Teorema 90 de Hilbert

Autor
Andrés Luciano Barraza Medina

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2023

Teorema 90 de Hilbert

Autor
Andrés Luciano Barraza Medina

Trabajo de grado como requisito para optar al título de:
Matemático

Director:
Héctor Edonis Pinedo Tapia
Ph.D. en Matemáticas

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2023

Dedicatoria

En memoria de mi madre (q.e.p.d), Triny.

Agradecimientos

Me agradezco exclusivamente a mí y al azar. ¿Por qué?, sin estos dos elementos, de seguro no habría tenido una familia que me apoyara hasta el final, sin importar, en muchos casos, mi carácter. En particular, no habría tenido esa fuente de inspiración en mi vida como fue y será, mi madre. Sin el azar deambulando en mi vida no habría tenido la oportunidad de conocer a amigos como los tuve, con unas cualidades y aptitudes fenomenales pero más que ello con una calidad humana que hizo de mi instancia en la universidad una experiencia agradable. Y por último, con la ausencia de estos factores, no habría conocido a mi director, Héctor Pinedo Tapia, un profesor que admiro por la naturalidad con la desarrolla su trabajo, sus contribuciones hicieron posibles la realización de este humilde trabajo.

CONTENIDO

LISTA DE FIGURAS

pág.

“If I feel unhappy, I do mathematics to become happy. If I am happy, I do mathematics to keep happy”.

Pál Turán

RESUMEN

TÍTULO: TEOREMA 90 DE HILBERT [*]

AUTOR: ANDRÉS LUCIANO BARRAZA MEDINA [**]

PALABRAS CLAVE: HILBERT, APLICACIONES, PITAGÓRICAS.

DESCRIPCIÓN:

En este trabajo, abordamos el Teorema 90 de Hilbert empezando con los elementos básicos necesarios para definir este resultado. Posterior a esto, veremos algunas aplicaciones interesantes del Teorema 90 de Hilbert en la solución de problemas matemáticos. Problemas que involucran desde triplas pitagóricas hasta condiciones para la irreducibilidad de polinomios. Por último, mostraremos una generalización de la solución para una ecuación de Pell.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Dr. Héctor Edonis Pinedo Tapia

ABSTRACT

TITLE: HILBERT'S THEOREM 90 [*]

AUTHOR: ANDRÉS LUCIANO BARRAZA MEDINA [**]

KEYWORDS: HILBERT, APPLICATIONS, PYTHAGOREAN.

DESCRIPTION:

In this document, we address Hilbert's Theorem 90 by starting with the basic elements necessary to define this result. After this, we will see some interesting applications of Hilbert's Theorem 90 in solving mathematical problems. Problems from Pythagorean triples to conditions for polynomial irreducibility. Finally, we will show a generalization of the solution for a Pell equation.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Dr. Hector Edonis Pinedo Tapia

INTRODUCCIÓN

En 1897, David Hilbert presentó su libro *Theorie der Algebraischen Zahlkorper* en el cual aparece un teorema 90, que en términos modernos establece que, dada una extensión de Galois $E|F$ con grupo de Galois $G = Gal(E|F)$, vale que $H^1(G, E^\times) = 0$, es decir, el primer grupo de cohomología de G con valores en $E^\times$ es trivial. Este teorema es el principal objeto de estudio en el presente trabajo y es conocido como *Teorema 90 de Hilbert*, debido a que fue en esta obra donde obtuvo reconocimiento, acogió el nombre de este matemático, sin embargo, este teorema fue descubierto por Ernst Eduard Kummer para el caso especial de la extensión de campos $\mathbb{Q}(\zeta_p)|\mathbb{Q}$, siendo ζ_p una raíz $n-$ésima de la unidad y posteriormente generalizado, como se puede observar en [1] por Emmy Noether. Este resultado basado en la teoría de extensiones de campos, tiene diversas aplicaciones desde condiciones para la irreducibilidad de polinomios hasta la obtención de triplas pitagóricas.

En este proyecto estamos interesados en un cierto tipo de extensiones, llamadas extensiones de Galois. Estas extensiones desempeñan un papel importante en álgebra debido a que implican diversos resultados, como por ejemplo, la demostración de la imposibilidad de una solución general para encontrar las raíces de polinomios por medio de radicales de grado mayor que 5, además, para nuestro caso servirá de gran ayuda para fundamentar el resultado principal.

Nuestro propósito es estudiar el trabajo de Seewoo Lee [2] en el que se discuten los elementos básicos necesarios para comprender la demostración del Teorema 90 de Hilbert, posterior a ello, observar este resultado en su versión clásica y moderna y concluir mostrando las diversas aplicaciones que tiene el Teorema 90 de Hilbert para la solución de problemas en varias ramas de la matemática.

El trabajo se encuentra estructurado de la siguiente manera. Primero recordamos unos conceptos básicos sobre extensiones de campos, seguido a esto, introducimos los elemen-

---

[1] A.N ARTIN Emil y Milgram. *Galois Theory*. Notre Dame Mathematical Lectures, New Jersey, 1971.

[2] Seewoo LEE. “Hilbert’s theorem 90”. En: *Berkeley University Library* (2018).

tos necesarios de la teoría de Galois, posteriormente, presentamos el concepto de $G-$módulo, siendo G un grupo, hasta llegar a enunciar el Teorema 90 de Hilbert concluyendo con algunas aplicaciones de este resultado para varios problemas en la matemática. Por ejemplo, procederemos a encontrar la solución de la ecuación $x^2 + y^2 = 1$, para x, y números racionales, llegando a una pequeña generalización de este problema. Además de esto, estamos interesados en trabajar sobre extensiones de Kummer, en particular, veremos que en el caso de una extensión cíclica de Galois que contenga una raíz $n-$ésima de la unidad, podemos mediante el Teorema 90 de Hilbert, conocer la forma explícita de esta extensión. Por otra parte, veremos una condición de irreducibilidad para polinomios con cierta forma y estructura, lo que nos llevará a probar, por ejemplo, que el polinomio, $x^p - x - 1$ es irreducible sobre $\mathbb{F}_p$. Por último nos sumergiremos en el campo de funciones racionales de una variable, observando que, para funciones que cumplan ciertas condiciones algebraicas, es posible hallar de manera explicita la apariencia de estas funciones.

1. EXTENSIONES DE CAMPOS

El propósito de este capítulo es presentar los elementos básicos y necesarios para comprender la idea en que se formula este trabajo de grado. Se expondrán los resultados en forma de teoremas y proposiciones abordando la teoría de extensiones de campos, mismos, que serán utilizados en gran parte del recorrido de estas notas, esto, con el objetivo de aproximarnos a los resultados principales. Las demostraciones de estos resultados pueden ser consultadas en por ejemplo ([3] y [4]). La sección 4.20 en [3] ofrece información detallada sobre los temas centrales donde se fundamenta este trabajo, por lo que invitamos al lector revisarla para una mayor comprensión del presente documento.

1.1. PRELIMINARES

Definición 1.1.1. *Sea $(F, +, \cdot)$ un campo. Decimos que un campo E es una extensión de F si F es un subcampo de E. Si E es una extensión de F escribimos $E|F$.*

Ejemplo 1.1.2. *Es fácil ver que $\mathbb{R}|\mathbb{Q}$ es una extensión del campo de números racionales con las operaciones de suma y producto usuales en los números reales.*

Notación: Dado un campo F, denotaremos por $F[x]$ a su anillo de polinomios. Si todas las raíces de un polinomio $p(x)$ están en un campo, diremos que el polinomio rompe en dicho campo.

Enunciaremos a continuación el *Teorema de Kronecker* el cual garantiza la existencia de raíces para todo polinomio no nulo en alguna extensión. Este resultado es considerado como el Teorema Fundamental de la teoría de campos.

Teorema 1.1.3. *Sean F un campo y $f(x)$ un polinomio no constante en $F[x]$. Entonces existe una extensión E de F en la cual $f(x)$ tiene una raíz.*

Ejemplo 1.1.4. *Considere $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Dado que $f(x)$ se descompone en $\mathbb{R}$, como $f(x) = (x-\sqrt{2})(x+\sqrt{2})$, sigue que $\mathbb{R}$ es una extensión de $\mathbb{Q}$ que contiene las raíces de $f(x)$.*

---

[3] J.A GALLIAN. *Contemporary Abstract Algebra*. Cengage learning, Minnesota, 2010.

[4] A.N DUMMIT D.S y FOOTE. *Abstract Algebra.* John Wiley & Sons, Vermont, 2004.

Una pregunta que resulta natural es si dado un polinomio $f(x)$ con coeficientes en algún campo, podemos encontrar una extensión que contenga todas sus raíces y además sea la menor, en el sentido de contenencia. La respuesta es sí y lo enmarcaremos en la siguiente definición.

Definición 1.1.5. *Sean E una extensión del campo F y $f(x) \in F[x]$. Decimos que $f(x)$ se descompone en E cuando podemos escribir a $f(x)$ como producto de factores lineales en $E[x]$. Si $f(x)$ se descompone en E, pero no lo hace en un subcampo propio de E, decimos que E es un campo de ruptura de $f(x)$ sobre F.*

Con la ayuda del Teorema de Kronecker 1.1.3 e inducción sobre el grado de $f(x)$, se prueba la existencia de un campo de ruptura para $f(x)$. Más exactamente se tiene.

Proposición 1.1.6. *Sean F un campo y $p(x) \in F[x]$ un polinomio no constante. Entonces existe E campo de ruptura de $f(x)$ sobre F.*

Si el lector requiere una prueba detallada de este resultado en [1] la puede encontrar con facilidad.

Ejemplo 1.1.7. *Sea $p(x) = x^2 - 2$ en $\mathbb{Q}[x]$ el polinomio que consideramos en $Ejemplo$ 1.1.4. Vimos que $p(x)$ rompe en $\mathbb{R}$, sin embargo, el campo de ruptura para $p(x)$ viene dado por $\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2} \mid r,s \in \mathbb{Q}\}$.*

Un ejemplo un poco más general, que permite visualizar la definición de campo de ruptura viene dado a continuación.

Ejemplo 1.1.8. *Si $f(x) = x^2 + a^2$ en $\mathbb{C}[x]$, con $a \in \mathbb{R}$, es claro que $f(x)$ rompe en $\mathbb{C}$, dado que $f(x) = (x - ai)(x + ai)$. Sin embargo, un campo de ruptura de $f(x)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(i) = \{r + si | r, s \in \mathbb{Q}\}$.*

Notemos que para un polinomio $p(x)$ con coeficientes en F, el campo de ruptura de $p(x)$ es el menor campo que contiene a F y a sus raíces simultáneamente. A pesar que, por la Proposición 1.1.6, garantizamos la existencia del campo de ruptura, pero no afirmamos nada acerca de la unicidad. Una pregunta válida es, dado $p(x) \in F[x]$ ¿es único su campo de ruptura? La respuesta a esta pregunta es el contenido del siguiente resultado.

Proposición 1.1.9. *Sean F un campo y $f(x) \in F[x]$. Entonces cualquier dos campos de ruptura de $p(x)$ son isomorfos.*

Un hecho muy interesante que se deduce de esta proposición queda plasmado a continuación.

Ejemplo 1.1.10. *Sea* $p(x) = x^2 + 1 \in \mathbb{R}[x]$*, es fácil ver que,* $\mathbb{R}[x]/\langle x^2 + 1\rangle$ *y* $\mathbb{R}(i) = \{r+si|r, s \in \mathbb{R}\}$ *son campos de rupturas de* $p(x)$ *sobre* $\mathbb{R}$*, así las cosas, por la Proposición 1.1.9, tenemos:*

$$\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{R}(i) = \{r + si|r, s \in \mathbb{R}\} \cong \mathbb{C} \tag{1.1}$$

Este resultado fue descubierto por el matemático francés *Augustin Louis Cauchy* en 1847, posteriormente fue generalizado y hoy es el llamado *Teorema de Kronecker*.

Definición 1.1.11. *Decimos que* $h(x)$ *es un polinomio reducible sobre F si existen elementos no unidades* $f(x), h(x), \in F[x]$ *tales que* $h(x) = f(x)g(x)$*. Caso contrario, decimos que* $h(x)$ *es irreducible sobre F.*

Si E es una extensión de campos de F, es posible ver a E como espacio vectorial sobre F, en otras palabras, los elementos de E son vectores y los de F escalares. Así las cosas, tiene sentido el siguiente concepto.

