, tenemos el conmutador de gag^{-1} y gbg^{-1}.

Supongamos que, si $y \in [G, G]$ y $g \in G$ tal que

$$y = [a_1, b_1] \cdots [a_n, b_n]$$

con $a_i, b_i \in G$, $0 \leq i \leq n$. Entonces

$$gyg^{-1} = g[a_1, b_1] \cdots [a_n, b_n]g^{-1} \in [G, G]\,.$$

Demostremos que, si x es un producto de $n+1$ elementos de $[G, G]$ y $g \in G$, entonces

$$gxg^{-1} \in [G, G]$$

Sea $x \in [G, G]$ un producto de $n + 1$ conmutadores y $g \in G$. Entonces,

$$x = [a_1, b_1] \cdots [a_n, b_n] \cdot [a_{n+1}, b_{n+1}]$$

con $a_i, b_i \in G$, $0 \leq i \leq n + 1$.Notemos que

$$gxg^{-1} = g[a_1, b_1] \cdots [a_n, b_n]g^{-1} \cdot g[a_{n+1}, b_{n+1}]g^{-1}.$$

Sabemos que

$$g[a_1, b_1] \cdots [a_n, b_n]g^{-1} \in [G, G],$$

por hipótesis de inducción, además

$$g[a_{n+1}, b_{n+1}]g^{-1} \in [G, G],$$

por el caso $n = 1$. Entonces, como $[G, G]$ es un grupo, tenemos que $gxg^{-1} = g[a_1, b_1] \cdots [a_n, b_n]g^{-1} \cdot g[a_{n+1}, b_{n+1}]g^{-1} \in [G, G]$. En consecuencia, $[G, G]$ es normal en G.

(2) Sea $a \cdot [G, G]$ y $b \cdot [G, G] \in G/[G, G]$ con $a, b \in G$. Entonces

$$\begin{aligned}(a \cdot [G, G]) \cdot (b \cdot [G, G]) &= ab \cdot [G; G]. \\ &= (ab)(b^{-1}a^{-1}ba) \cdot [G, G] \text{ ya que } b^{-1}a^{-1}ba \in [G, G]. \\ &= (ba) \cdot [G, G]. \\ &= (b \cdot [G, G]) \cdot (a \cdot [G, G]) \ .\end{aligned}$$

Así, el grupo $G/[G, G]$, es abeliano.

(3) Afirmación: cualquier generador del conmutador es elemento de en M. En efecto, sea a y $b \in G$. Entonces, como $G/[G, G]$ es abeliano, tenemos

$$ab \cdot M = ba \cdot M.$$

Si multiplicamos por la clase lateral $a^{-1}b^{-1} \cdot M$ a la ecuación anterior, obtenemos:

$$(ab \cdot M) \cdot (a^{-1}b^{-1} \cdot M) = (ba \cdot M) \cdot (a^{-1}b^{-1} \cdot M).$$

Entonces

$$aba^{-1}b^{-1} \cdot M = M.$$

En consecuencia, $aba^{-1}b^{-1} \in M$.

Como M es un subgrupo de G, entonces, es cerrado bajo productos finitos de sus elementos, en particular para los elementos del conmutador. Luego $[G, G] \subset M$.♦

Una observación importante del inciso (3) , es que el conmutador de un grupo es el mínimo grupo que hace conmutativo los cocientes con respecto de la contención.

Denotemos con $G^1 = [G, G]$ y construyamos la siguiente sucesión.

$$\begin{aligned} G^2 &= [G^1, G^1] \\ G^3 &= [G^2, G^2] \\ &\vdots \\ G^{n+1} &= [G^n, G^n] \\ &\vdots \end{aligned}$$

Observaciones:
Por definición, $G^{i+1} = [G^i, G^i]$. Entonces, por **Lema 3.3**, como G^{i+1} es el subgrupo conmutador de G^i, tenemos $G^{i+1} \lhd G^i$.

Sabemos que $[G, G]$ es caracteristico en G y como $\left[G^1, G^1\right] = G^2 \lhd G^1$ entonces, $G^2 \lhd G$ (Ver Lema 5.20 de [7]) . Haciendo este paso recursivamente, se tiene

$$G^n \lhd G \text{ para toda } n \geq 0$$

En **Lema 3.3** se mostró que el cociente entre un grupo y su conmutador es abeliano. Así G^i/G^{i+1} es abeliano.
Resumiendo lo anterior, nuestras observaciones son:

1) $G^{i+1} \lhd G^i$ para $i \geq 0$
2) $G^n \lhd G$ para toda $n \geq 0$
3) G^i/G^{i+1} para es abeliano. $i \geq 0$

Dadas estas observaciones, es sencillo dar una equivalencia de la definición de grupo soluble, qué es el propósito del siguiente teorema.

Teorema 3.4. Sea G un grupo. Entonces G es soluble si, y sólo si, existe un natural n tal que $G^n = e$. (e es el elemento neutro de G).

Demostración:

Supongamos que G es soluble. Por definición, existe una cadena

$$e = G_0 \subset G_1 ... \subset G_n = G$$

tal que $G_i \lhd G_{i+1}$, $0 \leq i \leq n-1$, y los cocientes G_{i+1}/G_i son abelianos.

Entonces, como los G_{i+1}/G_i son abelianos y el conmutador de un grupo está contenido en el grupo ($[G_{i+1}, G_{i+1}] \subset G_{i+1}$), por **Lema 3.3** parte (3) , tenemos:

$G^1 = [G, G] = [G_n, G_n] \subseteq G_{n-1}$

$G^2 = [G^1, G^1] \subseteq [G_{n-1}, G_{n-1}] \subseteq G_{n-2}$
.
.
.
$G^n = [G^{n-1}, G^{n-1}] \subseteq [G_1, G_1] \subseteq G_0 = e$
Así, $G^n = e$.

Supongamos que $G^n = e$. Por las observaciones anteriores, la cadena

$$e = G^n \subseteq ... \subseteq G^1 \subseteq G^0 = G$$

cumple que $G^{i+1} \lhd G^i$ para toda $i \geq 0$ y los cocientes G^i/G^{i+1} son abelianos. Por lo tanto, G es soluble.♦

Teorema 3.5. Sea G un grupo. Entonces

(1) Si H es un subgrupo de G y G es soluble entonces, H es soluble.

(2) Si H es un subgrupo normal de G y G es soluble entonces, G/H es soluble

(3) Si H es normal en G tal que H y G/H son solubles entonces, G es soluble.

Demostración:

(1) Sea G un grupo soluble. Por **Teorema 3.1**, tenemos que

$$G^n = e.$$

Además, como $H \subseteq G$ entonces, $H^n \subseteq G^n = e$. En consecuencia $H^n = e$.

(2) Consideremos

$$\varphi : G \longrightarrow (G/H)$$

el epimorfismo canónico. Sabemos que φ suprayectivo implica $\varphi(G^n) = \varphi(G)^n$. Luego, como G es soluble, por **Teorema 3.4,** existe n tal que $G^n = e$. Así,

$$e \cdot H = \varphi(e) = \varphi(G^n) = \varphi(G)^n$$

y como $\varphi(G) = G/H$ entonces

$$e \cdot H = \varphi(G)^n = (G/H)^n.$$

Por lo tanto G/H es soluble.

(3) Sea (G/H) soluble, entonces por **Teorema 3.4,** existen un naturales n, m tales que $G/H \supseteq (G/H)^1 .... \supseteq (G/H)^n = e \cdot H$ y $H^m = e$. Tomemos φ igual que del inciso anterior. Sabemos que $(G/H)^n = e$ implica que $\varphi(G^n) = e$. Por lo tanto $G^n \subset H$. Así, $(G^n)^m = G^{m+n} = H^m = e$. Se sigue que G es soluble.

Proposición 3.6. Sea S_n, $n \geq 5$. Si N un subgrupo normal de G contiene todos los 3-ciclos de S_n, entonces $N^1 = [N, N]$ contiene todos los 3-ciclos de S_n.

Demostración: Sean $a, b, c, d, e \in S_n$, distintas, como N contiene a todos los 3-ciclos, en particular $\sigma = (abc)$ y $\tau = (ade)$ están en N. Luego

$$\begin{aligned} \sigma\tau\sigma^{-1} &= (abc)(ade)(cba)(eda) \\ &= (abd) \in N^1. \end{aligned}$$

Como $N^1 \lhd S_n$, para todo $\pi \in G$,

$$\pi(abd)\pi^{-1} \in N^1.$$

En particular, para $\pi \in S_n$ tal que

$$\begin{aligned} \pi(a) &= r \\ \pi(b) &= s \\ \pi(d) &= t \end{aligned}$$

donde r, s, t son elementos adbitrarios diferentes de S_n. Entonces, $\pi(abd)\pi^{-1} = (rst) \in N^1$ para cualquier (rst) 3-ciclo de S^n.♦

Estamos preparados para probar el resultado fundamental de esta sección.

Teorema 3.7. Si $n \geq 5$. El grupo S_n no es soluble.

Demostración: Sabemos que A_n es subgrupo normal de S_n . Entonces, por **Teorema 3.6** tenemos que $A_n^1 = [A_n, A_n]$ contiene todos los tres ciclos de S_n. Ahora como A_n está generado por todos los tres ciclos de S_n, se tiene que

$$A_n \subset A_n^1 = [A_n, A_n] .$$

Luego, como A_n es el único subgrupo de S_n obtenemos

$$A_n = A_n^1 = [A_n, A_n] .$$

haciendo lo mismo recursivamente, obtenemos

$$A_n^n = A_n \neq e.$$

Así, por **Teorema 3.4,** S_n no es soluble.♦

3.2 Extensiones ciclotómicas.

A partir de este momento trabajaremos con campos de característica cero. Supondremos el siguiente resultado que puede ser consultado en [11] página 120.

Teorema. Sea K un campo. Si G es un subgrupo finito del grupo multiplicativo $K - \{0\}$, entonces G es cíclico.

Consideremos $x^n - a \in K[x]$ y L campo de descomposición de $x^n - a$ sobre K. Como K es de característica cero el polinomio $x^n - a$, es separable, sean $\alpha_1, ..., \alpha_n$ las raíces distintas de $x^n - a$. Entonces, se tiene

$$\left(\alpha_i \alpha_j^{-1}\right)^n = (\alpha_i)^n \left(\alpha_j^{-1}\right)^n = a\,(a)^{-1} = 1.$$

Así, los elementos $\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, .., \alpha_n\alpha_1^{-1}$, son las n raíces n-ésimas de $x^n - 1$ en L. Entonces conviene primero estudiar los campos de descomposición de polinomios de la forma $x^n - 1$.

