Universidad Autónoma del Estado de México

Facultad de Ciencias
Departamento de Matemáticas

Solubilidad de ecuaciones ciclotómicas

T E S I S

que para obtener el título de:

Licenciado en Matemáticas

presenta:

Elizabeth Torres Falcon Piza

Asesor de tesis:

Dr. Alfredo Cano Rodríguez

Toluca, Estado de México, 2020.

Contenido

Introducción

La teoría de Galois es usualmente interesante y se remonta a 1600 AC, desde entonces hubo un gran interés en la búsqueda de soluciones de las ecuaciones polinómicas, desde entonces los polinomios siempre han tenido gran importancia en las matemáticas, en particular los polinomios ciclotómicos, pues aparecen con frecuencia en todo el álgebra [Ste]. Estos polinomios son de particular importancia porque para cualquier entero positivo n, los factores irreducibles de $x^n - 1$ sobre los racionales (y enteros) son polinomios ciclotómicos. Además, el polinomio mínimo de cualquier n-ésima raíz de la unidad sobre los racionales es un polinomio ciclotómico [Cox].

A lo largo de la historia muchos matemáticos han intentado dar una fórmula con la cual calcular las raíces del polinomio, como es bien sabido durante un gran tiempo la única fórmula conocida fue para polinomios de grado dos, hasta el método de Cardano y Ferrari con el cual se resuelve analíticamente cualquier ecuación cúbica y cuártica, estos métodos aparecieron por primera vez en el libro Ars Magna en 1545 publicado por el matemático italiano Gerolamo Cardano (1501-1576), y de su estudiante Ludovico Ferrari (1522-1565) [Ste] [Rom]. Durante los posteriores años no se logró encontrar una fórmula para polinomios de grado igual o mayor a cinco, hasta Ruffini y Abel los cuales demostraron que dicha fórmula no existe para polinomios de grado cinco.

Por su parte Galois con el estudio de extensiones de campos (lo que conocemos como teoría de Galois) consigue explicar cuando un polinomio es soluble por radicales y cuando no, concretamente con el gran Teorema de Galois, además de establecer relaciones entre estas extensiones y la solubilidad por radicales de un polinomio [Rot1].

Capítulo 1

Conceptos básicos

La matemática es el trabajo del espíritu humano que está destinado tanto a estudiar como a conocer, tanto a buscar la verdad como a encontrarla.

Évariste Galois

1.1. Grupos, Anillos y Campos

Los siguientes conceptos y definiciones son esenciales para poder entender apropiadamente lo que es una extensión de campos y un campo de descomposición, con la finalidad de poder definir un grupo de Galois llegando así al Teorema de Galois y posteriormente saber cuándo un polinomio es soluble por radicales. Para los siguientes conceptos y definiciones nos basamos en los libros [Hun] y [Her].

Definición 1.1.1. *Un par* $\langle \mathbf{G}, * \rangle$ *donde* $\mathbf{G}$ *es un conjunto y* $*$ *es una operación binaria en* $\mathbf{G}$*, es un* ***grupo*** *si se satisfacen los siguientes axiomas:*

a) $*$ *es una operación asociativa, es decir, para todos* $a, b, c \in \mathbf{G}$ *se cumple,*

$$a * (b * c) = (a * b) * c.$$

b) Existe un elemento $e \in \mathbf{G}$ *el cual llamamos identidad de* $*$ *el cual cumple que para todo* $a \in \mathbf{G}$*,*

$$a * e = a = e * a.$$

c) Cada $a \in \mathbf{G}$ *es invertible, es decir, existe un elemento* $a' \in \mathbf{G}$ *tal que,*

$$a * a' = e = a' * a.$$

Decimos que un grupo $\langle \mathbf{G}, * \rangle$ *es* ***abeliano*** *si* $a * b = b * a \ \ \forall \ a, b \in \mathbf{G}$.

Desde ahora $\mathbf{G}$ será el grupo $\langle \mathbf{G}, * \rangle$.

Definición 1.1.2. *Si* $\mathbf{G}$ *es un grupo finito entonces el* ***orden*** *de* $\mathbf{G}$ *es el número cardinal de* $|\mathbf{G}|$.

Ejemplo 1.1.1. *Sea* $n \in \mathbb{N}$, *fijo. Definimos* $\mathbb{U}_n$ *como el conjunto de las raíces n-ésimas de la unidad en* $\mathbb{C}$, *es decir*

$$\mathbb{U}_n = \{w \in \mathbb{C} \mid w^n = 1\}$$

Con estas características $\mathbb{U}_n$ *es un grupo abeliano con la operación multiplicación.*

Demostración. Veamos que $\langle \mathbb{U}_n, \times \rangle$ es un grupo abeliano.

a) Para la cerradura tenemos que si $a,\ b \in \mathbb{U}_n$, entonces $a^n = 1\ y\ b^n = 1$, de esta manera tenemos $(a \times b)^n = a^n \times b^n = 1 \times 1 = 1$, entonces $(a \times b)^n$ también es una raíz n-ésima de la unidad y con esto se muestra la cerradura.

b) Para el elemento identidad dado que 1 cumple que $1^n = 1$ y 1 es la identidad multiplicativa para los números complejos, entonces el elemento de identidad en $\mathbb{U}_n$ es 1.

c) Si $a \in \mathbb{U}_n$ y además $a \neq 0$, entonces $\left(\frac{1}{a}\right)^n = \frac{1}{a^n} = \frac{1}{1} = 1$ así $\frac{1}{a}$ es un elemento de $\mathbb{U}_n$, es decir es raíz de la unidad y además es el elemento inverso de a.

d) Para la propiedad asociativa, dado que las raíces de la unidad son números complejos, y en los números complejos la operación multiplicación es asociativa, las raíces de la unidad heredan esta propiedad de los números complejos.

e) Para la propiedad conmutativa tenemos que si $a,\ b \in \mathbb{U}_n$, entonces $a^n = 1\ y\ b^n = 1$, luego $(a \times b)^n = (b \times a)^n$, pues en los números complejos la operación multiplicación es conmutativa, entonces también se hereda.

□

Definición 1.1.3. *Decimos que un grupo* $\mathbf{G}$ *es un* ***grupo cíclico*** *cuando hay un elemento a del grupo* $\mathbf{G}$, *tal que todo elemento de* $\mathbf{G}$ *puede ser expresado como una potencia de a.*

Definición 1.1.4. *Sean* $\mathbf{G}_1\ y\ \mathbf{G}_2$ *grupos, una función* $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ *es un* ***homomorfismo*** *de grupos si y sólo si para todo* $a, b \in \mathbf{G}_1$*:*

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Donde $*_1$, $*_2$ *son las operaciones binarias de* $\mathbf{G}_1\ y\ \mathbf{G}_2$ *respectivamente.*

Definición 1.1.5. *Decimos que un homomorfismo de grupos es un* ***isomorfismo*** *si es* ***biyectivo*** *(es decir,* φ *es inyectivo y sobreyectivo).*

Definición 1.1.6. *Sean* $\mathbf{G}_1\ y\ \mathbf{G}_2$ *grupos. Se dice que los grupos* $\mathbf{G}_1\ y\ \mathbf{G}_2$ *son* ***isomorfos*** *o que* $\mathbf{G}_1$ *es* ***isomorfo*** *a* $\mathbf{G}_2$, *y se denota por* $\mathbf{G}_1 \cong \mathbf{G}_2$, *si y sólo si existe un isomorfismo* $\varphi : \mathbf{G}_1 \longrightarrow \mathbf{G}_2$.

Definición 1.1.7. *Sean* $\mathbf{G}$ *un grupo y* $\mathbf{H} \subseteq \mathbf{G}$. *Se dice que* $\mathbf{H}$ *es un* ***subgrupo*** *de* $\mathbf{G}$ *si y sólo si* $\mathbf{H}$ *es un grupo bajo la operación inducida por* $\mathbf{G}$ *y lo denotamos por* $\mathbf{H} \leq \mathbf{G}$.

Observe que $\mathbf{G}$ y $\{e\}$ son subgrupos de $\mathbf{G}$.

Definición 1.1.8. *Sea* $\mathbf{G}$ *un grupo y* $\mathbf{H}$ *un subgrupo de* $\mathbf{G}$, *donde g es un elemento cualquiera de* $\mathbf{G}$, *entonces:*

a) $g\mathbf{H}=\{gh \mid h \in \mathbf{H}\}$ *es una* ***clase lateral izquierda*** *de* $\mathbf{H}$ *en* $\mathbf{G}$.

b) $\mathbf{H}g=\{hg \mid h \in \mathbf{H}\}$ *es una* ***clase lateral derecha*** *de* $\mathbf{H}$ *en* $\mathbf{G}$.

Definición 1.1.9. *Sea* $\mathbf{G}$ *un grupo y* $\mathbf{N} \leq \mathbf{G}$. *Se dice que* $\mathbf{N}$ *es un* ***subgrupo normal*** *de* $\mathbf{G}$, *denotado por* $\mathbf{N} \lhd \mathbf{G}$, *si y sólo si la familia de clases laterales izquierdas de* $\mathbf{N}$ *en* $\mathbf{G}$ *coincide con la familia de clases laterales derechas de* $\mathbf{N}$ *en* $\mathbf{G}$, *es decir, para toda* $g \in \mathbf{G}$ *se cumple* $g\mathbf{N}=\mathbf{N}g$.

Definición 1.1.10. *Se dice que un grupo* $\mathbf{G}$ *es* ***simple*** *si los únicos subgrupos propios normales son* $\mathbf{G}$ *y* $\{e\}$ *(el mismo y el trivial).*

Definición 1.1.11. *Sea* $\mathbf{G}$ *un grupo y* $\mathbf{H}$ *un subgrupo de* $\mathbf{G}$, *llamaremos* ***índice*** *al número de clases laterales ya sea de izquierda o de derecha de* $\mathbf{H}$ *en* $\mathbf{G}$ *y lo denotamos* $[\mathbf{G} : \mathbf{H}]$.

Teoremas importantes de Grupos. Algunos de los resultados importantes que ocuparemos más adelante, son los siguientes:

Teorema 1.1.1. *(**Teorema de Lagrange.**) Si* $\mathbf{G}$ *es un grupo finito y* $\mathbf{H}$ *es un subgrupo normal de* $\mathbf{G}$, *entonces* $|\mathbf{G}| = |\mathbf{H}|\,[\mathbf{G} : \mathbf{H}]$, *donde* $|\mathbf{G}|$ *y* $|\mathbf{H}|$ *son el orden del grupo* $\mathbf{G}$ *y* $\mathbf{H}$ *respectivamente, en tanto que* $[\mathbf{G} : \mathbf{H}]$ *es el índice de* $\mathbf{H}$ *en* $\mathbf{G}$.

Teorema 1.1.2. *(**Teorema de Cauchy.**) Dado un grupo finito* $\mathbf{G}$ *y un número primo p que divida al orden de* $\mathbf{G}$, *existe un elemento de orden p en* $\mathbf{G}$.

Teorema 1.1.3. *(**Primer teorema de Sylow.**) Para cualquier factor primo p con multiplicidad n en el orden del grupo finito* $\mathbf{G}$, *existe un subgrupo de* $\mathbf{G}$ *de orden* p^n. *A este subgrupo se le conoce como p-subgrupo de Sylow de* $\mathbf{G}$.

Teorema 1.1.4. *(**Segundo teorema de Sylow.**) Dado un grupo finito* $\mathbf{G}$, *y un número primo p que divide al orden de* $\mathbf{G}$, *entonces todos los p-subgrupos de Sylow son conjugados entre sí. Es decir, si* $\mathbf{H}$ *y* $\mathbf{K}$ *son p-subgrupos de Sylow entonces existe un elemento g en* $\mathbf{G}$ *tal que* $g^{-1}\mathbf{H}g = \mathbf{K}$.

Teorema 1.1.5. *(**Tercer teorema de Sylow.**) Sea p un factor primo con multiplicidad n en el orden del grupo finito* $\mathbf{G}$, *de manera que el orden de* $\mathbf{G}$ *puede escribirse como* mp^n *donde* $n > 0$ *y p no divide a m. Sea* n_p *el número de p-subgrupos de Sylow de* $\mathbf{G}$. *Entonces se cumple que* n_p *divide a m, que es el índice del p-subgrupos de Sylow de* $\mathbf{G}$, $n_p \equiv 1 \bmod p$.

La demostración de los teoremas anteriores se puede consultar en [Fra] y [Her].

Definición 1.1.12. *Un* ***anillo*** *es una terna* $\langle \mathbf{F}, +, \times \rangle$ *formada por un conjunto* $\mathbf{F}$ *junto con dos operaciones binarias, denotadas por* $+$ *y* $\times$*, llamadas adición y multiplicación, definidas en* $\mathbf{F}$*, además satisface lo siguiente:*

a) $\langle \mathbf{F}, + \rangle$ *es un grupo abeliano.*

b) $\langle \mathbf{F}, \times \rangle$*, la operación* $\times$ *es asociativa.*

c) Las propiedades distributivas de la multiplicación sobre la adición:

i) Propiedad distributiva izquierda. Para todos $a, b, c \in \mathbf{F}$ *:*

$$a \times (b + c) = (a \times b) + (a \times c).$$

ii) Propiedad distributiva derecha. Para todos $a, b, c \in \mathbf{F}$ *:*

$$(a + b) \times c = (a \times c) + (b \times c).$$

Para simplificar la notación escribiremos $\mathbf{F}$ en lugar del anillo $\langle \mathbf{F}, +, \times \rangle$.

Definición 1.1.13. *Un elemento* $1 \in \mathbf{F}$*, es llamado* ***identidad multiplicativa*** *o* ***unitario****, si para todo* $a \in \mathbf{F}$ *se cumple que* $a \times 1 = a = 1 \times a$*. Si* $\mathbf{F}$ *tiene identidad multiplicativa o unitario, se dice que* $\mathbf{F}$ *es un* ***anillo con unitario****.*

Definición 1.1.14. $\mathbf{F}$ *es un* ***anillo conmutativo*** *si y sólo si la operación multiplicación en* $\mathbf{F}$ *es una operación conmutativa, es decir para todos* $a, b \in \mathbf{F}$ *tal que* $a \times b = b \times a$*.*

Definición 1.1.15. $\mathbf{F}$ *es un* ***anillo con división****, si todo elemento no nulo de* $\mathbf{F}$ *es unidad, es decir, para* $u \in \mathbf{F}$*,* u *es unidad en* $\mathbf{F}$ *si y sólo si* u *tiene inverso multiplicativo*

Definición 1.1.16. *Sean* $\mathbf{F}_1$ *y* $\mathbf{F}_2$ *anillos. Una función* $\varphi : \mathbf{F}_1 \longrightarrow \mathbf{F}_2$ *es un* ***homomorfismo de anillos*** *de* $\mathbf{F}_1$ *en* $\mathbf{F}_2$*, si* φ *satisface las siguientes condiciones, para todos* $a, b \in \mathbf{F}_1$*:*

a) $\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b)$*.*

b) $\varphi(a \times_1 b) = \varphi(a) \times_2 \varphi(b)$*.*

Donde los subíndices de la operaciones corresponden al anillo respectivo.

Definición 1.1.17. *Para isomorfismo de anillos se tiene:* φ *es* ***isomorfismo*** *si y sólo si* φ *es función biyectiva y decimos que* $\mathbf{F}_1$ *es* ***isomorfo*** *a* $\mathbf{F}_2$*, o que* $\mathbf{F}_1$ *y* $\mathbf{F}_2$ *son anillos isomorfos, y lo denotamos por* $\mathbf{F}_1 \cong \mathbf{F}_2$*, si y sólo si existe un isomorfismo* $\varphi : \mathbf{F}_1 \longrightarrow \mathbf{F}_2$*.*

De ahora en adelante por notación usaremos ab para la operación $a \times b$.

Definición 1.1.18. *Sean* $\mathbf{F}$ *un anillo y* $a, b \in \mathbf{F}$ *ambos no cero. Si* $ab = 0$ *entonces, se dice que* a *y* b *son* ***divisores de cero****.*

Definición 1.1.19. *Sea* **S** *un anillo.* **S** *es un* ***dominio entero*** *si y sólo si:*

a) **S** *es conmutativo, si la operación multiplicación es conmutativa,*

b) **S** *tiene unitario,*

b) **S** *no tiene divisores de cero.*

Definición 1.1.20. *Sea* **K** *un anillo con unitario* 1, **K** *es* ***campo*** *si y sólo si*

a) **K** *es anillo conmutativo,*

b) **K** *es anillo con división.*

Ejemplo 1.1.2. *Los siguientes conjuntos son anillos con las operaciones binarias usuales,*
a)$\langle \mathbb{Q}, +, \times \rangle$, *b)*$\langle \mathbb{Z}, +, \times \rangle$, *c)* $\langle \mathbb{R}, +, \times \rangle$, *d)*$\langle \mathbb{C}, +, \times \rangle$.
Además el inciso (a), (c) y (d) son campo por lo tanto también son dominio entero y el inciso (b) solo es dominio entero.

Definición 1.1.21. *Sea* **F** *un anillo. La* ***característica*** *de* **F**, *denotada por Char(***F***), se define de la siguiente manera: considerando el conjunto*

$$A = \{n \in \mathbb{N} \mid \forall r \in \mathbf{F} : nr = \underbrace{r + \cdots + r}_{n-veces} = 0\},$$

se tiene que

a) Si $A = \{0\}$ *entonces, la característica de* **F** *es cero, es decir* $Char(\mathbf{F}) = 0$.

b) Si $A \neq \{0\}$, *es decir* $\{0\} \subsetneq A$, *entonces, la característica de* **F** *es* $Char\,(\mathbf{F}) = \min\,(A - \{0\})$.

1.2. Anillo de polinomios

Ahora queremos establecer las condiciones para poder definir un anillo de polinomios y poder trabajar con estos en los diferentes campos, como se verá más adelante con los polinomios ciclotómicos.

Definición 1.2.1. *Sea* **F** *un anillo.*

a) Un ***polinomio*** $p\,(x)$ *con* ***coeficientes*** *en* **F** *es una suma formal infinita (serie)*

$$p\,(x) = \sum_{i \in \mathbb{N}} a_i\, x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_i x^i + \cdots$$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_i x^i + \cdots$$

tal que

i) Para todo $i \in \mathbb{N}$, $a_i \in \mathbf{F}$.

ii) El conjunto $S(p(x)) = \{i \in \mathbb{N} | \ a_i \neq 0\}$ *es finito (en otras palabras a partir de alguna* i, $a_i = 0$*).*

También se tiene que x *es llamada* ***indeterminada*** *y para cada* $i \in \mathbb{N}$, a_i *es llamado* ***coeficiente*** *de* $p(x)$.

b) Sea $p(x) = \sum_{i \in \mathbb{N}} a_i x^i$ *un polinomio con coeficientes en* $\mathbf{F}$ *y considérese el conjunto* $S(p(x))$.

i) Si $S(p(x)) = \emptyset$ *entonces, se dice que* $p(x)$ *es polinomio nulo o cero, y se escribe* $p(x) = 0$.

ii) Si $S(p(x)) \neq \emptyset$ *entonces, el grado de* $p(x)$ *se denota y define por:*

$$grd[p(x)] = \max(S(p(x))) = \max\{i \in \mathbb{N} \mid a_i \neq 0\}.$$

En estas condiciones $\mathbf{F}[x]$ es el conjunto de todos los polinomios en la indeterminada x con coeficientes en el anillo $\mathbf{F}$, es decir,

$$\mathbf{F}[x] = \{p(x) = \sum_{i \in \mathbb{N}} a_i x^i \mid p(x) \text{es polinomio con coeficientes en } \mathbf{F}\}.$$

Observación 1.2.1. *Sean* $\mathbf{F}$ *un anillo y* $\mathbf{F}[x]$ *el conjunto de todos los polinomios en una indeterminada* x.

a) Las operaciones usuales de adición y multiplicación polinomial son operaciones binarias en $\mathbf{F}[x]$*, con las cuales* $\mathbf{F}[x]$ *es un anillo.*

b) Si $\mathbf{F}$ *es anillo conmutativo entonces,* $\mathbf{F}[x]$ *es anillo conmutativo.*

c) Si $\mathbf{F}$ *tiene unitario* 1 *entonces,* $\mathbf{F}[x]$ *es anillo con unitario, a saber el polinomio constante* $1(x) = 1$.

Sean $f(x)$, $p(x)$ polinomios en la indeterminada x con coeficientes en el campo $\mathbf{F}$ tales que

$$\begin{aligned} f(x) &= \sum_{i=0}^{n} a_i \, x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \\ p(x) &= \sum_{i=0}^{m} b_i \, x^i = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \end{aligned}$$

Se definen las operaciones binarias de la siguiente manera:

Adición de polinomios:

$$\begin{aligned} f(x)+p(x) &= \sum_{i=0}^{n} a_i\, x^i + \sum_{i=0}^{m} b_i\, x^i \\ &= a_0+b_0+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_m)x^{n+m} \end{aligned}$$

Multiplicación de polinomios:

$$\begin{aligned} f(x)p(x) &= \left(\sum_{i=0}^{n} a_i\, x^i\right)\left(\sum_{i=0}^{m} b_i\, x^i\right) \\ &= \sum_{k=0}^{m+n} e_k\, x^k, \end{aligned}$$

donde $e_k = \sum_{c=0}^{k} a_c\, b_{k-c}$.

Con estas operaciones $\mathbf{F}[x]$ será el anillo de polinomios con coeficientes en un campo $\mathbf{F}$.

Definición 1.2.2. *Sea $p(x) \in \mathbf{F}[x]$, llamaremos **raíz** del polinomio $p(x)$ al elemento u, tal que $p(u) = 0$.*

Definición 1.2.3. *Sea $p(x) \in \mathbf{F}[x]$, no nulo ni constante. $p(x)$ es **irreducible** sobre $\mathbf{F}$ o es **un polinomio irreducible** en $\mathbf{F}[x]$ si $p(x)$ no puede expresarse como un producto $g(x)h(x)$ de dos polinomios $g(x)$ y $h(x)$ en $\mathbf{F}[x]$, ambos de grado menor que el de $p(x)$.*
*Diremos que es **separable**, si dicho polinomio se descompone completamente en productos de factores con raíces simples, es decir, si la multiplicidad de las raíces es* 1.

Diremos que un polinomio es **mónico** si su coeficiente principal es 1, es decir, para el polinomio $p(x) = \sum_{i=0}^{n} a_i\, x^i = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$ tenemos que este será mónico si $a_n = 1$.
La función φ de **Euler** (ver [Jon]), es una función que utilizaremos mas adelante y que se define como

$$\varphi(n) = |\,\{m < n \mid (m,n) = 1\}\,|\,.$$

Se cumplen las siguientes igualdades

$$\begin{aligned} \varphi(p) &= p-1, \\ \varphi(p^k) &= (p-1)p^{k-1}, \\ \varphi(mn) &= \varphi(m)\varphi(n). \end{aligned}$$

También nos sera de utilidad el siguiente teorema, su demostración la encontramos en [Jon].

Teorema 1.2.1. *(**Teorema chino del residuo.**) Sean* $p_1,\ p_2,\cdots,\ p_n \in \mathbb{N}$*, n números naturales de modo que* $(p_i, p_j) = 1$*, para* $i \neq j$*. Si para* $w_1,\ w_2,\cdots,\ w_n \in \mathbb{Z}$*, se plantean las siguentes n congruencias*

$$x \equiv w_i \quad \text{mód } p_i,$$

para toda $i = 1,\ 2,\cdots, n$*, entonces este sistema tiene una única solución dada por*

$$x = \sum_{i=1}^{n} w_i c_i d_i,$$

donde $c_i = \dfrac{p_1\ p_2 \cdots p_n}{p_i}$ *y* r_i *es el inverso de* c_i *en* $\mathbb{Z}_{n_i}$ *para* $i = 1,\ 2,\cdots, n$*.*

Capítulo 2

Extensiones, grupo de Galois y solubilidad de grupos.

