Sobre extensiones radicales simples y el teorema de Abel

Edson Jair Suárez Porras

Trabajo de Grado para optar al título de Matemáticas

Director

Héctor Edonis Pinedo Tapia

Doctor en Ciencias

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Matemáticas

Bucaramanga

2021

Agradecimientos

En primer lugar quiero dar las gracias a Dios por darme la vida, la inteligencia, el estudio y tantas cosas que me brinda a diario que me ayudan a crecer cada día como persona.

Estoy muy feliz de haber conocido a los profesores que estuvieron conmigo a lo largo de mi vida, tanto en el colegio como en la universidad, de cada uno de ellos aprendí grandes cosas y me apoyaron en todo lo que podían. A ellos muchas gracias por compartirme su conocimiento y en especial doy las gracias a mi director de tesis Héctor Edonis Pinedo Tapia por su compromiso, paciencia, sugerencias y por confiar en mi para este trabajo. A mis familiares y amigos que de una u otra manera estuvieron allí para apoyarme y ayudarme a salir adelante en todo lo que se me presentaba.

En especial quiero agradecer a mis padres, Yaneth y Benjamín quienes me apoyaron, formaron y estuvieron siempre presentes, a ellos les dedico este trabajo.

Tabla de Contenido

Resumen

Título: Sobre extensiones radicales simples y el teorema de Abel. [*]

Autor: Edson Jair Suárez Porras [**]

Palabras Clave: Grupo soluble, grupo Galois, soluble por radicales.

Descripción: Un problema asociado al Álgebra y especialmente a las ecuaciones de grado n, es la búsqueda de sus raíces que, consiste en encontrar valores tal que al evaluarlos en dicha ecuación, da como resultado cero; y más aún, como obtener una fórmula para encontrar todas sus raíces. Si tal fórmula existe, se dice que la ecuación se puede resolver por radicales.

Este trabajo se caracteriza por estudiar las ecuaciones de grado $n \geq 5$ y demostrar que dichas ecuaciones no tienen solución por radicales. En las primeras secciones se habla de grupos solubles y se recuerdan algunos resultados sobre grupos y cuerpos. Se estudian las extensiones radicales simples y los cuerpos intermedios que existen entre el cuerpo y su extensión radical. Se relaciona el grado de dichas extensiones intermedias con los divisores del grado de la extensión radical, a través del estudio de polinomios irreducibles en la extensión radical.

En las últimas secciones se enuncian y se demostraran resultados sobre extensiones radicales y sobre el grupo Galois de una ecuación general de grado n. Lo cual facilita la demostración del Teorema de Abel que nos dice: "La ecuación general de grado n no puede resolverse mediante radicales para $n \geq 5$".

---

[*] Tesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Ciencias.

Abstract

Title: Over simple radcial extensions and Abel's theorem [*]

Author: Edson Jair Suárez Porras [**]

Keywords: Solvable group, Galois group, solved by radicals.

Description: A problem related with the Algebra and particularly equations of degree n, is the search for its roots, which consists of finding values such that when evaluating them in said equation, as a result zero, and even more, how to get a formula to find all roots. If that formula exists, then the equation can be solved by radicals.

In this dissertation is going to be studied the equations of degree $n \geq 5$ and show that these equations have no solution by radicals. In the first sections, we will talk about soluble groups and recall some results about groups and fields. Are studied the simple radical extensions and the intermediate fields that exists between the field and its radical extension. The degree of these intermediate extensions is related to the divisors of the degree of the radical extension, as a result of the study of irreducible polynomials in radical extension.

In the last sections, will be enunciated and demostrated results on radical extensions and Galois group of a general equation of degree n which will facilitate the proof of Abel's Theorem thah tells us:"the general equation of degree n cannot be solved by radicals for $n \geq 5$".

---

[*] Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Ciencias.

Introducción

A lo largo de los años, uno de los estudios más importantes e interesantes sobre polinomios ha sido el estudio de sus raíces; dicho problema consiste en encontrar los puntos tal que su evaluación en el polinomio es igual a cero. En particular, se conocen fórmulas para encontrar las raíces de polinomios (ecuaciones) de grado $1, 2, 3$ e incluso 4. Estas fórmulas se llaman soluciones por radicales de la ecuación. Pero, ¿qué pasa para los polinomios cuyo grado es mayor que 4? ¿Qué sabemos de ellos? Podemos decir que de estos polinomios conocemos muchas propiedades gracias a dos jóvenes matemáticos: Niels Henrik Abel (5 de agosto de 1802 - 6 de abril de 1829) y Évariste Galois (25 de octubre de 1811 - 31 de mayo de 1832).

En el intento de encontrar estas soluciones por radicales, Gauss encontró la solución de la ecuación ciclotómica $x^m - 1 = 0$, donde $m \in \mathbb{N}$. Además, mostró que todo polinomio con coeficientes reales es el producto de factores de grado uno y dos, de donde se deriva el teorema fundamental del álgebra.

Abel envió una carta a Gauss, en la cual decía que podía demostrar la imposibilidad de resolver por radicales el caso general de la ecuación de grado cinco, aunque no le hizo mucho caso. Abel publicó en 1824 un panfleto titulado "Mémoire sur les équations algébriques"[1], donde

---

[1] Memoria sobre las ecuaciones algebraicas.

demostraba que resolver el caso general de la ecuación de grado cinco por radicales era imposible.

Por otro lado, Évariste Galois encontró una forma de determinar cuales ecuaciones de cualquier grado pueden resolverse por radicales, creando así el teorema de Galois:
Una ecuación es resoluble por radicales si, y sólo si, su grupo de Galois es resoluble.

Dando paso así a la creación de la teoría de grupos.

1. Grupos

En este capítulo enunciaremos definiciones y resultados sobre los grupos. A menos que se diga lo contrario la operación de grupo va a ser por concatenación, es decir, la notación multiplicativa. Podemos ver (Lezama, 2019b) y (John and Sons, 1975).

Definición 1.1. *Dado n entero positivo, denotamos por S_n el conjunto formado por todas las aplicaciones biyectivas del conjunto $I_n = \{1,2,3,...,n\}$ en si mismo, entonces S_n es un grupo con respecto a la composición.*
Para el caso de $n = 3$, tenemos que:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Definición 1.2. *Sea σ un elemento de S_n. Se dice que σ es un ciclo de longitud m, ($1 \leq m \leq n$), si existen $a_1, a_2, ..., a_m$ elementos diferentes de I_n tales que:*

1. $\sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1$.

2. $\sigma(x) = x$ *para* $x \notin \{a_1, a_2, ..., a_m\}$.

Se denota a σ *por:*

$$\sigma = (a_1a_2\cdots a_m) = (a_2a_3\cdots a_ma_1) = (a_3a_4\cdots a_ma_1a_2) = \cdots = (a_ma_1a_2\cdots a_{m-1}).$$

Definición 1.3. *Para* $n \geq 2$*, los ciclos de longitud 2 de* S_n *se conocen como transposiciones y se denotan por* σ_{ij}*, indicando que* $\sigma(i) = j$*,* $\sigma(j) = i$ *y* $\sigma(x) = x$ *donde* $x \neq i, j$*.*

Las transposiciones juegan un papel importante en la estructura de S_n, en efecto tenemos el siguiente resultado.

Teorema 1.4. *Cada permutación de* S_n *es representable como un producto finito de transposiciones. En particular,* S_n *es generado*[2] *por las transposiciones.*

Observación. *La representación de una permutación como producto de transposiciones no es única:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = (12435) = (51)(31)(41)(21) = (12)(52)(32)(42).$$

Definición 1.5. *Sea* G *un grupo y sea* X *un subconjunto de* G*, el subgrupo generado por* X *se denota por* $\langle X \rangle$ *y a* X *se le llama un conjunto de generadores de* $\langle X \rangle$*, donde*

$$\langle X \rangle = \left\{ x_1^{k_1} * \cdots * x_n^{k_n} \mid x_i \in X,\ k_i \in \mathbb{Z},\ 1 \leq i \leq n \right\}$$

---

[2] ver Definición 2.6

Definición 1.6. *Sea G un grupo cualquiera. Se dice que G es cíclico, si existe un elemento a en G tal que* $\langle a \rangle = G$.

Ejemplo 1.7. $\mathbb{Z}$ *es un grupo cíclico y en general todo subgrupo de un grupo cíclico es cíclico.*

Definición 1.8. *Sea G un grupo cualquiera y sean* a, b *elementos de G. Se denomina conmutador de los elementos a y b al elemento* (a,b) *de G definido por*

$$(a,b) := a^{-1}b^{-1}ab.$$

Se llama conmutador de G o subgrupo derivado de G al subgrupo generado por los conmutadores y se denota por G' *o también por* (G,G)*:*

$$G' = (G,G) := \langle (a,b) \mid a \in G,\ b \in G \rangle .$$

En general si $L, M \subseteq G$ *no vacíos. Se denomina el conmutador mutuo, o conmutante de L y M, al subgrupo*

$$(L,M) := \langle (a,b) \mid a \in L,\ b \in M \rangle .$$

Ejemplo 1.9. *Si G es un grupo abeliano, tenemos:*

$$(a,b) = a^{-1}b^{-1}ab = a^{-1}ab^{-1}b = ee = e, \text{ así } G' = \langle e \rangle .$$

Definición 1.10. *Sea G un grupo y* $H \neq \varnothing$ *un subconjunto de G. Se dice que H es un subgrupo de*

G si H bajo la operación $*$ tiene estructura de grupo. en tal caso se escribe $H \leq G$.

Definición 1.11. *Sea G un grupo*

1. *Si $H \leq G$. Se dice que H es un subgrupo normal de G, lo cual denotamos por $H \trianglelefteq G$, si H cumple la siguiente condición:*

$$\forall x \in G, \forall h \in H : x^{-1}hx \in H.$$

2. *Si $H \trianglelefteq G$. Sea $\equiv'$ la relación de G definida por:*

$$a \equiv' b \Leftrightarrow a^{-1}b \in H$$

$$\textit{(de forma equivalente } a \equiv b \Leftrightarrow ab^{-1} \in H\textit{)}$$

Y es fácil probar que esta relación, es una relación de equivalencia.

Sea G/H el conjunto de clases de equivalencia determinadas por la relación $\equiv$. Entonces definimos el producto de clases de G/H por:

$$aHbH := abH, \forall a,b \in G$$

$$(\overline{a}\overline{b} := \overline{ab})$$

G/H adquiere estructura de grupo. G/H se denomina el grupo cociente de G por H.

Definición 1.12. *Una cadena de un grupo G es una sucesión finita totalmente ordenada de subgrupos de G comenzando en $\{e\}$ y terminando en G:*

$$\{e\} = H_0 \leq H_1 \leq \cdots \leq H_n = G. \tag{1}$$

- *La cadena* (1) *se dice subnormal si* $H_i \trianglelefteq H_{i+1}$*, para cada* $0 \leq i \leq n-1$.

- *La cadena* (1) *se dice normal si* $H_i \trianglelefteq G$*, para* $0 \leq i \leq n$.

- *Se dice que un subgrupo* H *de un grupo* G *es subnormal en* G*, si* H *es miembro de una cadena subnormal de* G.

- *Si* (1) *es una cadena subnormal, los cocientes* H_{i+1}/H_i*,* $0 \leq i \leq n-1$*, se denominan secciones de la cadena subnormal* (1).

Ejemplo 1.13.

