USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Trabajo Fin de Grado

Un enfoque constructivo del problema inverso de Galois

David Quiroga Gutiérrez

2023/2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRADO DE MATEMÁTICAS

Trabajo Fin de Grado

Un enfoque constructivo del problema inverso de Galois

David Quiroga Gutiérrez

Julio, 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra

Título: Un enfoque construtivo do problema inverso de Galois

Breve descrición do contido

A teoría de Galois é unha disciplina esencial das matemáticas e conecta moitas ramas diferentes ao establecer unha ligazón entre a teoría de grupos, corpos e os polinomios.

En concreto, a teoría de Galois permite asociar a unha extensión finita dun corpo un grupo finito, chamado o grupo de Galois, ou asociar a un polinomio o grupo de Galois do seu corpo de escisión.

O problema inverso de Galois expón a enigmática cuestión de se para calquera grupo finito G, existe un polinomio cuxo grupo de Galois sobre o corpo dos números racionais é G? Este problema, exposto por primeira vez no século XIX, segue sen resolverse. Este enigma matemático é parte da motivación deste traballo. Outro acicate é enfocalo desde o punto de vista construtivo e computacional, é dicir, atopar polinomios ou familias de polinomios que teñan certos grupos como o seu grupo de Galois.

Bibliografía

H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1996.

C. U. Jensen, A. Ledet, N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, Cambridge, 2002.

Recomendacións (non vinculantes)

Índice general

Resumen

O problema inverso de Galois expón a enigmática cuestión de se para calquera grupo finito G, existe un polinomio cuxo grupo de Galois sobre o corpo dos números racionais é G. Este problema, exposto por primeira vez no século XIX, segue sen resolverse, e é parte da motivación deste traballo. Outro acicate é enfocalo desde o punto de vista construtivo e computacional, é dicir, atopar polinomios cuxo grupo de Galois sexa un grupo dado.

Abstract

The inverse Galois problem poses the enigmatic question of whether for any finite group G, there is a polynomial whose Galois group over the field of rational numbers is G. This problem, first posed in the 19th century, remains unsolved, and this mathematical puzzle is part of the motivation of this work. Another incentive is to approach it from a constructive and computational point of view, finding polynomials whose Galois group is a given group.

Introducción

Évariste Galois (1811–1832) fue un brillante matemático francés que tan sólo con 20 años revolucionó el mundo del álgebra abstracta: Descubrió una condición necesaria y suficiente para que las ecuaciones algebraicas fueran resolubles por radicales. Para explicar su teoría definió los llamados "Grupos de Galois", y asignó a cada extensión algebraica de cuerpos uno de estos grupos, compuestos por $\mathbb{Q}$-automorfismos que permutaban las raíces del polinomio que generaba la extensión. Estos grupos estaban dotados de unas características concretas, en función del polinomio que los generaba. Una de esas características, la resolubilidad, determinaba esa condición necesaria y suficiente para que tal polinomio fuera resuelto por radicales.

Ante este descubrimiento tan grande, cabe esperar que la contribución de Galois al álgebra marcase un antes y un después en la historia de las matemáticas, pero, desgraciadamente, murió en un duelo por amor el 30 de mayo de 1832, a la edad de 20 años.

Es más, sus revolucionarios trabajos fueron reconocidos de manera póstuma, ya que, asumiendo la posible derrota en aquel fatídico duelo, pasó a limpio todos sus apuntes el día antes de morir, y los dejó en manos de su mejor amigo para que los entregase en la Academia de París. Allí fueron estudiados en profundidad y aceptados con la importancia que merecían, inaugurando lo que hoy conocemos como *Teoría de Galois*, la cual abrió debates en el mundo del álgebra y dio lugar a una gran cantidad de incógnitas surgidas de esta innovadora manera de entender las ecuaciones algebraicas.

Una de esas incógnitas fue bautizada por Hilbert como *Problema inverso de Galois*, y planteaba una pregunta natural derivada del Teorema Fundamental de la Teoría de Galois. Recordemos que este teorema establece una biyección entre las subextensiones de una extensión algebraica $E|K$, y los subgrupos del grupo de Galois (de la extensión E sobre K). Pues bien, en el *Problema inverso de Galois* se estudia si dado un grupo finito G, existe una extensión de Galois $E|K$ tal que su grupo de Galois es isomorfo a G.

Esta enigmática cuestión es la que abordaremos en el presente trabajo, pero considerando K como el cuerpo de los números racionales $\mathbb{Q}$, y tratando el problema en subgrupos de S_n con $n \leq 3$, en grupos cíclicos, abelianos finitos y, en general, para todos los grupos simétricos S_n.

De todas maneras, se trata de un problema abierto, ya que no tiene solución para todos los grupos finitos conocidos. Por ejemplo, no se conoce la solución de este problema para el grupo de Mathieu M_{23}, de orden 10 200 960. De hecho es el único grupo simple esporádico de los 26 grupos simples esporádicos que no se conoce solución. Otros ejemplos son los grupos simples de tipo Lie, como el grupo lineal especial proyectivo $\mathrm{PSL}_2(\mathbb{F}_{3^3}) = \mathrm{SL}_2(\mathbb{F}_{3^3})/Z\ \mathrm{SL}_2(\mathbb{F}_{3^3})$ de orden 9828, o el grupo unitario especial proyectivo $\mathrm{PSU}_3(\mathbb{F}_{3^2}) = \mathrm{PSU}_3(\mathbb{F}_{3^2})/Z\ \mathrm{PSU}_3(\mathbb{F}_{3^2})$, de orden 42 573 600.

En este trabajo abordaremos el Problema Inverso de Galois considerando K como el cuerpo de los números racionales $\mathbb{Q}$, y tratando el problema de manera constructiva, es decir, durante las demostraciones que llevemos a cabo ya daremos un método para construir un polinomo cuyo grupo de Galois sea el requerido en cada capítulo.

La estructura del trabajo se divide en cinco capítulos. El primero 1 se corresponde con resultados sobre teoría de grupos (Teoremas de Isomorfía, el grupo simétrico, Teoría de Sylow, ...), teoría de cuerpos, en la que introducimos los resultados que emplearemos en el trabajo sobre la Teoría de Galois, y polinomios ciclotómicos.

En el segundo capítulo 2 se empieza resolviendo el Problema Inverso de Galois para los subgrupos de S_n con $n \leq 3$. Este capítulo es una pequeña iniciación al problema, ya que se pueden emplear razonamientos elementales para hallar la solución.

En el tercer capítulo 3 se estudia la solución al problema en grupos cíclicos finitos. Para ello, cobran gran importancia los polinomios ciclotómicos, porque el grupo de Galois de una extensión ciclotómica p-ésima es $(\mathbb{Z}/p\mathbb{Z})^*$, así que trabajando con cuerpos fijos por subgrupos de $(\mathbb{Z}/p\mathbb{Z})^*$, y empleando ciertos resultados derivados del Pequeño Teorema de Fermat, ya obtenemos el polinomio deseado para un grupo cíclico de cualquier orden finito.

En el cuarto capítulo 4 se resuelve el problema para grupos abelianos finitos, empleando el Teorema Fundamental de los Grupos Abelianos Finitos, el cual nos proporciona una relación muy estrecha con los grupos cíclicos finitos. Por tanto, se emplearán razonamientos ya utilizados en el capítulo anterior.

Y para terminar, en el quinto capítulo 5 resolveremos el problema para grupos simétricos, empleando el Teorema de Dedekind, el polinomio $x^{p^n} - x \in \mathbb{F}_p[X]$, y construyendo directamente el polinomio cuyo grupo de Galois sea S_n.

Cada uno de los capítulos (a excepción del primero) van acompañados de código de SageMath `https://www.sagemath.org/` para resolver el problema en cada uno de los gru-

pos que se proponen. Empleamos este software de código abierto porque goza de bastantes herramientas para resolver problemas relacionados con la Teoría de Galois, como lo es el planteado.

Capítulo 1

Resultados preliminares

Para empezar, citaremos un conjunto de resultados y definiciones sobre la teoría de grupos y cuerpos, que serán de gran utilidad para el tratamiento del presente problema. Para el desarrollo de esta memoria, usaremos las siguientes referencias [1, 2, 3, 4].

1.1. Teoría de Grupos

Un grupo es un par $(G, \cdot)$ donde G es un conjunto y $\cdot$ es una operación interna que satisface las siguientes condiciones:

- Asociatividad; $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, para todo $x, y, z \in G$.
- Existencia de un elemento neutro ($e \in G$ tal que $x \cdot e = x = e \cdot x$, para todo $x \in G$).
- Todo elemento de G tiene simétrico ($x' \in G$ tal que $x \cdot x' = e = x' \cdot x$).

Solemos referirnos al simétrico de un elemento como inverso, y denotarlo por x^{-1}.

Definición 1.1. Sea H un subconjunto de G no vacío, decimos que H es un *subgrupo* de G si $(H, \cdot)$ es un grupo. Lo denotaremos $H < G$.

Sea $N < G$, se dice que N es un *subgrupo normal* de G ($N \lhd G$) si $aNa^{-1} \subset N$, $\forall a \in G$.

Un grupo se dice *simple* si un es grupo no trivial y no tiene subgrupos normales propios.

Observación 1.2. En un grupo conmutativo todos los subgrupos son normales.

Definición 1.3. Sea $X \subset G$, el subgrupo generado por X se define como el menor subgrupo de G que contiene a X

$$\langle X \rangle = \bigcap_{H<G, X \subset H} H$$

Diremos que un subgrupo es cíclico si está generado por un sólo elemento (existe un $x \in G$ tal que $G = \langle x \rangle$).

Proposición 1.4. *Todo grupo cíclico es abeliano.*

Definición 1.5. Definimos el orden de un grupo $|G|$ como el número de elementos del grupo. Así, el orden de un elemento de G, $|x|$, será el número de elementos de $\langle x \rangle$.

Observación 1.6. Si el orden del grupo coincide con el orden de un elemento del grupo, entonces el grupo es cíclico (existirá un $x \in G$ tal que $|G| = |x| \Longrightarrow G = \langle x \rangle$).

1.1.1. Teorema de Lagrange

Definición 1.7. Dado un subgrupo $H < G$, definimos la siguiente relación de equivalencia:

$$x \sim y \iff x^{-1} \cdot y \in H.$$

Cuyas clases de equivalencia serán

$$[x] = \{y \in G \mid x \sim y\} = \{x^{-1} \cdot y = h \in H\} = x \cdot H.$$

Y el conjunto cociente se denotaría por:

$$G/H = \{[x] \mid x \in G\} = \{x \cdot H \mid x \in G\}.$$

Teorema 1.8. *(Teorema de Lagrange). Sea G un grupo finito y H subgrupo de G, se cumple que $|G| = |H|[G : H]$, siendo $[G : H]$ el índice de H en G (el orden del grupo cociente G/H).*

Corolario 1.9. *Todo grupo de orden primo es cíclico.*

Demostración. Por el Teorema de Lagrange 1.8, el orden de cada elemento tiene que dividir al orden del grupo p, y por ser p un número primo, el orden del elemento será 1 en el caso del neutro, y p en el caso de cualquier elemento no neutro. Lo cual hace que el grupo sea cíclico. □

Proposición 1.10. *Dados dos enteros positivos m, n tal que $\gcd(m, n) = 1$, se cumple que:*

$$\frac{\mathbb{Z}}{n \cdot m\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

1.1.2. Teoremas de Isomorfía

Definición 1.11. Una aplicación $f : G \longrightarrow G'$ es un homomorfismo de grupos si $f(x \cdot y) = f(x) \cdot f(y)$, para $x, y \in G$.