La matemática es el alfabeto con el que Dios escribió al mundo.

Galileo Galilei.

Antes de entrar con el estudio de la solubilidad de los polinomios por radicales, tenemos que analizar algunos resultados de la solubilidad de grupos (sección 2.3) y los principales teoremas de la teoría de Galois, para lo cual necesitamos conocer acerca de las extensiones de campos. Para ello, tomaremos como referencia los libros [Hun] y [Cox]. Empezaremos introduciendo conceptos que serán de utilidad para este capítulo.

2.1. Extensiones

Para comenzar con el estudio de extensiones, recordemos la estructura algebraica creada a partir de un conjunto no vacío, la cual llamaremos espacio vectorial. Además mostraremos que dado un polinomio $f(x)$ en un campo $\mathbf{K}[x]$ existe un campo $\mathbf{E}$ tal que $\mathbf{K} \subseteq \mathbf{E}$ y además dicho campo contendrá todas las raíces de $f(x)$, teniendo en un principio que $f(x)$ es tal que tiene alguna raíz en $\mathbf{E}$. Véase [Fra].

Definición 2.1.1. *Sea* $\mathbf{K}$ *un campo con elementos* $a, b, \ldots$, *los cuales llamaremos coeficientes o escalares, y* $\mathbf{G}$ *un grupo abeliano aditivo, con elementos* $x, y, \ldots$, *los cuales llamaremos vectores, tales que cumplen las siguientes condiciones:*

a) Para todos $x, y \in \mathbf{G}$, $x + y \in \mathbf{G}$.

b) Para todos $x, y \in \mathbf{G}$, $x + y = y + x$.

c) Para todos $x, y, z \in \mathbf{G}$, $z + (x + y) = (z + y) + x$.

d) Existe un elemento neutro $w \in \mathbf{G}$ *tal que* $x + w = w + x = x$.

e) Existe un elemento inverso $-x \in \mathbf{G}$ *tal que* $x + (-x) = w = -x + x$.

f) Para toda $a \in \mathbf{K}$ *y toda* $x \in \mathbf{G}$, $ax \in \mathbf{G}$.

g) Para toda $a \in \mathbf{K}$ *y* $x, y, z \in \mathbf{G}$ *se cumple* $a(x+y) = ax + ay$.

h) Para toda $a, b \in \mathbf{K}$ *y* $x \in \mathbf{G}$ *se cumple* $(a+b)x = ax + bx$.

i) Sean $a, b \in \mathbf{K}$ *y* $x \in \mathbf{G}$ *se cumple que* $(ab)x = a(bx)$.

j) Para el elemento identidad $1 \in \mathbf{K}$ *y* $x \in \mathbf{G}$ *se cumple que* $1x = x = x1$.

Decimos entonces que **G** *es un* ***espacio vectorial*** *sobre el campo* **K**, *más precisamente,* **G** *es un* **K***-espacio vectorial.*

Definición 2.1.2. *Un campo* ***E*** *es una* ***extensión*** *de* **K**, *si* **K** *es un subcampo de* ***E***, *es decir si* $\langle \mathbf{E}, +, \times \rangle$ *es un campo y* $\langle \mathbf{K}, +, \times \rangle$ *es un campo con las operaciones* $+$ *y* $\times$ *de* ***E***. *Denotemos a la extensión* **E** *sobre* **K** *como* ***E*** *:* **K**.

Ejemplo 2.1.1. *Consideremos los siguientes campos y subcampos,* $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{C}$, *de está manera tenemos que* $\mathbb{R} : \mathbb{Q}$, $\mathbb{C} : \mathbb{R}$, $\mathbb{C} : \mathbb{Q}$, *es decir* $\mathbb{R}$ *es una extensión de* $\mathbb{Q}$, $\mathbb{C}$ *es una extensión de* $\mathbb{R}$ *y* $\mathbb{C}$ *es una extensión de* $\mathbb{Q}$.

Supongamos que $\mathbf{E} : \mathbf{K}$ es una extensión de campo. Entonces **E** tiene estructura de un **K** espacio vectorial (**K** el campo de los escalares). Como todo espacio vectorial tiene base, podemos calcular la dimensión de **E** como espacio vectorial sobre **K**, denotado por $\dim_{\mathbf{K}}(\mathbf{E})$.

Definición 2.1.3. *Se denomina* ***grado de la extensión*** $\mathbf{E} : \mathbf{K}$ *a la dimensión de* **E** *como* **K***-espacio vectorial,* $|\, \mathbf{E} : \mathbf{K} \,| = \dim_{\mathbf{K}}(\mathbf{E})$, *si el grado de la extensión* $\mathbf{E} : \mathbf{K}$ *es finito, lo denotamos* $|\, \mathbf{E} : \mathbf{K} \,| < \infty$.

Definición 2.1.4. *Sea* **E** *un campo de extensión de* **K**. *Se dice que un elemento* $u \in \mathbf{E}$ *es* ***algebraico*** *sobre* **K** *si u es una raíz de algún polinomio no cero* $f \in \mathbf{K}[x]$.
Una extensión de campo $\mathbf{E} : \mathbf{K}$ *se dice* ***algebraica*** *si cada elemento de* **E** *es algebraico sobre* **K**, *es decir, si cada elemento de* **E** *es una raíz de algún polinomio distinto de cero con coeficientes en* **K**.

Ejemplo 2.1.2. *Los siguientes son ejemplos de elementos algebraicos en un campo.*

a) El elemento $\sqrt{2} \in \mathbb{R}$ *es algebraico sobre* $\mathbb{Q}$, *pues* $\sqrt{2}$ *es una raíz del polinomio* $x^2 - 2 \in \mathbb{Q}[x]$.

b) El elemento $\xi_n = e^{2\Pi i/n} \in \mathbb{C}$ *es algebraico sobre* $\mathbb{Q}$ *pues es una raíz de* $x^n - 1 \in \mathbb{Q}[x]$.

c) El elemento $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ *es algebraico sobre* $\mathbb{Q}$, *pues es raíz del polinomio*

$$\left(x - \sqrt{2} - \sqrt{3}\right)\left(x - \sqrt{2} + \sqrt{3}\right)\left(x + \sqrt{2} - \sqrt{3}\right)\left(x + \sqrt{2} + \sqrt{3}\right) = x^4 - 10x^2 + 1.$$

Definición 2.1.5. *Sea* $\mathbf{E} : \mathbf{K}$ *una extensión de campo, se dice que* $\mathbf{E} : \mathbf{K}$ *es* ***extensión finita*** *si el grado de la extensión* $|\ \mathbf{E} : \mathbf{K}\ |$ *es un número finito. En concreto, una extensión se dice que es* ***finita*** *si es de grado finito.*

Definición 2.1.6. *Sea* $\mathbf{E}$ *una extensión del campo* $\mathbf{K}$ *(*$\mathbf{E} : \mathbf{K}$*), para el polinomio* $f \in \mathbf{K}[x]$ *sea* $\alpha \in \mathbf{E}$ ***algebraico*** *sobre* $\mathbf{K}$ *y* $p_\alpha(x)$ *el* ***polinomio minimo*** *de grado* n *que es anulado por* α*, entonces*

$$\mathbf{E}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbf{K}\}$$

Ejemplo 2.1.3. *Consideremos la extensión* $\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}$*, donde*

$$\mathbb{Q}\left(\sqrt{2}\right) = \{x + y\sqrt{2} :\ x,\ y \in \mathbb{Q}\}.$$

Afirmamos que $|\ \mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\ | = 2$*. Notemos que los elementos* $1,\ \sqrt{2}$ *generan al espacio vectorial* $\mathbb{Q}\left(\sqrt{2}\right)$*, recordemos que* $\sqrt{2} \notin \mathbb{Q}$*, si los elementos* $1,\ \sqrt{2}$ *fueran linealmente dependientes tendriamos que* $u + v\sqrt{2} = 0$ *para algunos* $u,\ v \in \mathbb{Q}$ *no ambos cero, de hecho tenemos que ambos no son cero, de esta manera*

$$\sqrt{2} = \frac{-u}{v} \in \mathbb{Q},$$

lo cual no es cierto. Entonces los elementos $1,\ \sqrt{2}$ *son linealmente independientes y así forman una base para* $\mathbb{Q}\left(\sqrt{2}\right)$ *sobre* $\mathbb{Q}$*, de esta manera* $|\ \mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\ | = 2$*.*

Recordemos que un campo $\mathbf{K}$ es **finitamente generado** si existe un conjunto finito de elementos $\mathbf{A} = \{x_1, \cdots,\ x_n\}$ tal que $\mathbf{A}$ genera a $\mathbf{K}$ y lo denotamos $\langle \mathbf{A} \rangle = \mathbf{K}$. Así no debemos confundir el término extensión finita con el de extensión finitamente generada. Toda extensión finita es finitamente generada, pero no es cierto el recíproco, véase [Hun].

Proposición 2.1.1. *Sea* $\mathbf{E} : \mathbf{K}$ *una extensión de campo finita, entonces* $\mathbf{E}$ *es finitamente generado y algebraico sobre* $\mathbf{K}$*.*

Demostración. Supongamos que $|\ \mathbf{E} : \mathbf{K}\ | = n$ y sea $u \in \mathbf{E}$, entonces el conjunto de $n + 1$ elementos

$$S = \{1_{\mathbf{K}}, u, u^2, \cdots,\ u^n\}$$

es un conjunto linealmente dependiente (pues $dim_{\mathbf{K}}(\mathbf{E}) = n = |\ \mathbf{E} : \mathbf{K}\ |$), así existen $a_i \in \mathbf{K}$ con $i = \{0, \cdots,\ n\}$ tal que para algún $j \in \{0, \cdots,\ n\}$ se tiene $a_j \neq 0$ donde

$$a_0 + a_1 u + \cdots +\ a_n u^n = 0,$$

lo cual implica que u es algebraico sobre $\mathbf{K}$ y como u fue arbitrario entonces tenemos que $\mathbf{E}$ es algebraico sobre $\mathbf{K}$. Como $\mathbf{E}$ tiene estructura de $\mathbf{K}$-espacio vectorial entonces existe $B = \{v_1, \cdots,\ v_n\}$ una base de $\mathbf{E}$ sobre $\mathbf{K}$ así $\mathbf{E} = \mathbf{K}(v_1, \cdots,\ v_n)$, lo cual implica que $\mathbf{E}$ es finitamente generado sobre $\mathbf{K}$. □

Definición 2.1.7. *Un campo* $\mathbf{K}$ *es* ***algebraicamente cerrado*** *si todo polinomio* $p(x) \in \mathbf{K}[x]$ *se descompone sobre* $\mathbf{K}$*. La* ***clausura algebraica*** *de* $\mathbf{K}$*, es la extensión más pequeña* $\mathbf{E} : \mathbf{K}$ *tal que* $\mathbf{E}$ *es algebraicamente cerrado, y lo denotamos* $\overline{\mathbf{K}}$*.*

Proposición 2.1.2. *Sea* $\mathbf{K}$ *un campo, si* $\mathbf{E} : \mathbf{K}$ *es una extensión algebraica, entonces* $\overline{\mathbf{E}} = \overline{\mathbf{K}}$*.*

Demostración. Sea $p(x) \in \mathbf{K}[x]$ y $\mathbf{E}$ una extensión de $\mathbf{K}$, tal que $p(x)$ se descompone sobre $\mathbf{E}$, entonces por la definición 2.1.7, tenemos $\overline{\mathbf{K}} = \mathbf{E}$. Ahora solo falta ver que $\mathbf{E} = \overline{\mathbf{E}}$, como la extensión de campo depende del polinomio $p(x)$ que se toma en el campo $\mathbf{K}$, entonces por el argumento anterior $p(x)$ se descompone en $\mathbf{E}$, es decir $\mathbf{E}$ es algebraicamente cerrado, por lo cual $\mathbf{E} = \overline{\mathbf{E}}$. □

Definición 2.1.8. *Sea* $\mathbf{E} : \mathbf{K}$ *una extensión algebraica, decimos que es una* ***extensión normal*** *si todo polinomio* $p(x) \in \mathbf{K}[x]$ *que tiene una raíz en* $\mathbf{E}$ *se descompone en factores lineales en* $\mathbf{E}[x]$*.*

Definición 2.1.9. *Sea* $\mathbf{E} : \mathbf{K}$ *una extensión y supongamos que* $\alpha \in \mathbf{E}$ *es algebraico sobre* $\mathbf{K}$ *entonces el* ***polinomio mínimo*** *de* α *sobre* $\mathbf{K}$ *es el único polinomio mónico* m *sobre* $\mathbf{K}$ *de menor grado tal que* $m(\alpha) = 0$

Ejemplo 2.1.4.

a) Del ejemplo 2.1.2 inciso a) el polinomio mínimo de $\sqrt{2}$ *sobre* $\mathbb{Q}$ *es* $x^2 - 2$*, lo cual se deduce de la irracionalidad de* $\sqrt{2}$*, lo cual implica que* $\sqrt{2}$ *no puede ser la raíz de un polinomio de grado* 1 *en* $\mathbb{Q}$*.*

b) Del ejemplo 2.1.2 inciso b) el polinomio mínimo de $\xi_n = e^{2\Pi i/n}$ *sobre* $\mathbb{Q}$*, es el polinomio* $\Phi_n(x) = x^n - 1$*.*

Definición 2.1.10. *Si* $\mathbf{E} : \mathbf{K}$ *es una extensión algebraica, se dice que* $\alpha \in \mathbf{E}$ *es* ***separable*** *sobre* $\mathbf{K}$ *si su polinomio mínimo lo es. Se dice que una extensión* $\mathbf{E} : \mathbf{K}$ *es una* ***extensión separable*** *si todo* $\alpha \in \mathbf{E}$*, es separable sobre* $\mathbf{K}$*.*

Definición 2.1.11. *Un campo es* ***perfecto*** *si todas sus extensiones algebraicas son separables.*

Para saber si un campo es perfecto, nos fijamos en su característica, esté será perfecto si su característica es 0, ó es p y todo elemento del campo es una raíz p-ésima. En particular todo campo de característica cero y todo campo finito es perfecto [Mor].

Definición 2.1.12. *Una extensión finita es de* ***Galois*** *si es una extensión normal y separable.*

Definición 2.1.13. *Una extensión* $\mathbf{E} : \mathbf{K}$ *es una* ***extensión simple****, si es tal que* $\mathbf{E} = \mathbf{K}(\alpha)$*, para algún* $\alpha \in \mathbf{E}$*.*

Definición 2.1.14. *Dado un campo* $\mathbf{K}$*, y un polinomio no constante* $p(x) \in \mathbf{K}[x]$ *de grado* $n > 0$*, se define el* ***campo de descomposición*** *de* p *como un campo* $\mathbf{E}_p$ *que cumple que el polinomio* $p(x)$ *se descompone completamente en* $\mathbf{E}_p$*, es decir,* $p(x)$ *se expresa como producto de polinomios de grado* 1*,* $p(x) = b\prod_{i=1}^{n}(x - \alpha_i)$*,* $b, x \in \mathbf{K}$*,* $\alpha_i \in \mathbf{E}_p$*.*

El campo de descomposición de p es el que resulta de adjuntar a $\mathbf{K}$ todas las raíces del polinomio $p(x)$, con lo cual $\mathbf{E}_p = \mathbf{K}(\alpha_1, \cdots, \alpha_n)$. Este campo no es único, sin embargo si hay dos campos de descomposición tendrían que ser isomorfos [Her], y además es el campo mas pequeño que contiene a las raices de p. Cuando se construye una extensión de un campo, se busca un conjunto más grande en el que las operaciones suma y producto sigan funcionando bien y además se puedan resolver las ecuaciones polinómicas.

Ejemplo 2.1.5. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\pm\sqrt{2}, \pm\sqrt{3}\right)$ *es un campo de descomposición del polinomio* $\left(x^2-2\right)\left(x^2-3\right) = x^4 - 5x^2 + 6$ *sobre* $\mathbb{Q}$.

2.2. El grupo de Galois

Un grupo de Galois es un grupo asociado a un cierto tipo de extensión de campo. El estudio de las extensiones de campos (y los polinomios que dan lugar a ellas) mediante el grupo de Galois es conocido como teoría de Galois.
Galois notó que el problema de si las soluciones de una ecuación se pueden expresar en términos de sumas, productos y raíces n-ésimas (radicales) de los coeficientes de la ecuación, se podía resolver comparando el campo generado por los coeficientes con el campo generado por las soluciones de la ecuación. Ahora veamos qué es un grupo de Galois.

Definición 2.2.1. *Sea* $Aut(\mathbf{E})$*, el grupo de todos los* ***automorfismos*** *de* $\mathbf{E}$*, esto es el conjunto de isomorfismos de campos* $\varphi : \mathbf{E} \longrightarrow \mathbf{E}$*. Si* $\mathbf{E}$ *es una extensión del campo* $\mathbf{K}$*. El* ***grupo de Galois*** *de* $\mathbf{E}$ *sobre* $\mathbf{K}$ *queda definido como el grupo de automorfismos de* $\mathbf{E}$ *que dejan fijo al campo* $\mathbf{K}$*, es decir* $Gal(\mathbf{E} : \mathbf{K}) = \{\phi \in Aut(\mathbf{E}) : \phi(a) = a, \text{ para todo } a \in \mathbf{K}\}$.

Definición 2.2.2. *Una extensión* $\mathbf{E} : \mathbf{K}$ *es* ***abeliana*** *si el grupo* $Gal(\mathbf{E} : \mathbf{K})$ *es abeliano.*

Definición 2.2.3. *Una extensión finita* $\mathbf{E} : \mathbf{K}$ *se llama* ***cíclica*** *si es de Galois y su grupo de Galois es cíclico.*

Proposición 2.2.1. *Supongamos que* $\mathbf{E}$ *es una extensión sobre* $\mathbf{K}$ *y sea* $f \in \mathbf{K}[x]$*. Si* $a \in \mathbf{E}$ *es una raíz de* $f(x)$*, entonces* $\sigma(a)$ *es una raíz de* $f(x)$*, donde* σ *es una permutación.*

Demostración. Sea A el conjunto de raíces de f en $\mathbf{E}$. Definimos una acción de $\mathrm{Gal}(\mathbf{E} : \mathbf{K})$ sobre A tal que $a\sigma = \sigma(a)$. Si $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $f(a) = 0$, entonces para toda $\sigma \in$

Gal($\mathbf{E}:\mathbf{K}$) y $a \in A$, tenemos que

$$\begin{aligned} f(\sigma(a)) &= f(a\sigma) \\ &= a_0 + a_1\sigma(a) + \cdots + a_n(\sigma(a))^n \\ &= a_0 + a_1 a\sigma + \cdots + a_n \left(\underbrace{\sigma(a) \times \cdots \times \sigma(a)}_{n-veces} \right) \\ &= \sigma^n(a_0 + a_1 a + \cdots + a_n a^n) \\ &= \sigma^n(f(a)) \\ &= \sigma^n(0) = 0\sigma = 0. \end{aligned}$$

□

Sea $\mathbf{E}_p$ un campo de descomposición de un polinomio $p(x)$ sobre un campo $\mathbf{K}[x]$. Para $d_1, \cdots, d_m$ que son raíces de $p(x)$ en $\mathbf{K}$ y $\sigma \in Gal(\mathbf{E}_p : \mathbf{K})$, entonces σ envía raíces de $p(x)$ en raíces de $p(x)$ por lo tanto existe $\sigma_p \in S_m$ tal que $\sigma(d_i) = d_{\sigma_{p(i)}}$, $\forall i \in 1, \cdots, m$, donde S_m es el grupo de permutaciones de m elementos. En resumen un grupo de Galois manda raíces en raíces y además como consecuencia se tendrá que Gal($\mathbf{E}_p : \mathbf{K}$) $\cong S_m$, lo cual se verá mas adelante para $m = 3$.

Definición 2.2.4. *El **Grupo de Galois de un polinomio** $f \in \mathbf{K}[x]$ denotado por Gal($f : \mathbf{K}$) y se define como el grupo de Galois del campo de descomposición $\mathbf{E}_f$ de f sobre $\mathbf{K}$, es decir Gal($f : \mathbf{K}$)= $\{\phi \in Aut(\mathbf{E}_f) : \phi(a) = a$ para todo $a \in \mathbf{K}\}$.*

Proposición 2.2.2. *Si $f(x) = p_1^{e_1}(x) \cdots p_n^{e_n}(x)$ es una factorización de $f(x)$ en potencias de polinomios irreducibles distintos sobre $\mathbf{K}$, entonces $\mathbf{E}_f$ también es un campo de descomposición para el polinomio $q(x) = p_1(x) \cdots p_n.(x)$*

Demostración. Como $p_i(x)$ es irreducible en $\mathbf{K}[x]$ $\forall i \in \{1, \cdots, n\}$ y como $\mathbf{E}_f$ es el campo de descomposición de $f(x)$ se tiene que cada $p_i(x)$ se descompone en factores lineales en $\mathbf{E}_f$, es decir, $p_i(x) = (x - a_{1\,i})(x - a_{2\,i}) \cdots \left(x - a_{s_i\,i}\right)$ para $i \in \{1, \cdots, n\}$ de esta manera

$$\begin{aligned} f(x) &= p_1^{e_1}(x) \cdots p_n^{e_n}(x) \\ &= \left((x - a_{1\,1})(x - a_{2\,1}) \cdots \left(x - a_{s_i\,1}\right)\right)^{e_i} \cdots \left((x - a_{1\,n})(x - a_{2\,n}) \cdots \left(x - a_{s_i\,n}\right)\right)^{e_n}, \end{aligned}$$

es decir

$$\mathbf{E}_f = \mathbf{K}\left(a_{1\,1},\ a_{2\,1}, \cdots,\ a_{s_i\,1}, \cdots,\ a_{1\,n},\ a_{2\,n}, \cdots,\ a_{s_i\,n}\right).$$

Ahora sea $q(x) = p_1(x) \cdots p_n(x)$, como $p_i(x)$ son irreducible en $\mathbf{K}[x]$, y cada $p_i(x)$ se factoriza en $\mathbf{E}_f$ tenemos

$$q(x) = (x - a_{1\,1})(x - a_{2\,1}) \cdots \left(x - a_{s_i\,1}\right) \cdots (x - a_{1\,n})(x - a_{2\,n}) \cdots \left(x - a_{s_i\,n}\right),$$

con lo que

$$\mathbf{E}_q = \mathbf{K}\left(a_{1\,1},\ a_{2\,1}, \cdots,\ a_{s_i\,1}, \cdots,\ a_{1\,n},\ a_{2\,n}, \cdots,\ a_{s_i\,n}\right),$$

así $\mathbf{E}_f = \mathbf{E}_q$. □

Definición 2.2.5. *Una secuencia de campos para los cuales $\mathbf{E}_{i+1} : \mathbf{E}_i$, le llamaremos **Torre de campos** y se escribe como*

$$\mathbf{E}_0 \subseteq \mathbf{E}_1 \subseteq \mathbf{E}_2 \subseteq \cdots \subseteq \mathbf{E}_{n-1} \subseteq \mathbf{E}_n.$$

Ejemplo 2.2.1. *Del ejemplo 3.1.1 tenemos la siguiente torre*

$$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C},$$

pues tenemos que $\mathbb{R} : \mathbb{Q}$, $\mathbb{C} : \mathbb{R}$ y $\mathbb{C} : \mathbb{Q}$ son extensiones.