Ahora, como las raíces n-ésimas de la unidad forman un grupo finito contenido en $L - \{0\}$, por el teorema anterior se tiene que ese grupo es cíclico. Entonces, si ω es generador de ese grupo, le llamaremos una **raíz primitiva n-ésima de la unidad**.

Observación:
El polinomio $x^n - a$, se factoriza

$$(x - \alpha)(x - \alpha\omega) \cdots \left(x - \alpha\omega^{n-1}\right).$$

En efecto, como cualquiera de $\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, .., \alpha_n\alpha_1^{-1}$ es una raíz de la unidad, si ω una raíz primitiva n-ésima de la unidad entonces, $\alpha_j\alpha_1^{-1}$ es una potencia de ω. Así, reordenando si fuera necesario, tenemos lo siguiente

$$\alpha_j\alpha_1^{-1} = \omega^{j-1}.$$

Multiplicando por α_1, obtenemos que

$$\alpha_j = \alpha_1\omega^{j-1}.$$

Además, como $\alpha_1, ..., \alpha_n$ son todas las raíces de $x^n - a$ entonces, este polinomio se factoriza

$$(x - \alpha_1)(x - \alpha_1\omega) \cdots \left(x - \alpha_1\omega^{n-1}\right).$$

Luego, como α_1 es cualquier raíz de $x^n - a$, se sigue

$$(x - \alpha)(x - \alpha\omega) \cdots \left(x - \alpha\omega^{n-1}\right),$$

con α, cualquier raíz de $x^n - a$.

Observación: si $x^n - a \in K[x]$, L su campo de descomposición y ω una raíz primitiva n-ésima de la unidad. Entonces, cada automorfismo de

$Gal\left(K\left(\omega\right) \rightarrowtail L\right)$ queda determinado por su acción sobre α, con α alguna raíz de $x^n - a$. Esto es, si $\sigma \in Gal\left(K\left(\omega\right) \rightarrowtail L\right)$ entonces

$$\sigma\left(\alpha\right) = \alpha\omega^{j(\sigma)}$$

con $1 \leq j\left(\sigma\right) < n$.

En efecto, como $x^n - a$ se factoriza

$$\left(x - \alpha\right)\left(x - \alpha\omega\right) \cdots \left(x - \alpha\omega^{n-1}\right)$$

entonces $L = K\left(\alpha, \omega\right)$ es el campo de descomposición de $x^n - a$. Luego, si $\sigma \in Gal\left(K\left(\omega\right) \rightarrowtail K\left(\alpha, \omega\right)\right)$

$$\begin{aligned} \left(\sigma\left(\alpha\right)\right)^n &= \sigma\left(\alpha^n\right) \\ &= \sigma\left(a\right) \\ &= a, \end{aligned}$$

ya que α es raíz del polinomio $x^n - a$ y $a \in K$. Entonces, $\left(\sigma\left(\alpha\right)\right)$ es alguna raíz de $x^n - a$. Así, por la observación anterior

$$\sigma\left(\alpha\right) = \alpha\omega^{j(\sigma)}$$

con $1 \leq j\left(\sigma\right) < n$.

Sea

$$\rho : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$

el epimorfimos canonico. Denotaremos $\rho\left(q\right) = \overline{q}^{\mathbb{Z}_n}$ donde $q \in \mathbb{Z}$.

Teorema 3.8. Sea K un campo. Si L es campo de descomposición de $x^n - a \in K\left[x\right]$. Entonces, L contiene una raíz primitiva n-ésima de la unidad y el grupo $Gal\left(K\left(\omega\right) \rightarrowtail L\right)$ es cíclico y su orden divide a n.

Demostración: Por las observaciones anteriores, $L = K\left(\alpha, \omega\right)$ con α cualquier raíz de $x^n - a$ y ω raíz primitiva de la unidad. Sólo falta mostrar que el grupo de automorfismos es cíclico.

Definamos

$$\Pi : Gal\left(K\left(\omega\right) \rightarrowtail K\left(\omega, \alpha\right)\right) \rightarrow \mathbb{Z}_n$$

de la siguiente manera. Si $\sigma \in Gal\left(K\left(\omega\right) \rightarrowtail K\left(\omega, \alpha\right)\right)$

$$\Pi\left(\sigma\right) = \overline{j\left(\sigma\right)}^{\mathbb{Z}_n}$$

con $\sigma(\alpha) = \alpha\omega^{j(\sigma)}$.

Afirmación: Π está bien definida. Sean $\sigma, \tau \in Gal(K(\omega) \rightarrowtail K(\omega, \alpha))$ tales que $\sigma = \tau$. Por las observaciones anteriores

$$\sigma(\alpha) = \alpha\omega^{j(\sigma)}$$

$$\tau(\alpha) = \alpha\omega^{j(\tau)}.$$

Además, como $\sigma = \tau$, se sigue $j(\sigma) = j(\tau)$. Luego

$$\Pi(\sigma) = \Pi(\tau).$$

Así, Π está bien definida.

Mostremos que Π es un homomorfismo de grupos. Sean $\sigma, \tau \in Gal(K(\omega) \rightarrow K(\omega, \alpha))$. Calculemos $(\sigma \circ \tau)(\alpha)$

$$\begin{aligned}(\sigma \circ \tau)(\alpha) &= \sigma \circ \tau(\alpha) \\ &= \sigma(\tau(\alpha)) \\ &= \sigma\left(\alpha\omega^{j(\tau)}\right)\end{aligned}$$

$$\sigma\left(\omega^{j(\tau)}\right) = \omega^{j(\tau)}$$

ya que $\omega \in K(\omega)$,

$$\begin{aligned}(\sigma \circ \tau)(\alpha) &= \sigma(\alpha)\,\omega^{j(\tau)} \\ &= \alpha\omega^{j(\sigma)+j(\tau)}.\end{aligned}$$

Entonces

$$\begin{aligned}\Pi(\sigma \circ \tau) &= \overline{j(\sigma) + j(\tau)} \\ &= \overline{j(\sigma)} + \overline{j(\tau)} \\ &= \Pi(\sigma) + \Pi(\tau).\end{aligned}$$

Luego, Π es homomorfismo de grupos.

Π es inyectivo. Sea $\sigma \in Gal(K(\omega) \rightarrowtail K(\omega, \alpha))$ tal que $\Pi(\sigma) = \overline{0}$. Sabemos que dado $\tau \in Gal(K(\omega) \rightarrowtail K(\omega, \alpha))$

$$\tau(\alpha) = \alpha\omega^{j(\tau)}$$

con $0 \leq j(\tau) \leq n-1$. Se sigue que $\Pi(\sigma) = \overline{0}$ si, y sólo si, $j(\sigma) = 0$ ya que $0 \leq j(\tau) \leq n-1$. Luego, $j(\sigma) = 0$ si, y sólo si, $\sigma(\alpha) = \alpha\omega^{j(\sigma)} = \alpha$,

entonces, σ es el morfismo identidad de $Gal\left(K\left(\omega\right) \rightarrowtail K\left(\omega,\alpha\right)\right)$, se sigue que $\Pi\left(\sigma\right) = \overline{0}$ si, y sólo si, σ es el morfismo identidad. Por lo tanto Π es inyectiva. Así, $Gal\left(K\left(\omega\right) \rightarrowtail K\left(\omega,\alpha\right)\right)$ es isomorfo a un subgrupo de $\mathbb{Z}_n$. Luego $Gal\left(K\left(\omega\right) \rightarrowtail K\left(\omega,\alpha\right)\right)$ es cíclico y su orden divide a n. ♦

3.3 Extensiones radicales.

Definición 3.9. Una extensión finita $L \rightarrowtail K$ se llama una **extensión radical** si existe una torre de campos de la forma

$$K = K_0 \subset K_1 \subset ... \subset K_n = L \tag{1}$$

donde cada subextensión $K_j \rightarrowtail K_{j+1}$ se obtiene adjuntando una raíz de un polinomio $x^{n_j} - a_j$ con $a_j \in K_j$ y un entero n_j.

A una torre de la forma (1) le llamaremos una **torre radical**

Una extensión finita $K \rightarrowtail M$ se le llama **soluble por radicales** si existe una extensión radical $K \rightarrowtail L$ tal que $M \subset L$.

Definición 3.10. Sea K un campo, $f \in K[x]$ y M campo de descomposición de f. Diremos que f **es soluble por radicales** si la extensión $K \rightarrowtail M$ es soluble por radicales.

Lema 3.11. Sea $K \rightarrowtail L$ una extensión finita. Si N es la cerradura normal de $K \rightarrowtail L$. Entonces, N está generado por subcampos $L_1, ..., L_r$ que contienen a K y tales que las extensiones $K \rightarrowtail L_j$ son isomorfas a $K \rightarrowtail L$.

Demostración: Como $K \rightarrowtail L$ es finita, entonces $L = K(a_1, ..., a_n)$ con los a_j algebraicos sobre K. Ahora, para cada a_j, consideremos $\theta_j = Irr(K, a_j)$ y M el campo de descomposición de $f = \theta_1 \cdots \theta_n$. Como a_j son algunas raíces de f, tenemos que $L \subseteq M$. Luego, como M es campo de descomposición de f, la extensión $K \rightarrowtail M$ es normal y por definición de cerradura normal, $N = M$. Sea b_j cualquier raíz de θ_j, como a_j es raíz de θ_j, por **Teorema 2.24**, las extensiones $K \rightarrowtail L = K \rightarrowtail K(a_1, ..., a_j, ..., a_n)$ y $K \rightarrowtail L_j = K \rightarrowtail K(a_1, ..., b_j, ..., a_n)$ son isomorfas. Luego, si hacemos variar b_j sobre todas las raíces de θ_j, y hacemos variar j de 1 a n , generamos al campo $N = M$.♦

Observación:

En el lema anterior obtuvimos:

$$L = K \rightarrowtail K(a_1, ..., a_j, ..., a_n) \cong L_j = K \rightarrowtail K(a_1, ..., b_j, ..., a_n).$$

Si $a_1, ..., a_n \in L$ forman una torre radical sobre $K \rightarrowtail L$

$$K \subset K(a_1) \subset ... \subset K(a_1, ..., a_n) = L,$$

entonces, también los $b_1, ...b_n$ forman una torre radical

$$K \subset K\left(b_1\right) \subset ... \subset K\left(b_1, ..., b_n\right)$$

donde b_j es alguna raíz de $Irr\left(a_j, K\right)$ con $1 \leq j \leq n$.

