UNIVERSIDAD DEL BÍO-BÍO
FACULTAD DE EDUCACIÓN Y HUMANIDADES
ESCUELA DE PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

Teoría de Galois y ecuaciones algebraicas

AUTOR: Riquelme Faúndez Edgardo Andrés
PROFESOR GUÍA: Basso Basso Ivo Roberto

MEMORIA PARA OPTAR AL TÍTULO DE PROFESOR DE EDUCACIÓN MEDIA EN EDUCACIÓN MATEMÁTICA

CHILLÁN 2007

Al dedicarme al conocimiento de la sabiduría y a la observación de todo cuanto se hace en la tierra, sin que pudiera conciliar el sueño ni de día ni de noche, pude ver todo lo hecho por Dios. ¡El hombre no puede comprender todo lo que Dios ha hecho en esta vida! Por más que se esfuerce por hallarle sentido, no lo encontrará; aun cuando el sabio diga conocerlo, no lo puede comprender.

Eclesistés 8:16-17

Agradecimientos

Quiero comenzar agradeciendo a mi profesor guía Ivo Basso quien no solamente ha sido importante en la dirección de este trabajo, sino también en mi formación matemática y en mi formación como profesor, en particular le agradezco su ayuda a la hora de redactar y ordenar el contenido de esta memoria y por todas las observaciones realizadas a mi trabajo durante este año.

Agradezco también a mi profesor Roberto Cabrales a quien debo mis conocimientos sobre látex y le doy gracias por atender mis dudas acerca de la digitalización de este trabajo y por la buena disposición que ha tenido para enseñar no solo cuando he sido su alumno en alguna asignatura.

En especial quiero mencionar a mi familia por su preocupación por mis reiterados trasnoches realizando este trabajo, por su apoyo en esta etapa de mi vida y por ser de gran importancia en mi formación como persona.

Gracias a mis compañeros de carrera y mis amigos que me preguntaron por este trabajo, a quienes a veces aburrí explicándoles lo hermoso que me parecían algunos de los resultados que estaba estudiando.

En lo personal creo importante agradecer a la gente de GBUCh, no solo por su preocupación en lo relacionado a mi actividad de titulación, sino por ser de gran importancia en mi paso por la universidad.

Finalmente no puedo dejar de dar gracias a quien es una realidad en mí vida y a quien le debo el sentido de ésta, a mi Dios quién siempre ha estado conmigo, a pesar de mis errores y defectos, a quien le debo mis valores y mis deseos de ser una mejor persona cada día.

Resumen

Resolubilidad por Radicales.

Nuestro objetivo principal consiste en saber si existen fórmulas como las de segundo, tercer y cuarto grado para ecuación de grado $n \geq 5$ lo que en lenguaje técnico es saber cuando una ecuación es soluble por radicales.

La primera idea para resolver este problema es ver que los coeficientes de una ecuación se pueden escribir en función de sus raíces por ejemplo para la ecuación de grado dos tenemos que:

$$(x-\alpha_1)(x-\alpha_2) = x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2$$

Por lo que esta ecuación la podemos escribir como x^2+bx+c donde $b = \alpha_1+\alpha_2$ y $c = \alpha_1\alpha_2$ que son funciones racionales que tiene las raíces α_1, α_2 como variables, luego aparece $\sqrt{b^2-4c}$ que nos hace pasar de una función simétrica $b^2-4c = (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2 = (\alpha_1-\alpha_2)^2$ a $\sqrt{b^2-4c} = \pm(\alpha_1-\alpha_2)$, es decir, dos funciones no simétricas.

Ahora veamos que si $K_0 = K(b,c)$ y $K_1 = K_0(\sqrt{b^2-4c})$ donde K es un cuerpo con característica cero y que contiene las raíces primitivas del unitario, tenemos que como b, c y todas las expresiones que se pueden obtener con las operaciones del cuerpo quedan invariantes por las permutaciones de sus raíces, luego podemos asociar a K_0 el grupo S_2, pero como las funciones de K_1 no son en general simétricas le vamos a asociar el grupo trivial $\{e\}$ lo que representaremos en el siguiente esquema:

$$\begin{array}{ccc} K_0 & \text{———} & K_1 = K_0(\sqrt{b^2-4c}) \\ G_0 = S_2 & \text{———} & G_1 = \{e\} \end{array}$$

De manera similar para la ecuación de tercer grado tenemos el siguiente esquema:

$$\begin{array}{ccccc} K_0 & \text{———} & K_1 = K_0(\sqrt{D}) & \text{———} & K_2 = K_1(\sqrt[3]{E}) \\ G_0 = S_3 & \text{———} & G_1 = A_3 & \text{———} & G_2 = \{e\} \end{array}$$

Y para la ecuación de cuarto grado el siguiente:

$$\begin{array}{ccccccccc} K_0 & \text{———} & K_1 & \text{———} & K_2 & \text{———} & K_3 & \text{———} & K_4 \\ G_0 = S_4 & \text{———} & G_1 = A_4 & \text{———} & G_2 & \text{———} & G_3 & \text{———} & G_4 = \{e\} \end{array}$$

De esta manera vemos que los métodos para resolver se ven reflejados en una cadena de subcuerpos a los que les asociamos una cadena de subgrupos. Lo interesante es que para

encontrar dichas fórmulas debemos introducir radicales los que disminuyen el número de permutaciones de raíces que dejan invariantes todas expresiones que se obtienen al operar con los coeficientes, por lo que a la cada extensión de cuerpo le podemos asociar un grupo de una cadena que cumple que $G_i \lhd G_{i+1}$ y que G_{i+1}/G_{i+1} es un grupo cíclico, lo que nos muestra las condiciones para la definición de un grupo soluble.

Además es importante notar que cada extensión es de la forma $K_{i+1} = K_i(r)$ con $r^d \in K_i$ y así cada extensión es el cuerpo de descomposición de un polinomio de la forma $x^d - r^d$ lo que nos dejan ver cuáles son las condiciones que cumplen las extensiones en donde podremos resolver las ecuaciones polinomiales.

Gracias a las observaciones anteriores podemos ver que el siguiente teorema el que será el objetivo principal de este trabajo nos da las condiciones necesarias y suficientes para encontrar las fórmulas buscadas.

Teorema de Galois *Sea $f(x) \in K[x]$ con característica cero y se E su cuerpo de descomposición, entonces $f(x)$ es soluble por radicales si y sólo si $\mathcal{G}(E/K)$ es un grupo soluble.*

Por último como para la ecuación de grado mayor o igual que cinco no podemos encontrar cadenas de subgrupos similares a las de las ecuaciones de segundo, tercer y cuarto grado; Como consecuencia tampoco podemos encontrar una fórmula para las ecuaciones de grado superior o igual a cinco.

Teorema Fundamental del Álgebra.

Otro de los objetivos de este trabajo será presentar una demostración del teorema fundamental del álgebra. La prueba que veremos aquí se basa en la teoría de Galois y en dos resultados bastante conocidos. El primero que polinomio de grado impar con coeficientes reales tiene al menos una raíz real y el segundo que todo número complejo tiene una raíz cuadrada, los que en el lenguaje de extensiones algebraicas se traducen a que toda extensión propia de los reales es de grado par y que no existen extensiones algebraicas de los complejos de grado dos. Resultados que gracias al teorema fundamental de la teoría de Galois y a uno de los teoremas de Sylow nos permite probar que los complejos no tiene extensiones algebraicas propias, es decir extensiones algebraicas distintas de si misma, lo que es equivalente a demostrar que todo polinomio no constante con coeficientes complejos tiene al menos una raíz compleja.

Índice general

Introducción

La resolución de ecuaciones polinomiales es un problema que ha inquietado al hombre desde tiempos muy antiguos: los egipcios tenían métodos para resolver ecuaciones simples, los babilonios desarrollaron métodos para resolver ecuaciones de primer y segundo grado, incluso algunos casos particulares de ecuaciones cúbicas, los griegos también se dedicaron a estos problemas pero solo lograron resolver casos particulares de ecuaciones cúbicas.

Tuvieron que pasar varios siglos hasta que fue en el siglo XVI en el que Tartaglia aprendió un método general para resolver la ecuación cúbica, método que Cardano difundió, sin embargo, al parecer fue Scipione Ferro el primero en conocer un método para resolverla, aunque nunca lo publico. Luego Ferrari logro un método para resolver ecuaciones cuárticas, pero el problema de encontrar una fórmula para la ecuación de quinto grado seguía sin resolverse a pesar de que ya D'Alembert en 1746 y más tarde Gauss en 1799 habían demostrado el teorema fundamental del álgebra, que afirma que todo polinomio no constante con coeficientes complejos tiene al menos una raíz. Por lo que el problema ahora no era saber si un polinomio con coeficientes reales o complejos tenía raíces o no, sino saber si estas se podían expresar en términos de los coeficientes mediante sumas, restas, multiplicaciones, divisiones y radicales; problema que tuvo que esperar hasta el siglo XIX donde Abel demostró la imposibilidad de encontrar una fórmula general para ecuaciones de grado mayor o igual que cinco. Finalmente fue Galois quien nos da las condiciones necesarias y suficientes para la resolubilidad por radicales.

Pero este problema no solo tiene una importancia histórica la cual puede ser motivacional a la hora de presentar el tema de las ecuaciones polinomiales tanto en la universidad como en enseñanza media sino también nos permitirá conocer distintas las maneras de pensar a la hora de enfrentar un problema y la comprensión de la necesidad de desarrollar conceptos e ideas para alcanzar dicho objetivo, desde maneras bastante sencillas como las usadas para resolver ecuaciones de primer o segundo grado a unas mucho más elaboradas como las herramientas de álgebra abstracta que son necesarias para demostrar la imposibilidad de resolver mediante sumas, multiplicaciones y radicales las ecuaciones de grado mayor o igual que cinco.

Este texto no pretende estudiar detalladamente las estructuras de grupos, anillos y cuerpos sino más bien utilizar algunos elementos de estas para presentar la solución a los problemas mencionados anteriormente esperando puedan apreciar la belleza e importancia de dichas estructuras y del álgebra abstracta en general.

Capítulo 1
Ecuaciones de 2º, 3º y 4º grado

A la hora de estudiar ecuaciones de segundo, tercer y cuarto grado vamos a tratar de reducir estas a casos más simples que podamos enfrentar con éxito. Esto constituye una manera de razonar muy común en matemáticas.

1.1. Ecuación de 2º grado

La ecuación general de segundo grado es de la forma:

$$ax^2 + bx + c = 0 \tag{1.1}$$

con $a, b, c \in \mathbb{C}$ y $a \neq 0$.

Lo primero que vamos a hacer es reducir esta ecuación a una donde el polinomio general de grado 2 asociado a la ecuación sea mónico por lo que dividiendo por a obtenemos:

$$x^2 + b'x + c' = 0 \tag{1.2}$$

con $b' = \dfrac{b}{a}$ y $c' = \dfrac{c}{a}$.

Luego completando cuadrados y despejando tenemos que:

$$\left(x + \frac{b'}{2}\right)^2 = \frac{b'^2 - 4c'}{4}$$

Por último extrayendo la raíz cuadrada y despejamos las soluciones son:

$$x = \frac{-b' \pm \sqrt{b'^2 - 4c'}}{2}$$

1.2. Ecuación de 3º grado

La ecuación general de tercer grado es de la forma:

$$ax^3 + bx^2 + cx + d = 0 \tag{1.3}$$

con $a, b, c, d \in \mathbb{C}$ y $a \neq 0$. Para resolver la ecuación de grado tres al igual que en el caso de la ecuación de segundo grado es reducir esta ecuación a una donde el polinomio general de grado 3 asociado a la ecuación sea mónico por lo que dividiendo por a obtenemos:

$$x^3 + b'x^2 + c'x + d' = 0 \tag{1.4}$$

con $b' = \frac{b}{a}$, $c' = \frac{c}{a}$ y $d' = \frac{d}{a}$.

Ahora vamos a usar el siguiente cambio de incógnita $y = x + \frac{b'}{3}$ conocido como una transformación de Tchirnhausen y así tenemos que el problema de la ecuación de tercer grado se reduce a resolver.

$$y^3 + py + q = 0 \tag{1.5}$$

con $p = \frac{3c' - b'^2}{3}$ y $q = \frac{2b'^3 - 9b'c' + 27d'}{27}$.

¿Cómo resolvemos $y^3+py+q=0$?

El primero en dar solución a esta ecuación fue Scipione Ferro(1465-1526) aunque este nunca la publicó, sino que antes de su muerte la reveló a uno de sus alumnos, Antonio María Fior, el que no fue un gran matemático y solo conocía la solución de este caso.

Luego fue Niccolo Tartaglia (1500-1577) quien aprendió a resolver la ecuación de tercer grado que contenía cubos y cuadrados seguramente reduciendo esta al caso que estudiaremos a continuación.

Finalmente fue Cardano en 1545 quien divulgo la solución de la ecuación cúbica en su obra Ars magna y no sólo ésta sino también la solución de la cuártica que descubrió su antiguo secretario Luigi Ferrari.

La idea para resolver este caso es suponer que la solución de la ecuación es de la forma $u + v$ entonces sustituyendo en 1.5 obtenemos

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

Pero si $u + v$ es solución tenemos que

$$\begin{aligned} 3uv &= -p \\ u^3 + v^3 &= -q \end{aligned}$$

O lo que es equivalente

$$\begin{aligned} u^3v^3 &= \frac{-p^3}{27} \\ u^3 + v^3 &= -q \end{aligned}$$

Asi u^3 y v^3 son soluciones de

$$z^2 + qz - \frac{p^3}{27}$$

Que por la ecuación de segundo grado tiene por soluciones a

$$z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

Por la simetría de u y v podemos elegir

$$\begin{aligned} u^3 &= -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \\ v^3 &= -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \end{aligned}$$

Luego

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

es una raíz de la ecuación 1.5.

¿Cómo obtener las otras raices de $y^3+py+q=0$?

Si $\omega \neq 1$ es una raíz cubica de 1 la ecuación $u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ tiene tres soluciones de la forma

$$\begin{aligned} u_1 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ u_2 &= \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ u_3 &= \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \end{aligned}$$

Además como $v = -\frac{p}{3u}$ entonces $v_i = -\frac{p}{3u_i}$ por lo que tenemos que:

$$\begin{aligned} v_1 &= -\frac{p}{3u_1} = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ v_2 &= -\frac{p}{3u_2} = \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ v_3 &= -\frac{p}{3u_3} = \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \end{aligned}$$

Por lo que concluimos que si $\omega \neq 1$ es una raíz cubica de 1 entonces

$$\begin{aligned} y_1 &= u_1 + v_1 \\ y_2 &= u_1\omega + v_1\omega^2 \\ y_3 &= u_1\omega^2 + v_1\omega \end{aligned}$$

donde $u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ y $v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$

Ejemplo 1.1 *Resolver la ecuación* $x^3 - 3x + 2$

Resolución:

$$\begin{aligned} x_1 &= \sqrt[3]{-\frac{2}{2} + \sqrt{\frac{2^2}{4} + \frac{-3^3}{27}}} + \sqrt[3]{-\frac{2}{2} - \sqrt{\frac{2^2}{4} + \frac{3^3}{27}}} \\ &= \sqrt[3]{-1 + \sqrt{1-1}} + \sqrt[3]{-1 - \sqrt{1-1}} \\ &= \sqrt[3]{-1+0} + \sqrt[3]{-1-0} \\ &= -1 + -1 = -2 \\ x_2 &= -\omega - \omega^2 = 1 \\ x_3 &= -\omega^2 - \omega = 1 \end{aligned}$$

1.3. Ecuación de 4º grado

La ecuación general de tercer grado es de la forma:

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \tag{1.6}$$

con $a, b, c, d, e \in \mathbb{C}$ y $a \neq 0$.
Al igual que en los casos anteriores la ecuación de cuarto grado es reducir esta ecuación a una donde el polinomio general de grado 4 asociado a la ecuación sea mónico por lo que dividiendo por a obtenemos:

$$x^4 + b'x^3 + c'x^2 + d'x + e' = 0 \tag{1.7}$$

con $b' = \dfrac{b}{a}$, $c' = \dfrac{c}{a}$, $d' = \dfrac{d}{a}$ y $d' = \dfrac{e}{a}$.

Mediante la siguiente transformación de Tchirnhausen $y = x + \dfrac{b'}{4}$ el problema de la ecuación de cuarto grado se reduce a resolver

$$y^4 + py^2 + qy + r = 0 \tag{1.8}$$

con $p = \dfrac{8c' - 3b'^2}{8}$, $q = \dfrac{b'^3 - 4b'c' + 8d'}{8}$ y $r = \dfrac{-3b'^4 + 16b'^2c' - 64b'd' + 256e'}{256}$.

¿Cómo resolvemos $y^4+py^2+qy+r=0$?

El método que utilizaremos fue presentado por Descartes en 1637; De todas maneras cabe mencionar que como dijimos anteriormente esta había sido resuelta por Luigi Ferrari en 1545.

La idea es factorizar de la siguiente manera $y^4+py^2+qy+r=(y^2+jy+l)(y^2-jy+m)$ por lo que desarrollando la expresión del lado derecho tenemos que:

$$\begin{aligned} l+m-j^2 &= p && (1.9)\\ jm-jl &= q && (1.10)\\ lm &= r && (1.11)\end{aligned}$$

Restando y sumando 1.9 y 1.10 tenemos que

$$\begin{aligned} 2l &= j^2+p-\frac{q}{j} && (1.12)\\ 2m &= j^2+p+\frac{q}{j} && (1.13)\end{aligned}$$

Y reemplazando 1.11 obtenemos la siguiente ecuación

$$(j^2)^3+2p(j^2)^2+(p^2-4r)j^2-q^2=0$$

Entonces por la ecuación de tercer grado obtenemos j y luego l y m.

Por último se resuelven $y^2+jy+l=0$ y $y^2-jy+m=0$

Ejemplo 1.2 *Resolver la ecuación* $x^4-6x^2-8x-3=0$

Resolución: Para encontrar la factorización en dos polinomios cuadráticos debemos resolver

$$(j^2)^3-12(j^2)^2+48j^2-64=0$$

que es lo mismo que

$$(j^2-4)^3=0$$

lo que implica que

$$j^2-4=0$$

por lo que $j=\pm 2$. Luego usando las ecuaciones 1.12 y 1.13 obtenemos que

$$l=\frac{4-6+4}{2}=1$$

$$m=\frac{4-6-4}{2}=-3$$

Así

$$\begin{aligned} x^4-6x^2-8x-3 &= (x^2+2x+1)(x^2+2x-3)\\ &= (x+1)(x+1)(x-1)(x+3)\end{aligned}$$

Finalmente las raíces buscadas son $1,-3$ y -1 con multiplicidad dos.

Capítulo 2
Cuerpos y polinomios

En este capítulo recordaremos la definición de cuerpo y estudiaremos las propiedades de $K[x]$ donde K es un cuerpo, es decir, el conjunto de los polinomios en la indeterminada x que tienen sus coeficientes en un cuerpo. Además veremos algunas propiedades de las raíces de estos polinomios.

2.1. Definición de cuerpo

El estudio de los cuerpos es fundamental para nuestro objetivo puesto que es la estructura algebraica ideal para estudiar raíces de polinomios debido a que en esta estructura podemos tanto sumar, restar, multiplicar y dividir sin problemas.

Antes de definir cuerpo recordaremos las definiciones de grupo y anillo las que estarán presentes en la definición de cuerpo.

Definición 2.1 *Un grupo G, es un conjunto no vacío provisto de una operación cerrada $*$, tal que se verifican la siguientes propiedades:*

1. *$\star$ es asociativa: $g \star (h * f) = (g * h) * f$.*
2. *Existe un elemento neutro: $\exists\ e \in G / e * g = g * e = g\ \forall\ g \in G$.*
3. *Existe el elemento inverso: $\forall\ g \in G\ \exists\ g^{-1} / g^{-1} * g = g * g^{-1} = e$.*

Un grupo G es abeliano si su operación $*$ es conmutativa $(g * h = h \star g)$.