1. $0 \leq 6\mathbb{Z} \leq 3\mathbb{Z} \leq \mathbb{Z}$ *y* $0 \leq 45\mathbb{Z} \leq 15\mathbb{Z} \leq 3\mathbb{Z} \leq \mathbb{Z}$ *son cadenas de* $\mathbb{Z}$ *con secciones*

$$6\mathbb{Z}/0 \cong \mathbb{Z},\ 3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_2,\ \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3;$$

$$45\mathbb{Z}/0 \cong \mathbb{Z},\ 15\mathbb{Z}/45\mathbb{Z} \cong \mathbb{Z}_3,\ 3\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}_5\ \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$$

2. *Definamos el grupo de los cuaterniones como:*

$$Q_8 = \left\langle a, b \mid a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1} \right\rangle$$

$$Q_8 = \left\{1, a, a^2, a^3, b, ab, a^2b, a^3b\right\}$$

Entonces $1 \leq \left\langle a^2 \right\rangle \leq \langle b \rangle \leq Q_8$*;* $1 \leq \left\langle a^2 \right\rangle \leq \langle a \rangle \leq Q_8$*;* $1 \leq \left\langle a^2 \right\rangle \leq \langle ab \rangle \leq Q_8$ *son cadenas normales de* Q_8 *con secciones isomorfas a* $\mathbb{Z}_2$*. Note que en* Q_8 *toda cadena es normal ya que todos los subgrupos son normales.*

Proposición 1.14. *Sea* G *un grupo y sean* $L, M \trianglelefteq G$*. Entonces:*

1. $(L,M) \trianglelefteq G$. *En particular* $G' \trianglelefteq G$.

2. *Si* $G' \leq K \leq G$ *entonces* $K \trianglelefteq G$. *Además,* G/G' *es un grupo abeliano y* G' *está contenido en cada subgrupo normal* K *de* G *tal que* G/K *sea abeliano.*

Demostración.

1. Cada elemento z de (L,M) es de la forma $z = z_1 \cdots z_k$, donde cada z_i, $1 \leq i \leq k$ es de la forma (a,b) o $(a,b)^{-1}$ con $a \in L$ y $b \in M$. Sea x un elemento cualquiera de G. Entonces $z^x = x^{-1}zx = z_1^x \cdots z_k^x$. Pero

   $(a,b)^x = (a^x, b^x)$ y $a^x \in L$, $b^x \in M$, ya que

   $(a,b)^x = (a^{-1}b^{-1}ab)^x = (a^{-1})^x(b^{-1})^x a^x b^x = (a^x)^{-1}(b^x)^{-1}a^x b^x = (a^x, b^x)$.

   Y ademas, $((a,b)^{-1})^x = ((a,b)^x)^{-1} = (a^x, b^x)^{-1}$, pues

   $((a,b)^{-1})^x = ((a^{-1}b^{-1}ab)^{-1})^x = (b^{-1}a^{-1}ba)^x = (b^x)^{-1}(a^x)^{-1}b^x a^x$, y

   $((a,b)^x)^{-1} = ((a^x)^{-1}(b^x)^{-1}a^x b^x)^{-1} = (b^x)^{-1}(a^x)^{-1}b^x a^x$.

   Se obtiene entonces que $z^x \in (L,M)$, es decir, $(L,M) \trianglelefteq G$.

2. Sea K tal que $G' \leq K \leq G$. Tomando $x \in G$ y a un elemento cualquiera de K. Entonces $(x^{-1}ax)a^{-1} \in G' \leq K$, así $x^{-1}ax \in K$, es decir, $K \trianglelefteq G$. Sean $x, y \in G$. Entonces, $\overline{x}^{-1}\overline{y}^{-1}\overline{xy} = \overline{x^{-1}y^{-1}xy} = \overline{e}$, es decir, $\overline{xy} = \overline{yx}$ y así G/G' es abeliano.

   Sea ahora $K \trianglelefteq G$ tal que G/K es abeliano. Eligiendo $z = z_1 \cdots z_k$ un elemento cualquiera de G'. Cada z_i es de la forma $(a,b) = a^{-1}b^{-1}ab$ o de la forma $(a,b)^{-1} = b^{-1}a^{-1}ab$, donde $a, b \in G$. Consideremos la clase de $a^{-1}b^{-1}ab$ en el cociente G/K: $\overline{a^{-1}b^{-1}ab} = \overline{a^{-1}b^{-1}}\overline{a}\overline{b} = \overline{e}$, o sea que $(a^{-1}b^{-1}ab)^{-1} \in K$. De lo anterior se desprende que $z \in K$ y en total $G' \leq K$.

■

El siguiente teorema trata sobre algunas propiedades de las cadenas 1 cuando tenemos un grupo cualquiera G.

Teorema 1.15. *Sea G un grupo. Entonces las siguientes afirmaciones son equivalentes:*

i) *G posee una cadena subnormal con secciones abelianas.*

ii) *La cadena de conmutadores*

$$G \geq G_1 \geq G_2 \geq \cdots \geq G_m \geq \cdots, \tag{2}$$

del grupo G se estabiliza en $\{e\}$ después de un número finito de pasos, donde

$$G_k := (G_{k-1}, G_{k-1}), \qquad k \geq 1; \qquad G_0 := G.$$

iii) *G posee una cadena normal con secciones abelianas.*

Demostración. *i*) $\Rightarrow$ *ii*) :

Suponga que

$$\{e\} = H_0 \leq H_1 \leq \cdots \leq H_n = G$$

es una cadena subnormal de G con secciones abelianas. Puesto que $H_{n-1} \trianglelefteq G$ y G/H_{n-1} es abeliano entonces de acuerdo con la **Proposición 1.14**, $G' \leq H_{n-1}$. Supóngase inductivamente que $G_k \leq H_{n-k}$, $1 \leq k \leq n$. De nuevo, como $H_{n-k-1} \trianglelefteq H_{n-k}$ y H_{n-k}/H_{n-k-1} es abeliano entonces, $(H_{n-k})' \leq H_{n-k-1}$, pero $G_k' \leq (H_{n-k})'$, luego $G_{k+1} \leq H_{n-k-1}$. Así por inducción, $G_n \leq H_{n-n} = \{e\}$ y entonces

$G_n = \{e\}$.

$ii) \Rightarrow iii)$:

Note que $G \trianglelefteq G$ y $G_1 = (G,G)$, así por la **Proposición 1.14** $G_1 \trianglelefteq G$, ahora como $G_1 \trianglelefteq G$ y $G_2 = (G_1,G_1)$, entonces $G_2 \trianglelefteq G$, realizando el mismo proceso obtenemos que para cada $1 \leq k \leq n$ $G_k \trianglelefteq G$.

$iii) \Rightarrow i)$:

Es evidente. ■

Definición 1.16. *Un grupo G se dice que es soluble si satisface una y por tanto todas las condiciones del* ***Teorema 1.15****.*

Definición 1.17. *Para* $n \geq 2$*, sea*

$$A_n := \{\sigma \in S_n \mid \sigma \textit{es producto de un número par de transposiciones } \}.$$

A_n se denomina el grupo alternante o grupo de permutaciones pares.

Ejemplo 1.18.

i) Todo grupo abeliano es soluble. Por tanto el concepto de solubilidad tiene entonces interés para los grupos no abelianos.

ii) S_3 *es soluble: pues para* S_3 *podemos construir la siguiente cadena subnormal*

$$\{e\} \trianglelefteq A_3 \trianglelefteq S_3,$$

con secciones S_3/A_3 *y* $A_3/\{e\}$ *abelianas*

iii) S_4 *es soluble: pues podemos construir la siguiente cadena subnormal*

$$\{e\} \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4,$$

con secciones S_4/A_4, A_4/V, $V/\{e\}$ *abelianas.*

Donde

$$V = \{(1),(12)(34),(13)(24),(14)(23)\} \subset A_4.$$

es el grupo de Klein, también llamado $4-$*grupo de Klein.*

Corolario 1.19. *El grupo* S_n *no es soluble, para* $n \geq 5$.

Demostración. En primer lugar vamos a probar que cuando $n \geq 5$, G_k para $k = 1,2,...,$ contiene cada $3-$ciclo de S_n.

Primero veremos que si N distinto del neutro, es un subgrupo normal del S_n, entonces N' también debe contener cada $3-$ciclo. Supongamos $a = (1,2,3)$, $b = (1,4,5)$ están en N (dado que para $n \neq 4$ el único subgrupo normal propio de S_n es A_n el cual contiene los 3-ciclos); entonces $a^{-1}b^{-1}ab = (3,2,1)(5,4,1)(1,2,3)(1,4,5) = (1,4,2)$, como conmutador de elementos de N debe estar en N'. Ya que N' es un subgrupo normal de S_n, para cualquier $\sigma \in S_n$, $\sigma^{-1}(1,4,2)\sigma$ también debe estar en N'. Eligiendo a $\sigma \in S_n$ tal que $\sigma(1) = i_1$, $\sigma(4) = i_2$ y $\sigma(2) = i_3$, donde i_1, i_2, i_3 son cualquieras 3 enteros distintos en el rango de 1 a n; entonces $\sigma^{-1}(1,4,2)\sigma = (i_1, i_2, i_3)$ esta en N'. Así N' contiene todos los $3-$ciclos.

Tomando $N = G$, que es claramente normal en G y contiene todos los $3-$ciclos, obtenemos que G' contiene todos los $3-$ciclos; dado que G' es normal en G, G_2 contiene todos los $3-$ciclos; ya que G_2 es normal en G, G_3 contiene todos los $3-$ciclos. continuando este proceso obtenemos que G_k contiene todos los $3-$ciclos para k arbitrario.

Como ya vimos que G_k contiene todos los $3-$ciclos en S_n para cada k. Por lo tanto, $G_k \neq \{e\}$ para cualquier k, es decir, la cadena (2) nunca se estabiliza, entonces S_n para $n \geq 5$ no es soluble. ■

2. Sobre extensiones de cuerpos

El estudio de los cuerpos es importante debido a que son el ambiente en donde tomaremos los coeficientes de los polinomios. Podemos ver (Lezama, 2019a) y (Roman, 2005).

2.1. Extensiones de cuerpos

Definición 2.1. *Sean $\mathbb{L}$ y $\mathbb{F}$ cuerpos:*

- *Se dice que $\mathbb{L}$ es una extensión de $\mathbb{F}$, si $\mathbb{F}$ es un subcuerpo de $\mathbb{L}$, esto es $\mathbb{F} \subset \mathbb{L}$, esto lo indicaremos con el siguiente diagrama:*

$$\begin{array}{c} \mathbb{L} \\ | \\ | \\ \mathbb{F} \end{array}$$

- *Sea $\mathbb{L}$ una extensión de $\mathbb{F}$. Se denomina grado de la extensión a la dimensión de $\mathbb{L}$ considerado como espacio vectorial sobre $\mathbb{F}$ y se denota por $[\mathbb{L} : \mathbb{F}] := dim_{\mathbb{F}}(\mathbb{L})$. La extensión se dice finita si su grado es finito.*

- *Sea* $\mathbb{L}$ *una extensión de* $\mathbb{F}$ *y sea* $\alpha \in \mathbb{L}$*. La adjunción* $\mathbb{F}(\alpha)$ *se conoce como extensión simple de* $\mathbb{F}$*, se dice que* α *es un elemento generador de la extensión* $\mathbb{F}(\alpha)$.

La siguiente proposición caracteriza los elementos de $\mathbb{F}(\alpha)$.

Proposición 2.2. *Sea* $\mathbb{L}$ *una extensión del cuerpo* $\mathbb{F}$ *y sea* $\alpha \in \mathbb{L}$*. Entonces*

$$\mathbb{F}(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p(x),\ q(x) \in \mathbb{F}[x],\ q(\alpha) \neq 0 \right\}.$$

Definición 2.3. *Sean* $\mathbb{F}$ *un cuerpo y* $f(x) \in \mathbb{F}[x]$ *un polinomio de grado* $n \geq 1$*. Una extensión* $\mathbb{K}$ *de* $\mathbb{F}$ *es llamada un cuerpo de descomposición de* $f(x)$ *respecto a* $\mathbb{F}$ *si:*

i) $f(x)$ *se descompone completamente en n factores lineales en* $\mathbb{K}[x]$.

ii) *No existe subcuerpo propio de* $\mathbb{K}$ *para el cual se cumple i*).