Definición 1.1.12. *Sea* $E|F$ *una extensión, decimos que E es una extensión finita, si la dimensión de E como F-espacio vectorial es finita y lo denotaremos por* $[E : F] = dim_F(E) < +\infty$*.*

Estamos interesados en extensiones que cumplan ciertas propiedades sobre sus subcampos. La siguiente definición muestra un tipo de extensión de interés en este trabajo.

Definición 1.1.13. *Sea E una extensión de F. Decimos que* $\alpha \in E$ *es algebraico sobre F, si existe* $p(x) \in F[x]$ *no cero, tal que* $p(\alpha) = 0$*. Caso contrario, es llamado trascendente.*

Una extensión $E|F$, donde todo $\alpha \in E$ es algebraico sobre F, la llamamos una **extensión algebraica** de F, caso contrario, es llamada trascendente. Una extensión E de F de la forma $F(\alpha)$, que se lee F extendido a α, es llamada una extensión simple de F y se define como el menor campo que contiene a F y a α simultaneamente.

El siguiente teorema relaciona las extensiones finitas con las extensiones algebraicas.

Teorema 1.1.14. *Si E es una extensión finita de F, entonces E es una extensión algebraica de F.*

Veamos una breve aplicación de este resultado.

Ejemplo 1.1.15. *Dado que una $\mathbb{R}$-base para $\mathbb{C}$ está dada por $\mathbb{B}_{\mathbb{R}} = \{1, i\}$, tenemos que, $[\mathbb{C} : \mathbb{R}] = 2$, de esa manera, por el Teorema 1.1.14, $\mathbb{C}$ es una extensión algebraica de $\mathbb{R}$.*

El recíproco del Teorema 1.1.14 no es cierto, a continuación, veremos una extensión algebraica de $\mathbb{Q}$ que no es finita.

Ejemplo 1.1.16. *$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, ...)$ es una extensión algebraica de $\mathbb{Q}$, sin embargo, no es finita sobre $\mathbb{Q}$.*

Demostración. Sea $F = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$. En primer lugar, notemos que F es una extensión algebraica, para esto, sea $x \in F$, entonces existe $k \in \mathbb{Z}$, con la propiedad que, $x \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots \sqrt[k]{2})$, por la Proposición 1.1.19, la extensión $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[k]{2})|\mathbb{Q}$ es finita y por tanto algebraica. Ahora bien, notemos que $[F : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, para todo $n \in \mathbb{N}$, con lo que tenemos que, $[F : \mathbb{Q}]$ es infinita. □

Es posible demostrar que si $E|F$ y $\alpha \in E$, entonces si α es trascendente sobre F, $F(\alpha) \cong F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F[x], q(x) \neq 0 \right\}$, este último conjunto es llamado campo de cocientes de $F[x]$. Por otro lado, cuando α es algebraico sobre F, entonces $F(\alpha) \cong \frac{F[x]}{\langle p(x) \rangle}$, donde $p(x) \in F[x]$ es el polinomio de menor grado, tal que $p(\alpha) = 0$. La existencia de este último polinomio queda garantizada por la siguiente proposición.

Proposición 1.1.17. *Si α es algebraico sobre F, entonces existe un único polinomio mónico $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Este polinomio es llamado el polinomio **mínimo** de α sobre F.*

El polinomio mínimo de un elemento sobre un campo dado cumple ciertas propiedades que lo convierten pieza clave en el desarrollo del trabajo, para ejemplo de esto, tenemos la siguiente proposición.

Proposición 1.1.18. *Sea $\alpha \in F$ algebraico. Entonces el polinomio mínimo de α sobre F es irreducible.*

Demostración. Sea α un elemento algebraico de F, y $p(x)$ el polinomio mínimo de α, supongamos que es reducible, esto es, $p(x) = f(x)g(x)$, es claro que, grad $p(x) >$ grad $f(x)$ y análogamente, grad $p(x) >$ grad $g(x)$, como $p(\alpha) = 0$, entonces $f(\alpha) = 0$ o $g(\alpha) = 0$, en cualquier caso, se contradice la minimalidad de $p(x)$ y tenemos lo deseado. □

Cuando trabajamos extensiones simples, podemos conocer de manera detallada a la extensión, este hecho lo plasmaremos a continuación.

Proposición 1.1.19. *Sea F un campo y $p(x) \in F[x]$ un polinomio irreducible. Si a es un cero de $p(x)$ en alguna extensión E de F, entonces $F(a) \cong F[x]/\langle p(x)\rangle$. Además, si tenemos que, grad $p(x) = n$, entonces cada elemento de $F(a)$ puede ser escrito de forma única como:*

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0, \tag{1.2}$$

donde, $c_0, c_1, \ldots, c_{n-1} \in F$.

Una aplicación de la proposición anterior viene dada a continuación.

Ejemplo 1.1.20. *Consideremos el polinomio irreducible $p(x) = x^6 - 6$ sobre $\mathbb{Q}$. Tenemos que $\sqrt[6]{6}$ es un cero de $p(x)$ y además, $\sqrt[6]{6} \notin \mathbb{Q}$. Por lo tanto, aplicando la Proposición 1.1.19, tenemos que:*

$$\mathbb{Q}(\sqrt[6]{6}) \cong \mathbb{Q}/\langle x^6 - 6\rangle \tag{1.3}$$

Y, el conjunto $\{1, 6^{\frac{1}{6}}, 6^{\frac{2}{6}}, 6^{\frac{3}{6}}, 6^{\frac{4}{6}}, 6^{\frac{5}{6}}\}$ es una base para $\mathbb{Q}(\sqrt[6]{6})$ como $\mathbb{Q}$-espacio vectorial.

En 1882, el matemático alemán *Ferdinand von Lindemann* probó que π no es el cero de ningún polinomio no nulo con coeficientes en $\mathbb{Q}$. Por esta razón, la Proposición 1.1.19 no es aplicable a la extensión $\mathbb{Q}(\pi)|\mathbb{Q}$.

1.2. ELEMENTOS DE LA TEORÍA DE GALOIS

Definición 1.2.1. *Sea $E|F$ una extensión de campo. Entonces el conjunto de automorfismos de E, $\{f : E \to E \mid$ f es un isomorfismo$\}$, será denotado por $\mathrm{Aut}(E)$. Además, el conjunto de automorfismos de E que dejan fijo a F se denotará por $\mathrm{Aut}(E|F)$.*

Es bien conocido que, $\mathrm{Aut}(E)$ forma un grupo con la operación dada por la composición, además, podemos probar lo siguiente.

Proposición 1.2.2. *$\mathrm{Aut}(E|F)$ es un subgrupo de $\mathrm{Aut}(E)$.*

Demostración. Note que $\mathrm{Aut}(E|F) \neq \varnothing$, pues $\mathrm{Id}_E \in \mathrm{Aut}(E|F)$. Además, dados $f, g \in \mathrm{Aut}(E|F)$ y $x \in F$, se tiene que

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

de donde, $f \circ g \in \mathrm{Aut}(E|F)$. Por último, dado $f \in \mathrm{Aut}(E|F)$, como f es biyectiva existe

f^{-1}, veamos que $f^{-1} \in \mathrm{Aut}(E|F)$, sea $x \in F$ entonces $f(x) = x$, de esa manera

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

como $x \in F$ se tomó de manera arbitraria, tenemos que $f^{-1} \in \mathrm{Aut}(E|F)$ y podemos concluir que $\mathrm{Aut}(E|F)$ es un subgrupo de $\mathrm{Aut}(E)$. □

Sean $(E, +, \times)$ un campo y $W \subseteq \mathrm{Aut}(E)$, un conjunto de automorfismos de E. El conjunto fijado por W, denotado por E^W, se define por:

$$E^W = \{x \in E \,|\, \sigma(x) = x, \forall \sigma \in W\} \tag{1.4}$$

La siguiente proposición garantiza que el conjunto definido en (1.4) con las operaciones heredadas de E tiene estructura de campo.

Proposición 1.2.3. *Sean E un campo y W un conjunto de distintos automorfismos de E, es decir, $W \subseteq \mathrm{Aut}(E)$. Entonces E^W forma un campo con las operaciones heredadas de E.*

Demostración. Notemos que $E^W \neq \varnothing$, pues $1_E \in E^W$. Además dados $x, y \in E^W$, entonces $\sigma(x) = x$ y $\sigma(y) = y$ para todo $\sigma \in W$. Luego, como σ es un automorfismo, entonces; $\sigma(x + y) = x + y$, de ahí que, $x + y \in E^W$. Además, $\sigma(xy) = xy$, así $xy \in E^W$. Para terminar, dado $x \in E^W$ no nulo, tenemos que $\sigma(x^{-1}) = (\sigma(x))^{-1} = x^{-1}$ para todo $\sigma \in W$, así $x^{-1} \in E^W$ con lo que concluimos que E^W es un campo con las operaciones de E. □

De ahora en adelante, cuando W forme un grupo con la operación composición lo denotaremos mediante G y a su campo fijado E^G por F. Nuestro propósito en este momento es observar cómo se relaciona el orden de dicho grupo G con la dimensión de la extensión E sobre F. Dicho resultado, es parte fundamental en el desarrollo del trabajo.
Para probar este resultado, requerimos demostrar unos resultados previos. El primero de ellos estable la independencia lineal de un conjunto finito cualquiera de automorfismos de un campo dado.

Proposición 1.2.4. *Sean E un campo y $W = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ un conjunto de automorfismos de E. Entonces, W es un conjunto linealmente independiente. Es decir, si para todo $x \in E$,*

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_n\sigma_n(x) = 0, \tag{1.5}$$

entonces, $c_1 = c_2 = \cdots = c_n = 0$.

Demostración. Para la prueba de este hecho, procederemos por contradicción, es decir, asumamos que existen $c_1, c_2, \ldots, c_n \in E$, no todos ceros tales que:

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_n\sigma_n(x) = 0, \tag{1.6}$$

para todo $x \in E$.
Sea r el menor entero tal que $c_i \neq 0$ para todo $i \in \{1, 2, \ldots, r\}$ y reordenando de ser necesario se tiene,

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_r\sigma_r(x) = 0,$$

para todo $x \in E$. Ahora bien, es claro que $r > 1$, pues de lo contrario, como $\sigma_1(1) = 1$, debido a que σ_1 es un automorfismo, tendríamos que:

$$c_1(1) = c_1\sigma_1(1) = 0,$$

lo que implicaría que $c_1 = 0$, que contradice la suposición inicial.
Ahora, como los automorfismos de W son distintos, existe $a \in E$ tal que $\sigma_1(a) \neq \sigma_r(a)$. Así las cosas, consideremos las siguiente expresión.

$$c_1\sigma_1(ax) + c_2\sigma_2(ax) + \cdots + c_r\sigma_r(ax) = 0 \tag{1.7}$$

Como cada σ_i es un automorfismo, la expresión (1.7) equivale a lo siguiente:

$$c_1\sigma_1(a)\sigma_1(x) + c_2\sigma_2(a)\sigma_2(x) + \cdots + c_r\sigma_r(a)\sigma_r(x) = 0 \tag{1.8}$$

Ahora, por hipótesis tenemos que:

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_r\sigma_r(x) = 0 \tag{1.9}$$

Multiplicando a ambos lados de (1.9) por $\sigma_r(a)$, obtenemos lo siguiente:

$$c_1\sigma_r(a)\sigma_1(x) + c_2\sigma_r(a)\sigma_2(x) + \cdots + c_r\sigma_r(a)\sigma_r(x) = 0 \tag{1.10}$$

Restando (1.8) y (1.10) se obtiene:

$$c_1(\sigma_1(a)-\sigma_r(a))\sigma_1(x)+c_2(\sigma_2(a)-\sigma_r(a))\sigma_2(x)+\cdots+c_{r-1}(\sigma_{r-1}(a)-\sigma_r(a))\sigma_{r-1}(x) = 0 \tag{1.11}$$

Pero tenemos que $\sigma_1(a) - \sigma_r(a) \neq 0$, esto viene del hecho de que $\sigma_1(a) \neq \sigma_r(a)$. De esa manera, la afirmación (1.11) contradice la minimalidad de r. Así, el conjunto de automorfismos $\sigma_1, \sigma_2, \ldots, \sigma_n$ es linealmente independiente. □

La proposición anterior fue probada por primera vez por el matemático alemán *Richard Dedekind* (1831-1916) cuando quería garantizar la existencia de bases normales para extensiones de campos con ciertas propiedades. Dicho resultado es considerado por muchos matemáticos como el punto de partida de la teoría de Galois moderna.

El siguiente resultado es una versión más general del teorema que queremos garantizar. Para este caso, solo vamos a considerar un conjunto de automorfismos de un campo E.