- Definimos el núcleo del homomorfismo f como $\ker(f) = \{x \in G \mid f(x) = 1\}$ (considerando 1 el elemento neutro).
- Definimos la imagen de f como $\mathrm{Im}(f) = \{y \in G' \mid f(x) = y, x \in G\}$.

Proposición 1.12. *Sea $f : G \longrightarrow G'$ un homomorfismo de grupos*

- *f inyectiva* $\iff \ker(f) = 1$.
- *f sobreyectiva* $\iff \mathrm{Im}(f) = G'$.

Teorema 1.13. *(Primer Teorema de Isomorfía). Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, entonces*

$$\frac{G}{\ker(f)} \simeq \mathrm{Im}(f).$$

Teorema 1.14. *(Segundo Teorema de Isomorfía). Sea G un grupo, $H, K \lhd G$ subgrupos normales de G con $K \subset H$ entonces se tiene:*

$$\frac{G/K}{H/K} \simeq G/H.$$

Teorema 1.15. *(Teorema de Correspondencia). Sea $f : G \longrightarrow G'$ un homomorfismo sobreyectivo de grupos, se verifica que la aplicación:*

$$\begin{aligned} f : \{T \mid T < G, \ker(f) \subset T\} &\longrightarrow \{\textit{subgrupos de } G'\} \\ T &\longmapsto f(T) \end{aligned}$$

es biyectiva, y su inversa es β definida por

$$\beta(T') = f^{-1}(T'), \quad T' < G'$$

1.1.3. Acciones de grupos en conjuntos

Sea G un grupo (con la operación $\cdot$) y X un conjunto arbitrario, una acción de G en X por la izquierda es una aplicación

$$\begin{aligned} f : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g * x \end{aligned}$$

verificando las siguientes condiciones:

- $g * (g' * x) = (g \cdot g') * x$, $g, g' \in G$, $x \in X$.
- $1 * x = x$, $x \in X$.

Definición 1.16. Para cada $x \in X$ se define:

- Grupo de isotropía o estabilizador de x; $G_x = \{g \in G \text{ tal que } g * x = x\} \subset G$.
- Órbita de x; $Gx = \{g * x \text{ tal que } g \in G\} \subset X$.

Proposición 1.17. *Si G es un grupo finito, entonces $|Gx| = |G/G_x| = |G|/|G_x|$.*

La demostración de esta proposición se basa en comprobar que la aplicación

$$\begin{aligned} f : Gx &\longrightarrow G/G_x \\ g * x &\longmapsto g * G_x \end{aligned}$$

es biyectiva.

Teorema 1.18. *(Fórmula de las clases). Si G finito (actuando sobre X), se verifica:*

$$|X| = \sum |Gx|.$$

Observación 1.19. En este teorema y en la anterior proposición, denotamos $|\cdot|$ como el cardinal del conjunto (número de elementos).

1.1.4. Grupo simétrico

Sea X un conjunto, $S_X = \{f \colon X \longrightarrow X \mid f \text{ biyectiva }\}$, se tendrá que $(S_X, \circ)$ es un grupo (siendo $\circ$ la composición de aplicaciones):

- La identidad es el elemento neutro.
- Por ser biyectivas todas las aplicaciones, su composición será biyectiva (y definida sobre X).

- La inversa de las aplicaciones de S_X también será biyectiva.

Si $X = \{1, \ldots, n\}$ denotaremos S_X como S_n y lo llamaremos grupo de permutaciones o grupo simétrico.

Para describir cada permutación, solemos denotarlas $\sigma \in S_n$ tal que:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. \tag{1.1}$$

Observación 1.20. $|S_n| = n!$.

Definición 1.21. Un ciclo de orden r es una permutación σ de r elementos $a_1, \ldots, a_r$ tales que

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_r) = a_1.$$

Y una trasposición es un ciclo de orden 2.

Teorema 1.22. *Toda permutación se puede descomponer en producto de ciclos, actuando sobre conjuntos disjuntos, de manera única (salvo orden de los factores).*

Todo ciclo se puede descomponer en producto de trasposiciones.

Definición 1.23. El signo de una permutación σ es $(-1)^{\text{n}^\text{o} \text{ trasposiciones}}$, si es -1 se dice que σ es impar, si es 1 se dice permutación par.

Definición 1.24. El conjunto $A_n = \{\sigma \in S_n \mid sign(\sigma) = 1\}$ es el subgrupo alternado de S_n.

Proposición 1.25. *A_n es un subgrupo normal de S_n y $|A_n| = \frac{|S_n|}{2}$.*

Teorema 1.26. *(Teorema de Cayley). Todo grupo es isomorfo a un grupo de permutaciones, y, en particular, si G es de orden n, entonces es isomorfo a un subgrupo de S_n*

Demostración. Sea G un grupo arbitrario, para cada $a \in G$, la aplicación $\gamma_a : G \longrightarrow G$ definida por $\gamma_a(x) = a \cdot x$ es una aplicación biyectiva ($\gamma_a^{-1}(y) = a^{-1} \cdot y = \gamma_{a^{-1}}(y)$).

Consideramos ahora $\gamma : G \longrightarrow S_G$ tal que $\gamma(a) = \gamma_a$, veamos que es un isomorfismo de grupos entre G e $\text{Im}(\gamma)$:

- $\gamma(a \cdot b) = \gamma(a) \circ \gamma(b)$ porque $\gamma(a \cdot b) = \gamma_{a \cdot b}$, y además, $\gamma_{a \cdot b}(x) = a \cdot b \cdot x = a \cdot \gamma_b(x) = \gamma_a(\gamma_b(x)) = \gamma_a \circ \gamma_b(x), \forall x \in G$, por lo tanto es un homomorfismo de grupos.
- La inyectividad se sigue de que $\gamma(a) = \gamma_(b) \iff \gamma_a(x) = \gamma_b(x), \forall x \in G \iff a = b \iff \gamma$ inyectiva.
- Por ser homomorfismo de grupos, $\text{Im}(\gamma) < S_G$.

Así tenemos que todo grupo es isomorfo a un subgrupo de su grupo de permutaciones, lo cual también es un grupo de permutaciones.

□

1.1.5. Teorema de Sylow

Definición 1.27. G se dice p-grupo si $|G|$ es una potencia de p. Así, un subgrupo $H < G$ se dirá p-subgrupo si es un p-grupo.

Un subgrupo $S < G$ es un p-subgrupo de Sylow si $|S|$ es la mayor potencia de p que divide a $|G|$.

Teorema 1.28. *(Teorema de Sylow). Sea G un grupo finito, con p primo dividiendo a $|G|$, se verifica:*

- *G tiene p-subgrupos de Sylow, y cada p-subgrupo está contenido en un p-subgrupo de Sylow.*
- *Todos los p-subgrupos de Sylow de G son conjugados (es decir, que si S es p-subgrupo de Sylow, entonces gSg^{-1} también es p-subgrupo de Sylow, $g \in G$).*
- *Si S es p-subgrupo de Sylow, el número de p-subgrupos de Sylow es divisor de $(G : S)$ (por tanto, de $|G|$).*
- *El número de p-subgrupos de Sylow de G es congruente con 1 módulo p.*

Mediante el segundo punto del Teorema de Sylow 1.28, podemos deducir que S es el único p-subgrupo de Sylow de G si, y sólo si, S es un subgrupo normal de G.

Teorema 1.29. *(Teorema de Cauchy). Sea G un grupo finito, con p primo dividiendo a $|G|$, se verifica:*

- *Existe un $x \in G$ tal que $|x| = p$.*
- *Si $p^k \mid |G|$, entonces existe un subgrupo $H < G$ tal que $|H| = p^k$.*

Por el Teorema de Sylow podemos saber qué grupos existen y qué forma tienen en función del número de elementos que tengan, lo cual nos será de gran ayuda en el primer capítulo del trabajo.

Proposición 1.30. *Sea G un grupo abeliano finito de orden n, si p divide a n, entonces G contiene un elemento de orden p.*

Lema 1.31. *Si G es un grupo abeliano finito de orden $n = p_1^{a_1} \cdot \cdots \cdot p_m^{a_m}$ con p_i primos distintos y a_i enteros positivos, entonces $G \simeq G_1 \times \cdots \times G_m$ donde G_j es el subgrupo que contiene a todos los elementos de G de orden p_j^k para cierto k entero.*

Lema 1.32. *Sea G un p-grupo abeliano finito y $g \in G$ un elemento con orden maximal, entonces $G \simeq \langle g \rangle \times H$ para algún subgrupo $H < G$.*

1.2. Teoría de cuerpos

Un anillo es una terna $(R, +, \cdot)$ donde R es un conjunto, $+$, $\cdot$ dos operaciones internas ("suma y multiplicación") satisfaciendo:

- $(R, +)$ es un grupo abeliano.
- $\cdot$ es asociativa en R.
- $\cdot$ es distributiva sobre $+$.

Un **cuerpo** es un anillo en el que todos los elementos tienen inverso multiplicativo (es decir, $(R - \{0\}, \cdot)$ es un grupo, o todos los elementos de R son unidades).

Definición 1.33. Un homomorfismo de anillos es una aplicación $\phi : A \longrightarrow B$ entre anillos A, B que cumple, para todo elemento $x, y \in A$:

- $f(x + y) = f(x) + f(y)$.
- $f(x \cdot y) = f(x) \cdot f(y)$.
- $f(1) = 1$ y $f(0) = 0$ con 1 denotando el neutro de $\cdot$, y 0 el neutro de $+$.

Será inyectivo si $\ker \phi = \{0\}$ y sobreyectivo si $\operatorname{Im} \phi = B$.

Definición 1.34. Un ideal I de un anillo A es un subconjunto de A que cumple, para todo $x, y \in I$ y todo $a \in A$:

- $x - y \in I$.
- $a \cdot x \in I$.

Definición 1.35. Se dice que dos ideales son coprimos si el mínimo ideal que contiene a ambos es el propio anillo que los contiene.

Teorema 1.36. *(Teorema Chino de los Restos). Sea A un anillo, $I_1, \ldots, I_n$ ideales de A, se verifica que:*

- *La siguiente aplicación es un homomorfismo de anillos:*

$$\begin{aligned} \phi : A &\longrightarrow \prod_{k=1}^{n} A/I_k \\ x &\longmapsto (x + I_1, \ldots, x + I_n). \end{aligned}$$

- *ϕ es inyectivo si, y sólo si:*

$$\bigcap_{k=1}^{n} I_k = 0.$$

- *ϕ es sobreyectivo si, y sólo si, I_k e I_j son coprimos para todo $j \neq k$.*

Definición 1.37. Sean K y F cuerpos, tal que $K \subset F$ y K subcuerpo de F, entonces se dice que F es una extensión de K $(F|K)$.

- Se denomina *grado de la extensión* al entero $[F : K] = \dim_K F$.
- Se dice extensión *finita* si el grado de la extensión es finito.
- Se dice *finitamente generada* si existen $\alpha_1, \ldots, \alpha_n \in F$ tales que $F = K(\alpha_1, \ldots, \alpha_n)$.
- Si $n = 1$, $F = K[\alpha]|K$ es una extensión *simple*.

Definición 1.38. Sean $F_1, \ldots, F_k$ cuerpos, tal que $F_i \subset F_{i+1}$, con $i \in \{1, \ldots, n\}$ entonces $F_1 \subset F_2 \subset \cdots \subset F_{n-1} \subset F_n$ se denomina torre de cuerpos.

Teorema 1.39. *(Teorema del grado). Sea $K \subset F \subset E$ torre de cuerpos, se verifica:*

$$E|K \text{ finita} \iff F|K \text{ y } E|F \text{ son finitas.}$$

Además se da la igualdad $[E : K] = [E : F] \cdot [F : K]$.