Ejemplo 2.4. *El cuerpo de descomposición de* $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ *es* $\mathbb{Q}(\sqrt{2})$*. Note que en* $\mathbb{Q}(\sqrt{2})[x]$ *tenemos que* $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ *y además como* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$*, no existen cuerpos* $\mathbb{K}$ *tales que* $\mathbb{Q} \nsubseteq \mathbb{K} \nsubseteq \mathbb{Q}(\sqrt{2})$.

2.2. Extensiones radicales simples

En esta sección hablaremos sobre extensión radical simple y los cuerpos intermedios entre esta y el cuerpo base y además estableceremos algunas propiedades de los polinomios irreducibles en estos cuerpos. Podemos ver (Conrad, 2010).

Definición 2.5. *Una extensión de cuerpos* $\mathbb{L}/\mathbb{K}$ *es llamada radical simple si* $\mathbb{L} = \mathbb{K}(\alpha)$ *donde* $\alpha^n = a$ *para algún* $n \geq 1$ *y* $a \in \mathbb{K}^*$.

Ejemplo 2.6. *Algunos ejemplos de radicales simples de* $\mathbb{Q}$ *son:* $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$. *En general* $\mathbb{Q}(\sqrt[n]{2})$ *con* $n > 1$.

Observación. *Una raíz de la ecuación* $x^n - a$ *se denotará por* $\sqrt[n]{a}$, *así una extensión radical simple de* $\mathbb{K}$ *es de la forma* $\mathbb{K}(\sqrt[n]{a})$, *pero la notación* $\sqrt[n]{a}$ *en cuerpos es ambigua (a pesar de esto, usaremos esta notación dejando en claro de que raíz estamos hablando); dado que, diferentes raíces n-ésimas de a pueden generar diferentes extensiones de* $\mathbb{K}$.

Ejemplo 2.7. *En* $\mathbb{C}$ *las tres raíces de la ecuación* $x^3 - 8$ *son* 2, $2w$ *y* $2w^2$, *donde w es una raíz cubica de la unidad no trivial. La extensión* $\mathbb{Q}(2w) = \mathbb{Q}(w) = \mathbb{Q}(2/w)$ *tiene grado* 2 *sobre* $\mathbb{Q}$. *Note que* $w^2 = 1/w$ *y w es raíz de* $(x^3 - 1)/(x - 1) = x^2 + x + 1$.

Ejemplo 2.8. *En el cuerpo* $\mathbb{Q}(\sqrt{5})$ *el número* $2 + \sqrt{5}$ *es un cubo, ya que:* $2 + \sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^3$. *Así el polinomio* $x^3 - (2 + \sqrt{5})$ *se puede factorizar sobre* $\mathbb{Q}(\sqrt{5})$ *como:*

$$x^3 - (2 + \sqrt{5}) = \left(x - \tfrac{1+\sqrt{5}}{2}\right)\left(x^2 + \tfrac{1+\sqrt{5}}{2}x + \tfrac{3+\sqrt{5}}{2}\right),$$

donde el segundo factor de la derecha de la ecuación es irreducible sobre $\mathbb{Q}(\sqrt{5})$, *ya que es irreducible sobre el cuerpo mas grande* $\mathbb{R}$. *Si* $\sqrt[3]{2+\sqrt{5}}$ *representa a* $(1 + \sqrt{5})/2$, *entonces*

$$\mathbb{Q}\left(\sqrt[3]{2+\sqrt{5}}\right) = \mathbb{Q}((1+\sqrt{5})/2) = \mathbb{Q}(\sqrt{5}),$$

por otro lado si $\sqrt[3]{2+\sqrt{5}}$ *es una raíz del factor cuadrático de* $x^3 - (2 + \sqrt{5})$, *es decir es una raíz de* $\left(x^2 + \frac{1+\sqrt{5}}{2}x + \frac{3+\sqrt{5}}{2}\right)$, *entonces la extensión* $\mathbb{Q}(\sqrt[3]{2+\sqrt{5}})$ *es una extensión cuadrática (el*

grado es 2) de $\mathbb{Q}(\sqrt{5})$*, ya que este polinomio seria el mónico irreducible.*

Sea $a \in \mathbb{K}$ vamos a centrarnos en el grado $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}]$ y relaciones de irreducibilidad para $x^n - a$ para cualquier valor $n \in \mathbb{N}$, y los cuerpos intermedios entre $\mathbb{K}$ y $\mathbb{K}(\sqrt[n]{a})$.

Teorema 2.9. *El grado* $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}]$ *es a lo sumo n, y es n, si y solo si,* $x^n - a$ *es irreducible sobre* $\mathbb{K}$*, en cuyo caso en el cuerpo* $\mathbb{K}(\sqrt[n]{a})$ *salvo isomorfismos es independiente de la elección de* $\sqrt[n]{a}$*.*

Demostración. Como $\sqrt[n]{a}$ es raíz de $x^n - a$, que esta en $\mathbb{K}[x]$ el polinomio mínimo de $\sqrt[n]{a}$ bajo $\mathbb{K}$ tiene como máximo grado n y por tanto $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] \leq n$

$\Rightarrow$) Si $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = n$ entonces el polinomio mínimo de $\sqrt[n]{a}$ sobre $\mathbb{K}$ tiene grado n por lo que debe ser $x^n - a$ ya que es un polinomio mónico de grado n en $\mathbb{K}[x]$ con $\sqrt[n]{a}$ como una raíz.

$\Leftarrow$) Supongamos que $x^n - a$ es irreducible sobre $\mathbb{K}$. Entonces $\sqrt[n]{a}$ tiene un polinomio mínimo $x^n - a$ sobre $\mathbb{K}$, por lo tanto $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = grad(x^n - 1) = n$.

cuando $x^n - a$ es irreducible sobre $\mathbb{K}$, el cuerpo $\mathbb{K}(\sqrt[n]{a})$ es isomorfo a $\mathbb{K}[x]/(x^n - a)$, usando la evaluación en $\sqrt[n]{a}$ y por lo tanto, bajo isomorfismo del cuerpo $\mathbb{K}(\sqrt[n]{a})$ es independiente de la elección de $\sqrt[n]{a}$. ■

Ejemplo 2.10. *El polinomio* $x^3 - 2$ *es irreducible sobre* $\mathbb{Q}$ *y los cuerpos* $\mathbb{Q}(\sqrt[3]{2})$*,* $\mathbb{Q}(\sqrt[3]{2}w)$ *y* $\mathbb{Q}(\sqrt[3]{2}w^2)$ *son isomorfos entre si, donde* $\sqrt[3]{2}$ *es la raíz cúbica real de* 2 *(o cualquier raíz cúbica de 2 en característica cero) y w es una raíz cúbica no trivial de la unidad. Esto no es cierto si reemplazamos* $\mathbb{Q}$ *por* $\mathbb{R}$*, ya que* $x^3 - 2$ *tiene una raíz en* $\mathbb{R}$*.*

Deseamos saber de que forma podemos ver las raíces del polinomio $x^n - a$ en un cuerpo de descomposición. Para esto, tenemos el siguiente resultado.

Teorema 2.11. *Las raíces de $x^n - a$ en un cuerpo de descomposición sobre $\mathbb{K}$, son de la forma $\zeta \sqrt[n]{a}$ donde ζ es una raíz n-ésima de la unidad en $\mathbb{K}$.*

Demostración. Sea $\alpha = \sqrt[n]{a}$ una raíz fija de $x^n - a$ sobre $\mathbb{K}$. Si β es otra raíz en el cuerpo de descomposición de $x^n - a$ sobre $\mathbb{K}$, entonces $\beta^n = a = \alpha^n$, así $(\beta/\alpha)^n = 1$. Sea $\zeta = \beta/\alpha \in K$, entonces $\beta = \zeta\alpha = \zeta\sqrt[n]{a}$ y $\zeta^n = (\beta/\alpha)^n = 1$. Y ya que $\zeta^n = 1$ y $\zeta \in \mathbb{K}$, entonces $(\zeta\sqrt[n]{a})^n = \zeta^n a = a$, así $\zeta\sqrt[n]{a}$ es raíz de $x^n - a$ en $\mathbb{K}$. ■

Para polinomios de grado mayor a 3 la falta de raíces no necesariamente implica irreducibilidad. Por ejemplo $(x^2-1)(x^2-2)$ en $\mathbb{Q}[x]$. El polinomio $x^p - a$, siendo p un número primo, es un contraejemplo; para estos polinomios la falta de raíz es equivalente a irreducibilidad. Esto es consecuencia del siguiente teorema.

Teorema 2.12. *Para un cuerpo arbitrario $\mathbb{K}$ y un número primo p y $a \in \mathbb{K}^*$, el polinomio $x^p - a$ es irreducible en $\mathbb{K}[x]$, si y solo si no tiene raíces en $\mathbb{K}$.*

Demostración.

$\Rightarrow$) Claramente si $x^p - a$ es irreducible en $\mathbb{K}[x]$ entonces no tiene raíces en $\mathbb{K}$ (ya que si existe un $b \in \mathbb{K}$ raíz de $x^p - a$, entonces $x^p - a = f(x)(x-b)$, donde $f(x) \in \mathbb{K}[x]$, pero esto contradice que $x^p - a$ se irreducible).

$\Leftarrow$) Para mostrar en este sentido, mostraremos la contra positiva: Si $x^p - a$ es reducible en $\mathbb{K}[x]$ entonces tiene una raíz en $\mathbb{K}$. Escribamos $x^p - a = g(x)h(x)$ en $\mathbb{K}[x]$, donde $m = grad(g)$ satisface $1 \leq m \leq p-1$. Como $x^p - a$ es mónico los coeficientes principales de g y h se multiplican por 1, por lo que podemos asumir que g es mónico y así h es mónico. Sea $\mathbb{L}$ un cuerpo de descomposición

de $x^p - a$ sobre $\mathbb{K}$ y $\alpha = \sqrt[p]{a}$ una raíz de $x^p - a$ en $\mathbb{L}$. Las otras raíces en $\mathbb{L}$ son $\zeta\alpha$ donde $\zeta^p = 1$ (Por **Teorema 2.11**), entonces en $\mathbb{L}[x]$.

$$x^p - a = (x - \zeta_1\alpha)(x - \zeta_2\alpha)\cdots(x - \zeta_p\alpha)$$

donde $\zeta_i^p = 1$ (posiblemente $\zeta_i = \zeta_j$ con $i \neq j$). Por factorización única en $\mathbb{L}[x]$ (recordando que como $\mathbb{L}$ es un cuerpo entonces $\mathbb{L}[x]$ es un dominio de ideales principales y por lo tanto un dominio de factorización única), cada factor mónico de $x^p - a$ en $\mathbb{L}[x]$ es producto de algunos $(x - \zeta_i\alpha)$ por lo tanto:

$$g(x) = (x - \zeta_{i_1}\alpha)(x - \zeta_{i_2}\alpha)\cdots(x - \zeta_{i_m}\alpha) \tag{3}$$

Para algunas raíces p-ésimas de la unidad $\zeta_{i_1}, \zeta_{i_2} \ldots, \zeta_{i_m}$. Ahora veamos los términos constantes en **(3)**. Sea $c = g(0)$, entonces

$$c = (-1)^m(\zeta_{i_1}\zeta_{i_2}\cdots\zeta_{i_m})\alpha^m \tag{4}$$

Ya que $g(x) \in \mathbb{K}[x]$, $c \in \mathbb{K}$ no nulo, ya que $g(0)h(0) = 0^p - a = -a$. Por lo tanto $c \in \mathbb{K}^*$. Queremos reemplazar α^m con α, y haremos elevando α^m a una potencia adicional para hacer que el exponente de α sea congruente a 1 *mod* p, es decir, que si y es el exponente de α entonces, p divide a $y - 1$. Como p es primo y $1 \leq m \leq p - 1$, m y p son primos relativos: podemos escribir $mt + pr = 1$ con