Teorema 2.2.1. *(**Teorema Fundamental de la Teoría de Galois.**) Sea $\mathbf{K} : \mathbf{F}$ una extensión de Galois y sea $\mathbf{G}$ =Gal($\mathbf{K} : \mathbf{F}$) el grupo de Galois de $\mathbf{K} : \mathbf{F}$, entonces hay una correspondencia uno a uno entre $\boldsymbol{L}$ el conjunto de todos los campos intermedios de $\mathbf{K} : \mathbf{F}$ ($\mathbf{F} \subset \mathbf{E}_1 \subset \mathbf{E}_2 \subset \cdots \subset \mathbf{E}_n = \mathbf{K}$) y el conjunto de todos los subgrupos de Gal($\mathbf{K} : \mathbf{F}$), mediante la función $F : \boldsymbol{L} \longrightarrow Gal(\mathbf{K} : \mathbf{F})$ la cual está dada por $\mathbf{E}_i \longrightarrow F(\mathbf{E}_i) = Gal(\mathbf{E}_i : \mathbf{F}) \leqslant Gal(\mathbf{K} : \mathbf{F})$, además $Gal(\mathbf{K} : \mathbf{E}_i) \lhd Gal(\mathbf{K} : \mathbf{F})$ $\forall\ i = 1, \cdots, n$, de donde*

$$Gal\,(\mathbf{E}_i : \mathbf{F}) \cong \frac{Gal\,(\mathbf{K} : \mathbf{F})}{Gal\,(\mathbf{K} : \mathbf{E}_i)}.$$

Para la demostración véase [Hun].

El Teorema fundamental de la teoría de Galois es un resultado que describe la estructura de ciertos tipos de extensiones de campos.

2.3. Solubilidad de grupos

Para poder establecer la definición de grupo soluble, definimos lo siguente.

Definición 2.3.1. *Una serie de subgrupos $\mathbf{G}_i$ de $\mathbf{G}$ se dice **serie normal** si $\mathbf{G}_0 = 1$, $\mathbf{G}_r = \mathbf{G}$ y $\mathbf{G}_i$ es normal en $\mathbf{G}_{i+1}$ es decir, $\mathbf{G}_i \lhd \mathbf{G}_{i+1}$. Los grupos cocientes $\mathbf{G}_{i+1}/\mathbf{G}_i$ se dicen **factores de la serie**.*

$$1 = \mathbf{G}_0 \subseteq \mathbf{G}_1 \subseteq \cdots \subseteq \mathbf{G}_r = \mathbf{G}$$

Definición 2.3.2. *Un grupo se dice **soluble** si contiene una serie normal $\mathbf{G}_i$ de factores abelianos.*

Ejemplo 2.3.1. *a) Sea S_n es el grupo simétrico de n elementos, formado por las funciones biyectivas (permutaciones) de un conjunto X en sí mismo. Sabemos que toda permutación se puede descomponer en producto de trasposiciones, en este sentido tenemos que una permutación par es una permutación que puede ser representada por un número par de trasposiciones. Recordemos que si $\sigma \in S_n$, ésta será una trasposición si existen $j, k \in \mathbb{N}$, $j \neq k$, tal que*

$$\sigma(i) = \begin{cases} k & \text{si } i = j \\ j & \text{si } i = k \\ i & \text{si } i \neq j, k \end{cases}$$

Así sea $A_n = \{\sigma \in S_n : \sigma \text{ es par}\}$ llamado el grupo alternante. Entonces A_4 es el grupo alternante de grado 4 el cual admite la serie normal $1 \lhd V \lhd A_4$, donde V es el subgrupo de orden 4 formado por los productos de trasposiciones, y como V/A_4 es abeliano [Hun], entonces A_4 es soluble.

b) El grupo A_5 no puede ser soluble, sea A_5 el grupo mas pequeño simple y no abeliano [Ste], al ser simple sus únicos subgrupos normales son el mismo y el trivial, así A_5 tiene la serie $1 \lhd A_5$ de esta manera tenemos el factor $A_5/\{e\}$, y sabemos que este factor será abeliano si y solo si A_5 es abeliano [Fra], lo cual no sucede, por tanto A_5 no es soluble.

Definición 2.3.3. *Dado un grupo $\mathbf{G}$, llamamos **serie de composición** a una serie normal de factores simples.*

Ejemplo 2.3.2. *a) Para este ejemplo consideremos S_5 como el grupo de permutaciones de 5 elementos y A_5 como el grupo alternante.*
La serie $1 \lhd A_5 \lhd S_5$ es de composición en S_5, pues los factores $A_5/1 = A_5$ y S_5/A_5 son simples, y además S_5 solo tiene como subgrupo normal a A_5[Fra].
Para el factor $A_5/1 = A_5$ tenemos que este es simple pues A_5 es simple [Ste].
Para el factor S_5/A_5 veamos que sus únicos subgrupos normales son el mismo y el trivial, sabemos que $S_5/A_5 \lhd S_5/A_5$ es cierto pues todo grupo se tiene a si mismo como subgrupo normal. Ahora veamos que A_5 es el grupo trivial para S_5/A_5, sabemos que $S_5/A_5 = \{aA_5 \mid a \in S_5\}$, sea $\bar{a} \in S_5/A_5$, entonces

$$\bar{a}A_5 = aA_5A_5 = aA_5 = \bar{a}$$

y

$$A_5\bar{a} = A_5aA_5 = A_5A_5a = aA_5 = \bar{a},$$

pues $A_5 \lhd S_5$, es decir $aA_5 = A_5a \ \forall a \in S_5$.
Solo falta ver que no existe un grupo $\mathbf{G}$ tal que $A_5 \subseteq \mathbf{G} \subseteq S_5/A_5$ con $\mathbf{G} \lhd S_5/A_5$, supongamos lo contrario, es decir, $\mathbf{G} \lhd S_5/A_5$, entonces tenemos las siguientes equivalencias,

$$\begin{aligned} \bar{a}\mathbf{G} &= \mathbf{G}\bar{a} \\ \bar{a}\mathbf{G}\bar{a}^{-1} &= \mathbf{G} \end{aligned}$$

si y solo si $aa^{-1} \in \mathbf{G}$ pero notemos que $\bar{a}\mathbf{G} \neq \mathbf{G}\bar{a}$ puesto que $\bar{a} = aA_5$ y $\forall g \in \mathbf{G}$ tenemos que $\bar{a}g \neq g\bar{a}$, así $aA_5g \neq gaA_5$, si $aA_5g = gaA_5$, entonces $(ga)^{-1}aA_5g = A_5$ si y solo si $(ga)^{-1}(ag) \in A_5$ lo cual no pasa, pues $A_5 \neq \mathbf{G}$, de esta manera el factor S_5/A_5 es simple y por tanto la serie $1 \lhd A_5 \lhd S_5$ es de composición.

b) Para V del ejemplo 2.3.1, la serie $1 \lhd V \lhd A_4$ no es de composición en A_4, pues $V/1 \cong V$ no es simple.

Proposición 2.3.1. *Un grupo simple y soluble es cíclico de orden primo.*

Demostración. Sea A un grupo simple y soluble, por ser A simple no tiene subgrupos propios y por ser soluble es abeliano. Además sabemos que un grupo será abeliano y simple si y solo si $A \cong \mathbb{Z}_p$ con p primo [Art], como los $\mathbb{Z}_p$ son cíclicos [Fra], entonces A es un grupo cíclico de orden primo. □

Proposición 2.3.2. *Si* $\mathbf{G}$ *es un grupo soluble, entonces cada subgrupo de* $\mathbf{G}$ *también es soluble.*

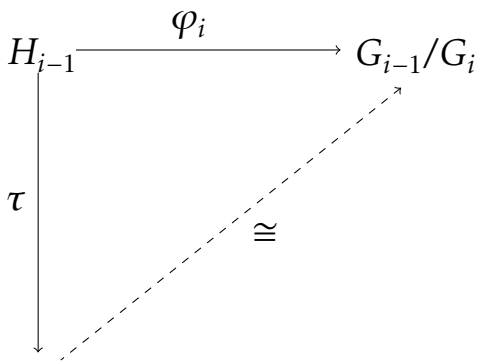
Demostración. Sea $\mathbf{H} \leq \mathbf{G}$, si $\mathbf{G}_i$ es un subgrupo de la serie de subgrupos de $\mathbf{G}$ y hacemos $\mathbf{H}_i = \mathbf{G}_i \cap \mathbf{H}$ para cada $i = 0, \cdots, n$, de esta manera tenemos que

$$\begin{aligned} \mathbf{H}_0 &= \mathbf{G}_0 \cap \mathbf{H} = \mathbf{G} \cap \mathbf{H} = \mathbf{H}, \\ \mathbf{H}_n &= \mathbf{G}_n \cap \mathbf{H} = \{e\} \cap \mathbf{H} = \{e\}. \end{aligned}$$

Ahora consideremos el homomorfismo $\varphi_i : \mathbf{H}_{i-1} \longrightarrow \mathbf{G}_{i-1}/\mathbf{G}_i$ donde $\mathbf{G}_{i-1}/\mathbf{G}_i = \{g\mathbf{G}_i \mid g \in \mathbf{G}_{i-1}\}$ y además el homomorfismo manda un elemento $h_{i-1} \in \mathbf{H}_{i-1}$ a $h_{i-1}\mathbf{G}_i \in \mathbf{G}_{i-1}/\mathbf{G}_i$. Ahora un elemento $h_{i-1} \in \mathbf{H}_{i-1}$ está en el kernel de φ_i si y solo si $\varphi_i(h_i) = \mathbf{G}_i$ si y solo si $h_{i-1}\mathbf{G}_i = \mathbf{G}_i$, lo cual solo pasa si $h_{i-1} \in \mathbf{H}_{i-1} \cap \mathbf{G}_i$ pues $h_{i-1} \in \mathbf{H}_{i-1}$, pero

$$\begin{aligned} \mathbf{H}_{i-1} \cap \mathbf{G}_i &= (\mathbf{G}_{i-1} \cap \mathbf{H}) \cap \mathbf{G}_i \\ &= (\mathbf{G}_{i-1} \cap \mathbf{G}_i) \cap \mathbf{H} \\ &= \mathbf{G}_i \cap \mathbf{H} = \mathbf{H}_i, \end{aligned}$$

por lo que $ker(\varphi_i) = \mathbf{H}_i = \mathbf{G}_i \cap \mathbf{H}$, lo cual implica que $\mathbf{H}_i \lhd \mathbf{H}_{i-1}$, en estas condiciones tenemos el siguiente diagrama



$$H_{i-1}/H_i = H_{i-1}/Ker(\varphi_i)$$

Como φ_i y τ son sobre por el primer Teorema de Isomorfismo de grupos (ver[Rot2]), tenemos que $\mathbf{H}_{i-1}/\mathbf{H}_i$ es isomorfo a $\mathbf{G}_{i-1}/\mathbf{G}_i$, por el Teorema 2.3.1 el grupo $\mathbf{G}_{i-1}/\mathbf{G}_i$ es cíclico de orden primo, entonces $\mathbf{H}_{i-1}/\mathbf{H}_i$ también es cíclico de orden primo, así $|\ \mathbf{H}_{i-1} : \mathbf{H}_i\ |$ es primo, de esta forma hay una y solo una inclusión propia de la cadena, con lo cual

$$\{e\} = \mathbf{H}_n \subseteq \cdots \subseteq \mathbf{H}_i \subseteq \mathbf{H}_0 = \mathbf{H},$$

así $\mathbf{H}$ es soluble, y como $\mathbf{H}$ fue arbitrario entonces todo subgrupo de $\mathbf{G}$ será soluble. □

Proposición 2.3.3. *Todo grupo* **G** *finito abeliano es soluble.*

Demostración. Haremos inducción sobre el orden de **G**.
Sea $|\mathbf{G}| = n$ el orden del grupo, y sabemos que si **G** es finito el orden de **G** coincide con su cardinalidad [Fra].
Para $n = 1$, tenemos que $\mathbf{G} = \{e\}$ y $|\mathbf{G}| = 1$, de esta manera tenemos la serie

$$1 = \mathbf{G}_0 \subseteq \mathbf{G}_1 = \mathbf{G},$$

donde $1 \lhd \mathbf{G}$, así el único factor de esta serie está dado por $\mathbf{G}_1/\mathbf{G}_0 = \mathbf{G}/1 = \mathbf{G}$, como **G** es abeliano por hipótesis, el factor $\mathbf{G}_1/\mathbf{G}_0$ necesariamente es abeliano, por lo tanto **G** es soluble.
Supongamos que **G** es un grupo abeliano de orden $n > 1$ y supongamos que para $|\mathbf{G}| < n$ se tiene que **G** es soluble, es decir **G** tiene la serie normal

$$1 = \mathbf{G}_0 \subseteq \mathbf{G}_1 \subseteq \cdots \subseteq \mathbf{G}_r = \mathbf{G},$$

donde cada $\mathbf{G}_{i+1}/\mathbf{G}_i$ factor es abeliano con $\mathbf{G}_i \lhd \mathbf{G}_{i+1}$.
Ahora veamos que el resultado es cierto para $|\mathbf{G}| \geq n$.
Sea p primo divisor de $|\mathbf{G}|$.
Si $p = |\mathbf{G}|$, entonces **G** es cíclico de orden p [Art] y de esta manera es soluble.
Si $p < |\mathbf{G}|$, entonces podemos encontrar $g \in \mathbf{G}$ de orden p (Teorema de Cauchy [Fra]). Ahora sea $\mathbf{H} = \langle g \rangle$ el subgrupo generado por g, entonces **H** es normal (Teorema de Lagrange [Fra]) pues **G** es abeliano y $p = |\mathbf{H}|$, por lo tanto el orden de **H** y **G**/**H** necesariamente es mas pequeño que $|\mathbf{G}| = n$, así **H** y **G**/**H** por hipótesis de inducción son grupos solubles, por Proposición 2.3.2 el grupo **G** es soluble. □

Proposición 2.3.4. *S_n es soluble para $n \leq 4$, pero no es soluble para $n \geq 5$.*

Demostración. Si $m < n$, entonces S_m es isomorfo a un subgrupo de S_n, como cada subgrupo de un grupo soluble es soluble por la Proposición 2.3.2, tenemos que demostrar que S_4 es soluble y S_5 no es soluble.
Ahora la serie normal de S_4 dada por $1 \lhd V \lhd A_4 \lhd S_4$ tiene como factores a grupos abelianos y por definición 2.3.2 concluimos que S_4 es soluble y así S_n es soluble para $n \leq 4$.
Si S_5 fuera soluble, entonces A_5 sería soluble, y por el ejemplo 2.3.1 sabemos que no lo es, pues tenemos que el factor $A_5/1 \cong A_5$ no es abeliano y $1 \lhd A_5 \lhd S_5$ de esta manera S_5 no es soluble, por la Proposición 2.3.2 S_n no es soluble para $n \geq 5$, pues $S_5 \subseteq S_n$. □

Capítulo 3

Solubilidad por radicales

No te preocupes por tus dificultades en matemáticas. Te puedo asegurar que las mías son aún mayores.

Albert Einstein.

En este capítulo queremos conocer algunas características esenciales de cuándo un polinomio es soluble por radicales, relacionaremos esta idea con la extensión de campo y algunos resultados de este hecho, para posteriormente hacer el análisis con los polinomios ciclotómicos. Tomaremos como referencia el libro [Cox].

3.1. Extensión radical

Para formalizar la idea de la solubilidad por radicales, iniciamos desde el punto de vista de las extensiones de campo. Informalmente obtenemos una extensión radical si le agregamos las n-ésimas raíces, para distintos n, por ejemplo, la siguiente expresión radical

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}}+\sqrt[4]{1+\sqrt[3]{4}}. \tag{3.1}$$

Para encontrar una extensión de $\mathbb{Q}$ que contenga a la expresión (3.1) como elemento, servirá unir sus elementos.

$$\alpha=\sqrt[3]{11},\ \beta=\sqrt{3},\ \gamma=\sqrt[5]{\frac{7+\beta}{2}},\ \delta=\sqrt[3]{4},\ \eta=\sqrt[4]{1+\delta}.$$

Por ejemplo la expresión (3.1) está contenida en una extensión radical de la forma

$$\mathbb{Q}(\alpha,\ \beta,\ \gamma,\ \delta,\ \eta)$$

de $\mathbb{Q}$, donde $\alpha^3=11,\ \beta^2=3,\ \gamma^5=\dfrac{7+\beta}{2},\ \delta^3=4,\ \eta^4=1+\delta$. De esta manera cualquier expresión similar a (3.1), estará contenida en una extensión radical. Así un polinomio debe considerarse soluble por radicales, siempre que todos sus ceros sean expresiones radicales sobre el campo. Con estas ideas definimos lo que será una extensión radical.

Definición 3.1.1. *Sea* $\mathbf{K}$ *un campo con Char*$(\mathbf{K}) = 0$. *La extensión* $\mathbf{E} : \mathbf{K}$ *se dice que es una* ***extensión radical*** *si* $\mathbf{E} = \mathbf{K}(\alpha)$ *donde* α *es raíz de* $x^n - a \in \mathbf{K}[x]$ $n \in \mathbb{Z}^+$, *es decir,* $\mathbf{E} = \mathbf{K}(\alpha)$ *con* $\alpha^n = a$, *o si se quiere* $\mathbf{E} = \mathbf{K}\left(\sqrt[n]{a}\right)$.

Ejemplo 3.1.1. *Para la extensión de campo* $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}$, *hacemos* $\gamma_1 = \sqrt{2}$ *y* $\gamma_2 = \sqrt{2+\sqrt{2}}$ *como*

$$\mathbb{Q} \subset \mathbb{Q}(\gamma_1) \subset \mathbb{Q}(\gamma_1)(\gamma_2),$$

entonces tenemos las extensiones $\mathbb{Q}(\gamma_1) : \mathbb{Q}$ *y* $\mathbb{Q}(\gamma_1)(\gamma_2) : \mathbb{Q}(\gamma_1)$ *por tanto*

$$\mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q},$$

donde $\gamma_1^2 = \sqrt{2}^2 = 2 \in \mathbb{Q}$ *y* $\gamma_2^2 = \sqrt{2+\sqrt{2}}^2 = 2+\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$. *Como* $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$, *y*

$$\mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{2+\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right),$$

$\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}$ *es una extensión radical.*

Con esta definición y el ejemplo concretamos el significado de que los elementos de una extensión radical se puedan expresar como radicales.
Nótese que $x^n - a$ es separable (independientemente de que sea irreducible) pues si α es una raíz en $\mathbf{K} \subseteq \mathbb{C}$ las restantes raíces son $\xi\alpha$, $\xi^1\alpha, \cdots, \xi^{n-1}\alpha$, donde $\xi \in \mathbb{C}$ es una raíz n-ésima primitiva de 1.

Definición 3.1.2. *Sea* $\mathbf{K}$ *un campo con Char(*$\mathbf{K}$*)*$= 0$. *Una* ***Torre Radical*** *para una extensión* $\mathbf{E} : \mathbf{K}$ *es una torre de campos*

$$\mathbf{K} = \mathbf{K}_0 \subseteq \mathbf{K}_1 \subseteq \cdots \subseteq \mathbf{K}_{i-1} \subseteq \mathbf{K}_i \subseteq \cdots \subseteq \mathbf{K}_r$$

donde, para cada $i = 1, \cdots, r$, *la extensión* $\mathbf{K}_i : \mathbf{K}_{i-1}$ *es radical, es decir,* $\mathbf{K}_i = \mathbf{K}_{i-1}(\alpha_i)$ *con* $\alpha_i \in \mathbf{K}_i$ *tal que* $a_i^{n_i} = \alpha_i \in \mathbf{K}_{i-1}$ *para ciertos enteros positivos* n_i, *además* $\mathbf{E} = \mathbf{K}(\alpha_1, \alpha_2, \cdots, \alpha_r)$.

Teorema 3.1.1. *Si* $\mathbf{E} : \mathbf{F}$ *y* $\mathbf{F} : \mathbf{K}$ *tienen torres radicales,* $\mathbf{E} : \mathbf{K}$ *tiene una torre radical.*

Demostración. Notemos que al encadenar las dos torres radicales existentes por hipótesis, esto nos proporciona una torre radical para la extensión $\mathbf{E} : \mathbf{K}$

$$\mathbf{K} = \mathbf{K}_0 \subseteq \mathbf{K}_1 \subseteq \cdots \subseteq \mathbf{K}_{i-1} \subseteq \mathbf{K}_i \subseteq \cdots \subseteq \mathbf{K}_r = \mathbf{F} = \mathbf{F}_0 \subseteq \mathbf{F}_1 \subseteq \cdots \subseteq \mathbf{F}_{j-1} \subseteq \mathbf{F}_j \subseteq \cdots \subseteq \mathbf{F}_s = \mathbf{E}.$$

□

Teorema 3.1.2. *Una extensión finita y separable* $\mathbf{E} : \mathbf{K}$ *es soluble por radicales si y solo si* $\mathbf{E} : \mathbf{K}$ *es soluble.*

Para la demostración véase [Rom].
Con este teorema garantizamos que la solubilidad por radicales y la solubildad de una extensión están relacionadas.

3.2. Solubilidad por radicales de un polinomio

Ahora ya sabemos como determinar si un grupo o una extensión es soluble por radicales, pero como podemos relacionar estos resultados con los de un polinomio, el siguiente teorema es justo lo que hace.

Teorema 3.2.1. *(**Gran teorema de Galois.**) Sea* $\mathbf{K}$ *un campo con Char(*$\mathbf{K}$*)*$= 0$ *y sea* $f \in \mathbf{K}[x]$ *no constante. Entonces la ecuación* $f(x) = 0$ *es soluble por radicales sobre* $\mathbf{K}$ *si y sólo si, el grupo de Galois Gal*$(f : \mathbf{K})$ *es un grupo soluble.*

Para la demostración véase [Mor].
Ya sabemos que un polinomio $f(x)$ no constante será soluble por radicales si su grupo de Galois asociado es soluble por radicales, es decir si Gal$(f : \mathbf{K})$ contiene una serie normal de factores abelianos, una forma análoga de poder conocer si un polinomio es soluble por radicales es la siguiente definición. Para ello tomaremos como referencia el libro [Mor] Capítulo 3, Sección 16.

Definición 3.2.1. *Sea* $\mathbf{K}$ *un campo con Char(*$\mathbf{K}$*)*$= 0$*. Un polinomio* $f(x) \in \mathbf{K}[x]$ *se dice que es* ***soluble por radicales*** *sobre* $\mathbf{K}$ *(o que la ecuación* $f(x) = 0$ *es soluble por radicales sobre* $\mathbf{K}$*) si existe* $\mathbf{K}_r : \mathbf{K}$ *una extensión radical tal que*

$$\mathbf{K} = \mathbf{K}_0 \subseteq \mathbf{K}_1 \subseteq \cdots \subseteq \mathbf{K}_{i-1} \subseteq \mathbf{K}_i \subseteq \cdots \subseteq \mathbf{K}_r,$$

y f *se descompone completamente en* $\mathbf{K}_r$ *(es decir, un campo de descomposición de* f *está contenido en* $\mathbf{K}_r$*).*

Para entender mejor la definición, veamos un ejemplo de un polinomio.

Ejemplo 3.2.1. *Sea el polinomio* $p(x) = x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 3 \in \mathbb{Q}[x]$*, y* $\mathbf{K} = \mathbb{Q}$*. Afirmamos que es soluble por radicales, pues podemos escribir*

$$\begin{aligned} p(x) &= x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 3 \\ &= x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 - 2 \\ &= (x-1)^5 - 2 \\ &= q(x) - 2, \end{aligned}$$

Notemos primeramente que $x^5 - 1 = 0$*, resuelve la raíz quinta de la unidad y las raíces están ubicadas en el círculo unitario del plano complejo, ahora para* $x^5 - 2 = 0$ *las raíces son las mismas que para* $x^5 - 1 = 0$ *multiplicadas por* $\sqrt[5]{2}$*, así para* $(x-1)^5 - 2 = 0$ *sus raíces están*

ubicadas en el círculo de radio 2 *con centro* $(0, 1)$ *del plano complejo. Por tanto todas las raíces para el polinomio* $p(x) = (x-1)^5 - 2$ *son de la forma* $1 + \xi^k\left(\sqrt[5]{2}\right)$ *con* $\xi = e^{2\pi i/5}$, $0 \leq k < 5$, *donde el campo de descomposición es* $\mathbf{E}_p = \mathbb{Q}\left(\xi, \sqrt[5]{2}\right)$, *además la extensión* $\mathbf{E}_p : \mathbb{Q}$ *es radical, pues* ξ *es una raíz quinta de la unidad. Más explícitamente*

$$\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq \mathbb{Q}\left(\xi, \sqrt[5]{2}\right) = \mathbf{E}_p,$$

con $\xi^5 = 1 \in \mathbb{Q}$ *y* $\left(\sqrt[5]{2}\right) \in \mathbb{Q}\left(\xi, \sqrt[5]{2}\right) = \mathbf{K}_r$.