Teorema 1.2.5. *Sean E un campo y, F el campo fijado por* $W = \{\sigma_1, \sigma_2, \ldots, \sigma_n\} \subseteq \mathrm{Aut}$*(E); es decir,* $F = E^W$*. Entonces* $[E : F] \geq n$*.*

Demostración. Procederemos mediante contradicción, es decir, asumamos que $[E : F] = r < n$, y que $B = \{\beta_1, \beta_2, \ldots, \beta_r\}$ es una base para $E|F$ como espacio vectorial. Entonces dado $\theta \in E$, existen escalares $c_1, c_2, \ldots, c_r \in F$, tal que:

$$\theta = c_1\beta_1 + c_2\beta_2, \cdots + c_r\beta_r \tag{1.12}$$

Consideremos el siguiente sistema de ecuaciones homogéneas de r ecuaciones con n incógnitas:

$$\begin{cases} \zeta_1\sigma_1(\beta_1) + \zeta_2\sigma_2(\beta_1) + \cdots + \zeta_n\sigma_n(\beta_1) = 0 \\ \zeta_1\sigma_1(\beta_2) + \zeta_2\sigma_2(\beta_2) + \cdots + \zeta_n\sigma_n(\beta_2) = 0 \\ \qquad\qquad\qquad \vdots \\ \zeta_1\sigma_1(\beta_r) + \zeta_2\sigma_2(\beta_r) + \cdots + \zeta_n\sigma_n(\beta_r) = 0 \end{cases} \tag{1.13}$$

Como $n > r$, entonces existe al menos una solución no trivial para el sistema 1.13; esto es; existen $\zeta_1, \zeta_2, \ldots, \zeta_n \in E$, no todos ceros, que satisfacen 1.13. Ahora, consideremos el sistema obtenido a partir de 1.13, multiplicando cada ecuación i por c_i; es decir,

$$\begin{cases} \zeta_1 c_1\sigma_1(\beta_1) + \zeta_2 c_1\sigma_2(\beta_1) + \cdots + \zeta_n c_1\sigma_n(\beta_1) = 0 \\ \zeta_1 c_2\sigma_1(\beta_2) + \zeta_2 c_2\sigma_2(\beta_2) + \cdots + \zeta_n c_2\sigma_n(\beta_2) = 0 \\ \vdots \\ \zeta_1 c_r\sigma_1(\beta_r) + \zeta_2 c_r\sigma_2(\beta_r) + \cdots + \zeta_n c_r\sigma_n(\beta_r) = 0 \end{cases} \tag{1.14}$$

Dado que cada σ_i deja fijo los elementos de F y $c_j \in F$ para todo $j \in \{1, 2, \ldots, r\}$, entonces $\sigma_i(c_j) = c_j$, para todo $i \in \{1, 2, \ldots, n\}$ y $j \in \{1, 2, \ldots, r\}$. Luego, el sistema (1.14) se puede expresar en la forma.

$$\begin{cases} \zeta_1\sigma_1(c_1\beta_1) + \zeta_2\sigma_2(c_1\beta_1) + \cdots + \zeta_n\sigma_n(c_1\beta_1) = 0 \\ \zeta_1\sigma_1(c_2\beta_2) + \zeta_2\sigma_2(c_2\beta_2) + \cdots + \zeta_n\sigma_n(c_1\beta_2) = 0 \\ \vdots \\ \zeta_1\sigma_1(c_r\beta_r) + \zeta_2\sigma_2(c_{1r}\beta_r) + \cdots + \zeta_n\sigma_n(c_r\beta_r) = 0 \end{cases} \tag{1.15}$$

Sumando las ecuaciones de (1.15) y utilizando (1.12). Obtenemos,

$$\zeta_1\sigma_1(\theta) + \zeta_2\sigma_2(\theta) + \cdots + \zeta_n\sigma_n(\theta) = 0 \tag{1.16}$$

Como $\zeta_1, \zeta_2, \ldots, \zeta_n \in E$, no son todos ceros y $\theta \in E$ es arbitrario. La ecuación (1.16) implica que $\sigma_1, \sigma_2, \ldots, \sigma_n$ son linealmente dependientes. Lo que contradice la Proposición 1.2.4.

□

Dado un campo K, denotaremos por $K[x_1, x_2, \ldots, x_n]$ al anillo de polinomios en n variables con coeficientes en K con las operaciones de suma y producto usual. Además, denotaremos por $K(x_1, x_2, \ldots, x_n)$ al conjunto de funciones racionales en n variables sobre el campo K. Es decir,

$$K(x_1, x_2, \ldots, x_n) = \left\{ \frac{p(x_1, x_2, \ldots, x_n)}{q(x_1, x_2, \ldots, x_n)} : p, q \in K[x_1, x_2, \ldots, x_n], q \neq 0 \right\}.$$

Es posible demostrar que el conjunto $K(x_1, x_2, \ldots, x_n)$ con las operaciones del anillo de polinomios es un campo, llamado campo de funciones racionales. Ahora bien, dado un conjunto X, denotaremos por S_X al conjunto de todas las biyecciones de X en X, es decir $S_X = \{f : X \to X | f \text{ es biyectiva}\}$. Dicho conjunto es un grupo con la composición

de funciones. Cuando $X = \{1, 2, \ldots, n\}$ es un conjunto finito, S_X se denota por S_n y es llamado grupo simétrico de permutaciones de orden n. Es bien conocido que el cardinal de S_n es $|S_n| = n!$.

En el siguiente ejemplo veremos cómo aplicar el Teorema 1.2.5 para solucionar un problema que relaciona el grupo simétrico y al campo de funciones racionales en n variables.

Ejemplo 1.2.6. *Sea K un campo y $E = K(x_1, x_2, \ldots, x_n)$ el campo de funciones racionales en n variables $x_1, x_2, \ldots, x_n$. Dado $\tau \in S_n$, definimos:*

$$\begin{aligned} \widehat{\tau} : E &\to E \\ f(x_1, x_2, \ldots, x_n) &\mapsto f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}), \end{aligned}$$

La primera afirmación es que el conjunto $\widehat{S_n} = \{\widehat{\tau} \,|\, \tau \in S_n\} \subseteq \mathrm{Aut}(E)$. En efecto, dados $\widehat{\tau} \in \widehat{S_n}$ y $f, g \in E$, entonces:

$$\begin{aligned} \widehat{\tau}(f(x_1, x_2, \ldots, x_n) + g(x_1, x_2, \ldots, x_n)) =& \widehat{\tau}(f+g)(x_1, x_2, \ldots, x_n)) \\ =& (f+g)(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) \\ =& f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) + g(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) \\ =& \widehat{\tau}(f) + \widehat{\tau}(g). \end{aligned}$$

Con el producto usual de funciones, es posible ver que:

$$\widehat{\tau}(f(x_1, x_2, \ldots, x_n) \cdot g(x_1, x_2, \ldots, x_n)) = \widehat{\tau}(f(x_1, x_2, \ldots, x_n)) \cdot \widehat{\tau}(g(x_1, x_2, \ldots, x_n)).$$

Además, es un ejercicio simple establecer que, $(\widehat{\tau})^{-1} = \widehat{\tau^{-1}}$; es decir, todo elemento $\widehat{\tau} \in \widehat{S_n}$ es un automorfismo sobre E y así, $\widehat{S_n} \subseteq \mathrm{Aut(E)}$.
La segunda afirmación es que $|\widehat{S_n}| \geq n!$, para esto consideremos la siguiente función:

$$\begin{aligned} \varphi : S_n &\to \hat{S}_n \\ \tau &\mapsto \widehat{\tau} \end{aligned}$$

y veamos que φ es inyectiva, sean $\tau_1, \tau_2 \in S_n$, con $\tau_1 \neq \tau_2$, entonces existe r, con $1 \leq r \leq n$, tal que $\tau_1(r) \neq \tau_2(r)$. Entonces, para $f(x_1, x_2, \ldots, x_n) = x_r \in E$. $\widehat{\tau_1}(f) = x_{\tau_1(r)} \neq x_{\tau_2(r)} = \widehat{\tau_2}(f)$. Lo cual implica que φ es inyectiva y por tanto,

$$n! = |S_n| \leq |\hat{S_n}|$$

Ahora bien, por las condiciones anteriores y a consecuencia del Teorema 1.2.5 podemos afirmar que,

$$[K(x_1, x_2, \ldots, x_n) : K(x_1, x_2, \ldots, x_n)^{\hat{S_n}}] \geq n!$$

Denotando a $F = K(x_1, x_2, \ldots, x_n)^{\hat{S_n}}$*, se concluye que,*

$$[E : F] \geq n!$$

En estos momentos disponemos de las herramientas necesarias para poder demostrar el teorema fundamental de esta sección. Dicho resultado es un caso particular de 1.2.5 considerando al conjunto W como un grupo con la composición.

Teorema 1.2.7. *Sean E un campo y,* $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ *un grupo de automorfismos de E. Si F es el campo fijado por G, entonces* $[E : F] = n$*.*

Demostración. Para esto, es suficiente ver que $[E : F] \leq n$, ya que a consecuencia del $Teorema$ 1.2.5 tenemos que $[E : F] \geq n$ por lo que concluiríamos que $[E : F] = n$, teniendo el resultado que queríamos probar.
Sea $\alpha_1, \alpha_2, \ldots, \alpha_m \in E$, con $m > n$. Probaremos que los α_i son linealmente dependientes. Con este objetivo, consideremos el sistema

$$\begin{cases} x_1\sigma_1(\alpha_1) + x_2\sigma_1(\alpha_2) + \cdots + x_m\sigma_1(\alpha_m) = 0 \\ x_1\sigma_2(\alpha_1) + x_2\sigma_2(\alpha_2) + \cdots + x_m\sigma_2(\alpha_m) = 0 \\ \vdots \\ x_1\sigma_n(\alpha_1) + x_2\sigma_n(\alpha_2) + \cdots + x_m\sigma_n(\alpha_m) = 0 \end{cases} \tag{1.17}$$

Notemos que el sistema anterior, es un sistema homogéneo con n ecuaciones y m incógnitas y además $m > n$, por lo tanto existe una solución no trivial, $x_1, x_2, \ldots, x_m \in E$, sin perdida de generalidad, digamos $x_1 \neq 0$, es claro que $\lambda x_1, \lambda x_2, \ldots, \lambda x_m$ es también una solución del sistema para todo $\lambda \in E$, además por la proposición 1.2.4 podemos encontrar $\theta \in E$ tal que:

$$\sigma_1(\theta) + \sigma_2(\theta) + \cdots + \sigma_n(\theta) = a \neq 0 \tag{1.18}$$

De esa manera, tomamos $\lambda \in E$ de manera que $\lambda x_1 = \theta$, en efecto existe $x_1 \neq 0$. Ahora definimos $y_j = \lambda x_j$ para todo $j \in \{1, 2, \ldots, n\}$, es claro que $y_1 = \theta$. Como los y_j son

también solución del sistema (1.17), podemos asumir que nuestra solución inicial de $x'_j s$ coincide con la solución de los $y'_j s$, en particular podemos asumir que $x_1 = \theta$.
Ahora aplicamos σ_i a cada una de las ecuaciones del sistema (1.17), obteniendo,

$$\sigma_i(x_1)\sigma_i\sigma_k(\alpha_1) + \sigma_i(x_2)\sigma_i\sigma_k(\alpha_2) + \cdots + \sigma_i(x_m)\sigma_i\sigma_k(\alpha_m) = 0$$

Para todo $k \in \{1, 2, \ldots, n\}$, notemos que $\sigma_i(x_1), \sigma_i(x_2), \ldots, \sigma_i(x_m)$ es también una solución para el sistema (1.17). Para ver la validez de este hecho es suficiente ver que el conjunto $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n\}$ es una reordenación del conjunto $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, es decir, debemos ver que $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n\} = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Procederemos a mostrar cada una de las inclusiones.

- $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n\} \subseteq \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ para todo $i = 1, 2, \ldots, n$, esto es claro, pues dado un elemento en $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_2\}$, él es de la forma $\sigma_i\sigma_k$ para algún k, pero como G es un grupo, en particular cerrado con la operación composición, tenemos que $\sigma_i\sigma_k \in G$.
- Para ver la otra contenencia, note que $\sigma_i\sigma_j = \sigma_i\sigma_k$ si y solo si $\sigma_j = \sigma_k$ esto implica que $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n\}$ tiene n elementos pues cada uno de ellos es diferente y por la afirmación anterior, es decir, $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n\} \subseteq \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, podemos concluir que $\{\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n\} = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$.