$t, r \in \mathbb{Z}$. Elevando en **(4)** a la potencia t para hacer el exponente de α igual a $mt = 1 - pr$:

$$c^t = (-1)^{mt}(\zeta_{i_1}\zeta_{i_2}\cdots\zeta_{i_m})^t\alpha^{mt}$$

$$= (-1)^{mt}(\zeta_{i_1}\zeta_{i_2}\cdots\zeta_{i_m})^t\alpha^{1-pr}$$

$$= (-1)^{mt}(\zeta_{i_1}\zeta_{i_2}\cdots\zeta_{i_m})^t\frac{\alpha}{(\alpha^p)^r}$$

$$= (-1)^{mt}(\zeta_{i_1}\zeta_{i_2}\cdots\zeta_{i_m})^t\frac{\alpha}{\alpha^r}$$

Así

$$\alpha^r(-1)^{mt}c^t = (\zeta_{i_1}\zeta_{i_2}\cdots\zeta_{i_m})^t\alpha \in \mathbb{K}^*$$

y el lado de la derecha tiene la forma $\zeta\alpha$, donde $\zeta^p = 1$ entonces $\mathbb{K}$ tienen una raíz en $x^p - a$. ■

Observación. *Para un primo impar p y cualquier cuerpo $\mathbb{K}$, la irreducibilidad de $x^p - a$ sobre $\mathbb{K}$ implica la irreducibilidad de $x^{p^r} - a$ con $r \geq 1$, lo cual no es evidente. Y esto no es cierto cuando $p = 2$, pues la irreducibilidad de $x^4 - a$ implica la irreducibilidad de $x^{2^r} - a$ para todo $r \geq 2$ (lo cual de nuevo no es evidente), pero la irreducibilidad de $x^2 - a$ no necesariamente implica la irreducibilidad de $x^4 - a$. Por ejemplo $x^2 + 4$ es irreducible en $\mathbb{Q}[x]$ pero $x^4 + 4 = x^{2^2} + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ no lo es.*

Cuando tenemos que un polinomio es irreducible sobre un cuerpo, a partir de este podemos encontrar otros polinomios y encontrar una relación con los grados, lo cual se enuncia en el siguiente teorema.

Teorema 2.13. *Sea $\mathbb{K}$ un cuerpo, $a \in \mathbb{K}^*$ y asuma que $x^n - a$ es irreducible sobre $\mathbb{K}$. Si $d|n$ entonces $x^d - a$ es irreducible sobre $\mathbb{K}$. Equivalentemente, si $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = n$ para alguna raíz n-ésima de a sobre $\mathbb{K}$ entonces para todo $d|n$ tenemos que $[\mathbb{K}(\sqrt[d]{a}) : \mathbb{K}] = d$ para cada raíz d-ésima de a.*

Demostración. Probaremos que la irreducibilidad de $x^n - a$ implica la irreducibilidad de $x^d - a$ de dos maneras: trabajando con polinomios, y trabajando con extensiones de cuerpos.

POLINOMIOS: Asumamos $x^d - a$ reducible sobre $\mathbb{K}$, entonces $x^d - a = g(x)h(x)$ donde $0 < grad(g(x)) < d$. Reemplazando x con $x^{n/d}$ en esta ecuación, obtenemos: $x^n - a = g(x^{n/d})h(x^{n/d})$ donde $grad(g(x^{n/d})) = \frac{n}{d} grad(g) < \frac{n}{d} d = n$ y claramente $grad(x^{n/d}) > 0$ entonces, $x^n - a$ es reducible, lo cual es una contradicción, con lo cual $x^d - a$ es irreducible.

EXTENSIONES DE CUERPO: Sea $\sqrt[n]{a}$ una raíz n-ésima de a sobre $\mathbb{K}$, entonces $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = n$ por **Teorema 2.9**. Definamos $\sqrt[d]{a} = \sqrt[n]{a^{n/d}}$. Esto es una raíz de $x^d - a$ ya que $\sqrt[d]{a}^d = (\sqrt[n]{a^{n/d}})^d = \sqrt[n]{a}^n = a$. Para probar que $x^d - a$ es irreducible sobre $\mathbb{K}$ probaremos que $[\mathbb{K}(\sqrt[d]{a}) : \mathbb{K}] = d$ usando la elección de $\sqrt[d]{a}$.

En la torre $\mathbb{K} \subset \mathbb{K}(\sqrt[d]{a}) \subset \mathbb{K}(\sqrt[n]{a})$, tenemos que $[\mathbb{K}(\sqrt[d]{a}) : \mathbb{K}] \leq d$ y $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}(\sqrt[d]{a})] \leq n/d$ por **Teorema 2.9**, como $\sqrt[d]{a}$ es raíz de $x^d - a \in \mathbb{K}[x]$ y $\sqrt[n]{a}$ es raíz de $x^{n/d} - \sqrt[d]{a} \in \mathbb{K}(\sqrt[d]{a})[x]$. Tenemos:

$$[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = [\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}(\sqrt[d]{a})][\mathbb{K}(\sqrt[d]{a}) : \mathbb{K}]$$

Y nuestra hipótesis de irreducibilidad implica que $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = n$, por lo que nuestros limites superiores n/d y d para los factores de la derecha deben ser iguales, es decir, n/d y d respectivamente, debido a que $n = \frac{n}{d} d$. En particular $[\mathbb{K}(\sqrt[d]{a}) : \mathbb{K}] = d$ entonces $x^d - a$ es irreducible sobre

$\mathbb{K}$ (tiene una raíz con grado d sobre $\mathbb{K}$). ■

Un calculo importante que en la demostración del teorema anterior y que se usará más adelante es el siguiente: Si $d|n$ entonces $\mathbb{K}(\sqrt[n]{a})$ contiene a $\mathbb{K}(\sqrt[d]{a})$, pues $\sqrt[d]{a} = \sqrt[n]{a}^{n/d}$. Además como $\sqrt[d]{a}$ es una raíz de $x^d - a$, podemos ver que la raíz esta bien definida, pero note que $\sqrt[d]{a}$ no es cualquier raíz d-ésima de a, ya que depende de la elección de $\sqrt[n]{a}$.

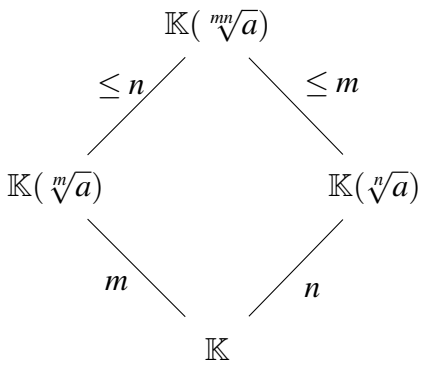
Cuando el polinomio es de la forma $x^p - a$, con $p = mn$ donde m y n son primos relativos se puede saber si dicho polinomio es irreducible o no. Más exactamente.

Teorema 2.14. *Para enteros positivos m y n primos relativos, $x^{mn} - a$ es irreducible sobre $\mathbb{K}$, si y solo si, $x^m - a$ y $x^n - a$ son irreducibles sobre $\mathbb{K}$. Equivalentemente, si m y n son primos relativos entonces $[\mathbb{K}(\sqrt[mn]{a}) : \mathbb{K}] = mn$, si y solo si, $[\mathbb{K}(\sqrt[m]{a}) : \mathbb{K}] = m$ y $[\mathbb{K}(\sqrt[n]{a}) : \mathbb{K}] = n$.*

Demostración.

$\Rightarrow$) La irreducibilidad de $x^{mn} - a$ implica la irreducibilidad de $x^m - a$ y $x^n - a$ gracias al **Teorema 2.13**.

$\Leftarrow$) Para demostrar el reciproco trabajaremos con las raíces del polinomio. Es conveniente seleccionar las raíces m-ésimas, n-ésimas y mn-ésimas de a de una manera multiplicativamente conveniente: Una raíz fija $\sqrt[mn]{a}$ de $x^{mn} - a$ sobre $\mathbb{K}$ y definamos $\sqrt[m]{a} := \sqrt[mn]{a}^n$ y $\sqrt[n]{a} := \sqrt[mn]{a}^m$. Entonces $\sqrt[m]{a}$ es raíz de $x^m - a$ y $\sqrt[n]{a}$ raíz de $x^n - a$, entonces así tenemos el siguiente diagrama:



(En el diagrama, los valores $n, m, \leq m, \leq n$ representan el grado de la extensión). Los valores del grado del cuerpo inferior provienen de $x^m - a$ y $x^n - a$ los cuales son irreducibles sobre $\mathbb{K}$, y los limites superiores del cuerpo superior provienen de $\sqrt[mn]{a}$ raíz de $x^n - \sqrt[m]{a} \in \mathbb{K}(\sqrt[m]{a})[x]$ y $x^m - \sqrt[n]{a} \in \mathbb{K}(\sqrt[n]{a})[x]$. Sea $d = [\mathbb{K}(\sqrt[mn]{a}) : \mathbb{K}]$, entonces leyendo el diagrama de cuerpo a lo largo de izquierda a derecha tenemos $d \leq mn$. Ademas d es divisible por m y n ya que los grados de cuerpo son multiplicativos en torres. Como m y n son primos relativos tenemos que $m|d$, $n|d$ entonces $mn|d$, así $mn \leq d$. Por lo tanto $d = mn$, entonces $x^{mn} - a$ es el polinomio minimal de $\sqrt[mn]{a}$ sobre $\mathbb{K}$ y así es irreducible sobre $\mathbb{K}$. ■

Como consecuencia del **Teorema 2.14**, se tiene el siguiente resultado.

Corolario 2.15. *Para un entero $N > 1$ con factorización prima $p_1^{e_1} \cdots p_k^{e_k}$, el polinomio $x^N - a$ es irreducible sobre $\mathbb{K}$, si y solo si, cada $x^{p_i^{e_i}} - a$ es irreducible sobre $\mathbb{K}$.*

Demostración. Usando **Teorema 2.14** con la factorización $N = p_1^{e_1}(p_2^{e_2} \cdots p_k^{e_k})$ para ver la irreducibilidad de $x^N - a$ sobre $\mathbb{K}$ es equivalente a la irreducibilidad de $x^{p_1^{e_1}} - a$ y $x^{p_2^{e_2} \cdots p_k^{e_k}} - a$ sobre $\mathbb{K}$, y entonces, por inducción sobre el número de diferentes potencias primas en el grado, la irreducibilidad de $x^{p_2^{e_2} \cdots p_k^{e_k}} - a$ sobre $\mathbb{K}$ es equivalente a la irreducibilidad de $x^{p_i^{e_i}} - a$ para $i = 1, \ldots, k$. ■

Ejemplo 2.16. *La irreducibilidad de $x^{90}-a$ sobre $\mathbb{K}$ es equivalente a la irreducibilidad de x^2-a, x^5-a y x^9-a sobre $\mathbb{K}$, debido al Corolario anterior, y dado que $90=2\cdot 3^2\cdot 5$.*

Observación. *Por la **Observación 2.2** y el **Teorema 2.13**, si N es impar entonces la irreducibilidad de x^N-a es equivalente a la irreducibilidad de $x^{p_i}-a$ sobre $\mathbb{K}$ cuando p_i recorre los factores primos de N (note que la multiplicidad e_i no importa), y por el **Teorema 2.12** esto implica que $x^{p_i}-a$ no tiene raíces en $\mathbb{K}$ para cada p_i.*

Ejemplo 2.17. *La irreducibilidad de $f(x)=x^{45}-a$ sobre $\mathbb{K}$ es equivalente a que $f(x)$ no tiene raíces cubicas o quintas en $\mathbb{K}$, es decir, $\sqrt[3]{a}$, $\sqrt[5]{a}\notin\mathbb{K}$.*

Para cualquier elección de una raíz n-ésima de a, $\sqrt[n]{a}$ y un divisor $d|n$, $\sqrt[d]{a}:=\sqrt[n]{a}^{n/d}$ es raíz de x^d-a en $\mathbb{K}(\sqrt[n]{a})$ entonces tenemos el siguiente diagrama:

$$\begin{array}{c}\mathbb{K}(\sqrt[n]{a})\\ |\\ \mathbb{K}(\sqrt[d]{a})\\ |\\ \mathbb{K}\end{array}$$

Lo natural en este punto es preguntarse si cada cuerpo entre $\mathbb{K}$ y $\mathbb{K}(\sqrt[n]{a})$ es de la forma $\mathbb{K}(\sqrt[d]{a})$ para algún d divisor de n.