Ejemplo 2.1 *$\mathbb{Z}$ y $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \,/\, a, b \in \mathbb{Z}\}$ con p primo son grupos abelianos.*

Ejemplo 2.2 *$G = \{(a, b) / a \in \mathbb{Q} \setminus \{0\}, b \in \mathbb{Q}\}$ con la siguiente operación:*

$$(a, b) \star (c, d) = (ac, ad + b)$$

es un grupo no abeliano.

Definición 2.2 *Un anillo A, es un conjunto, provisto de dos operaciones, $\oplus$ y $\otimes$ (Suma y multiplicación), de modo que se verifican las siguientes propiedades:*

1. *A es un grupo abeliano respecto $\oplus$.*
2. *$\otimes$ es una operación asociativa en A.*
3. *Se cumplan las leyes distributivas $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ y $c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$.*

Un anillo A se dice conmutativo si su operación cerrada $\otimes$ es conmutativa $(g \otimes h = h \otimes g)$.

Ejemplo 2.3 *$M_{n\times n}(\mathbb{R})$ es un anillo no conmutativo.*

Ejemplo 2.4 *$\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z} = \{(x, y, z) \,/\, x \in \mathbb{Z}, y \in \mathbb{Q}, z \in \mathbb{Z}\}$ con las siguiente operaciones:*

$$(a, b, c) \oplus (e, f, g) = (a + e, b + f, c + g), \qquad (a, b, c) \odot (e, f, g) = (a \cdot e, b \cdot f, c \cdot g).$$

donde $+$ y $\cdot$ son la suma y el producto usual de números reales es un anillo conmutativo.

Observación 2.1 *Desde ahora en adelante anotaremos $a \otimes b$ como ab.*

Definición 2.3 *Un cuerpo K es un anillo tal que $K - \{0\}$ es un grupo abeliano respecto a la multiplicación.*

Ejemplo 2.5 *$\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.*

Ejemplo 2.6 *$\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \,/\, a, b \in \mathbb{Q}\}$ con p primo es un cuerpo.*

Definición 2.4 *Diremos que un cuerpo tiene característica n, si n es el menor número natural tal que $1 + 1 + 1 + ... + 1$ para n sumandos es igual a 0. Si esta suma fuera siempre distinta de cero se dice que el cuerpo tiene característica cero.*

Ejemplo 2.7 *$\mathbb{R}$ es un cuerpo con característica cero y $\mathbb{Z}_p$ con p primo es un cuerpo con característica p.*

2.2. Polinomios

El objetivo de esta sección es estudiar nociones de anillos de polinomios, puesto que nos interesa saber que estructura tiene el conjunto de los polinomios con coeficientes en un cuerpo K.

¿Qué es formalmente un polinomio?

Definición 2.5 *Sea A un anillo. Un polinomio $f(x)$ con coeficientes en A, es una suma formal infinita*

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + ... + a_n x^n + ...,$$

donde x es una indeterminada y $a_i \in A$ con $a_i = 0$ para todo i, excepto un número finito de valores de subindices.

Definición 2.6 *Si $f(x)$ es un polinomio es de la forma:*

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + ... + a_n x^n + ...,$$

entonces diremos que si para alguna $i > 0$ es cierto que $a_i \neq 0$, el mayor de dichos valores de i es el grado de $f(x)$ y se escribe grad $f(x)$ o también $\partial f(x)$. De no existir $i > 0$, entonces el grado de $f(x)$ es de grado cero .

Observación 2.2 *El grado del polinomio $f(x) = 0$ lo dejaremos sin definir.*

Definición 2.7 *Diremos que $f(x) \in A[x]$ es un polinomio constante si $\partial f(x) = 0$ o $f(x) = 0$*

La suma y multiplicación de polinomios con coeficientes en A están definidas de la siguiente manera. Sean $f(x) = a_0 + a_1 x + ... + a_n x^n + ...$, y $g(x) = b_0 + b_1 x + ... + b_n x^n + ...$, entonces, para el polinomio suma tenemos:

$$f(x) + g(x) = c_0 + c_1 x + ... + c_n x^n + ..., \text{donde } c_n = a_n + b_n$$

y para el polinomio multiplicación, tenemos:

$$f(x) \cdot g(x) = d_0 + d_1 x + ... + d_n x^n + ..., \text{donde } d_n = \sum_{i=0}^{n} a_i b_{n-i}$$

El conjunto formado por todos los polinomios con coeficientes en un anillo A en la indeterminada x es un anillo y lo denotaremos $A[x]$. La demostración de que $A[x]$ es un anillo no es complicada pero si bastante engorroso por lo que la omitiremos.

Si A es un anillo y x_1, x_2 son indeterminadas, podemos formar el anillo $(A[x_1])[x_2]$ el que es naturalmente isomorfo a $(A[x_2])[x_1]$. Identificaremos estos anillos mediante un isomorfismo con $A[x_1, x_2]$. Análogamente podemos definir $A[x_1, x_2, ..., x_n]$ para polinomios en n indeterminadas con coeficientes en A. Notar que $A[x_1, x_2]$,$A[x_1, x_2, x_3]$,..., $A[x_1, x_2, ..., x_n]$ corresponden a polinomios de varias variables.

¿Que estructura tiene K[x]?

Como dijimos al inicio de la sección nos interesa saber que tipo de estructura es $K[x]$ cuando K es un cuerpo, es por eso que previamente vamos a recordar las definiciones de algunos casos especiales de anillo.

Definición 2.8 *Una anillo A con identidad multiplicativa 1, es decir, $1x = x1 = x$ para todas las $x \in A$ es un anillo unitario. Llamaremos unitario a la identidad multiplicativa de un anillo.*

Ejemplo 2.8 *$\mathbb{Z}$ y $\mathbb{Z}_n$ para cualquier n en los naturales son anillos conmutativo unitario.*

Definición 2.9 *Si a y b son dos elementos distintos de cero de un anillo A tal que $ab = 0$, entonces a y b son divisores de cero.*

Ejemplo 2.9 *Sean* $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$ *luego multiplicando ambas matrices tenemos que:*

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

por lo tanto A, B *son divisores de cero.*

Definición 2.10 *Un dominio entero* D *es un anillo conmutativo unitario que no contiene divisores de cero.*

Ejemplo 2.10 $\mathbb{Z}$ *y* $\mathbb{Z}_p$ *para cualquier* p *primo son dominios enteros.*

Observación 2.3 *Así como a través de los enteros podemos construir el cuerpo de los racionales, a partir de un dominio entero podemos construir el campo de las fracciones de este dominio entero.*

Definición 2.11 *Se dice que un dominio entero* D *es un dominio euclidiano si existe una función* $d : D - \{0\} \to \mathbb{N}$ *tal que:*

1. *Para cualesquiera* $a, b \in D - \{0\}$, $d(a) \leq d(ab)$.
2. *Para cualesquiera* $a, b \in D - \{0\}$, *existen* $t, r \in A$ *tales que* $a = tb + r$, *con* $r = 0$ *o* $d(r) < d(b)$.

Ejemplo 2.11 $\mathbb{Z}$ *es un dominio euclidiano con* $d(a) =\mid a \mid$.

Ejemplo 2.12 *Si* K *es un cuerpo* $K[x]$ *es un dominio euclidiano con* $d\left(f(x)\right) = \partial f(x)$.

K[x] es un dominio euclidiano

La importancia de un dominio euclidiano es que en él se tiene un análogo al algoritmo de euclides en $\mathbb{Z}$.

Definición 2.12 *Un elemento* u *de un dominio entero* D *es una unidad de* D *si* u *divide* 1, *esto es, si* u *tiene inverso multiplicativo en* D.

Ejemplo 2.13 *Los enteros* 1 *y* -1 *son unidades en* $\mathbb{Z}$ *y los polinomios constantes son unidades en* $K[x]$ *donde* K *es un cuerpo.*

Definición 2.13 *Dos elementos* $a, b \in D$ *donde* D *es un dominio entero se dicen asociados si* $a = bu$, *donde* u *es una unidad en* D.

Ejemplo 2.14 *Los enteros* 2 *y* -2 *son asociados en* $\mathbb{Z}$ *y los polinomios* $x^2 - 2$ *y* $2x^2 - 4$ *son asociados en* $\mathbb{Q}[x]$.

Teorema 2.1 (Algoritmo de la división para K[x]) *Sean* $f(x) = a_0 + a_1x + ... + a_nx^n + ...$, *y* $g(x) = b_0 + b_1x + ... + b_mx^m + ...$, *dos elementos de* $K[x]$, *con* a_n *y* b_m *distintos del cero de* K *y* $m > 0$. *Entonces, existen dos polinomios únicos* $q(x)$ *y* $r(x)$ *en* $K[x]$ *tales que*

$$f(x) = g(x)q(x) + r(x)$$

donde $r(x) = 0$ *o el* $\partial r(x)$ *es menor que el* $\partial g(x)$.

La demostración de este teorema es análoga a la demostración del algoritmo de Euclides en $\mathbb{Z}$ (ver, por ejemplo, [8])

Definición 2.14 *Si* $f(x), g(x) \in K[x]$ *se dice que* $d(x) \in K[x]$ *es un máximo común divisor de* $f(x)$ *y* $g(x)$ *si* $d(x)/f(x)$ *y* $d(x)/g(x)$ *y cualquier otro divisor común de* $f(x)$ *y* $g(x)$ *divide* $d(x)$.

Definición 2.15 *Si* $f(x), g(x) \in K[x]$ *se dice que estos son primos relativos si el máximo común divisor entre ellos es igual a* 1.

Algunas consecuencias importantes

Teorema 2.2 *Dados dos polinomios en* $K[x]$ *no simultáneamente nulos, tienen un máximo común divisor y es único salvo unidades.*

Demostración: Sean $a(x), b(x) \in K[x]$ supongamos que $\partial a(x) > \partial b(x)$.

$$\begin{array}{rcll} a(x) & = & q_1(x)b(x) + r_1(x), & 0 < \partial r_1(x) < \partial b(x) \\ b(x) & = & q_2(x)r_1(x) + r_1(x), & 0 < \partial r_2(x) < \partial r_1(x) \\ r_1(x) & = & q_3(x)r_2(x) + r_3(x), & 0 < \partial r_3(x) < \partial r_2(x) \\ \vdots & & \vdots & \vdots \\ r_{k-3}(x) & = & q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x), & 0 < \partial r_{k-1}(x) < \partial r_{k-2}(x) \end{array}$$

El proceso debe terminar para algún $r_k(x) = 0$ pues

$$\partial r_{k-1}(x) < \partial r_{k-2}(x) < ... < \partial r_1(x) < \partial b(x)$$

y entre 0 y $\partial b(x)$ hay un número finito de enteros y por lo tanto $r_{k-2}(x) = q_k(x)r_{k-1}(x)$. Como $r_{k-1}(x)/r_{k-1}(x) \wedge r_{k-1}(x)/r_{k-2}(x)$, entonces $r_{k-1}(x)/r_{k-3}(x)$ y así sucesivamente $r_{k-1}(x)/b(x)$ y $r_{k-1}(x)/a(x)$. Por lo que el mcd entre $r_{k-1}(x)$ y 0 es el mismo que el mcd entre $a(x), b(x)$ el que debe ser $r_{k-1}(x)$ o $\lambda r_{k-1}(x)$ lo que prueba lo deseado.

Teorema 2.3 *Si* $a(x), b(x) \in K[x] - \{0\}$ *y* $d(x)$ *es su máximo común divisor, entonces existen* $h(x), s(x) \in K[x]$ *tales que* $d(x) = a(x)h(x) + b(x)s(x)$.

Demostración: Del teorema anterior tenemos que

$$\begin{array}{rcll} a(x) & = & q_1(x)b(x) + r_1(x), & 0 < \partial r_1(x) < \partial b(x) \\ b(x) & = & q_2(x)r_1(x) + r_1(x), & 0 < \partial r_2(x) < \partial r_1(x) \\ r_1(x) & = & q_3(x)r_2(x) + r_3(x), & 0 < \partial r_3(x) < \partial r_2(x) \\ \vdots & & \vdots & \vdots \\ r_{k-4}(x) & = & q_{k-2}(x)r_{k-3}(x) + r_{k-2}(x), & 0 < \partial r_{k-2}(x) < \partial r_{k-3}(x) \\ r_{k-3}(x) & = & q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x), & 0 < \partial r_{k-1}(x) < \partial r_{k-2}(x) \end{array}$$

y de la última fila obtenemos que $r_{k-1}(x) = r_{k-3}(x) - q_{k-1}(x)r_{k-2}(x)$ análogamente de la penúltima fila obtenemos que $r_{k-2}(x) = r_{k-4}(x) - q_{k-2}(x)r_{k-3}(x)$ y así podemos escribir $r_{k-1}(x) = [1 + q_{k-1}(x)q_{k-2}(x)]r_{k-3}(x) - q_{k-1}(x)r_{k-4}(x)$, por lo que repitiendo este proceso podremos escribir $r_{k-1}(x)$ en función de $a(x)$ y $b(x)$. Finalmente como $r_{k-1}(x)$ es igual a $d(x)$ salvo unidades hemos probado lo deseado.

Corolario 2.3.1 *Si $a(x), b(x) \in K[x]-\{0\}$ son primos relativos, entonces existen $h(x), s(x) \in K[x]$ tales que $1 = a(x)h(x) + b(x)s(x)$.*

Demostración: Es consecuencia inmediata del teorema anterior.

Antes de continuar recordemos algunas definiciones.

Definición 2.16 *Sea A un anillo, se dice que un subanillo I es un ideal si:*

1. *$a, b \in I \Rightarrow a + b \in I$.*
2. *$a \in A \Rightarrow aI \subseteq I$ y $Ia \subseteq I$.*

Observación 2.4 *Si un ideal I de un anillo con unitario A contiene una unidad u, entonces $I = A$, debido a que si $u \in I$ tenemos que $1 = u^{-1}u \in I$ y si $a \in A$ tenemos que $a = a \cdot 1 \in I$ por lo que todo elemento de A está en I.*

Definición 2.17 *Si I es un ideal diferente de A tal que no existe ningún ideal propio N de A que contenga propiamente a I diremos que I es ideal maximal de una anillo A.*

Ejemplo 2.15 *Los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ donde n es un entero cualquiera y si p es un primo los ideales de la forma $p\mathbb{Z}$ son ideales maximales.*

No es difícil ver que $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ es un cuerpo si y solo si p es primo, lo que no es una casualidad puesto que se puede probar que si A un anillo conmutativo unitario entonces A/I es un campo I si y sólo si I es un Ideal maximal de A.

Definición 2.18 *Un ideal $I \neq A$ en un anillo conmutativo A es un un ideal primo si $ab \in I$ implica que $a \in I$ o $b \in I$ para todo $a, b \in A$.*

Los ideales de $\mathbb{Z}$ de la forma $p\mathbb{Z}$ con p primo cumplen la propiedad que si $ab \in p\mathbb{Z}$ entonces p divide a a o b lo que motiva el nombre de la definición anterior.

Definición 2.19 *Un ideal de un dominio D es principal si esta generado por un solo elemento, es decir, si es de la forma $\langle a \rangle = \{ra/r \in A\}$.*
Un dominio de ideales principales(DIP) es un dominio entero en el que todo ideal I es un ideal principal.

Ejemplo 2.16 *El conjunto $\langle x \rangle$ de todos los polinomios que tienen término constante igual a cero en $K[x]$ es un ideal principal.*

Teorema 2.4 *En un dominio entero, todo ideal maximal es primo.*

Demostración: Si M un ideal maximal en un dominio entero D y $ab \in M$, pero si $a \notin M$, tenemos que $M \subset M+\langle a \rangle \subset D$ y como $M \neq M+\langle a \rangle$ y M es maximal entonces $M+\langle a \rangle = D$, por lo que $1 = m + xa$ con $m \in M$ y $x \in D$, de esta manera $b = mb + xab$ luego $b \in M$. Análogamente si $b \notin M$ tendremos que $a \in M$ lo que prueba que M es primo.

K[x] es un dominio de ideales principales

Teorema 2.5 *Si K es un cuerpo $K[x]$ es un DIP.*

Demostración: Sea I un ideal de $K[x]$. Si $I = \{0\}$ entonces $I = \langle 0\rangle$. Ahora si $I \neq \{0\}$ y $s(x)$ es un polinomio en I tal que $\partial s(x)$ es mínimo en I. Si $f(x) \in I$ por el algoritmo de euclides en $K[x]$ tenemos que $f(x) = s(x)q(x) + r(x)$ donde $r(x) = 0$ o $\partial r(x) < \partial s(x)$. Pero como $r(x) = f(x) - s(x)q(x)$ y $f(x), s(x) \in I$ entonces $r(x) \in I$ y como $s(x)$ es el polinomio de grado mínimo en I tenemos que $\partial s(x) < \partial r(x)$ por lo que hace imposible que $\partial r(x) < \partial s(x)$. Por lo tanto $r(x) = 0$ de manera que $f(x) = s(x)q(x)$ por lo que $f(x) \in \langle s(x)\rangle$ y como esto se cumple para todo $f(x) \in I$ tenemos que $I = \langle s(x)\rangle$ lo que prueba lo deseado.

Definición 2.20 *Sean $f(x), g(x) \in K[x]$, diremos que $g(x)$ divide a $f(x) \in K[x]$ si existe $q(x) \in K[x]$ tal que $f(x) = g(x)q(x)$, y se denota $g(x)/f(x)$.*

Definición 2.21 *Un polinomio no constante $f(x)$ es irreducible sobre K o es un polinomio irreducible en $K[x]$, si en cualquier factorización $f(x) = g(x)h(x)$ de dos polinomios en $K[x]$, $g(x)$ o $h(x)$ es una unidad .*

Ejemplo 2.17 *El polinomio $f(x) = x^2 - 3$ es irreducible en $\mathbb{Q}[x]$; no obstante $f(x)$ no es irreducible en $\mathbb{Q}(\sqrt{3})[x]$. pues $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3}) \in \mathbb{Q}(\sqrt{3})$.*

Ejemplo 2.18 *El polinomio $f(x) = x^2 + 1$ es irreducible en $\mathbb{R}[x]$; no obstante $f(x)$ no es irreducible en $\mathbb{C}[x]$. pues $x^2 + 1 = (x - i)(x + i) \in \mathbb{C}[x]$.*

Teorema 2.6 *Un ideal $\langle p(x)\rangle \neq \{0\}$ de $K[x]$ es maximal si y sólo si $p(x)$ es irreducible sobre K.*

Demostración: $\Rightarrow$) Supongamos que $\langle p(x)\rangle \neq \{0\}$ es un ideal maximal de $K[x]$ entonces $\langle p(x)\rangle \neq K[x]$ y por lo tanto $p(x)$ no es una unidad en $K[x]$. Si $p(x)$ no es un irreducible en $K[x]$ entonces $p(x) = f(x)q(x)$ es una factorización de $p(x)$ en $K[x]$ donde $f(x)$ y $q(x)$ no pueden ser una unidad en $F[x]$ por lo que los grados de $f(x)$ y $q(x)$ son menores que el grado de $p(x)$, además tenemos que $p(x) = f(x)q(x) \in \langle p(x)\rangle$, pero como $\langle p(x)\rangle$ es ideal maximal es también un ideal primo lo que implica que $f(x) \in \langle p(x)\rangle$ o $q(x) \in \langle p(x)\rangle$ por lo que $p(x)$ es factor de $f(x)$ o de $q(x)$ lo que es imposible porque el grado de $p(x)$ es mayor que el grado de $q(x)$ y de $f(x)$. Lo que prueba que $p(x)$ es un irreducible en $K[x]$.
$\Leftarrow$) Supongamos que $p(x)$ es un irreducible en $K[x]$ y que I es un ideal maximal tal que $\langle p(x)\rangle \subseteq I \subset K[x]$. Como $K[x]$ es un DIP entonces existe un $g(x) \in I$ tal que $I = \langle g(x)\rangle$ entonces tenemos que $p(x) = g(x)q(x)$ y como $p(x)$ es irreducible $g(x)$ o $q(x)$ es una unidad. Si $g(x)$ es una unidad $I = K[x]$ lo que no es posible porque I es ideal maximal por lo que $q(x)$ es una unidad entonces tenemos $g(x) = p(x)(q(x))^{-1}$ por lo que $g(x) \in \langle p(x)\rangle$ entonces $\langle p(x)\rangle = I$ lo que prueba que $\langle p(x)\rangle$ es maximal.