Por lo que podemos concluir que, $\sigma_i(x_1), \sigma_i(x_2), \ldots, \sigma_i(x_m)$ es una solución para el sistema (1.17). Ahora bien, como la suma de soluciones de un sistema de ecuaciones homogéneas es también una solución, tenemos que:

$$x'_j = \sum_{i=1}^{n} \sigma_i(x_j)$$

es también solución de (1.17) para $j \in \{1, 2, \ldots, m\}$. Notemos que $x'_1 = \sum_{i=1}^{n} \sigma_i(x_1)$ pero sabemos que $x_1 = \theta$, utilizando (1.18) obtenemos:

$$x'_1 = \sum_{i=1}^{n} \sigma_i(x_1) = \sum_{i=1}^{n} \sigma_i(\theta) = a \neq 0$$

Además, notemos que $x'_1, x'_2, \ldots, x'_m \in F$.

$$\sigma_k(x'_j) = \sigma_k\left(\sum_{i=1}^{n} \sigma_i(x_j)\right) = \sum_{i=1}^{n} \sigma_k\sigma_i(x_j) = \sum_{i=1}^{n} \sigma_i(x_j) = x'_j$$

Para todo $j = 1, 2, \ldots, m$ y $k = 1, 2 \ldots, n$, esto proviene del hecho que $\{\sigma_k\sigma_1, \sigma_k\sigma_2, \ldots, \sigma_k\sigma_n\} = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Por otro lado, como G es un grupo, entonces el automorfismo $\mathrm{Id} \in G$, por el sistema (1.17), se tiene que:

$$x'_1\alpha_1 + x'_2\alpha_2 +, \cdots + x'_m\alpha_m = 0$$

Donde $x'_1, x'_2, \ldots, x'_m \in F$ es una solución no trivial de (1.17) debido a que $x'_1 = a \neq 0$, lo cual implicaría que el conjunto $\{\alpha_1, \alpha_2 \ldots, \alpha_m\}$ es linealmente dependiente y obteniendo lo deseado. □

El Teorema 1.2.7 es una herramienta de gran utilidad para resolver distintos tipos de problemas, en particular, para el cálculo de la dimensión de un espacio vectorial sobre un cuerpo fijado, como lo evidenciaremos a continuación.

Ejemplo 1.2.8. *Sea $\mathbb{C}$ el cuerpo de los números complejos con las operaciones de suma y producto usuales. Consideremos el grupo de automorfismos de $\mathbb{C}$ dado por $G = \{\mathrm{Id}, \sigma_1\}$, donde Id es el automorfismo identidad y σ_1 es el automorfismo de conjugación en $\mathbb{C}$; es decir,*

$$\begin{aligned} \sigma_1 : \mathbb{C} &\to \mathbb{C} \\ z &\mapsto \bar{z} \end{aligned}$$

Dado que $\mathrm{Id}^2 = \mathrm{Id}$ y $\sigma_1^2 = \mathrm{Id}$, sigue que G es un grupo con la operación composición de orden 2, por lo que:

$$[\mathbb{C} : \mathbb{C}^G] = |G| = 2$$

Pero, ¿quién en es $\mathbb{C}^G$?. Para responder esta pregunta recordemos que $\mathbb{C}^G$ es el campo fijado por los automorfismos de G; es decir, los elementos $z \in \mathbb{C}$ que están en $\mathbb{C}^G$ deben verificar que $\sigma(z) = z$, para todo $\sigma \in G$. Es claro que el automorfismo identidad fija todos los elementos de $\mathbb{C}$, de esa manera vamos a interesarnos en los elementos fijados por σ_1.
Sea $z \in \mathbb{C}$, supongamos que $z = x + iy$ y que $\sigma_1(z) = z$, esto implica que, $x - iy = x + iy$ y así, $-y = y$ y $x = x$. Por lo tanto, $x \in \mathbb{R}$ y $y = 0$.
Así, tenemos que:

$$\mathbb{C}^G = \{x + iy | x \in \mathbb{R}, y = 0\} \cong \mathbb{R}$$

Lo anterior prueba que,

$$[\mathbb{C} : \mathbb{R}] = 2.$$

Un ejemplo análogo y que relaciona una extensión algebraica de $\mathbb{Q}$, es el presentado a continuación.

Ejemplo 1.2.9. *Considere el cuerpo $\mathbb{Q}(\sqrt{2})$ y sea $G = \{Id, \sigma\}$, donde Id es el automorfismo identidad y σ es el automorfismo de $\mathbb{Q}(\sqrt{2})$ que mapea $\sqrt{2}$ en $-\sqrt{2}$, de manera análoga al ejemplo anterior, es posible ver que G es un grupo con la operación composición y por el Teorema 1.2.7, tenemos:*

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt{2})^G] = 2,$$

pero el campo fijado por G es precisamente $\mathbb{Q}$, así:

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

El siguiente resultado establece bajo qué condiciones podemos determinar explícitamente el conjunto $\mathrm{Aut(E|F)}$. Más exactamente.

Proposición 1.2.10. *Sean E un campo y $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ un grupo finito de automorfismos de E y F el campo fijado por G. Entonces cada automorfismo de E que deja fijo a F está en G; es decir, $G = \mathrm{Aut}(E|F)$.*

Demostración. Por el Teorema 1.2.7 tenemos que $[E : F] = |G| = n$. Procedemos vía contradicción, es decir, supongamos que existe $\tau \in \mathrm{Aut}(E|F)$ tal que $\tau \notin G$. Consideremos a H el subgrupo generado por G y τ. Entonces H tiene orden mayor que n. Pero H también deja fijo a F, por lo tanto, $[E : F] = |H| > n$, lo cual contradice la conclusión inicial. □

El Teorema 90 de Hilbert se fundamenta en las extensiones de Galois, por tal motivo, es imprescindible definir y conocer las propiedades algebraicas que envuelve este tipo de extensiones. Este hecho queda registrado a continuación.

Definición 1.2.11. *Sea $E|F$ una extensión finita. Si el campo fijado por $\mathrm{Aut}(E|F)$ es F; es decir, $E^{\mathrm{Aut(E|F)}} = F$, decimos que $E|F$ es una **extensión de Galois**. En este caso, $\mathrm{Aut}(E|F)$ es el grupo de Galois asociado a $E|F$ y lo denotaremos como $Gal(E|F)$.*

Es importante disponer de diferentes caracterizaciones del concepto de extensión de Galois, por el hecho de que nos serán útiles en posteriores resultados. Las siguientes definiciones nos permitirán lograr este objetivo.

Definición 1.2.12. *Sea $E|F$ una extensión y $p(x) \in F[x]$.*

- *Decimos que $p(x) \in F[x]$ es separable en E, si $p(x)$ no tiene raíces múltiples en E.*
- *Si $E|F$ es una extensión algebraica, decimos que E es separable si el polinomio mínimo de cada $\alpha \in E$ es separable, de otra forma, la llamamos inseparable.*
- *Si $E|F$ es una extensión algebraica, decimos que E es normal si el polinomio mínimo para cada $\alpha \in E$ rompe en E.*

El siguiente resultado será pieza clave para obtener una caracterización del concepto de extensión de Galois. En términos generales dicho resultado soluciona el problema de extender un isomorfismo de subcampos a un isomorfismo de campos. Antes de mencionar dicho resultado, debemos tener presente lo siguiente. Si E y $E^{'}$ son isomorfos, es decir, existe $\varphi : E \to E^{'}$ un isomorfismo, podemos hallar una correspondencia entre los polinomios con coeficientes en E y los polinomios con coeficientes en $E^{'}$. Dicha relación está dada por:

$$\begin{aligned} \varphi : E[x] &\to E^{'}[x] \\ p(x) &\mapsto \hat{p}(x) \end{aligned}$$

donde,

$$p(x) = \sum_{k=1}^{n} a_k x^k \longmapsto \hat{p}(x) = \sum_{k=1}^{n} \varphi(a_k) x^k$$

Teorema 1.2.13. *Sean F y $\hat{F}$ campos isomorfos. Sea $p(x) \in F[x]$ y $\hat{p}(x)$ el polinomio correspondiente vía isomorfismo en $\hat{F}[x]$. Asumamos que $\Omega|F$ y $\hat{\Omega}|\hat{F}$ son extensiones de campos en las cuales $p(x)$ y $\hat{p}(x)$ rompen, respectivamente. Sea E el campo de ruptura entre Ω y F de $p(x)$. Sea $\hat{E}$ de manera análoga para $\hat{p}(x)$. Entonces, el isomorfismo entre F y $\hat{F}$ puede ser extendido a un isomorfismo entre E y $\hat{E}$.*

Demostración. Dadas las condiciones anteriores, factorizando $p(x) \in F[x]$ en Ω, tenemos,

$$p(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Factorizando $\hat{p}(x) \in \hat{F}[x]$ en $\hat{\Omega}$

$$\hat{p}(x) = (x - \hat{\alpha_1})(x - \hat{\alpha_2}) \dots (x - \hat{\alpha_n}).$$

De esa manera, al ser E el menor cuerpo que contiene a F y las raíces de $p(x)$, tenemos, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. De forma análoga, $\hat{E} = \hat{F}(\hat{\alpha_1}, \hat{\alpha_2}, \ldots, \hat{\alpha_n})$, es el campo de ruptura de $\hat{p}(x)$ sobre $\hat{F}[x]$. Como $F \cong \hat{F}$, entonces $F[x]/\langle p(x)\rangle \cong \hat{F}[x]/\langle \hat{p}(x)\rangle$, y por lo tanto $F(\alpha_1) \cong \hat{F}(\hat{\alpha_1})$, debido a que, por la Proposición 1.1.19 tenemos que, $F[x]/\langle p(x)\rangle \cong F(\alpha_1)$ y $\hat{F}[x]/\langle \hat{p}(x)\rangle \cong F(\hat{\alpha_1})$. Procediendo de forma inductiva se prueba que

$$F[\alpha_1, \ldots, \alpha_{n-1}]/\langle p(x)\rangle \cong \hat{F}[\hat{\alpha_1}, \ldots, \hat{\alpha_{n-1}}]/\langle \hat{p}(x)\rangle,$$

y nuevamente por la Proposición 1.1.19, tenemos $F(\alpha_1, \ldots, \alpha_n) \cong \hat{F}(\hat{\alpha_1}, \ldots, \hat{\alpha_n})$, que era lo que queríamos probar. □

Observación: El principio de inducción matemática afirma que si una proposición $P(n)$, es tal que si $P(n)$ es cierta, $P(n+1)$ vale, entonces $P(n)$ es valida para el conjunto $\mathbb{N}$. Ahora bien, una versión equivalente a este principio afirma que, si $P(n+1)$ se tiene, $P(n)$ vale, entonces, la proposición vale para el conjunto de números naturales. Este principio será utilizado para demostrar el siguiente resultado.

Teorema 1.2.14. *Sea F un campo y $p(x) \in F[x]$, de la forma*

$$p(x) = c(x - \alpha_1) \ldots (x - \alpha_r) p_1(x) \ldots p_s(x),$$

donde cada $p_i(x)$ es un factor de grado mayor que 1. Si E es el campo de ruptura de $p(x)$ sobre F y $p_i(x)$ no tiene raíces múltiples para cada $i = 1, 2, \ldots, s$, entonces el conjunto de elementos en E que son fijados por $\mathrm{Aut}(E|F)$ coincide con F.