Sea $\theta_j = Irr(a_j, K)$. Como b_j es raíz de θ_j. Mostremos que

$$\theta_j = Irr(a_j, K) = Irr(b_j, K).$$

En efecto, si suponemos que $\theta_j = Irr(a_j, K) \neq Irr(b_j, K) = \delta_j$. Como ambos son mónicos, irreducibles, únicos y b_j es raíz de θ_j tenemos que $gr(\theta_j) > gr(\delta_j)$, (no puede ser $gr(\theta_j) < gr(\delta_j)$ ya que θ_j sería un polinomio de grado menor, que se anula en b_j y esto contradice que $Irr(b_j, K) = \delta_j$.) Como K es un campo, podemos ocupar el algoritmo de la división en $K[x]$.

Para θ_j, δ_j existen f, g tales que

$$\theta_j = f\delta_j + g \ \text{ donde } gr(\delta_j) > gr(g)$$

Evaluando en b_j tenemos

$$\theta_j(b_j) = f(b_j)\delta_j(b_j) + g(b_j) = 0$$

como $\delta_j(b_j) = 0$, entonces $g(b_j) = 0$. Claramente $g = 0$ ya que de lo contrario, g sería un polinomio de grado menor que δ_j que se anula en b_j. Así, $\theta_j = f\delta_j$. Por otro lado, $gr(\theta_j) = gr(f\delta_j) = gr(f) + gr(\delta_j)$ y como $gr(\theta_j) > gr(\delta_j) \neq 0$, entonces, $1 \leq gr(f) < gr(\theta_j)$.

Luego, evaluando en a_j, tenemos $\theta_j(a_j) = f(a_j)\delta_j(a_j) = 0$. Sabemos que $\delta_j(a_j) \neq 0$ ya que de lo contrario sería un polinomio de grado menor que θ_j que se anula en a_j y esto contradice $\theta_j = Irr(a_j, K)$. Entonces, como $K\left[x\right]$ es dominio entero ya que K es un campo, tenemos que $f(a_j) = 0$, esto contradice que $\theta_j = Irr(a_j, K)$ pues f es un polinomio de grado menor que se anula en a_j. Luego, $\theta_j = \delta_j = Irr(a_j, K) = Irr(b_j, K)$.

Así, la extensión $K(b_1, ..., b_{j-1}) \rightarrowtail K(b_1, ..., b_j)$ es obtenida de adjuntar una raíz de un polinomio de la forma $x^n - a$ con $a \in K(b_1, ..., b_{j-1})$, ya que b_j es raíz del mismo polinomo que a_j, y como $Irr\,(a_j, K)$ divide a cualquier polinomio del cual a_j sea raíz, en particular, divide a $x^n - a$. Se concluye que $K \rightarrow K\,(b_1, ..., b_n)$ es una extensión radical.

Proposición 3.12. Si $K \rightarrowtail L$ es una extensión radical y N es la cerradura normal de $K \rightarrowtail L$, entonces $K \rightarrowtail N$ es radical.

Demostración: Por **Lema 3.11**, N está generada por los subcampos $L_1, .., L_n$ tales que $K \rightarrowtail L_j \cong K \rightarrowtail L$. Probemos por inducción sobre el número de subcampos que generan a N y contienen a K. Si $n = 2$, N está generado por los subcampos L_1 y L_2. Demostremos que $K \rightarrowtail N$ es radical. Por la observación anterior, cada $K \rightarrowtail L_j$ es radical. Entonces, si $a_1, ..., a_n \in L_1$ forman una torre radical sobre $K \rightarrowtail L_1$, se tiene que

$$K \subset K(a_1) \subset ... \subset K(a_1, ..., a_n) = L_1,$$

cumple que cada subextensión $K_i \rightarrow K_{i+1}$ es obtenida de adjuntar una raíz de un polinomio de la forma $x^n - a$ con $a \in K_i$.

Sean $b_1, ..., b_m \in L_2$ los que forman una torre radical sobre $K \rightarrowtail L_2$, entonces

$$K \subset K(b_1) \subset ... \subset K(b_1, ..., b_m)$$

cumple que cada subextensión $K_i \rightarrowtail K_{i+1}$ es obtenida de adjuntar una raíz de un polinomio de la forma $x^n - a$ con $a \in K_i$. Consideremos las extensiones

$$\begin{aligned} K \quad &\subset \quad K(a_1) \subset ... \subset K(a_1, ..., a_n) \subset \\ &\subset \quad K(a_1, ..., a_n, b_1) \subset K(a_1, ..., a_n, b_1, b_2) \subset .... \subset \\ &\subset \quad K(a_1, ..., a_n, b_1, ..., b_m) = N. \end{aligned}$$

Notamos que, cada subextensión $K_i \rightarrowtail K_{i+1}$ se obtiene de adjuntar una raíz de un polinomio de la forma $x^n - a$ con $a \in K_i$, ya que los a_j, b_i son raíz del mismo polinomio. En consecuencia $K \rightarrowtail N$ es radical.

Supongamos, que si M está generado por n subcampos que contienen a K, entonces $K \rightarrowtail M$ es radical. Mostremos que si $K \rightarrowtail N$ esta generado por $n + 1$ subcampos entonces, $K \rightarrowtail N$ es radical. Sean $L_1, ..., L_n, L_{n+1}$ subcampos que generan a N y contiene a K. Consideremos primero L_1, L_2.

Sean $a_1, ..., a_n, b_1, ..., b_m$ los que forman la torre radical de $K \rightarrowtail L_1$ y $K \rightarrowtail L_2$ respectivamente. Por el caso $n = 2$

$$N' = K \rightarrowtail K(a_1, ...a_n, b_1, ..., b_m)$$

es radical. Luego, considerando $N', L_3, ..., L_{n+1}$, tenemos n subcampos que generan a N y contienen a K. Así, por hipótesis de inducción, $K \rightarrowtail N$ es radical.♦

Observación: Si K es un campo y ω es raíz primitiva $n - ésima$ de la unidad, entonces $Gal\,(K \rightarrowtail K\,(\omega))$ es abeliano.

En efecto, sea $\sigma \in Gal\,(K \rightarrowtail K\,(\omega))$ y $a + b\omega$ con $a, b \in K$. Entonces, como σ es homomorfismo de campos

$$\sigma\,(a + b\omega) = a + b\sigma\,(\omega)\,.$$

Así, basta calcular $\sigma\,(\omega)$ para determinar σ. Para esto observemos que

$$\begin{aligned} \sigma\,(\omega)^n &= \sigma\,(\omega^n) \\ &= \sigma\,(1) \\ &= 1. \end{aligned}$$

Entonces, $\sigma\,(\omega)$ es una raíz $n - ésima$ de la unidad. Luego, como ω es raíz primitiva $n - ésima$ de la unidad, $\sigma\,(\omega)$ debe ser alguna potencia de ω, digamos $j\,(\sigma)$ con $1 \leq j\,(\sigma) < n$.

Mostremos que $Gal\,(K \rightarrowtail K\,(\omega))$ es abeliano.

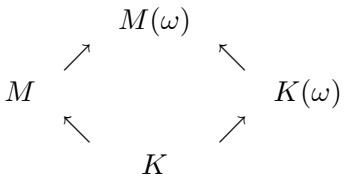
Sean $\sigma, \tau \in Gal\,(K \rightarrowtail K\,(\omega))$ y $a + b\omega \in K\,(\omega)$. Entonces

$$\begin{aligned} (\sigma \circ \tau)\,(a + b\omega) &= \sigma \circ \tau\,(a + b\omega) \\ &= \sigma \circ \tau\,(a) + \sigma \circ \tau\,(b\omega) \\ &= \sigma\,(a) + \sigma\,(b\tau\,(\omega)) \\ &= a + b\sigma\left(\omega^{j(\tau)}\right) \\ &= a + b\sigma\,(\omega)^{j(\tau)} \\ &= a + b\,(\sigma\,(\omega))^{j(\tau)} \\ &= a + b\,(\tau\,(\omega))^{j(\sigma)} \\ &= \tau \circ \sigma\,(a) + \tau \circ \sigma\,(b\omega) \\ &= \tau \circ \sigma\,(a + b\omega) \\ &= (\tau \circ \sigma)\,(a + b\omega)\,. \end{aligned}$$

Luego, $Gal\,(K \rightarrowtail K\,(\omega))$ es abeliano.

Teorema 3.13. Sea $K \rightarrowtail M$ una extensión finita, normal y radical. Entonces, $Gal(K \rightarrowtail M)$ es soluble.

Demostración: Sea m el producto de todos los primos diferentes que dividen a $n = [M : K]$ y $F = K(\omega)$ donde ω es una raíz primitiva $m-ésima$ de la unidad. Consideremos el diagrama de campos:



Sabemos que $M\,(\omega)$ es campo de descomposición de $x^m - 1$. Por **Teorema 2.25**, $M \rightarrowtail M\,(\omega)$ es de Galois. Luego, $K \rightarrowtail M(\omega)$ es de Galois, pues $K \rightarrowtail M$ es radical, finita y normal. Entonces, por el teorema fundamental de la teoría de Galois

$$Gal(K \rightarrowtail M) \cong Gal(K \rightarrowtail M(\omega))/Gal(M \rightarrowtail M(\omega)).$$

Así, si mostramos que $Gal(K\,(\omega) \rightarrowtail M(\omega))$ es soluble entonces, por **Teorema 3.5** también lo será $Gal(K \rightarrowtail M\,(\omega))$, ya que $Gal(K\,(\omega) \rightarrowtail M(\omega))$ es subgrupo de $Gal(K \rightarrowtail M(\omega))$. Además, si $Gal(K \rightarrowtail M(\omega))$ es soluble, entonces el cociente con cualquier subgrupo normal H de $Gal(K \rightarrowtail M(\omega))$ también lo será por **Teorema 3.5.** Entonces, basta mostrar que $Gal(K\,(\omega) \rightarrowtail M(\omega))$ es soluble. Ahora, como $K \rightarrowtail K(\omega)$ es campo de descomposición de $x^m - 1$, por **Teorema 2.25**, $K \rightarrowtail K(\omega)$ es de Galois, y por la observación anterior, $Gal\,(K \rightarrowtail K(\omega))$ es abeliano y por lo tanto, es soluble. Así, por el Teorema Fundamental de la Teoría de Galois

$$Gal(K \rightarrowtail K(\omega)) \cong Gal(K \rightarrowtail M(\omega))/Gal(K(\omega) \rightarrowtail M(\omega)).$$