Teorema 2.7 *Sea $p(x)$ un polinomio irreducible en $K[x]$. Si $p(x)$ divide $r_1(x)r_2(x)$ para $r_1(x), r_2(x) \in K[x]$, entonces $p(x)$ divide $r_1(x)$ o $p(x)$ divide $r_2(x)$.*

Demostración: Supongamos que $p(x)$ es un polinomio irreducible en $K[x]$ tal que $p(x)$ divide $r_1(x)r_2(x)$, entonces $r_1(x)r_2(x) \in \langle p(x)\rangle$ y $\langle p(x)\rangle$ es un ideal maximal y por lo tanto un ideal primo lo que implica que $r_1(x) \in \langle p(x)\rangle$ o $r_2(x) \in \langle p(x)\rangle$. Ahora si $r_1(x) \in \langle p(x)\rangle$ tenemos que $p(x)$ divide a $r_1(x)$ o si $r_2(x) \in \langle p(x)\rangle$ tenemos que $p(x)$ divide a $r_2(x)$.

Corolario 2.7.1 *Sea $p(x)$ un polinomio irreducible en $K[x]$. Si $p(x)$ divide $r_1(x)....r_n(x)$ para $r_1(x), ..., r_n(x) \in K[x]$, entonces $p(x)$ divide a algún $r_1(x), ..., r_n(x)$.*

Demostración: Inducción sobre n.

Definición 2.22 *Un dominio entero D es un dominio de factorización única (DFU), si se satisfacen que:*

1. *Todo elemento de D que no sea ni 0 ni una unidad se puede factorizar en un número finito de irreducibles.*
2. *Si $p_1...p_r$ y $q_1..q_s$ son factorizaciones en irreducibles del mismo elemento de D, entonces $r = s$ y q_j pueden renumerarse de manera que p_i y q_i sean asociados.*

K[x] es un dominio de factorización única

Teorema 2.8 *Si K un cuerpo entonces $K[x]$ es un DFU.*

Demostración: Sea $f(x) \in K[x]$ un polinomio no constante. Si $f(x)$ no es irreducible entonces $f(x) = g(x)h(x)$ donde $g(x)$ y $h(x)$ no pueden ser unidades por lo que los grados de $g(x)$ y $h(x)$ son menores que el grado de $f(x)$. Si $g(x)$ y $h(x)$ son polinomios irreducibles $f(x)$ nos detenemos aqui. Si esto no ocurre alguno de ellos se factoriza en polinomios de grado menor y así sucesivamente ,pero como el grado es finito este proceso debe terminar por lo que $f(x) = p_1(x)p_2(x)....p_n(x)$ donde los $p_i(x)$ son irreducibles.

Ahora nos falta mostrar la unicidad. Supongamos que $f(x) = p_1(x)p_2(x)....p_r(x)$ y que $f(x) = q_1(x)q_2(x)....q_s(x)$ son dos factorizaciones en irreducibles de $f(x)$ en $K[x]$ donde $r \leq s$ entonces $p_1(x)$ divide a $q_1(x)q_2(x)....q_s(x)$ y por el corolario 2.7.1 $p_1(x)$ divide algún $q_1(x), q_2(x), ..., q_s(x)$, ahora si suponemos que divide a $q_1(x)$ y como $q_1(x)$ es irreducible $q_1(x) = p_1(x)u_1$ donde $u_1 \neq 0$ es una unidad . Luego si sustituimos $q_1(x)$ por $u_1p_1(x)$ tenemos que:

$$p_1(x)p_2(x)....p_r(x) = p_1(x)u_1q_2(x)....q_s(x)$$

y cancelando p_1 a la derecha obtenemos.

$$p_2(x)....p_r(x) = u_1q_2(x)....q_s(x)$$

repitiendo el mismo razonamiento podemos decir que $q_2(x) = p_2(x)u_2$ y reemplazando y cancelando de la misma manera obtenemos:

$$p_3(x)....p_r(x) = u_1u_2q_3(x)....q_s(x)$$

continuado de la misma manera llegaremos a:

$$1 = u_1u_2...u_rq_{r+1}(x)....q_s(x)$$

lo que es posible si $r = s$ por lo que la igualdad debe ser $1 = u_1u_2...u_r$, por lo que irreducibles son los mismos salvo por el orden y por factores unidad por lo que los $q_r(x)$ pueden renumerarse de manera que $p_r(x)$ y $q_r(x)$ sean asociados lo que prueba lo deseado.

2.3. Raíces de polinomios

Definición 2.23 *Sea K un subcuerpo de un cuerpo E, α un elemento de E y $f(x) = a_0 + a_1x + ... + a_nx^n$ en $K[x]$. Entonces α se llama raíz de $f(x)$ si y solo si $f(\alpha) = 0$.*

Teorema 2.9 *Un elemento $\alpha \in K$ es un cero de $f(x) \in K[x]$ si y sólo si $x - \alpha$ es factor de $f(x)$ en $K[x]$.*

Demostración: $\Rightarrow$) Supongamos que para $\alpha \in K$ tenemos que $f(\alpha) = 0$ por el algoritmo de euclides para $K[x]$ existen $q(x)$, $r(x) \in K[x]$ tales que:

$$f(x) = (x - \alpha)q(x) + r(x)$$

donde el grado de $r(x)$ es menor que el grado de $(x - \alpha)$ que es igual a 1. Entonces $r(x) = c$ para $c \in K$, luego tenemos que:

$$f(x) = (x - \alpha)q(x) + c$$

Evaluando $f(\alpha)$ tenemos que:

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + c = 0q(x) + c = 0 + c = c$$

Por lo tanto $c = 0$, entonces $f(x) = (x - \alpha)q(x)$ lo que prueba que $(x - \alpha)$ es factor de $f(x)$.
$\Leftarrow$) Supongamos que $(x - \alpha)$ es factor de $f(x)$ en $K[x]$ donde $a \in K$, luego como $(x - \alpha)$ es factor de $f(x)$ existe $q(x)$ tal que

$$f(x) = (x - \alpha)q(x)$$

ahora evaluando a en $f(x)$ tenemos que:

$$f(\alpha) = (\alpha - \alpha)q(x) = 0q(x) = 0$$

lo que prueba que α es raíz de $f(x)$

Definición 2.24 *Sea a un cero de un polinomio $f(x)$ de $K[x]$. se dice que tiene multiplicidad n si $(x - \alpha)^n / f(x)$ y $(x - \alpha)^{n+1} \not| f(x)$.*

¿Cuántas raíces puede tener un polinomio?

Corolario 2.9.1 *Un polinomio distinto de cero $f(x) \in K[x]$ de grado n puede tener a los más n ceros en un cuerpo K considerando sus raíces múltiples .*

Demostración: Probaremos este corolario usando inducción matemática sobre el grado del polinomio:

a) Si $n = 1$ entonces $f(x) = a_0 + a_1x = a_1\left(\frac{a_0}{a_1} + x\right)$, luego $\frac{a_0}{a_1}$ es el único cero. Por lo que $f(x)$ tiene a lo más 1 cero.

b) Supongamos que todo polinomio de grado n tiene a lo más n ceros. Ahora lo que debemos demostrar es que si el grado de un polinomio $f(x)$ es igual a $n+1$ tiene a lo más $n+1$ ceros.

Si $f(x)$ no tiene ningún cero entonces el corolario se cumple. Si a es un cero de $f(x)$ tenemos por la proposición anterior que $f(x) = (x-\alpha)q(x)$ donde $\partial q(x) = n$. Luego por hipótesis de inducción tenemos que $q(x)$ tiene a los más n ceros y como los ceros de $f(x)$ son a y los ceros de $q(x)$ tiene a lo más $n+1$ ceros lo que prueba lo deseado.

Capítulo 3
Extensiones de cuerpos

En este capítulo nos concentraremos en presentar el lugar en donde viven las raíces de los polinomios, caracterizando estos conjuntos y estudiando algunas de sus propiedades, las que serán fundamentales a la hora de conocer la solución de nuestro problema.

3.1. Introducción a las extensiones de cuerpo

Como decíamos anteriormente la estructura de cuerpo es ideal para estudiar raíces de polinomios pero a veces es necesario extender estos cuerpos para encontrar dichas raíces .

Definición 3.1 *Diremos que el cuerpo E es una extensión de K, si K es subcuerpo de E. Para denotar una extensión usaremos E/K o $E : K$.*

Ejemplo 3.1 $\mathbb{C}$ *es un cuerpo de extensión de* $\mathbb{R}$ *y* $\mathbb{R}$ *es un cuerpo de extensión de* $\mathbb{Q}$.

Ejemplo 3.2 $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$ *es un cuerpo de extensión de* $\mathbb{Q}$.

¿Todo polinomio siempre tiene alguna raíz en algún cuerpo?

Teorema 3.1 (Kronecker) *Sea K un cuerpo y sea $f(x)$ un polinomio no constante en $K[x]$. Entonces, existe un cuerpo de extensión E de K y algún $\alpha \in E$ tal que $f(\alpha) = 0$.*

Demostración: Como $K[x]$ es un DFU, $f(x)$ tiene factorización en polinomios irreducibles en $K[x]$. Sea $p(x)$ un factor irreducible de $f(x)$. Luego como $p(x)$ es irreducible tenemos que $\langle p(x)\rangle$ es un ideal maximal en $K[x]$ y como $\langle p(x)\rangle$ es un ideal maximal en $K[x]$ entonces $K[x]/\langle p(x)\rangle$ es un cuerpo. Veamos que $K[x]/\langle p(x)\rangle$ es una extensión de K. Para esto veremos que K es isomorfo a algún subcuerpo de $K[x]/\langle p(x)\rangle$. Consideremos el siguiente conjunto $\{a + \langle p(x)\rangle/a \in K\}$ y la siguiente transformación $\psi : K \longrightarrow K[x]/\langle p(x)\rangle$ definida por $\psi(a) = a + \langle p(x)\rangle$ para $a \in K$. Es fácil ver que esta transformación es un homomorfismo tomando como representante de la clase de $(a + \langle p(x)\rangle)$ precisamente a a, Además esta es uno a uno. En efecto, sean $a, b \in K$ entonces si $\psi(a) = \psi(b)$, es decir $a + \langle p(x)\rangle = b + \langle p(x)\rangle$ para $a, b \in K$, tenemos que $(a - b) \in \langle p(x)\rangle$ por lo que $p(x)$ tiene que ser factor de $(a - b)$ o $(a - b) = 0$, pero como $a, b \in K$ tenemos que $(a - b) \in K$, no queda otra opción que $(a - b) = 0$ por lo que $a = b$ lo que prueba la inyectividad. Para completar la demostración falta ver que existe $\alpha \in K[x]/\langle p(x)\rangle$ tal que $f(\alpha) = 0$. Si $\alpha = x + \langle p(x)\rangle$ y suponemos que

$p(x) = a_0 + a_1x + ... + a_nx^n$ tenemos que $p(\alpha) = a_0 + a_1(x + \langle p(x)\rangle) + ... + a_n(x + \langle p(x)\rangle)^n$ y si elegimos a x como representante de la clase de $x + \langle p(x)\rangle$ entonces tenemos lo deseado que $p(\alpha) = (a_0 + a_1x + ... + a_nx^n) + \langle p(x)\rangle = p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0$.

Definición 3.2 *Un elemento α de un cuerpo K es algebraico sobre K si $f(x) = 0$ para algún $f(x) \in K(x)$ distinto de cero. Si α no es algebraico sobre K, es trascendente sobre K.*

Ejemplo 3.3 *i es algebraico sobre $\mathbb{R}$ y $\sqrt{2}$ es algebraico sobre $\mathbb{R}$.*

Ejemplo 3.4 *π y e son trascendente sobre $\mathbb{Q}$.*

Observación 3.1 *Sea E/K una extensión luego todo elemento a de un cuerpo K es algebraico pues es raíz del polinomio $x - a \in K[x]$.*

Definición 3.3 *Se dice que una extensión E/K es:*

1. *algebraica, si todo $\alpha \in E$ es algebraico sobre K.*
2. *trascendente, si todo $\alpha \in E$ es trascendente sobre K.*

Ejemplo 3.5 *La extensión $\mathbb{C}/\mathbb{R}$ es algebraica y la extensión $\mathbb{Q}(x)/\mathbb{Q}$ es trascendente.*

Definición 3.4 *Sea E/K y α un elemento de E; Se llama subcuerpo generado por α al menor subcuerpo de E que contiene K y α. Denotaremos este conjunto como $K(\alpha)$.*

Ejemplo 3.6 $\mathbb{R}(i) = \{a + bi \ / \ a, b \in \mathbb{R}\}$ *y* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ / \ a, b \in \mathbb{Q}\}$.

Observación 3.2 *Si α es trascendente sobre K, podemos definir $K[\alpha] = \{f(\alpha)/f(x) \in K[x]\}$ el cual es un dominio entero. Luego podemos construir el cuerpo de los cocientes que denotaremos como $K(\alpha) = \{\frac{f(\alpha)}{q(\alpha)}/f(x), q(x) \neq 0 \in K[x]\}$ el cual será el menor subcuerpo de una extensión E que contiene a α y K. Si α es algebraico podemos definir análogamente a $K[\alpha]$ y $K(\alpha)$, además se puede demostrar que $K[\alpha] = K(\alpha)$ el cual será el menor subcuerpo de una extensión E que contiene a α y K.*

Definición 3.5 *Sea E/K y $\alpha_1, \alpha_2, ..., \alpha_n$ elementos de E, se llama subcuerpo generado por $\alpha_1, \alpha_2, ..., \alpha_n$ al menor subcuerpo de E que contiene K y $\alpha_1, \alpha_2, ..., \alpha_n$. Denotaremos este conjunto como $K(\alpha_1, \alpha_2, ..., \alpha_n)$.*

Ejemplo 3.7 $\mathbb{C}(x, y)$ *el cuerpo de fracciones de los polinomios en dos variables sobre* $\mathbb{C}$.

Observación 3.3 *No es difícil probar que la intersección de todos los subcuerpos de E que contienen K y todas las α_i para $i = 1, 2, .., n$ es un cuerpo, tampoco es difícil ver que este será el menor subcuerpo que cumpla tales condiciones.*

Definición 3.6 *Se dice que una extensión E/K es simple si $E = K(\alpha)$.*

Ejemplo 3.8 $\mathbb{Q}(\sqrt{3} + \sqrt{5})/\mathbb{Q}$ *y* $\mathbb{R}(x)/\mathbb{R}$ *son simples y* $\mathbb{C}(x, y)/\mathbb{C}$ *no lo es.*

Observación 3.4 *Una extension puede ser simple aunque este generada por un conjunto de varios elementos. Por ejemplo porque se puede probar que* $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$.

Teorema 3.2 *Si* E/K *es una extensión de* K*, entonces* E *es un espacio vectorial sobre* K*.*

Demostración: Como E es un cuerpo es por definición un grupo abeliano con la suma además las propiedades con del producto por un escalar se cumplen trivialmente por las propiedades de grupo de la multiplicación del cuerpo y las propiedades distributivas de la suma respecto a la multiplicación en E.

Definición 3.7 *La dimensión de* E *como espacio vectorial sobre* K *se llama grado de* E/K *y se escribe* $[E:K]$*. Si el grado es finito se dice que la extensión es finita, Si el grado de la extensión no es finito se dice que la extensión es infinita.*

Teorema 3.3 *Si* E *es un cuerpo de extensión finita de un cuerpo* K *y* F *es un cuerpo de extensión finita de* E*, entonces* F *es una extensión finita de* K*, y*

$$[F:K] = [F:E][E:K].$$

Demostración: Sea $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ una base para E como espacio vectorial sobre K y sea $\{\beta_1, \beta_2, ..., \beta_m\}$ una base para F como espacio vectorial sobre E. Para demostrar este teorema basta con probar que $\{\alpha_1\beta_1, \alpha_1\beta_2, ..., \alpha_n\beta_m\}$ es una base para F como espacio vectorial sobre K
Primero Veamos que $\{\alpha_1\beta_1, \alpha_1\beta_2, ..., \alpha_n\beta_m\}$ generan F con coeficientes en K. Si $x \in F$ entonces como F es un espacio vectorial sobre E con base $\{\beta_1, \beta_2, ..., \beta_m\}$

$$x = \sum_{i=1}^{m} \lambda_i\beta_i = \lambda_1\beta_1 + \lambda_2\beta_2 + ... + \lambda_m\beta_m \text{ con } \lambda_i \in E \tag{3.1}$$

Pero como $\lambda_i \in K$

$$\lambda_i = \sum_{j=1}^{n} \mu_{ji}\alpha_j = \mu_{1i}\alpha_1 + \mu_{2i}\alpha_2 + ...\mu_{ni}\alpha_n \text{ con } \mu_{ni} \in K \tag{3.2}$$

Luego reemplazando 3.2 en 3.1 tenemos que:

$$x = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \mu_{ji}\alpha_j \right) \beta_i = \sum_{i.j} \mu_{ji} \left(\alpha_j\beta_i\right) \text{ con } \mu_{ji} \in K.$$

Ahora veamos que los elementos de $\{\alpha_1\beta_1, \alpha_1\beta_2, ..., \alpha_n\beta_m\}$ son linealmente independientes. Supongamos que

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \lambda_{ji}\alpha_j\beta_i = 0 \text{ con } \lambda_{ji} \in K$$

Lo que es lo mismo que

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} \lambda_{ji}\alpha_j \right) \beta_i = 0 \text{ con } \lambda_{ji} \in K$$

Pero como los términos entre paréntesis pertenecen a E y los $\beta_i, \beta_2, ..v\beta_m$ son una base de F, tenemos que

$$\sum_{j=1}^{n} \lambda_{ji}\alpha_j = 0 \text{ para todas las } i$$

Como los α_j son una base de E implica que $\lambda_{ji} = 0$ para toda las i, j.
Lo que prueba lo deseado.
Finalmente como el conjunto $\{\alpha_1\beta_1, \alpha_1\beta_2, ..., \alpha_n\beta_m\}$ genera y sus elementos son linealmente independientes son una base de F como espacio vectorial sobre K.

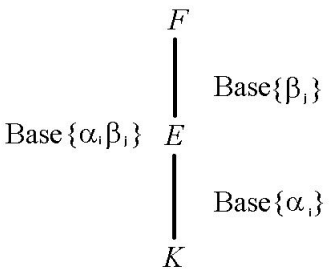

Figura 3.1: Torre de cuerpos

Corolario 3.3.1 *Si K_i es un cuerpo para $i = 1, ..., r$ y K_{i+1} es una extensión finita de K_i, entonces K_r es una extensión finita de K_1 y*

$$[K_r : K_1] = [K_r : K_{r-1}][K_{r-1} : K_{r-2}] \cdots [K_r : K_2] : [K_r : K_1]$$

.

Demostración: Inducción sobre n .

Definición 3.8 *Se dice que un polinomio de $f(x)$ es mónico si el coeficiente de mayor grado de x es igual* 1 .