Demostración. Supongamos que grad $p(x) = n$ y r es el número de factores. Vamos a proceder mediante el método de inducción matemática. Para la base de inducción, tomemos a $r = n$, esto implica que $p(x)$ rompe totalmente en F, así $F = E$ es el campo de ruptura y por tanto el campo fijado por $\mathrm{Aut}(E|F) = \{Id\}$ es precisamente F. Ahora, supongamos que la proposición se verifica para $r = k + 1$ y probemos que también se cumple para $r = k$.
Sea $p(x)$ con k factores lineales. Si α_{k+1} es una raíz de de $p_1(x)$, el campo F puede ser extendido a $F(\alpha_{k+1})$ en el cual $p(x)$ tiene al menos $k + 1$ factores. Factorizando $p(x)$ con las condiciones del teorema y cada $p_i(x)$ sobre $F(\alpha_{k+1})$, tenemos:

$$p(x) = c(x - \alpha_1) \ldots (x - \alpha_r)(x - \alpha_{k+1})(x - \beta_1) \ldots (x - \beta_s) q_1(x) q_2(x) \ldots q_v(x) \qquad (1.19)$$

Donde cada $q_i(x)$ es un polinomio irreducible sobre $F(\alpha_{k+1})$ y de grado mayor a 1, obtenidos de la factorización de algún $p_j(x)$. Notemos que E continúa siendo el campo de ruptura de $F(\alpha_{k+1})$ y cada $q_k(x)$ no contiene factores repetidos, pues caso contrario, algún $p_i(x)$ los tendría, esto contradice la hipótesis inicial.
Dadas las condiciones anteriores y por la hipótesis de inducción, si $\theta \in E$ es fijado por $\mathrm{Aut}(E|F(\alpha_{k+1}))$, entonces $\theta \in F(\alpha_{k+1})$.
Ahora supongamos que $\theta \in E$ es fijado por $\mathrm{Aut}(E|F)$, ahora, como $F \subseteq F(\alpha_{k+1})$, es claro que,

$$\mathrm{Aut}(E|F[\alpha_{k+1}]) \subseteq \mathrm{Aut}(E|F)$$

Luego θ es dejado fijo por $\mathrm{Aut}(E|F[k+1])$ y por tanto $\theta \in F(\alpha_{k+1})$.
Asumamos que grad $p_1(x) = t$, puesto $\theta \in F[\alpha_{k+1}]$, sigue de la Proposición 1.1.19, que existen $c_0, c_1, \ldots, c_{t-1} \in F$, tal que,

$$\theta = c_0 + c_1\alpha_{k+1} + \cdots + c_{t-1}\alpha_{k+1}^{t-1} \tag{1.20}$$

Por el hecho que $p_i(x)$ no posee factores repetidos, podemos escribir:

$$p_1(x) = (x - \alpha_{k+1})(x - \alpha_{k+2}) \ldots (x - \alpha_{k+t}), \tag{1.21}$$

donde $\alpha_{k+1}, \alpha_{k+2}, \ldots, \alpha_{k+t}$ son las distintas raíces de $p_1(x)$. Por el Teorema 1.2.14, los automorfismos que mandan α_{k+1} en α_{k+j}, para todo $j \in \{1, 2, \ldots, t\}$ están en $\mathrm{Aut}(E|F)$. Ahora bien, como $\theta \in F$, sigue que θ es fijado por los automorfismos, así las cosas, aplicando cada uno de los automorfismos a la expresión en 1.20, se tiene:

$$\theta = c_0 + c_1\alpha_{k+1} + \cdots + c_{t-1}\alpha_{k+1}^{t-1} \tag{1.22}$$

$$\theta = c_0 + c_1\alpha_{k+2} + \cdots + c_{t-1}\alpha_{k+2}^{t-1} \tag{1.23}$$

$$\vdots$$

$$\theta = c_0 + c_1\alpha_{k+t} + \cdots + c_{t-1}\alpha_{k+t}^{t-1} \tag{1.24}$$

y consideremos el siguiente polinomio,

$$\phi(x) = (c_0 - \theta) + c_1 x + \cdots + c_{t-1} x^{t-1} \tag{1.25}$$

Es fácil ver, a consecuencia de las ecuaciones en (1.22),(1.23). . . ,(1.24) que los elementos $\alpha_{k+1}, \alpha_{k+2}, \ldots, \alpha_{k+t}$, son raíces para el polinomio $\phi(x)$, sin embargo, el grado de $\phi(x)$ es $t-1$. Luego, $\phi(x) = 0$ para todo $x \in F(\alpha_{k+1})$. Con lo que podemos concluir que $(c_0 - \theta) = 0$, así, $c_0 = \theta \in F$.
De esa manera, por inducción matemática esta proposición vale para todo n, que era lo que queríamos probar. □

Cuando trabajamos con grupos de automorfismos, la extensión de campo $E|E^G$ posee muy buenas propiedades desde el punto de vista algebraico. Un ejemplo de este hecho viene enmarcado en la siguiente proposición.

Proposición 1.2.15. *Sean E un campo y $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ un grupo finito de automorfismos de E, y F el campo fijado por G; es decir, $F = E^G$. Entonces $E|F$ es una extensión algebraica.*

Demostración. Sea $\alpha \in E$, veamos que es algebraico sobre F. Para no recargar la notación, vamos a definir $\alpha_i = \sigma_i(\alpha)$ para todo $i \in \{1, 2, \ldots, n\}$. Supongamos que r de estos elementos son diferentes. Puesto que G es un grupo con la operación composición, tenemos que el automorfismo identidad es uno de estos automorfismos; es decir, existe $j \in \{1, 2, \ldots, n\}$ tal que $\sigma_j = Id$. Luego, $\alpha_j = \sigma_j(\alpha) = Id(\alpha) = \alpha$. Ahora bien, el conjunto $\{\sigma_i\sigma_1(\alpha), \sigma_i\sigma_2(\alpha), \ldots, \sigma_i\sigma_r(\alpha)\}$ consiste en r diferentes valores, debido a la inyectividad de σ_i. Además, este conjunto está contenido en:

$$\{\sigma_i\sigma_1(\alpha), \sigma_i\sigma_2(\alpha), \ldots, \sigma_i\sigma_n(\alpha)\} = \{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\},$$

que es una reordenación de $\alpha_1, \alpha_2, \ldots, \alpha_r$. Dadas estas condiciones, procedemos a construir el siguiente polinomio,

$$\phi(x) = \prod_{i=1}^{r} (x - \alpha_i), \tag{1.26}$$

lo primero que evidenciamos es que α es una raíz de $\phi(x)$, esto a causa de que el factor $(x - \alpha)$ aparece en la factorización. Basta probar que $\phi(x) \in F[x]$. Para esto, sea $\sigma_i \in G$,

entonces,

$$\sigma_i(\phi(x)) = \prod_{i=1}^{r} \sigma_i(x - \alpha_i) = \prod_{i=1}^{r} (\sigma_i(1)x - \sigma_i(\alpha_i)) = \prod_{i=1}^{r} (x - \sigma_i(\alpha_i)) = \phi(x), \tag{1.27}$$

por lo tanto, los coeficientes de $\phi(x)$ son fijados por σ_i para todo $i = 1, 2, \ldots, n$, de esa manera los coeficientes están en F, esto equivale a decir que, $\phi(x) \in F[x]$ que era lo que queríamos probar. □

El polinomio $\phi(x)$ definido anteriormente en (1.26) será de ayuda para posteriores argumentos debido a sus diversas propiedades. En particular, nos resulta importante el siguiente hecho.

Proposición 1.2.16. *El polinomio $\phi(x)$ definido en (1.26) es irreducible sobre F.*

Demostración. Sea $p(x) \in F[x]$ tal que $p(\alpha) = 0$. A causa de que los coeficientes de $p(x)$ pertenecen a F, se tiene que estos son fijados por los automorfismos σ_i para $i = 1, 2, \ldots, n$, por lo tanto,

$$p(\alpha_i) = p(\sigma_i(\alpha)) = \sigma_i(p(\alpha)) = \sigma_i(0) = 0 \tag{1.28}$$

De esa manera, $\alpha_1, \alpha_2, \ldots, \alpha_r$ son raíces de $p(x)$, lo cual implica que grad $p(x) \geq r$. Así, $\phi(x)$ es el polinomio mínimo de α, y por la Proposición 1.1.18, $\phi(x)$ es irreducible. □

Procedemos con el siguiente resultado que nos permite caracterizar las extensiones de Galois.

Teorema 1.2.17. *Sea $E|F$ una extensión de campos algebraica. Las siguientes afirmaciones son equivalentes.*

1. *$E|F$ es una extensión de Galois.*
2. *F es el campo fijado por un grupo finito G de automorfismos de E.*
3. *E es el campo de ruptura de algún polinomio separable de $F[x]$.*
4. *$E|F$ es normal, separable y finita.*

Demostración. Procedemos con la prueba de las equivalencias de la siguiente manera. $(3) \Rightarrow (1)$. Supongamos que E es el campo de ruptura de algún polinomio $p(x) \in F[x]$. Por el Teorema 1.2.14, F es el campo fijado por $\mathrm{Aut}(E|F)$. Luego $E|F$ es una extensión

de Galois.
$(1) \Rightarrow (2)$. Supongamos que $E|F$ es una extensión de Galois, por definición $E|F$ es finita. Tomemos a $G = \mathrm{Aut}(E|F)$. Puesto que F es el campo fijado por G; es decir, $F = E^G$ y utilizando el Teorema 1.2.7 se tiene $[E : F] = |G|$. Luego G es finito.
$(2) \Rightarrow (4)$. Sean G un grupo finito de automorfismos de E, y F el campo fijado por G. A consecuencia del Teorema 1.2.7, $[E : F] = |G|$. Luego $E|F$ es una extensión finita. Ahora probemos que $E|F$ es separable y normal. Sea $\alpha \in E$, tomemos la orbita de α sobre G y construyamos $\phi(x)$ el polinomio de la ecuación 1.26, recordemos que $\phi(x)$ es el polinomio mínimo de α y además, tiene grad $\phi(x)$ factores distintos en E. Por lo tanto $\phi(x)$ rompe en factores lineales en E. Luego $E|F$ es normal y separable.
$(4) \Rightarrow (3)$. por el hecho que $E|F$ es una extensión finita, existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ tal que $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Sea $p_i(x) \in F[x]$ el polinomio mínimo de α_i, y consideremos,

$$p(x) := \prod_{i=1}^{n} p_i(x) \tag{1.29}$$

Por el hecho de que $E|F$ es una extensión normal, cada $p_i(x)$ rompe en E. Luego E es el campo de ruptura de $p(x)$. Adicionalmente, como $E|F$ es una extensión separable entonces $p(x)$ es separable. □

Tener equivalencias de la definición de extensión de Galois nos será de utilidad a la hora de probar ciertos resultados, como caso particular de esto, podemos obtener un ejemplo ilustrativo de una extensión de Galois.

Ejemplo 1.2.18. *Es bien sabido que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. A consecuencia de la proposición 1.1.19, la extensión $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es algebraica. Además, $\mathbb{Q}(\sqrt{2})$ es el campo de ruptura del polinomio separable $x^2 - 2$, así por el Teorema 1.2.17, tenemos que, $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es una extensión de Galois.*

Ejemplo 1.2.19. *$\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ es una extensión de Galois, este hecho radica en que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el campo de ruptura del polinomio $p(x) = (x^2 - 3)(x^2 - 2) \in \mathbb{Q}[x]$, siendo $p(x)$ separable, debido a que tienes sus 4 raíces distintas, de esa manera, utilizando las equivalencias de la definición de extensión de Galois tenemos lo deseado.*

En los ejemplos anteriores hemos visto como cierto tipo de extensiones sobre un cuerpo dado son de Galois. En este orden de ideas, es de esperar que las extensiones simples sobre un campo sean, en general de Galois, sin embargo, este hecho no es cierto y queda enmarcado en el siguiente ejemplo.

Ejemplo 1.2.20. *La extensión de campos $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ no es de Galois. Puesto que el polinomio mínimo de $\sqrt[3]{2}$ viene dado por $p(x) = x^3 - 2$, sin embargo, $p(x)$ no rompe en $\mathbb{Q}(\sqrt[3]{2})$, por lo tanto, la extensión $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ no es normal. Luego por el Teorema 1.2.17, tenemos que la extensión $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ no es de Galois.*

Definición 1.2.21. *Sea $E|F$ una extensión de campos. Una subextensión o también llamado campo intermedio de $E|F$ es una extensión $M|F$ con $M \subseteq E$, es decir, M es una extensión de campo tal que $F \subseteq M \subseteq E$.*

Cuando trabajamos con extensiones de Galois, una propiedad importante que cumplen los campos intermedios es que preservan la condición de ser de Galois. Este hecho es el queda indicado en la siguiente proposición.

Proposición 1.2.22. *Sean $E|F$ una extensión de Galois con $G = Gal(E|F)$ y M un campo intermedio de $E|F$. Entonces $E|M$ es de Galois.*

Demostración. Sea $E|F$ una extensión de Galois. Por el Teorema 1.2.17 E es el campo de ruptura de algún polinomio $p(x) \in F[x]$ separable, como $F \subseteq M$ entonces $p(x) \in M[x]$. De esa manera, nuevamente por el Teorema 1.2.17 concluimos que $E|M$ es una extensión de Galois. □

Definición 1.2.23. *Sea G un grupo y H un subgrupo de G. El índice de H en G, denotado por $(H : G)$, es el menor número de coclases tal que la unión es G. Para un grupo finito G y H un subgrupo, el índice viene dado por:*

$$(H : G) = \frac{|G|}{|H|} \tag{1.30}$$

Dada $E|F$ una extensión de Galois, con $G = Gal(E|F)$ grupo de Galois, es posible hallar una correspondencia entre los campos intermedios de $E|F$ y los subgrupos de $Gal(E|F)$. Dicha afirmación es considerada como el teorema fundamental de la teoría de Galois y queda registrada a continuación.