Para este caso lo más sencillo es estudiar cuando x^n-a es irreducible sobre $\mathbb{K}$ (y por lo tanto x^d-a también es irreducible sobre $\mathbb{K}$, por el **Teorema 2.13**), luego $[\mathbb{K}(\sqrt[d]{a}):K]=d$. La pregunta es:

¿$\mathbb{K}(\sqrt[d]{a})$ es la única extensión de $\mathbb{K}$ de grado d dentro de $\mathbb{K}(\sqrt[n]{a})$? Para comprobar esto, podemos ver el **Ejemplo 2.19**.

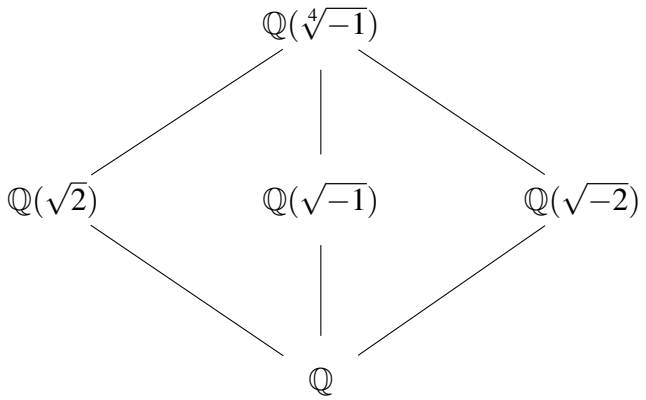
Teorema 2.18. ***(Criterio de irreducibilidad de Eisenstein)*** *Sea R un dominio entero y sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Si existe un primo $p \in R$ que satisfaga:*

$$p|a_i \text{ para } 0 \leq i < n,\ p \nmid a_n,\ p^2 \nmid a_0,$$

entonces $f(x)$ es irreducible.

Ejemplo 2.19. *Sea $\mathbb{K} = \mathbb{Q}$ y el cuerpo $\mathbb{Q}(\sqrt[4]{-1})$. Si $\alpha = \sqrt[4]{-1}$, entonces $\alpha^4 + 1 = 0$. Al hacer el cambio de x por $x+1$, del **Teorema 2.18** concluimos que $x^4 + 1$ es irreducible sobre $\mathbb{Q}$. Además como*

$[\mathbb{Q}(\sqrt[4]{-1}) : \mathbb{Q}] = 4$, cualquier cuerpo estrictamente entre $\mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{-1})$ es cuadrático sobre $\mathbb{Q}$. Claramente uno de estos es $\mathbb{Q}(\sqrt{-1})$, pero no es el único. Veamos el siguiente diagrama de cuerpo (latice de subgrupos de $\mathbb{Q}(\sqrt[4]{-1})$):



Si $\alpha^4 = -1$ entonces $(\alpha + 1/\alpha)^2 = -2$, así $\mathbb{Q}(\sqrt[4]{-1})$ contiene $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2})$. Además, nin-

guno de los cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ *y* $\mathbb{Q}(\sqrt{-2})$ *son el mismo, por lo tanto tenemos 3 (y de hecho solo son esas 3) extensiones cuadradas de* $\mathbb{Q}$ *en* $\mathbb{Q}(\sqrt[4]{-1})$.

En este ejemplo, la razón por la cual hay más cuerpos intermedios entre $\mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{-1})$ que solo $\mathbb{Q}(\sqrt{-1})$ es que en $\mathbb{Q}(\sqrt[4]{-1})$ hay 4 raíces de la unidad que no están en $\mathbb{Q}$. Por lo tanto, obtenemos el siguiente teorema que muestra que no obtenemos tales cuerpos inesperados si todas las raíces n-ésimas de la unidad en el cuerpo superior están en el cuerpo base.

Teorema 2.20. *Sea* $\mathbb{K}$ *un cuerpo,* $a \in \mathbb{K}^*$ *y asuma que* $x^n - a$ *es irreducible sobre* $\mathbb{K}$. *Si todas las raíces n-ésimas de la unidad en* $\mathbb{K}(\sqrt[n]{a})$ *están en* $\mathbb{K}$, *entonces para cada* $d|n$ *el único cuerpo entre* $\mathbb{K}$ *y* $\mathbb{K}(\sqrt[n]{a})$ *de grado d sobre* $\mathbb{K}$ *es* $\mathbb{K}(\sqrt[d]{a})$, *cuando* $\sqrt[d]{a} := (\sqrt[n]{a})^{n/d}$.

Demostración. Cada cuerpo entre $\mathbb{K}$ y $\mathbb{K}(\sqrt[n]{a})$ tienen un grado sobre $\mathbb{K}$ que divide a n. Para $d|n$ supongamos que $\mathbb{L}$ es cuerpo con $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\sqrt[n]{a})$ y $[\mathbb{L} : \mathbb{K}] = d$. Para probar que $\mathbb{L} = \mathbb{K}(\sqrt[d]{a})$ es suficiente probar que $\sqrt[d]{a} \in \mathbb{L}$ ya que esto nos daría que $\mathbb{K}(\sqrt[d]{a}) \subseteq \mathbb{L}$ y sabemos que $\mathbb{K}(\sqrt[d]{a})$ tiene grado d sobre $\mathbb{K}$, así tendríamos la contenencia $\mathbb{L} \subseteq \mathbb{K}(\sqrt[d]{a})$

$$
\begin{array}{c}
\mathbb{K}(\sqrt[n]{a}) \\
\Big| \\
n/d \\
\Big| \\
\mathbb{L} \\
\Big| \\
d \\
\Big| \\
\mathbb{K}
\end{array}
$$

Sea $f(x)$ el polinomio mínimo de $\sqrt[n]{a}$ sobre $\mathbb{L}$, entonces $f(x)|(x^n-a)$ y $grad(f)=n/d$. Podemos escribir cualquier otra raíz de $f(x)$ como $\zeta\sqrt[n]{a}$ para alguna raíz n-ésima de la unidad ζ (**Teorema 2.11**). En el cuerpo de descomposición de x^n-a sobre $\mathbb{K}$, la factorización de $f(x)$ es $\prod_{i\in I}(x-\zeta_i\sqrt[n]{a})$ para algunas raíces n-ésimas de la unidad ζ_i. El término constante de $f(x)$ esta en $\mathbb{L}$, entonces $(\prod_{i\in I}\zeta_i)\sqrt[n]{a}^{n/d}\in\mathbb{L}$. Por lo tanto $(\prod_{i\in I}\zeta_i)\sqrt[n]{a}^{n/d}\in\mathbb{K}(\sqrt[n]{a})$, entonces $\prod_{i\in I}\zeta_i\in\mathbb{K}(\sqrt[n]{a})$. Las únicas raíces n-ésimas de la unidad en $\mathbb{K}(\sqrt[n]{a})$ están, por hipótesis, en $\mathbb{K}$, entonces $\prod_{i\in I}\zeta_i\in\mathbb{K}\subseteq\mathbb{L}$. Por lo tanto $\sqrt[n]{a}^{n/d}=\sqrt[d]{a}$ esta en $\mathbb{L}$. ■

Veamos un ejemplo donde no todas las raíces n-ésimas de la unidad en $\mathbb{K}(\sqrt[n]{a})$ están en $\mathbb{K}$, pero la conclusión del **Teorema 2.20** es verdadera.

Ejemplo 2.21. *Tomando $\mathbb{K}=\mathbb{Q}(i)$, $a=2$ y $n=8$: se puede demostrar que $[\mathbb{Q}(i,\sqrt[8]{2}):\mathbb{Q}(i)]=8$ y los únicos cuerpos entre $\mathbb{Q}(i)$ y $\mathbb{Q}(i,\sqrt[8]{2})$ son $\mathbb{Q}(i,\sqrt[d]{2})$ cuando $d=1,2,4,8$, mientras $\frac{1+i}{\sqrt{2}}$ es una octava raíz de la unidad en $\mathbb{Q}(i,\sqrt[8]{2})$ que no está en $\mathbb{Q}(i)$.*

2.3. Extensiones radicales y solubles

En esta última sección se hablará sobre extensiones de Galois y el grupo Galois de un polinomio para finalmente poder enunciar el Teorema de Abel que nos dice: "La ecuación general de grado n no puede resolverse mediante radicales para $n\geq 5$". Podemos ver (Dummit and Foote, 2004).

Definición 2.22. *Sea $\mathbb{K}/\mathbb{F}$. Decimos que*

- $\alpha\in\mathbb{K}$ *es algebraico sobre $\mathbb{F}$ si es raíz de un polinomio no nulo de $\mathbb{F}[x]$.*

- $\mathbb{K}$ *es algebraica, si cada* $\alpha \in \mathbb{K}$ *es algebraico sobre* $\mathbb{F}$.

Definición 2.23. *Una extensión* $\mathbb{K}$ *de un cuerpo* $\mathbb{F}$ *se dice de Galois si satisface las siguientes condiciones:*

i) $\mathbb{K}$ *es una extensión algebraica de* $\mathbb{F}$.

ii) *Si* $p(x) \in \mathbb{F}[x]$ *es irreducible y tiene al menos una raíz en* $\mathbb{K}$, *entonces* $p(x)$ *se descompone completamente en* $\mathbb{K}[x]$ *en factores lineales.*

Definición 2.24. *Sea* $\mathbb{K}$ *una extensión de Galois de* $\mathbb{F}$. *El conjunto*

$$Gal(\mathbb{K}/\mathbb{F}) := \{\varphi \in Aut(\mathbb{K}) \mid \varphi(a) = a, \text{ para cada } a \in \mathbb{F}\}$$

es un subgrupo de $Aut(\mathbb{K})$ *y se denomina el grupo de Galois de* $\mathbb{K}$ *sobre* $\mathbb{F}$.

Recuerde que: Una función $\varphi : \mathbb{K} \to \mathbb{K}$ *es llamada automorfismo de* $\mathbb{K}$ *si para todos* $a, b \in \mathbb{K}$,

- $\varphi(a+b) = \varphi(a) + \varphi(b)$,
- $\varphi(ab) = \varphi(a)\varphi(b)$, *y,*
- φ *es biyectivo.*

Como es usual $Aut(\mathbb{K})$ *denota el conjunto de todos los automorfismos de* $\mathbb{K}$.

Proposición 2.25. *Si* $\mathbb{K}$ *es una extensión finita, normal y separable de* $\mathbb{F}$, *entonces* $|Gal(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$. *Ver Cuadernos De Álgebra-Cuerpos página 84.*

Definición 2.26. *Sean* $\mathbb{F}$ *un cuerpo,* $f(x) \in \mathbb{F}[x]$ *un polinomio de grado* $n \geq 1$ *y* $\mathbb{K}$ *el cuerpo de descomposición de* $f(x)$, *el grupo Galois* $Gal(\mathbb{K}/\mathbb{F})$ *se conoce como el grupo de Galois de* $f(x)$.

Ejemplo 2.27. *Calculemos el grupo Galois de* $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

Paso 1. *El cuerpo de descomposición de* $f(x)$ *es* $\mathbb{K} = \mathbb{Z}_2(\alpha)$, *con* $\alpha := \overline{x} \in \mathbb{Z}[x]/\langle f(x)\rangle$, *y además,* $[\mathbb{K} : \mathbb{F}] = 3$, *con* $\mathbb{F} = \mathbb{Z}_2$.

Paso 2. $|Gal(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}] = 3$, *orden del grupo Galois.*

Paso 3. $Gal(\mathbb{K}/\mathbb{F}) \cong \mathbb{Z}_3$, *donde solo existe un grupo de orden 3.*

Paso 4. $\{0\}$ *y* $\mathbb{Z}_3$, *son los únicos subgrupos de* $Gal(\mathbb{K}/\mathbb{F})$.