Definición 3.9 *Si α es algebraico sobre K, se dice que $f(x) \in K[x]$ es el polinomio mínimo de α si $f(x)$ es mónico, α es cero de $f(x)$ y no hay otro polinomio de grado menor con estas características.*

Observación 3.5 *No es difícil ver que si $f(x)$ es el polinomio mínimo de α entonces:*

- *$f(x)$ es único.*
- *$f(x)$ es irreducible.*
- *Si $g(\alpha) = 0$ entonces $f(x)/g(x)$.*

Si α es algebraico ¿Cómo son los elementos de K(α)?

Teorema 3.4 *Sea E una extensión simple $K(\alpha)$ de un cuerpo K y sea α algebraico sobre K . Sea $n \geq 1$ el grado del polinomio mínimo de α, entonces:*

$$K(\alpha) = \{k_0 + k_1\alpha + ... + k_{n-1}\alpha^{n-1} \text{ con } k_i \in K\}.$$

Demostración: Sea $A = \{k_0 + k_1\alpha + ... + k_{n-1}\alpha^{n-1}$ con $k_i \in K\}$. Vamos a probar que A es un subcuerpo de $K(\alpha)$ ya que como $K(\alpha)$ es el menor subcuerpo entonces A debe ser igual a $K(\alpha)$. Notar que $\alpha \in A$ y que $A \subset K(\alpha)$ además es fácil ver que si $a, b \in A$ entonces $(a - b) \in A$ lo que prueba que A es un subgrupo abeliano para la operación suma. Ahora nos falta ver que A es un subgrupo abeliano para la multiplicación, es decir, que si $a, b \in A$ entonces $ab^{-1} \in A$. Como $a, b \in A$ entonces $a = q_1(\alpha)$ y $b = q_2(\alpha)$ donde $q_1(x), q_2(x) \neq 0 \in K[x]$ son polinomios de grado menor que n y además si $f(x)$ es el polinomio mínimo tenemos que $q_2(x)$ y $f(x)$ son primos relativos entre sí, por lo que existen $g(x), h(x) \in K[x]$ tales que $1 = f(x)g(x) + q_2(x)h(x)$. Luego si multiplicamos la igualdad anterior por $q_1(x)(q_2(x))^{-1}$ tenemos que $q_1(x)(q_2(x))^{-1} = q_1(x)(q_2(x))^{-1}g(x)f(x)+q_1(x)(q_2(x))^{-1}q_2(x)h(x)$ que evaluado en α es igual a $q_1(\alpha)(q_2(\alpha))^{-1} = q_1(\alpha)h(\alpha)$. Por último nos falta ver que $q_1(\alpha)h(\alpha)$ es de grado menor que n. Como $q_1(x)h(x) \in K[x]$ por el algoritmo de euclides tenemos que $q_1(x)h(x) = p(x)s(x) + r(x)$ con $\partial r(x) < \partial p(x) = n$ y evaluado en α tenemos que $q_1(\alpha)h(\alpha) = r(\alpha)$ lo que prueba lo deseado.

Corolario 3.4.1 *Sea E una extensión simple $K(\alpha)$ de un cuerpo K y sea α algebraico sobre K . Sea $n \geq 1$ el grado del polinomio mínimo de α, entonces $\{\alpha, ..., \alpha^{n-1}\}$ es una base de $K(\alpha)$.*

Demostración: Por el teorema anterior $\{\alpha, ..., \alpha^{n-1}\}$ generan $K(\alpha)$ como espacio vectorial sobre K, luego si estos fueran linealmente dependientes existiría una combinación lineal $k_0+k_1\alpha+...+k_{n-1}\alpha^{n-1} = 0$ con los k_i no todos nulos y así un polinomio $k_0+k_1x+...+k_{n-1}x^{n-1}$ que tiene como raíz α de grado menor que el polinomio mínimo $\Rightarrow\Leftarrow$ por lo tanto son linealmente independientes y así conforman un base de $K(\alpha)$ sobre K lo que prueba lo deseado.

Corolario 3.4.2 *Sea E una extensión simple $K(\alpha)$ de un cuerpo K y sea α algebraico sobre K . Sea $n \geq 1$ el grado del polinomio mínimo de α, entonces $[K(\alpha) : K] = n$.*

Demostración: Es consecuencia directa de que $\{\alpha, ..., \alpha^{n-1}\}$ es un base de $K(\alpha)$ como espacio vectorial sobre K.

Ejemplo 3.9 *Como la extensión $\mathbb{Q}(\sqrt[4]{5})$ es simple y $x^4 + 5$ es el polinomio mínimo de $\sqrt[4]{5}$ sobre $\mathbb{Q}$ tenemos que*

$$\mathbb{Q}(\sqrt[4]{5}) = \{a + b\sqrt[4]{5} + c\sqrt[4]{25} + d\sqrt[4]{125} \ / \ a, b, c, d \in \mathbb{Q}\}$$

donde $1, \sqrt[4]{5}, \sqrt[4]{25}, \sqrt[4]{125}$ es una base de $\mathbb{Q}(\sqrt[4]{5})$.

Teorema 3.5 *Sea E/K y sea $f(x)$ el polinomio mínimo de $\alpha \in E$ sobre K, entonces*

$$\psi : K[x]/\langle f(x)\rangle \to K(\alpha)$$

con $\psi(x + \langle f(x)\rangle) = \alpha$, define un isomorfismo de cuerpos.

Demostración: Consideremos el siguiente homomorfismo $\phi_\alpha : K[x] \to K(\alpha)$ definido por $\phi(g(x)) = g(\alpha)$. Es fácil ver que ϕ es sobreyectivo además el núcleo de ϕ es $\langle f(x)\rangle$ y así por el teorema fundamental del homomorfismo $K[x]/\langle f(x)\rangle \cong K(\alpha)$ y la imagen de $x + \langle f(x)\rangle$ es α lo que prueba lo deseado.

Ejemplo 3.10 $\mathbb{C}$ *es isomorfo a* $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

Teorema 3.6 *Toda extensión finita es algebraica.*

Demostración: Sea E/K una extensión finita de grado n y $\alpha \in E$, Ahora consideremos las siguientes potencias

$$1, \alpha, \alpha^2, ..., \alpha^n$$

Si dos de estas potencias son iguales, es decir, $\alpha^i = \alpha^j$ con $i \neq j$ implica que $\alpha^i - \alpha^j = 0$ por lo tanto α es raíz del polinomio $x^i - x^j \in E[x]$.
Si todas estas potencias son distintas, Existen coeficientes $\lambda_0, \lambda_1, ..., \lambda_n$ no todos nulos tal que $\lambda_0 + \lambda_1\alpha + ... + \lambda_n\alpha^n = 0$ puesto que E es un espacio vectorial de dimensión n, lo que implica que α es raíz del polinomio no nulo $\lambda_0 + \lambda_1 x + ... + \lambda_n x^n \in E[x]$
Lo que que prueba lo deseado.

3.2. Cerraduras algebraicas

¿Dónde viven las raíces de todos los polinomios de K[x]?

Definición 3.10 *Un cuerpo K es algebraicamente cerrado si todo polinomio no constante en $K[x]$ tiene algún cero en K.*

Observación 3.6 *La definición de cerradura algebraica es equivalente a las cualquiera de las siguientes condiciones:*

- *Todo polinomio no constante de $K[x]$ tiene todas sus raíces en K .*
- *Todo polinomio de $K[x]$ se descompone linealmente en $K[x]$.*
- *Los polinomios irreducibles en $K[x]$ son de grado 1.*
- *K no tiene extensiones algebraicas distintas de si misma.*

Ejemplo 3.11 $\mathbb{C}$ *es cerrado algebraicamente.*

Observación 3.7 *Si bien es conocido que $\mathbb{C}$ es la cerrado algebraicamente tendremos que esperar hasta el capítulo 4 para dar un demostración de este resultado.*

Para probar la existencia y la unicidad de las cerraduras algebraicas necesitaremos conocer algunos elementos de la teoría de conjuntos.

Definición 3.11 *Un* ***orden parcial en un conjunto*** S *está dado por una relación* $\leq$ *definida para ciertos pares ordenados de elementos de* S *tales que se satisfacen las siguientes condiciones*

- $a \leq a$ *para todo* $a \in S$, ***ley reflexiva***.
- *Si* $a \leq b$ *y* $b \leq a$, *entonces* $a = b$, ***ley antisimétrica***.
- *Si* $a \leq b$ *y* $b \leq c$, *entonces* $a \leq c$, ***ley transitiva***.

Definición 3.12 *Un* ***orden total en un conjunto*** T *si es parcialmente ordenado y cada par de elementos* a *y* b *en* T, *son comparables, es decir, si* $a \leq b$ *o* $b \leq a$.

Observación 3.8 *Un conjunto totalmente ordenado generalmente recibe el nombre cadena.*

Definición 3.13 *Sea* S *un conjunto parcialmente ordenado y* X *un subconjunto de* S *un elemento* $a \in S$ *es:*

- *Una cota superior de* X *si* $x \leq a$ *para todo* $x \in X$.
- *Una cota inferior de* X *si* $a \leq x$ *para todo* $x \in X$.
- *Un elemento maximal de* X *si* $a \in X$ *y* $x \nleq a$ *para todo* $x \in X$.
- *Un elemento minimal de* X *si* $a \in X$ *y* $a \nleq x$ *para todo* $x \in X$.

Ahora estamos en condiciones de conocer el ***Lema de Zorn*** que es lo que utilizaremos para probar la unicidad y existencia de cerraduras algebraicas.

Lema de Zorn *Si* S *es un conjunto parcialmente ordenado tal que toda cadena en* S *tienen una cota superior en* S, *entonces* S *tiene al menos un elemento maximal.*

Observación 3.9 *El lema de Zorn es equivalente al axioma de elección*

Existencia de una cerradura algebraica

Teorema 3.7 *Todo cuerpo* K *tienen una cerradura algebraica, es decir, una extensión algebraica* $\overline{K}$ *que esta algebraicamente cerrada.*

Demostración: Sea K un cuerpo y sea $S = \{E_i \ / \ i \in I\}$ el conjunto de todas las extensiones algebraicas de K ordenado parcialmente a través de la relación de inclusión usual $\leq$ de los subcuerpos.
Sea $T = E_{ij}$ una cadena en S y sea $W = \bigcup_j E_{ij}$. Notar que W es un cuerpo y además es una extensión algebraica de K por lo que $W \in S$. Además por construcción tenemos que :

$$E_{ij} \leq W \text{ para todo } \ E_{ij} \in T$$

Luego W es una cota superior para S.
$\therefore$ Por el Lema de Zorn existe al menos un elemento maximal.
Sea $\overline{K}$ este elemento maximal y supongamos que $\overline{f}(x) \in \overline{K}[x]$ no tiene ningún cero en $\overline{K}$, luego por el Teorema de Kronecker podemos encontrar $\overline{K}(\alpha)$ donde $\overline{f}(\alpha)$ es una extensión algebraica de K $\therefore$ $\overline{K}(\alpha) \subset S$ y $\overline{K} \leq \overline{K}(\alpha) \Rightarrow\Leftarrow$ debido a que $\overline{K}$ es un elemento maximal. Entonces $\overline{K}$ es cerrado algebraicamente. Lo que prueba lo deseado.

Teorema 3.8 (Extensión de isomorfismo) *Sea E una extensión algebraica de un cuerpo K, Sea σ un isomorfismo de K en K'. Sea $\overline{K'}$ una cerradura algebraica de K', entonces σ se puede extender a un monomorfismo τ de E en $\overline{K'}$ tal que $\tau(a) = \sigma(a)$ para todas las $a \in K$.*

Demostración: Considere todos los pares (L, τ) donde L es un cuerpo tal que $K \leq L \leq E$ y τ es un monomorfismo de L en $\overline{K'}$ tal que $\tau(a) = \sigma(a)$ con $a \in K$.
Sea S el conjunto de los pares (L, λ) en el que se define el siguiente orden parcial $(L_1, \lambda_1) \leq (L_2, \lambda_2)$ si $L_1 \leq L_2$ y $\lambda_2(a) = \lambda_1(a)$ para $a \in L_1$.
Sea $T = \{(H_i, \lambda_i) \ / \ i \in I\}$ una cadena de S y sea $H = \bigcup_{i \in I} H_i$, luego si $b \in H$ entonces $b \in H_i$ para algún $i \in I$ considere entonces $\lambda_H : H \to \overline{K'}$ tal que $\lambda_H(b) = \lambda_i(b)$. De esta manera λ_H es un monomorfismo por lo que $(H, \lambda_H) \in S$ y $(H_i, \lambda_i) \leq (H, \lambda_H)$ $\forall i \in I$.
$\therefore$ (H, λ_H) es una cota superior en S por lo que por el lema de Zorn existe un elemento maximal (F, τ) de S.
Sea $\tau(F) = F'$ donde $F' \leq \overline{K'}$. Supongamos que $F \neq E$ y sea $\alpha \in E$, pero $\alpha \notin F$.
Luego α es algebraico sobre K por lo que también es algebraico sobre F. Sea $f(x)$ el polinomio mínimo irreducible de α sobre F y sea $\psi_\alpha : F[x]/\langle f(x)\rangle \to F(\alpha)$ el isomorfismo del teorema 3.4 y considere $\tau(f(x)) = g(x) \in F'[x]$ y como τ es un isomorfismo de F en F' tenemos que $g(x)$ es un polinomio irreducible en $F'[x]$ para algún α' en $\overline{K'}$ debido a que $F' \leq \overline{K'}$.
Luego $\psi_{\alpha'} : F'[x]/\langle g(x)\rangle \to F'(\alpha')$ es también un isomorfismo.
Naturalmente podemos construir otro isomorfismo $\tau^* : F[x]/\langle f(x)\rangle \to F'[x]/\langle g(x)\rangle$ tal que $\tau^*(x + \langle f(x)\rangle) = x + \langle g(x)\rangle$.
Entonces la composición de transformaciones $(\psi_\alpha)^{-1}\tau^*\psi_{\alpha'} : F(\alpha) \to F(\alpha')$ es un monomorfismo de $F(\alpha)$ en $\overline{K'}$, por lo que $(F, \tau) \leq (F(\alpha), (\psi_\alpha)^{-1}\tau^*\psi_{\alpha'}) \Rightarrow\Leftarrow$ debido que (F, τ) es maximal. $\therefore F = E$.

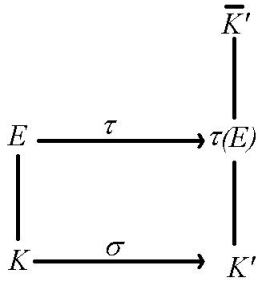

Figura 3.2: Extensión de isomorfismo

Unicidad de la cerradura algebraica

Teorema 3.9 *Sea $\overline{K}$ y $\overline{K'}$ dos cerraduras algebraicas de K. Entonces, $\overline{K}$ es isomorfo a $\overline{K'}$ bajo un isomorfismo que deja fijo cada elemento de K.*

Demostración: Por el teorema de extensión de isomorfismo 3.8 el isomorfismo identidad puede extenderse a un isomorfismo $\tau : \overline{K} \to \overline{K'}$. Ahora veamos que τ es sobreyectivo. Pero por el teorema de extensión de isomorfismo la transformación $\tau^{-1} : \tau(\overline{K}) \to \overline{K}$ puede extenderse a un isomorfismo de $\overline{K'}$ en $\overline{K}$. Como τ^{-1} ya es sobreyectivo, entonces tenemos que $\tau(\overline{K}) = \overline{K'}$. Lo que prueba lo deseado.

3.3. Extensiones normales y separables

¿Cuál es la menor extensión donde viven todas las raíces de un polinomio?

Definición 3.14 *Sea E/K una extensión. Se dice que E es un cuerpo de descomposición de $f(x) \in K[x]$, $\partial f(x) > 1$, si $f(x)$ se descompone en factores lineales en $E[x]$, esto es, $f(x) = k(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$, y no existe ningún subcuerpo propio de E con esta propiedad.*

Ejemplo 3.12 *El cuerpo de descomposición de $f(x) = x^n - 1 \in \mathbb{Q}[x]$ es $\mathbb{Q}(e^{2\pi i/n})$.*

Unicidad del cuerpo de descomposición

Teorema 3.10 *Para cada $f(x) \in K[x]$ existe un único cuerpo de descomposición E de $f(x)$ salvo isomorfismos que dejan fijo K.*

Demostración: Sean E y E' dos cuerpos de descomposición de un polinomio $f(x)$ sobre un cuerpo K. Sean $\overline{E}$ y $\overline{E'}$ dos clausuras algebraicas de E y E' respectivamente. Por el teorema de extensión de isomorfismo $\sigma : \overline{E} \to \overline{E'}$ que deja fijo K. Ahora veamos que $\tau(E) = E'$. Supongamos que $\partial f(x) = n$ y como $\overline{E'}$ es una cerradura algebraica de K tenemos que $f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot ... \cdot (x - \alpha_n)$ con $\alpha_1, \alpha_2, ..., \alpha_n \in \overline{E'}$ luego $E' = K(\alpha_1, \alpha_2, ..., \alpha_n)$. Además como σ es un isomorfismo $\sigma(E)$ es también un cuerpo de descomposición de $f(x)$ en $\overline{E'}$ por lo que $\sigma(E) = K(\alpha_1, \alpha_2, ..., \alpha_n)$. Lo que prueba lo deseado.

Definición 3.15 *Se dice que una extensión algebraica E/K es normal si todo polinomio irreducible $f(x) \in K[x]$ que tiene una raíz en E se descompone en factores lineales en $E[x]$.*

¿Cuándo un polinomio con una raíz en una extensión E tiene todas sus raíces en E?

Teorema 3.11 *Una extensión E/K es normal y finita si y sólo si E es el cuerpo de descomposición de un polinomio de $K[x]$.*

Demostración: $\Rightarrow$) Sea $E = K(\alpha_1, .., \alpha_n)$ y $f(x) = f_1(x) \cdot ... \cdot f_n(x)$ donde $f_i(x)$ es el polinomio mínimo de α_i sobre K y como E es normal y los $f_i(x)$ tienen una raíz en E se descompone

en factores lineales en $E[x]$ y así el cuerpo de descomposición de $f(x)$ está contenido en E y como está generado por sus raíces coincide con él.
$\Leftarrow$) Sea E el cuerpo de descomposición de un polinomio $f(x) \in K[x]$ y sean α y β las raíces de un polinomio irreducible en $K[x]$ luego existe un isomorfismo $\psi : K(\alpha) \to K(\beta)$ que deja fijo a K. Por otro lado $E(\alpha)$ es el cuerpo de descomposición de $K(\alpha)$ y $E(\beta)$ es el cuerpo de descomposición de $K(\beta)$ y como $K(\alpha)$ y $K(\beta)$ isomorfos $E(\beta)$ puede considerarse una extensión de $K(\alpha)$. Si $\alpha \in E$ entonces tenemos que

$$[E(\beta) : E] = \frac{[E(\beta) : K(\alpha)][K(\alpha) : K]}{[E : K]} = \frac{[E(\alpha) : K(\alpha)][K(\alpha) : K]}{[E : K]} = [E(\alpha) : E] = 1$$

por lo que β tambien esta en E por lo tanto E/K es normal y finita.