Así, si probamos que $Gal(K(\omega) \rightarrowtail M(\omega))$ es soluble entonces, $Gal(K \rightarrowtail M(\omega))$ también lo será por **Teorema 3.5** parte (1). Entonces, basta probar que $Gal(K(\omega) \rightarrowtail M(\omega))$ es soluble. Para esto, como $K \rightarrowtail M$ es radical, existe una torre radical

$$K = L_0 \subset ... \subset L_r = M$$

donde cada subxtensión $L_i \rightarrowtail L_{i+1}$ es obtenida de adjuntar un raíz de un polinomio de la forma $x^{k_i} - a_i$ con $a_i \in L_i$. Definiendo $L_j\prime = L_j(\omega)$, se tiene una torre de extensiones

$$K(\omega) = L_0\prime \subset ... \subset L_r\prime = M(\omega)$$

que es radical, ya que cada subextensión $L_i\prime \rightarrowtail L_{i+1}\prime$, se obtiene de adjuntar una raíz de $x^{k_i} - a_i$, con $a_i \in L_i \subset L_i\prime$. Luego, como la subextensión $L_{j-1}\prime \rightarrow L_j\prime$ es de la forma $L_j\prime = L_j\prime(u_j)$ donde u_j es raíz del polinomio $x^{n_j} - a_j \in L_{j-1}\prime[x]$, entonces, como $n_j|m$ y $L_{j-1}\prime$ contiene la raíz primitiva $m-$ésima de la unidad ω, en consecuencia $L_{j-1}\prime$ contiene a la raíz primitiva n_j-énesima $\varsigma = \omega^{\frac{m}{n_j}}$. Así, $L_j\prime(u_j)$ contiene todas la raíces de $x^{n_j} - a_j$, es decir, $L_j\prime(u_j)$ es campo de descomposición de $x^{n_j} - a_j$. Luego, por **Teorema 2.25,** se tiene que la subextensión $L_i\prime \rightarrowtail L_{i+1}\prime$ es de Galois. Entonces, por **Teorema 3.8,** el grupo $Gal(L_{j-1}\prime \rightarrowtail L_j\prime)$ es cíclico y su orden divide a n_j.

Definamos

$$\begin{aligned} G_j &= Gal(L_j\prime \rightarrowtail M(\omega)) \\ G_{j-1} &= Gal(L_{j-1}\prime \rightarrowtail M(\omega)) \end{aligned}$$

Ahora, por el Teorema Fundamental de la Teoría de Galois, en la torre de campos $L_{j-1}\prime \subset L_j\prime \subset M(\omega)$, y como cada subextensión es de Galois, se sigue

$$G_j \lhd G_{j-1}$$

y como $Gal(L_{j-1}\prime \rightarrowtail L_j\prime)$ es cíclico, la sucesión de subgrupos

$$1 = Gal(L_r\prime \rightarrowtail M(\omega)) \subset ... \subset Gal(L_0\prime \rightarrowtail M(\omega)) = Gal(K(\omega) \rightarrowtail M(\omega))$$

nos dice que, $Gal(K(\omega) \rightarrowtail M(\omega))$ es un grupo soluble. Así, $Gal(K \rightarrowtail M)$ es soluble.♦

Corolario 3.14. Sea $f(x) \in K[x]$ y M campo de descomposición de $f(x)$. Si $f(x)$ es soluble por radicales, entonces $Gal(K \rightarrowtail M)$ es un grupo soluble.

Demostración: Como M es campo de descomposición de $f(x)$ entonces la extensión $K \rightarrowtail M$ es normal. Luego, como N es la cerradura normal de $K \rightarrowtail M$ y M su campo de descomposición de $f(x)$, tenemos que $M = N$. Así, por **Proposición 3.12**, $K \rightarrowtail M$ es radical, y por **Teorema 3.13**, $Gal(K \rightarrowtail M)$ es soluble. Luego, $f(x)$ es soluble por radicales.♦

3.4 El problema inverso de Galois.

Definición 3.15. Sea $\mathbb{Q} \rightarrowtail L$ una extensión. Un elemento $\alpha \in L$ es **trascendente** sobre $\mathbb{Q}$, si no existe polinomio con coeficientes en $\mathbb{Q}$ tal que α sea raíz.

Definición 3.16. Se dice que un conjunto $\{t_1, ..., t_n\}$ es **algebraicamente independiente** sobre $\mathbb{Q}$, si dado cualquier $f(x_1, ..., x_n) \in \mathbb{Q}[x_1, ..., x_n]$, se tiene que $f(t_1, ..., t_n) \neq 0$.

Supondremos los dos siguientes teoremas que pueden ser consultados en [3].

Teorema 3.17. Sea α algebraico sobre $\mathbb{Q}$. Entonces

$$e^{\alpha}$$

con e el número de Euler, es trascendente sobre $\mathbb{Q}$.

Teorema 3.18. Consideremos $\alpha_1, ..., \alpha_n$ algebraicos distintos sobre $\mathbb{Q}$. Entonces el conjunto

$$\{e^{\alpha_1}, ..., e^{\alpha_n}\}$$

es algebraicamente independiente.

La siguiente proposición se puede consultar en [11] página 56.

Proposición 3.19. Sea $K \rightarrowtail L$ una extensión y $\alpha \in L$. Si $K \rightarrowtail K(\alpha)$ es la extensión simple obtenida al adjuntar α a K. Entonces,

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in K[x] \text{ y } g(\alpha) \neq 0 \right\}$$

Corolario 3.20. Sea K un campo. Consideremos la extensión $K(t_1, ...t_n)$ con $\{t_1, ..., t_n\}$ algebraicamente independiente. Entonces, cada elemento de $K(t_1, .., t_n)$ es de la forma

$$\frac{f(t_1, ..., t_n)}{g(t_1, ..., t_n)}$$

con $f(x_1, ..., x_n), g(x_1, ..., x_n) \in K[x_1, ..., x_n]$.

Recordemos los siguiente resultados de Teoría de Campos; pueden ser consultados en [11] página 49 y 64 respectivamente.

Teorema 3.21. Sean $M \rightarrowtail L$ y $K \rightarrowtail M$ extensiones finitas. Entonces la extensión $K \rightarrowtail L$ es finita y

$$[L : K] = [L : M] \cdot [M : K]$$

Teorema 3.22. Sea K un campo y $f(x) \in K[x]$ un polinomio de grado $n \geq 1$. Entonces, si L es campo de descomposición de $f(x)$ sobre K

$$[L : K] \leq n!$$

Lo primero que vamos a ver, es cómo podemos representar a S_n como subgrupo de $Gal(K \rightarrowtail K(t_1, ...t_n))$.

Por el corolario anterior, cada elemento de $K(t_1, .., t_n)$ es de la forma

$$r = \frac{f(t_1, ..., t_n)}{g(t_1, ..., t_n)}.$$

Tomando cualquier permutación $\sigma \in S_n$, definimos $\sigma(t_j) = t_{\sigma(j)}$. Así, r queda determinado

$$\sigma(r) = \frac{f\left(t_{\sigma(1)}, ..., t_{\sigma(n)}\right)}{g\left(t_{\sigma(1)}, ..., t_{\sigma(n)}\right)}.$$

Entonces, por definición, σ es un isomorfismo en $K(t_1, ..., t_n)$ que deja fijo a K.

Observaciones:

Si definimos

$$\begin{aligned}
r_1 &: = s_1(t_1,...,t_n) = \sum_{1=i}^{n} t_i \\
r_2 &: = s_2(t_1,...,t_n) = \sum_{i<j}^{n} t_i t_j \\
r_3 &: = s_3(t_1,...,t_n) = \sum_{i<j<k}^{n} t_i t_j t_k \\
&\vdots \\
r_n &: = s_n(t_1,...,t_n) = \prod_{i=1}^{n} t_i
\end{aligned}$$

tenemos que $\sigma(r_i) = r_i$ para cualquier $\sigma \in S_n$ con nuestra definición de σ.

En efecto,

$$\begin{aligned}
\sigma(r_1) &= (t_1 + ... + t_n) \\
&= \sigma(t_1) + ... + \sigma(t_n) \\
&= t_{\sigma(1)} + ... + t_{\sigma(n)},
\end{aligned}$$

y como σ es una biyección del conjunto $\{t_1,...,t_n\}$, se tiene que

$$\sigma(r_1) = r_1.$$

Para $\sigma(r_2)$ se tiene que

$$\begin{aligned}
\sigma(r_2) &= \sigma\left(\sum_{i<j}^{n} t_i t_j\right) \\
&= \sum_{i<j}^{n} \sigma(t_i t_j) \\
&= \sum_{i<j}^{n} \sigma(t_i)\,\sigma(t_j) \\
&= \sum_{i<j}^{n} t_{\sigma(i)} t_{\sigma(j)}.
\end{aligned}$$

Luego, como σ es biyección e $i < j$, se tiene que $\sigma(i) \neq \sigma(j)$. Así, $\sigma(j) < \sigma(i)$ ó $\sigma(i) > \sigma(j)$. Haciendo esto para cada j, i, se tiene

$$\sum_{i<j}^{n} t_{\sigma(i)} t_{\sigma(j)} = \sigma(r_2).$$

Para los demás r_i es un proceso análogo. Por lo tanto,

$$\sigma(r_i) = r_i.$$

Definición 3.23. A cada r_i le llamaremos **funcion simétrica.**

Teorema 3.24. Sea K un campo y $t_1, ..., t_n$ trascendentes algebraicamente independientes. Entonces,

$$K(r_1, ..., r_n) \rightarrowtail K(t_1, ..., t_n)$$

es finita de Galois. Más aún, $K(t_1, ..., t_n)$ es campo de descomposición del polinomio

$$f(x) = x^n - r_1 x^{n-1} + ... + (-1)^n r_n$$

sobre $K(r_1, ..., r_n)$ y

$$Gal(K(r_1, ..., r_n) \rightarrow K(t_1, ..., t_n)) \approxeq S_n.$$

Demostración: Definamos

$$F = K(t_1, ..., t_n)^{S_n}.$$

Por las observaciones anteriores,

$$K(r_1, ..., r_n) \subset F$$

ya que para cualquier $\sigma \in S_n$, cumple $\sigma(r_i) = r_i$.