Teorema 1.2.24. ***Teorema fundamental de la teoría de Galois:*** *Sea $E|F$ una extensión de Galois con $G = Gal(E|F)$, Existe una correspondencia uno a uno entre los subgrupos de G y los campos intermedios de $E|F$, dada por la siguiente biyección:*

$$\Phi : \{H|H \preceq G\} \to \{M|F \subseteq M \subseteq E\}$$
$$H \mapsto E^H$$

Con inversa dada por:

$$\Phi^{-1} : \{M|F \subseteq M \subseteq E\} \to \{H|H \preceq G\}$$
$$M \mapsto Gal(E|M)$$

Además,

1. *La correspondencia de inclusión es reversa, es decir,* $H_1 \supseteq H_2 \Leftrightarrow E^{H_1} \subseteq E^{H_2}$.
2. *Correspondencia entre sus índices, i.e,* $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$.

Demostración. Lo primero que debemos verificar es que efectivamente Φ^{-1} es la inversa de Φ. Para esto, sea H un subgrupo de G. Veamos que $Gal(E|E^H) = H$, tenemos que $E|E^H$ es una extensión de Galois por la Proposición 1.2.22, entonces es finita y por la Proposición 1.2.10 tenemos que $\mathrm{Aut}(E|E^H) = Gal(E|E^H) = H$. Para ver la otra afirmación, tomemos M un campo intermedio de $E|F$, por la Proposición 1.2.22, $E|M$ es de Galois, por lo que, debido a la caracterización en el Teorema 1.2.17, M es el campo fijado por un grupo finito de automorfismos, que viene dado por $Gal(E|M)$. De esa manera, vale que $E^{Gal(E|M)} = M$ con lo que obtenemos lo deseado.
Procedamos con la prueba de las afirmaciones (1) y (2).

(1) Para esta afirmación tenemos las siguientes implicaciones.
Es claro que si, $H_1 \supseteq H_2$, entonces $E^{H_1} \subseteq E^{H_2}$. Recíprocamente, supongamos que $E^{H_1} \subseteq E^{H_2}$, esto implica que $Gal(E|E^{H_1}) \supseteq Gal(E|E^{H_2})$, recordemos que $Gal(E|E^{H_i}) = H_i$, entonces $H_1 \supseteq H_2$.
(2) Sea H_1 subgrupo de G y $H_2 = \{\mathrm{id}\} = 1$, el subgrupo trivial de G, es claro que, $E^{H_2} = E^1 = E$, entonces se tiene.

$$[E : E^{H_1}] = |Gal(E|E^{H_1})| = (Gal(E|E^{H_1}) : 1) \tag{1.31}$$

Para probar la afirmación de manera general, consideremos:

$$(H_1 : 1) = (H_1 : H_2)(H_2 : 1) \tag{1.32}$$

y,

$$[E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}] \tag{1.33}$$

Por el hecho que,

$$[E : E^{H_i}] = |Gal(E|E^{H_i})| = |H_i| = (H_i : 1) \tag{1.34}$$

Igualando (1.32) y (1.33), tenemos que:

$$(H_1 : H_2) = [E^{H_2} : E^{H_1}]$$

□

Si el lector requiere mayor información acerca de la teoría de Galois, puede consultar [1] y [5] para obtener de manera clara y concisa detalles de esta teoría.

1.3. INTRODUCCIÓN AL CONCEPTO DE $G-$MÓDULO

Vamos a definir un concepto que será pieza importante para la formulación del Teorema 90 de Hilbert. Su definición viene dada a continuación.

Definición 1.3.1. *Sea G un grupo. Un G-módulo es un grupo abeliano M, junto con una acción de G en M, es decir, una función $G \times M \to M$, que satisface:*

- $\sigma(m + m') = \sigma m + \sigma m'$*, para todo* $\sigma \in G$ *y* $m, m' \in M$*.*
- $(\sigma\tau)(m) = \sigma(\tau m)$*, para todo* $\sigma, \tau \in G$ *y* $m \in M$*.*
- $1_G m = m$*, para todo* $m \in M$*.*

Dado $(M, +)$ un grupo abeliano. Entonces M es un $\mathbb{Z}-$modulo. Este hecho queda garantizado a continuación.

Ejemplo 1.3.2. *Sea M un grupo abeliano, entonces M tiene estructura de $\mathbb{Z}$-módulo, mediante la siguiente función.*

$$\begin{aligned} f : \mathbb{Z} \times M &\to M \\ (n, m) &\mapsto nm \end{aligned}$$

---

[5] J.S MILNE. *Fields and Galois Theory*. Princeton Mathematical Series, New Jersey, 2021.

Es fácil ver que f verifica las condiciones de $G-$módulo descritas en la Definición 1.3.1. Por lo tanto, M es un $\mathbb{Z}$-módulo.

A consecuencia del ejemplo anterior, se tiene el siguiente hecho.

Ejemplo 1.3.3. *Sea R un anillo y $M_n(R)$ el grupo de matrices de orden n con la operación de suma usual dada componente a componente. Entonces $M_n(R)$ tiene estructura de $\mathbb{Z}$-módulo con la siguiente operación.*

$$(n, A) \mapsto nA,$$

donde, si $A = (a_{i,j})$. Entonces, $nA = (na_{i,j})$.

Un ejemplo de $G-$módulo relacionado con el tema de estudio de este trabajo, involucra las extensiones de Galois y el grupo de Galois asociado. Dicho ejemplo queda enmarcado a continuación.

Ejemplo 1.3.4. *Sea $E|F$ una extensión de Galois y $G = Gal(E|F)$, entonces $M = (E, +)$ grupo abeliano, es un $G-$módulo con la acción de G en M dada por la evaluación. Dado que σ es un automorfismo de E, entonces*

$$\sigma(m + m') = \sigma(m) + \sigma(m')$$

para todo $m, m' \in M$ y $\sigma \in G$, además por la definición de función se tiene

$$\sigma\tau(m) = \sigma(\tau m)$$

por último:

$$1_G m = m$$

para todo $m \in M$, pues recordemos que 1_G es el automorfismo identidad de E. Luego, $M = (E, +)$ es un G módulo con $G = Gal(E|F)$.

La siguiente definición es necesaria para poder mencionar más adelante al teorema principal.

Definición 1.3.5. *Sea M un G-módulo, definimos un homomorfismo cruzado, como una*

función, $f : G \to M$*, que verifica:*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau),$$

para todo $\sigma, \tau \in G$*.*

Lo primero veremos es que el conjunto de llegada de un homomorfismo cruzado es efectivamente M, para esto, recordemos que el dominio de definición es G, notemos que $\sigma\tau \in G$ pues el producto que se efectúa viene de G y tenemos que éste último es un grupo, por lo que es cerrado. Ahora, por la definición tenemos que $f(\sigma), f(\tau) \in M$ y por el hecho que M es un G-módulo $\sigma f(\tau) \in M$, así tenemos que $f(\sigma) + \sigma f(\tau) \in M$.

Un hecho importante de los homomorfismos cruzados es que cuando trabajamos con un grupo cíclico de orden n generado por un elemento σ, el homomorfismo queda totalmente descrito por la imagen del elemento generador. La observación anterior queda registrada en la siguiente proposición.

Proposición 1.3.6. *Sea M un G-módulo con G un grupo cíclico generado por* σ *y sea* $f : G \to M$ *un homomorfismo cruzado, entonces* $f(\sigma^n) = f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma)$*.*

Demostración. La prueba de este hecho la haremos mediante inducción matemática, para el caso base con $n = 2$, se tiene que:

$$f(\sigma^2) = f(\sigma\sigma) = f(\sigma) + \sigma f(\sigma)$$

Suponemos vale para n (hipótesis de inducción), es decir:

$$f(\sigma^n) = f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma)$$

Veamos la validez para $n + 1$, esto es:

$$f(\sigma^{n+1}) = f(\sigma\sigma^n) = f(\sigma) + \sigma(f(\sigma^n)) = f(\sigma) + \sigma(f(\sigma^n) = f(\sigma) + \sigma(f(\sigma) + \cdots + \sigma^{n-1} f(\sigma)).$$

Utilizando la hipótesis de inducción y por M ser $G-$módulo, tenemos:

$$f(\sigma^{n+1}) = f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma) + \sigma^n f(\sigma).$$

Y así concluimos la demostración de la proposición. □

Definición 1.3.7. *Sean* $(M,+)$ *un grupo abeliano y* $x \in M$*, llamamos homomorfismo principal a* $f : G \to M$*, tal que,* $f(\sigma) = \sigma x - x$*, para todo* $\sigma \in G$*.*

Si f es un homomorfismo principal, entonces $f(\sigma) = \sigma(\beta) - \beta$, para algún $\beta \in M$ y $f(\tau) = \tau(\beta) - \beta$, además es claro que, $f(\sigma\tau) = \sigma\tau(\beta) - \beta$. Entonces:

$$\begin{aligned} f(\sigma) + \sigma f(\tau) &= \sigma(\beta) - \beta + \sigma(\tau(\beta) - \beta) \\ &= \sigma(\beta) - \beta + \sigma\tau(\beta) - \sigma(\beta) \\ &= \sigma\tau(\beta) - \beta \\ &= f(\sigma\tau) \end{aligned}$$

por lo que todo homomorfismo principal es un homomorfismo cruzado. Además, la suma de homomorfismos cruzados es nuevamente un homomorfismo cruzado. Dado que si $f, g : G \to M$ son homomorfismos cruzados, entonces.

$$\begin{aligned} (f+g)(\sigma\tau) &= f(\sigma\tau) + g(\sigma\tau) \\ &= f(\sigma) + \sigma f(\tau) + g(\sigma) + \sigma g(\tau) \\ &= f(\sigma) + g(\sigma) + \sigma f(\tau) + \sigma g(\tau) \\ &= (f+g)(\sigma) + \sigma(f+g)(\tau) \end{aligned}$$

Análogamente, la suma de dos homomorfismos principales resulta ser un homomorfismo principal. Puesto que si $f, g : G \to M$, son tal que $f(\sigma) = \sigma\beta - \beta$ y $g(\sigma) = \sigma\alpha - \alpha$, para algunos $\beta, \alpha \in M$, entonces.

$$\begin{aligned} (f+g)(\sigma) &= f(\sigma) + g(\sigma) \\ &= \sigma\beta - \beta + \sigma\alpha - \alpha \\ &= \sigma\beta + \sigma\alpha - (\beta + \alpha) \\ &= \sigma(\beta + \alpha) - (\beta + \alpha) \end{aligned}$$

Así, resulta un ejercicio simple probar que el conjunto de homomorfismos principales es un subgrupo normal del grupo de homomorfismos cruzados con la suma de funciones usual. Así las cosas, tiene sentido la siguiente definición.

Definición 1.3.8. *Sea M un G-módulo, definimos a*

$$H^1(G, M) = \{\textit{homomorfismos cruzados}\}/\{\textit{homomorfismos principales}\},$$

el cual es llamado ***primer grupo de cohomología de G en M.***

Definición 1.3.9. *Sea E un campo, denotaremos al grupo multiplicativo $(E \setminus \{0\}, \cdot)$ como $E^\times$.*

Ahora veremos en su forma moderna el Teorema 90 de Hilbert. Dicho resultado es el tema central que nos disponemos a estudiar.