Ejemplo 3.13 *La extensión $\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}$ con p primo no es normal puesto que contiene a sólo una de las raíces de $x^n - p$ sobre $\mathbb{Q}$ puesto que las otras son números complejos.*

Ejemplo 3.14 *La extensión $\mathbb{Q}(e^{2\pi i/mcm(n,m)}, \sqrt[n]{p}, \sqrt[m]{d})/\mathbb{Q}$ con p y d primos es normal puesto que $\mathbb{Q}(e^{2\pi i/mcm(n,m)}, \sqrt[n]{p}, \sqrt[m]{d})$ es el cuerpo de descomposición de $(x^n - p)(x^m - d)$ sobre $\mathbb{Q}$.*

Definición 3.16 *: Se dice que un polinomio irreducible $f(x) \in K[x]$ es separable en $K[x]$ si no tiene raíces múltiples (en su cuerpo de descomposición). Si E/K es una extensión algebraica, se dice que $\alpha \in E$ es separable en $K[x]$ si su polinomio mínimo lo es. En caso de que un polinomio o elemento no sea separable se dice que es inseparable.*

Definición 3.17 *Se dice que una extensión E/K es separable si todo $\alpha \in E$ es separable en $K[x]$. En caso de que una extensión no sea separable, se dice que es inseparable.*

Ejemplo 3.15 *La extensión $\mathbb{Z}_3(y)/\mathbb{Z}_3(y^3)$ es inseparable, puesto que el polinomio mínimo de y sobre $\mathbb{Z}_3(y^3)$ es $x^3 - y^3 \in \mathbb{Z}_3(y^3)[x]$ que tiene una raíz de multiplicidad tres en $\mathbb{Z}_3(y)$ debido a que $x^3 - y^3 = (x - y)^3$ en $\mathbb{Z}_3(y)[x]$.*

Definición 3.18 *Dado $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$, al polinomio $f'(x) = a_1 + 2a_2x + ... + na_nx^{n-1}$, se le llama derivada formal de $f(x)$*

Las siguientes propiedades son consecuencias de la definición:

Teorema 3.12 *Para cualesquiera $f(x), g(x) \in K[x]$ y cualquier $\alpha \in K$*

1. $(f(x) + g(x))' = f'(x) + g'(x)$;
2. $(\alpha f(x))' = \alpha f'(x)$;
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;

Ejemplo 3.16 *Sea $f(x) = (x - 2)(x - 3)(x - 5)$ entonces*

$$\begin{aligned} f'(x) &= 1 \cdot [(x-3)(x-5)] + (x-2)[1 \cdot (x-5) + (x-3) \cdot 1] \\ &= (x-3)(x-5) + (x-2)(x-5) + (x-2)(x-3) \\ &= \frac{f(x)}{x-2} + \frac{f(x)}{x-3} + \frac{f(x)}{x-5}. \end{aligned}$$

¿Cuándo un polinomio tiene raíces múltiples en su cuerpo de descomposición?

Teorema 3.13 *Si $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ es irreducible, entonces $f(x)$ es inseparable si y sólo si $f'(x) = 0$.*

Demostración: $\Rightarrow$) Como $f(x)$ es inseparable, existe α en el cuerpo de descomposición tal que $(x-\alpha)^2/f(x)$ por lo que existe $q(x)$ en el cuerpo de descomposición de $f(x)$ tal que $f(x) = (x-\alpha)^2q(x)$, luego tenemos que $f'(x) = 2(x-\alpha)q(x) + (x-\alpha)^2q'(x)$ lo que implica que $(x-\alpha)/mcd(f'(x), f(x))$. Como $f'(x) \neq 0$ entonces $1 < \partial mcd(f'(x), f(x)) < \partial f(x)$ por lo que $mcd(f'(x), f(x))$ es un polinomio no constante de grado menor que $f(x)$ lo que es un contradicción, puesto que $f(x)$ es irreducible en $K[x]$.
$\Leftarrow$) Supongamos $f(x)$ es separable, luego tenemos que $f(x) = u(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ con $\alpha_i \neq \alpha_j$ en el cuerpo de descomposición de $f(x)$ sobre K. Entonces tenemos que:

$$f'(x) = \sum_{i=1}^{n} f_i(x) \text{ donde } f_i(x) = \frac{f(x)}{x-\alpha_i}.$$

Como $(x-\alpha_i)/f_i(x)$ para $2 \leq i \leq n$ y $(x-\alpha_i) \not| f_1(x)$ se tiene que $(x-\alpha_1) \not| f'(x)$ lo que es una contradicción, puesto que $f'(x) = 0$

Teorema 3.14 *Si K es un cuerpo de característica cero, todo polinomio irreducible en $K[x]$ es separable. Si K es un cuerpo de característica cero, todo polinomio irreducible en $K[x]$ es separable.*

Demostración: Si $f(x) \in K[x]$ es irreducible por el teorema anterior sabemos que si $f'(x) = 0$ entonces $f(x)$ es inseparable. Supongamos que $f(x)' = 0$ luego $ia_i = 0$ para todo $1 \leq i \leq n$ y como en un cuerpo de característica cero $i = 1+1+...+1$ i veces es distinto de cero implica que $a_i = 0$ para todo $1 \leq i \leq n$, es decir $f(x)$ es un polinomio constante, lo que prueba lo deseado.

Capítulo 4
Teoría de Galois

La teoría de Galois lleva su nombre en honor a Evaristo Galois (1811-1832) que a pesar de fallecer antes de cumplir 21 años y de no ser reconocido en su época, fue quien dio respuesta al problema de la solubilidad de ecuaciones algebraicas por medio radicales y de paso creó una de las más hermosas teorías algebraicas.

En este capítulo conoceremos uno de los resultados principales de nuestro estudio, puesto que aquí veremos bajo que condiciones un grupo finito nos puede entregar información relevante acerca de un cuerpo y sus extensiones, además, gracias a este resultado, podremos presentar un demostración del teorema fundamental del álgebra.

4.1. Automorfismos de cuerpo y grupo de Galois

¿Se puede asociar un grupo a cada extensión de un cuerpo?

Definición 4.1 *Un isomorfismo de un cuerpo sobre si mismo es un automorfismo de cuerpo.*

Definición 4.2 *Si σ es un isomorfismo de cuerpo E en algún cuerpo que contenga a E, entonces un elemento a de E queda fijo bajo σ si $\sigma(a) = a$. Una colección S de isomorfismos de E deja fijo un subconjunto K de E si cada $a \in K$ queda fijo bajo toda $\sigma \in S$.*

Ejemplo 4.1 *Considere el cuerpo $\mathbb{C}$ luego $\psi_{i,-i} : \mathbb{C} \to \mathbb{C}$ definido por $\psi_{i,-i}(a + bi) = a - bi$ es un automorfismo de $\mathbb{C}$ y además como $\psi_{i,-i}(a + bi) = a + bi$ cuando $b = 0$ entonces los elementos de $\mathbb{R}$ quedan fijos por $\psi_{i,-i}$. Ahora si σ_0 es el automorfismo identidad y $\sigma_1 = \psi_{i,-i}$ tenemos que $H = \{\sigma_0, \sigma_1\}$ deja fijo $\mathbb{R}$.*

Teorema 4.1 *Sea E un cuerpo y K un subcuerpo de E entonces, el conjunto $\mathcal{G}(E/K)$ de todos lo automorfismos de E que dejan fijo K forma un subgrupo del grupo S_E el grupo de todas las permutaciones de E.*

Demostración: Sean $\sigma, \tau \in \mathcal{G}(E/K)$ y $a \in K$. Notar que si $\tau \in \mathcal{G}(E/K)$ entonces $\tau^{-1} \in \mathcal{G}(E/K)$ puesto que si $\tau(a) = a$ tenemos que $a = \tau^{-1}(a)$. Ahora veamos que $\sigma\tau^{-1} \in \mathcal{G}(E/K)$, en efecto $\sigma\tau^{-1}(a) = \sigma\left(\tau^{-1}(a)\right) = \sigma(a) = a$ lo que prueba lo deseado.

Teorema 4.2 *Sea H un subgrupo de $\mathcal{G}(E/K)$. Entonces el conjunto H' de todos los $a \in E$ que quedan fijos bajo toda $\sigma \in H$ forman un subcuerpo de E.*

Demostración: Sean a y b en H' y $\sigma \in H$, veamos que $(a-b) \in H'$. Como $a, b \in H'$ entonces $\sigma(a) = a$ y $\sigma(b) = b$, luego $a - b = \sigma(a) - \sigma(b) = \sigma(a-b)$. Ahora nos falta ver que $ab^{-1} \in H'$, en efecto $ab^{-1} = \sigma_i(a)\sigma_i(b^{-1}) = \sigma_i(ab^{-1})$ lo que prueba lo deseado.

Definición 4.3 *Dada un extensión E/K, se dice que un automorfismo de E que deja fijos los elementos de K es un K-automorfismo . Al conjunto $\mathcal{G}(E/K)$ formado por todos los K-automorfismos se le llama grupo de Galois de la extensión.*

Teorema 4.3 *Sea E/K y $f(x) \in K[x]$. Si $\alpha \in E$ es un cero de $f(x)$, entonces $\sigma(\alpha)$ con $\sigma \in \mathcal{G}(E/K)$ también lo es.*

Demostración: Sea $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ y α es una raíz de $f(x)$ entonces $0 = a_0 + a_1\alpha + ... + a_n\alpha^n$ luego $\sigma(0) = \sigma(a_0 + a_1\alpha + ... + a_n\alpha^n)$ y como $a_1, a_2, ..., a_n \in K$ tenemos que $0 = a_0 + a_1\sigma(\alpha) + ... + a_n(\sigma(\alpha))^n$, por lo tanto $\sigma(\alpha)$ también es una raíz de $f(x)$.

Ejemplo 4.2 $\mathcal{G}(\mathbb{Q}(\sqrt[3]{p})/\mathbb{Q}) = \{\sigma_0\}$ *donde σ_0 es la identidad y p es un número primo .*

Como $\mathbb{Q}(\sqrt[3]{p})/\mathbb{Q}$ no es normal y los $\mathbb{Q}$-automorfismos envían raíces en raíces, tenemos que el único $\mathbb{Q}$-automorfismo es la identidad.

Ejemplo 4.3 $\mathcal{G}(\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ *donde σ_0 es la identidad y σ_1, σ_2 son los $\mathbb{Q}$-automorfismo que cumplen $\sigma_1(\sqrt{3}) = -\sqrt{3}, \sigma_1(\sqrt{7}) = \sqrt{7}$,$\sigma_2(\sqrt{3}) = \sqrt{3}, \sigma_2(\sqrt{7}) = -\sqrt{7}$ y $\sigma_3 = \sigma_1\sigma_2$.*

Como $\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q})$ es normal debido a que es el cuerpo de descomposición del polinomio $q(x) = (x^2 - 3)(x^2 - 7)$ y como los Q-autormorfismos envian raíces en raíces estos quedan determinados por las imágenes $\sqrt{3}, \sqrt{7}$ que también son raíces de $q(x)$. Como solo hay cuatro posibilidades están son las que vemos en la siguiente tabla:

Automorfismos	Imagen de $\sqrt{3}$	Imagen de $\sqrt{7}$
σ_0	$\sqrt{3}$	$\sqrt{7}$
σ_1	$-\sqrt{3}$	$\sqrt{7}$
σ_2	$\sqrt{3}$	$-\sqrt{7}$
σ_3	$-\sqrt{3}$	$-\sqrt{7}$

Ahora veamos que estos forman un grupo pues

	σ_0	σ_1	σ_2	σ_3
σ_0	σ_0	σ_1	σ_2	σ_3
σ_1	σ_1	σ_0	σ_3	σ_2
σ_2	σ_2	σ_3	σ_0	σ_1
σ_3	σ_3	σ_2	σ_1	σ_0

Claramente $\mathcal{G}(\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q})$ es un grupo isomorfo al grupo de Klein.

Teorema 4.4 *Sea $K \subset L \subset E \subset F$ una cadena de extensiones algebraicas, donde E/K es finita normal. Sea $\sigma : L \longrightarrow F$ un monomorfismo que deja fijo K. Entonces se cumple que $\sigma(L) \subset E$ y σ se extiende a un K-automorfismo de E.*

Demostración: Sea $\overline{F}$ la cerradura algebraica de F y por el teorema de extensión de isomorfismo, σ puede extenderse a un isomorfismo σ^* que deja fijo a K. Ahora veamos que $\sigma^*(E) = E$. Como E es una extensión algebraica de K entonces existe un polinomio $f(x) \in K[x]$ tal que $E = K(\alpha_1, \alpha_2, ..., \alpha_n)$ donde $\alpha_1, \alpha_2, ..., \alpha_n$ son raíces de dicho polinomio, luego tenemos que $\sigma^*(E) = K(\sigma^*(\alpha_1), \sigma^*(\alpha_2), ..., \sigma^*(\alpha_n))$, además por el teorema 4.3 $\sigma^*(\alpha_i)$ es una raíz de $f(x)$, además σ^* actuando sobre $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ es una inyección de dicho conjunto en sí mismo. Supongamos que $\sigma^*(\alpha_k) = \sigma^*(\alpha_j)$ implica que $\sigma^*(\alpha_k - \alpha_j) = 0$ entonces $\alpha_k = \alpha_j$ y como el conjunto $\alpha_1, \alpha_2, ..., \alpha_n$ es finito es un biyección, es decir $\{\alpha_1, \alpha_2, ..., \alpha_n\} = \{\sigma^*(\alpha_1), \sigma^*(\alpha_2), ..., \sigma^*(\alpha_n)\}$. Por lo tanto $\sigma^*(E) = E$ y la restricción de σ^* a E es el automorfismo buscado.

Teorema 4.5 *Sea E/K normal y finita y $\alpha, \beta \in E$ son raíces de $f(x)$ donde $f(x)$ es el polinomio mínimo irreducible sobre K de α, β, entonces existe $\sigma \in \mathcal{G}(E/K)$ tal que $\sigma(\alpha) = \beta$.*

Demostración: Como $f(x)$ es el polinomio mínimo irreducible y $\alpha, \beta \in E$ existen los siguientes isomorfismo $\psi_\alpha^{-1} : K(\alpha) \longrightarrow K[x]/\langle f(x)\rangle$ y $\psi_\beta : K[x]/\langle f(x)\rangle \longrightarrow K(\beta)$ luego la composición de estos automorfismos nos dan un K-isomorfismo $i : K(\alpha) \longrightarrow K(\beta)$ y por el teorema 4.4 se extiende a K-automorfismo de K. Lo que prueba lo deseado.

4.2. Teorema fundamental de la teoría de Galois

Antes de probar el teorema fundamental de la teoría de Galois debemos probar algunos resultados previamente.

Teorema 4.6 (Independencia de Dedekind) *Sea K un cuerpo y $\sigma_1, \sigma_2, ..., \sigma_n$ automorfismos distintos de K. Si $\lambda_1, \lambda_2, ..., \lambda_n$ son elementos de K tales que:*

$$\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + ... + \lambda_n\sigma_n(\alpha) = 0$$

para todo $\alpha \in K$, entonces $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$.

Demostración: Supongamos que $\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + ... + \lambda_n\sigma_n(\alpha) = 0 \ \forall \ \alpha \in K$ ahora tenemos que probar que $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$.
Supongamos que los λ_i con $i = 1, 2, .., n$ no son todos nulos, entonces podemos suponer que r es el menor número de escalares λ_i no nulos tales que

$$\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + ... + \lambda_r\sigma_r(\alpha) = 0 \ \forall \ \alpha \in K. \tag{4.1}$$

Como $\sigma_1 \neq \sigma_r$ existe $\beta \in K$ tal que $\sigma_1(\beta) \neq \sigma_r(\beta)$, además $\alpha\beta \in K$ y por hipótesis

$$\lambda_1\sigma_1(\alpha\beta) + \lambda_2\sigma_2(\alpha\beta) + ... + \lambda_r\sigma_r(\alpha\beta) = 0 \ \forall \ \alpha \in K. \tag{4.2}$$

Es decir

$$\lambda_1\sigma_1(\alpha)\sigma_1(\beta) + \lambda_2\sigma_2(\alpha)\sigma_2(\beta) + ... + \lambda_r\sigma_r(\alpha)\sigma_r(\beta) = 0 \ \forall \ \alpha \in K. \tag{4.3}$$

Ahora multiplicando 4.1 por $\sigma_r(\beta)$ obtenemos

$$\lambda_1\sigma_1(\alpha)\sigma_r(\beta) + \lambda_2\sigma_2(\alpha)\sigma_r(\beta) + ... + \lambda_r\sigma_r(\alpha)\sigma_r(\beta) = 0 \ \forall \ \alpha \in K. \tag{4.4}$$

Restando 4.4 a 4.3 tenemos que

$$\lambda_1\sigma_1(\alpha)(\sigma_1(\beta) - \sigma_r(\beta)) + \lambda_2\sigma_2(\alpha)(\sigma_2(\beta) - \sigma_r(\beta)) + ... + \lambda_r\sigma_r(\alpha)(\sigma_r(\beta) - \sigma_r(\beta)) = 0 \ \forall \ \alpha \in K.$$

Si $\lambda_i' = \lambda_i(\sigma_i - \sigma_r)$ con $i = 1, 2, ..., r$ vemos que

$$\lambda_1'\sigma_1(\alpha) + \lambda_2'\sigma_2(\alpha) + ... + \lambda_{r-1}'\sigma_{r-1}(\alpha) = 0 \ \forall \ \alpha \in K.$$

$\Rightarrow\Leftarrow$ puesto que r los λ_i con $i = 1, 2, .., r-1$ no son nulos y r es el número de la combinación lineal más corta.
Lo que prueba lo deseado.

Teorema 4.7 *Sea H un subgrupo finito de $\mathcal{G}(E/K)$. Si H' es el subcuerpo fijo por los automorfismos de H, entonces*

$$[E : H'] = |H|.$$

Demostración: Sean $\{\alpha_1, \alpha_2, ..., \alpha_r\}$ un base de E/H' y $H = \sigma_1, \sigma_2, ..., \sigma_n$ por lo tanto tenemos que $[E : H' = r]$ y $|H| = n$

- Supongamos $n > r$ y consideremos el siguiente sistema de ecuaciones

$$\begin{array}{ccccccc} \sigma_1(\alpha_1)x_1 & +\sigma_2(\alpha_1)x_2 & +... & +\sigma_n(\alpha_1)x_n & = & 0 \\ \sigma_1(\alpha_2)x_1 & +\sigma_2(\alpha_2)x_2 & +... & +\sigma_n(\alpha_2)x_n & = & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ \sigma_1(\alpha_r)x_1 & +\sigma_2(\alpha_r)x_2 & +... & +\sigma_n(\alpha_r)x_n & = & 0 \end{array}$$

  Como $n > r$ el sistema es compatible indeterminado entonces existen soluciones no triviales $\lambda_1 = x_1, \lambda_2 = x_2, ..., \lambda_n = x_n$, Así

$$\sigma_1(\alpha_i)\lambda_1 \ +\sigma_2(\alpha_i)\lambda_2 \ +... \ +\sigma_n(\alpha_i)\lambda_n \ = \ 0 \text{ con } 1 \leq i \leq r.$$

  Pero como $\{\alpha_1, \alpha_2, ..., \alpha_r\}$ es una base, se tiene que:

$$\sigma_1(\alpha)\lambda_1 + \sigma_2(\alpha)\lambda_2 + ... + \sigma_n(\alpha)\lambda_n = 0 \ \forall \alpha \in E.$$

  $\Rightarrow\Leftarrow$ Puesto que los $\sigma_1, \sigma_2, ..., \sigma_n$ son linealmente independientes por el teorema 4.6.