Definición 1.40. Sea una extensión de cuerpos $F|K$, y $\alpha \in F$:

- Se dice que α es *algebraico sobre* K si existe $f \in K[X]$ no nulo tal que $f(\alpha) = 0$ (si α no es algebraico, se dirá que es *trascendente*).
- Una extensión $E|K$ se dice algebraica si todo elemento $\alpha \in E$ es algebraico sobre K.

Observación 1.41. Tomando la extensión de cuerpos $E|K$, y el elemento $\alpha \in E$, la aplicación $\mathrm{ev}_\alpha : K[X] \longrightarrow E$ induce un isomorfismo de anillos

$$\frac{K[X]}{\ker(\mathrm{ev}_\alpha)} \cong \mathrm{Im}(\mathrm{ev}_\alpha) = K[\alpha]$$

Además, si tomamos $\alpha \in E$ algebraico, entonces $\ker(\mathrm{ev}_\alpha) = (f)$, siendo f el irreducible de α, así que se da el isomorfismo:

$$\frac{K[X]}{(f)} \simeq K[\alpha] \simeq K(\alpha).$$

Definición 1.42. Se dice que un polinomio es irreducible en $\mathbb{Q}$ si no se puede descomponer como producto de polinomios definidos sobre $\mathbb{Q}$.

Existen distintos criterios de irreductibilidad sobre $\mathbb{Q}$, veremos dos de los más importantes:

Proposición 1.43. *(Criterio de Eisenstein). Sea $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$, si existe un primo $p \in \mathbb{Z}$ que divide a los a_i con $i = 0, \ldots, n-1$, pero $p \nmid a_n$ y $p^2 \nmid a_0$, entonces f es irreducible en $\mathbb{Q}[X]$.*

Proposición 1.44. *(Reducción a módulo p). Sea $f \in \mathbb{Z}[X]$ definido como anteriormente, y $p \in \mathbb{Z}$ primo que no divide a a_n, si la reducción a $\mathbb{F}_p[X]$ del polinomio f es irreducible, entonces f es irreducible en $\mathbb{Q}[X]$.*

Proposición 1.45. *Sea $E|K$ extensión de cuerpos, $\alpha \in E$ algebraico sobre K, son equivalentes:*

- $\deg(\mathrm{Irr}(\alpha, K)) = n$.
- $[K(\alpha) : K] = n$.
- $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *es K-base de $K(\alpha)$.*

Proposición 1.46. *Sea $E|K$ extensión de cuerpos, $\alpha \in E$, son equivalentes:*

- *α es algebraico sobre K.*
- *La extensión $K(\alpha)|K$ es finita.*

Proposición 1.47. *Toda extensión finita es algebraica, toda extensión finitamente generada por elementos algebraicos es finita, y toda extensión finita está finitamente generada por elementos algebraicos.*

Teorema 1.48. *Sea $K \subset F \subset E$ torre de cuerpos, se verifica:*

$$E|K \text{ algebraica} \iff F|K \text{ y } E|F \text{ son algebraicas.}$$

Así, denominamos clausura algebraica de K en E al subcuerpo formado por todos los elementos de E que son algebraicos sobre K.

Definición 1.49. Sea $\sigma : K \longrightarrow K$ homomorfismo de cuerpos, $F|K$ y $F'|K'$ extensiones de cuerpos. Un monomorfismo $\tau : F \longrightarrow F'$ se dirá *extensión* de σ si $\tau_{|K} = \sigma$, es decir, si es conmutativo el diagrama siguiente (siendo i la inclusión $K \subset F$, e i' la inclusión $K' \subset F'$):

$$\begin{array}{ccc} K & \xrightarrow{\ i\ } & F \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\tau} \\ K' & \xrightarrow{\ i'\ } & F' \end{array}$$

Teorema 1.50. *(Teorema de extensión de monomorfismos para extensiones simples). Sean $L|K$ y $L'|K'$ extensiones y $\sigma : K \longrightarrow K'$ isomorfismo. Sean $\alpha \in L$ algebraico sobre K, $\beta \in L'$ algebraico sobre K', serán equivalentes:*

- *Existe un único isomorfismo $\tau : K(\alpha) \longrightarrow K'(\beta)$ que extiende σ y es tal que $\tau(\alpha) = \beta$.*
- $\mathrm{Irr}(\beta, K') = \tilde{\sigma}(\mathrm{Irr}(\alpha, K))$.

Siendo $\tilde{\sigma} : K[X] \longrightarrow K'[X]$ el isomorfismo de anillos determinado por $\tilde{\sigma}(X) = X$, y $\tilde{\sigma}(K) = \sigma(K)$.

1.2.1. Cuerpos de escisión

Teorema 1.51. *(Teorema de Kronecker). Si $f \in K[X]$ es irreducible, existe una extensión simple $K(\alpha)|K$ con $f(\alpha) = 0$, y además $[K(\alpha) : K] = \deg(f)$.*

Definición 1.52. Sea $E|K$ una extensión de cuerpos, $f \in K[X]$ de grado $n \geq 1$, diremos que:

- *f escinde en E*, si f tiene todas sus raíces en este cuerpo.
- *E es el cuerpo de escisión de f* en K si f escinde en E y, además, $E = K(\alpha_1, \ldots, \alpha_n)$.

Teorema 1.53. *(Teorema de extensión de isomorfismos para cuerpos de escisión). Sea $\sigma : K \longrightarrow K'$ isomorfismo de cuerpos, $f \in K[X] - 0$, entonces $\tilde{\sigma} f \in K'[X]$ es no nulo tal que $\deg(f) = \deg(\tilde{\sigma} f)$. Sea E cuerpo de escisión de f sobre K, y E' cuerpo de escisión de $\tilde{\sigma} f$ sobre K', entonces existe un isomorfismo $\tau : E \longrightarrow E'$ que extiende σ.*

Teorema 1.54. *(Teorema de Steinitz). Si K es un cuerpo, existe $E|K$ clausura algebraica de K, determinada salvo K-isomorfismos.*

1.2.2. Extensiones separables y normales

Definición 1.55. Sea $f \in K[X]$, y α un cero de f, el entero $m = \max\{s \in \mathbb{N} \mid (X - \alpha)^s | f$ en $K(\alpha)[X]\} \geq 1$ se denomina multiplicidad de α como raíz de f. Si $m = 1$ diremos que α es una raíz simple de f (y si es mayor diremos que es múltiple).

Definición 1.56. (Separabilidad)

- Un **polinomio** $f \in K[X]$ es *separable* si todas sus raíces son simples.
- Un **elemento** $\alpha \in E$ es *separable* sobre K si es algebraico sobre K y $\mathrm{Irr}(\alpha, K)$ es separable.

- La **extensión** $E|K$ es *separable* si α es separable sobre K para todo $\alpha \in E$.

Proposición 1.57. *Sea $f \in K[X]$ un polinomio, si f y f' son coprimos, entonces f tiene todas sus raíces distintas.*

Proposición 1.58. *Sea $f \in K[X]$ irreducible:*

$$f \text{ posee una raíz múltiple} \iff f' = 0.$$

Proposición 1.59. *Si $f \in K[X]$ es irreducible y $\operatorname{car}(K) = 0$, entonces f es separable.*

Observación 1.60. De esta manera, toda extensión algebraica sobre un cuerpo de característica 0, en particular, sobre $\mathbb{Q}$, es separable.

Definición 1.61. Sea $E|K$ una extensión, $\alpha \in E$ es un elemento primitivo de la extensión si $E = K(\alpha)$.

Teorema 1.62. *(Caracterización de los cuerpos finitos). Sea F un cuerpo finito de $\operatorname{car}(F) = p$ y con $|F| = q$, se tiene:*

- *$q = p^n$ siendo $n = [F : \mathbb{F}_p]$ ($\mathbb{F}_p$ es el subcuerpo primo de F)*
- *F es cuerpo de escisión del polinomio $x^{p^n} - x$ sobre $\mathbb{F}_p$, y $F \mid \mathbb{F}_p$ es separable.*
- *Existe un elemento $\alpha \in F$ separable sobre $\mathbb{F}_p$ tal que $F = \mathbb{F}_p(\alpha)$.*
- *$\operatorname{Aut}_{\mathbb{F}_p}(F)$ es cíclico de orden n, cuyo generador es el endomorfismo de Frobenius.*

Teorema 1.63. *(Teorema del elemento primitivo para cuerpos finitos). Sea F un cuerpo finito y $E|F$ una extensión finita entonces existe un $\alpha \in E$ tal que $E = F(\alpha)$ (extensión separable y simple).*

Teorema 1.64. *(Teorema del elemento primitivo para cuerpos no finitos). Sea K un cuerpo infinito y $E|K$ una extensión finita y separable entonces existe un $\alpha \in E$ tal que $E = K(\alpha)$ (extensión separable y simple).*

En virtud del *Teorema del elemento primitivo*, podemos decir que toda extensión finita $E|\mathbb{Q}$ es simple.

Definición 1.65. Decimos que una extensión $E|K$ es *normal* si es algebraica y para cada $f \in K[X]$ irreducible, si tiene una raíz en E, entonces las tiene todas (escinde en E).

Teorema 1.66. *Para una extensión E/K equivalen:*

- *E/K finita y normal.*

- *Existe un polinomio no nulo $f \in K[X]$ tal que E es cuerpo de escisión de f sobre K.*

Proposición 1.67. *Si $K \subset F \subset E$ es una torre de cuerpos, y $E|K$ normal, entonces $E|F$ es normal.*

Proposición 1.68. *Si $E|K$ es normal, $\alpha, \beta \in E$ son tales que $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$, entonces existe $\tau : E \longrightarrow E$ un K-automorfismo tal que $\tau(\alpha) = \beta$.*

1.2.3. Teoría de Galois

Dada una extensión de cuerpos $E|K$, denotamos por *Grupo de Galois* de la extensión:

$$\mathrm{Gal}(E|K) := \mathrm{Aut}_K(E) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma_{|K} = \mathrm{Id}_K\}.$$

Proposición 1.69. *Si $K(\alpha)|K$ es una extensión simple y α sobre K, entonces:*

- *Un K-isomorfismo $\sigma : K(\alpha) \longrightarrow K(\alpha)$ queda determinado por $\sigma(\alpha)$.*
- *Sean $\{\alpha_1, \ldots, \alpha_s\} \subset K(\alpha)$ todas las raíces del polinomio $\mathrm{Irr}(\alpha, K)$ en $K(\alpha)$, entonces la correspondencia siguiente es biyectiva:*

$$\begin{aligned} \mathrm{Gal}(K(\alpha)|K) &\longrightarrow \{\alpha_1, \ldots, \alpha_s\} \\ \sigma &\longmapsto \sigma(\alpha). \end{aligned}$$

- $|\mathrm{Gal}(K(\alpha)|K)| \leq \deg(\mathrm{Irr}(\alpha, K))$.

Definición 1.70. Una extensión $E|K$ se dice de *Galois* si es finita y $E^{\mathrm{Gal}(E|K)} = K$, siendo $E^H = \{a \in E \mid \sigma(a) = a, \sigma \in H\} \subset E$ el subcuerpo de E fijo por H.

Observación 1.71. Si $E|K$ finita, se cumple que $[E : E^H] = |H|$ y $H = \mathrm{Gal}(E|E^H)$.

Teorema 1.72. *Para una extensión finita $E|K$ equivalen:*

- *$E|K$ es de Galois.*
- *$E|K$ es normal y separable.*
- $|\mathrm{Gal}(E|K)| = [E : K]$.