1.4. TEOREMA 90 DE HILBERT

Teorema 1.4.1. *Sean $E|F$ una extensión de campos de Galois, y $G = Gal(E|F)$, entonces $H^1(G, E^\times) = 0$; es decir, todo homomorfismo cruzado de G en $E^\times$ es un homomorfismo principal.*

Demostración. Sea $f : G \to E^\times$ un homomorfismo cruzado, en notación multiplicativa esto implica que:

$$f(\sigma\tau) = f(\sigma)\sigma(f(\tau)) \text{ para todo } \sigma, \tau \in G,$$

queremos probar que existe $\beta \in E^\times$ tal que $f(\sigma) = \dfrac{\sigma(\beta)}{\beta}$, para todo $\sigma \in G$. Ahora bien, dado que $f(\tau) \in E^\times$, entonces $f(\tau) \neq 0$ para todo $\tau \in G$. Luego por la Proposición 1.2.4 se tiene que la función:

$$\sum_{\tau \in G} f(\tau)\tau : E \to E, \tag{1.35}$$

no es idénticamente la función cero; es decir, existe $\alpha \in E$ tal que:

$$\beta := \sum_{\tau \in G} f(\tau)\tau(\alpha) \neq 0 \tag{1.36}$$

Notemos que lo anterior vale dado que $E|F$ es una extensión de Galois, entonces la combinación lineal en (1.36) es finita pues $\tau \in G$ y $G = Gal(E|F)$ es finito. Es claro que $\alpha \neq 0$, pues caso contrario la función en (1.35) resulta igual a 0, contradiciendo la

afirmación (1.36). Luego, $\alpha \in E^{\times}$.
Aplicando β en cada $\sigma \in G$ se tiene:

$$\begin{aligned}\sigma(\beta) =& \sigma\left(\sum_{\tau\in G} f(\tau)\tau(\alpha)\right)\\ =& \sum_{\tau\in G}\sigma(f(\tau))\sigma\tau(\alpha),\end{aligned}$$

como sabemos $f(\sigma\tau) = f(\sigma)\sigma f(\tau)$, entonces $f^{-1}(\sigma)f(\sigma\tau) = \sigma(f(\tau))$, así la expresión anterior, se puede escribir como:

$$\begin{aligned}&\textstyle\sum_{\tau\in G} f^{-1}(\sigma)f(\sigma\tau)\sigma\tau(\alpha)\\ &= f^{-1}(\sigma)\sum_{\tau\in G} f(\sigma\tau)\sigma\tau(\alpha),\end{aligned} \tag{1.37}$$

notemos que $\{\sigma\tau \,|\, \sigma \in G\}$ es una reordenación de los elementos de G, así la expresión (1.37) se puede escribir como:

$$= f^{-1}(\sigma)\textstyle\sum_{\phi\in G} f(\phi)\phi(\alpha) = f^{-1}(\sigma)\beta,$$

con lo que concluimos $f(\sigma) = \dfrac{\beta}{\sigma(\beta)} = \dfrac{\sigma(\beta^{-1})}{\beta^{-1}}$ y tomando $\gamma = \beta^{-1}$, obtenemos:

$$f(\sigma) = \frac{\sigma(\gamma)}{\gamma},$$

que era lo que queríamos probar. □

El Teorema anterior es la versión moderna del Teorema de Hilbert 90, para su versión clásica, es necesario definir la siguiente herramienta.

Definición 1.4.2. *Sea $E|F$ una extensión de Galois con grupo de Galois G, definimos la norma de $\beta \in E$ como:*

$$N(\beta) = \prod_{\sigma\in G}\sigma(\beta)$$

Note que, para todo $\tau \in G$:

$$\tau N(\alpha) = N(\alpha),$$

por lo que, $N(\alpha) \in F$, para todo $\alpha \in E$, de esa manera:

$$N(\alpha) : E^{\times} \to F^{\times}$$

Además es fácil ver que $N(\alpha)$ es un homomorfismo.

Ejemplo 1.4.3. *Es bien sabido que $\mathbb{C}|\mathbb{R}$ es una extensión de Galois y $[\mathbb{C} : \mathbb{R}] = 2$. Luego, por el Teorema 1.2.17, el grupo de Galois $G = Gal(\mathbb{C}|\mathbb{R})$ tiene dos elementos, el homomorfismo identidad y el homomorfismo conjugación en $\mathbb{C}$. Entonces,*

$$N(x+iy) = (x+iy)(x-iy) = x^2 + y^2 = |x+iy|^2.$$

Observación: Dada un elemento de la forma $\frac{\beta}{\tau(\beta)}$ entonces la norma de este elemento es 1. Esto se tiene pues:

$$Nm\left(\frac{\beta}{\tau(\beta)}\right) = \prod_{\sigma\in G} \sigma\left(\frac{\beta}{\tau(\beta)}\right) = \prod_{\sigma\in G} \frac{\sigma(\beta)}{\sigma\tau(\beta)}, \tag{1.38}$$

como $\{\sigma\tau|\sigma \in G\}$ es una reordenación de G, se tiene que:

$$\prod_{\sigma\in G} \frac{\sigma(\beta)}{\sigma\tau(\beta)} = 1$$

El siguiente resultado evidencia que para el caso de extensiones cíclicas el recíproco de esta observación se cumple.

Definición 1.4.4. *Una extensión finita es llamada cíclica, si $E|F$ es una extensión de Galois, y Gal($E|F$) es cíclico respectivamente.*

Teorema 1.4.5. ***Versión clásica del Teorema 90 de Hilbert:*** *Sea $E|F$ una extensión cíclica finita con grupo de Galois $G = \langle\sigma\rangle$ y $\alpha \in E$. Si $N(\alpha) = 1$ entonces $\alpha = \frac{\beta}{\sigma(\beta)}$ para algún $\beta \in E$.*

Demostración. Sea $n = [E : F]$ y $\alpha \in E$, tal que $Nm(\alpha) = 1$. Por el hecho de que $E|F$ es una extensión de Galois cíclica generada por σ, vale que σ posee orden n, por lo tanto:

$$\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha) = 1,$$

de esa manera, podemos construir recursivamente un homomorfismo cruzado, tal que $f(\sigma) = \alpha$, por el Teorema de Hilbert 90 en su versión moderna, todo homomorfismo cruzado es un homomorfismo principal, así existe $\beta \in E$, tal que $\alpha = f(\sigma) = \frac{\beta}{\sigma(\beta)}$, que era lo que queríamos mostrar. □

Observación: Como $E|F$ es una extensión cíclica sabemos que el valor de un homomorfismo cruzado, queda totalmente descrito por $f(\sigma) = \alpha$, puesto que para $i > 1$:

$$f(\sigma^i) = f(\sigma)\sigma(f(\sigma)) \cdots \sigma^{i-1}(f(\sigma)) \tag{1.39}$$

Además, $f(\mathrm{Id}) = f(\sigma^n) = Nm(\alpha) = 1$, esto permite construir un homomorfismo cruzado tal que $f(\sigma) = \alpha$.

A continuación veremos el Teorema de 90 Hilbert en su versión clásica y aditiva. Esta presentación fue la primera en trabajarse y fue demostrada por la matemática alemana *Emmy Noether* (1832-1935). Para llevar a cabo esta tarea necesitamos la siguiente definición.

Definición 1.4.6. *Sea $E|F$ una extensión de Galois con grupo de Galois $G = Gal(E|F)$. Para $\alpha \in E$ definimos su traza como:*

$$Tr(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$$

Procedemos a ver el Teorema 90 de Hilbert en su forma aditiva, esta variante nos permitirá en breve solucionar el problema de las triplas pitagóricas.

Teorema 1.4.7. ***Versión clásica del teorema 90 de Hilbert en su forma aditiva:*** *Sea $E|F$ una extensión cíclica de orden n con grupo de Galois $G = \langle\sigma\rangle$. Entonces para $\alpha \in E$, $Tr(\alpha) = 0$ si, y solo si, $\alpha = \beta - \sigma(\beta)$ para algún $\beta \in E$.*

Demostración. Nuevamente por la Proposición 1.2.4 y por el hecho que G es finito puesto que $E|F$ es una extensión de Galois, tenemos que existe $\theta \in E$ tal que:

$$Tr(\theta) = \theta + \sigma(\theta) + \sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta) \neq 0.$$

Ahora tomando,

$$\beta := \frac{1}{Tr(\theta)}(\alpha\sigma(\theta) + (\alpha + \sigma(\alpha))\sigma^2(\theta)) + \cdots + (\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha))\sigma^{n-1}(\theta)) \tag{1.40}$$

se tiene que:

$$\alpha = \beta - \sigma(\beta)$$

concluyendo lo deseado.

Recíprocamente, supongamos $\alpha \in E$, es de la forma $\alpha = \beta - \sigma(\beta)$, para algún $\beta \in E$ y veamos que $Tr(\alpha) = 0$, para esto, tenemos

$$\sum_{\tau \in G} \tau(\alpha) = \sum_{\tau \in G} \tau(\beta - \sigma(\beta)) = \sum_{\tau \in G} \tau(\beta) - \tau\sigma(\beta) \tag{1.41}$$

De manera análoga, tenemos que $\{\tau\sigma | \tau \in G\}$ es una reordenación de G, por lo que:

$$\sum_{\tau \in G} \tau(\beta) - \tau\sigma(\beta) = 0 \tag{1.42}$$

Concluyendo que, $Tr(\alpha) = 0$. □

2. APLICACIONES DEL TEOREMA 90 DE HILBERT

En este capitulo veremos de qué forma el Teorema 90 de Hilbert puede ser utilizado para la solución de diversos problemas en varias áreas de la matemática. El primero de ellos está relacionado con un problema de triplas pitagóricas. El teorema que ha sido objeto de estudio en este trabajo permite encontrar sus soluciones racionales. Dicho resultado queda enmarcado a continuación.

2.1. TRIPLAS PITÁGORICAS

Proposición 2.1.1. *Sean $a, b \in \mathbb{Q}$, tal que $a^2 + b^2 = 1$, entonces existen $c, d \in \mathbb{Q}$ tal que:*

$$(a, b) = \left(\frac{c^2 - d^2}{c^2 + d^2}, \frac{2cd}{c^2 + d^2} \right) \tag{2.1}$$

Es decir, cada punto racional en $S^1 = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ es de la forma descrita en (2.1).

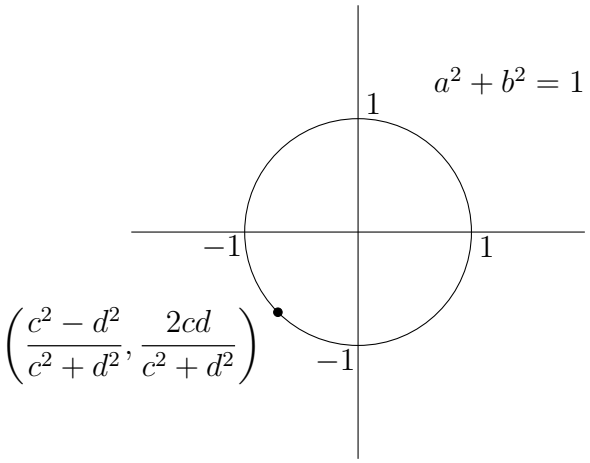

Figura 2.1: Solución ecuación de Pell

Demostración. Consideremos a $\mathbb{Q}(i) = \{a+bi | a, b \in \mathbb{Q}\}$ y $G = \langle \sigma \rangle$, grupo cícilico de orden 2, generado por:

$$\begin{aligned} \sigma : \mathbb{Q}(i) &\to \mathbb{Q}(i) \\ a + bi &\mapsto a - bi \end{aligned}$$

Es fácil ver que el campo fijado por G es el campo de los números racionales $\mathbb{Q}$. Luego, la extensión $\mathbb{Q}(i)|\mathbb{Q}$ es de Galois y cíclica, generada por el automorfismo σ. Si $\alpha = x + iy \in \mathbb{Q}(i)$, entonces su norma está dada por:

$$Nm(\alpha) = \prod_{\sigma \in G} \sigma(x+iy) = \sigma(x+iy)\mathrm{Id}(x+iy). \tag{2.2}$$

$$= (x-iy)(x+iy) = x^2 + y^2. \tag{2.3}$$

Es decir, $a^2 + b^2 = 1$, con $a, b \in \mathbb{Q}$, equivale a decir que $a + bi \in \mathbb{Q}(i)$ tiene norma 1. Luego, sigue directamente del Teorema 90 de Hilbert en su versión clásica aplicada a la extensión $\mathbb{Q}(i)|\mathbb{Q}$ que existe $c + di \in \mathbb{Q}(i)$ tal que:

$$a + bi = \frac{c+di}{\sigma(c+di)} = \frac{c+di}{c-di} \tag{2.4}$$

$$= \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2} i \tag{2.5}$$

Igualando cada una de las componentes obtenemos lo deseado. □

De manera general, para $d > 0$ libre de cuadrados, si consideramos la extensión $\mathbb{Q}(\sqrt{-d})|\mathbb{Q}$, tenemos lo siguiente.

Proposición 2.1.2. *Sea $a, b \in \mathbb{Q}$, tal que $a^2 + db^2 = 1$, entonces existen $r, s \in \mathbb{Q}$ tal que:*

$$(a, b) = \left(\frac{r^2 - ds^2}{r^2 + ds^2}, \frac{2rs}{r^2 + ds^2} \right)$$

Es decir, cada punto que satisface la anterior ecuación es de esta forma.