Paso 5. *Los subgrupos normales de* $Gal(\mathbb{K}/\mathbb{F})$, *son* $\{0\}$ *y* $\mathbb{Z}_3$.

Paso 6. *Así, los subcuerpos intermedios (normales)* $\mathbb{F} \subset \mathbb{L} \subset \mathbb{K} : \mathbb{L} = \mathbb{Z}_2, \mathbb{Z}_2(\alpha)$.

Definición 2.28. *La extensión* $\mathbb{K}/\mathbb{F}$ *se dice que es cíclica si es de Galois con un grupo de Galois cíclico.*

Veamos ahora en cuales casos las extensiones pueden ser cíclicas.

Proposición 2.29. *Sea* $\mathbb{F}$ *un cuerpo tal que su característica no divide a n que contiene las raíces n-ésimas de la unidad. Entonces la extensión* $\mathbb{F}(\sqrt[n]{a})$ *para* $a \in \mathbb{F}$ *es cíclica sobre* $\mathbb{F}$ *cuyo grado divide a n.*

Demostración. La extensión $\mathbb{K} = \mathbb{F}(\sqrt[n]{a})$ es Galois sobre $\mathbb{F}$ si $\mathbb{F}$ contiene las raíces $n-$ésimas de la unidad ya que es un cuerpo de descomposición para $x^n - a$. Para cualquier $\sigma \in Gal(\mathbb{K}/\mathbb{F})$, $\sigma(\sqrt[n]{a})$ es otra raíz de este polinomio, por lo tanto $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ para alguna raíz n-ésima de la unidad ζ_σ.

Esto da un mapa

$$Gal(\mathbb{K}/\mathbb{F}) \to \mu_n \tag{5}$$

$$\sigma \mapsto \zeta_\sigma$$

Donde μ_n denota el grupo de las raíces n-ésimas de la unidad. Ya que $\mathbb{F}$ contiene a μ_n cada raíz n-ésima de la unidad se fija por cada elemento de $Gal(\mathbb{K}/\mathbb{F})$. Por lo tanto

$$\begin{aligned}\sigma\tau(\sqrt[n]{a}) &= \sigma(\zeta_\tau \sqrt[n]{a}) \\ &= \zeta\, \tau\sigma \sqrt[n]{a} \\ &= \zeta_\tau \zeta_\sigma \sqrt[n]{a} = \zeta_\sigma \zeta_\tau \sqrt[n]{a}\end{aligned}$$

que muestra que $\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau$ entonces el mapa (5) es un homomorfismo. El Kernel consiste precisamente en los automorfismos que fijan a $\sqrt[n]{a}$, es decir la identidad. Dado que (5) es un homomorfismo y su Kernel es la identidad, obtenemos una inyección del $Gal(\mathbb{K}/\mathbb{F})$ en el grupo cíclico μ_n de orden n. Es decir que $Gal(\mathbb{K}/\mathbb{F})$ es isomorfo a un subgrupo H de μ_n y como μ_n es cíclico y de grado n, H es cíclico cuyo grado divido a n. Por tanto $\mathbb{K}$ es cíclico con grado que divide a n. ■

Definición 2.30.

1. *Un elemento $\alpha \in \mathbb{K}$ puede ser expresado por radicales o resolverse en términos de radicales*

si α se puede obtener por una sucesión de extensiones radicales simples

$$\mathbb{F} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_i \subset \mathbb{K}_{i+1} \subset \cdots \subset \mathbb{K}_s = \mathbb{K} \tag{6}$$

donde $\mathbb{K}_{i+1} = \mathbb{K}_i(\sqrt[n_i]{a_i})$ para algunos $a_i \in \mathbb{K}_i, i = 0,1,\ldots,s-1$. Aquí $\sqrt[n_i]{a_i}$ denotan las raíces del polinomio $x^{n_i} - a_i$. En este caso $\mathbb{K}$, se llama extensión radical de $\mathbb{F}$.

2. *Un polinomio $f(x) \in \mathbb{F}[x]$ es soluble por radicales si todas sus raíces pueden ser expresadas por radicales.*

Ejemplo 2.31. *Sea*

$$\alpha = -1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}.$$

Entonces α es expresado por radicales.

En efecto tomando

$$\mathbb{K}_0 = \mathbb{Q}$$

$$\mathbb{K}_1 = \mathbb{K}_0(\sqrt{a_0}) \qquad a_0 = 17$$

$$\mathbb{K}_2 = \mathbb{K}_1(\sqrt{a_1}) \qquad a_1 = 2(17 - \sqrt{17})$$

$$\mathbb{K}_3 = \mathbb{K}_2(\sqrt{a_2}) \qquad a_2 = 2(17 + \sqrt{17})$$

$$\mathbb{K}_4 = \mathbb{K}_3(\sqrt{a_3}) \qquad a_3 = 17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})},$$

donde cada una de estas extensiones es una extensión radical.

Definición 2.32. *Sean $x_1, x_2, ..., x_n$ indeterminadas. Las funciones simétricas elementales $s_1, s_2, ..., s_n$ son definidas por:*

$$s_1 = x_1 + x_2 + \cdots + x_n$$

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n$$

$$\vdots$$

$$s_n = x_1x_2 \cdots x_n$$

Teorema 2.33. *El polinomio general*

$$x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

sobre el cuerpo $\mathbb{F}(s_1, s_2, ..., s_n)$ es separable con grupo Galois S_n.

Podemos observar la demostración de este teorema en *Abstract algebra* página 609.

Recordando de la **sección 2.1** que un grupo finito G es soluble si existe una cadena de subgrupos

$$\{e\} = G_s \leq G_{s-1} \leq \cdots \leq G_{i+1} \leq G_i \leq \cdots \leq G_0 = G \tag{7}$$

con G_i/G_{i+1} abeliano, $i = 0, 1, \ldots, s-1$.

Definición 2.34. *Sea $\mathbb{F}$ un cuerpo:*

1. *Dada una extensión $\mathbb{E}/\mathbb{F}$, entonces la extensión mas pequeña de $\mathbb{F}$ que contiene a $\mathbb{E}$ y que es una extensión de Galois de $\mathbb{F}$ es llamada la clausura Galois.*

2. *Si $\mathbb{K}$ y $\mathbb{L}$ son subcuerpos de $\mathbb{F}$. La compuesta $\mathbb{KL}$ de $\mathbb{K}$ y $\mathbb{L}$ es el subcuerpo de $\mathbb{F}$ mas pequeño que contiene a $\mathbb{K}$ y $\mathbb{L}$.*

   Por tanto si $a \in \mathbb{KL}$, existen $n_1, n_2 \in \mathbb{N}$, $\{k_i\}_{i=1}^{n_1}$, $\{k'_i\}_{i=1}^{n_2} \subseteq \mathbb{K}$ y $\{l_i\}_{i=1}^{n_1}$, $\{l'_i\}_{i=1}^{n_2} \subseteq \mathbb{L}$ tal :

$$a = \frac{\sum_{i=1}^{n_1} k_i l_i}{\sum_{j=1}^{n_2} k'_j l'_j}$$

Observación. *Suponga que tenemos 2 extensiones radicales: $\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_p$, y $\mathbb{F} = \mathbb{G}_0 \subset \mathbb{G}_1 \subset \cdots \subset \mathbb{G}_q$, tal que $\mathbb{F}_{i+1} = \mathbb{F}_i(\sqrt[n_i]{a_i})$ para algún $a_i \in \mathbb{F}_i$ y lo mismo para $\mathbb{G}_i$. Podemos asumir que $q = p$.*

Entonces la compuesta de $\mathbb{G}_p$ y $\mathbb{F}_p$ es de nuevo extensión radical. Ya que como $\mathbb{G}_1 = \mathbb{G}_0(\sqrt[k_0]{b_0})$, $b_0 \in \mathbb{G}_0 = \mathbb{F} = \mathbb{F}_0$. Así, tenemos que $\mathbb{H}_1 = \mathbb{F}_1(\sqrt[k_0]{b_0}) = \mathbb{F}_0(\sqrt[n_0]{a_0})(\sqrt[k_0]{b_0})$, y podemos ver que $\mathbb{H}_1$ es

extensión radical, y $\mathbb{F}_1 \subset \mathbb{H}_1$, $\mathbb{G}_1 \subset \mathbb{H}_1$, *de hecho,* $\mathbb{H}_1$ *es la compuesta de* $\mathbb{F}_1$ *y* $\mathbb{G}_1$. *Similarmente, ya que* $a_1, b_1 \in \mathbb{H}_1$, *tenemos que* $\mathbb{H}_2 = \mathbb{H}_1(\sqrt[n_1]{a_1})(\sqrt[k_1]{b_1})$, *y de nuevo* $\mathbb{H}_2$ *es extensión radical, y la compuesta de* $\mathbb{F}_2$ *y* $\mathbb{G}_2$. *Realizando el mismo proceso obtendremos que* $\mathbb{H}_p$ *es extensión radical y es la compuesta de* $\mathbb{F}_p$ *y* $\mathbb{G}_p$. *Por lo tanto la compuesta de extensiones radicales es de nuevo extensión radical.*

Note que la clausura de Galois siempre existe debido a que si tenemos $f(x) \in \mathbb{F}[x]$ irreducible con k raíces $\zeta_1, ..., \zeta_k$, entonces la extensión $\mathbb{E}[\zeta_1, .., \zeta_k]$ es Galois, por tanto es la clausura Galois de $\mathbb{F}$.

Proposición 2.35. *Sean* $\mathbb{K}_1$ *y* $\mathbb{K}_2$ *extensiones Galois de un cuerpo* $\mathbb{F}$. *Entonces*

i)*La intersección* $\mathbb{K}_1 \cap \mathbb{K}_2$ *es Galois sobre* $\mathbb{F}$.

ii) *La composición* $\mathbb{K}_1\mathbb{K}_2$ *es Galois sobre* $\mathbb{F}$. *El grupo Galois es isomorfo a el subgrupo*

$$\mathbb{H} = \left\{(\sigma, \tau) | \sigma|_{\mathbb{K}_1 \cap \mathbb{K}_2} = \tau|_{\mathbb{K}_1 \cap \mathbb{K}_2}\right\}$$

de producto directo $Gal(\mathbb{K}_1/\mathbb{F}) \times Gal(\mathbb{K}_2/\mathbb{F})$ *que consiste en los elementos cuyas restricciones a la intersección* $\mathbb{K}_1 \cap \mathbb{K}_2$ *son iguales.*

Demostración.

Suponga que $f(x)$ es un polinomio irreducible sobre $\mathbb{F}[x]$ con raíz α en $\mathbb{K}_1 \cap \mathbb{K}_2$. Ya que $\alpha \in \mathbb{K}_1$ y $\mathbb{K}_1/\mathbb{F}$ es Galois, todas las raíces de $f(x)$ están en $\mathbb{K}_1$. Similarmente todas las raíces están el $\mathbb{K}_2$, por lo tanto todas las raíces de $f(x)$ están en $\mathbb{K}_1 \cap \mathbb{K}_2$. Se sigue fácilmente que $\mathbb{K}_1 \cap \mathbb{K}_2$ es Galois.