Teorema 1.73. *(Teorema Fundamental de la Teoría de Galois). Sea $E|K$ una extensión de Galois y $G = \mathrm{Gal}(E|K)$ su grupo de Galois. Consideramos los conjuntos:*

$$SubExt(E|K) = \{F \mid K \subset F \subset E\}.$$

$$SubGr(G) = \{H \mid H < G\}.$$

entonces las siguientes correspondencias son biyectivas, una inversa de la otra:

$$\begin{aligned} SubExt(E|K) &\longrightarrow SubGr(G) & SubGr(G) &\longrightarrow SubExt(E|K) \\ F &\longmapsto \mathrm{Gal}(E|F) & H &\longmapsto E^H \end{aligned}$$

Proposición 1.74. *Sea $E|K$ una extensión de Galois, y $G = \mathrm{Gal}(E|K)$ su grupo de Galois. Si $H < G$ es un subgrupo, entonces*

$$H \lhd G \iff E^H|K \text{ normal.}$$

Corolario 1.75. *Sea $E|K$ una extensión de Galois, $K \subset F \subset E$ una torre de cuerpos, se tiene:*

$$\mathrm{Gal}(E|F) \lhd \mathrm{Gal}(E|K) \iff F|K \text{ normal.}$$

Además, con las mismas condiciones:

$$\frac{\mathrm{Gal}(E|K)}{\mathrm{Gal}(E|F)} \simeq \mathrm{Gal}(F|K).$$

1.2.4. Gran Teorema de Galois

Definición 1.76. Un grupo G es *resoluble* si existe una serie normal y finita $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ de subgrupos normales de G tal que $\frac{G_i}{G_{i+1}}$ es abeliano, $i \in \{1, \ldots, r\}$.

Teorema 1.77. *Dados $p, q \in \mathbb{N}$ primos distintos, se tiene:*

- *Todo grupo abeliano es resoluble.*
- *(Burnside) Todo grupo de orden $p^n \cdot q^m$ es resoluble.*
- *(Feit-Thompson) Todo grupo de orden impar es resoluble.*

Definición 1.78. La extensión $F|K$ es *radical* si existe una torre de cuerpos $K = K_0 \subset K_1 \subset \cdots \subset K_r = F$ tal que $K_i = K_{i-1}(\alpha_i)$, y un $n_i \in \mathbb{N}$ con $\alpha_i^{n_i} \in K_{i-1}$, $i \in \{1, \ldots, r\}$.

Así, un polinomio $f \in K[X]$ es *resoluble por radicales* sobre K si E_f (cuerpo de escisión de f) está contenido en una extensión radical de K.

Observación 1.79. Denotaremos por $\mathrm{Gal}_K(f)$ el grupo de Galois de la extensión $K|E_f$, E_f con cuerpo de escisión de f.

Teorema 1.80. *(Gran Teorema de Galois). Dado $f \in K[X]$ no nulo:*

$$f \text{ resoluble por radicales} \iff \mathrm{Gal}_K(f) \text{ es un grupo resoluble.}$$

1.3. Polinomios ciclotómicos

Tomando $n > 0$ entero, llamamos *raíz n-ésima de la unidad* a las raíces complejas del polinomio $X^n - 1 \in \mathbb{Q}[X]$. Así, estas raíces tienen la forma:

$$\epsilon_k = e^{\frac{2k\pi}{n}i}, \quad 0 \leq k < n.$$

El conjunto de las raíces n-ésimas de la unidad será $U_n = \{\epsilon \in \mathbb{C} \mid \epsilon^n = 1\}$, que es un grupo cíclico, con la multiplicación usual, de orden n y generado por $\epsilon_1 = e^{\frac{2\pi}{n}i}$.

- Se denomina *raíz primitiva n-ésima de la unidad* a cualquier generador de U_n.
- *El indicador de Euler de n*, $\phi(n)$, es el número de generadores de U_n, ya que su definición formal es $\phi(n) = |\{m \in \mathbb{N} \mid m \leq n, \gcd(m,n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^*|$ (unidades de $\mathbb{Z}/n\mathbb{Z}$). Además, cumple que:
  - Si $n, m \in \mathbb{Z}$ son coprimos; $\phi(mn) = \phi(m)\phi(n)$.
  - Si p es primo y $k \geq 1$ entero, $\phi(p^k) = (p-1) \cdot p^{k-1}$.
- El n-ésimo *polinomio ciclotómico* es el polinomio $\Phi_n(X) = \mathrm{Irr}(\epsilon, \mathbb{Q})$.
- La extensión $\mathbb{Q}(\epsilon)|\mathbb{Q}$ se denomina extensión ciclotómica.

Proposición 1.81. *Sea $\epsilon \in \mathbb{C}$ raíz primitiva n-ésima de la unidad y un entero $1 \leq r < n$ tal que $\gcd(r,n) = 1$, entonces:*

- $\mathrm{Irr}(\epsilon^r, \mathbb{Q}) = \mathrm{Irr}(\epsilon, \mathbb{Q})$.
- $\Phi_n(X) = \mathrm{Irr}(\epsilon, \mathbb{Q}) \in \mathbb{Z}[X]$.
- $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = \phi(n)$.

De esta forma también se cumplen las siguientes igualdades siendo $n > 0$ entero:

$$\Phi_n(X) = \prod_{r<n \,|\, \gcd(r,n)=1} (X - \epsilon^r), \qquad X^n - 1 = \prod_{d|n} \Phi_d(X).$$

1.3.1. Grupo de Galois de una extensión ciclotómica

Pongamos $\mathbb{Q}(\epsilon)|\mathbb{Q}$ extensión ciclotómica (siendo ϵ raíz primitiva n-ésima), generada por el polinomio $f = \mathrm{Irr}(\epsilon, \mathbb{Q}) = \mathrm{Irr}(\epsilon^r, \mathbb{Q})$ con $\gcd(r,n) = 1$, $1 \leq r < n$. Sabemos que el grado de la extensión es $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = \phi(n)$, que coincide con el número de generadores de U_n (los ϵ^r tal que $\gcd(r,n) = 1$), y además se tiene que $\{\epsilon^{r_1}, \ldots, \epsilon^{r_k}\}_{\gcd(r_i,n)=1}$ es el conjunto de las raíces del irreducible f.

Ahora bien, en virtud de la proposición 1.69, tenemos la siguiente biyección:

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) &\longrightarrow \{\epsilon^{r_1}, \ldots, \epsilon^{r_k}\} \\ \sigma &\longmapsto \sigma(\epsilon) = \epsilon^{r_j} \end{aligned}$$

Es decir, cada elemento de $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$ queda definido determinando la imagen de ϵ, así que $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) = \{\sigma_i \mid \sigma_i(\epsilon) = \epsilon^{r_i}$, con $\gcd(r_i, n) = 1$, y $1 \leq r_i < n\}$. Podemos observar que la aplicación $h : \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ tal que $h(\sigma_i) = r_i$ ($r_i \in (\mathbb{Z}/n\mathbb{Z})^*$ porque $\gcd(r_i, n) = 1$, y $1 \leq r_i < n$) es un isomorfismo de grupos, y de esta forma tenemos demostrado el siguiente resultado:

Proposición 1.82. *Para toda extensión ciclotómica $\mathbb{Q}(\epsilon)|\mathbb{Q}$, con ϵ raíz primitiva n-ésima de la unidad, se tiene que* $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Capítulo 2

Subgrupos de S_n con $n \leq 3$

Debido a la doble implicación dada por el *Gran Teorema de Galois*, el problema inverso (de Galois) cobra gran interés para solucionar la incógnita de la resolubilidad por radicales. Podríamos estudiar el problema inverso en grupos resolubles, y así obtener polinomios que se pueden resolver por radicales.

Esto mismo es lo que haremos en el presente capítulo con los subgrupos de S_n con $n \leq 3$, los cuales son todos resolubles. Pero antes de nada, veremos un resultado cuya demostración se entiende por la definición del grupo de Galois (un grupo que actúa como permutación de las raíces de un polinomio), y por ser normal la extensión del cuerpo de escisión de un polinomio $f \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$:

Proposición 2.1. *Sea α una raíz del irreducible $f \in \mathbb{Q}[X]$, de grado $n \geq 1$ (siendo $\mathbb{Q}(\alpha)|\mathbb{Q}$ una extensión algebraica de Galois), se tiene que* $\mathrm{Gal}_{\mathbb{Q}}(f) \lhd S_n$.

Además, por ser $\mathrm{Gal}_{\mathbb{Q}}(f) \lhd S_n$*, existe una órbita única para cada acción de* $\mathrm{Gal}_{\mathbb{Q}}(f)$ *en las raíces α_i de f.*

Denotando $G = \mathrm{Gal}_{\mathbb{Q}}(f)$, la definición de órbita de un elemento $\alpha_j \in \{\alpha_1, \ldots, \alpha_n\}$ (conjunto de raíces de f) sobre la acción de G en este conjunto es; $G\alpha_j = \{\sigma * \alpha_j$ tal que $\sigma \in G\} \subset \{\alpha_1, \ldots, \alpha_n\}$. Y lo que quiere decir la segunda parte de este resultado tan sólo es una generalización de la proposición 1.69.

El caso $n = 1$ no lo vamos a tratar en profundidad, ya que S_1 es el grupo trivial, el cual es grupo de Galois de cualquier extensión cuyo polinomio tenga todas sus raíces en $\mathbb{Q}$. Y los únicos polinomios irreducibles que cumplen esto son los de grado 1 (todos, porque escinden en $\mathbb{Q}$, y el único $\mathbb{Q}$-automorfismo que relacione las raíces será la identidad).

2.1. Subgrupos de S_2

El orden de S_2 es 2, y el único grupo de orden 2 es $\mathbb{Z}/2\mathbb{Z}$ (por el *Teorema de Lagrange* y ser 2 un número primo), así que sólo hay que estudiar el problema en este grupo cíclico.

Como el grupo de Galois, por definición, se trata del grupo de homomorfismos de cuerpos que, dejando fijos los elementos de $\mathbb{Q}$, relacionan de todas las maneras posibles las raíces del polinomio que genera la extensión (porque un homomorfismo de cuerpos se puede definir simplemente sabiendo cómo actúa sobre la base), entonces ese polinomio sólo podrá tener dos raíces fuera de $\mathbb{Q}$, así que será un irreducible en $\mathbb{Q}$ de grado 2.

$$\mathrm{Gal}(E|\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(E) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma_{|\mathbb{Q}} = id_{|\mathbb{Q}}\}$$

Las raíces de estos polinomios son de la forma $a \pm \sqrt{b}$ con $b \in \mathbb{R}$ (por tanto la raíz puede ser irracional o compleja), así que los dos únicos $\mathbb{Q}$-automorfismos que las relacionen serán:

$\sigma_0(a + \sqrt{b}) = a + \sqrt{b} \quad \sigma_1(a + \sqrt{b}) = a - \sqrt{b}.$

$\sigma_0(a - \sqrt{b}) = a - \sqrt{b} \quad \sigma_1(a - \sqrt{b}) = a + \sqrt{b}$.

Las cuales representan σ_0 la identidad y σ_1 la conjugación, y tienen respectivamente orden 1 y 2 (es decir, $\sigma_0^1 = id$ y $\sigma_1^2 = id$), por lo tanto el grupo de estos $\mathbb{Q}$-automorfismos sería isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

Proposición 2.2. *Todos los irreducibles de grado 2 tienen como grupo de Galois a $\mathbb{Z}/2\mathbb{Z}$ y, recíprocamente, todos los polinomios irreducibles en $\mathbb{Q}$ que generen una extensión de cuerpos normal y separable cuyo grupo de Galois sea $\mathbb{Z}/2\mathbb{Z}$, son de grado 2.*

2.2. Subgrupos de S_3

Los subgrupos no isomorfos de S_3, por ser un grupo de orden 6 ($|S_3| = 3! = 1 \cdot 2 \cdot 3 = 6$), son el grupo trivial $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$ (orden 2), $\mathbb{Z}/3\mathbb{Z}$ (orden 3), y el propio S_3 (orden 6). El grupo trivial y $\mathbb{Z}/2\mathbb{Z}$ ya fueron mencionados, por lo tanto sólo queda estudiar $\mathbb{Z}/3\mathbb{Z}$ y S_3.