Este ejemplo también es una excepción a la no solubilidad de los polinomios de grado cinco, la cual se verá mas delante.
En las condiciones del Teorema 3.2.1 tenemos la siguiente proposición, de hecho con el Teorema de Galois a nuestra disposición, podemos deducir que es posible resolver por radicales todas las ecuaciones hasta grado cuatro, y como la demostración es constructiva en principio podríamos elaborar una fórmula explícita para resolverla.

Proposición 3.2.1. *Sea* $\mathbf{K}$ *un campo y* $f(x) \in \mathbf{K}[x]$ *con* $Char(\mathbf{K}) = 0$. *Si* $grd[f(x)] \leq 4$ *entonces* f *es soluble por radicales y consecuentemente la ecuación* $f(x) = 0$ *es soluble por radicales sobre* $\mathbf{K}$.

Demostración. El polinomio f será soluble por Teorema 3.2.1 si $\mathrm{Gal}(f : \mathbf{K})$ es un grupo soluble. Sabemos que el grupo de Galois permuta las raíces, con lo cual es isomorfo a un subgrupo de $S_m \subseteq S_4$ donde m es el número de raíces distintas, por tanto, basta probar que S_4 es soluble, lo cual se garantiza por las proposiciones 2.3.2 y 2.3.4. □

Proposición 3.2.2. *Sea* $\mathbf{K}$ *un campo con* $Char(\mathbf{K}) = 0$, *un polinomio* $f(x)$ *con grupo de Galois abeliano es soluble por radicales.*

Demostración. Sabemos que el polinomio $f(x)$ será soluble por radicales si su grupo de Galois asociado es soluble. Por hipótesis tenemos que el grupo de Galois es abeliano, y como todo grupo finito abeliano es soluble por la Proposición 2.3.3, tenemos que $f(x)$ es soluble por radicales. □

3.2.1. Solubilidad de polinomios de grado 2, 3 y 4.

Para los polinomios de grado uno y dos es fácil demostrar que son solubles por radicales, debido a la existencia de procedimientos para conocer sus raíces. Existen fórmulas más complejas para polinomios de grado tres y cuatro los cuales por la Proposición 3.2.1 son solubles por radicales. Por otro lado, los polinomios de grado cinco no son solubles por radicales, y por lo tanto no existen fórmulas generales, sin embargo hay casos específicos de polinomios de grado cinco que son solubles, es decir, polinomios reducibles sobre números racionales (como en el ejemplo 3.2.1) y polinomios ciclotómicos. Analizaremos los polinomios de grado 2,3 y 4, para los últimos nos basaremos en el libro [Cox] Capítulo 1,

Sección 1.1 y en el libro [Ste] Capítulo 2, Sección 5.

Polinomios de grado 2

La solución de los polinomios de grado dos lo podemos hacer mediante la fórmula general.

Sea $p(x) \in \mathbf{K}[x]$ tal que $\text{grd}[p(x)] = 2$, este polinomio tiene la forma

$$p(x) = ax^2 + bx + c.$$

Sabemos que podemos resolver la ecuación $ax^2 + bx + c = 0$ calculando sus dos raíces con las siguientes ecuaciones. Sea $\triangle = b^2 - 4ac$ el discriminate de $p(x)$.

$$x = \begin{cases} \dfrac{-b \pm \sqrt{\triangle}}{2a} & \text{si } \triangle \geq 0 \\ \dfrac{-b \pm i\sqrt{\triangle}}{2a} & \text{si } \triangle < 0 \end{cases}$$

Notemos que los posibles valores que puede tomar x están expresados en términos de radicales.

Polinomios de grado 3

La solución de los polinomios cúbicos se puede hacer utilizando el método de Cardano, en donde se elimina de la ecuación normal el término x^2 y se obtiene la ecuación reducida.

Sea $p(x) \in \mathbf{K}[x]$ tal que $\text{grd}[p(x)] = 3$, este polinomio tiene la forma

$$p(x) = Ax^3 + Bx^2 + Cx + D = 0.$$

Como es más fácil trabajar con un polinomio mónico, podemos dividir la ecuación completa para obtener

$$x^3 + ax^2 + bx + c = 0, \tag{3.2}$$

hacemos $x = y - \dfrac{a}{3}$ y obtenemos

$$x^3 + ax^2 + bx + c = y^3 + y\left(\frac{a^2}{3} - \frac{2a^2}{3} + b\right) + \left(-\frac{a^3}{27} + \frac{a^3}{9} - \frac{ba}{3} + c\right),$$

con $p = \dfrac{a^2}{3} - \dfrac{2a^2}{3} + b$ y $q = -\dfrac{a^3}{27} + \dfrac{a^3}{9} - \dfrac{ba}{3} + c$ hacemos,

$$y^3 + py + q = 0. \tag{3.3}$$

Así podemos resolver la ecuación (3.3) para y y de esta manera las soluciones para la ecuación (3.2) están dadas por,

$$x = -\frac{a}{3} + \frac{\xi_i a}{3}\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\right).$$

Con $i = \{1, 2, 3\}$ y donde ξ_i es una raíz 3-ésima de la unidad. Notemos que los posibles valores que puede tomar x están expresados en términos de radicales.
Si consideraremos el grupo de Galois de la ecuación cúbica reducida e irreducible, el grupo de Galois del campo de descomposición de está ecuación cúbica es S_3.

Teorema 3.2.2. *Si* $\mathbf{E} : \mathbf{K}$ *es una extensión de Galois, entonces* $|\, Gal\,(\mathbf{E} : \mathbf{K})\,| = |\,\mathbf{E} : \mathbf{K}\,|$.

Para la demostración véase [Art].

Teorema 3.2.3. *Si* $\mathbf{E} : \mathbf{K}$ *es una extensión,* $\mathbf{F}$ *es un subcampo intermedio tal que* $\mathbf{K} \subseteq \mathbf{F} \subseteq \mathbf{E}$ *y además* $: \mathbf{F} : \mathbf{K}$, $\mathbf{E} : \mathbf{F}$ *son extensiones, entonces* $|\,\mathbf{E} : \mathbf{K}\,| = |\,\mathbf{E} : \mathbf{F}\,||\,\mathbf{F} : \mathbf{K}\,|$.

Para la demostración véase [Ste].

Proposición 3.2.3. *El grupo de Galois de cualquier polinomio cúbico es isomorfo a cualquiera de los dos grupos* S_3 *o* A_3.

Demostración. Sea $f(x) = x^3 + px + q$ un polinomio en su forma reducida e irreducible en $\mathbf{K}[x]$ donde Char($\mathbf{K}$)= 0, con raíces $y_1,\ y_2,\ y_3$. Como

$$f(x) = x^3 + px + q = (x - y_1)(x - y_2)(x - y_3), \tag{3.4}$$

tenemos las siguientes relaciones

$$\begin{aligned} y_1 + y_2 + y_3 &= 0, \\ y_1y_2 + y_3y_2 + y_3y_1 &= p, \\ y_1y_2y_3 &= -q, \end{aligned}$$

así de la primera relación tenemos que la raíz y_3 está en el campo generado por las raíces y_1, y_2, de esta manera tenemos la siguiente torre de campos

$$\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{E}, \tag{3.5}$$

donde $\mathbf{L} = \mathbf{K}(y_1)$ y $\mathbf{E} = \mathbf{K}(y_1,\ y_2) = \mathbf{K}(y_1,\ y_2,\ y_3)$, pues si dos raíces están en el campo, la tercera automáticamente estará en el campo.
Buscamos saber quién es Gal($\mathbf{E} : \mathbf{K}$).
Primeramente de la torre (3.5) debemos saber si $\mathbf{L} = \mathbf{E}$ o $\mathbf{L} < \mathbf{E}$, es decir si hay un subcampo entre $\mathbf{K}$ y $\mathbf{E}$, para analizar esta dicotomía tomamos el polinomio $f(x)$ el cual es irreducible en $\mathbf{K}[x]$ y además se descompone en factores lineales en $\mathbf{E}$. Sabemos que en $\mathbf{L}$, $f(x)$ tiene como factor a $(x - y_1)$, pues $f(y_1) = 0$, entonces $f(x) = (x - y_1)h(x)$ con $h(x)$ un polinomio de grado dos con coeficientes en $\mathbf{L}$. De (3.4) tenemos que $h(x) = (x - y_2)(x - y_3)$ y $h(x) \in \mathbf{E}$, entonces $\mathbf{L}$ es subcampo de $\mathbf{E}$ si y solo si $h(x)$ es irreducible en $\mathbf{L}$, el grado de

$$\mathbf{L}(y_2) = \mathbf{K}(y_1)(y_2) = \mathbf{K}(y_1,\ y_2) = \mathbf{E} = \mathbf{K}(y_1,\ y_2,\ y_3)$$

sobre **L** es dos, es decir, $|\,\mathbf{L}(y_2):\mathbf{L}\,|=2$, como $f(x)$ es irreducible en **K**, entonces $|\,\mathbf{L}:\mathbf{K}\,|=3$, ahora por el Teorema 3.2.3 tenemos que

$$|\,\mathbf{E}:\mathbf{K}\,|=|\,\mathbf{E}:\mathbf{L}\,||\,\mathbf{L}:\mathbf{K}\,|,$$

de esta manera tenemos lo siguiente,

$$|\,\mathbf{E}:\mathbf{K}\,|=\begin{cases}3 & \text{si } \mathbf{L}=\mathbf{E}\\ 6 & \text{si } \mathbf{L}<\mathbf{E}\end{cases}$$

Ahora de acuerdo al Teorema 3.2.2 el orden de un grupo de Galois **G** =Gal(**E** : **K**) es el grado de la extensión **E** : **K**, como $\mathbf{G}<S_3$ y S_3 tiene orden 6, entonces si

$$|\,\mathbf{E}:\mathbf{K}\,|=6$$

se tiene que $\mathrm{Gal}(\mathbf{E}:\mathbf{K})\cong S_3$ y si

$$|\,\mathbf{E}:\mathbf{K}\,|=3$$

se tiene que $\mathrm{Gal}(\mathbf{E}:\mathbf{K})\cong A_3$. □

Polinomios de grado 4

La solución de polinomios de grado cuatro se puede hacer utilizando el método de Ferrari, que transforma un polinomio de grado cuatro en una ecuacion reducida que no tiene el término x^3. Sea $p(x)\in\mathbf{K}$ tal que $\mathrm{grd}[p(x)]=4$, este polinomio tiene la forma

$$p(x)=Ax^4+Bx^3+Cx^2+Dx+E.$$

Análogo al polinomio de grado tres, hacemos mónico al polinomio, dividiendo por el coeficiente principal y reescribiendo tenemos

$$x^4+ax^3+bx^2+cx+d=0, \tag{3.6}$$

y si hacemos $x=y-\dfrac{a}{4}$ obtenemos

$$y^4+py^2+qy+r=0, \tag{3.7}$$

sumando $2zy^2+z^2$ a la ecuación (3.7) obtenemos

$$y^4+2zy^2+z^2=(2z-p)\,y^2-qy+\left(z^2-r\right) \tag{3.8}$$

y ahora hacemos el discriminate del lado derecho igual a 0, es decir

$$q^2-4\left(z^2-r\right)(2z-p)=0,$$

de donde obtenemos

$$8z^3 - 4pz^2 - 8rz + 4rp - q^2 = 0. \tag{3.9}$$

De esta manera para resolver la ecuación (3.6) tenemos que resolver la ecuación (3.9) y así una raíz de (3.9) se ve de la siguiente manera,

$$x = \frac{1}{2}\sqrt{2z_i - p} \pm \sqrt{\frac{1}{2}z_i - \frac{1}{4}p \pm \sqrt{z_i^2 - r}} - \frac{a}{4}$$

siendo z_i las soluciones de la ecuación (3.6), con $i = 1,\ 2,\ 3,\ 4$.
Hemos mostrado no solo que los polinomios de grado menor o igual que cuatro son solubles por radicales, si no que además podemos dar explícitamente cómo se ven sus raíces.
De la definición 3.2.1 tenemos que si $\mathbf{K}$ es un campo, decimos que $f(x) \in \mathbf{K}[x]$ es soluble por radicales si y solo si hay una extensión radical $\mathbf{E} : \mathbf{K}$ tal que $f(x)$ se descompone sobre $\mathbf{E}$. No es evidente, que esto implica que el campo de descomposición de f sobre $\mathbf{K}$ sea una extensión radical de $\mathbf{K}$.

Para mostrar esta idea tenemos el siguiente ejemplo, el cual exhibirá un polinomio soluble por radicales cuyo campo de descomposición no es una extensión radical.

Ejemplo 3.2.2. *Sea* $\mathbf{K} = \mathbb{Q}$ *y* $f(x) = x^3 - 3x + 1$.
Veamos que este polinomio es soluble por radicales, pero no podemos encontrar una extensión radical $\mathbf{E} : \mathbf{K}$ *tal que* $f(x)$ *se descompone sobre* $\mathbf{E}$.
Para ver que el polinomio cúbico $f(x)$ *con coeficientes en* $\mathbb{Q}$, *es soluble por radicales, sea* $\mathbf{E}$ *el campo de descomposición de* $f(x)$ *sobre* $\mathbb{Q}$, *como* f *es irreducible en* $\mathbb{Q}$ *pues* $f(x)$ *no tiene raíces en* $\mathbb{Q}$ *y el* $grd(f(x)) = 3$. *Ahora determinemos el grado de la extensión* $\mathbf{E} : \mathbb{Q}$, *sabemos por la Proposición 3.2.3 que si* $\mathbf{G} = Gal(f : \mathbb{Q})$ *es un grupo de Galois de* $f(x)$ *sobre* $\mathbb{Q}$, $\mathbf{G} \cong A_3$, *como* $\mathbb{Q}$ *es perfecto (véase definición 2.1.11 y su comentario) pues su característica es* 0, *tenemos que* $|\ \mathbf{E} : \mathbb{Q}\ | = |\ \mathbf{G}\ | = 3$, *así* $Gal(\mathbf{E} : \mathbb{Q}) \cong A_3$, *de esta manera por la Proposición 2.3.4* $Gal(\mathbf{E} : \mathbb{Q})$ *es soluble por radicales pues* $A_3 < S_3$ *y por el gran Teorema de Galois 3.2.1* $f(x)$ *es soluble por radicales.*
Para ver que $\mathbf{E}$ *no es una extensión radical de* $\mathbb{Q}$, *supongamos lo contrario. Si* $\mathbf{E}$ *es una extensión radical de* $\mathbb{Q}$, *entonces hay una cadena de campos*

$$\mathbb{Q} \subseteq \mathbf{K}_0 \subseteq \mathbf{K}_1 \subseteq \cdots \subseteq \mathbf{K}_r = \mathbf{E},$$

con $\mathbf{K}_i \subseteq \mathbf{K}_{i-1}(\alpha_i)$ *y* $\alpha_i^n \in \mathbf{K}_{i-1}$ *para alguna n, como* $|\ \mathbf{E} : \mathbb{Q}\ | = 3$ *y al ser tres un número primo, hay una y solo una inclusión propia en la cadena, es decir* $\mathbf{E} = \mathbb{Q}(b)$, *tal que* $b^n = u \in \mathbb{Q}$ *para algún n, sea* $p(x)$ *el polinomio mínimo para el cual b es raíz, donde* $p(x)$ *se factoriza en términos lineales en* $\mathbf{E}$, *por ser* $\mathbf{E} : \mathbb{Q}$ *una extensión normal.*
Sea $b' \in \mathbf{E}$ *otra raíz de* $p(x)$, *entonces* $b^n = (b')^n = u$, *así* $1 = \left(\frac{b'}{b}\right)^n$, *es decir* $\frac{b'}{b}$ *es una raíz n-ésima de la unidad. Supomgamos que* $r = \frac{b'}{b}$ *es una raíz m-ésima primitiva de la unidad, tal*

que $m \mid n$, *entonces* $\mathbb{Q}(r) = \mathbb{Q}\left(\frac{b'}{b}\right) \subset \mathbf{E}$, *con lo que*

$$|\,\mathbf{E} : \mathbb{Q}\,| = |\,\mathbf{E} : \mathbb{Q}(r)\,|\,|\,\mathbb{Q}(r) : \mathbb{Q}\,|\,. \tag{3.10}$$

Como $|\,\mathbb{Q}(r) : \mathbb{Q}\,| = \varphi(m)$ *(ver [Ste] y sección 1.2), por (3.10) y como* $|\,\mathbf{E} : \mathbb{Q}\,| = 3$ *tenemos que* $\varphi(m) = 1$ *o* 3.
Pero tenemos que, para todo entero positivo m, $\varphi(m) \neq 3$. *En efecto,* $\varphi(1) = 1$ *y para*

$$\beta \geq 1,\ \varphi\left(2^{\beta}\right) = 2^{\beta-1}(2-1) = 2^{\beta-1} \neq 3,$$

así que podemos suponer que m *no es una potencia de* 2, *digamos que* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ *con* $p_1, p_2, \cdots, p_s$ *primos distintos y* $s, \alpha_1, \alpha_2, \cdots, \alpha_s$ *enteros positivos. Entonces*

$$\varphi(m) = \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)\cdots\varphi\left(p_s^{\alpha_s}\right).$$

Sea p *un primo impar que divida a* m. *Así, si* $\varphi(m) = 3$, $\varphi(p^{\alpha})$ *dividiría a* 3, *para algún entero positivo* α. *Ahora,* $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$. *Pero,* $p-1$ *siendo par, no divide a* 3. *Así,* $|\,\mathbb{Q}(r) : \mathbb{Q}\,| = \varphi(m) = 1$, *y entonces* $r \in \mathbb{Q}$. *Ahora, las únicas raíces de la unidad que son racionales son* ± 1, *por lo que* $r = \pm 1$. *Tenemos entonces que* $b' = b$.
Con lo cual mostramos que $p(x)$ *tiene almenos dos raíces entonces,*

$$1 = |\,\mathbb{Q}(b) : \mathbb{Q}\,| \leq 2 < |\,\mathbf{E} : \mathbb{Q}\,| = 3,$$

lo cual contradice el hecho de que $\mathbf{E} = \mathbb{Q}(b)$, *por lo cual* $\mathbf{E}$ *no es una extensión radical de* $\mathbb{Q}$.

Con el ejemplo 3.2.2 tenemos la idea de que existen polinomios en $\mathbb{Q}$ solubles por radicales, pero que no tienen una extensión radical, lo cual es un teorema que demostraremos mas adelante, para el cual necesitamos el siguente teorema.

Teorema 3.2.4. *Sea* $f(x) \in \mathbb{Q}[x]$ *un polinomio cúbico irreducible con raíces* u, v, w. *Sea* $\mathbf{E} = \mathbb{Q}(u, v, w)$ *un campo de descomposición de* $f(x)$, *y sea* $\mathbb{Q} = \mathbf{K}_0 \subseteq \mathbf{K}_1 \subseteq \cdots \subseteq \mathbf{K}_t$ *una torre radical con* $\mathbf{E} \subseteq \mathbf{K}_t$. *Entonces* $\mathbf{K}_t$ *no es subcampo de* $\mathbb{R}$.

Para la demostración véase [Cox].

Para concluir la idea del ejemplo 3.2.2 tenemos el siguiente teorema.

Teorema 3.2.5. *Existen polinomios con coeficientes racionales solubles por radicales tales que su campo de descomposición sobre* $\mathbb{Q}$ *no es una extensión radical.*

Demostración. Considérese cualquier polinomio cúbico cuyo discriminante sea positivo. Como sus tres raíces son reales, su campo de descomposición es subcampo de $\mathbb{R}$, así que si $\mathbf{E} : \mathbb{Q}$ fuera una extensión radical, se contradice el Teorema 3.2.4. □

Capítulo 4

Polinomio ciclotómico y la solubilidad por radicales

Las matemáticas consisten en probar lo más obvio de la manera menos obvia.

George Pólya.

Ahora que ya sabemos en que casos un polinomio es soluble por radicales y hemos conocido la relación con las extensiones de campo, queremos relacionar toda esta teoría con los polinomios ciclotómicos. En esta sección nos basaremos en el libro [Cox].

4.1. Polinomio ciclotómico

Consideremos el polinomio $x^n - 1$ con $n \in \mathbb{N}$, gracias a las propiedades de los números complejos, sabemos que las raíces de estos polinomios son los que forman el conjunto:

$$\mathbb{U}_n = \left\{\xi_k = e^{2\pi ki/n} \mid k = 1, \cdots, n\right\} = \{w \in \mathbb{C} \mid w^n = 1\}.$$

Notemos que el conjunto $\mathbb{U}_n$ junto con el producto usual forman un grupo (ejemplo 1.1.1), y además a los elementos de $\mathbb{U}_n$ se les llama raíces n-ésimas de la unidad. En general, si estamos en un campo $\mathbf{K}$ y $\xi \in \mathbf{K}$ es una raíz del polinomio $p(x) = x^n - 1$, entonces ξ es una raíz n-ésima de la unidad si $\xi^n = 1$, y es primitiva n-ésima si además n es el entero positivo más pequeño para el cual ξ elevado a la n es 1.
Observemos que si $Char(\mathbf{K}) = s$, entonces s no divide a n, pues de lo contrario tendríamos $n = sq$ para algún $q \in \mathbb{N}$, y por tanto, por ser s la característica, $x^s = 1$ para todo $x \in \mathbf{K}$, entonces, $x^n = (x^s)^q = 1$ para todo $x \in \mathbf{K}$, de modo que todos los elementos del campo $\mathbf{K}$ serían raíces n-ésimas de la unidad.

Definición 4.1.1. *Un polinomio se denomina* ***ciclotómico*** *de orden n sobre un campo* $\mathbf{K}$ *cuando la característica de* $\mathbf{K}$ *no divide a n y además es mónico cuyas raíces son todas las raíces*

primitivas de orden n de la unidad, $\xi_k \in \mathbb{U}_n$ por lo que podemos escribir,

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \xi_k).$$

Como $\xi \in \mathbb{U}_n$ recorre las n-ésimas raíces primitivas de la unidad, el grado de dicho polinomio coincide con el orden de $\mathbb{U}_n$, es decir, con el total de raíces n-ésimas primitivas de la unidad.
La definición 4.1.1 se aclara en la siguiente parte, en la cual se expone de manera más precisa cómo podemos calcular a los distintos Φ_n.

Definición 4.1.2. *Sean* **K** *un campo, n un entero positivo y $x^n - 1$ el polinomio ciclotómico, también sea ξ una raíz n-ésima de la unidad. Llamamos n-**ésima extensión ciclotómica** de* **K** *a la extensión* $\mathbf{K}(\xi) : \mathbf{K}$

Definición 4.1.3. *Decimos que un campo* **E**, *es un **campo de descomposición ciclotómico** de orden n sobre* **K**, *si* **E** *es un campo de descomposición de $x^n - 1$ sobre* **K**.