Si $\mathbb{K}_1$ es el cuerpo de descomposición del polinomio separable $f_1(x)$ y $\mathbb{K}_2$ es el cuerpo de descomposición del polinomio separable $f_2(x)$ entonces la compuesta es el cuerpo de descomposición para la parte libre de cuadrados del polinomio $f_1(x)f_2(x)$ (un polinomio $f \in \mathbb{K}[x]$ es libre de cuadrados si y solo sí, $b^2 \nmid f$ para cada polinomio $b \in \mathbb{K}[x]$ de grado positivo), por lo tanto es Galois sobre $\mathbb{F}$. El mapa

$$\varphi : Gal(\mathbb{K}_1\mathbb{K}_2/\mathbb{F}) \to Gal(\mathbb{K}_1/\mathbb{F}) \times Gal(\mathbb{K}_2/\mathbb{F})$$

$$\sigma \mapsto (\sigma|_{\mathbb{K}_1}, \sigma|_{\mathbb{K}_2})$$

Es claramente un homomorfismo. El kernel consiste en los elementos σ que son triviales en los $\mathbb{K}_1$ y $\mathbb{K}_2$, por lo tanto triviales en la compuesta, así el mapa es inyectivo. La imagen esta en el subgrupo $\mathbb{H}$, así

$$(\sigma|_{\mathbb{K}_1})|_{\mathbb{K}_1\cap\mathbb{K}_2} = \sigma_{\mathbb{K}_1\cap\mathbb{K}_2} = (\sigma|_{\mathbb{K}_2})|_{\mathbb{K}_1\cap\mathbb{K}_2}.$$

El orden de $\mathbb{H}$ puede ser calculado observando que para cada $\sigma \in Gal(\mathbb{K}_1/\mathbb{F})$ existen $|Gal(\mathbb{K}_2/\mathbb{K}_1 \cap \mathbb{K}_2)|$ elementos $\tau \in Gal(\mathbb{K}_2/\mathbb{F})$ cuya restricción de $\mathbb{K}_1 \cap \mathbb{K}_2$ es $\sigma|_{\mathbb{K}_1\cap\mathbb{K}_2}$. Por lo tanto

$$\begin{aligned} |\mathbb{H}| &= |Gal(\mathbb{K}_1/\mathbb{F})| \cdot |Gal(\mathbb{K}_2/\mathbb{K}_1 \cap \mathbb{K}_2)| \\ &= |Gal(\mathbb{K}_1/\mathbb{F})| \frac{|Gal(\mathbb{K}_2/\mathbb{F})|}{|Gal(\mathbb{K}_1\cap\mathbb{K}_2/\mathbb{F})|} \end{aligned}$$

Podemos ver que los ordenes de $\mathbb{H}$ y $Gal(\mathbb{K}_1\mathbb{K}_2/\mathbb{F})$ son entonces ambos iguales a

$$[\mathbb{K}_1\mathbb{K}_2 : \mathbb{F}] = \frac{[\mathbb{K}_1 : \mathbb{F}][\mathbb{K}_2 : \mathbb{F}]}{[\mathbb{K}_1 \cap \mathbb{K}_2 : \mathbb{F}]}$$

Por lo tanto la imagen de φ es precisamente $\mathbb{H}$. ■

Lema 2.36. *Si α esta contenida en una extensión radical $\mathbb{K}$ como en **(6)**, entonces α esta contenida en una extensión radical que es Galois sobre $\mathbb{F}$ y donde cada extensión $\mathbb{K}_{i+1}/\mathbb{K}_i$ es cíclica.*

Demostración. Sea $\mathbb{L}$ la clausura Galois de $\mathbb{K}$ sobre $\mathbb{F}$. Para cualquier $\sigma \in Gal(\mathbb{L}/\mathbb{F})$ tenemos la cadena de subcuerpos

$$\mathbb{F} = \sigma\mathbb{K}_0 \subset \sigma\mathbb{K}_1 \subset \cdots \subset \sigma\mathbb{K}_i \subset \sigma\mathbb{K}_{i+1} \subset \cdots \subset \sigma\mathbb{K}_s = \sigma\mathbb{K}$$

donde $\sigma\mathbb{K}_{i+1}/\sigma\mathbb{K}_i$ es de nuevo una extensión radical simple (ya que es generado por el elemento $\sigma \sqrt[n_i]{a_i}$, que es una raíz de la ecuación $x^{n_i} - \sigma(a_i)$ sobre $\sigma(\mathbb{K}_i)$). Recordando de la **Observación 2.3** que la compuesta de dos extensiones radicales es de nuevo una extensión radical (si $\mathbb{K}'$ es otra extensión radical con subcuerpos $\mathbb{K}'_i$, primero tomamos la compuesta de $\mathbb{K}'_1$ con los cuerpos $\mathbb{K}_0, \mathbb{K}_1, \ldots, \mathbb{K}_s$, luego la compuesta de estos cuerpos con $\mathbb{K}'_2$, etc. para que cada extensión individual en este proceso sea extensión radical simple). Se sigue que la compuesta de todos cuerpos conjugados $\sigma(\mathbb{K})$ para $\sigma \in Gal(\mathbb{L}/\mathbb{F})$ es de nuevo extensión radical. Ya que este cuerpo es precisamente $\mathbb{L}$, podemos ver que α esta contenido en la extensión radical Galois.

Ahora vamos a unir a $\mathbb{F}$ las raíces n_i-ésimas de la unidad para todas las raíces $\sqrt[n_i]{a_i}$ de la extensión radical simple en la extensión radical Galois $\mathbb{K}/\mathbb{F}$, obteniendo el cuerpo $\mathbb{F}'$, y entonces formamos la compuesta de $\mathbb{F}'$ con la extensión radical:

$$\mathbb{F} \subseteq \mathbb{F}' = \mathbb{F}'\mathbb{K}_0 \subseteq \mathbb{F}'\mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{F}'\mathbb{K}_i \subseteq \mathbb{F}'\mathbb{K}_{i+1} \subseteq \cdots \subseteq \mathbb{F}'\mathbb{K}_s = \mathbb{F}'\mathbb{K}$$

El cuerpo $\mathbb{F}'\mathbb{K}$ es una extensión Galois de $\mathbb{F}$ ya que es compuesta por dos extensiones Galois. La extensión de $\mathbb{F}$ a $\mathbb{F}' = \mathbb{F}'\mathbb{K}_0$ se le puede dar una cadena de subcuerpos con cada extensión

individual cíclica (esto es verdad para cualquier extensión abeliana, recordando que una extensión $\mathbb{F}/\mathbb{K}$ es abeliana si es Galois y su grupo Galois es abeliano). Cada extensión $\mathbb{F}'\mathbb{K}_{i+1}/\mathbb{F}'\mathbb{K}_i$ es una extensión radical simple y ahora nosotros tenemos la raíces apropiadas de la unidad en el cuerpo base, cada una de estas extensiones individuales de $\mathbb{F}'$ a $\mathbb{F}'\mathbb{K}$ es cíclica por la **Proposición 2.29**. Por lo tanto $\mathbb{F}'\mathbb{K}/\mathbb{F}$ es una extensión radical que es Galois sobre $\mathbb{F}$ con extensiones intermedias cíclicas. ■

Definición 2.37. *Sea $\mathbb{K}/\mathbb{F}$ con grupo Galois $Gal(\mathbb{K}/\mathbb{F})$. Si $\mathbb{H}$ es un sugrupo de $Gal(\mathbb{K}/\mathbb{F})$, el cuerpo fijo de $\mathbb{K}$ se define:*

$$\mathbb{K}_{\mathbb{H}} = \{a \in \mathbb{K} \mid \sigma(a) = a \text{para cada } \sigma \in \mathbb{H}\}.$$

Proposición 2.38. *Suponga que $\mathbb{K}/\mathbb{F}$ es una extensión Galois y $\mathbb{F}'/\mathbb{F}$ es cualquier extensión. Entonces $\mathbb{K}\mathbb{F}'/\mathbb{F}'$ es una extensión Galois, con grupo Galois*

$$Gal(\mathbb{K}\mathbb{F}'/\mathbb{F}') \cong Gal(\mathbb{K}/\mathbb{K}\cap\mathbb{F}')$$

isomorfico a un subgrupo de $Gal(\mathbb{K}/\mathbb{F})$.

Demostración. Si $\mathbb{K}/\mathbb{F}$ es Galois, entonces $\mathbb{K}$ es el cuerpo de descomposición para algún polinomio separable $f(x) \in \mathbb{F}[x]$. Así $\mathbb{K}\mathbb{F}'/\mathbb{F}'$ es el cuerpo de descomposición de $f(x)$ visto como un polinomio en $\mathbb{F}'[x]$, por lo tanto esta extensión es Galois. Ya que $\mathbb{K}/\mathbb{F}$ es Galois, cada monomorfismo de $\mathbb{K}$ fijando $\mathbb{F}$ es un automorfismo de $\mathbb{K}$, entonces el mapa

$$\varphi : Gal(\mathbb{K}\mathbb{F}'/\mathbb{F}') \to Gal(\mathbb{K}/\mathbb{F})$$

$$\sigma \mapsto \sigma|_{\mathbb{K}}$$

definido restringiendo un automorfismo σ a el subcuerpo $\mathbb{K}$ esta bien definido. Es claramente un homomorfismo, con kernel

$$Ker\varphi = \{\sigma \in Gal(\mathbb{K}\mathbb{F}'/\mathbb{F}') \mid \sigma|_{\mathbb{K}} = 1\}$$

Ya que un elemento en $Gal(\mathbb{K}\mathbb{F}'/\mathbb{F}')$ es trivial en $\mathbb{F}'$, los elementos en el kernel son triviales en $\mathbb{K}$ y en $\mathbb{F}'$, por lo tanto en su compuesta, así el kernel consiste solo en el automorfismo identidad. Por lo tanto φ es inyectiva.

Sea $\mathbb{H}$ la imagen de φ en $Gal(\mathbb{K}/\mathbb{F})$ y sea $\mathbb{K}_{\mathbb{H}}$ el correspondiente cuerpo fijo de $\mathbb{K}$ contenido en $\mathbb{F}$. Ya que cada elemento en $\mathbb{H}$ fija $\mathbb{F}'$, $\mathbb{K}_{\mathbb{H}}$ contiene $\mathbb{K} \cap \mathbb{F}'$. Por otro lado, la compuesta $\mathbb{K}_{\mathbb{H}}\mathbb{F}'$ esta fijada por $Gal(\mathbb{K}\mathbb{F}'/\mathbb{F}')$ (ningún $\sigma \in Gal(\mathbb{K}\mathbb{F}'/\mathbb{F}')$ fija $\mathbb{F}'$ y actúa sobre $\mathbb{K}_{\mathbb{H}} \subseteq \mathbb{K}$ a través de su restricción $\sigma|_{\mathbb{K}} \in \mathbb{H}$, que fijo $\mathbb{K}_{\mathbb{H}}$ por definición). Por el teorema fundamental de la teoría de Galois (ver *Abstract algebra* capítulo 14) esto prueba que $\mathbb{K}_{\mathbb{H}}\mathbb{F}' = \mathbb{F}'$, así que $\mathbb{K}_{\mathbb{H}} \subseteq \mathbb{F}'$, que da la inclusión inversa $\mathbb{K}_{\mathbb{H}} \subseteq \mathbb{K} \cap \mathbb{F}'$. Por lo tanto $\mathbb{K}_{\mathbb{H}} = \mathbb{K} \cap \mathbb{F}'$, y de nuevo por el teorema fundamental, $\mathbb{H} = Gal(\mathbb{K}/\mathbb{K} \cap \mathbb{F}')$. ■

Ahora podemos saber cuando un polinomio se puede o no resolver por radicales, información contendida en el siguiente teorema.

Teorema 2.39. *El polinomio $f(x)$ puede resolverse mediante radicales, si y solo si, su grupo de Galois es un grupo soluble.*

Demostración.

$\Rightarrow$) Cada raíz de $f(x)$ esta contenida en una extensión como en el **Lema 2.36**. El compuesto $\mathbb{L}$ de la extensión es de nuevo del mismo tipo según la **Proposición 2.35**. Sea G_i los subgrupos correspondientes a los subcuerpos $\mathbb{K}_i, i = 0, \ldots, s-1$. Como

$$Gal(\mathbb{K}_{i+1}/\mathbb{K}_i) = G_i/G_{i+1} \qquad\qquad i = 0, \ldots, s-1$$

se deduce que el grupo Galois $G = Gal(\mathbb{L}/\mathbb{F})$ es un grupo solucionable. El cuerpo $\mathbb{L}$ contiene el cuerpo de descomposición de $f(x)$, así el grupo Galois de $f(x)$ es un grupo cociente del grupo soluble G, por lo tanto es soluble.