Por definición de r_i, el polinomio $f(x) = x^n - r_1 x^{n-1} + ... + (-1)^n r_n$, se factoriza

$$(x - t_1) \cdots (x - t_n).$$

Entonces, $K(t_1, ..., t_n)$ es campo de descomposición del polinomio

$$f(x) = x^n - r_1 x^{n-1} + ... + (-1)^n r_n$$

sobre $K(r_1, ..., r_n)$. Luego, como grad $(f) = n$, por **Teorema 3.22**

$$[K(t_1, ..., t_n) : K(r_1, ..., r_n)] \leq n!.$$

Entonces, la extensión $K(r_1, ..., r_n) \rightarrowtail K(t_1, ..., t_n)$ es finita y como $K(t_1, ..., t_n)$ es campo de descomposición del polinomio

$$f(x) = x^n - r_1 x^{n-1} + ... + (-1)^n r_n,$$

por **Teorema 2.25**, la extensión $K(r_1, ..., r_n) \rightarrowtail K(t_1, ..., t_n)$ es de Galois. Por otro lado, como S_n deja fijo a $K(r_1, ..., r_n)$, tenemos que

$$S_n \subset Gal(K(r_1, ..., r_n) \rightarrowtail K(t_1, ..., t_n)).$$

Entonces,

$$|S_n| \leq |Gal(K(r_1, ..., r_n) \rightarrowtail K(t_1, ..., t_n))|.$$

Así, como $|S_n| = n!$ y $[K(t_1, ..., t_n) : K(r_1, ..., r_n)] \leq n!$, se sigue

$$[K(t_1, ..., t_n) : K(r_1, ..., r_n)] = n!.$$

También, por **Corolario 2.22,**

$$Gal\left(K(t_1, ..., t_n)^{S_n} \rightarrowtail K(t_1, ..., t_n)\right) = S_n.$$

Luego, como

$$n! = |Gal(F \rightarrowtail K(t_1, ..., t_n))|,$$

por **Corolario 2.11**

$$|Gal(F \rightarrowtail K(t_1, ..., t_n))| \leq [K(t_1, ..., t_n) : F].$$

Sabemos

$$[K(t_1, ..., t_n) : K(r_1, ..., r_n)] = n!.$$

Entonces

$$[K(t_1, ..., t_n) : F] = n!.$$

Por lo tanto

$$[F : K(r_1, ..., r_n)] = 1.$$

Esto es

$$F = K(r_1, ..., r_n).$$

Luego

$$Gal(K(r_1, ..., r_n) \rightarrowtail K(t_1, ..., t_n)) \cong S_n.$$

♦

3.5 Solubilidad por radicales y fórmulas generales.

Ya sabemos que significa que un polinomio sea soluble por radicales, ahora veamos una relación que existe entre la solubilidad por radicales y las fórmulas generales. Esto es, dada la fórmula general, construiremos una extensión radical.

3.5.1 Extensión radical para polinomios de segundo grado.

Consideremos un polinomio de segundo grado

$$ax^2 + bx + c$$

con $a, b, c \in \mathbb{Q}$. En el primer capítulo se observó que el polinomio anterior tiene dos raíces y son:

$$\begin{aligned} x_1 &= \frac{-b + \sqrt{b^2 - 4ac}}{2a} \\ x_2 &= \frac{-b - \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

construyamos una torre de campos. Nuestro primer campo es $K = \mathbb{Q}(a, b, c)$.

Claramente

$$ax^2 + bx + c \in K.$$

Luego, observemos que

$$\left(\sqrt{b^2 - 4ac}\right)^2 \in K.$$

entonces, $\sqrt{b^2 - 4ac}$ es raíz de

$$x^2 - b^2 + 4ac$$

con $b^2 - 4ac \in K$.

Mostremos que

$$K \rightarrowtail K\left(\sqrt{b^2 - 4ac}\right)$$

es una extensión radical. Sólo falta ver que

$$K\left(\sqrt{b^2 - 4ac}\right)$$

es campo de descomposición de $ax^2 + bx + c$. En efecto,

$$2a \in K\left(\sqrt{b^2 - 4ac}\right)$$

entonces,

$$(2a)^{-1} \in K\left(\sqrt{b^2 - 4ac}\right).$$

También,

$$-b \pm \sqrt{b^2 - 4ac} \in K\left(\sqrt{b^2 - 4ac}\right).$$

Así, obtenemos que

$$(2a)^{-1} \cdot -b \pm \sqrt{b^2 - 4ac} \in K\left(\sqrt{b^2 - 4ac}\right).$$

Por lo tanto, $K\left(\sqrt{b^2 - 4ac}\right)$ es campo de descomposición de $ax^2 + bx + c$. Luego $ax^2 + bx + c$ es soluble por radicales.

3.5.2 Extensión radical para polinomios de tercer grado.

Consideremos el polinomio

$$x^3 + ax^2 + bx + c$$

con a, b y $c \in \mathbb{Q}$. En el primer capítulo se obtuvo la raíz

$$x_1 = y + z - d$$

con

$$\begin{aligned} y &= -\frac{1}{3\left(\sqrt[3]{\frac{-\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}\right)} \\ z &= \left(\sqrt[3]{\frac{-\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}\right) \\ d &= \frac{a}{3}. \end{aligned}$$

Definamos

$$w = \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}$$

y observemos que w es raíz del polinomio

$$x^2 - \frac{\beta^2}{4} - \frac{\alpha^3}{27}.$$

Tomemos

$$K_0 = \mathbb{Q}(a, b, c)$$

y

$$K_1 = K_0(w).$$

Recordando

$$z = \sqrt[3]{\frac{-\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}} = \sqrt[3]{\frac{-\beta}{2} + w}$$

con

$$\alpha = b - \frac{1}{3}a^2, \beta = -\frac{1}{3}ba + c + \frac{2}{27}a^3.$$

Así,

$$z^3 = \frac{-\beta}{2} + w$$

es raíz de $x^3 + \frac{\beta}{2} - w$.

Definamos

$$K_2 = K_1(z).$$

Sabemos

$$y = \frac{-1\alpha}{3z}.$$

Entonces, como

$$\alpha = b - \frac{1}{3}a^2, \beta = -\frac{1}{3}ba + c + \frac{2}{27}a^3,$$

se tiene que $y \in K_1$. Además, como $d = \frac{a}{3}$

$$\begin{aligned} x_1 &= \frac{1}{3\left(\sqrt[3]{\frac{-\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}\right)} + \left(\sqrt[3]{\frac{-\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}\right) - d \\ &= y + z - d \in K_1(z) = K_2. \end{aligned}$$

Así, tenemos una raíz de $x^3 + ax^2 + bx + c$. Aún hacen faltan dos raíces más. Las otra raíces son

$$y\omega^2 + z\omega$$
$$y\omega + z\omega^2$$

con ω raíz de la unidad. Así, si consideramos $K_3 = K_2(\omega)$, el polinomio

$$x^3 + ax^2 + bx + c$$

se descompone en téminos lineales en K_3.

Por construcción, la torre de campos

$$K_0 \subset K_1 \subset K_2 \subset K_3$$

cumple que cada subextensión $K_i \rightarrowtail K_{i+1}$ se obtiene de adjuntar una raíz de un polinomio de la forma $x^n - a$ con $a \in K_i$. En consecuencia, la extensión $K_0 \rightarrowtail K_3$ es una extensión radical. Además, como K_3 es campo de descomposición de $x^3 + ax^2 + bx + c$ y $x^3 + ax^2 + bx + c \in K_0$ obtenemos que, $x^3 + ax^2 + bx + c$ es soluble por radicales.

3.5.3 Extensión radical para polinomios de cuarto grado.

Consideremos el polinomio

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

con a, b, c y $d \in \mathbb{Q}$.

Recordemos que η es raíz del polinomio

$$X^3 - bX^2 + (ac - 4d)X - a^2d + 4bd - c^2.$$

Luego, ocupando la fórmula general de polinomios de tercer grado,

$$\eta = y + z - d\prime$$

donde

$$d\prime = \frac{-b}{3}$$

$$\begin{aligned} y &= -\frac{1}{3}\frac{\alpha}{z} \\ z &= \sqrt[3]{\frac{-\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}} \\ \alpha &= ac - 4d + \frac{b^3}{3} \\ \beta &= (ac - 4d)(-b) - a^2d + 4bd - c^2 - \frac{2b^3}{27}. \end{aligned}$$

Sea

$$K_0 = \mathbb{Q}(a, b, c, d).$$

Definamos

$$w = \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}.$$

Así

$$w^2 = \frac{\beta^2}{4} + \frac{\alpha^3}{27}.$$

Entonces, w es raíz del polinomio

$$x^2 - \frac{\beta^2}{4} + \frac{\alpha^3}{27}$$

con $\frac{\beta^2}{4} + \frac{\alpha^3}{27} \in \mathbb{Q}(a, b, c)$. Tomemos $K_0(w) = K_1$, la extensión

$$K_0 \to K_1$$

cumple que, w es raíz de un polinomio de la forma $x^2 - a$ con $a \in K_0$. Por otro lado,

$$z = \sqrt[3]{\frac{-\beta}{2} + w}$$

entonces, si elevamos al cubo ambos lado de la igualdad, tenemos

$$z^3 = \frac{-\beta}{2} + w.$$

Luego, z es raíz del polinomio $x^3 + \frac{\beta}{2} - w$ con $\frac{\beta}{2} - w \in K_1$.

Definamos

$$K_2 = K_1(z).$$

Como

$$y = -\frac{1}{3}\frac{\alpha}{z}$$

se sigue que $z + y \in K_2$. Así

$$\eta = y + z - d\prime$$

con

$$d\prime = \frac{a}{3}$$

cumple que

$$\eta \in K_2.$$

Por otro lado, al deducir la fórmula general de cuarto grado, se mostró que existen complejos A, B que cumplen:

$$\begin{aligned} A^2 &= \frac{1}{4}b^2 - c + \eta \\ B^2 &= -e + \frac{1}{4}\eta^2 \\ 2AB &= -d + \frac{1}{2}b\eta. \end{aligned}$$

Definamos

$$K_3 = K_2(A).$$

Observemos que A es una raíz del polinomio $x^2 - \frac{1}{4}b^2c - \eta$, con $\frac{1}{4}b^2c - \eta \in K_2$. Tomemos

$$K_4 = K_3(B).$$

Observemos que B es raíz del polinomio $x^2 + e - \frac{1}{4}\eta^2$ con $e - \frac{1}{4}\eta^2 \in K_3$. Luego, las soluciones

$$x^4 + bx^3 + cx^2 + dx + e = 0$$

son las raíces de los polinomios

$$\begin{aligned} x^2 + \frac{1}{2}bx + \frac{1}{2}\eta &= Ax + B \\ x^2 + \frac{1}{2}bx + \frac{1}{2}\eta &= -Ax - B. \end{aligned}$$