Para estudiar este caso, introduciremos varios resultados sobre el discriminante, y lo relacionaremos con el grupo alternado A_n, que en el caso de $n = 3$ coincide con el grupo $\mathbb{Z}/3\mathbb{Z}$.

Definición 2.3. Sea $L|K$ una extensión finita y separable, con $\{\alpha_1, \ldots, \alpha_n\}$ base de L sobre K, y $\sigma_1, \ldots, \sigma_n$ homomorfismos de K-álgebras de L en K, se define el *discriminante de la base* como

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Proposición 2.4. *Con las condiciones anteriores, siendo* $[L : K] = n$*, y* $L = K(\alpha)$*, se tiene que:*

$$\operatorname{disc}(1, \ldots, \alpha^{n-1}) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

Demostración. Por ser $L|K$ finita y separable, existe un $\alpha \in L$ tal que $L = K(\alpha)$, por tanto, $\{1, \ldots, \alpha^{n-1}\}$ es una base de $L|K$, y $\sigma(\alpha)^n = \sigma(\alpha^n)$ para toda σ que sea K-álgebra de L en K, así que:

$$\operatorname{disc}(1, \ldots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2 = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2. \tag{2.1}$$

□

A partir de esta proposición, podemos llegar a maneras equivalentes de definir el discriminante.

Proposición 2.5. *Sea* $f \in \mathbb{Q}[X]$ *irreducible de grado* n *con raíces* $\alpha_1, \ldots, \alpha_n$*, y* $E_f|\mathbb{Q}$ *extensión finita de Galois, se tiene que:*

$$\operatorname{disc}(f) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Esto sucede por ser separable cada polinomio definido en $\mathbb{Q}$, y por la definición de cada elemento del grupo de Galois de la extensión.

Mediante la siguiente proposición relacionaremos ciertas propiedades del discriminante de un polinomio con el grupo alternado A_n.

Proposición 2.6. $\operatorname{Gal}_{\mathbb{Q}}(f) < A_n \iff \operatorname{disc}(f)$ *es un cuadrado.*

Demostración. Sean α_k las raíces de f, el discriminante será de la forma $\operatorname{disc}(f) = H^2$ con $H = \prod_{i<j}(\alpha_i - \alpha_j) \neq 0$ (por ser raíces distintas). Por la definición de H (y por ser un entero algebraico), y siendo $\epsilon(\sigma)$ la signatura de $\sigma \in S_n$ (será 1 si $\sigma \in A_n$, y -1 en caso contrario):

$$\text{para todo } \sigma \in \operatorname{Gal}_{\mathbb{Q}}(f), \text{ se tiene } \sigma(H) = \epsilon(\sigma) \cdot H.$$

Si suponemos que $\operatorname{Gal}_{\mathbb{Q}}(f) < A_n$, tendríamos que $\sigma(H) = \epsilon(\sigma) \cdot H = H$, por lo tanto $H \in \mathbb{Q}$, y como H es un entero algebraico se tendría que $H \in \mathbb{Q}$.

La implicación hacia la derecha es simple; si $H \in \mathbb{Q}$ (es decir, el discriminante es un cuadrado) tendríamos, para todo $\sigma \in \operatorname{Gal}_{\mathbb{Q}}(f)$, que $\sigma(H) = \epsilon(\sigma) \cdot H = H$, así que $\epsilon(\sigma) = 1$ y entonces $\operatorname{Gal}_{\mathbb{Q}}(f) < A_n$.

□

Pues por esta proposición vamos a tener la siguiente propiedad para los polinomios de grado 3:

Proposición 2.7. *Sea $f \in \mathbb{Q}[X]$ irreducible de grado 3:*

- $\mathrm{Gal}_{\mathbb{Q}}(f) \simeq A_3 \iff \mathrm{disc}(f)$ *es un cuadrado.*
- $\mathrm{Gal}_{\mathbb{Q}}(f) \simeq S_3 \iff \mathrm{disc}(f)$ *no es un cuadrado.*

El razonamiento simplemente se debe a que, como todas sus raíces son distintas (es separable por estar definido en $\mathbb{Q}$ y ser irreducible), el grupo de Galois debe tener orden 3 o superior.

Teniendo en cuenta la computación del discriminante [2] para polinomios mónicos de grado 3 de la forma $f = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[X]$:

$$d(f) = a_1^2 \cdot a_2^2 - 4a_1^3 - 4a_0 \cdot a_2^2 - 27a_0^2 + 18a_0 \cdot a_1 \cdot a_2.$$

Entonces, basándonos en la fórmula, ya daríamos con polinomios cuyo grupo de Galois fuera $A_3 = \mathbb{Z}/3\mathbb{Z}$ o S_3, tendríamos, por ejemplo:

$$f_s = x^3 - 4x^2 + 2x + 9, \qquad \mathrm{Gal}_{\mathbb{Q}}(f) \simeq S_3.$$
$$f_a = x^3 - \frac{21}{4}x + \frac{7}{2}, \qquad \mathrm{Gal}_{\mathbb{Q}}(f) \simeq A_3.$$

Como bien podemos comprobar en SageMath:

```
fs=x^3+4*x^2+2*x+9;fs.is_irreducible()
```

```
True
```

```
ds=fs.discriminant();sqrt(ds)
```

```
sqrt(-3163)
```

El discriminante de nuestro polinomio de grado 3 no es un cuadrado, así que su grupo de Galois será isomorfo a S_3:

```
Gs=fs.galois_group();Gs
```

```
Transitive group number 2 of degree 3
```

```
Gs.is_isomorphic(SymmetricGroup(3))
```

```
True
```

```
fa=x^3-21/4*x+7/2;fa.is_irreducible()
```

```
True
```

```
da=fa.discriminant();sqrt(da)
```

```
63/4
```

En este caso, el discriminante de nuestro polinomio de grado 3 es un cuadrado, concretamente $(63/4)^2$, así que cabe esperar que su grupo de Galois sea isomorfo a A_3:

```
Ga=fa.galois_group();Ga
```

```
Transitive group number 1 of degree 3
```

```
Ga.is_isomorphic(CyclicPermutationGroup(3))
```

```
True
```

Capítulo 3

Grupos cíclicos finitos

Para comenzar este capítulo, es de gran importancia abordar los siguientes dos resultados, para delimitar lo que entendemos por grupo cíclico:

Proposición 3.1. *Si G es un grupo cíclico de orden n finito, entonces $G \simeq \mathbb{Z}/n\mathbb{Z}$.*

Demostración. Tomando la aplicación sobreyectiva f definida como sigue:

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G \\ i &\longmapsto a^i \end{aligned}$$

Sabemos que el núcleo de esta aplicación serán los $m \in \mathbb{Z}$ tal que $n|m$, ya que de esta manera $a^m = a^{n \cdot k} = (a^n)^k = 1^k = 1$. Por lo tanto, $\ker(f) = n\mathbb{Z}$, y aplicando el Primer Teorema de Isomorfía 1.13, obtenemos que $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Observación 3.2. Con el mismo razonamiento podemos concluir que si G es no finito y cíclico, entonces es isomorfo a $\mathbb{Z}$.

Proposición 3.3. *Sea G grupo cíclico de orden n finito, para cada divisor d de n, G tiene un único subgrupo de orden d.*

Demostración. Por ser G cíclico, $G \simeq \mathbb{Z}/n\mathbb{Z}$ para cierto n natural, y por ser d divisor de n, tenemos que $n = d \cdot a$, así que $H = c\mathbb{Z}/n\mathbb{Z}$ será un subgrupo de $\mathbb{Z}/n\mathbb{Z}$.

- Orden de H: como $\mathbb{Z}$ es abeliano, se tiene que $c\mathbb{Z}$ y $n\mathbb{Z}$ son subgrupos normales de $\mathbb{Z}$ tales que $n\mathbb{Z} \subset c\mathbb{Z}$, aplicando el Segundo Teorema de Isomorfía 1.14 se tiene:

$$\frac{\mathbb{Z}/n\mathbb{Z}}{c\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/c\mathbb{Z} \Longrightarrow n = c \cdot |H| \Longrightarrow |H| = d.$$

- Unicidad: supongamos que existe otro subgrupo $K < G$ tal que $|K| = d$, por ser cíclico G, se tendrá $K = b\mathbb{Z}/n\mathbb{Z}$, por el Segundo Teorema de Isomorfía se tendrá:

$$\frac{\mathbb{Z}/n\mathbb{Z}}{b\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/b\mathbb{Z} \Longrightarrow n/|K| = b \Longrightarrow b = d \Longrightarrow K = b\mathbb{Z}/n\mathbb{Z} = c\mathbb{Z}/n\mathbb{Z} = H.$$

□

3.1. Problema inverso de Galois en grupos cíclicos finitos

Para dar respuesta al problema en grupos de la forma $\mathbb{Z}/n\mathbb{Z}$ con n entero arbitrario, necesitaremos tratar algunos resultados previos:

Lema 3.4. *Sea $(E, +, \cdot)$ un cuerpo finito y $(E^*, \cdot)$ su grupo multiplicativo. Si $G \leq E^*$, entonces es G cíclico.*

Demostración. Tenemos que demostrar que $exp(G) = \text{mín}\{t \in \mathbb{Z}$ tal que para todo $g \in G$, $g^t = 1\} = |G|$ siendo $G \leq E^*$.

Por definición, al menos un elemento de G tiene orden $exp(G)$ (por lo menos el neutro), así que por el Teorema de Lagrange 1.8, $exp(G) \mid |G|$, entonces, $exp(G) \leq |G|$.

Y a su vez, para todo elemento $x \in G$, se cumple por definición $x^{exp(G)} = 1$. Pero la ecuación $x^n - 1$ tiene, en un cuerpo E^*, como mucho n soluciones, por lo tanto, habrá a lo sumo $exp(G)$ elementos en G, así que $|G| \leq exp(G)$.

Empleando las conclusiones de ambos párrafos, se tiene $exp(G) = |G|$ □

Lema 3.5. *Sea $n \in \mathbb{N}$, tomemos un primo p que no divida a n, entonces se cumple:*

$$p \mid \Phi_n(c) \iff \textit{el orden de } c \textit{ en } \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \textit{ es } n.$$

Demostración. i) $\Longrightarrow$ ii): Tenemos $p \mid \Phi_n(c)$, por lo tanto, $p \mid c^n - 1$ (por ser $x^n - 1$ el producto de los $\Phi_d(c)$ con $d \mid n$), y así se tiene $c^n \equiv 1 \pmod{p}$.