- Supongamos ahora que $n > r$ y consideremos el siguiente sistema de ecuaciones

$$\begin{array}{ccccccc} \sigma_1(\alpha_1)x_1 & +\sigma_1(\alpha_2)x_2 & +... & +\sigma_1(\alpha_r)x_r & = & 0 \\ \sigma_2(\alpha_1)x_1 & +\sigma_2(\alpha_2)x_2 & +... & +\sigma_2(\alpha_r)x_r & = & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ \sigma_n(\alpha_1)x_1 & +\sigma_n(\alpha_2)x_2 & +... & +\sigma_n(\alpha_r)x_r & = & 0 \end{array}$$

  Como $r > n$ el sistema es compatible indeterminado entonces existen en soluciones no triviales $\lambda_1 = x_1, \lambda_2 = x_2, ..., \lambda_r = x_r$, además hay $r - n$ variables que se pueden

elegir arbitrariamente, supongamos ahora que estas variables arbitrarias son las $n-r$ primeras. Ahora consideremos los siguientes elementos

$$\Lambda_i \quad = \quad \sigma_1(\lambda_i) \quad +\sigma_2(\lambda_i) \quad +... \quad +\sigma_n(\lambda_i) \text{ con } i = 1,2,..,r$$

Como $\lambda_1, \lambda_2, ..., \lambda_{n-r}$ son arbitrarios, pueden escogerse de manera que Λ_i sea no nulo para $1 \leq i \leq n-r$ y como H es un grupo $\sigma(\Lambda_i) = \Lambda_i \ \forall \sigma \in H$ y por lo tanto $\Lambda_i \in H'$. Como $\lambda_1 = x_1, \lambda_2 = x_2, ..., \lambda_r = x_r$

$$\sigma_j(\alpha_1)\lambda_1 \quad +\sigma_j(\alpha_2)\lambda_2 \quad +... \quad +\sigma_j(\alpha_r)\lambda_r \quad = \quad 0 \text{ con } j = 1,2,..,n$$

Y multiplicando cada fila por σ_j^{-1} obtenemos

$$\sigma_j^{-1}(\lambda_1)\alpha_1 \quad +\sigma_j^{-1}(\lambda_2)\alpha_2 \quad +... \quad +\sigma_j^{-1}(\lambda_r)\alpha_r \quad = \quad 0 \text{ con } j = 1,2,..,n$$

Como H es un grupo cada σ_j^{-1} con $j = 1,2,..,n$ debe ser igual a σ_k con $k = 1,2,..,n$ entonces

$$\sigma_k(\lambda_1)\alpha_1 \quad +\sigma_k(\lambda_2)\alpha_2 \quad +... \quad +\sigma_k(\lambda_r)\alpha_r \quad = \quad 0 \text{ con } k = 1,2,..,n$$

Por último

$$\sum_{i=1}^{r} \Lambda_i\alpha_i = \sum_{i=1}^{r} \sigma_1(\lambda_i)\alpha_i + \sum_{i=1}^{r} \sigma_2(\lambda_i)\alpha_i + ... + \sum_{i=1}^{r} \sigma_n(\lambda_i)\alpha_i = 0$$

$\Rightarrow\Leftarrow$ Puesto que los Λ_i con $i = 1,2,..,r$ no son todos nulos, lo que contradice que los $\alpha_1, \alpha_2, ..., \alpha_r$ son base.
Por lo tanto $n = r$ lo que prueba lo deseado.

Corolario 4.7.1 *Sea H un subgrupo finito de $\mathcal{G}(E/K)$. Si H' es el subcuerpo fijo por los automorfismos de H, entonces*

$$[H' : K] = \frac{[E : K]}{|H|}.$$

Demostración: Como E es una extensión finita de K tenemos que $[E : K] = [E : H'][H' : K]$, reemplazando $[E : K] = |H|[H' : K]$ entonces $[H' : K] = \dfrac{[E : K]}{|H|}$, lo que prueba lo deseado.

Ejemplo 4.4 *Si $H = \mathcal{G}(\mathbb{C}/\mathbb{R}) = \{\sigma_0, \sigma_1\}$ como en el ejemplo 4.1 se tiene que $[\mathbb{C} : H'] = [\mathbb{C} : \mathbb{R}] = 2 = |H|$.*

Ejemplo 4.5 *Si $H = \{\sigma_0, \sigma_2\} \subset \mathcal{G}(\mathbb{Q}(\sqrt{3}, \sqrt{7}/\mathbb{Q})$ como en el ejemplo 4.3 se tiene que $H' = \mathbb{Q}(\sqrt{3})$ así $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : H'] = 2 = |H|$ y $[H' : \mathbb{Q}] = 2 = \dfrac{4}{2} = \dfrac{[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]}{|H|}$.*

Definición 4.4 *Se dice que E/K es una extensión de Galois si es normal, finita y separable.*

¿Bajo qué condiciones un grupo nos entrega información relavante de un cuerpo?

Teorema 4.8 (Teorema fundamental de la teoría de Galois) *Sea E/K una extensión finita de Galois.*

1. *Existe una biyección entre los cuerpos intermedios $K \subset L \subset E$ y los subgrupos de $\mathcal{G}(E/L)$. Esta biyección asigna a cada cuerpo L el grupo $\mathcal{G}(E/L)$ y a su inversa a cada grupo H el cuerpo H'.*

2. *Si $K \subset L \subset E$, la extensión E/L es normal si y sólo si $\mathcal{G}(E/L)$ es un subgrupo normal de $\mathcal{G}(E/K)$.*

3. *Si $K \subset L \subset E$ y E/K es de Galois, la aplicación $r : \mathcal{G}(E/K) \longrightarrow \mathcal{G}(L/K)$ dada por $r(\sigma) = \sigma|_L$ es un epimorfismo de grupo cuyo núcleo es $\mathcal{G}(E/L)$, luego $\mathcal{G}(L/K) \cong \mathcal{G}(E/K)/\mathcal{G}(E/L)$.*

Demostración:

1. Para probar que la aplicación que cada L le asigna $\mathcal{G}(E/L)$ es biyectiva primero veamos que $(\mathcal{G}(E/L))' = L$, es fácil ver que $L \subset (\mathcal{G}(E/L))'$ luego nos falta ver que $(\mathcal{G}(E/L))' \subset L$. Como E/K es una extensión de Galois y $K \subset L \subset E$ entonces E/L es una extensión de Galois. Supongamos que $\alpha \in (\mathcal{G}(E/L))'$ y que $\alpha \notin L$. Como E/L es normal y separable el polinomio mínimo de α sobre L se factoriza totalmente en $E[x]$ y sus raíces son distintas, entonces por el Teorema 4.5 existe un $\sigma \in \mathcal{G}(E/L)$ que no deja fijo a α y que lo envía a otra raíz distinta $\Rightarrow\Leftarrow$ puesto que $\alpha \in (\mathcal{G}(E/L))'$, por lo tanto todo elemento de $(\mathcal{G}(E/L))'$ esta en L, así $(\mathcal{G}(E/L))' = L$.
   Ahora probemos la inyectividad. Supongamos que $\mathcal{G}(E/L) = \mathcal{G}(E/L')$ por lo que $(\mathcal{G}(E/L))' = (\mathcal{G}(E/L'))'$ y como las extensiones son de Galois $L = L'$ lo que prueba lo deseado.
   Ahora probemos la sobreyectividad. Sea $H \leq \mathcal{G}(E/K)$, es fácil ver que $H \leq \mathcal{G}(E/H')$. Supongamos que $\sigma \in \mathcal{G}(E/H')$ y que $\sigma \notin H$ entonces $|H| \leq |\mathcal{G}(E/H')| \Rightarrow\Leftarrow$ debido que $|H| = [E : H'] = [E : (\mathcal{G}(E/H'))'] = |\mathcal{G}(E/H')|$ puesto que la extensión es de Galois. Así $\mathcal{G}(E/H') = H$ lo que prueba lo deseado. Por lo tanto la aplicación es biyectiva y su inversa es la aplicación que enuncia el teorema.

2. $\Rightarrow$) Supongamos que L/K es normal, luego L es el cuerpo de descomposición de algún polinomio de $K[x]$. Sea $\alpha \in L$ y $\tau \in \mathcal{G}(E/K)$ entonces $\tau(\alpha) \in L$. Ahora si $\sigma \in \mathcal{G}(E/L)$ tenemos que $\tau^{-1}\sigma\tau(\alpha) = \tau^{-1}\sigma(\tau(\alpha)) = \tau^{-1}\tau(\alpha) = \alpha$ por lo tanto $\tau^{-1}\sigma\tau \in \mathcal{G}(E/L)$ $\forall$ $\sigma \in \mathcal{G}(E/L)$, es decir, $\mathcal{G}(E/L) \triangleleft \mathcal{G}(E/K)$.
   $\Leftarrow$) Supongamos que $\mathcal{G}(E/L) \triangleleft \mathcal{G}(E/K)$. Sean α, β raíces de un mismo polinomio irreducible en $K[x]$ de manera que $\alpha \in L$. Ahora veamos que $\beta \in L$, para esto basta con probar que $\sigma(\beta) = \beta$. Como $\alpha \in L$ luego por el teorema 4.5 existe $\tau \in \mathcal{G}(E/K)$ tal que $\tau(\alpha) = \beta$ y como $\mathcal{G}(E/L) \triangleleft \mathcal{G}(E/K)$ si $\sigma \in \mathcal{G}(E/L)$ implica que $\tau^{-1}\sigma\tau \in \mathcal{G}(E/L)$ por lo que $\tau^{-1}\sigma\tau(\alpha) = \alpha$. Por último $\sigma(\beta) = \sigma(\tau(\alpha)) = \tau(\tau^{-1}\sigma\tau(\alpha)) = \tau(\alpha) = \beta$ lo que prueba lo deseado.

3. Primero veamos que r es sobreyectivo. Sea $\sigma_L \in \mathcal{G}(L/K)$ luego σ_L por el teorema de extension de isomorfismo puede extenderse a un automorfismo σ de E que deje fijo K así $r(\sigma) = \sigma_L$ lo que prueba lo deseado. Además el núcleo de r es $\mathcal{G}(E/L)$ puesto que los elementos cuya imagen es el neutro de $\mathcal{G}(L/K)$ deben dejar fijo a L. Por último por el Teorema Fundamental del Homomorfismo tenemos que $\mathcal{G}(L/K) \cong \mathcal{G}(E/K)/\mathcal{G}(E/L)$.

Ejemplo 4.6 *Hallar todos los subcuerpos del cuerpo de descomposición E de $x^4 - 9x + 14$ sobre $\mathbb{Q}$.*

Como $x^4 - 9x + 14 = (x^2 - 3)(x^2 - 7)$ que por el ejemplo 4.3 sabemos que su grupo de Galois $\mathcal{G}(\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ donde σ_0 es la identidad y σ_1, σ_2 son los $\mathbb{Q}$-automorfismo que cumplen $\sigma_1(\sqrt{3}) = -\sqrt{3}, \sigma_1(\sqrt{7}) = \sqrt{7}$,$\sigma_2(\sqrt{3}) = \sqrt{3}, \sigma_2(\sqrt{7}) = -\sqrt{7}$ y $\sigma_3 = \sigma_1\sigma_2$, es isomorfo al grupo de Klein.
Como este grupo tiene sólo tres subgrupos propios $\langle\sigma_1\rangle$,$\langle\sigma_2\rangle$ y $\langle\sigma_3\rangle$ por el teorema fundamental de la teoría de Galois tenemos que E sólo tiene tres subcuerpos propios:
$K_1 = \langle\sigma_1\rangle' = \{\sigma_0, \sigma_1\}$, $K_2 = \langle\sigma_2\rangle' = \{\sigma_0, \sigma_2\}$ y $K_3 = \langle\sigma_3\rangle' = \{\sigma_0, \sigma_3\}$.
Notar que el conjunto $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ es una base de $\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q}$.
Por lo tanto $E = \{\lambda_0 + \lambda_1\sqrt{3} + \lambda_3\sqrt{7} + \lambda_4\sqrt{21}\}$ y así no es difícil ver que $K_1 = \mathbb{Q}(\sqrt{3})$, $K_2 = \mathbb{Q}(\sqrt{7})$ y $K_3 = \mathbb{Q}(\sqrt{21})$.
Por último como el grupo de Klein es abeliano todos sus subgrupos son normales y por el teorema de Galois todas la extensiones de cuerpo correspondientes a cada subgrupo son normales.

4.3. Teorema fundamental del Álgebra

Para demostrar que $\mathbb{C}$ es cerrado algebraicamente previamente debemos probar algunos resultados acerca de extensiones de $\mathbb{R}$ y $\mathbb{C}$. Primero veamos que todas las extensiones de $\mathbb{R}$ son de grado par.

Teorema 4.9 *Todo $f(x) \in \mathbb{R}[x]$ con $\partial f(x)$ impar tiene una raíz real.*

Demostración: Sea $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in \mathbb{R}[x]$ y sea $t = 1 + |a_0| + |a_1| + ... + |a_n|$ luego tenemos que $t - 1 \geq |a_i|$ para $i = 1, 2, .., n$. Sea $h(x) = f(x) - x^n$ entonces tenemos que:

$$\begin{array}{rrcl} & |h(t)| & = & |a_0 + a_1t + a_2t^2 + ... + a_{n-1}t^{n-1}| \\ & & \geq & (t-1)(1 + t + t^2 + ... + t^{n-1}) \\ & & = & t^n - 1 \\ & & < & t^n \\ \therefore & |h(t)| & < & t^n \\ \Rightarrow & h(t) & > & -t^n \\ \Rightarrow & h(t) + t^n & > & -t^n + t^n \\ \Rightarrow & f(t) & > & 0 \end{array}$$

Y además tenemos que:

$$\begin{array}{rrcl} & |h(-t)| & = & |a_0 - a_1 t + a_2 t^2 - ... + a_{n-1} t^{n-1}| \\ & & \geq & (t-1)(1 + t + t^2 + ... + t^{n-1}) \\ & & = & t^n - 1 \\ & & < & t^n \\ \therefore & |h(-t)| & < & t^n \\ \Rightarrow & h(-t) & < & t^n \\ \Rightarrow & h(-t) + (-t)^n & < & -t^n + (-t)^n \\ \Rightarrow & f(-t) & < & 0 \end{array}$$

Por último por el teorema del valor intermedio existe $r \in \mathbb{R}$ tal que $f(r) = 0$ luego $f(x)$ tiene una raíz real.

Teorema 4.10 *Toda extensión propia $E/\mathbb{R}$ es de grado par.*

Demostración: Sea E una extensión finita de $\mathbb{R}$ y sea $\alpha \in E$ de manera que $\alpha \notin \mathbb{R}$. Como no existen polinomios irreducibles en $\mathbb{R}[x]$ de grado impar, el grado del polinomio mínimo irreducible de α es de grado par y como $[E : \mathbb{R}] = [E : \mathbb{R}(\alpha)][\mathbb{R}(\alpha) : \mathbb{R}]$ y $[\mathbb{R}(\alpha) : \mathbb{R}]$ es de grado par entonces $[E : \mathbb{R}]$ es de grado par.

Ahora veamos que no existen extensiones de $\mathbb{C}$ de grado igual a 2.

Teorema 4.11 *Todo $g(x) \in \mathbb{C}[x]$ con $\partial g(x) = 2$ tiene sus raices en $\mathbb{C}$.*

Demostración: Primero veamos que todo número complejo z tiene una raíz cuadrada compleja. Como todo $z \in \mathbb{C}$ lo podemos escribir en forma polar $z = re^{i\theta}$ con r mayor que cero tenemos que $\sqrt{z} = \sqrt{r}\ e^{\frac{i\theta}{2}}$ es la raiz buscada. Sea $g(x) = z_0 + z_1 x + z_2 x^2 \in \mathbb{C}[x]$. Luego por la fórmula de la ecuación de segundo grado la demostración se reduce probar que $z_1^2 - 4z_0 z_2$ tiene una raiz cuadrada compleja, lo que es cierto para todo $z \in \mathbb{C}$.

Teorema 4.12 *No existe una extensión algebraica $E/\mathbb{C}$ de grado 2.*

Demostración: Supongamos que existe una extensión de $E/\mathbb{C}$ grado 2, luego debe existir un polinomio irreducible en $\mathbb{C}[x]$ de grado 2 $\Rightarrow\Leftarrow$ puesto que todo polinomio en $\mathbb{C}[x]$ con grado igual a 2 tiene sus raices en $\mathbb{C}$.

Antes de dar la demostración del teorema fundamental del álgebra recordemos uno de los teoremas de Sylow.

Teorema 4.13 (Teorema de Sylow) *Sea G un grupo finito, p un número primo y n un número natural tal que $p^n/|G|$. Entonces G tiene un subgrupo de orden p^n.*

Es importante mencionar que el teorema fundamental del álgebra fue conjeturado por Girard y fue demostrado por D'Alembert en 1746 y más tarde por Gauss en 1799 quien además presentó dos nuevas demostraciones de este resultado en el año 1816 y otra en 1849 encontrándose con el problema de dar una demostración netamente algebraica de este resultado.

La demostración que damos a continuación tampoco es completamente algebraica, puesto que para probar el teorema 4.9 tuvimos que recurrir al análisis.

Teorema 4.14 (Teorema fundamental del álgebra) $\mathbb{C}$ *es algebraicamente cerrado.*

Demostración: Para demostrar que $\mathbb{C}$ es algebraicamente cerrado hay que probar que $\mathbb{C}$ no tiene extensiones algebraicas propias. Sea E una extensión de $\mathbb{C}$, así adjuntando $\alpha \in E$ que no este en $\mathbb{C}$ obtenemos una extensión propia y finita de $\mathbb{C}$.
Podemos suponer que E es una extensión propia y finita de $\mathbb{C}$ y como existe una extensión finita normal de $\mathbb{R}$ que contiene a E, Podemos suponer que $E/\mathbb{R}$ es una extensión finita de Galois.
Como $[E:\mathbb{R}]$ es un número par tenemos que $[E:\mathbb{R}] = 2^n \cdot m$ con $n \geq 1$ y m impar.
Luego $|\mathcal{G}(E/\mathbb{R})| = 2^n \cdot m$ y por el teorema de Sylow existe un subgrupo H de $\mathcal{G}(E/\mathbb{R})$ de orden 2^n y así $[E:H'] = 2^n$ y $[H':\mathbb{R}] = m$, pero como m es impar y todo extensión de $\mathbb{R}$ es de grado par. $[H':\mathbb{R}] = 1$ por lo que $[E:\mathbb{R}] = 2^n$ y por lo tanto $[E:\mathbb{C}] = 2^{n-1}$ y así $|\mathcal{G}(E/\mathbb{C})| = 2^{n-1}$, pero como $E/\mathbb{C}$ es una extensión propia $n-1 \geq 1$ luego por el teorema de sylow existe un subgrupo N de $\mathcal{G}(E/\mathbb{C})$ de manera que $|N| = 2^{n-2}$ y así $[E:N] = 2^{n-2}$ y $[N':\mathbb{C}] = 2 \Rightarrow\Leftarrow$ puesto que no existen extensiones de $\mathbb{C}$ de grado 2.

Observación 4.1 *El problema de encontrar un demostración totalmente algebraica pasa porque los reales están construidos en función de análisis.*

Capítulo 5
Resolubilidad por radicales

En este capítulo estudiaremos en profundidad las características de las extensiones de cuerpo en las que es posible resolver las ecuaciones polinomiales, conociendo cuales son las condiciones necesarias y suficientes para encontrar solución a dichas ecuaciones. Como consecuencia de estos vamos a concluir que el caso general de grado n no tiene solución para $n \geq 5$.

5.1. Grupos solubles

Como vimos en el capítulo anterior los grupos nos pueden dar información importante acerca de los cuerpos, es por eso que veremos algunos teoremas acerca de grupos que nos permitirán obtener propiedades importantes de los cuerpos.

Definición 5.1 *Se dice que un grupo G es simple si no tiene subgrupos normales propios.*

Definición 5.2 *Sea G un grupo finito, se dice que una cadena de subgrupos de G*

$$\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 ... \subsetneqq G_n = G$$

es una serie de composición si $G_{i-1} \lhd G_i$ y G_i/G_{i-1} es un grupo simple para $0 \leq i \leq n$.

Definición 5.3 *Un grupo finito G es soluble si tiene una serie de composición*

$$\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 ... \subsetneqq G_n = G$$

tal que G_i/G_{i-1} sea un grupo abeliano.

Ejemplo 5.1 *S_3 es un grupo soluble pues tiene la serie de composición:*

$$\{e\} \subset A_3 = \langle (1,2,3) \rangle \subset S_3$$

con cocientes isomorfos a $\mathbb{Z}_3$ y $\mathbb{Z}_2$ respectivamente.