Así, usando la fórmula general para calcular las raíces de polinomios de segundo grado, obtenemos

$$\begin{aligned} x_1 &= \frac{-\left(\frac{1}{2}b - A\right) + \sqrt{\left(\frac{1}{2}b - A\right)^2 - 4\left(\frac{1}{2}\eta - B\right)}}{2} \\ x_2 &= \frac{-\left(\frac{1}{2}b - A\right) - \sqrt{\left(\frac{1}{2}b - A\right)^2 - 4\left(\frac{1}{2}\eta - B\right)}}{2} \\ x_3 &= \frac{-\left(\frac{1}{2}b + A\right) + \sqrt{\left(\frac{1}{2}b + A\right)^2 - 4\left(\frac{1}{2}\eta + B\right)}}{2} \\ x_4 &= \frac{-\left(\frac{1}{2}b + A\right) - \sqrt{\left(\frac{1}{2}b - A\right)^2 - 4\left(\frac{1}{2}\eta + B\right)}}{2}. \end{aligned}$$

Definamos

$$m = \sqrt[2]{\left(\frac{1}{2}b - A\right)^2 - 4\left(\frac{1}{2}\eta - B\right)}.$$

Luego, m es raíz del polinomio

$$x^2 - \left(\frac{1}{2}b - A\right)^2 + 4\left(\frac{1}{2}\eta - B\right)$$

con

$$\left(\frac{1}{2}b - A\right)^2 + 4\left(\frac{1}{2}\eta - B\right) \in K_4.$$

Tomemos

$$K_5 = K_4\left(m\right).$$

Entonces $x_1, x_2 \in K_5$, ya que

$$\frac{-\left(\frac{1}{2}b - A\right)}{2} \in K_5$$

y

$$\frac{\sqrt{\left(\frac{1}{2}b - A\right)^2 - 4\left(\frac{1}{2}\eta - B\right)}}{2} = \frac{m}{2} \in K_5.$$

Definamos

$$n = \sqrt{\left(\frac{1}{2}b - A\right)^2 - 4\left(\frac{1}{2}\eta + B\right)}.$$

Es claro que, n es raíz del polinomio

$$x^2 - \left(\frac{1}{2}b - A\right)^2 + 4\left(\frac{1}{2}\eta + B\right).$$

Tomemos

$$K_6 = K_5\left(n\right).$$

Entonces

$$x_3, x_4 \in K_6.$$

análogo a mostrar que $x_1, x_2 \in K_5$. Así, K_6 es campo de descomposición del polinomio

$$x^4 + ax^3 + bx^2 + cx + d.$$

Luego, la torre de campos

$$\mathbb{Q}\left(a, b, c, d\right) = K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 \subset K_5 \subset K_6$$

cumple que

$$x^4 + ax^3 + bx^2 + cx + d \in K_0\left[x\right]$$

y K_6 es campo de descomposición de

$$x^4 + ax^3 + bx^2 + cx + d.$$

Entonces, como cada subextensión $K_i \rightarrowtail K_{i+1}$ cumple ser obtenida adjuntando una raíz de un polinomio de la forma $x^n - a$ con $a \in K_i$, la extensión $K_0 \rightarrowtail K_6$ es radical. Además, como K_6 es campo de descomposición de $x^4 + ax^3 + bx^2 + cx + d$, obtenemos que los polinomios de cuarto grado en general son solubles por radicales.

3.6 El Teorema de Abel-Ruffini.

Teorema de Abel-Ruffini: Los polinomios en general de grado mayor igual que 5 no pueden ser solubles por radicales.

Demostración: Sean $t_1, ..., t_n$ trascendentes algebraicamente independientes sobre $\mathbb{Q}$, $n \geq 5$, la existencia de $t_1, ..., t_n$ la tenemos por **Teorema 3.18.** Consideremos $\mathbb{Q}(t_1, ..., t_n)$ y $\mathbb{Q}(r_1, ...r_n)$ con r_i, las funciones simétricas definidas en la sección anterior. Por **Teorema 3.24**, la extensión

$$\mathbb{Q}(r_1, ..., r_n) \rightarrowtail \mathbb{Q}(t_1, ..., t_n)$$

es finita de Galois con

$$Gal(\mathbb{Q}(r_1, ...r_n) \rightarrowtail \mathbb{Q}(t_1, ..., t_n)) \approxeq S_n.$$

Entonces, como $n \geq 5$ se tiene que, S_n no es un grupo soluble. Así, por **Teorema 3.13**, la extensión $\mathbb{Q}(r_1, ..., r_n) \rightarrowtail \mathbb{Q}(t_1, ..., t_n)$ no es radical, ya que es finita de Galois. Luego, como $\mathbb{Q}(t_1, ..., t_n)$ es campo de descomposición de

$$x^n - r_1 x^{n-1} + ... + (-1)^n r_n \in \mathbb{Q}(r_1, ..., r_n),$$

entonces

$$x^n - r_1 x^{n-1} + ... + (-1)^n r_n,$$

no es soluble por radicales. Así, los polinomios en general de grado mayor igual que 5 no pueden ser solubles por radicales.

Apéndice.

Funciones algebraicas y sus superficies de Riemann.

Una función algebraica $y = f(x)$, se define por la siguiente ecuación:

$$g_n(x)\, y^n + g_{n-1} y^{n-1} + ... + g_0 = 0$$

donde cada g_i es un polinomio. Consideraremos $g_i = x$, así aseguramos que nuestras raíces no serán complejas.

La ecuación

$$g_n(x)\, y^n + g_{n-1} y^{n-1} + ... + g_0 = 0$$

podemos considerarla como una función implicita $F(x, y) = 0$ con $x, y \in \mathbb{C}$. Sea $a \in \mathbb{C}$, tal que $F(a, y) = 0$ tiene n raíces distintas, digamos $z_1, ..., z_n$.

Entonces

$$F\prime(a, z_i) \neq 0.$$

Luego, por el Teorema de la Función Implicita, ocurre que para cualquier x, existe una vecindad u_a del punto a tal que la ecuación $F(x, y) = 0$, tiene también n soluciones distintas. Así, se definen funciones

$$f_{a,1}(x), ..., f_{a,i}(x), ..., f_{a,n}(x)$$

con dominio u_a, que pueden ser expandidas en series de Taylor convergentes en el punto a; luego, escogeremos u_a como un disco con centro en a, contenido en el disco de convergencia de estas series.

Los pares $(f_{a,i}(x),\ u_a)$ son llamados elementos analíticos de la función f. En general un elemento analítico es denotado (f_a, u_a), donde u_a es un disco con centro en a, al cual la serie de Taylor de la función f_a es convergente. Un elemento analítico puede ser prolongado. Si la ecuación

$$g_n(x)\, y^n + g_{n-1} y^{n-1} + ... + g_0 = 0$$

tiene soluciones únicas entonces, los elementos analíticos podrían ser prolongados a todo el plano complejo.

Por ejemplo, para la ecuación

$$F(x,y) = (y-x)(y-1)$$

tenemos dos elementos analíticos que se prolongan a las funciones $y = x$ y $y = 1$ sobre $\mathbb{C}$.

También, podría pasar que varias soluciones o elementos analíticos se pegasen y esto constituiría un obstáculo para la prolongación. En este ejemplo, tenemos un pegado en $x = 1$ (porque cada solución es analíticamente prolongada en este punto); pero para la ecuación $y^3 - x = 0$, la singularidad de $x = 0$ no puede ser removida de esta manera.

Sean $x_1, ..., x_n$ los puntos singulares de la función f. Tomemos el elemento analítico (f_a, u_a), $a \in \mathbb{C} - \{x_1, ..., x_n\}$, construiremos la superficie de Riemann M de la función f. Prolongamos el elemento (f_a, u_a) a lo largo de la trayectoria $\gamma \subset \mathbb{C} - \{x_1, ..., x_n\}$ con inicio en a y final en b. Cubrimos γ por medio de una cantidad finita de vecindades u_{a_i}, $a_i \in \gamma$, que son dominios de elementos analíticos (fa_i, ua_i) compatibles en las intersecciones $f_{ai} \equiv f_{ai-1}$ en $u_{a_i} \cap u_{a_{i-1}}$, y asumimos que $u_{a_0} = u_a$.

El elemento analítico final (f_b, u_b), constituye una prolongación del elemento analítico (f_a, u_a) a lo largo de la trayectoria γ.

Aquí surge la cuestión de la unicidad de la prolongación analítica. Resulta que si dos trayectorias γ^1 y γ^2 en $\mathbb{C} - \{x_1, ..., x_n\}$, con inicio en a y final en b; son homotópicas, entonces los resultados de prolongaciones a lo largo de estas trayectorias son los mismos, $f_b^1 = f_b^2$. Este es el Teorema de Monodromía.

Esto puede probarse fácilmente por convergencia de dominios barridos, cubriendo el dominio barrido con las trayectorias deformadas y usando dominios u_c de elementos analíticos .

A la superficie formada por la unión de todos los elementos analíticos obtenidos del elemento (f_a, u_a) a lo largo de todas las posibles trayectorias se le llama superficie de Riemann M de la función algebraica f. Esta superficie M es equipada con la proyección natural $\pi : M \to \mathbb{C} - \{x_1, ..., x_n\}$ que asocia al valor $f_c(x)$ su argumento x.

Para que la superficie de Riemann M sea la superficie de Riemann completa, se debe compactificar (en la topología inducida por los elementos analíticos) y suavizar las cúspides. Esto nos debería dar una superficie analítica, compacta y suave sin autointersecciones.

Ejemplo 1. Tomemos $f(x) = \sqrt{x}$

La superficie de Riemann de esta función es bien conocida. Empezamos con el punto $a = 1$ y la rama $f_a(x) = \sqrt{x}$ que es postiva en la línea real derecha. Prolongando esta rama a lo largo del círculo unitario, tenemos la rama $-f_a(x)$.

Con el fin de imaginar las superficies de Riemann en esta raíz, tomamos dos copias del plano $\mathbb{C}$ cortadas a lo largo de la mitad de la línea real negativa, ponemos una encima de la otra y pegamos los lados del corte de la hoja superior con los lados opuestos del corte de la hoja inferior. No podemos dibujarlo en una figura plana sin autointersecciones , pero cuando giramos la hoja superior, entonces podemos realizar los pegados sin autointersecciones. Esto es justamente la superficie de Riemann (sobre $\mathbb{C}^* = \mathbb{C} - \{0\}$). Notemos que esto es un homeomorfismo con $\mathbb{C}^*$. Este homeomorfismo puede ser realizado analíticamente $t \to (x, y) = (t^2, t)$, $t \in \mathbb{C}^*$.

Ejemplo 2. Tomemos $f(x) = \sqrt{x^3 - x}$.

La raíz cúbica tiene tres ceros $0, \pm 1$. Tomamos dos copias del plano cortado a lo largo de los intervalos $(-\infty, -1]$ y $[0, 1]$. Giramos la hoja superior y pegamos. Uno puede ver que M es homeomorfo con el toro T^2 menos 4 puntos. Uno de estos puntos corresponde a $x = y = \infty$.