De esta manera, podría darse que el orden de c fuera un cierto $d < n$ con $d \mid n$, y así se tendría que $c^d \equiv 1 \pmod{p}$, pero como $x^d - 1 = \prod_{e|d} \Phi_e(X)$, tendríamos que c sería raíz de algún $\Phi_e(X)$ y de $\Phi_n(X)$ en $\mathbb{F}_p$, es decir, $x^n - 1$ tendría una raíz múltiple en $\mathbb{F}_p$. Esto no se puede dar porque $nx^{n-1} \nmid x^n - 1$ (la derivada y la función son coprimas y no nulas en $\mathbb{F}_p$ por no dividir p a n), así que el orden de c en $\mathbb{F}_p$ es n.

ii) $\Longrightarrow$ i): Si el orden de c es n en $\mathbb{F}_p$, se tiene que n es el mínimo entero tal que $c^n - 1 \equiv 0 \pmod{p}$ (es decir, no existe ningún $d < n$ tal que $c^d - 1 \equiv 0 \pmod{p}$), y como $c^n - 1 = \prod_{d|n} \Phi_d(c)$, necesariamente c ha de ser raíz de $\Phi_n(x)$ en $\mathbb{F}_p$, y así $p \mid \Phi_n(c)$ □

Lema 3.6. *Sea $f(x) \in \mathbb{Z}[X]$ polinomio con coeficientes enteros, entonces existen infinitos primos que dividen a algún elemento del conjunto $\{f(0), f(1), f(2), \dots\}$.*

Demostración. Supongamos que el término independiente de f es 1, y que el conjunto de los primos que dividen a $\{f(0), f(1), f(2), \dots\}$ es finito, pongamos que son $p_1, \dots, p_s$. Tomando el entero $f(p_1 \cdot \dots \cdot p_s \cdot y)$ (con y cierto entero positivo) tenemos que será congruente con 1 en módulo p_i para cualquier $i \in \{1, \dots, s\}$, por ser 1 el término independiente, y así existirá un primo p distinto de los anteriores dividiendo a $f(p_1 \cdot \dots \cdot p_s \cdot y)$. Por tanto, el conjunto de primos que dividen a algún $\{f(0), f(1), f(2), \dots\}$ no puede ser finito.

Si el término independiente de f fuera un entero c distinto de 1, tendríamos que el polinomio $f(c \cdot x)$ es divisible por c, y podríamos realizar el anterior razonamiento con el polinomio $h(x)$ tal que $f(c \cdot x) = c \cdot h(x)$. De esta manera, existirán infinitos primos que dividan a algún elemento del conjunto $\{h(0), h(1), h(2), \dots\}$, que, por la anterior igualdad, dividirán a algún elemento del conjunto $\{f(0), f(a), f(2 \cdot a), \dots\}$, el cual está contenido en el conjunto $\{f(0), f(1), f(2), \dots\}$, es decir, existen infinitos primos dividiendo a algún elemento del conjunto $\{f(0), f(1), f(2), \dots\}$. □

Emplearemos estos tres lemas para demostrar la siguiente proposición que, a su vez, nos servirá para demostrar el teorema mediante el cual daremos respuesta al problema inverso de Galois en grupos cíclicos.

Proposición 3.7. *Dado $n \in \mathbb{N}$, existen infinitos primos cumpliendo que $p \equiv 1 \mod n$.*

Demostración. La demostración de esta proposición tan sólo requiere de razonar con los lemas anteriores:

- Por tener $\Phi_n(x)$ coeficientes enteros (proposición 1.81), podemos aplicar el lema 3.6, y así existen infinitos primos dividiendo a algún elemento del conjunto $\{\Phi_n(c)\}_{c \in \mathbb{N}}$.

- De estos infinitos primos, tan sólo una cantidad finita dividirán a n, así que descartando esos, nuestro conjunto de primos seguirá siendo infinito. Aplicando ahora el lema 3.5, tendremos que serán infinitos los primos tales que $c^n \equiv 1 \mod p$ (el orden de cada c en $\mathbb{F}_p$ sea n).

- Por el Pequeño Teorema de Fermat lo anterior implica que $n \mid (p-1)$, así tendremos que $p \equiv 1 \mod n$ para infinitos p primos.

□

Observación 3.8. El Pequeño Teorema de Fermat dice que si p es primo entonces para cada a coprimo con p se cumple que $a^{p-1} \equiv 1 \mod p$. Entonces, como c era coprimo con p (porque sino $c^m \equiv 0 \mod p$ para todo m natural), $c^{p-1} \equiv 1 \mod p$, pero como el orden de c en $\mathbb{F}_p$ era n, tendremos que $n \mid (p-1)$.

Teorema 3.9. *Para cualquier G grupo cíclico, existe una extensión de Galois $E|\mathbb{Q}$ tal que* $\mathrm{Gal}(E|\mathbb{Q}) \simeq G$.

Demostración. La prueba se basa simplemente en recopilar los resultados vistos hasta ahora:

- Por la proposición 3.1 se tiene que G es de la forma $\mathbb{Z}/n\mathbb{Z}$ por ser cíclico.
- Por la proposición 3.7 existirá algún primo cumpliendo $p - 1 = n \cdot m$ para un cierto $m \in \mathbb{N}$.
- Dada una raíz primitiva p-ésima de la unidad, ϵ, se tiene, por la proposición 1.82, que $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \simeq \mathbb{F}_p^*$.
- Por el lema 3.4, ya que $\mathbb{F}_p$ es un cuerpo finito, se tiene que cualquier subgrupo del grupo $\mathbb{F}_p^*$ (grupo multiplicativo de $(\mathbb{F}_p, +, \cdot)$) es cíclico.
- Retomando la proposición 3.3, y sabiendo por definición que $|\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})| = \phi(p) = p - 1 = n \cdot m$, se tiene que para cada m divisor de $p-1$, existe un único subgrupo de $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$, H tal que $|H| = m$. Tomemos E como el cuerpo fijo por H, es decir, $E = \mathbb{Q}(\epsilon)^H$.
- Por ser $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$ y H grupos multiplicativos cíclicos (por el lema 3.4), se tendrá $H \lhd \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$, y por la proposición 1.74 posterior al Teorema Fundamental de la Teoría de Galois, $E|\mathbb{Q}$ será extensión de Galois (separable por ser sobre $\mathbb{Q}$ y normal por ser $H \lhd \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$).
- Por definición del cuerpo fijo, se tiene que $H = \mathrm{Gal}(\mathbb{Q}(\epsilon)|E) = \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}(\epsilon)^H)$, y por el corolario 1.75, se tiene:

$$\mathrm{Gal}(E|\mathbb{Q}) \simeq \frac{\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\epsilon)|E)} \simeq \frac{\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}(\epsilon)^H)} \simeq \frac{\mathbb{F}_p^*}{H} \simeq \mathbb{Z}/n\mathbb{Z} \simeq G.$$

  La equivalencia $\mathbb{F}_p^*/H \simeq \mathbb{Z}/n\mathbb{Z}$ se deduce de que tanto $\mathbb{F}_p^*$ como H son grupos cíclicos, de orden $p-1$ y m respectivamente, así que su cociente será cíclico de orden $\frac{p-1}{m} = n$, es decir, $\mathbb{Z}/n\mathbb{Z} \simeq G$.

□

3.2. Cálculo de polinomios con grupo de Galois cíclico

Para proceder en esta sección emplearemos el programa informático SageMath `https://www.sagemath.org/`, ya que goza de grandes ayudas en los problemas relacionados con polinomios y teoría de Galois. El código que se utilice será redactado junto a los razonamientos seguidos.

En la demostración del teorema 3.9 se explica cómo proceder para dar con el polinomio cuyo grupo de Galois sea cíclico finito, es decir, de la forma $\mathbb{Z}/n\mathbb{Z}$. En ella se empieza buscando un $m \in \mathbb{Z}$ tal que $n \cdot m + 1$ sea primo, por tanto, a través del siguiente bucle, buscamos esa m:

```
def gener(n):
    m=1
    while (n*m+1).is_prime()==False:
        m=m+1;
    return m
```

Por ejemplo, con $n = 8$, el m más bajo con el que daríamos sería el 2, ya que $8 \cdot 2 + 1 = 17$ es primo.

```
gener(8)
```

```
2
```

A continuación, definimos el programa que nos dará como resultado el polinomio el cual tiene a $\mathbb{Z}/n\mathbb{Z}$ como grupo de Galois (entonces, lógicamente, el único dato que necesita para compilar es la n), y lo explicamos brevemente:

```
def cicl(n):
    x=polygen(QQ,'x');
    m=gener(n);
    p=(n*m)+1;
    if m==1:
        return cyclotomic_polynomial(p)
    Unidp=CyclotomicField(p).galois_group();
    H=Unidp;
    i=0;
    while H.order()!=m:
        H=Unidp.subgroup([Unidp[i]]);
        i=i+1;
```

```
    E=H.fixed_field()[0];
    return E.defining_polynomial()
```

Para empezar, se establece el cuerpo en el que se definen los polinomios empleados (primera línea de código), y se busca, en la siguiente línea, la m cumpliendo las condiciones explicadas. En la siguiente línea se toma ese número primo $p = n \cdot m + 1$, y si coincide que $n + 1 = p$ primo, ya se tiene que $\mathbb{Z}/n\mathbb{Z}$ es grupo de Galois de la extensión ciclotómica $\mathbb{Q}(\epsilon)|\mathbb{Q}$, con ϵ raíz primitiva p-ésima de la unidad, por lo tanto, el polinomio que define esa extensión será el irreducible de ϵ; $\Phi_p(x)$, que por ser p primo coincide con el polinomio $x^{p-1} + x^{p-2} + \cdots + x + 1$.

Un ejemplo de este caso sería $\mathbb{Z}/4\mathbb{Z}$, que es grupo de Galois del polinomio $x^4 + x^3 + x^2 + x + 1$:

```
cicl(4)
```

```
x^4 + x^3 + x^2 + x + 1
```

Sin embargo, puede ser que $m \neq 1$, y así $n+1$ no sería primo. En ese caso, como hicimos en la demostración, se define el grupo de las unidades de $\mathbb{F}_p$ como `Unidp`, y buscamos H como en la demostración del teorema 3.9, primero asumimos que es el grupo total y después vamos probando con cada subgrupo de $(\mathbb{F}_p)^*$ hasta que demos con uno que tenga orden m (eso quiere decir el bucle `while`), que será único por la proposición 3.3. Para terminar, sacamos el cuerpo fijo por H (`fixed field`) y tomamos el polinomio que define la extensión de $\mathbb{Q}$ sobre ese cuerpo mediante el comando `defining polynomial`.

Un ejemplo en este caso es $\mathbb{Z}/5\mathbb{Z}$, que es grupo de Galois del polinomio $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$:

```
cicl(5)
```

```
x^5 - x^4 - 4*x^3 + 3*x^2 + 3*x - 1
```

Capítulo 4

Grupos abelianos finitos

Aprovechando que hemos resuelto el problema para grupos cíclicos finitos, presentamos un teorema que nos ayudará a resolverlo en grupos abelianos finitos, a partir de lo que sabemos sobre el problema en grupos cíclicos:

Teorema 4.1. *(Teorema Fundamental de los Grupos Abelianos Finitos). Si G es un grupo abeliano finito, entonces se tiene el siguiente isomorfismo de grupos; $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ con $n_k \mid n_{k+1}$ para todo k.*

Demostración. Por inducción en el orden del grupo G (abeliano finito), sea g un elemento con orden maximal, si $G \simeq \langle g \rangle$ cíclico ya está, sino, por el lema 1.32, $G \simeq \mathbb{Z}/|g|\mathbb{Z} \times H$, y que por ser $|H| < |G|$ le aplicamos nuestra hipótesis de inducción y queda demostrado el resultado. □

4.1. Problema Inverso de Galois en grupos abelianos finitos

Lema 4.2. *Sean $n_1, \ldots, n_r$ naturales coprimos entre sí, y ϵ_i una raíz primitiva n_i-ésima de la unidad, entonces se tiene que $\epsilon = \epsilon_1 \ldots \epsilon_r$ es una raíz $n_1 \ldots n_r$-ésima de la unidad y además* $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \simeq (\mathbb{Z}/n_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^*$.

Demostración. Es claro que el orden de ϵ va a ser $n_1 \ldots n_r$, por ser estos naturales coprimos entre si, y por la forma que tienen las raíces de la unidad.