$\Leftarrow$) Sea $\mathbb{K}$ el cuerpo de descomposición de $f(x)$. Tomando los cuerpos fijos de las subgrupos en la cadena **(7)** para G da una cadena

$$\mathbb{F} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_i \subset \mathbb{K}_{i+1} \subset \cdots \subset \mathbb{K}_s = \mathbb{K}$$

donde $\mathbb{K}_{i+1}/\mathbb{K}_i, i = 0, \ldots, s-1$ es una extensión cíclica de grado n_i. Sea $\mathbb{F}(\zeta_n)$ el cuerpo ciclotómico sobre $\mathbb{F}$ de todas las raíces de la unidad de orden $n_i, i = 0, \ldots, s-1$ y forme los cuerpos compuestos $\mathbb{K}'_i = \mathbb{F}'\mathbb{K}_i$ obtenemos una sucesión de extensiones

$$\mathbb{F} \subseteq \mathbb{F}' = \mathbb{F}'\mathbb{K}_0 \subseteq \mathbb{F}'\mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{F}'\mathbb{K}_i \subseteq \mathbb{F}'\mathbb{K}_{i+1} \subseteq \cdots \subseteq \mathbb{F}'\mathbb{K}_s = \mathbb{F}'\mathbb{K}$$

La extensión $\mathbb{F}'\mathbb{K}_{i+1}/\mathbb{F}'\mathbb{K}_i$ es cíclico con grado que divide a $n_i, i = 0, \ldots, s-1$ (Por **Proposición**

2.38). Dado que ahora tenemos las raíces apropiadas de la unidad en los cuerpos base, cada una de estas extensiones cíclicas es una extensión radical simple por **Proposición 2.29**. Por lo tanto, cada una de estas raíces de $f(x)$ esta contenida en una extensión raíz $\mathbb{F}'\mathbb{K}$ entonces $f(x)$ puede resolverse mediante radicales. ■

Del **Teorema 2.39** se tiene lo siguiente.

Corolario 2.40. ***(Teorema de Abel)***

La ecuación general de grado n no puede resolverse mediante radicales para $n \geq 5$.

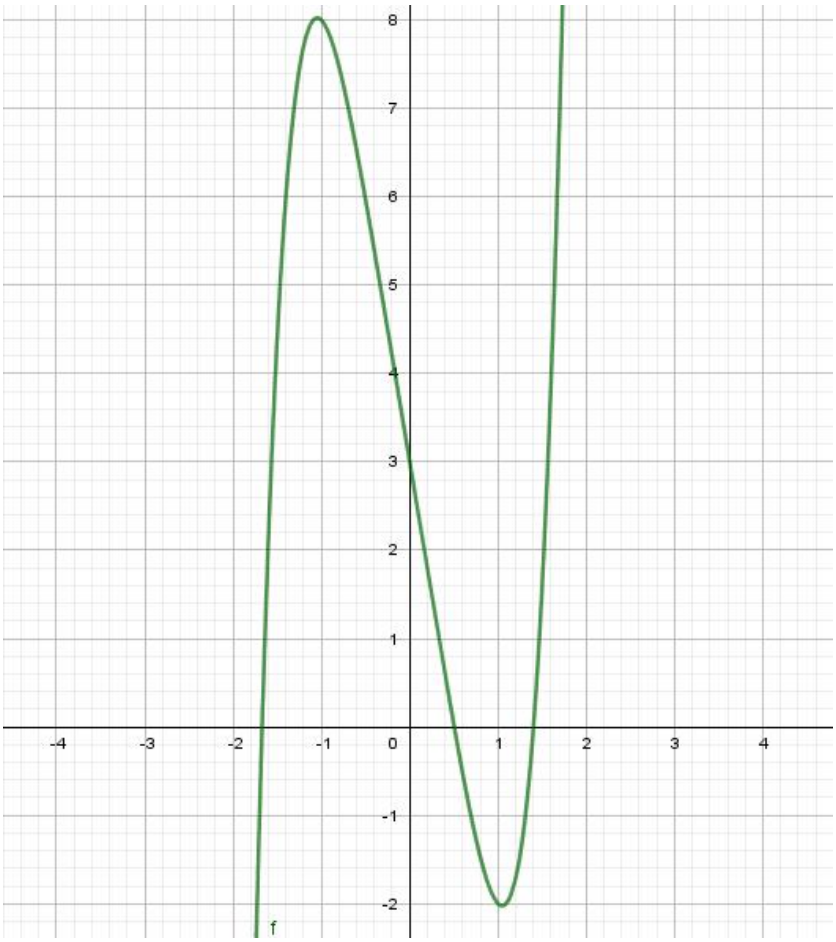
Demostración. Para $n \geq 5$ el grupo S_n no es soluble como vimos el el **capitulo 2.1**. El Corolario se demuestra inmediatamente por **Teorema 2.33** y **Teorema 2.39** ■

Este corolario muestra que no existe una formula general que involucre radicales análogos a la formula cuadrática para polinomios de grado 2 para las raíces de un polinomio de grado 5. Para dar un ejemplo de un polinomio especifico sobre $\mathbb{Q}$ de grado 5 cuyas raíces no pueden expresarse en términos de radicales debemos mostrar un polinomio de grado 5 con coeficientes racionales que no tienen a S_5(o A_5, que tampoco es soluble) como grupo de Galois.

Ejemplo 2.41. *Considere el polinomio* $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. *Nos podemos ayudar también con la gráfica de la función, para ello podemos verla a continuación:*

Figura 1.

Función $y = x^5 - 6x + 3$.



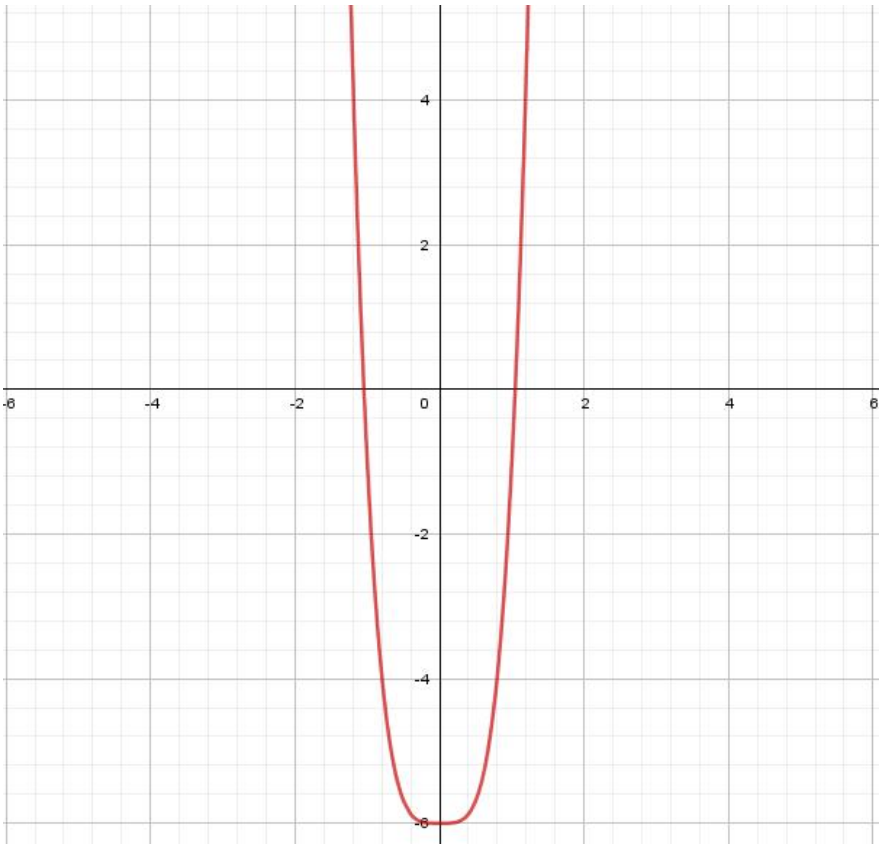
Nota. Esta imagen representa la gráfica del polinomio con el cual vamos a trabajar.

Este polinomio es irreducible ya que es Eisenstein en 3. El cuerpo de descomposición K para este polinomio, por lo tanto tiene un grado divisible por 5, ya que al unir una raíz de $f(x)$ *a* $\mathbb{Q}$ *genera una extensión de grado 5. El grupo G de Galois es, por lo tanto, un subgrupo de* S_5 *de orden divisible por 5. Los únicos elementos de orden 5 de* S_5 *son* 5*-ciclos, entonces G contiene los 5-ciclos.*

Como $f(-2) = -17, f(0) = 3, f(1) = -2$ *y* $f(2) = 23$ *podemos ver que* $f(x)$ *tiene una raíz en cada uno de los intervalos* $(-2,0),(0,1)$ *y* $(1,2)$*. Por el teorema del valor medio, si hubiera 4 raíces reales entonces la derivada* $f'(x) = 5x^4 - 6$ *tendría al menos 3 ceros reales, lo cual no es así (podemos ver la gráfica).*

Figura 2.

Función $y = 5x^4 - 6$.



Nota. Esta imagen representa la gráfica de la derivada del polinomio $x^5 - 6x + 3$.

Por lo tanto estas son las únicas raíces reales (esto también se sigue fácilmente por la regla de signos de Descartes). Por el teorema fundamental del álgebra $f(x)$ *tiene 5 raíces en* $\mathbb{C}$. *Por lo tanto* $f(x)$ *tiene 2 raíces complejas que no son reales. Sea* τ *el automorfismo de conjugación compleja en* $\mathbb{C}$. *Dado que los coeficientes de* $f(x)$ *son reales, las 2 raíces complejas deben intercambiarse por* τ*(ya que no son fijas, no son reales). Por lo tanto, la restricción de la conjugación*

compleja a K fija 3 de las raíces de $f(x)$ y intercambia las otras 2. Como un elemento de G, τ/K es una transposición.

Ahora es un ejercicio sencillo mostrar que cualquier 5-ciclos junto con cualquier transposición genera todo S_5. Se deduce que $G = S_5$, por lo que las raíces de $x^5 - 6x + 3$ no se pueden expresar por radicales.

Por el **Teorema 2.39**, cualquier polinomio de grado ≤ 4 puede resolverse por radicales , ya que S_n es un grupo soluble para estos n. Para $n = 2$ esta es solo la formula cuadrática familiar. Para $n = 3$ la formula es conocida como **Formula de Cardano** (nombre por Geronimo Cardano (1501-1576)) y la formula para $n = 4$ puede ser reducida a esta. Las formulas son validas para cualquier cuerpo $\mathbb{F}$ de característica $\neq 2, 3$, que son las características que dividen los ordenes de los posibles grupos de Galois(que son los subgrupos S_3 y S_4).

3. Conclusiones

Todos los objetivos del trabajo de grado se llevaron acabo de la siguiente manera:

- En el Capítulo 1, demostramos que para $n \leq 5$ el grupo S_n no es soluble.
- En la Sección 2.1, estudiamos resultados sobre extensiones radicales y el cuerpo de descomposición de un polinomio.
- En la Sección 2.2, definimos lo que es una extensión simple y demostramos resultados sobre estas extensiones, sobre las raíces de ecuaciones y sus relaciones.
- Finalmente en la Sección 2.3 definimos el grupo Galois, enunciamos la ecuación general de grado n, para la cual su grupo Galois es S_n y enunciamos el teorema que nos relaciona

cuando un polinomio se puede resolver por radicales con su grupo Galois, para finalmente demostrar el Teorema de Abel.

Referencias Bibliográficas

Conrad, K. (2010). *Simple radical extensions*.

Dummit, D. S. and Foote, R. M. (2004). *Abstract algebra*, volume 3. Wiley Hoboken.

John, W. and Sons (1975). *Topics in algebra Second edition*. Herstein.

Lezama, O. (2019a). Cuadernos de algebra-cuerpos.

Lezama, O. (2019b). Cuadernos de algebra-grupos.

Roman, S. (2005). *Field theory*, volume 158. Springer Science & Business Media.