Se puede ver fácilmente que la superficie de Riemman de la función $\sqrt[2]{x^2 - 1}$ es homeomorfa a $\mathbb{C} - \{\text{dos puntos}\}$.

Ejemplo 3. Tomemos $y^3 - y = x$

Aquí la superficie de Riemman es homeomorfa a $\mathbb{C} - \{$ dos puntos$\}$

En general, la construcción de la superficie de Riemman de una función algebraica $y = f(x)$, definida por una ecuación algebraica de grado n es la siguiente:

Sean $x_1, .., x_n$ los puntos singulares. Cortamos el plano recto a lo largo de radios que comienzan en los puntos x_i, que varían hasta el infinito y son mutuamente disjuntos. Así, tomamos n copias del plano complejo cortado de esta forma. Después, pegamos sus lados de manera que queden determinados por la variación de $f(x)$ cuando el argumento está cerca de un punto singular. Esto puede ser complicado en ejemplos concretos.

El grupo de monodromía de una función algebraica.

Consideramos una función algebraica $f(x) = y$ definida por la ecuación $F(x, y) = y^n + y^{n-1} + ... + g_0(x) = 0$ con sus puntos singulares $x_1, ..., x_n$.

Si tomamos un punto $a \in \mathbb{C} - \{x_1, ..., x_n\}$ tal que $F(a, y)$ tenga n raíces distintas, por lo visto anteriormente, se tiene que existen n elementos analíticos $(f_{a,i}(x), u_a)$ con $i = 1, ...n$. Definimos el conjunto $M_a = \{z_1, ..., z_n\}$ con los valores de las funciones en a, esto es, $f_{a,i}(a) = z_i$.

El grupo de monodromía de f es un subgrupo del grupo $S(M_a) = S_n$ de las permutaciones de M_a, que se define como sigue. Si γ es una trayectoria en $\mathbb{C}-\{x_1, ..., x_n\}$ tal que inicia y acaba en a (se les suele llamar lazos), entonces, la prolongación analítica de cualquier elemento analítico a lo largo de γ, conduce a otro elemento analítico que coincide con otro de $(f_{a,j}(x), u_a)$. En particular, se tiene que el elemento $z_i = f_{a,i}(a)$ se transforma en el elemento $z_j = f_{a,j}(a)$ y nosotros denotaremos $\Delta_\gamma(z_i) = z_j$. En la superficie, se tiene que existe una trayectoria δ_i que va desde (a, z_i) y acaba en $(a, \Delta_\gamma(z_i))$ que es un levantamiento de la trayectoria γ sobre M, es decir, $\pi(\delta_i) = \gamma$ con π la proyección natural. El mapeo $\Delta_\gamma : M_a \to M_a$ se llama la transformación de monodromía del lazo γ. El grupo generado por los mapeos Δ_γ con γ lazo, se le llama el grupo de monodromía de f y es denotado $Mon = Mon(f)$.

Por el teorema de monodromía, se tiene que, si el mapeo $\Delta\gamma$ es localmente constante en el espacio de lazos, entonces no cambia bajo una homotopía del lazo. Las clases de equivalencia de los lazos bajo la relación de equivalencia de ser homotópicos es el grupo fundamental de $\mathbb{C} - \{x_1, ..., x_n\}$ con punto base a. Este es grupo con la operación de composición de lazos. Tenemos un homomorfismo desde $\pi_1(\mathbb{C} - \{x_1, ..., x_n\})$ a $S(M_a)$ cuya imagen es $Mon(f)$.

En los **ejemplos 1 y 2**, tenemos que $M_a = \{z_1, z_2\}$ y el grupo $S(M_a) \backsimeq \mathbb{Z}/2\mathbb{Z}$ es generado por la transposición $(1, 2)$. Ahora, si γ es un lazo que rodea cualquier número de singularidades, entonces, $\Delta_\gamma = id = e$. En otro caso se tiene $(1, 2)$. Por lo tanto $Mon(f) = \mathbb{Z}/2\mathbb{Z}$

En el **ejemplo 3**, si tomamos $a = 0$, entonces $M_a = \{-1, -0, +1\}$. Si γ_1 es el camino alrededor de $x_2 = -2$, la transpocisión de los valores $z_1 = 0$ y $z_2 = 1$ es asociado, en otras palabras $\Delta_{\gamma_1} = (1, 2)$. Si γ_2 es el camino al rededor de $x_2 = 2$ la transposición de los valores $z_1 = 0$ y $z_3 = -1$ es asociado, por lo tanto $\Delta_{\gamma_2} = (1, 3)$. Entonces, se tiene que $Mon(f) = S_3$.

Recordando, $(142)(36)$ vista como pemutación, hace lo siguiente

$$\begin{array}{ccc} 1 & \rightarrow & 4 \\ 4 & \rightarrow & 2 \\ 2 & \rightarrow & 1 \\ 3 & \rightarrow & 6 \\ 6 & \rightarrow & 3 \\ 5 & \rightarrow & 5 \end{array}$$

en S_6 y también $\sigma \cdot (i_1, ..., i_j) \cdot \sigma^{-1} = (\sigma(i_1), ..., \sigma(i_k))$ para cualquier permutación σ.

Observación 1: El grupo de monodromía $Mon(f)$ puede ser identificado con un cierto grupo de Galois de una cierta extensión. Como campo incial K, nosotros tomaremos el campo $\mathbb{C}(x)$ de funciones racionales de una variable x. Aquí trataremos elementos de K, como funciones sobre u_a. Definiremos L como $K(f_{a,1}(x), ..., f_{a,n}(x))$ adjuntando las ramas de la función algebraica. Afirmación, se tiene que el grupo de automorfismos (grupo de Galois) de la extensión $K \rightarrow L$ coincide con el grupo de monodromia $Mon(f)$. En efecto, como $Mon(f)$ permuta las ramas y eso induce un automorfismo del campo $\mathbb{C}(x)$, y como los elementos de $\mathbb{C}(x)$ son de un sólo valor, entonces son invariantes bajo la monodromía. Por lo tanto $Mon(f) \subset Gal(K \rightarrow L)$.

Supongamos que $Mon(f) \neq Gal(K \rightarrow L)$, entonces, por el teorema fundamental de la teoría de Galois, sea $L_1 = L^{Mon(f)}$ el campo intermedio tal que $Gal(K_1 \rightarrow L) = Mon(f)$. El campo L_1 consiste de aquellas funciones que son invariantes con respecto de la monodromía. Por lo tanto, son funciones de un sólo valor. Es fácil ver que son racionales; multiplicando por $(x - x_i)^k$ y aplicando el teorema de Riemann sobre las singularidades removibles, implica que $L_1 = K$ y esto es una contradicción.

Suponían que la superficie de Riemann M es suave, compacta y equipada con un holomorfismo $\pi : M \rightarrow N = \mathbb{C}P^1$ llamada cubierta ramificada. El campo inicial es el campo de las funciones racionales sobre N, $K = C(N)$ el cual coincide con $C(x)$. Sin embargo la extensión del campo L es el campo de funciones racionales sobre M; aquí K está metido por $\pi^* : \varphi \rightarrow \varphi \circ \pi$. Para esta teoría es esencial el grupo $Deck = Deck_N M$ de automorfismos de la cubierta $M \rightarrow N$ que consiste de los homeomorfismos de M que preserve las fibras de la cubierta.

Para que el grupo $Deck$ sea el grupo de Galois de la extensión $K \rightarrow M$ se tiene que suponer que actúa transitivamente sobre las fibras típicas. Los

cubiertas que tienen esta propiedad son llamadas cubiertas de Galois. Las cubiertas de los **Ejemplos 1 y 2** son cubiertas de Galois, pero en **Ejemplo 3** *Deck* es trivial.

El grupo de monodromía de una función típica algebraica.

Llamaremos función algebraica típica, a la función dada por una ecuación $F(x,y) = y^n + g_{n-1}(x)y^{n-1} + ... = 0$ que satisface las siguientes condiciones:

i) La curva algebraica compleja $\Gamma = \{F(x,y) = 0\} \subset C2$ es suave y la restricción π de la proyección $(x,y) \to x$ a la curva Γ tiene sólo las singularidades más simples: puntos críticos no degenerativos con diferentes valores críticos.

ii) La curva es irreducible, es decir, la F no puede ser escrita como el producto F^1F^2 de dos polinomios.

La condición de suavidad significa que el gradiente complejo de la función F no se anula. Ya sea $F'_x \neq 0$ ó $F'_y \neq 0$. Los puntos críticos (x_i, y_i) de la proyección π son los puntos donde Γ es vertical, es decir, $F'_y = 0$. Luego, como Γ es no singular tenemos $F'_x \neq 0$, y localmente Γ es definida por la función $x - x_i = \vartheta(y)$, más aun, $\vartheta(y_i) = 0$. La condición de no degeración significa que $\vartheta'_y(yi) = -Fyy/Fx \neq 0$; solo los brazos de la función algebraica están pegados. Los valores críticos de la proyección son iguales a los x_i, esto supone que son diferentes. Bajo la condición (1), la superficie de Riemann puede ser identificada con $\Gamma - \{$ puntos criticos$\}$ y las singularidades de la función algebraica son los valores críticos de la proyección π.

La irreducibilidad de la curva algebraica compleja Γ garantiza la conectividad topológica, y también la conectividad de la superficie de Riemann $\Gamma - \{$ puntos criticos$\}$.

En efecto, si suponemos que Γ no es conexo, y con la hipótesis, entonces Γ consta de dos curvas disjuntas Γ^1, Γ^2. Sean $f_i(x)$ $i = 1, ..., k$ los brazos adecuadamente numerados de la función $y = f(x)$ que se encuentran en Γ^1 y sean $f_i(x)$ $i = k+1, ..., n$ los brazos de la otra curva. Definimos las funciones

$$F^{(1)}(x,y) = (y - f_1(x))(y - f_2(x)) \cdots (y - f_k(x))$$

y

$$F^{(2)}(x,y) = (y - f_{k+1}(x)) \cdots (y - f_n(x))$$

se tiene que $F = F^{(1)}F^{(2)}$.

Por otro lado, $\Gamma^{(i)}$ están conectados cerca de los puntos de ramificación, así las permutaciones de estas ramas de un grupo no se salen del grupo, esto significa que los coeficientes de las funciones $F^{(i)}$ son analíticos de un solo valor polinomial creciendo al infinito. Por lo tanto $F^{(i)}$ son también polinomios.