Notemos que el campo de descomposición ciclotómico de orden n, sobre un campo **K**, cumple que su característica no divide a n, si eso ocurriera, entonces cualquier elemento de **K** sería solución de la ecuación ciclotómica de orden n.
Podemos concluir que si la característica del campo **K** es 0 para el polinomio $f \in \mathbf{K}[x]$ tal que el grado de f es n, este es irreducible, pues cada raíz de este polinomio será simple, de esta manera la extensión algebraica con estas características, será separable, en consecuencia tendríamos un polinomio separable si la característica del campo es 0 o p donde $p \nmid n$ (veasé [Hun]).

4.1.1. Cálculo de polinomios ciclotómicos

Analizaremos algunas propiedades de los polinomios ciclotómicos y cómo calcularlos de una manera más fácil. Por simplicidad de los cálculos trabajaremos en $\mathbb{C}$.

Lema 4.1.1. $grd\,[\Phi_n(x)] = \varphi(n)$

Demostración. Como el grado de $\Phi_n(x)$ es el número de n-ésimas raíces primitivas de la unidad. Sea ξ una raíz n-ésima de la unidad, entonces ξ^i con $1 \leq i \leq n$ es otra raíz primitiva, si y solo si $(i,n) = 1$, por lo tanto el número de raíces primitivas es $\varphi(n)$. □

Notemos que apartir del lema 4.1.1 deducimos la expresión de Φ_n como el n-ésimo polinomio ciclotómico para cualquier entero positivo n, como el polinomio mónico cuyas raíces son las n-ésimas raíces primitivas de la unidad

$$\Phi_n(x) = \prod_{k=1}^{\varphi(n)} (x - w_k)$$

con w_k raíces primitivas de la unidad.

Lema 4.1.2. $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Demostración. Las raíces del polinomio ciclotómico $x^n - 1$ son las raíces n-ésimas de la unidad, ahora si ξ es una raíz primitiva d-ésimas de la unidad es una raíz de Φ_d pero $d \mid n$ entonces existe $t \in \mathbb{N}$ tal que $n = dt$ y así, $\xi^n = \xi^{dt} = (\xi^d)^t = 1$ y es raíz de polinomio $x^n - 1$. Como tienen las mismas raíces y ambos son mónicos, por la factorización única de los polinomios tenemos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$. □

El lema anterior nos permite calcular recurrentemente la expresión explícita del polinomio ciclotómico.

Teorema 4.1.1. *Sea $n \in \mathbb{N}$, $\mathbf{K}$ un campo tal que $Char(\mathbf{K}) \nmid n$, y $\Phi_n(x)$ el n-ésimo polinomio ciclotómico sobre $\mathbf{K}$. Entonces*

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

Demostración. Sea $\mathbf{E}$ el campo de descomposición ciclotómico de orden n sobre $\mathbf{K}$ y $\xi \in \mathbf{E}$ una raíz primitiva de la unidad, $\mathbb{U}_n = \langle \xi \rangle$ es el grupo de todas las n-ésimas raíces de la unidad y como este es un grupo cíclico, contiene todas las d-ésimas raíces de la unidad para cada d divisor de n, η será una d-ésima raíz de la unidad, si y sólo si, $| \eta | = d$. Por tanto, para cada d divisor de n tenemos que

$$\Phi_d(x) = \prod_{\substack{\eta \in \mathbb{U}_n \\ |\eta| = d}} (x - \eta)$$

y así, multiplicando todos los polinomios ciclotómicos d-ésimos con d divisor de n tenemos:

$$x^n - 1 = \prod_{\eta \in G} (x - \eta) = \prod_{d|n} \left(\prod_{\substack{\eta \in G \\ |\eta| = d}} (x - \eta) \right) = \prod_{d|n} \Phi_d(x). \tag{4.1}$$

De la ecuación (4.1) tenemos $x^n - 1 = \prod_{d|n} \Phi_d(x)$ el cual es un procedimiento constructivo para calcular los polinomios ciclotómicos de grado n, a partir de los de menor grado.
Ahora de la igualdad $x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ despejamos el polinomio ciclotómico de grado n y obtenemos:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}.$$

□

Notemos que esta expresión nos permite establecer cómo son los coeficientes de $\Phi_n(x)$. Veamos esto con un ejemplo.

Ejemplo 4.1.1. *Calculemos Φ_{12}. Por el Teorema 4.1.1 tenemos:*

$$\Phi_{12}(x) = \frac{x^{12}-1}{\Phi_1\Phi_2\Phi_3\Phi_4\Phi_6},$$

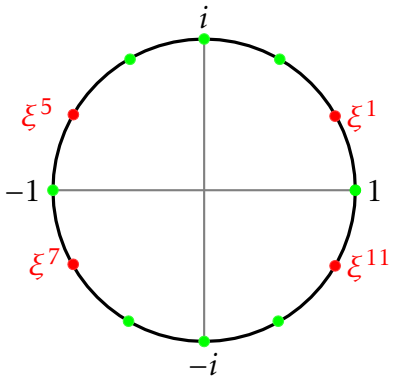
Donde, aplicando el mismo teorema se tiene:

$$\begin{aligned}
\Phi_1 &= x-1,\\
\Phi_2 &= \frac{x^2-1}{\Phi_1} = \frac{x^2-1}{x-1} = x+1,\\
\Phi_3 &= \frac{x^3-1}{\Phi_1} = \frac{(x-1)(x^2+x+1)}{x-1} = x^2+x+1,\\
\Phi_4 &= \frac{x^4-1}{\Phi_1\Phi_2} = \frac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = x^2+1,\\
\Phi_6 &= \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{(x^3-1)(x^3+1)}{(x-1)(x+1)(x^2+x+1)} = \frac{(x^2-x+1)(x+1)}{(x+1)} = x^2-x+1.
\end{aligned}$$

Así

$$\Phi_{12} = \frac{x^{12}-1}{\Phi_1\Phi_2\Phi_3\Phi_4\Phi_6} = \frac{x^{12}-1}{(x^6-1)\Phi_4} = \frac{x^6+1}{x^2+1} = x^4-x^2+1.$$

Para el siguiente diagrama, tenemos cuando $n=12$, las raíces primitivas son las ξ^k, con $k = 1,5,7,11$, ya que son los valores de k tales que $mcd(12,k)=1$



En rojo tenemos las raíces primitivas para $\Phi_{12} = (x-\xi)\left(x-\xi^5\right)\left(x-\xi^7\right)\left(x-\xi^{11}\right)$.

Recordemos la siguiente definición.

Definición 4.1.4. *Un anillo no trivial* $\mathbf{F}$ *es un* ***anillo primo*** *si para dos elementos cualesquiera a y b de* $\mathbf{F}$*, tales que $arb = 0$ para todo $r \in \mathbf{F}$, entonces $a = 0$ o $b = 0$.*

Lema 4.1.3. *Φ_n tiene coeficientes en el anillo primo $\mathbf{K}[x]$.*

Demostración. Demostración por inducción sobre n.
Si $n = 1$, $\Phi_1 = x - 1$, notemos que el polinomio tiene sus coeficientes en el anillo primo.
Supongamos por inducción que $\forall d < n$, Φ_d tiene sus coeficientes en el anillo primo.
Veamos que $x^n - 1$ verifica la propiedad. En la expresión para Φ_n dada por el teorma 4.1.1 el numerador y el denominador tienen sus coeficientes en al anillo primo, así por el algoritmo de la división de polinomios sabemos que el cociente también será mónico y con coeficientes en el anillo primo, es decir Φ_n tiene sus coeficientes en el anillo primo. □

Recordemos que $\mathrm{Irr}(x, \mathbf{K})$ denota al polinomio mónico $p(x) \in \mathbf{K}[x]$ de menor grado tal que $p(x) = 0$.

Lema 4.1.4. *Sean* $m = p_1^{e_1-1} p_2^{e_2-1} \cdots p_r^{e_r-1}$ *y* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, *entonces* $\Phi_d(x)$ *divide a* $\Phi_{d_1}(x^m)$, *donde* $d_1 = \dfrac{d}{(m,d)}$, *para todo* $d \mid n$.

Demostración. Primero observemos que $d = d_1(m,\ d) \mid d_1 m$ pues $(m,\ d) \mid m$, por lo que podemos escribir $d_1 m = dk$ y así $k = (d_1 m)/d$.
Sea ξ una raíz d-ésima primitiva de la unidad, de donde

$$\prod_{t \mid d_1} \Phi_t(\xi^m) = (\xi^m)^{d_1} - 1 = (\xi^d)^k - 1 = \xi^{dk} - 1 = 0.$$

Si demostramos que para $t \neq d_1$ se verifica que $\Phi_t(\xi^m) \neq 0$, simplificando tendremos $\Phi_{d_1}(\xi^m) = 0$, luego $\Phi_d(x) = Irr(\xi, \mathbb{Q}) \mid \Phi_{d_1}(x^m)$ que es lo que buscábamos. $d_1 \mid \dfrac{n}{m} = p_1 \cdots p_r$, luego todo $t \mid d_1$ es de la forma $t = p_{i1} \cdots p_{ij}$. Sea $t \neq d_1$ y por sencillez enumeramos los primos de forma que $t = p_1 \cdots p_j$ con $j < r$. Entonces

$$\Phi_t(\xi^m) \mid (\xi^m)^t - 1 = \xi^{mt} - 1 \neq 0$$

ya que $mt < md_1$ y el orden multiplicativo de ξ es exactamente $d = md_1$. Luego $\Phi_t(\xi^m) \neq 0$. □

Lema 4.1.5. *Sean* $m = p_1^{e_1-1} p_2^{e_2-1} \cdots p_r^{e_r-1}$ *y* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, *con* $d \mid n$ *y* $d_1 = \dfrac{d}{(m,d)}$ *entonces*

$$\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) = \prod_{\substack{d_1 \mid p_1 \cdots p_r \\ d_1 \neq p_1 \cdots p_r}} \Phi_{d_1}(x^m).$$

Demostración. Notemos que $k = (d_1 m)/d$ como antes. Por el lema 4.1.4, cada factor de $\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)$ divide a $\prod_{\substack{d_1 \mid p_1 \cdots p_r \\ d_1 \neq p_1 \cdots p_r}} \Phi_{d_1}(x^m)$, así $\Phi_d(x) \mid \prod_{\substack{d_1 \mid p_1 \cdots p_r \\ d_1 \neq p_1 \cdots p_r}} \Phi_{d_1}(x^m)$. Por el Teorema 4.1.6 tenemos que todos los factores de la izquierda $\Phi_d(x)$ son irreducibles sobre $\mathbb{Q}$ y distintos,

entonces su producto dividirá al polinomio que está a la derecha, así

$$\prod_{\substack{d|n\\ d\neq n}} \Phi_d(x) \mid \prod_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}} \Phi_{d_1}(x^m).$$

Como cada $\Phi_d(x)$ y $\Phi_{d_1}(x^m)$ son mónicos, tendremos que $\prod_{\substack{d|n\\ d\neq n}} \Phi_d(x)$ será mónico y también

$$\prod_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}} \Phi_{d_1}(x^m),$$

así ambos productos son mónicos.

Ahora solo hace falta ver que $grd\left(\prod_{\substack{d|n\\ d\neq n}} \Phi_d(x)\right) = grd\left(\prod_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}} \Phi_{d_1}(x^m)\right)$. Entonces, usando el Teorema 4.1.1

$$grd\left(\prod_{\substack{d|n\\ d\neq n}} \Phi_d(x)\right) = grd\left(\frac{x^n-1}{\Phi_n(x)}\right) = n-\varphi(n)$$

y

$$grd\left(\prod_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}} \Phi_{d_1}(x^m)\right) = grd\left(\frac{(x^m)^{p_1\cdots p_r}-1}{\Phi_{p_1\cdots p_r}(x^m)}\right) = n-\varphi(p_1\cdots p_r)m.$$

Por la fórmula para el cálculo de $\varphi(n)$, tenemos:

$$\begin{aligned} n-\varphi(n) &= n-\varphi(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}) \\ &= n-\left[(p_1-1)\,p_1^{e_1-1}(p_2-1)\,p_2^{e_2-1}\cdots(p_r-1)\,p_r^{e_r-1}\right] \\ &= n-\left[((p_1-1)(p_2-1)\cdots(p_r-1))\,p_1^{e_1-1}p_2^{e_2-1}\cdots p_r^{e_r-1}\right] \\ &= n-[(p_1-1)(p_2-1)\cdots(p_r-1)]\,m \\ &= n-\varphi(p_1\cdots p_r)m. \end{aligned}$$

Así ambos grados son iguales. Por tanto podemos concluir que los dos polinomios son iguales. □

Los dos lemas anteriores nos serán de utilidad en la demostración de una parte de la siguiente proposición.

Proposición 4.1.1. *Reglas de cálculo para los polinomios ciclotómicos,*

a) Si p es un primo, $\Phi_p(x) = x^{p-1}+x^{p-2}+\cdots+x+1$.

b) Para todo $e \geq 1$, *con p primo,se cumple* $\Phi_{p^e}(x) = \Phi_p\left(x^{p^{e-1}}\right)$.

c) Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, *entonces* $\Phi_n(x) = \Phi_{p_1 \cdots p_r}\left(x^{p_1^{e_1-1}} \cdots x^{p_r^{e_r-1}}\right)$.

d) Si $n > 1$ *es impar* $\Phi_{2n}(x) = \Phi_n(-x)$, *con n como producto de primos.*

Demostración. a) Sea p un primo, queremos ver que $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Del Teorema 4.1.1 tenemos que

$$\Phi_p(x) = \frac{x^p - 1}{\prod\limits_{\substack{d|p \\ d \neq p}} \Phi_d(x)},$$

al ser p primo, sus únicos divisores son p y 1 entonces,

$$\frac{x^p - 1}{\prod\limits_{\substack{d|p \\ d \neq p}} \Phi_d(x)} = \frac{x^p - 1}{x - 1},$$

pues $\Phi_1 = x - 1$, así tenemos,

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

y por tanto $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

b) Sean $e \geq 1$ y p un primo queremos ver que $\Phi_{p^e}(x) = \Phi_p\left(x^{p^{e-1}}\right)$. Como consecuencia inmediata del Teorema 4.1.1 se tiene

$$\Phi_{p^e} = \frac{x^{p^e} - 1}{\prod\limits_{d|p^e} \Phi_d(x)}$$

y como los divisores de p^e son $1, p, p^2, \cdots, p^{e-1}$ entonces,

$$\frac{x^{p^e} - 1}{\prod\limits_{d|p^e} \Phi_d(x)} = \frac{x^{p^e} - 1}{\Phi_1 \Phi_p \Phi_{p^2} \cdots \Phi_{p^{e-1}}},$$

donde para calcular Φ_{p^i} con $i = 1, \cdots, e - 1$, hacemos lo mismo que en el ejemplo

4.1.1

$$\begin{aligned}
\Phi_p &= \frac{x^p-1}{\Phi_1} \\
\Phi_{p^2} &= \frac{x^{p^2}-1}{\Phi_1\Phi_p} = \frac{x^{p^2}-1}{\Phi_1\cdot\dfrac{x^p-1}{\Phi_1}} = \frac{x^{p^2}-1}{x^p-1} \\
\Phi_{p^3} &= \frac{x^{p^3}-1}{\Phi_1\Phi_p\Phi_{p^2}} = \frac{x^{p^3}-1}{\Phi_1\cdot\dfrac{x^p-1}{\Phi_1}\cdot\dfrac{x^{p^2}-1}{x^p-1}} = \frac{x^{p^3}-1}{x^{p^2}-1},
\end{aligned}$$

haciendo esto de manera recursiva y con varios cálculos más, podemos continuar con la prueba y vemos que,

$$\begin{aligned}
\frac{x^{p^e}-1}{\Phi_1\Phi_p\Phi_{p^2}\cdots\Phi_{p^{e-1}}} &= \frac{x^{p^e}-1}{\Phi_1\cdot\dfrac{x^p-1}{\Phi_1}\cdot\dfrac{x^{p^2}-1}{\Phi_1\Phi_p}\cdot\cdots\cdot\dfrac{x^{p^{e-2}}-1}{\Phi_1\cdots\Phi_{p^{e-3}}}\cdot\dfrac{x^{p^{e-1}}-1}{\Phi_1\cdots\Phi_{p^{e-2}}}} \\
&= \frac{x^{p^e}-1}{\Phi_1\cdot\dfrac{x^p-1}{\Phi_1}\cdot\dfrac{x^{p^2}-1}{x^p-1}\cdot\cdots\cdot\dfrac{x^{p^{e-2}}-1}{x^{p^{e-3}}-1}\cdot\dfrac{x^{p^{e-1}}-1}{x^{p^{e-2}}-1}} \\
&= \frac{x^{p^e}-1}{x^{p^{e-1}}-1} \\
&= \Phi_{p^e}(x^{p^e}).
\end{aligned}$$

De esta manera tenemos que $\Phi_{p^e}(x) = \Phi_p\left(x^{p^{e-1}}\right)$ lo cual es el resultado deseado.

c) Sean $m = p_1^{e_1-1}p_2^{e_2-1}\cdots p_r^{e_r-1}$ y $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, queremos ver que

$$\Phi_n(x) = \Phi_{p_1\cdots p_r}\left(x^{p_1^{e_1-1}}\cdots x^{p_r^{e_r-1}}\right).$$

Por el Teorema 4.1.1 tenemos que $\Phi_n(x) = \dfrac{x^n-1}{\displaystyle\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)}$, como

$$\begin{aligned}
n &= p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r} \\
&= p_1p_1^{e_1-1}p_2p_2^{e_2-1}\cdots p_rp_r^{e_r-1} \\
&= \left(p_1^{e_1-1}p_2^{e_2-1}\cdots p_r^{e_r-1}\right)p_1p_2\cdots p_r \\
&= m(p_1p_2\cdots p_r),
\end{aligned}$$

por el lema 4.1.5 tenemos $\displaystyle\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x) = \prod_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}}\Phi_{d_1}(x^m)$, y como los d_1 son todos los

posibles productos de las combinaciones de r en k con $k \in \{1, \cdots k-1\}$, entonces el polinomio nos queda de la siguiente manera.

$$\begin{aligned}\Phi_n(x) &= \frac{x^n-1}{\prod\limits_{\substack{d|n\\ d\neq n}} \Phi_d(x)} \\ &= \frac{(x^m)^{p_1\cdots p_r}-1}{\prod\limits_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}} \Phi_{d_1}(x^m)},\end{aligned}$$

de donde por el teorema 4.1.1 tenemos que

$$\frac{(x^m)^{p_1\cdots p_r}-1}{\prod\limits_{\substack{d_1|p_1\cdots p_r\\ d_1\neq p_1\cdots p_r}} \Phi_{d_1}(x^m)} = \Phi_{p_1\cdots p_r}(x^m) = \Phi_{p_1\cdots p_r}(x^{p_1^{e_1-1}\cdots p_r^{e_r-1}}).$$

d) Probaremos por inducción:
Notemos que $\Phi_2(-x) = -x+1 = -\Phi_1(x)$.
Sea $n > 1$ impar, es decir para $n = 2k+1$, realizaremos la inducción sobre k. Queremos ver que $\Phi_{2n}(x) = \Phi_n(-x)$.
Para $k = 1$, tenemos $\Phi_6(x) = x^2 - x + 1$, y por otra parte

$$\begin{aligned}\Phi_3(x) &= x^2+x+1, \\ \Phi_3(-x) &= (-x)^2 - x + 1 \\ &= x^2 - x + 1,\end{aligned}$$

de esta manera $\Phi_6(x) = x^2 - x + 1 = \Phi_3(-x)$.
Hipótesis de inducción.
Supongamos válido para $k < r$ y $n = 2r+1$, es decir $\Phi_{2d}(x) = \Phi_d(-x)$ y d tal que $d \mid 2r+1 = n$.
Ahora veamos que se cumple para $k > r$.

$$\begin{aligned}\Phi_{2n}(x) &= \frac{x^{2n}-1}{\prod\limits_{\substack{d|2n\\ d<2n}} \Phi_d(x)} \\ x^{2n}-1 &= \prod_{\substack{d|2n\\ d<2n}} \Phi_d(x)\cdot\Phi_{2n}(x).\end{aligned}$$

En esta última desigualdad notemos los d que cumplen que $d < 2n$ y $d \mid 2n$, con n impar, son todos los divisores de n y los números de la forma $2 \cdot$ (divisores de n)

excepto el $2n$ pues no se considera desde un principio. Así

$$\Phi_{2n}(x) = \frac{x^{2n}-1}{\prod\limits_{d|n}\Phi_d(x)\cdot\prod\limits_{\substack{d|n\\ d<n}}\Phi_{2d}(x)} = \frac{x^{2n}-1}{(x^n-1)\cdot\prod\limits_{\substack{d|n\\ d<n}}\Phi_{2d}(x)}.$$

Por hipótesis de inducción, tenemos $\Phi_{2d}(x) = \Phi_d(-x)$, puesto que d es divisor de n impar, entonces d es impar.

$$\begin{aligned}
\Phi_{2n}(x) &= \frac{x^{2n}-1}{(x^n-1)\cdot\prod\limits_{\substack{d|n\\ d<n}}\Phi_{2d}(x)} \\
&= \frac{x^{2n}-1}{(x^n-1)\prod\limits_{\substack{d|n\\ d<n}}\Phi_d(-x)} \\
&= \frac{(x^n-1)(x^n+1)}{(x^n-1)\prod\limits_{\substack{d|n\\ d<n}}\Phi_d(-x)} \\
&= \frac{(x^n+1)\Phi_n(-x)}{\prod\limits_{\substack{d|n\\ d<n}}\Phi_d(-x)\cdot\Phi_n(-x)} \\
&= \frac{(x^n+1)\Phi_n(-x)}{\prod\limits_{d|n}\Phi_d(-x)} \\
&= \frac{(x^n+1)\Phi_n(-x)}{((-x)^n-1)(-1)} = \Phi_n(-x)
\end{aligned}$$

donde el (-1) en el denominador es porque $\Phi_2(x) = -\Phi_1(-x)$, además $(-1)^n = -1$ pues n es impar, los divisores de n son $\{1, d_1, d_2, \cdots, d_n = n\}$, donde $d_i \mid n$ con $i = 1, \cdots, n$ y de esta manera siempre estamos tomando al uno entre los divisores.

□

En esta parte tomaremos como referencia principal el Capítulo 6 del libro [Jon].
A partir de este momento, consideraremos a $\mathbb{U}_n$ el conjunto de las unidades de $\mathbb{Z}_n$. Recordemos que las unidades de $\mathbb{Z}_n$, son los números que cumplen; $1 \leqslant k \leqslant n$ y $(n,k) = 1$, por lo tanto, el orden de este grupo es $\varphi(n)$ véase la definición en [Her]. En este primer teorema, vamos a encontrar una caracterización de las raíces primitivas, que nos ayudará a localizarlas con mayor facilidad.
Recordemos que el orden de $a \in \mathbb{U}_n$ es el menor entero positivo $b \in \mathbb{Z}^+$ tal que $a^b = 1$.