Así, por la proposición 1.82 se tiene que $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \simeq (\mathbb{Z}/n_1 \ldots n_r\mathbb{Z})^*$. Simplemente aplicando la proposición 1.10 se tendrá el isomorfismo:

$$\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \simeq (\mathbb{Z}/n_1 \ldots n_r\mathbb{Z})^* \simeq (\mathbb{Z}/n_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^*$$

□

Teorema 4.3. *(Solución del problema inverso de Galois para grupos abelianos finitos). Sea G un grupo abeliano finito, entonces existe una extensión $E|\mathbb{Q}$ tal que $G \simeq \mathrm{Gal}(E|\mathbb{Q})$.*

Demostración. Por el Teorema Fundamental de los Grupos Abelianos Finitos 4.1 sabemos que todo grupo abeliano finito es de la forma $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$.

Por la proposición 3.7 existirán un conjunto de primos $p_1, \dots p_r$ tales que $p_i - 1 = n_i \cdot m_i$. Empleando la proposición 3.3 tenemos que existen unos subgrupos $H_i < (\mathbb{Z}/p_i\mathbb{Z})$ únicos de orden m_i.

Tomamos $\epsilon = \epsilon_1 \cdot \cdots \cdot \epsilon_r$ una raíz $p_1 \cdot \cdots \cdot p_r$-ésima de la unidad, que por el lema 4.2 cumple que $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \simeq (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^*$.

Por ser este grupo abeliano, se tendrá que $H_1 \times \cdots \times H_r \lhd \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$cuyo cuerpo fijo llamaremos E, y aplicando el Teorema Fundamental de la Teoría de Galois tenemos que $E|\mathbb{Q}$ es de Galois y:

$$\mathrm{Gal}(E|\mathbb{Q}) \simeq \frac{\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})}{H_1 \times \cdots \times H_r} \simeq \frac{(\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^*}{H_1 \times \cdots \times H_r} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} = G.$$

El último isomorfismo se tiene de la demostración de la proposición 3.3, ya que:

$$\frac{(\mathbb{Z}/p_i\mathbb{Z})^*}{H_i} \simeq \mathbb{Z}/n_i\mathbb{Z}.$$

□

4.2. Cálculo de polinomios con grupo de Galois abeliano finito

Como cabe esperar, en este capítulo emplearemos parte del código del anterior, ya que los grupos abelianos finitos y los cíclicos están muy relacionados, por el Teorema Fundamental de los Grupos Abelianos Finitos 4.1. De hecho, necesitaremos de la siguiente proposición para relacionar ambos códigos:

Proposición 4.4. *Dados $f_1, \dots, f_k \in \mathbb{Q}[X]$ polinomios irreducibles con grupos de Galois cíclicos; pongamos $\mathbb{Z}/n_1\mathbb{Z}, \dots, \mathbb{Z}/n_k\mathbb{Z}$ respectivamente. Para cada $j \in \{1, \dots, k\}$ tomemos L_j como el cuerpo de escisión de $\{f_1, \dots, f_j\}$, y supongamos que los f_i son irreducibles también en $L_j[X]$ para todo $i > j$, entonces, siendo $E = L_k$ el cuerpo de escisión de $\{f_1, \dots, f_k\}$, se tiene que* $\mathrm{Gal}(E|\mathbb{Q}) = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$.

Demostración. Lo probaremos por inducción. Si $k = 2$ tenemos dos polinomios f_1, f_2 irreducibles, cumpliendo que $\mathrm{Gal}(L_1|\mathbb{Q}) = \mathbb{Z}/n_1\mathbb{Z}$, y $\mathrm{Gal}(F_2|\mathbb{Q}) = \mathbb{Z}/n_2\mathbb{Z}$, siendo L_1 cuerpo de escisión de f_1, y F_2 cuerpo de escisión de f_2.

Si tomamos L_2 el cuerpo de escisión de $\{f_1, f_2\}$ como definimos en la proposición anterior, podemos trazar los elementos de su grupo de Galois $\mathrm{Gal}(L_2|\mathbb{Q})$ simplemente mediante la composición de los automorfismos de $\mathrm{Gal}(L_1|\mathbb{Q})$ con los de $\mathrm{Gal}(F_2|\mathbb{Q})$, ya que como L_1 y F_2 son subcuerpos de L_2, se tendrá que $\mathrm{Gal}(L_1|\mathbb{Q}), \mathrm{Gal}(F_2|\mathbb{Q}) < \mathrm{Gal}(L_2|\mathbb{Q})$ y así está bien definida la composición en este grupo, que precisamente será isomorfo a $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ por la manera en la que lo hemos construido.

$$\begin{aligned} \mathrm{Gal}(L_1|\mathbb{Q}) \times \mathrm{Gal}(F_2|\mathbb{Q}) &\longrightarrow \mathrm{Gal}(L_2|\mathbb{Q}) \\ (\sigma, \phi) &\longmapsto \phi \circ \sigma \end{aligned}$$

Una vez demostrado que funciona para $k = 2$, es fácil ver que se cumple para cualquier k natural, ya que el grupo $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ se puede expresar como producto de dos grupos $G \times \mathbb{Z}/n_k\mathbb{Z}$, donde, por hipótesis de inducción, $G = \mathrm{Gal}(L_{k-1}|\mathbb{Q})$. Por el Teorema del Elemento Primitivo 1.64, podríamos tomar un irreducible g_k que definiese la extensión $L_{k-1}|\mathbb{Q}$, por tanto, mediante el razonamiento del párrafo anterior, podríamos llegar a que $\mathrm{Gal}(L_k|\mathbb{Q}) = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, siendo L_k el cuerpo de escisión de $\{g, f_k\}$ que coincide con el de $\{f_1, \ldots, f_k\}$.

□

Una vez más, utilizaremos de guía la demostración del Teorema de Solución del problema para grupos abelianos finitos. Para empezar, debemos factorizar el grupo abeliano en distintos grupos cíclicos, agrupando las potencias (es decir, no nos vale la función de SageMath que, por ejemplo, factorizando el 18 devuelve $3^2, 2$, necesitaríamos 9 y 2), así que para ello emplearemos el siguiente código:

```
def factoriza(n):
    L=[];
    S=n.factor()
    for i in srange(len(S)):
        L.append((S[i][0])^(S[i][1]));
    return L
```

Como vemos en el ejemplo al que nos referíamos, en el caso del programa "factoriza", se cumple lo que queríamos:

```
factoriza(18)
```

```
[2, 9]
```

La factorización debe seguir un orden de menor a mayor, por lo tanto debemos definir dos códigos, uno que busque el máximo de la lista, y otro que lo reordene:

```
def maxi(M):
    i=0;
    for k in srange(len(M)):
        if M[k]>i:
            i=M[k];
    return i
```

```
def ordena(M):
    m=maxi(M);
    S=[];
    for j in [0..m]:
        if j in M:
            l=M.count(j);
            for i in srange(l):
                S.append(j);
    return S
```

Ahora ya tenemos el grupo definido, así que procedemos a buscar el polinomio del que es grupo de Galois:

```
def grupoabeliano(M):
    x=polygen(QQ,'x');
    if len(M)==1:
        return cicl(M[0])
    M=ordena(M);
    J=[];
    for i in srange(len(M)):
        if (M[i] in J)==False:
            J.append(M[i]);
    E=QQ;
    for i in srange(len(J)):
        k=1;
        l=M.count(J[i]);
        for j in srange(l):
            y=polygen(E,'y');
```

```
            G=ciclico2(J[i],k);
            f=G[0].subs(x=y);
            while (f.is_irreducible())==False:
                k=k+1;
                G=ciclico2(J[i],k);
                f=G[0].subs(x=y);
            L.<a>=NumberField(f);
            E.<b>=L.absolute_field();
    return E.defining_polynomial()
```

Para empezar el código, definimos en $\mathbb{Q}$ el polinomio que queremos hallar, y se introduce al programa el grupo abeliano como producto de cíclicos (la lista `M`), como dicta el Teorema Fundamental de los Grupos Abelianos 4.1. A continuación, se buscan los elementos distintos de la factorización para elaborar las extensiones con grupo de Galois cíclico como en el anterior capítulo, y se utiliza una variación del programa redactado en tal capítulo cuando se presentan dos grupos cíclicos del mismo orden:

```
def gen2(n,k):
    while(n*k+1).is_prime()==False:
        k=k+1;
    return k
```

```
def ciclico2(n,k):
    x=polygen(QQ,'x');
    m=gen2(n,k);
    p=(n*m)+1;
    if m==1:
        return cyclotomic_polynomial(p)
    Unidp=CyclotomicField(p).galois_group();
    H=Unidp;
    i=0;
    while H.order()!=m:
        H=Unidp.subgroup([Unidp[i]]);
        i=i+1;
    E=H.fixed_field()[0];
    return[E.defining_polynomial(),m]
```

En la última parte del código de resolución del problema en grupos abelianos, simplemente se aplica la proposición 4.4 y se determinan en orden las extensiones de cuerpos, redefiniendo la variable y para que cada polinomio que construyamos sea irreducible en el cuerpo anteriormente computado `L` (como dicta la proposición). Finalmente construimos el cuerpo de escisión E de todos los polinomios elaborados, y el programa devuelve el polinomio que define al cuerpo E, es decir, el polinomio del que es grupo de Galois el grupo abeliano que indicamos.

Para ejemplificar este apartado, tomamos el grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, el cual se nos da en el programa que es grupo de Galois del polinomio $x^10 + 3x^9 - 11x^8 - 32x^7 + 30x^6 + 92x^5 - 4x^4 - 63x^3 - 11x^2 + 5x + 1$. Posteriormente comprobamos que el grupo de Galois de este polinomio es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$:

```
f=grupoabeliano(M);f
```

```
x^10 + 3*x^9 - 11*x^8 - 32*x^7 + 30*x^6 + 92*x^5 - 4*x^4 - 63*x^3 - 11*x^2
+ 5*x + 1
```

```
G=f.galois_group();G
```

```
Transitive group number 1 of degree 10
```

Este caso se podía haber resuelto por el programa que atribuimos a resolver el problema en grupos cíclicos, ya que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/10\mathbb{Z}$ (porque $\gcd(5, 2) = 1$), pero de esta manera comprobamos que nuestro programa de grupos abelianos también funciona para grupos cíclicos (que, en efecto, también son abelianos).

Otro ejemplo que podemos poner es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, el cual se diferencia bastante del anterior por no ser isomorfo a un cíclico ($\gcd(2, 4) = 2$), y obtenemos que es grupo de Galois del polinomio $x^8 + 2x^7 + 8x^5 + 27x^4 + 62x^3 + 117x^2 + 23x + 29$:

```
M=[2,4];M
```

```
[2, 4]
```

```
f=grupoabeliano(M);f
```

```
x^8 + 2*x^7 + 8*x^5 + 27*x^4 + 62*x^3 + 117*x^2 + 23*x + 29
```

```
G=f.galois_group();G
```

`Transitive group number 2 of degree 8`

Bajo la comprobación hecha determinamos que el grupo de Galois del polinomio obtenido es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (`Transitive group number 2 of degree 8`).

Capítulo 5

Grupos simétricos

Para empezar este capítulo, introduciremos el Teorema de Dedekind, del cual no veremos demostración, pero nos será de gran ayuda para construir el polinomio del que es grupo de Galois S_n para n dado.

Teorema 5.1. *(Teorema de Dedekind). Sea $f \in \mathbb{Z}[X]$ separable de grado n y p un primo tal que $f(x)$ se puede descomponer en $\mathbb{F}_p[X]$ como:*

$$\tilde{f}(x) \equiv f_1(x) \cdots f_r(x) \in \mathbb{F}_p[X]$$

donde los $f_i(x)$ son polinomios mónicos distintos, de grado n_i.