A veces, la irreducibilidad puede ser probada directamente. Por ejemplo, cuando Γ es la imagen de una curva algebraica irreducible bajo un mapeo algebraico, entonces es irreducible. Si la cerradura algebraica de Γ, sobre el plano proyectivo complejo $\mathbb{C}P^2$, es una curva suave, entonces Γ también es conexo. La última propiedad significa que el polinomio de la parte homogénea del grado más alto se factoriza en diferentes factores lineales.

Las propiedades mencionadas implican lo siguiente.

Lema 1 : Consideremos una función algebraica que cumple (1) y (2). Entonces:

(a) Mon es generado por las transposiciones (k,l) correspondientes a los intercambios de las ramas $f_k(x)$, $f_l(x)$ que se pegan en los puntos críticos (x_i, y_i).

(b) Mon actúa transitivamente sobre el conjunto $M_a = \{z_1, ..., z_n\}$. Esto es, que para cualesquiera dos valores distintos z_l, z_k existe un $\sigma \in Mon$ tal que $\sigma(z_l) = z_k$.

Demostración: La propiedad (a) es evidente, ya que cualquier transposición es generada por lazos alrededor de x_i. La propiedad (b) se sigue de la conexidad de $\Gamma - \{\text{puntos críticos}\}$. Los puntos (a, z_k) y (a, z_l) pueden ser unidos por medio de una curva real δ en Γ. Además, podemos asumir que la proyección $\gamma = \pi(\delta)$ no pasa por los puntos $x_i = \pi(x_i, y_i)$. Entonces γ cumple que es un lazo y $\Delta_\gamma(z_k) = z_l$. Así, tomamos $\Delta_\gamma = \sigma$.

Lema 2: Sea G un subgrupo de S_n tal que G es transitivo y está generado por transposiciones. Entonces, G coincide con S_n.

Demostración: Se dice que un subconjunto $A \subset \{1, ..., n\}$ es completo, si cualquier permutación de S_A puede ser prolongada a una permutación del conjunto $\{1, ..., n\}$ que está en G. Cualquier transposición (k,l) entre los generadores de G define un subconjunto completo $\{k, l\}$. Si A_0 es un subconjunto máximo completo, se tiene que $A_0 = \{1, ..., n\}$. Supongamos que A_0 es un conjunto máximo y propio. Entonces, existe una transposición $\tau = (k,l) \in G$ con $k \in A$ y $l \notin A$. Luego, el grupo generado por S_{A_0} y τ

sería igual a $S_{(A_0 \cup \{l\})}$. Así, el conjunto $A_0 \cup \{l\}$ sería completo y contiene propiamente a A_0 , por lo que, se tendría que A_0 no es maximal. ♦

Corolario: El grupo de monodromía de una función típica algebraica es igual a S_n.

Ejemplo 4. El grupo de monodromía de la función típica algebraica

$$F = 3y^5 - 25y^3 + 60y - x = 0$$

es igual a S_n.

En efecto, la condición para los puntos críticos de la proyección $\pi, F, F\prime_x = 15\left(y^2-4\right)\left(y^2-1\right) = 0$ da los cuatro puntos $(x_i, y_i) = \pm(16, 2), \pm(38, 1)$ críticos diferentes. En estos puntos la curva $F = 0$ es suave $(F\prime_x \neq 0)$ y la proyección es no degenerada $\left(F''_{yy} \neq 0\right)$. Por otro lado, la curva $F = 0$ es la imagen del plano complejo bajo un mapeo algebraico, ya que x se puede expresar en términos de y. Por lo tanto, satisface las condiciones (1) y (2).

Observaciones:

En el caso multidimensional, como los coeficientes dependen de muchos parámetros, estamos trabajando con superficies de Riemann multidimensionales. En general, se llama la ecuación universal algebraica $y^n + x_{n-1}y^{n-1} + ... + x_0 = 0$. La correspondiente superficie de Riemann es n-dimensional y constituye una doble cubierta sobre el discriminante $\sum = \{\Delta(x_0, ..., x_{n-1}) = 0\}$. El grupo fundamental de este complemento $\pi_1(C^n - \Sigma)$ es el mismo que el grupo trenzado B_n y el homomorfismo de monodromía resulta ser el mismo homomorfismo natural del grupo trenzado en S_n. Por supuesto también se tiene $Mon = S_n$.

El grupo de monodromía de una función expresada en radicales.

Si $f(x), g(x)$ son funciones algebraicas con ramas $f_1, ..., f_n, g_1, ..., g_n$ entonces, la suma $h(x) = f(x) + g(x)$ también es una función algebraica. En la esfera de Riemann se construye como sigue. Tomamos $n \cdot k$ copias del plano complejo, cortando a lo largo de radios de los puntos singulares de $f(x)$ y $g(x)$. Nosotros los llamaremos $h_{i,j}$. Después, pegamos los lados cortados usando los esquemas de pegado para las funciones f y g; significa que si después de superar un punto singular en la hoja f_{i1} pasa a la hoja f_{i2} y la hoja g_{i1} pasa a la hoja g_{i2}, entonces la hoja h_{i_1,j_1} pasa a la hoja h_{i_2,j_2}.

Análogamente, se define las funciones algebraicas y las superficies de Riemann para $g(x) - f(x)$, $g(x) f(x)$, $\frac{f(x)}{g(x)}$.

La función $h(x) = \sqrt[k]{f(x)}$ tiene kn ramas $h_{j,l}(x) = e^{2\pi ij/k} h_{0,l}(x)$ para $j = 1, ..., k-1$ $l = 1, ..., n$, donde $h_{0,l}(x)$ para $j = 0, ..., k-1$ es una rama distinguida de la raíz $\sqrt[k]{f_l(x)}$. En la construcción de estas superficies de Riemann, los puntos singulares son inicio de las funciones, obteniendo así los brazos y polos de $f_l(x)$. Entonces, tomamos n filas, cada una copia de k planos cortados. El pegado de los lados en este caso es similar al caso de la suma; si después, de pasar una singularidad x_i, f_{l1} pasa a f_{l2} entonces los cortes de las hojas desde la fila $l_1 th$ están pegadas con los cortes de las hojas desde la fila $l_2 th$, más aún, el número de hojas en las filas sufren un cambio cíclico (que es trivial cuando $f_{l_i} = 0, \infty$) .

Decimos que una función algebraica de una variable es representada en radicales si puede ser obtenida de las funciones constantes $x \to a$ y la función identidad x, por medio de las operaciones antes mencionadas.

Teorema 2: El grupo de monodromía de cualquier función algebraica representada en radicales es soluble.

Con este teorema podemos demostrar el Teorema de Abel-Ruffini, ya que hay ecuaciones algebraicas que no son solubles por radicales. El ejemplo siguiente lo muestra.

Ejemplo. La ecuación $F = 3y^5 - 25x^3 + 60 - x = 0$ no puede ser expresada en radicales.

Prueba de teorema 2. Es suficiente mostrar que si los grupos $Mon(f)$ y $G = Mon(g)$ son solubles, entonces los grupos $Mon(f \pm g), Mon(fg), Mon(f/g)$ y $Mon(\sqrt[k]{f})$ son solubles. Recordando la construcción de la superficie de Riemann de la función $f + g$, tomemos primero hk copias del plano complejo cortado, pegado de los bordes. Luego tenemos el pegado de todas las hojas con los mismos valores de las ramas $h_{ij} = f_i + g_i$. Por tanto, en el primer paso tenemos una cierta superficie M' cuyo grupo de monodromía es isomorfo con un subgrupo I del grupo $F \times G$ (eso puede ser un subgrupo apropiado, cuando algunas singularidades de f y g coinciden $Mon(\sqrt{x}) = \mathbb{Z}/2\mathbb{Z}$, $Mon(\sqrt[4]{x}) = \mathbb{Z}/4\mathbb{Z}$, pero $Mon(\sqrt{x} + \sqrt[4]{x})$ es cíclico en orden 4).

Cuando pegamos algunas hojas en el segundo paso, algunos elementos del grupo F, los que permutan las hojas pegadas, son expedidos para una transformación trivial desde el grupo de monodromía H. Además, cualquier

elemento desde H (inducido por un lazo en el $x-plano$) es una imagen de un elemento desde I, eso es imagen de la permutación de la fibra M'_a, inducida por el mismo camino. Por lo tanto, tenemos un homomorfismo suprayectivo $I \to H$. Ahora eso es suficiente para usar los puntos (a), (b), (c) de **Lema 3**.

.

Bibliografía.

[1]Aceff, F; Lluis-Puebla, E. Teoría de Galois, un primer curso, Tercera edición. Sociedad Matemática Mexicana. (2016).

[2]Baker, A. An Introduction to Galois Theory. School of Mathematics and Statistics. University of Glasgow. (2013).

[3]Baker, A. Transcendental Number Theory. Cambridge University Press. (1975).

[4]Bravo, A. Rincón, H. Rincón, C. Álgebra Superior. Facultad de Ciencias, UNAM. (2012)

[5]Burger, E. Tubbs R. Making Transcendence Transparent. Springer Science Bussiness Media Inc. (2004).

[6]Masser, D. Auxiliary Polinomials in Number Theory. Cambridge University Press. (2016).

[7]Rotman, J. An Introduction to the Theory of Groups Fourth Edition. Springer-Verlag (1994).

[8]Rotman, J. Galois Theory. Springer-Verlag, (1990)

[9]Van der Waerden, B. L. A History of Algebra: From al-Khwārizmī to Emmy Noether. New York: Springer-Verlag, pp. 85-88, 1985.

[10]Wells, D. The Penguin Dictionary of Curious and Interesting Numbers. Middlesex, England: Penguin Books, p. 59, 1986.

[11]Zaldívar, F. Teoría de Galois, ANTHROPOS, México (1996).

[12]Zoladek, H. The Topological Proof of Abel-Ruffini Theorem, Topological Methods in Nonlinear Analisis, Volume 16. (2000).

Agradecimientos.

A mis padres Salomón y Alejandra, a mi abuela Amalia y a mi hermana Alejandra por el apoyo y motivación que me han dado durante toda mi vida y que sin ellos no hubiera llegado a donde me encuentro.

A mi tios Rosario y Eusebio.

A todos mis profesores en especial a Ruben Antonio Molina Hernandez quien me impulsó a estudiar esta bella arte llamada matemática, a Ana Irene, a Emilio Lluis Puebla por ser mi guía en este este proyecto sus correciones y su paciencia.

A mi gran amigo Alan Cordero que estuvo durante toda la carrera en la buenas y malas, a mi novia Andrea por todas las experiencias que hemos vivido, a mi amiga Xochitl por todo lo que hemos compartido, a mis amigos Gilberto, Rodrigo, Ismael, Andres, Juan, Emanuel, Adrian y a todos mis amigos que he conocido a lo largo de mi vida.