Ejemplo 5.2 *S_4 es un grupo soluble pues tiene la serie de composición:*

$$\{e\} \subset \langle \tau \rangle \subset \langle \tau, \sigma \rangle \subset A_4 = \langle \tau, \sigma, \eta \rangle \subset S_4$$

con $\tau = (1,3)(2,4), \sigma = (1,2)(3,4)$ y $\eta = (1,2,3)$ con cocientes isomorfos a $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$ y $\mathbb{Z}_2$ respectivamente.

Antes de continuar recordemos los teoremas de isomorfía

Teorema 5.1 (Teorema de isomorfía) *Si $f : G \longrightarrow G'$ es un homomorfismo de grupos, entonces el núcleo de f es un subgrupo normal de G y*

$$G/Nuc(f) \cong Im(f)$$

Teorema 5.2 (Segundo teorema de isomorfía) *Sea G un grupo, $H \leq G$ y $N \lhd G$. entonces $HN = \{hn/n \in N, h \in H\}$ es un grupo, $N \lhd HN$, $HN = NH$ y*

$$HN/N \cong H/(H \cap N).$$

Teorema 5.3 (Tercer teorema de isomorfía) *Sea G un grupo, $H \lhd G$ y $N \lhd G$ tal que $N \leq H$. entonces*

$$(G/N)/(H/N) \cong G/H.$$

Teorema 5.4 *Se cumple que:*

1. *Si G es un grupo soluble y $H \leq G$, entonces H es soluble.*
2. *Si G es un grupo soluble y $N \lhd G$, entonces G/N es soluble.*
3. *Si G es un grupo y $N \lhd G$ tal que N y G/N son solubles, entonces G es soluble.*

Demostración:

1. Sea $\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 ... \subsetneqq G_n = G$ una serie abeliana de G, entonces

   $$\{e\} = G_0 \cap H \subsetneqq G_1 \cap H \subsetneqq G_2 \cap H ... \subsetneqq G_n \cap H = H$$

   Es un serie abeliana de H debido que por el segundo teorema de isomorfía tenemos que

   $$(G_i \cap H)/(G_{i-1}) = (G_i \cap H)/(G_{i-1} \cap (G_i \cap H)) \cong G_{i-1}(G_i \cap H)/G_{i-1}$$

   Como $G_{i-1}(G_i \cap H)/G_{i-1} \leq G_i/G_{i-1}$ entonces $G_{i-1}(G_i \cap H)/G_{i-1}$ es abeliano por lo que $(G_i \cap H)/(G_{i-1})$ también lo es. Por lo tanto H es soluble.

2. Sea $\{e\} = G_0 \subsetneqq G_1 \subsetneqq G_2 ... \subsetneqq G_n = G$ una serie abeliana de G, entonces

   $$\{e\} = G_0N/N \subsetneqq G_1N/N \subsetneqq G_2N/N ... \subsetneqq G_nN/N = G/N$$

   Es un serie abeliana de G/N debido que por los teoremas de isomorfía tenemos que

   $$\begin{aligned}(G_iN/N)/(G_{i-1}N/N) &\cong G_iN/G_{i-1}N = G_i(G_{i-1}N)/G_{i-1}N \\ &\cong G_i/(G_i \cap G_{i-1}N) \cong (G_i/G_{i-1})/((G_i \cap G_{i-1}N)/G_{i-1})\end{aligned}$$

   Como G_i/G_{i-1} es abeliano entonces $(G_i/G_{i-1})/((G_i \cap G_{i-1}N)/G_{i-1})$ es abeliano por lo que $(G_iN/N)/(G_{i-1}N/N)$ también lo es. Por lo tanto G/N es soluble.

3. Sea $\{e\} = N_0 \subsetneqq N_1 \subsetneqq N_2 ... \subsetneqq N_n = N$ una serie abeliana de N y $\{e\} = G_0/N \subsetneqq G_1/N \subsetneqq G_2/N ... \subsetneqq G_m/N = G/N$ na serie abeliana de G/N. Consideremos ahora la siguiente serie de G

$$\{e\} = N_0 \subsetneqq N_1 \subsetneqq N_2 ... \subsetneqq N_n = G_0 \subsetneqq G_1 \subsetneqq G_2 ... \subsetneqq G_m = G$$

Como $(G_i/N)/(G_{i-1}/N)$ es abeliano y $G_i/G_{i-1} \cong (G_i/N)/(G_{i-1}/N)$ esta serie es una serie de composición de un grupo soluble. Lo que prueba lo deseado.

Teorema 5.5 *Un grupo finito es simple si y sólo si es cíclico de orden primo.*

Demostración: $\Leftarrow$) Sea G un grupo cíclico de orden primo y como $|G|$ ni tiene divisores entonces G no tienen subgrupos propios por lo que G es simple y como es cíclico es abeliano, por lo tanto es soluble.
$\Rightarrow$) Sea G un grupo simple y soluble; su única serie es $\{e\} \leq G$ y como G es soluble esta serie es abeliana por lo que G debe ser abeliano. Como G es abeliano todos los subgrupos son abelianos y por lo tanto normales, pero G es simple por lo que G no puede tener subgrupos distintos de los triviales. Sea $g \in G$ tal que $g \neq e$, así $\langle g \rangle \neq \{e\}$, como G no tiene subgrupos propios $G = \langle g \rangle$, luego G es cíclico y como G no tiene subgrupos entonces $|G|$ no tiene divisores, puesto que un grupo cíclico posee subgrupos para los divisores de $|G|$, por lo que $|G|$ es un número primo.

Corolario 5.5.1 *Si G es un grupo soluble, entonces G tiene una serie cuyos factores son grupos cíclicos de orden primo.*

Demostración: Es consecuencia inmediata de la definición de grupo soluble y del teorema anterior.

Teorema 5.6 *Si $n \geq 5$ entonces el grupo alternado A_n es un grupo simple.*

Demostración:
Primero veamos que A_n esta generado por ciclos de longitud 3.
Como todo elemento de A_n se pude escribir como un número par de transposiciones veamos que cada par de transposiciones se puede escribir como un producto de ciclos de longitud 3. Como un par de transposiciones es de la forma $(a_1, a_2)(a_3, a_4)$ o $(a_1, a_2)(a_1, a_3)$. En el primer caso $(a_1, a_2)(a_3, a_4) = (a_1, a_2, a_3)(a_3, a_2, a_1)$ y en el segundo caso $(a_1, a_2)(a_1, a_3) = (a_1, a_2, a_3)$.
$\therefore$ toda permutación de A_n se puede expresar como un producto de ciclo de longitud 3.
Ahora veamos que si $N \lhd A_n$ contiene un ciclo de longitud 3 entonces $N = A_n$.
Sea $(a_1, a_2, a_3) \in N$ y sea $\sigma \in S_n$ un ciclo de longitud 3 existe una permutación $\tau \in S_n$ tal que $\tau^{-1}(a_1, a_2, a_3)\tau = \sigma$
Si $\sigma \in A_n$ entonces $\sigma = \tau^{-1}(a_1, a_2, a_3)\tau \in \tau^{-1}N\tau = N$
Si $\sigma \in B_n$ tenemos que

$$\sigma = \tau^{-1}(a_1, a_2, a_3)\tau = \tau^{-1}(a_3, a_1)(a_3, a_2, a_1)(a_1, a_3)\tau = ((a_1, a_3)\tau)^{-1}(a_3, a_2, a_1)((a_1, a_3)\tau)$$

y como $\tau \in B_n$ $(a_1, a_3)\tau \in A_n$ y como $(a_1, a_2, a_3) \in N$ entonces $(c, b, a) = (a, b, c)^{-1}N$ entonces $\sigma \in N$.
$\therefore$ N contiene a todos los ciclos de longitud 3 así $A_n \subseteq N$. Así $N = A_n$.
Por último vamos a probar por inducción sobre n que A_n es simple para $n \geq 5$

a) Si $n = 5$, es decir, debemos probar que A_5 es simple. Si $N \lhd A_5$ y $N \neq \{e\}$ un elemento de N es de la forma $(a_1, a_2, a_3), (a_1, a_2, a_3, a_4, a_5)$ o $(a_1, a_2)(a_3, a_4)$
Si N contiene un elemento de la forma (a_1, a_2, a_3) entonces $N = A_5$
Si N contiene un elemento de la forma $(a_1, a_2, a_3, a_4, a_5)$ entonces

$$\begin{aligned} & (a_1, a_2, a_3, a_4, a_5)((a_1, a_2)(a_4, a_5))^{-1}(a_1, a_2, a_3, a_4, a_5)((a_1, a_2)(a_4, a_5)) \\ = \; & (a_1, a_2, a_3, a_4, a_5)(a_5, a_4)(a_2, a_1)(a_1, a_2, a_3, a_4, a_5)(a_1, a_2)(a_4, a_5) \\ = \; & (a_2, a_5, a_3) \end{aligned}$$

$\therefore (a_2, a_5, a_3) \in N$ entonces $N = A_5$
Si N contiene un elemento de la forma $(a_1, a_2)(a_3, a_4)$ sea a_5 un elemento distinto de a_1, a_2, a_3, a_4 entonces

$$\begin{aligned} & ((a_1, a_2)(a_3, a_4))(a_1, a_2, a_5)^{-1}((a_1, a_2)(a_3, a_4))(a_1, a_2, a_5) \\ = \; & (a_1, a_2)(a_3, a_4)(a_5, a_2, a_1)(a_1, a_2)(a_3, a_4)(a_1, a_2, a_5) = (a_1, a_5, a_2) \end{aligned}$$

$\therefore (a_1, a_5, a_2) \in N$ entonces $N = A_5$

b) Supongamos que A_n es simple. Ahora lo que debemos demostrar es que A_{n+1} es simple. Sea $N \lhd A_{n+1}$ y $N \neq \{e\}$. Notar que podemos identificar A_n con el conjunto de las permutaciones de A_{n+1} que dejan fijo a $n+1$. Por lo que $A_n \leq A_{n+1}$.
Notar que $N \cap A_n \lhd A_n$ y como A_n es simple por hipótesis de inducción , tenemos que $N \cap A_n = A_n$ o $N \cap A_n \neq \{e\}$. Supongamos que $N \cap A_n \neq \{e\}$ y sea $\sigma \in N$ con $\sigma \neq e$ y $\sigma(n+1) = j \neq n+1$. Notar que la longitud de σ es mayor que 3 puesto que σ no puede ser un transposición porque $\sigma \in A_n$ y σ no es de longitud 3 puesto que así tendríamos que $N = A_{n+1}$, luego podemos encontrar k, l distintos entre si y distintos de j y $n+1$ tal que $\sigma(k) = l$. Sea $\tau = ((n+1, j)(k, l, s, t))^{-1}\sigma((n+1, j)(k, l, s, t))$ con s, t elementos distintos de los anteriores y como $((n+1, j)(k, l, s, t)) \in A_n$ tenemos que $\tau \in N$ y así $\sigma\tau \in N$. Notar que $\sigma\tau(n+1) = n+1$ y $\sigma\tau(k) = s$, así $\sigma\tau \neq e$ pero $\sigma\tau \in N \in A_n$ $\Rightarrow\Leftarrow$ Por lo tanto $N \cap A_n = A_n$ y a_{n+1} contiene a todos los ciclos de longitud 3 de A_n entonces $N = A_{n+1}$.

5.2. Extensiones radicales

Definición 5.4 *Un extensión de cuerpos E/K se dice radical si existe una cadena de subcuerpos:*

$$K = E_0 \subset E_1 \subset E_2 \subset ... \subset E_n$$

con $E \subset E_n$, tales que para cada $0 < i \leq n$ tenemos que $E_i = E_{i-1}(\alpha_i)$ donde $\alpha_i^{m_i} \in E_{i-1}$ y m_i son naturales no nulos.

Definición 5.5 *Un polinomio $f(x) \in K[x]$ se dice soluble por radicales si su cuerpo de descomposición es una extensión radical.*

Ejemplo 5.3 *El polinomio* $x^6 - 6x^3 + 3$ *es soluble por radicales puesto que su cuerpo de descomposición* $\mathbb{Q}(\sqrt{6}, \omega, \alpha, \beta)$ *con* $\omega = e^{\frac{2\pi i}{3}}, \alpha = \sqrt[3]{3-\sqrt{6}}$ *y* $\beta = \sqrt[3]{3+\sqrt{6}}$ *es radical como vemos en la siguiente cadena*

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{6}, \omega) \subset \mathbb{Q}(\sqrt{6}, \omega, \alpha) \subset \mathbb{Q}(\sqrt{6}, \omega, \alpha, \beta).$$

Teorema 5.7 *Sea* E/K *una extensión radical podemos modificar la cadena de subcuerpos de la definición a*

$$K = K_0 \subset K_1 \subset K_2 \subset ... \subset K_N$$

con propiedades análogas de forma que $K_N \supset E_n$ *y* K_N/K *sea normal.*

Demostración: Probaremos este teorema usando inducción matemática sobre n la longitud de la cadena inicial.

a) $n = 1$ luego la cadena inicial es $K = E_0 \subset E_1$ con $E_1 \supset E$ tal que $E_1 = E_0(\alpha_1)$ con $\alpha_1^{m_1} \in E_0$. Ahora si añadimos las raíces de $x^{m_1} - \alpha_1^{m_1}$ obtenemos un cuerpo de descomposición K_1 de K tal que $K_1 \supset E_1$ y así la cadena deseada.

b) Supongamos que se cumple para una cadena de longitud n entonces ahora debemos probar que se cumple para una cadena de longitud $n+1$.
Por hipótesis de inducción tenemos que si $K = E_0 \subset E_1 \subset ... \subset E_n$ con $E_n \supset E$ tal que $E_i = E_{i-1}(\alpha_i)$ con $\alpha_i^{m_i} \in E_{i-1}$ es la cadena de una extensión radical entonces $K = K_0 \subset K_1 \subset ... \subset K_N$ con $K_N \supset E_n$ es otra cadena con propiedades análogas de manera que K_N/K normal. Así K_N es el cuerpo de descomposición de un polinomio $f(x) \in K[x]$ y si $q(x)$ es el polinomio mínimo de α_{n+1} sobre K y $\beta_1 = \alpha_{n+1}, \beta_2, ..., \beta_k$ sus raíces y sea K' es cuerpo de descomposición de $f(x)q(x) \in K[x]$ luego existe $\sigma_i \in \mathcal{G}(K'/K)$ con $1 \leq i \leq k$ tal que $\sigma_i(\alpha_{n+1}) = \beta_i$ y como $\alpha_{n+1}^{m_{n+1}} \in E_n \subset K_N$ y K_N es normal $\sigma_i(\alpha_{n+1}^{m_{n+1}}) = \beta_i^{m_{n+1}} \in K_N$. Por último si $K_{N+i} = K_{N+i-1}(\beta_i)$ para $1 \leq i \leq k$ se tiene la extensión deseada $K = E_0 \subset E_1 \subset ... \subset E_n \subset K_N \subset K_{N+1} \subset ... \subset K_{N+k}$ con $K' = K_{N+k} \supset E_{n+1} = E_n(\alpha_{n+1})$.

Definición 5.6 *Un polinomio* $f(x) \in K[x]$ *es soluble por radicales si su cuerpo de descomposición es una extensión radical de* K.

Teorema 5.8 *Sea* E/K *una extensión de Galois y* $\omega \in K$ *una raíz* n*-ésima del unitario con* $n \in \mathbb{N}$*, entonces si* E *es el cuerpo de descomposición sobre* K *de un polinomio de la forma* $x^d - a$ *irreducible en* $K[x]$ *y* α *es una raíz en* E *de dicho polinomio, tenemos que* $E = K(\alpha)$ *si y solo si* $\mathcal{G}(E/K)$ *es cíclico de grado* d*, donde* d *es un divisor de* n.

Demostración: $\Leftarrow$) Sea $\mathcal{G}(E/K) = \langle\sigma\rangle$ y $\eta = \omega^{\frac{n}{d}} \in K$ una raíz d-ésima del unitario luego por la independencia de dedekind existe $\beta \in E$ tal que $\alpha' = \eta^0\sigma^0(\beta) + \eta\sigma(\beta) + ... + \eta^{d-1}\sigma^{d-1}(\beta) \neq 0$ luego $\eta\sigma(\alpha') = \eta\sigma(\beta) + \eta^2\sigma^2(\beta) + ... + \eta^d\sigma^d(\beta) = \alpha'$ y así $\sigma(\alpha') = \zeta\alpha'$ con $\zeta = \eta^{-1}$ y como η^{-1} es otra raíz d-ésima del unitario tenemos que $\sigma^i(\alpha) = \zeta^i\alpha'$ con $i = 0, 1, 2, ..., d-1$, luego los $\zeta^i\alpha'$ son raíces del mismo polinomio y además $\sigma(\alpha'^d) = (\sigma(\alpha'))^d = \zeta^d\alpha'^d = \alpha'^d$ y como $\sigma \neq e$ tenemos que $\alpha'^d \in K$ y el polinomio $x^d - \alpha'^d \in K[x]$ tiene todas sus raíces de la forma $\zeta^i\alpha'$ con $i = 1, 2, .., d-1$ y E es el cuerpo de descomposición de $x^d - \alpha'^d$ y como $\sigma \in \mathcal{G}(E/K)$ no

fija a las raíces estas no pertenecen a K así $x^d - \alpha'^d$ es irreducible sobre K y si adjuntamos cualquiera de sus raíces obtenemos una extensión de grado d y como $[E : K] = d$ tenemos que $E = K(\alpha)$ donde α es cualquiera de las raíces de $x^d - \alpha'^d$
$\Rightarrow$) Sea $a = \alpha^n$ asi $f(x) = x^n - a \in K[x]$ tiene n raíces distintas en E y son de la forma $\omega^i\alpha$ para $i = 1, 2, ..., n$ por lo tanto E es el cuerpo de descomposición de $f(x) = x^n - a$ y sus raíces son separables por lo que E/K es una extensión finita de Galois. Para cada $\sigma \in \mathcal{G}(E/K)$ tenemos que $\sigma(\alpha)$ es otra raíz de $f(x)$ luego existe un entero i módulo n tal que $\sigma(\alpha) = \omega^i\alpha$. Consideremos la siguiente aplicación $h : \mathcal{G}(E/K) \longrightarrow \mathbb{Z}_n$ definido por $h(\sigma) = i$. Ahora veamos que es un monomorfismo. Sean $\sigma, \tau \in \mathcal{G}(E/K)$ luego $\sigma(\alpha) = \omega^j\alpha$ y $\tau(\alpha) = \omega^k\alpha$ así $h(\sigma\tau) = j + k = h(\sigma) + h(\tau)$ además si $h(\sigma) = h(\tau)$ entonces $j = k$ lo que implica que $\alpha\omega^j = \alpha\omega^k$ es decir $\sigma(\alpha) = \tau(\alpha)$ y como $E = K(\alpha)$ entonces $\sigma = \tau$ debido a que los elementos de $\mathcal{G}(E/K)$ están determinados por la imagen de α por lo que h es inyectiva y así $\mathcal{G}(E/K)$ es isomorfo a un subgrupo de $\mathbb{Z}_n$ por lo tanto es cíclico y $|\mathcal{G}(E/K)|$ es un divisor de n.

¿Cuándo un polinomio es soluble por radicales?