Teorema 4.1.2. *Un elemento $a \in \mathbb{U}_n$ es una raíz primitiva de la unidad, si y sólo si, $a^{\varphi(n)/q} \neq 1$, para cada q primo que divida a $\varphi(n)$*

Demostración. Si a es una raíz primitiva de la unidad, entonces su orden es $\varphi(n)$, y por tanto $a^i \neq 1$ para $1 \leq i < \varphi(n)$ y en particular, es cierto para $i = \frac{\varphi(n)}{q}$ con q primo dividiendo a $\varphi(n)$.
Por otra parte si a no es una raíz primitiva, sea k el orden de a, y por ser un elemento de $\mathbb{U}_n$, entonces tiene que dividir al orden del grupo, es decir, $k \mid \varphi(n)$. Por tanto, $\frac{\varphi(n)}{k} > 1$, tomamos q un primo que divida a $\frac{\varphi(n)}{k}$, entonces k divide a $\frac{\varphi(n)}{q}$, y por tanto tenemos que $a^{\varphi(n)/q} = 1$ en $\mathbb{U}_n$. □

4.1.2. Los polinomios ciclotómicos y los campos $\mathbb{Q}$ y $\mathbb{Z}_n$

Una vez analizados los polinomios ciclotómicos en un campo cualquiera veamos algunos resultados en el campo $\mathbb{Q}$, posteriormente vamos a ver un ejemplo particular de los polinomios ciclotómicos sobre el campo de los $\mathbb{Z}_n$. Para este estudio, tomaremos como referencia el apartado 8 del Capítulo 5 del libro [Hun] y Capítulo 9 del libro [Cox].
Mediante el Teorema 4.1.1, los primeros polinomios ciclotómicos en el campo de los racionales quedan de las siguiente forma, en los primeros casos es claro que tenemos $\Phi_1(x) = x - 1$ y $\Phi_1(x) = x + 1$, y calculando los siguientes polinomios ciclotómicos de manera recursiva como en el ejemplo 4.1.1 obtenemos:

$$\begin{aligned}
\Phi_3(x) &= x^2 + x + 1, \\
\Phi_4(x) &= x^2 + 1, \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1, \\
\Phi_6(x) &= x^2 - x + 1, \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
\Phi_8(x) &= x^4 + 1, \\
\Phi_9(x) &= x^6 + x^3 + 1.
\end{aligned}$$

Proposición 4.1.2. *Sea* $\mathbf{K}(\xi) : \mathbf{K}$ *una extensión simple y algebraica, entonces* $| \mathbf{K}(\xi) : \mathbf{K} | = grd(m)$ *donde* m *es un polinomio mínimo para* ξ.

Para la demostración véase [Ste].

Teorema 4.1.3. *Sea* $\mathbf{E}$ *el campo de descomposición ciclotómico de orden* n *sobre* $\mathbb{Q}$, *entonces* $| \mathbf{E} : \mathbb{Q} | = \varphi(n)$

Demostración. Sabemos que $\mathbf{E} = \mathbb{Q}(\xi)$ con ξ una raíz de la unidad, y sabemos por el ejemplo 2.1.4 que $\Phi_n(x)$ es el polinomio mínimo irreducible para cualquier n-ésima raíz de la unidad, y por el Teorema 4.1.1 el grado del polinomio ciclotómico es $\varphi(n)$, de esta manera por la Proposición 4.1.2 tenemos $| \mathbf{E} : \mathbb{Q} | = \varphi(n)$. □

Teorema 4.1.4. *Si* $\mathbf{E}$ *es el campo de descomposición de un polinomio separable en* $\mathbf{K}[x]$, *entonces el grupo de Galois de* $\mathbf{K} \subset \mathbf{E}$, *tiene orden* $| Gal(\mathbf{E} : \mathbf{K}) | = | \mathbf{E} : \mathbf{K} |$.

Para la demostración véase [Cox].

Teorema 4.1.5. *Criterio de Eisenstein-Schonemann. Sea $f(x) \in \mathbb{Z}[x]$ un polinomo con $grd[f(x)] > 0$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y un número primo p tal que $p \mid a_i$ para toda $i \neq n$, pero no divide a a_n y además $p^2 \nmid a_0$ entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.*

Para la demostración véase [Art].

Teorema 4.1.6. *$\Phi_n(x)$ es irreducible sobre $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$.*

Para la demostración véase [Cox].

Proposición 4.1.3. *$\Phi_p(x) = x^{p-1} + \cdots + x + 1$ es irreducible sobre $\mathbb{Q}$ cuando p es primo.*

Demostración. Primero tenemos por el Teorema 4.1.1

$$\Phi_p(x) = \frac{(x^p - 1)}{x - 1},$$

entonces

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}.$$

Del Teorema del binomio tenemos lo siguiente

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{r}x^{p-r} + \cdots + \binom{p}{p-1}x + 1 \tag{4.2}$$

y la sustitución de (4.2) en la fórmula anterior para $\Phi_p(x+1)$ da

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{r}x^{p-r-1} + \cdots + \binom{p}{p-1}. \tag{4.3}$$

Sin embargo para $1 \leq r \leq p-1$, el entero

$$\binom{p}{r} = \frac{p!}{r!\,(p-r)!} = \frac{p\,(p-1)\cdots(p-r+1)}{r!}$$

es divisible por p, ya que p divide al numerador pero no al denominador, pues p es primo. Además, notemos que p^2 no divide $\binom{p}{p-1} = p$, entonces $\Phi_p(x+1)$ es irreducible, ya que (4.3) satisface el criterio del Teorema 4.1.5.
Ahora afirmamos que Φ_p es irreducible, ya que una factorización $\Phi_p(x) = g(x)h(x)$ en $\mathbb{Q}$ implicaría $\Phi_p(x+1) = g(x+1)h(x+1)$. Si g y h tienen un grado menor que $p-1$, lo mismo sería cierto para $g(x+1)$ y $h(x+1)$, lo que contradiría la irreductibilidad de $\Phi_p(x+1)$. □

$\mathbb{Z}_n$ y los polinomios ciclotómicos.

$\mathbb{Z}_n$ y los polinomios ciclotómicos. Ahora que ya analizamos los polinomios ciclotómicos sobre el campo $\mathbb{Q}$. Analicemos los polinomios ciclotómicos sobre el campo $\mathbb{Z}_n$, con $n \in \mathbb{N}$.

Es decir, veremos como resolver las ecuaciones de la forma:

$$x^k \equiv 1 \pmod{n} \quad k, n \in \mathbb{N}$$

Para analizar la solución de los polinomios ciclotómicos en $\mathbb{Z}_n$, tomaremos como referencia el Capítulo 6 del libro [Jon].

Caso 1. Estudiemos primero los casos $n = 2p^e,\ p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, donde p_i es un primo impar y para $e = 1,\ 2$ ([Jon]), pues son los casos en los que el grupo de las unidades de $\mathbb{Z}_n$ es cíclico. En este caso, al ser $\mathbb{U}_n$ cíclico, sabemos que existe una raíz primitiva (ver Teorema 4.1.2), de modo que ponemos a $x \in \mathbb{U}_n$ como potencia de una raíz primitiva cualquiera, es decir, escribimos;

$$x \equiv w^i \pmod{n}, \tag{4.4}$$

donde w es una raíz primitiva de $\mathbb{U}_n$, e i es desconocido. De modo, que la ecuación (4.4) queda

$$(w^i)^k \equiv w^{ik} \equiv 1 \pmod{n}$$

y además

$$1 \equiv w^{\varphi(n)} \pmod{n}.$$

Como la raíz primitiva tiene orden $\varphi(n)$, entonces.

$$w^{ik} \equiv w^{\varphi(n)} \pmod{n}.$$

Por este mismo motivo, se puede trasformar esta ecuación en una ecuación lineal

$$ik \equiv \varphi(n) \pmod{\varphi(n)},$$

de esta manera

$$ik \equiv 0 \pmod{\varphi(n)}.$$

Resolviendo esta última congruencia, obtenemos las soluciones, es decir buscamos las i tales que ik sea congruente con 0 módulo n, así las soluciones son: $i_1, i_2 \cdots, i_s$, de esta manera las soluciones del polinomio ciclotómico son: $x \equiv w^{i_1}, w^{i_2}, \cdots, w^{i_s}$ módulo n.

Ahora, que ya hemos visto el procedimiento para resolver la ecuación en el caso donde el grupo de las unidades sea cíclico, veamos un ejemplo.

Ejemplo 4.1.2. *Calculemos las soluciones del polinomio ciclotómico de grado* 4 *sobre*

$$\mathbb{Z}_{25} = \{0,\ 1,\ 2,\ 3, \cdots,\ 22,\ 23,\ 24\}.$$

La ecuación de congruencia queda dada por,

$$x^4 \equiv 1 \pmod{25}.$$

Como $\mathbb{U}_{25} = \mathbb{U}_{5^2}$, *y sabemos que* $\mathbb{U}_{5^2}$ *es cíclico ([Jon]), buscamos una raíz primitiva de la unidad. Como* $\varphi(25) = 20 = 2^2(5)$ *y necesitamos que* w *sea raíz primitiva, por el Teorema 4.1.2 veamos que* $w^{20/2} = w^{10} \neq 1$ *y* $w^{20/5} = w^4 \neq 1$ *en* $\mathbb{Z}_{25}$. *Notemos que como*

$$2^{10} \equiv 24 \pmod{25}$$

y también

$$2^4 \equiv 16 \pmod{25},$$

de esta manera 2 es raíz primitiva, así $\mathbb{U}_{5^2} = \left\{2, 2^1, 2^2, \cdots, 2^{19}, 2^{20}\right\}$, *ahora ponemos a* x *como potencia de* $w = 2$, $x \equiv 2^i \pmod{25}$, *y como* $1 \equiv 2^{\varphi(25)} \equiv 2^{20} \pmod{25}$, *por tanto, la ecuación queda:*

$$x^4 = 2^{4i} \equiv 2^{20} \pmod{25}.$$

Como a ambos lados de la equivalencia tenemos la misma potencia, podemos fijarnos únicamente en el exponente, de modo, que reducimos la congruencia no lineal, en una lineal

$$4i \equiv 20 \equiv 0 \pmod{20},$$

de donde tenemos, que las soluciones de esta ecuación son $i = 0, 5, 10, 15$, *y por tanto, tenemos:*

$$\begin{aligned} x &\equiv 2^0 = 1 \pmod{25} \\ x &\equiv 2^5 = 32 \equiv 7 \pmod{25} \\ x &\equiv 2^{10} = 1024 \equiv 24 \pmod{25} \\ x &\equiv 2^{15} = 32768 \equiv 18 \pmod{25}. \end{aligned}$$

Así las soluciones son $x = 1, 7, 24, 18$.

Caso 2. Ahora nos fijamos en los casos cuando $n = 2^e$ con $e \geq 3$. Queremos resolver el polinomio ciclotómico $x^k - 1 = 0$ en $\mathbb{Z}_{2^e}$ con $e \geq 3$, es decir buscamos los $x \in \mathbb{U}_{2^e}$ tales que

$$x^k \equiv 1 \pmod{2^e}. \tag{4.5}$$

Sabemos que $\mathbb{U}_{2^e} = \{\pm 5^i \mid 0 < i \leq 2^{e-2}\}$ ver [Jon], es decir el orden de x es 2^{e-2} si $x \in \mathbb{U}_{2^e}$, entonces

$$x \equiv 5^i \pmod{2^e}$$

$$1 \equiv 5^{2^{e-2}} \pmod{2^e}, \tag{4.6}$$

así

$$x^k \equiv 5^{ik} \pmod{2^e}, \tag{4.7}$$

de (4.5) y (4.7) tenemos que

$$5^{ki} \equiv 1 \pmod{2^e}, \tag{4.8}$$

como $0 < i \leq 2^{e-2}$ entonces de (4.6) y (4.8), tenemos

$$\begin{aligned} 5^{ki} &\equiv 5^{2^{e-2}} \pmod{2^e} \\ ki &\equiv 2^{e-2} \pmod{2^{e-2}} \\ ki &\equiv 0 \pmod{2^{e-2}}, \end{aligned}$$

es decir buscamos las $i \in \{0, 1, \cdots, 2^{e-2}\}$ tales que $ki = 0$ en $\mathbb{Z}_{2^{e-2}}$, de esta manera las soluciones de (4.5) son $x \equiv \pm 5^i \equiv 1 \pmod{2^e}$.

Ejemplo 4.1.3. *Buscamos resolver el polinomio ciclotómico $x^3 - 1 = 0$ en $\mathbb{Z}_8$, es decir buscamos los $x \in \mathbb{U}_8$ tales que*

$$x^3 \equiv 1 \pmod{8},$$

sabemos que

$$\mathbb{U}_8 = \left\{\pm 5^i \mid 0 < i \leq 2^{3-2}\right\} = \left\{\pm 5^i \mid 0 < i \leq 2\right\} = \left\{5,\ 5^2,\ -5,\ (-5)^2\right\} = \{5,\ 1,\ 3\},$$

entonces se tienen las siguientes congruencias

$$(\pm 5)^2 \equiv 1 \pmod{8},$$

como en el caso 1 ponemos a $x \in \mathbb{U}_8$ en términos de potencia de la raíz primitiva,

$$x \equiv (\pm 5)^i \pmod{8}$$

$$1 \equiv x^3 \equiv (\pm 5)^{3i} \pmod{8}$$

$$(\pm 5)^{3i} \equiv (\pm 5)^2 \pmod{8},$$

de esta manera podemos resolver ahora una congruencia lineal, en $\mathbb{Z}_2 = \{0,\ 2\}$

$$3i \equiv 2 \pmod{2}$$

$$3i \equiv 0 \pmod{2}$$

y como buscamos las $i \in \{0,\ 1\}$ tales que $3i = 0$, la única solución es cuando $i = 0$ (es decir, la solución trivial),

$$x \equiv (\pm 5)^0 \equiv 1 \pmod{8},$$

de esta manera la única solución en $\mathbb{Z}_8$ *para* $x^3 - 1 = 0$ *es* $x = 1$.

Caso general. Finalmente vamos a resolver $x^k - 1 = 0$ en $\mathbb{Z}_n$ para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Por el Teorema chino del residuo (ver 1.2.1), sabemos que para encontrar las soluciones de

$$x^k \equiv 1 \pmod{n},$$

dado que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ basta resolver las congruencias

$$\begin{aligned} w_1^k &\equiv 1 \pmod{p_1^{\alpha_1}} \quad \text{(la cual tiene } m_1 \text{ soluciones)} \\ w_2^k &\equiv 1 \pmod{p_2^{\alpha_2}} \quad \text{(la cual tiene } m_2 \text{ soluciones)} \\ &\vdots \\ w_s^k &\equiv 1 \pmod{p_s^{\alpha_s}} \quad \text{(la cual tiene } m_s \text{ soluciones).} \end{aligned}$$

Después de haber encontrado las distintas soluciones de $w_i^k \equiv 1 \pmod{p_i^{\alpha_i}}$ con $i = 1, \cdots, s$, por el Teorema chino del residuo (ver 1.2.1),

$$\begin{aligned} c_1 &= \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}}{p_1^{\alpha_1}}, \\ c_2 &= \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}}{p_2^{\alpha_2}}, \\ &\vdots \\ c_s &= \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}}{p_s^{\alpha_s}}, \end{aligned}$$

y resolvemos las siguientes conguencias

$$\begin{aligned} c_1 d_1 &\equiv 1 \pmod{p_1^{\alpha_1}} \\ c_2 d_2 &\equiv 1 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ c_s d_s &\equiv 1 \pmod{p_s^{\alpha_s}}, \end{aligned}$$

para hallar $d_1, d_2, \cdots, d_s$ finalmente, una solución de $x^k \equiv 1 \pmod{n}$ es $x = w_1 c_1 d_1 + w_2 c_2 d_2 + \cdot + w_s c_s d_s$, donde cada $w_i c_i d_i$ tiene m_i posibles soluciones, con $i = 1, 2, \cdots, s$.

Notemos que las soluciones se irán reduciendo a la hora de hacer los cálculos. Veamos un ejemplo de lo anterior.

Ejemplo 4.1.4. *Resolvamos el polinomio ciclotómico con* $k = 7$ *en* $\mathbb{Z}_{72}$. *Buscamos resolver la congruencia*

$$x^7 \equiv 1 \pmod{72},$$

para empezar, descomponemos 72 en factores primos, obteniendo; $72 = 2^3 \cdot 3^2$. *De esta manera tenemos las congruencias*

$$w_1^7 \equiv 1 \pmod{2^3},$$

$$w_2^7 \equiv 1 \pmod{3^2}.$$

Empecemos resolviendo la ecuación $w_1^7 \equiv 1 \pmod{2^3}$ *la cual entra en el caso 1, pues* $n = 2^3$. *Como ya sabemos,* $U_{2^3} = \left\{(\pm 5)^i \mid 0 \leq i \leq 2\right\}$ *y* $(\pm 5)^2 \equiv 1 \pmod{2^3}$. *Poniendo la incógnita* w_1 *como potencia de* ± 5, *es decir,*

$$w_1 \equiv (\pm 5)^i \pmod{2^3}$$

la ecuación nos queda:

$$1 \equiv w_1^7 \equiv (\pm 5)^{7i} \pmod{2^3}.$$

Solo basta resolver para las siguientes congruencias

$$w_1^{7i} \equiv (\pm 5)^2 \pmod{2^3}.$$

Como la base de las congruencias es la misma tenemos

$$7i \equiv 2 \equiv 0 \pmod{2},$$

ahora las $i \in \mathbb{Z}_2$ *tales que* $7i = 0$ *es* $i = 0$, *entonces la única solución para* w_1 *es* 1.
Calculemos ahora para la ecuación $w_2^7 \equiv 1 \pmod{3^2}$ *la cual entra en el caso 1, pues* $n = 3^2$, *con 3 número primo. Como* $\varphi\left(3^2\right) = \varphi(9) = 6$ *y como* $2^{\varphi(9)/2} = 2^3 = 8$ *y* $2^{\varphi(9)/3} = 2^2 = 4$ *por el Teorema 4.1.2 tenemos que 2 es raíz primitiva. Así, que ahora reescribimos la ecuación poniéndola como potencia de esta raíz primitiva y obtenemos:*

$$2^{7i} \equiv 2^{\varphi(9)} \equiv 2^6 \pmod{3^2}.$$

Como tienen la misma base nos fijamos únicamente en los exponentes y obtenemos la congruencia lineal

$$7i \equiv 6 \pmod{6},$$

$$7i \equiv 0 \pmod{6}.$$

Ahora buscando las $i \in \mathbb{Z}_6$ *tales que* $7i = 0$ *veamos que solo es* $i = 0$, *de donde tenemos que la única solución de la segunda congruencia es:*

$$w_2 \equiv 2^0 \equiv 1 \pmod{3^2}.$$

Ahora por el caso 3, calculamos los c_i *y tenemos,*

$$c_1 = \frac{72}{2^3} = 9,\ c_2 = \frac{72}{3^2} = 8,$$

y siguiendo el proceso del caso 3 el siguiente paso es calcular los d_i resolviendo las ecuaciones

$$9d_1 \equiv 1 \pmod 8 \ y \ 8d_2 \equiv 1 \pmod 9,$$

de donde obtenemos $d_1 \equiv 1 \pmod 8$ y $d_2 \equiv 1 \pmod 9$, así $d_1 = 1$ y $d_2 = 8$, por tanto, la única solución de la ecuación es: $x \equiv w_1c_1d_1 + w_2c_2d_2 = 1 \cdot 9 \cdot 1 + 1 \cdot 8 \cdot 8 = 73 \equiv 1 \pmod{72}$

Realizando los mismos pasos que en este ejemplo, podemos resolver cualquier polinomio ciclotómico en los anillos $\mathbb{Z}_n$ cuando n pertenece a los naturales.

4.2. Solubilidad por radicales de polinomios ciclotómicos

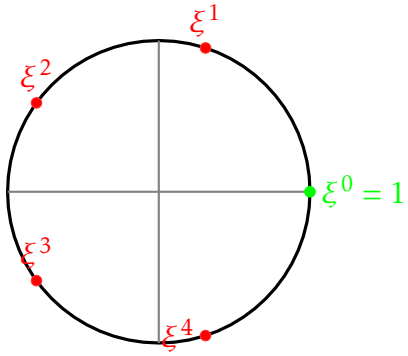
La siguiente proposición es una consecuencia directa del Teorema de Galois 3.2.1, la cual nos ayuda a establecer criterios para ver cuándo un polinomio ciclotómico es soluble por radicales.

Teorema 4.2.1. *Sea* **K** *con Char(***K***)= 0 y consideramos el polinomio ciclotómico $\Phi_p \in K[x]$, con p primo. Entonces la ecuación $\Phi_p(x) = 0$ es soluble por radicales sobre* **K**.

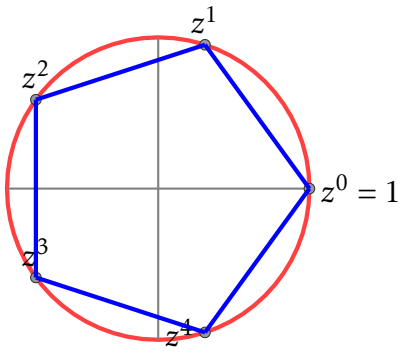
Demostración. Sabemos que $Gal(\mathbf{K}(\xi) : \mathbf{K})$ es un grupo abeliano y por tanto soluble. Por el Teorema de Galois 3.2.1 resulta que $\Phi_p(x) = 0$ es soluble por radicales sobre **K**. □

Ahora veamos algunos resultados para polinomio ciclotómico que relacionan la solubilidad por radicales y la extensión radical.

Ejemplo 4.2.1. *En el siguiente diagrama, mostramos que si $n = 5$, las raíces primitivas son ξ^k, con $k = 1, 2, 3, 4$ ya que son los valores de k tales que $mcd(5, k) = 1$.*



En rojo tenemos las raíces primitivas para $\Phi_5 = (x-\xi)\left(x-\xi^2\right)\left(x-\xi^3\right)\left(x-\xi^4\right)$. Además notemos que del dibujo anterior podemos obtener el polígono regular asociado a las raíces del polinomio Φ_5, como se muestra en el siguiente diagrama.