Entonces se tiene que $Gal_{\mathbb{Q}}(f)$, como subgrupo de S_n, posee una permutación $(n_1, \ldots, n_r)$ (composición de n_i-ciclos).

Observación 5.2. Se entiende $\mathrm{Gal}_{\mathbb{Q}}(f)$ como un subgrupo de S_n por el Teorema de Cayley 1.26, que nos dice que todo grupo finito puede ser expresado como un subgrupo de un grupo de permutaciones.

5.1. Problema Inverso de Galois en grupos simétricos

Antes de empezar con el teorema de solución del problema en este tipo de grupos, estudiaremos los polinomios de grado n irreducibles en $\mathbb{F}_p[X]$ para p primo, ya que son necesarios para la demostración.

Proposición 5.3. *Para todo $n \in \mathbb{N}$, existe un polinomio mónico, irreducible y de grado n en $\mathbb{F}_p[X]$ (siendo p primo).*

Demostración. Procederemos por inducción en n, ya que el resultado es obvio si $n = 1$.

Tomando el polinomio $f = x^{p^n} - x = x \cdot (x^{p^n-1} - 1) \in \mathbb{F}_p[X]$, con E su cuerpo de escisión y R_f el conjunto de sus raíces.

Está claro que f tiene todas sus raíces distintas porque 0 es una raíz, y $(x^{p^n-1} - 1$ es separable, por ser coprimo con su derivada $((p^n - 1)x^{p^n-2})$ en $\mathbb{F}_p[X]$ (proposición 1.57), con raíces no nulas. Así tenemos que R_f tiene p^n elementos.

Comprobemos que R_f es un cuerpo. Es claro que $0, 1 \in R_f$, y sabemos que cada un elemento x está en R_f si, y solamente si, $x^{p^n} = x$. Vemos pues que para $x, y \in R_f$, $(x \cdot y)^{p^n} = x^{p^n} \cdot y^{p^n} = x \cdot y$, entonces $x \cdot y \in R_f$, y de manera similar, $(x + y)^{p^n} = x^{p^n} + y^{p^n} = x + y$ por estar operando sobre una extensión de $\mathbb{F}_p$. Concluimos que, en efecto, R_f es un cuerpo, contenido en E, por tanto, $R_f = E$.

En las condiciones que definimos el cuerpo E, y aplicando el teorema 1.62, obtenemos que $E = \mathbb{F}_p(\alpha)$ y que $[E : \mathbb{F}_p] = n$, así que ya tendríamos $\mathrm{Irr}_{\mathbb{F}_p}(\alpha)$ un polinomio mónico irreducible de grado n sobre $\mathbb{F}_p$.

□

Como en el primer capítulo ya vimos resultados relacionados con S_3 y sus subgrupos, nos limitaremos a resolver, en esta sección, el problema inverso para los grupos simétricos S_n con $n \geq 4$.

Teorema 5.4. *(Solución del problema inverso de Galois para grupos simétricos). Para todo $n \geq 4$ existe una extensión de cuerpos $E|\mathbb{Q}$ tal que* $\mathrm{Gal}(E|\mathbb{Q}) \simeq S_n$.

Demostración. En esta demostración construiremos con detalle el polinomio del cual S_n será grupo de Galois.

Mediante la proposición 5.3, podemos tomar tres polinomios f_2, f_3, f_5 sobre $\mathbb{F}_2$, $\mathbb{F}_3$ y $\mathbb{F}_5$ respectivamente, de grado n y verificando:

- f_2 irreducible sobre $\mathbb{F}_2[X]$.
- $f_3 = g_3 \cdot h_3$ con g_3 irreducible de grado $n - 1$ y h_3 de grado 1, ambos coprimos y definidos sobre $\mathbb{F}_3[X]$.
- Si n es par, $f_5 = r_5 \cdot h_5 \cdot g_5$ siendo h_5 grado 2, r_5 grado 1, g_5 grado $n-3$, irreducibles, coprimos y definidos sobre $\mathbb{F}_5[X]$. Si n impar, $f_5 = h_5 \cdot g_5'$ con h_5 de grado 2, g_5' de grado $n - 2$ irreducibles, coprimos y definidos sobre $\mathbb{F}_5[X]$.

Sabemos ahora que, por el Teorema Chino de los Restos 1.36, la reducción en $\mathbb{F}_p[X]$ del siguiente polinomio mónico f va a ser congruente con f_p.

$$f = -15 \cdot f_2 + 10 \cdot f_3 + 6 \cdot f_5.$$

Dado el cuerpo de escisión E sobre $\mathbb{Q}$ de f, sabemos, por la proposición 1.44, que f es irreducible sobre $\mathbb{Q}$ por ser irreducible f_2, su clase en $\mathbb{F}_2[X]$. Y empleando la proposición 2.1, tendremos que el grupo de Galois es un subgrupo normal de S_n.

Como la clase en $\mathbb{F}_3[X]$ de f es $f_3 = g_3 \cdot h_3$, donde h_3, g_3 son mónicos y coprimos, f no tendrá raíces múltiples sobre $\mathbb{F}_3$ y podremos aplicar el Teorema de Dedekind 5.1, el cual nos asegura que $\mathrm{Gal}(E|\mathbb{Q})$, como subgrupo de S_n, tiene una permutación $(1, n-1)$, o lo que es lo mismo, un $(n-1)$-ciclo.

Razonando de la misma manera en $\mathbb{F}_5$, tendríamos, o bien una permutación $(2, n-2)$ si n fuera impar, o $(n-3, 2)$ si fuera n par, pero de todas formas, elevando tal permutación a $n-2$ o $n-3$ (respectivamente), daríamos con que $\mathrm{Gal}(E|\mathbb{Q})$ tiene una trasposición, por ser números impares.

Para concluir, y teniendo en cuenta lo demostrado hasta ahora, debemos probar que cualquier trasposición de la forma (r, t) (con $r, t \leq n$) pertenece a $\mathrm{Gal}(E|\mathbb{Q})$, ya que S_n tiene como generadores las trasposiciones de ese tipo, por el teorema 1.22. Pues bien, lo demostraremos por inducción, ya que como vimos en el párrafo anterior, $\mathrm{Gal}(E|\mathbb{Q})$ tiene por lo menos una trasposición, y anteriormente vimos que poseía un ciclo. Por lo tanto podemos establecer como hipótesis de inducción que $\mathrm{Gal}(E|\mathbb{Q})$ posee un ciclo de la forma $(1, 2, \ldots, n-1)$, y otro de la forma (i, j), con $i < j < n$, y debemos demostrar que para cualquier $r, t \leq n$ existe una trasposición (r, t) en el grupo de Galois de f.

En efecto, se tiene que $(1, 2, \ldots, n-1)(i, j)(1, 2, \ldots, n-1)^{-1} = (i+1, j+1) \in \mathrm{Gal}(E|\mathbb{Q})$ por ser conjugación de elementos del grupo, y aplicando $n - j$ veces esta operación al elemento (i, j) obtendríamos el elemento $(i+n-j, n)$, que conjugado de nuevo con el ciclo $(1, \ldots, n-1)$ obtendríamos un elemento $(i+n-j+1, n)$ (y si lo hubiéramos conjugado con $(1, \ldots, n-1)^{-1}$ obtendríamos $(i+n-j-1, n)$. Es decir, que para cualquier $k < n$ se tiene que $(k, n) \in \mathrm{Gal}(E|\mathbb{Q})$, y luego cualquier trasposición $(r, t) = (r, n)(t, n)(r, n) \in \mathrm{Gal}(E|\mathbb{Q})$, por tanto ya tenemos probado que cualquier trasposición (r, t) con $r, t \leq n$ está en $\mathrm{Gal}(E|\mathbb{Q})$, así que necesariamente $\mathrm{Gal}(E|\mathbb{Q}) \simeq S_n$.

□

5.2. Cálculo de polinomios con grupo de Galois simétrico

Para calcular polinomios cuyo grupo de Galois es isomorfo a S_n simplemente hay que guiarse de la demostración anterior, en la cual probamos que $f = -15 \cdot f_2 + 10 \cdot f_3 + 6 \cdot f_5$, tal y como la definíamos, tenía de grupo de Galois un grupo simétrico.

En el primer subprograma definimos el polinomio irreducible mónico de grado n sobre el cuerpo $\mathbb{F}_p$, que como vimos en la demostración de la proposición 5.3, se hallaría a partir

de las raíces de $x^{p^n} - x$ (que es separable pero no irreducible), que forman un cuerpo de escisión de p^n elementos, y ese cuerpo está generado por un irreducible en $\mathbb{F}_p[X]$, el cual obtenemos como resultado en el siguiente programa:

```
def irred(p,n):
    R.<x>=PolynomialRing(GF(p));
    f=x^(p^n)-x;
    F.<a>=f.splitting_field();
    irred=F.polynomial().subs(a=x);
    return irred
```

Unos ejemplos de irreducibles que podemos trazar serían los de grado 5 en $\mathbb{F}_2$, $\mathbb{F}_3$ o $\mathbb{F}_5$, que nos dan $x^5 + x^2 + 1$, $x^5 + 2x + 1$ y $x^5 + 4x + 3$, respectivamente:

```
irred(2,5);irred(3,5);irred(5,5)
```

```
x^5 + x^2 + 1
x^5 + 2*x + 1
x^5 + 4*x + 3
```

Como comentábamos, para calcular el polinomio simplemente debemos seguir la construcción que dicta el teorema 5.4 (exceptuando si $n = 1, 2, 3$, que ya lo vimos en el capítulo 2), definiendo los polinomios que se requieren en la demostración y cambiando su anillo de definición a $\mathbb{Q}$, ya que en el programa `irred` los definíamos sobre $\mathbb{F}_p$. Finalmente se construye $f = -15 \cdot f_2 + 10 \cdot f_3 + 6 \cdot f_5$ que es, como probamos, el polinomio cuyo grupo de Galois es isomorfo a S_n.

```
def gruposim(n):
    x = polygen(QQ,'x');
    f2 = irred(2,n)
    g3 = irred(3,n-1);
    h3 = irred(3,1);
    f3 = g3*h3;
    h5 = irred(5,2);
    if (n)%2==1:
        g5 = irred(5,n-2);
        f5 = h5*g5;
    else:
```

```
        g5 = irred(5,n-3);
        r5 = irred(5,1);
        f5 = h5*g5*r5;
    f2 = f2.change_ring(QQ);
    f3 = f3.change_ring(QQ);
    f5 = f5.change_ring(QQ);
    f = -15*f2 + 10*f3 + 6*f5;
    return f
```

Podemos comprobar el funcionamiento del programa con un ejemplo, pongamos S_5. Como se ve en el código, el polinomio cuyo grupo de Galois es isomorfo a S_5 es $x^5+44x^4-15x^2+38x-9$:

```
fsim=gruposim(5);fsim
```

```
x^5 + 44*x^4 - 15*x^2 + 38*x - 9
```

```
Gsim=fsim.galois_group();Gsim
```

```
Transitive group number 5 of degree 5
```

```
Gsim.is_isomorphic(SymmetricGroup(5))
```

```
True
```

Bibliografía

[1] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1996.

[2] C. U. Jensen, A. Ledet, N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, Cambridge, 2002.

[3] J. S. Milne, *Fields and Galois Theory*, 2022. `https://www.jmilne.org/math/CourseNotes/FT.pdf`

[4] T. Senovilla Polo, *Aspectos teóricos y computacionales del problema inverso de Galois*, Universidad Autónoma de Madrid, 2019.