Teorema 5.9 (Galois) *Sea $f(x) \in K[x]$ con característica cero y se E su cuerpo de descomposición, entonces $f(x)$ es soluble por radicales si y sólo si $\mathcal{G}(E/K)$ es un grupo soluble.*

Demostración: $\Rightarrow$) Sea E el cuerpo de descomposición de $f(x)$ sobre K y sea $E_n \supset E$ con E_n/K radical luego por el teorema 5.7 podemos suponer E_n/K es radical y de Galois. Así $E_n = K(\alpha_1, \alpha_2, ..., \alpha_n)$ con $\alpha_i^{m_i} \in K(\alpha_1, \alpha_2, ..., \alpha_{i-1})$ y $m_i \in \mathbb{N}$. Sea $\zeta \neq 1$ una raíz m-ésima primitiva del unitario con $m = m_1, m_2, ..., m_n$. Ahora vamos a suponer primero que K contiene a ζ por lo que además contiene a todas la raíces m_i-ésimas del unitario puesto que $\zeta^{\frac{m}{m_i}}$ es una raíz m_i-ésima del unitario. Por el teorema fundamental de la teoría de Galois tenemos que:

$$\{e\} = \mathcal{G}(E_n/E_n) \subset \mathcal{G}(E_n/E_{n-1}) \subset ... \subset \mathcal{G}(E_n/E_0) = \mathcal{G}(E_n/K) \tag{5.1}$$

Veamos que E_i/E_{i-1} es normal para $i = 1, 2, .., n$ puesto que E_i es el cuerpo de descomposición de $f_i(x) = x^{m_i} - \alpha^{m_i} \in E_{i-1}[x]$ porque $E_i = E_{i-1}(\alpha_i)$ y cualquier raíz de $f_i(x)$ es α_i por una raíz m_i-ésima del unitario. Notar que siempre podemos suponer que $E_i \neq E_{i-1}$ y así que $\alpha_i \notin E_{i-1}$ y luego que f_i es irreducible. Por el teorema fundamental de la teoría de Galois se tiene que $\mathcal{G}(E_n/E_i) \lhd \mathcal{G}(E_n/E_{i-1})$ y que $\mathcal{G}(E_n/E_{i-1})/\mathcal{G}(E_n/E_i) \cong \mathcal{G}(E_i/E_{i-1})$ que por teorema 5.8 es soluble y como $\mathcal{G}(E_n/K)$ es soluble por el teorema 5.4 el subgrupo $\mathcal{G}(E_n/E)$ también es soluble y $\mathcal{G}(E_n/E_i) \cong \mathcal{G}(E_n/K)/\mathcal{G}(E_n/E)$.
Ahora veamos el caso cuando K no contiene a las raíces m_i-ésimas del unitario. Si $\zeta \neq 1$ es un raíz m-ésima primitiva del unitario las raíces de $x^m - 1 \in K[x]$ son $1, \zeta, ..., \zeta^{m-1}$ y luego $K' = K(\zeta)$ es su cuerpo de descomposición. Como $\sigma \in \mathcal{G}(K'/K)$ lleva raíces en raíces entonces $\sigma_j(\zeta) = \zeta^j$ y $\sigma_k(\zeta) = \zeta^k$ por lo que $\sigma_j\sigma_k(\zeta) = \zeta^{jk} = \sigma_k\sigma_j(\zeta)$ así $\mathcal{G}(K'/K)$ es abeliano luego soluble. Si $E' \supset E$ es el cuerpo de descomposición de $f(x)$ sobre K' el problema se reduce al caso anterior y $\mathcal{G}(E'/K')$ es soluble. Como $\mathcal{G}(E'/K)/\mathcal{G}(E'/K') \cong \mathcal{G}(K'/K)$ y $\mathcal{G}(E'/K)$ y $\mathcal{G}(K'/K)$ son solubles $\mathcal{G}(E'/K)$ es soluble.
$\Leftarrow$) Si $\mathcal{G}(E/K)$ es soluble por teorema fundamental de la teoría de Galois podemos pasar de una serie de composición a una cadena de subcuerpos:

$$K = G'_n \subset G'_{n-1} \subset ... \subset G'_0 = E$$

además G'_{i-1}/G'_i es una extensión de Galois puesto que $G_{i-1} \lhd G_i$ y por el corolario 5.5.1 es un primo p_i. Primero supongamos que contiene a las raíces p_i-ésimas del unitario, notar que si $p = p_1 \cdot p_2 \cdot ... \cdot p_n$ entonces basta que K contenga una raíz p-ésima primitiva del unitario , así por el teorema 5.8 $G_{i-1} = G_i(\alpha)$ con $\alpha^{p_i} \in G_i$ por lo que E/K es radical.
Ahora veamos el caso cuando no contiene las raíces p_i-ésimas del unitario. Consideremos la extensión normal $G_{i-1}(\zeta)/G_i(\zeta)$ y el homomorfismo:

$$\begin{array}{rccc} \phi: & G_{i-1}(\zeta)/G_i(\zeta) & \longrightarrow & G_{i-1}/G_i \\ & \sigma & \longrightarrow & \sigma\mid_{G'_{i-1}} \end{array}$$

Notar que el núcleo de $\phi = \{e\}$ puesto que debe dejar fijos a los elementos de $G'_i(\zeta)$ y los de G'_{i-1} además es sobreyectivo puesto que para cada $\sigma\mid_{G'_{i-1}}$ existe un preimagen que es la extensión de este isomorfismo a otro $\sigma_{G'_{i-1}(\zeta)}$ y como G'_{i-1}/G'_i es de grado primo $G'_{i-1}(\zeta)/G'_i(\zeta)$ también lo es y análogamente al caso anterior $G'_{i-1}(\zeta)/G'_i(\zeta)$ es radical y luego por el isomorfismo G'_{i-1}/G'_i también es radical.

Teorema 5.10 *Si K tiene característica cero, la ecuación general de grado n de $K[x]$ es soluble por radicales para $n \leq 4$ sobre K.*

Demostración: Como el grupo de Galois permuta las raíces, debe ser isomorfo a un subgrupo $H \subset S_4$ que es soluble por el ejemplo 5.2 y como todo subgrupo de un grupo soluble es soluble, el resultado es consecuencia inmediata del teorema anterior.

Corolario 5.10.1 *Si K tiene característica cero, todo polinomio que sea producto de polinomios de grado $n \leq 4$ de $K[x]$ es soluble por radicales sobre K.*

Demostración: Es consecuencia inmediata del teorema anterior.

5.3. La ecuación general de grado n

En esta sección probaremos que la ecuación general de grado n no es soluble por radicales para $n \geq 5$, es decir no existen fórmulas similares a las de segundo, tercer y cuarto grado.

Definición 5.7 *Si $n \geq 1$ y K es un cuerpo y $E = K(a_0, ..., a_{n-1})$ es cuerpo de las fracciones algebraicas en las indeterminadas $a_0, .., a_{n-1}$, llamaremos polinomio general de grado n sobre K al polinomio*

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in K[x]$$

y $f(x) = 0$ ecuación de grado n.

Definición 5.8 *Diremos que un polinomio en varias variables es simétrico si queda invariante bajo cualquier permutación de sus variables.*

Ejemplo 5.4 $x_1^3 \cdot x_2^3 \cdot x_3^3$, $x_1^2 + x_2^2 + x_3^2$.

Definición 5.9 *Llamaremos polinomios simétricos elementales de* $K[x_1, ..., x_n]$ *a los polinomios*

$$s_0(x_1, .., x_n) = 1 \text{ y } s_k(x_1, .., x_n) = \sum_{1 \leq i_1 < .. < i_k \leq n} x_{i_1} x_{i_2} .. x_{i_k} \text{ para } k = 1, ..., n.$$

Ejemplo 5.5

Con $n = 2$

$$\begin{aligned} s_0(x_1, x_2) &= 1 \\ s_1(x_1, x_2) &= x_1 + x_2 \\ s_2(x_1, x_2) &= x_1 x_2 \end{aligned}$$

Con $n = 3$

$$\begin{aligned} s_0(x_1, x_2, x_3) &= 1 \\ s_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3 \\ s_2(x_1, x_2, x_3) &= x_1 x_2 + x_1 x_3 + x_2 x_3 \\ s_3(x_1, x_2, x_3) &= x_1 x_2 x_3 \end{aligned}$$

Observación 5.1 *Notar que los polinomios simétricos elementales de* $K[x_1, ..., x_n]$ *y* $K[x_1, ..., x_{n+1}]$ *están relacionados de la siguiente manera:*

- $s_{n+1}(x_1, ..., x_{n+1}) = x_{n+1} s_n(x_1, ..., x_n)$.
- $s_k(x_1, ..., x_{n+1}) = s_k(x_1, ..., x_n) + x_{n+1} s_{k-1}(x_1, ..., x_n)$.

Teorema 5.11 *Sea* K *un cuerpo y* $s_0, s_1, ..., s_n$ *los polinomios simétricos elementales en* $K[x_1, ..., x_n]$ *entonces*

$$(x - x_1)....(x - x_n) = \sum_{k=0}^{n} (-1)^{n-k} s_{n-k}(x_1, ..., x_n) x^k.$$

Demostración: Probaremos este teorema usando inducción matemática.
a) Si $n = 1$ entonces

$$x - x_1 = (-1)^0 s_0(x_1) x^1 + (-1)^1 s_1(x_1) x^0 = \sum_{k=0}^{1} (-1)^{1-k} s_{1-k}(x_1) x^k$$

b) Supongamos que se cumple para n. Ahora veamos que se cumple para $n+1$

$$\begin{aligned}
(x-x_1)...(x-x_{n+1}) &= \sum_{k=0}^{n}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^k(x-x_{n+1}) \\
&= \sum_{k=0}^{n}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^{k+1} - \sum_{k=0}^{n}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^k x_{n+1} \\
&= x^{n+1} + \sum_{k=0}^{n-1}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^{k+1} - (-1)^n s_n(x_1,..,x_n)x_{n+1} \\
&\quad - \sum_{k=1}^{n}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^k x_{n+1} \\
&= x^{n+1} + (-1)^{n+1}s_n(x_1,..,x_n)x_{n+1} + \sum_{k=0}^{n-1}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^{k+1} \\
&\quad - \sum_{k=1}^{n}(-1)^{n-k}s_{n-k}(x_1,..,x_n)x^k x_{n+1} \\
&= x^{n+1} + (-1)^{n+1}s_n(x_1,..,x_n)x_{n+1} + \sum_{k=1}^{n}(-1)^{n+1-k}s_{n+1-k}(x_1,..,x_n)x^k \\
&\quad + \sum_{k=1}^{n}(-1)^{n+1-k}s_{n-k}(x_1,..,x_n)x^k x_{n+1} \\
&= x^{n+1} + (-1)^{n+1}s_n(x_1,..,x_n)x_{n+1} \\
&\quad + \sum_{k=1}^{n}(-1)^{n+1-k}(s_{n+1-k}(x_1,..,x_n) + s_{n-k}(x_1,..,x_n)x_{n+1})x^k \\
&= x^{n+1} + (-1)^{n+1}s_n(x_1,..,x_{n+1}) + \sum_{k=1}^{n}(-1)^{n+1-k}s_{n+1-k}(x_1,..,x_{n+1})x^k \\
&= \sum_{k=0}^{n+1}(-1)^{n+1-k}s_{n+1-k}(x_1,..,x_n,x_{n+1})x^k
\end{aligned}$$

Lo que prueba lo deseado.

Teorema 5.12 *Sea K un cuerpo y $n \geq 1$ entonces el cuerpo de las fracciones algebraicas simétricas de $K(x_1,..,x_n)$ es $K(s_1,..,s_n)$ además $K(x_1,..,x_n)/K(s_1,..,s_n)$ es finita de Galois y su grupo de Galois es S_n.*

Demostración: Sea $p(x) = (x-x_1)....(x-x_n)$ entonces $p(x) = \sum_{k=0}^{n}(-1)^{n-k}s_{n-k}(x_1,...,x_n)x^k$ luego $p(x) \in K(s_1,..,s_n)[x]$ y como los $x_1,..,x_n$ son algebraicos sobre $K(s_1,..,s_n)$ y además son raíces simples de $p(x)$ tenemos que son separables por lo que $K(x_1,..,x_n)/K(s_1,..,s_n)$ es finita de Galois por lo que $|\mathcal{G}(K(x_1,..,x_n)/K(s_1,..,s_n))| \leq n!$.
Por otro lado si $\sigma \in S_n$ tenemos que la siguiente aplicación $\overline{\sigma} : K(x_1,..,x_n) \to K(x_1,..,x_n)$

definida por $\overline{\sigma}(p(x_1,..,x_n)) = p(x_{\sigma(1)},..,x_{\sigma(n)})$ es un homomorfismo de cuerpos. Ahora consideremos el siguiente homomorfismo de grupos $r : S_n \to$ Automorfimos de $K(x_1,..,x_n)$ definido por $r(\sigma) = \overline{\sigma}$. Notar que r es un homomorfismo inyectivo y como S_n deja fijos los elementos de $K(s_1,..,s_n)$ tenemos un monomorfismo de S_n en $K(x_1,..,x_n)/K(s_1,..,s_n)$ por lo que $n! = |S_n| \geq |\mathcal{G}(K(x_1,..,x_n)/K(s_1,..,s_n))|$ pero como $|\mathcal{G}(K(x_1,..,x_n)/K(s_1,..,s_n))| \leq n!$ tenemos que $|S_n| = |\mathcal{G}(K(x_1,..,x_n)/K(s_1,..,s_n))|$ por lo tanto $S_n \cong \mathcal{G}(K(x_1,..,x_n)/K(s_1,..,s_n))$.
Ahora veamos que el cuerpo de las fracciones de $K(x_1,..,x_n)$ es $K(x_1,..,x_n)$. Sea F dicho cuerpo, así de manera similar podemos ver que $S_n \cong \mathcal{G}(K(x_1,..,x_n)/F)$ y por teorema fundamental de la teoría de Galois tenemos que $F = K(s_1,..,s_n)$.

Teorema 5.13 *Sea K un cuerpo de característica cero. Entonces el grupo de Galois del polinomio general de grado n sobre K es isomorfo a S_n.*

Demostración: Sean $a_0,..,a_{n-1}$ los coeficientes de $f_n(x)$ y sean $\alpha_1,..,\alpha_n$ las raices de $f_n(x)$ en una extensión de $K(a_0,..,a_{n-1})$ luego tenemos que el cuerpo de descomposición de $f_n(x)$ sobre $K(a_0,..,a_{n-1})$ es $K(a_0,..,a_{n-1},\alpha_1,..,\alpha_n)$ y así tenemos que $f_n(x) = (x-\alpha_1)..(x-\alpha_n)$ por lo que $a_k = (-1)^{n-k}s_{n-k}(\alpha_1,..,\alpha_n)$ para $k = 0,..,n-1$. Consideremos el siguiente homomorfismo de anillos $\phi : K[a_0,..,a_{n-1}] \to K[(-1)^n s_n,..,-s_1]$ definido de la siguiente manera $\phi(h(a_0,..,a_{n-1})) = h((-1)^n s_n,..,-s_1)$. Ahora veamos que este homomorfismo es inyectivo. Si $\phi(h(a_0,..,a_{n-1})) = \phi(g(a_0,..,a_{n-1}))$ es decir $h((-1)^n s_n,..,-s_1) = g((-1)^n s_n,..,-s_1)$ por lo que $h((-1)^n s_n(\alpha_1,..,\alpha_n),..,-s_1(\alpha_1,..,\alpha_n)) = g((-1)^n s_n(\alpha_1,..,\alpha_n),..,-s_1(\alpha_1,..,\alpha_n))$ que es lo mismo que $h(a_0,..,a_{n-1}) = g(a_0,..,a_{n-1})$ lo que prueba lo deseado, No es difícil ver que además es sobreyectivo por lo que ϕ es un isomorfismo de anillos el que se puede extender a un isomorfismo ϕ' de $K(a_0,..,a_{n-1})$ en $K((-1)^n s_n,..,-s_1)$ y este a otro ϕ''de $K(a_0,..,a_{n-1})[x]$ en $K((-1)^n s_n,..,-s_1)[x]$. Así $\phi''(f_n(x)) = x^n - s_1 x^{n-1} + ... + (-1)^n s_n = (x-x_1)...(x-x_n)$. Por último como $K(a_0,..,a_{n-1},\alpha_1,..,\alpha_n)$ es el cuerpo de descomposición de $f_n(x)$ sobre $K(a_0,..,a_{n-1})$ y $K(x_1,..,x_n)$ es el cuerpo de descomposición de la imagen isomorfa de $f_n(x)$ sobre $K(s_1,..,s_n)$ tenemos que $K(a_0,..,a_{n-1},\alpha_1,..,\alpha_n)/K(a_0,..,a_{n-1}) \cong K(x_1,..,x_n)/K(s_1,..,s_n)$ y así también sus respectivos grupos de Galois, pero como por teorema 5.12 sabemos que $\mathcal{G}(K(x_1,..,x_n)/K(s_1,..,s_n)) \cong S_n$ tenemos que el grupo de Galois del polinomio f_n es S_n es decir $\mathcal{G}(K(a_0,..,a_{n-1},\alpha_1,..,\alpha_n)/K(a_0,..,a_{n-1})) \cong S_n$.

Teorema 5.14 (Abel) *Si K tiene característica cero, la ecuación general de grado n de $K[x]$ no es soluble por radicales para $n \geq 5$ sobre K .*

Demostración: Como S_n no es soluble para $n \geq 5$ el resultado es consecuencia inmediata del teorema anterior.

Conclusión

Al tratar de conocer la respuesta a la pregunta ¿Existen fórmulas para resolver ecuaciones de grado mayor o igual que cinco?, nos encontramos con diferentes maneras de pensar que se utilizaron para resolver las ecuaciones polinomiales, las cuales tienen un gran valor a la hora de observar como de acuerdo a lo conocido en su época los matemáticos intentaron abordar el tema, puesto que intentando dar con la solución del problema se encontraron con obstáculos impensados que los llevaron a cuestionar la existencia de la solución del problema y finalmente probar la imposibilidad de obtener el resultado buscado.

Además de aprender acerca de las distintas maneras de pensar nos encontramos con potentes teorías desarrolladas para resolver el problema, como la de Galois que no solo nos permite dar con la respuesta a la pregunta planteada, sino que también nos entrega herramientas para saber como abordar otros problemas importantes como el teorema fundamental del álgebra trasladando problemas acerca de cuerpos y extensiones a otros de grupos finitos, ampliando la visión y la madurez matemática.

Por último es importante mencionar que aunque algunas de las herramientas aprendidas nos permiten dar soluciones generales resultando de un gran interés teórico, estas tienen algunos inconvenientes prácticos, por ejemplo calcular el grupo de Galois de una ecuación particular para saber si esta es soluble por radicales.

Bibliografía

[1] ROTMAN, Joseph J. Advanced Modern Algebra. Editorial Prentice Hall; 1st edition (2002); 2nd printing (2003)

[2] IVORRA CASTILLO, Carlos. Algebra. http://www.uv.es/ ivorra/Libros/Libros.htm; Corregidas erratas el 31-7-07

[3] IVORRA CASTILLO, Carlos. Geometria. http://www.uv.es/ ivorra/Libros/Libros.htm; Corregidas erratas el 31-7-07

[4] DEL RÍO MATEO, Angel. Ecuaciones algebraicas. http://www.um.es/adelrio/; Última Revisión 16-5-2007

[5] CHAMIZO LORENTE, Fernando. Álgebra I. 1ºIngeniería en informática. Universidad Autónoma de Madrid. Curso 1996-1997

[6] CHAMIZO LORENTE, Fernando. Álgebra II. 3º de Matemáticas. Universidad Autónoma de Madrid. Curso 1996-1997

[7] CHAMIZO LORENTE, Fernando. ¡Que bonita es la teoría de Galois! Álgebra II. 3º de Matemáticas. Universidad Autónoma de Madrid. Curso 2003-2004

[8] FRALEIGH, John. B., Álgebra Abstracta. Editorial Addison-WesleyIberoamericana, 1988.

[9] HERSTEIN, I.N. Álgebra Moderna, Editorial Trillas, 1987.

[10] HALMOS, Paul R. Teoría intuitiva de los Conjuntos, Editorial C.E.C.S.A. Séptima impresión en español: Junio de 1972

[11] BOYER, Carl B. Historia de la Matemática, Alianza editorial, 1986