Sea $f(x) = \Phi_5(x) = x^4+x^3+x^2+x+1 = \prod_{i=1}^{4}(x-\xi_i)$, *donde* ξ_i *es una raíz primitiva del polinomio* $x^5-1=0$. *Además notemos que* $x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$.
Encontremos de forma explícita las raíces de Φ_5, *sea* $\xi = e^{2\pi i/5} = cos(2\pi/5)+isen(2\pi/5)$ *y sea* $\alpha = \xi+\bar{\xi} = 2Real(\xi)$.
Notemos en primer lugar que $\xi\bar{\xi} = 1 = \bar{\xi}\xi$, $\bar{\xi} = \xi^{-1}$, *así* $\xi^5 = 1 = \xi\bar{\xi}$, *entonces* $\xi\xi^4 = \xi\bar{\xi}$ *de esta manera tenemos*

$$\begin{aligned} \xi^4 &= \bar{\xi}, \\ \xi\xi^3 &= \bar{\xi}, \\ \xi^3 &= \bar{\xi}^2, \end{aligned}$$

y además

$$\alpha^2 = (\xi+\bar{\xi})^2 = \xi^2+2\xi\bar{\xi}+\bar{\xi}^2 = \xi^2+2+\bar{\xi}^2,$$

entonces $\alpha^2-2 = \xi^2+\bar{\xi}^2$. *Como* ξ *es raíz de* x^5-1, *entonces* $\xi^5-1=0$, *así* $(\xi-1)(\xi^4+\xi^3+\xi^2+\xi+1)$ *y como* $\xi \neq 1$ *tenemos*

$$\begin{aligned} \xi^4+\xi^3+\xi^2+\xi+1 &= 0 \\ \bar{\xi}+\bar{\xi}^2+\xi^2+\xi+1 &= 0 \\ \xi+\bar{\xi}+\xi^2+\bar{\xi}^2+1 &= 0 \\ \alpha+\alpha^2-2+1 &= 0 \\ \alpha^2+\alpha-1 &= 0. \end{aligned}$$

De esta manera sabemos que debemos resolver para α, *y como es una ecuación de grado dos, tenemos que sus soluciones se ven de la siguiente manera,*

$$\alpha = \frac{-1\pm\sqrt{5}}{2}.$$

Basta con tomar alguna de las soluciones para $\alpha^2+\alpha-1$, *entonces tenemos que* $\alpha = \dfrac{\sqrt{5}-1}{2}$ *es una raíz de* $\Phi_5(x)$, *pero como queremos conocer la raíz primitiva* ξ, *tenemos que como,*

$\alpha = 2Real(\xi)$ *y* $\xi = cos(2\pi/5) + isen(2\pi/5)$, *así,*

$$\frac{\sqrt{5}-1}{2} = 2cos(2\pi/5),$$

entonces $cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$. *Ahora solo hace falta conocer a* $sen(2\pi/5)$, *sabemos que*

$$sen^2(z) = 1 - cos^2(z),$$

por lo tanto

$$\begin{aligned} sen(2\pi/5) &= \sqrt{1-cos^2(2\pi/5)} \\ &= \sqrt{1-\left(\frac{5-2\sqrt{5}+1}{16}\right)} \\ &= \sqrt{\frac{16+2\sqrt{5}-6}{16}} \\ &= \sqrt{\frac{10+2\sqrt{5}}{(2)8}} \\ &= \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}, \end{aligned}$$

así

$$\xi = \frac{\sqrt{5}-1}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}},$$

la cual es una raíz primitiva de Φ_5, *de esta manera genera a todas las demás raíces de* Φ_5, *entonces* $\langle\xi\rangle = \{\xi,\ \xi^2,\ \xi^3,\ \xi^4,\ 1\}$. *Dado que ya tenemos las raíces primitivas de* Φ_5, *ahora queremos calcular su grupo de Galois y su campo de descomposición.*
Sea ξ *la raíz primitiva de* $x^5 - 1$, *entonces* $\mathbf{E} = \mathbb{Q}(\xi)$ *es el campo de descomposición del polinomio* Φ_5, *como sabemos que el grupo* $Gal(\mathbf{E} : \mathbb{Q}) = Aut(\mathbf{E} \to \mathbf{E})$ *deja fijo a* $\mathbb{Q}$ *y además* $\mathbf{E}$ *tiene estructura de un* $\mathbb{Q}$*-espacio vectorial, y por el Teorema 4.1.3 y la Proposición 4.1.4, la* $dim_{\mathbb{Q}}(\mathbf{E}) = 4$ *entonces,*

$$\mathbf{E} = \mathbb{Q}(\xi) = \left\{a + b\xi + c\xi^2 + d\xi^3 \mid a,\ b,\ c,\ d \in \mathbb{Q}\right\}.$$

Como $Gal(\mathbf{E} : \mathbb{Q})$ *es el grupo de automorfismos de* $\mathbf{E}$ *en* $\mathbf{E}$ *tenemos* σ_k *los automorfismos de* $\mathbf{E}$, *definidos como* $\sigma_k(\xi) = \xi^k$ *para* $k = 1,\ 2,\ 3,\ 4$. *Entonces* $\mathbf{G} = Gal(\mathbf{E} : \mathbb{Q}) = \{\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4\}$,

donde $\sigma_1 = id$, *pues* $\sigma_1(\xi) = \xi^1 = \xi$, *además*

$$\begin{aligned}
\sigma_2^1(\xi) &= \xi^2 \\
\sigma_2^2(\xi) &= \sigma_2(\sigma_2(\xi)) = \sigma_2\left(\xi^2\right) = \xi^4 \\
\sigma_2^3(\xi) &= \sigma_2\left(\sigma_2^2(\xi)\right) = \sigma_2\left(\xi^4\right) = \xi^8 = \xi^3 \\
\sigma_2^4(\xi) &= \sigma_2\left(\sigma_2^3(\xi)\right) = \sigma_2\left(\xi^3\right) = \xi^6 = \xi
\end{aligned}$$

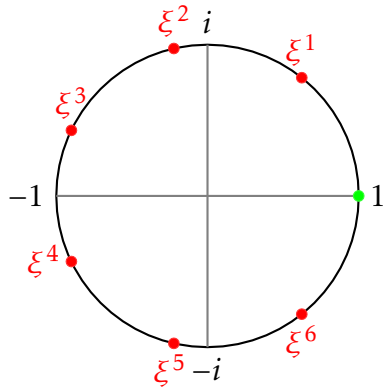
así $\langle\sigma_2^k(\xi)\rangle = \{\xi^2, \xi^4, \xi^3, \xi\} = (2\ 4\ 3\ 1)$ *con* $k = 1, 2, 3, 4$. *De esta manera tenemos la permutación* $(2\ 4\ 3\ 1) = \sigma$, *así* $Gal(\mathbf{E} : \mathbb{Q}) = \langle\sigma\rangle = \{(2\ 4\ 3\ 1), (4\ 3\ 2\ 1), (3\ 1\ 4\ 2), (1\ 2\ 3\ 4)\}$.
Tomamos la permutación $(4\ 3\ 2\ 1)$ *pues es el único subgrupo de* $\mathbf{G}$ *que tiene orden* 2, *ya que una permutación sabemos se puede descomponer en cíclos disjuntos, tenemos* $(1\ 4)(2\ 3)$, *esto nos permite tener la siguiente serie de composición,*

$$Gal(\mathbf{E} : \mathbb{Q}) \triangleright \langle(1\ 4)(2\ 3)\rangle \triangleright 1.$$

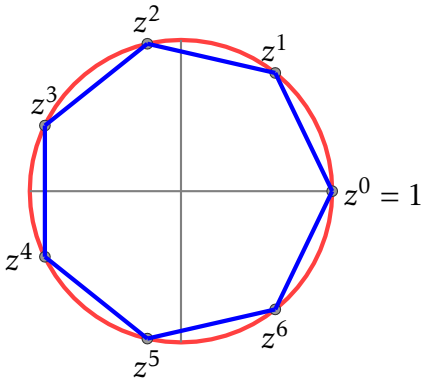
Notemos que por el ejemplo 3.1.1 la torre de descomposición de campos es

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{5}\right) \subset \mathbf{E}(\xi).$$

Ejemplo 4.2.2. *En el siguiente diagrama, tenemos el caso* $n = 7$. *Las raíces primitivas son las* ξ^k, *con* $k = 1, 2, 3, 4, 5, 6$, *ya que son los valores de* k *tales que* $mcd(7, k) = 1$



En rojo tenemos las raíces primitivas para $\Phi_7 = (x - \xi)\left(x - \xi^2\right)\left(x - \xi^3\right)\left(x - \xi^4\right)\left(x - \xi^5\right)\left(x - \xi^6\right)$.
Además notemos que del dibujo anterior podemos obtener el polígono regular asociado a las raíces del polinomio Φ_7, *como se muestra en la siguiente figura.*



Sea $f(x) = \Phi_7(x) = x^6 + x^5 + x^4 + x^3x^2 + x + 1 = \prod_{i=1}^{6}(x - \xi_i)$, *donde* ξ_i *es una raíz primitiva del polinomio* $x^7 - 1 = 0$. *Además tenemos que* $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$.
Encontremos de forma explícita las raíces de Φ_7, *sea* $\xi = e^{2\pi i/7} = cos(2\pi/7) + isen(2\pi/7)$, *y sea* $\alpha = \xi + \bar{\xi} = 2Real(\xi)$.
Notemos en primer lugar que: $\xi\bar{\xi} = 1 = \bar{\xi}\xi$, *de donde observamos que* $\bar{\xi} = \xi^{-1}$, *así* $\xi^7 = 1 = \xi\bar{\xi}$, *entonces de esta manera tenemos*

$$\begin{aligned} \xi^6 &= \bar{\xi} \\ \xi^5 &= \bar{\xi}^2 \\ \xi^4 &= \bar{\xi}^3, \end{aligned}$$

y además

$$\alpha^2 = (\xi + \bar{\xi})^2 = \xi^2 + 2\xi\bar{\xi} + \bar{\xi}^2 = \xi^2 + 2 + \bar{\xi}^2,$$

entonces $\alpha^2 - 2 = \xi^2 + \bar{\xi}^2$. *Como* ξ *es raíz de* $x^7 - 1$, *entonces* $x^7 - \xi = 0$, *así* $(\xi - 1)(x^6 + x^5 + \xi^4 + \xi^3 + \xi^2 + \xi + 1) = 0$, *y como* $\xi \neq 1$ *tenemos*

$$\begin{aligned} 0 &= \xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 + \xi + 1 \\ 0 &= \bar{\xi} + \bar{\xi}^2 + \bar{\xi}^3 + \xi^3 + \xi^2 + \xi + 1 \\ 0 &= \left(\xi^3 + 3\xi + 3\bar{\xi} + \bar{\xi}^3\right) + \left(\xi^2 + 2 + \bar{\xi}^2\right) + \left(\xi + \bar{\xi} + 1 - 3\bar{\xi} - 3\xi - 2\right) \\ 0 &= \left(\xi^3 + 3\xi^2\bar{\xi} + 3\bar{\xi}^2\xi + \bar{\xi}^3\right) + \left(\xi^2 + 2\xi\bar{\xi} + \bar{\xi}^2\right) - \left(2\bar{\xi} - 2\xi - 1\right) \\ 0 &= \left(\xi + \bar{\xi}\right)^3 + \left(\xi + \bar{\xi}\right)^2 - 2\left(\xi + \bar{\xi}\right) - 1 \\ 0 &= \alpha^3 + \alpha^2 - 2\alpha - 1. \end{aligned}$$

De esta manera sabemos que basta resolver para α, *y como es una ecuación de grado tres, podemos encontrar sus soluciones por la fórmula de Cardano (véase sección 3.2.1), de esta manera hacemos*

$$a = 1,\ b = -2,\ c = -1.$$

Sabemos que podemos calcular p y q descritos en la fórmula, de la siguiente manera,

$$p = \frac{3b - a^2}{3}, \quad q = \frac{2a^3 - 9ab + 27c}{27}$$

y además el discriminante está dado por

$$\triangle = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3,$$

como $p = \dfrac{-7}{3}$ *y* $q = \dfrac{-7}{9}$, *tenemos* $\triangle = \dfrac{-7^2}{2^2 \cdot 3^3}$, *entonces* $\sqrt{\triangle} = \dfrac{7i}{2 \cdot 3\sqrt{3}}$, *finalmente tenemos que*

$$\begin{aligned}
\alpha &= \sqrt[3]{\frac{-q}{2} + \sqrt{\triangle}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\triangle}} - \frac{a}{3} \\
&= \sqrt[3]{\frac{7}{18} + \frac{7i}{2 \cdot 3\sqrt{3}}} + \sqrt[3]{\frac{7}{18} - \frac{7i}{2 \cdot 3\sqrt{3}}} - \frac{1}{3} \\
&= \frac{1}{3}\left(-1 + \sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} + \sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}\right).
\end{aligned}$$

Como $\alpha = 2cos(2\pi/7)$, *entonces*

$$cos(2\pi/7) = \frac{1}{6}\left(-1 + \sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} + \sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}\right).$$

Ahora basta calcular $sen(2\pi/7)$ *para poder determinar completamente el valor de* ξ, *entonces usamos la identidad* $sen^2(z) = 1 - cos^2(z)$, *así*

$$\begin{aligned}
sen(2\pi/7) &= \sqrt{1 - \left(\frac{1}{6}\left(-1 + \sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} + \sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}\right)\right)^2} \\
&= \frac{1}{2}\sqrt{4 - \left(\frac{1}{3} - \frac{1}{3}\sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} - \frac{1}{3}\sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}\right)^2}
\end{aligned}$$

entonces

$$\xi = \frac{\left(-1 + \sqrt[3]{\dfrac{7\left(1 + 3i\sqrt{3}\right)}{2}} + \sqrt[3]{\dfrac{7\left(1 - 3i\sqrt{3}\right)}{2}}\right)}{6} + \frac{i\sqrt{4 - \left(\dfrac{1}{3} - \dfrac{\sqrt[3]{\dfrac{7\left(1 + 3i\sqrt{3}\right)}{2}}}{3} - \dfrac{\sqrt[3]{\dfrac{7\left(1 - 3i\sqrt{3}\right)}{2}}}{3}\right)^2}}{2},$$

la cual exhibe una solución por radicales del polinomio Φ_7 *y podemos notar que las otras soluciones tienen expresiones semejantes.*

Dado que ya encontramos las raíces primitivas de Φ_7, *ahora podemos calcular el grupo de Galois asociado a este polinomio, su campo de descomposición y su torre de campos. Como* ξ *es raíz primitiva de* $x^7 - 1$ *sabemos que*

$$\langle \xi \rangle = \{\xi,\ \xi^2,\ \xi^3,\ \xi^4,\ \xi^5,\ \xi^6,\ 1\},$$

entonces $\mathbf{E} = \mathbb{Q}(\xi)$ *el cual sabemos es el campo de descomposición de* $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. *Sabemos que* $Gal(\mathbf{E} : \mathbb{Q})$ *es el grupo de automorfismos de* $\mathbf{E}$ *en* $\mathbf{E}$, *que dejan fijo a* $\mathbb{Q}$. *Sea* σ_k *el automorfismo de* $\mathbf{E}$ *que está determinado por* $\sigma_k(\xi) = \xi^k$ *para* $k = 1,\ 2,\ 3,\ 4,\ 5,\ 6,$

de esta manera $Gal(\mathbf{E}:\mathbb{Q}) = \{\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4,\ \sigma_5,\ \sigma_6\}$, *notemos que* $\sigma_1(\xi) = \xi$ *es decir,* $\sigma_1 = id$, *entonces el automorfismo que nos sirve es* σ_3, *pues*

$$\begin{aligned}
\sigma_3(\xi) &= \xi^3 \\
\sigma_3^2(\xi) &= \sigma_3(\sigma_3(\xi)) = \sigma_3\left(\xi^3\right) = \xi^2 \\
\sigma_3^3(\xi) &= \sigma_3\left(\sigma_3^2(\xi)\right) = \sigma_3\left(\xi^2\right) = \xi^6 \\
\sigma_3^4(\xi) &= \sigma_3\left(\sigma_3^3(\xi)\right) = \sigma_3\left(\xi^6\right) = \xi^4 \\
\sigma_3^5(\xi) &= \sigma_3\left(\sigma_3^4(\xi)\right) = \sigma_3\left(\xi^4\right) = \xi^5 \\
\sigma_3^6(\xi) &= \sigma_3\left(\sigma_3^5(\xi)\right) = \sigma_3\left(\xi^5\right) = \xi
\end{aligned}$$

así tenemos $\langle\sigma_3(\xi)\rangle = \{\xi^3,\ \xi^2,\ \xi^6,\ \xi^4,\ \xi^5,\ \xi\}$, *entonces* $Gal(\mathbf{E}:\mathbb{Q}) = \langle(3\ 2\ 6\ 4\ 5\ 1)\rangle$, *es decir* $\sigma = (3\ 2\ 6\ 4\ 5\ 1)$. *Ahora como* $|\ Gal(\mathbf{E}:\mathbb{Q})\ | = 6 = 3\cdot 2$, *buscamos los subgrupos tal que su orden es* 3 *y* 2. *Notemos que si,* $\mathbf{H} \lhd Gal(\mathbf{E}:\mathbb{Q})$, *tal que* $|\ \mathbf{H}\ | = 2$, *tenemos* $\mathbf{H} = \langle(1\ 6)(2\ 5)(3\ 4)\rangle$ *y si* $\boldsymbol{L} \lhd Gal(\mathbf{E}:\mathbb{Q})$, *tal que* $|\ \boldsymbol{L}\ | = 3$, *tenemos* $\boldsymbol{L} = \langle(1\ \ 2)(3\ 5\ 6)\rangle$, *de esta manera tenemos las siguientes series*

$$Gal(\mathbf{E}:\mathbb{Q}) \rhd \langle(1\ 6)(2\ 5)(3\ 4)\rangle \rhd 1$$

y

$$Gal(\mathbf{E}:\mathbb{Q}) \rhd \langle(1\ \ 2)(3\ 5\ 6)\rangle \rhd 1.$$

Y la torre de campos está dada por

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{Q}(\xi) = \mathbf{E}.$$

Capítulo 5

No solubilidad por radicales

En los momentos de crisis solo la imaginación es más importante que el conocimiento.

Albert Einstein.

Regresamos al problema de, hallar la solución general de la ecuación

$$x^5 + 5x^4 + 10x^3 + 10x^2 - 4x - 5 = 0,$$

con la cual sabemos no es fácil trabajar y mucho menos encontrar sus raíces, pues no contamos con una fórmula que nos ayude con estos cálculos. Sin embargo queremos que las raíces que podamos encontrar estén en términos de operaciones como la suma, el producto, la división, la resta o la potencia a exponentes racionales. Anteriormente analizamos cuándo un polinomio es soluble por radicales, ahora veremos cuándo un polinomio no es soluble por radicales y para ello es importante conocer ciertos criterios que nos ayuden a determinar cuando esto sucede.

5.1. Criterios para determinar polinomios no solubles por radicales

Para la demostración del siguiente teorema enunciaremos la siguiente proposición que nos será de utilidad.

Proposición 5.1.1. *Sea $p(x)$ un polinomio de grado q en $\mathbf{K}[x]$, con q primo, irreducible sobre un campo $\mathbf{E}$ de característica cero, la única permutación de $\mathbf{H} \leq Gal(\mathbf{E} : \mathbf{K})$ que deja por lo menos dos elementos fijos es la identidad.*

Demostración. Sea $A = \{d_1, \cdots, d_q\}$ las raíces de $p(x)$ acomodadas en una previa numeración, es decir $d_i \to i$ con $i \in I_q = \{1, \cdots, q\}$. Como el grupo de Galois permuta las raíces del polinomio $p(x)$, es decir para $\sigma \in \mathbf{H}$ tenemos $\sigma(i) = j$ con $i \neq j$ si $\sigma \neq id$, tomando en

cuenta la previa numeración de las raíces, reescribiendo tenemos

$$\sigma(x) \equiv x + c \mod q \ \forall x \in I_q \ y \ c \in \mathbb{Z}^+,$$

así sea $\sigma \in \mathbf{H}$, entonces debe de existir b, $c \in \mathbb{Z}^+$ tal que

$$\sigma(x) \equiv bx + c \mod q \ \forall x \in I_q,$$

donde x es la posición de la raíz. Como buscamos una permutación que deje fijo por lo menos dos elementos, entonces buscamos una solución a

$$x \equiv bx + c \mod q$$

la cual tiene solución única en $\mathbb{Z}_q$, $x = [c]([1]-[b])^{-1}$, así cualquier permutación distinta de la identidad deja fijo solamente a un elemento, por lo cual la permutación que deja fijo a por lo menos dos elementos es la identidad. □

Teorema 5.1.1. *Sea $f(x)$ un polinomio de grado $q > 2$ primo, irreducible y soluble sobre un subcampo $\mathbf{F}$ de $\mathbb{R}$. Entonces, $f(x)$ tiene una única raíz real o todas sus raíces son reales.*

Demostración. Sea $\mathbf{E}$ un campo de descomposición de $f(x)$ sobre $\mathbf{F}$ y $\mathbf{H} \leq Gal(\mathbf{E} : \mathbf{F})$. Sabemos que la única permutación $\sigma \in \mathbf{H}$ que deja fijo por lo menos dos elementos, es la permutación idéntica (ver Proposición 5.1.1) y por otra parte como q es impar, afirmamos que $f(x)$ tiene por lo menos un raíz real, si tuviera dos o más, el automorfismo $\sigma \in Gal(\mathbf{E} : \mathbf{F})$, debería cumplir que $\sigma(z) = \bar{z}$, entonces σ dejaría fijas por lo menos a dos raíces de $f(x)$, entonces σ es la identidad, luego todas las raíces de $f(x)$ son reales. □

Proposición 5.1.2. *Sea $f(x)$ un polinomio irreducible sobre un subcampo $\mathbf{K}$ de $\mathbb{R}$ tal que el $grd[f(x)] = q \geq 5$ con q primo. Si $f(x)$ tiene exactamente n raíces reales, con $2 < n < q$, entonces no es soluble por radicales sobre $\mathbf{K}$.*

Demostración. Supongamos que $f(x)$ es soluble por radicales sobre $\mathbf{K} \subseteq \mathbb{R}$, entonces por el Teorema 5.1.1 tendría una raíz real, o todas sus raíces serían reales, lo cual contradice el hecho de que $f(x)$ tiene exactamente n raíces pues $2 < n < q$. □

Nota 5.1.1. *Observemos que tomamos $n > 2$ y no $n \geq 2$, pues si recordamos todo polinomio de grado impar sobre un subcampo de $\mathbb{R}$ que tenga por lo menos dos raíces reales, tiene por lo menos tres raíces reales.*

Proposición 5.1.3. *Sea $p(x) \in \mathbb{Q}[x]$ irreducible con $grd[p(x)] = 5$ con exactamente tres raíces reales, entonces el grupo de Galois de su campo de descomposición es isomorfo a S_5 y $p(x)$ no es soluble por radicales.*

Demostración. Sea $\mathbf{E}_p$ el campo de descomposición de $p(x)$ y $\mathrm{Gal}(\mathbf{E}_p : \mathbf{K}) = \mathbf{G}$ el grupo de Galois. Notemos que $p(x)$ no es soluble por radicales, pues si fuera soluble por radicales,

tendríamos que $\mathbf{G}$ es soluble por radicales y como $\mathbf{G} \cong S_5$, entonces S_5 sería un grupo soluble, lo que contradice el Teorema 2.3.4.

Ahora veamos que $\mathbf{G} \cong S_5$.
Sabemos que el grupo de Galois permuta las raíces de $p(x)$, de esta manera este grupo se puede identificar con un subgrupo $\mathbf{H}$ de S_5, es decir $\mathbf{G} \cong \mathbf{H}$. Sea $A = \{1, 2, 3, 4, 5\}$ el conjunto que denota las posiciones de las raíces de $p(x)$ previamente ordenadas, así para cualquiera $i, j \in A$ existe $\sigma \in \mathbf{H}$, tal que $\sigma(i) = j$, a esta propiedad se le denomina transitividad.
Recordemos que la conjugación compleja solo intercambia las dos raíces complejas, sin perdida de generalidad supongamos que (1 2) corresponde a la trasposición de las dos raíces complejas, vamos a probar que el único subgrupo transitivo de S_5 que contiene a (1 2) es S_5, para esto definimos en A la siguiente relación iRj si $i = j$ o $(i\ j) \in \mathbf{H} \rightarrow \{\sigma(i) = j$ para algún $\sigma \in \mathbf{H}\}$, además notemos que esta relación es de equivalencia, de esta manera todas las clases tienen la misma cantidad de elementos. Supongamos que hay c clases distintas y estas forman una partición en A, es decir $5 = \mid A \mid = c \mid [i] \mid$ en este caso para $\sigma \in \mathbf{H}$ donde σ es una trasposición simple, tenemos que $[i]$ tiene 5 trasposiciones simples, las cuales son $(1\ 2), (2\ 3), (3\ 4), (4\ 5), (5\ 1)$, por lo tanto $c = 1$, es decir solo hay una clase, de esta manera $\mathbf{H}$ contiene todas las trasposiciones de S_5, así $\mathbf{H} = \langle\sigma\rangle = S_5$. □

Resultados de no solubilidad por radicales

El siguiente teorema será de utilidad, su demostración la encontramos en cualquier libro de cálculo básico.

Teorema 5.1.2. *(**Teorema de Bolzano.**) Sea una función $f(x)$ continua definida en un intervalo $[a, b]$ entonces si se cumple que $f(a)f(b) < 0$ (es decir, $f(a) < 0$ y $f(b) > 0$, o $f(a) > 0$ y $f(b) < 0$), existe al menos un punto c perteneciente al intervalo (a, b) tal que $f(c) = 0$.*

Las siguientes proposiciones serán de utilidad para visualizar mejor cuándo un polinomio no es soluble por radicales.

Proposición 5.1.4. *Sean $q \geq 5$ con q primo y $a, b \in \mathbb{Q}$ tales que $1 < b < a - 1 < b^{q-1}$, si $f(x) = x^q - ax + b$ es irreducible sobre $\mathbb{Q}$, entonces no es soluble por radicales.*

Demostración. Como

$$\begin{aligned} f(0) &= b > 0 \\ f(1) &= 1 - a + b < 0 \\ f(b) &= b^q - ab + b = b(b^{q-1} - a + 1) > 0, \end{aligned}$$

pues $b < a - 1$, $b^{q-1} > a - 1$ y $f(x)$ es una función continua, entonces por el Teorema de Bolzano 5.1.2 su gráfica corta por lo menos dos veces al eje real, es decir $f(x)$ tiene por lo

menos dos raíces reales, lo cual implica que $f(x)$ tiene por lo menos tres raíces reales (ver nota 5.1.1).
Notemos que $f'(x) = qx^{q-1} - a$ y además $f'(0) = -a < 0$ y $f'(a) = qa^{q-1} - a > 0$, por el Teorema 5.1.2 y como $f(x)$ es no es reducible en $\mathbb{Q}[x]$, f' tiene solo dos raíces reales, esto es tiene a lo más dos puntos críticos y por tanto f corta al eje real en el mejor de los casos en tres puntos distintos.
De las observaciones anteriores se desprende que $f(x)$ tiene exactamente tres raíces reales, lo cual ímplica, por la Proposición 5.1.2 que $f(x)$ no es soluble por radicales. □

Otro resultado importante para determinar la no solubilidad por radicales de un polinomio es la siguiente proposición:

Proposición 5.1.5. *Sean $q \geq 5$ primo y $f(x) = x^q + a_{q-1}x^{q+1} + \cdots + a_3x^3 + a_0$ un polinomio irreducible sobre $\mathbb{Q}$. Si $f(x)$ tiene más de una raíz real, entonces no es soluble por radicales sobre $\mathbb{Q}$.*

Demostración. Si $f(x)$ tiene más de una raíz real entonces tiene por lo menos tres raíces reales pues q es impar (ver nota 5.1.1).
Por otra parte, como

$$f'(x) = x^2\left(qx^{q-3} + a_{q-1}(q-1)x^{q-4} + \cdots + 3a_3\right),$$

la ecuación $f'(x) = 0$ tiene, en el mejor de los casos, $q-2$ raíces distintas.
Por lo tanto hay a lo mas $q-2$ puntos críticos, lo cual implica que no se pueden presentar mas de $q-1$ cortes con el eje real, es decir no es posible que todas las raíces de $f(x)$ sean reales, como $f(x)$ es irreducible sobre $\mathbb{Q}$, no tiene raíces múltiples, entonces por la Proposición 5.1.2 podemos concluir que $f(x)$ no es soluble por radicales sobre $\mathbb{Q}$. □

Proposición 5.1.6. *Sean $q \geq 5$ y $p \geq 3$ con q, p primos, entonces el polinomio $f(x) = x^q + px^4 - p^2x^3 + p$ no es soluble por radicales sobre $\mathbb{Q}$.*

Demostración. Notemos que

$$\begin{aligned} f(0) &= p > 0 \\ f(p) &= p^q + p^5 - p^5 + p = p^q + p > 0 \\ f(1) &= 1 + p - p^2 + p = 1 + 2p - p^2 < 0, \end{aligned}$$

pues

$$1 + 2p - p^2 < p + 2p - p^2 \leq 3p - p^2 \leq p^2 - p^2 = 0.$$

Luego por el Teorema de Bolzano 5.1.2, tenemos que $f(x)$ tiene más de una raíz real, de esta manera estamos en las condiciones de la Proposición 5.1.5 y por tanto tenemos que $f(x)$ no es soluble por radicales sobre $\mathbb{Q}$. □

Como hemos visto, el criterio que se demostró en la Proposición 5.1.2, nos permite construir muchos ejemplos de polinomios no solubles, en general $\forall n \in \mathbb{Z}$, $n \geq 5$ siempre es posible encontrar, polinomios de grado n que no sean solubles por radicales. Además notemos que hay más resultados para determinar cuándo un polinomio no es soluble por radicales, que al contrario, es decir cuándo un polinomio si será soluble por radicales como vimos en el Capítulo 4.

5.1.1. El problema inverso

Recordemos que dado un polinomio $f(x) \in \mathbb{Q}[x]$, se puede calcular su grupo de Galois, ¿tendría sentido plantear el problema inverso?, es decir, dado un grupo finito **G**, ¿habría un polinomio $f(x)$ tal que su grupo de Galois sea isomorfo a **G**?
Si el campo de base **F** no se especifica, la respuesta es afirmativa. En efecto, dado un grupo **G**, digamos de orden n, consideramos un polinomio $f(x)$ separable de grado n, digamos con coeficientes en **F**, tal que su grupo de Galois sea S_n.

Teorema 5.1.3. ***Teorema de Cayley.*** *Todo grupo es isomorfo a un subgrupo de un grupo simétrico. Si el grupo es finito y tiene orden n, entonces es isomorfo a un subgrupo de* S_n.

Para la demostración véase [Her].

Proposición 5.1.7. *Todo grupo finito* **G** *es el grupo de Galois de algún polinomio.*

Demostración. Sea $\mathbf{E} : \mathbf{F}$ un campo de descomposición de $f(x)$. El Teorema de Cayley 5.1.3 asegura la existencia de $\mathbf{H} \leq S_n$ tal que $\mathbf{G} \cong \mathbf{H}$. Sea $\mathbf{E}^{\mathbf{H}}$ el campo que deja fijo a **H**, con **H** el conjunto de automorfismos de **E**. El teorema fundamental de la Teoría de Galois 2.2.1 garantiza que $Gal(\mathbf{E} : \mathbf{E}^{\mathbf{H}}) = \mathbf{H}$. Así, basta ver a $f(x)$ como un polinomio con coeficientes en $\mathbf{E}^{\mathbf{H}}$ para obtener que el grupo de Galois de $f(x)$ sobre $\mathbf{E}^{\mathbf{H}}$ es **H**, y por tanto isomorfo a **G**. □

Sin embargo, si se requiere que el campo de base sea $\mathbb{Q}$, el problema se vuelve mucho mas difícil, tanto que aún no se conoce una solución general.
En 1954 el matemático ruso Safarevich probó que tal polinomio $f(x)$ existe si **G** es soluble, se puede consultar algunos resultados parciales en [Rom]. En lo que resta de este capítulo, para $f(x) \in \mathbb{Q}[x]$, denotaremos como $Gal(f)$ al grupo de Galois de $f(x)$ sobre $\mathbb{Q}$. La teoría de grupos necesaria puede consultarse en [Rot1].
Supongamos que tenemos el siguiente problema.
Dado $\mathbf{H} \leq S_4$, hallar $f(x) \in \mathbb{Q}[x]$ tal que el grupo de Galois de $f(x)$ sea isomorfo a **H**.
Para intentar solucionar este problema primero necesitariamos determinar todos los subgrupos **H** de S_4.
Como $| S_4 | = 24$, por el Teorema de Lagrange 1.1.1 los posibles órdenes para **H** son 24, 12, 8, 6, 4, 3, 2 y 1. Los casos $|\mathbf{H}| = 24$ y $|\mathbf{H}| = 1$ son triviales.

Si $|\mathbf{H}| = 12$, entonces el índice es $[\mathbf{G} : \mathbf{H}] = 2$ y por tanto $\mathbf{H} \lhd \mathbf{G}$. Como los únicos subgrupos normales de S_4 son A_4 y V (el 4-grupo de Klein), así $\mathbf{H} \cong A_4$ y $\mathbf{H} \cong V$.

Si $|\mathbf{H}| = 8$, los teoremas de Sylow garantizan que la cantidad de subgrupos de S_4 de orden 8 es un número congruente con 1 módulo 2 (ver Teorema 1.1.5), es decir un número impar, que divide a 24, por lo tanto, es 1 o 3. Si hubiera uno, sería normal en S_4, pero $|A_4| \neq 8 \neq |V|$, así que hay 3, además los teoremas de Sylow aseguran que dos cualesquiera de estos $\mathbf{H}$'s son conjugados (ver Teorema 1.1.4), así que $\mathbf{H}$ es único salvo isomorfismos, entonces $\mathbf{H}$ es un 2−subgrupo de Sylow (ver Teorema 1.1.3) de S_4 y como $D_{2(4)}$ es el único grupo diédrico de orden 8 que es subgrupo de S_4, tenemos que $\mathbf{H} \cong D_{2(4)}$, donde el grupo diédrico es un grupo finito formado por las simetrías de un polígono regular (rotaciones y reflexiones).

Si $|\mathbf{H}| = 6$, $\mathbf{H} \cong \mathbb{Z}_6$ o $\mathbf{H} \cong S_3$, como en S_4 no hay elementos de orden 6, entonces $\mathbf{H} \cong S_3$ y además $\mathbf{H}$ tiene que ser de los subgrupos de S_4, dejan fijo a un elemento.

Si $|\mathbf{H}| = 4$, $\mathbf{H} \cong V$ o $\mathbf{H} \cong \mathbb{Z}_4$. Si $|\mathbf{H}| = 3$, $\mathbf{H} \cong \mathbb{Z}_3 \cong A_3$. Si $|\mathbf{H}| = 2$, $\mathbf{H} \cong \mathbb{Z}_2$.

De esta manera tenemos que $\mathbf{H}$ es isomorfo a $S_4, A_4, D_{2(4)}, S_3, V, \mathbb{Z}_4, A_3, \mathbb{Z}_2$ *o* 1.

Con lo anterior conocemos los grupos a los que podría ser isomorfo el $\mathrm{Gal}(f)$, pero sigue la incógnita acerca del polinomio, como antes ya se mencionó no es facíl encontrar este polinomio pero daremos algunos ejemplos.
Demos ahora los polinomios en $\mathbb{Q}[x]$ pedidos.
Recordemos que para $f(x) \in \mathbb{Q}[x]$, con $f(x)$ un polinomio cúbico e irreducible, 3 divide a $|Gal(f)|$, por lo que $Gal(f)$ es isomorfo a S_3 ó A_3 ver la Proposición 3.2.3. Además en [Rot1] se puede ver que el discriminate para un polinomo de la forma $x^3 + qx + r \in \mathbb{Q}[x]$ es $\triangle = -4q^3 - 27r^2$, y que se puede relacionar al grupo de Galois asociado a este polinomio dependiendo de lo siguiente, diremos que $\triangle$ es un cuadrado en $\mathbb{Q}$, si $\triangle$ es de la forma $\left(\frac{p}{q}\right)^2$ con $(p, q) = 1$, $p, q \in \mathbb{Z}$, entonces

a) Si $\triangle$ no es un cuadrado en $\mathbb{Q}$, entonces $Gal(f) \cong S_3$.

b) Si $\triangle$ es un cuadrado en $\mathbb{Q}$, entonces $Gal(f) \cong A_3$. (ver [Rot1])

Ejemplo 5.1.1. *a) Si $Gal(f) \cong 1$, el polinomio es $f(x) = x$.*

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

c) Si $Gal(f) \cong A_3$, el polinomio es $f(x) = x^3 - 3x + 1$, pues es un polinomio de grado tres $f(x)$ que no tiene raíces racionales y es irreducible sobre $\mathbb{Q}$ y además su discriminante es

$$-4(-3)^3 - 27(1)^2 = 81 = 9^2,$$

es decir $\sqrt{D} \in \mathbb{Q}$.

d) Si $Gal(f) \cong S_3$, *el polinomio buscado es* $f(x) = x^3 - 2$, *el cual es irreducible sobre* $\mathbb{Q}$, *por no tener raíces racionales o por el criterio de Eisenstein 4.1.5, y además su discrminante es* -108.

Ejemplo 5.1.2. *Si* $Gal(f) = (\mathbb{Q}(w_k) : \mathbb{Q}) \cong S_4$, *sabemos por el ejemplo 4.2.1 del Capítulo 4, que el polinomio*

$$f(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1} = \prod_{k=1}^{4} (x - w_k),$$

tiene como grupo de Galois asociado a $S_4 = \langle \sigma \rangle = \langle (2\ 4\ 3\ 1) \rangle$. *En este caso el polinomio buscado es* $\Phi_5(x) = \dfrac{x^5 - 1}{x - 1}$, *el cual es el quinto polinomio ciclotómico y donde* w_k *es una raíz quinta primitiva de la unidad.*

5.2. Polinomio no soluble por radicales, con grupo de galois soluble

Hemos analizado cuando un polinomio es soluble por radicales, y acuando no será soluble por radicales, pero podemos plantearnos la idea de que exista un polinomio que no sea soluble por radicales pero que su grupo de Galois asociado si sea soluble, veremos que este polinomio si existe y además lo exhibiremos. Recordemos el siguiente teorema.

Teorema 5.2.1. *(**Pequeño teorema de Fermat.**) Si p es un número primo, entonces para cada número natural a, con* $a > 0$, $a^p \equiv a \mod p$.

Para la demostración véase [Fra].
De entrada, el gran Teorema de Galois 3.2.1 nos orienta a buscar el ejemplo en un campo de característica positiva. Probemos primero una proposición, tomado de [Rot2].

Proposición 5.2.1. *Si p es primo y* $\mathbf{K} = \mathbb{Z}(t)$, *el campo de funciones racionales sobre el campo* $\mathbb{Z}_p$, *entonces* $f(x) = x^p - x - t$ *no tiene raíces en* $\mathbf{K}$.

Demostración. Si hubiera una raíz α de $f(x)$ en $\mathbf{K}$, habrían $g(t)$, $h(t) \in \mathbb{Z}_p(t)$ con $\alpha = \dfrac{g(t)}{h(t)}$, podemos suponer que $(g,\ h) = 1$. Como α es raíz de $f(x)$, tenemos que

$$\begin{aligned} t &= \alpha^p - \alpha \\ &= \left(\frac{g(t)}{h(t)}\right)^p - \left(\frac{g(t)}{h(t)}\right), \end{aligned}$$

la cual es una ecuación en $\mathbb{Z}_p(t)$, entonces

$$g^p - h^{p-1} g = t h^p, \tag{5.1}$$

así $g \mid th^p$, como $(g,\ h) = 1$, tenemos $g \mid t$, por lo que $g(t) = at$ o $g(t)$ es constante, digamos $g(t) = b$, donde $a, b \in \mathbb{Z}_p$. De la ecuación (5.1) tenemos que $h \mid g^p$, y como $(g,\ h) = 1$ necesariamente h es constante, ahora, sin perdida de generalidad tenemos que $\alpha = at$ o $\alpha = b$.
Si $\alpha = at$, por el pequeño Teorema de Fermat 5.2.1 tenemos que $a^p = a$ en $\mathbb{Z}_p$, ocurre que

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

Se sigue que $at^{p-1} - a - 1 = 0$, así $a \neq 0$, pero t es trascendente en $\mathbb{Z}_p$ pues no es solución del polinomio $f(x) = x^p - x - t$, entonces se contradice este hecho.
Si $\alpha = b \in \mathbb{Z}_p$, por el Teorema 5.2.1 tenemos que $b^p = b \in \mathbb{Z}_p$, así $0 = f(\alpha) = f(b) = b^p - b - t = -t \neq 0$, de esta manera tenemos que $\alpha \notin \mathbf{K}$. □

Proposición 5.2.2. *Sean p un primo, $\mathbf{F} = \mathbb{Z}_p(t)$ y $f(x) = x^p - x - t \in \mathbf{F}[x]$, el grupo de Galois de $f(x)$ sobre $\mathbf{F}$ es isomorfo a $\mathbb{Z}_p$, es decir $Gal(f : \mathbf{F}) \cong \mathbb{Z}_p$.*

Demostración. Veamos que el grupo de Galois de $f(x)$ sobre $\mathbf{F}$ es de orden p, y de esta manera $\mathrm{Gal}(f) \cong \mathbb{Z}_p$.
Sea α una raíz de $f(x)$ y sea $\mathbf{E} = \mathbf{F}(\alpha)$. Por el Teorema de Fermat 5.2.1, en $\mathbb{Z}_p$ para i tenemos que $i^p = i$, así para $i = 0, \cdots, p-1$ se tiene que

$$\begin{aligned} f(\alpha + i) &= (\alpha + i)^p - (\alpha + i) - t \\ &= \alpha^p + i^p - \alpha - i - t \\ &= \alpha^p + i - \alpha - i - t \\ &= \alpha^p - \alpha - t = f(\alpha) = 0 \end{aligned}$$

de esta manera $\alpha + i$ es raíz de $f(x)$ y además hay p raíces, como $f(x)$ es de grado p, ésas son todas sus raíces, y por tanto $\mathbf{E} = \mathbf{F}(\alpha)$ es un campo de descomposición de $f(x)$ sobre $\mathbf{F}$, y como todas son distintas, el polinomio es separable. Verifiquemos ahora que es irreducible sobre $\mathbf{F}$. Supongamos que $f(x) = u(x)v(x)$, con

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

y $0 < d < p$. Tenemos que $u(x)$ es el producto de d factores de la forma $x - (\alpha + i)$,

$$u(x) = \prod_{\substack{r=1 \\ i_r \in \mathbb{Z}_p}}^{d} (x - (\alpha + i_r)),$$

pues $\alpha + i$ es raíz de $f(x)$, de esta manera tendremos que $-c_{d-1}$ es la suma de las raíces, pues

$$\begin{aligned} c_{d-1} &= (-\alpha - i_1) + (-\alpha - i_2) + (-\alpha - i_3) + \cdots + (-\alpha - i_d) \\ &= -d\alpha - (i_1 + i_2 + \cdots + i_d) \\ &= -d\alpha - j, \end{aligned}$$

así que $-c_{d-1} = d\alpha + j$, para alguna $j \in \mathbb{Z}_p \subseteq \mathbf{F}$, por lo tanto, $d\alpha \in \mathbf{F}$. Como $0 < d < p$, tenemos que $d \neq 0$ en $\mathbf{F}$, obligando a que $\alpha \in \mathbf{F}$, lo cual contradice la Proposición 5.2.1, ahora ya que $f(x)$ es un polinomio irreducible de grado p, sabemos que $|\ \mathbf{E} : \mathbf{F}\ | = |\ \mathbf{F}(\alpha) : \mathbf{F}\ | = p$ (ver Proposición 4.1.2), y como $f(x)$ es separable, tenemos que $|\ Gal(\mathbf{E} : \mathbf{F})\ | = |\ \mathbf{E} : \mathbf{F}\ | = p$ (ver Proposición 3.2.2 y Teorema 4.1.4). Así, el grupo de Galois de $f(x)$ sobre $\mathbf{F}$ es $Gal(\mathbf{E} : \mathbf{F}) \cong \mathbb{Z}_p$. □

Proposición 5.2.3. *Sea* $\mathbf{E} : \mathbf{K}$ *una extensión normal y finita. Si p es un polinomio irreducible y* $\alpha,\ \beta \in \mathbf{E}$ *son raíces en p, entonces existe* $\sigma \in Gal\,(\mathbf{E} : \mathbf{K})$ *tal que* $\sigma\,(\alpha) = \beta$.

Para la demostración véase [Ste].

Proposición 5.2.4. *El polinomio* $f(x) = x^p - x - t \in \mathbf{F}[x]$ *no es soluble por radicales.*

Demostración. Supongamos que $f(x)$ es soluble por radicales, entonces existe una torre radical

$$\mathbf{F} = \mathbf{B}_0 \subseteq \mathbf{B}_1 \subseteq \cdots \subseteq \mathbf{B}_r,$$

con $\mathbf{E}_f \subseteq \mathbf{B}_r$. Supongamos que para $i = 1,\ 2, \cdots,\ r$ la extensión $\mathbf{B}_i : \mathbf{B}_{i-1}$ es pura de tipo primo, es decir si $\mathbf{B}_{i-1}$ tiene una raíz q_i-ésima, con q_i primo, $(x^{q_i} - 1 = 0)$, con u_i una raíz primitiva de la unidad, entonces $\mathbf{B}_i = \mathbf{B}_{i-1}\,(u_i)$, donde $u_i^{q_i} \in \mathbf{B}_{i-1}$. Como $\alpha \in \mathbf{B}_r$, pero $\alpha \notin \mathbf{B}_0$ $(\alpha \in \mathbf{B}_r - \mathbf{B}_0)$, por la Proposición 5.2.3 hay un $j \in \{1, \cdots, r\}$ tal que $\alpha \in \mathbf{B}_j - \mathbf{B}_{j-1}$, es un hecho conocido en [Rot2], o [Rot1] corolario 7, que el polinomio $x^{q_i} - u_i^{q_i} \in \mathbf{B}_{i-1}\,[x]$ no se descompone sobre $\mathbf{B}_{i-1}$, pues $u_i \notin \mathbf{B}_{i-1}$ es irreducible sobre $\mathbf{B}_{i-1}$ por lo tanto $|\ \mathbf{B}_i : \mathbf{B}_{i-1}\ | = q_i$ (ver Proposición 4.1.2). Entonces $\mathbf{B}_i : \mathbf{B}_{i-1}$ no tiene campos intermedios. Tenemos que

$$\mathbf{B}_{i-1} \subsetneq \mathbf{B}_{i-1}(\alpha) \subseteq \mathbf{B}_i$$

por lo que $\mathbf{B}_i = \mathbf{B}_{i-1}(\alpha)$. Ahora de manera análoga a como vimos que $f(x)$ es irreducible sobre $\mathbb{Z}_p$, también se tiene que lo es sobre $\mathbf{B}_{i-1}$. Entonces, α es raíz del polinomio irreducible $f(x) \in \mathbf{B}_{i-1}[x]$, de manera que $q_i = |\ \mathbf{B}_i : \mathbf{B}_{i-1}\ | = |\ \mathbf{B}_{i-1}(\alpha) : \mathbf{B}_{i-1}\ | = p$ (ver Proposición 4.1.2). Ahora, como $\mathbf{B}_{i-1}(\alpha) : \mathbf{B}_i$ es el campo de descomposición del polinomio separable $f(x) \in \mathbf{B}_{i-1}[x]$, y además la extensión $\mathbf{B}_i : \mathbf{B}_{i-1}$ es de Galois, y en particular separable (ver definición 2.1.12). Por lo tanto, $u_i \in \mathbf{B}_i$ es un elemento separable. Pero el polinomio irreducible de u_i sobre $\mathbf{B}_{i-1}$ es $x^{q_i} - u_i^{q_i} = (x - u_i)^{q_i} = (x - u_i)(x - u_i)^{q_i - 1}$, es decir el polinomio irreducible de u_i tiene raíces repetidas, lo cual no es posible. La contradicción provie-

ne de la suposición de que $f(x)$ es soluble por radicales, por lo tanto, no es soluble por radicales. □

De está manera hemos dado $f(x) = x^p - x - t$ un polinomio no soluble por radicales, cuyo grupo de Galois asociado es tal que $\mathrm{Gal}(f : \mathbf{F}) \cong \mathbb{Z}_p$ y sabemos que $\mathbb{Z}_p$ es soluble por radicales. Además este ejemplo muestra que en el enunciado del gran Teorema de Galois no se puede omitir la hipótesis de que la característica del campo sea 0. Cabe señalar que la definición de solubilidad por radicales se puede extender, debilitándola, a campos de característica arbitraria para que no sea necesario imponer tal hipótesis.

Bibliografía

[Art] Artin, M., ***Algebra.*** Prentice Hall, New Jersey, 1991.

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

[Art1] Artin, E., ***Galois Theory.*** Lectures Delivered at the University of Notre Dame, 2nd Edition, London: University of Notre Dame, 1944.

[Cox] Cox, David, A., ***Galois Theory.*** Amherst Collegue, Amherst, MA: Departament of Mathematics and Computer Science.

[Fra] Fraleigh, John B., ***A first course in abstract algebra.*** 3 th Edition, Pearson Education India, 2003.

[Hun] Hungerford, T., ***Algebra.*** 2nd Edition, Springer-Verlag, New York, 1974.

[Her] Herstein, I. N., ***Álgebra Moderna.*** 1ra Edición, Trillas, México, 1970.

[Mor] Morandi, P., ***Fields and Galois Theory.*** New York: Springer, 1996.

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

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

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

[Ste] Stewart, I., ***Galois Theory.*** 3 th Edition, London: Chapman and Hall, 2004.

[Jon] Jones, J., Jones, G., ***Elementary Number Theory.*** Springer, London, 1998.