Demostración. De manera análoga al resultado anterior, tenemos que $\mathbb{Q}(\sqrt{-d})|\mathbb{Q}$ es una extensión de Galois cíclica con grupo de Galois cíclico de orden 2, dado por $G = \langle \tau \rangle$, donde:

$$\begin{aligned} \tau : \mathbb{Q}(\sqrt{-d}) &\to \mathbb{Q}(\sqrt{-d}) \\ a + b\sqrt{-d} &\mapsto a - b\sqrt{-d} \end{aligned}$$

Notemos que $a^2 + db^2 = 1$ es equivalente al hecho de que $Nm(a + \sqrt{-d}b) = 1$, por lo que

sigue del Teorema 90 de Hilbert que existe $r + s\sqrt{-d} \in \mathbb{Q}(\sqrt{-d})$ tal que:

$$\begin{aligned} a + b\sqrt{-d} =& \frac{r + s\sqrt{-d}}{\tau(r + s\sqrt{-d})} = \frac{r + s\sqrt{-d}}{r - s\sqrt{-d}} \\ =& \frac{r^2 - s^2}{r^2 + s^2} + \frac{2rs}{r^2 + s^2}\sqrt{-d} \end{aligned}$$

□

y obtenemos lo deseado. Observemos que la Proposición 2.39 es un caso particular de este hecho tomando a $d = 1$.

2.2. EXTENSIONES DE KUMMER

La teoría de Kummer para campos es una parte del álgebra abstracta que se encarga de estudiar extensiones de campo obtenidas adjuntando raíces $n-$ésimas de algún elemento del campo base. Recibe este nombre en honor al matemático alemán *Ernst Eduard Kummer* quien fue el precursor de esta teoría. El Teorema 90 de Hilbert, permite solucionar cierto tipo de problemas en esta teoría, por ejemplo, permite probar que cualquier extensión cíclica de grado n puede ser obtenida adjuntado la raíz $n-$ésima de algún elemento. Este hecho queda registrado a continuación.

Teorema 2.2.1. *Sea F un campo y $n \geq 1$ un número natural, Asuma que F contiene una raíz $n-$ésima de la unidad, ζ_n. Si $E|F$ es una extensión cíclica de grado n, entonces existe $a \in F$ tal que $E = F(\sqrt[n]{a})$.*

Demostración. Sean $E|F$ una extensión cíclica de grado n, y $G = Gal(E|F) = \langle\sigma\rangle$, el grupo de Galois asociado, donde $\sigma \in \mathrm{Aut}$(E). Dado que $\zeta_n \in F$, y F es un cuerpo, tenemos que $\zeta_n^{-1} \in F$. Luego, ζ_n^{-1} es fijado los elementos de G; esto es, $\tau(\zeta_n^{-1}) = \zeta_n^{-1}$, para todo $\tau \in G$, de esa manera:

$$Nm(\zeta_n^{-1}) = \prod_{\tau \in G} \tau(\zeta_n^{-1}) = (\zeta_n^{-1})^n = (\zeta_n^n)^{-1} = 1, \tag{2.6}$$

entonces, por el Teorema 1.4.5, existe $\alpha \in E^\times$, tal que:

$$\zeta_n^{-1} = \frac{\alpha}{\sigma(\alpha)} \iff \sigma(\alpha) = \zeta_n \alpha \tag{2.7}$$

notemos que,

$$\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\zeta_n\alpha) = \sigma(\zeta_n)\sigma(\alpha) = \zeta_n(\zeta_n\alpha) = \zeta_n^2\alpha$$
$$\sigma^3(\alpha) = \sigma(\sigma^2(\alpha)) = \sigma(\zeta_n^2\alpha) = \sigma(\zeta_n^2)\sigma(\alpha) = \zeta_n^2(\zeta_n\alpha) = \zeta_n^3\alpha$$
$$\vdots$$
$$\sigma^{j+1}(\alpha) = \sigma(\sigma^j(\alpha)) = \sigma(\zeta_n^j\alpha) = \sigma(\zeta_n^j)\sigma(\alpha) = \zeta_n^j(\zeta_n\alpha) = \zeta_n^{j+1}\alpha$$

para todo $j \in \{1, 2, 3, \ldots, n\}$.
Luego, α tiene n distintos conjugados, dados por $\zeta_n\alpha, \zeta_n^2\alpha, \ldots, \zeta_n^n\alpha$. A consecuencia de la Proposición 1.1.19, sigue que $[F(\alpha) : F] =$ grad $p(x)$, con $p(x) \in F[x]$ el polinomio mínimo de α sobre F. Por la razón anterior, $p(\alpha) = 0$. Aplicando cada automorfismo, tenemos:

$$\sigma^j(0) = 0 = \sigma^j(p(\alpha)) = p(\sigma^j(\alpha)) = p(\zeta_n^{j+1}\alpha)$$

esto implica que $p(x)$ tiene como raíces a los n conjugados de α; es decir, grad $p(x) \geq n$. Luego, $[F(\alpha) : F] \geq n$. Sin embargo, $[E : F] = n$ y $F(\alpha) \subset E$, entonces $E = F(\alpha)$. Además, como:

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta^n\alpha)^n = \zeta_n^n\alpha_n = \alpha^n \tag{2.8}$$

Tenemos que $\alpha^n \in F$, así podemos escribir a como $E = F(\sqrt[n]{a})$, tomando a $\alpha^n = a$. □

2.3. EXTENSIONES DE ARTIN-SCHREIER

Usando la forma aditiva del Teorema 90 de Hilbert, es posible probar, de manera análoga a las extensiones de Kummer, que cualquier extensión cíclica de grado p y característica p es posible obtenerla adjuntando una raíz de algún polinomio. Este hecho queda demostrado en el siguiente teorema.

Teorema 2.3.1. *Sea F un campo de característica $p > 0$.*

1. *Para todo $a \in F$, el polinomio $x^p - x - a \in F[x]$ es completamente reducible, es decir, todas las raíces están en F ó es irreducible.*

2. *Recíprocamente, si $E|F$ es una extensión cíclica de Galois de grado p, entonces E es el campo de ruptura de $x^p - x - a$ para algún $a \in F$.*

Demostración. Sea $p(x) = x^p - x - a \in F[x]$. Para demostrar el primer enunciado, observemos que si $\alpha \in F$ es un raíz de éste polinomio, es decir, $\alpha^p - \alpha - a = 0$, entonces

$\alpha + j$ también lo es para $j \in \{0, 1, \ldots, p\}$. Lo anterior se tiene, pues:

$$\begin{aligned}(\alpha + j)^p - (\alpha + j) - a =& \alpha^p + j^p - \alpha - j - a \\ =& (\alpha^p - \alpha - a) + j^p - j \\ =& 0 + j^p - j = 0.\end{aligned}$$

Luego, si $p(x)$ posee una raíz en F, entonces todas sus raíces están en F.
Ahora asumamos que $p(x)$ no tiene raíces en F. Nuestra afirmación es que $p(x)$ es irreducible sobre F. Procedamos vía contradicción, asumamos las condiciones del teorema y que existen $f(x)$ y $h(x)$ en $F[x]$ polinomios no constantes tal que $p(x) = f(x)h(x)$. Sea α una raíz de $p(x)$, la existencia de α está garantizada por el Teorema de Kronocker, de manera análoga al argumento anterior, tenemos que $\alpha + j$ es una raíz de $p(x)$ para $0 \leq j \leq p - 1$, por lo que,

$$p(x) = \prod_{0 \leq j \leq p-1} (x - \alpha - j)$$

donde,

$$f(x) = \prod_{j \in S} (x - \alpha - j) \text{ y } h(x) = \prod_{j \notin S} (x - \alpha - j)$$

para todo $S \subseteq \{1, 2, \ldots, p - 1\}$. Supongamos que $|S| = d$, entonces el coeficiente $d - 1$ de $p(x)$ viene dado por:

$$-\sum_{j \in S} (\alpha + j) = -\sum_{j \in S} \alpha - \sum_{j \in S} j = d\alpha - \sum_{j \in S} j \in F.$$

por lo que, $d\alpha \in F$ y esto para $0 < d < p$. Luego $\alpha \in F$, llegando a una contradicción.

Para el segundo enunciado, consideremos $E|F$ una extensión cíclica de grado p, con grupo de Galois dado por $G = \langle \sigma \rangle$. Notemos que,

$$Tr(-1) = \sum_{\sigma \in G} \sigma(-1) = \sum_{\sigma \in G} (-1) = -p = 0$$

entonces por el Teorema 90 de Hilbert en forma aditiva existe $\alpha \in E$, tal que:

$$-1 = \alpha - \sigma(\alpha) \Leftrightarrow \sigma(\alpha) = \alpha + 1$$

por inducción matemática es fácil probar que, $\sigma^j(\alpha) = \alpha + j$, entonces α tiene p distintos

conjugados, por un argumento similiar al utilizado en el Teorema 2.2.1, se tiene que $[F(\alpha) : F] \geq p$, sin embargo, $[E : F] = p$, por lo que $F(\alpha) = E$.
Por otro lado, tenemos que,

$$\begin{aligned}\sigma(\alpha^p - \alpha) =& \sigma(\alpha)^p - \sigma(\alpha)\\ =& (\alpha+1)^p - (\alpha+1)\\ =& \alpha^p + 1 - \alpha - 1\\ =& \alpha^p - \alpha.\end{aligned}$$

Por lo que, $\alpha^p - \alpha \in F$. De esa manera, α es una raíz del polinomio $p(x) = x^p - x - a \in F[x]$, con $a = \alpha^p - \alpha$. Y concluimos lo deseado. □

En general, no es sencillo el trabajo de encontrar un polinomio irreducible sobre un campo finito. El teorema anterior nos da una forma de hallarlo. Un ejemplo de este hecho queda registrado en el siguiente resultado.

Ejemplo 2.3.2. *El polinomio $x^p - x - 1$ es irreducible sobre $\mathbb{F}_p$.*

Demostración. Por el teorema anterior, el polinomio $x^p - x - 1$, posee todas sus raíces en $\mathbb{F}_p$ ó es irreducible sobre $\mathbb{F}_p$. Sin embargo, $1_{\mathbb{F}_p} \in \mathbb{F}_p$ y $1^p - 1 - 1 = -1 \neq 0$, como $|\mathbb{F}_p| = p$, tenemos que $x^p - x - 1$ no posee todas sus raíces en $\mathbb{F}_p$, por lo tanto es irreducible sobre $\mathbb{F}_p$. □

2.4. CAMPO DE FUNCIONES

El siguiente resultado es una aplicación directa del Teorema 90 de Hilbert y que está relacionado con el campo de funciones racionales, en pocas palabras, nos indica la forma específica de una función bajo ciertas condiciones, involucrando una raíz $n-$ésima de la unidad. Dicho enunciado viene dado a continuación.

Teorema 2.4.1. *Sea $f(x) \in \mathbb{C}(x)$ una función racional que satisface.*

$$f(x)f(\zeta x)f(\zeta^2 x)\ldots f(\zeta^{n-1}x) = 1$$

para $\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$, raíz $n-$ésima de la unidad. Entonces existe $g(x) \in \mathbb{C}(x)$, tal que:

$$f(x) = \frac{g(x)}{g(\zeta x)}$$

Demostración. Para la prueba de este hecho, vamos a tomar a $E = \mathbb{C}(x)$ y $F = \mathbb{C}(x^n)$ como subcampo de E. Lo primero que debemos mostrar es que $E|F$ es una extensión de Galois. Para esto, notemos que $\mathbb{C}(x)$ es el campo de ruptura de $p(y) = y^n - x^n \in F[y] = C(x^n)[y]$ ya que $p(y)$ posee la siguiente factorización:

$$p(y) = (y - x)(y - \zeta x)(y - \zeta^2 x) \dots (y - \zeta^n x)$$

además, las raíces del polinomio $p(y)$ son distintas. Luego $p(y)$ es separable y utilizando el Teorema 1.2.17 concluimos que $E|F$ es de Galois. La segunda afirmación es que $Gal(E|F)$ es isomorfo a $\mathbb{Z}_n$. Para esto, vamos a considerar la siguiente función.

$$\begin{aligned} f : \mathbb{Z}_n &\to Gal(E|F) \\ k &\mapsto \sigma_k(x) \end{aligned}$$

donde,

$$\begin{aligned} \sigma_k : \mathbb{C}(x) &\to \mathbb{C}(x) \\ r(x) &\mapsto r(\zeta^k x) \end{aligned}$$

Lo primero que debemos verificar es que la función se encuentra bien definida. Para esto, sean $k, k' \in \mathbb{Z}_n$, con $k = k'$. Esto implica que, $k - k' = ln$, para algún $l \in \mathbb{Z}$. De esa manera, $1 = \zeta^{ln} = \zeta^{k-k'}$, por lo que, $\zeta^k = \zeta^{k'}$, concluyendo que $\sigma_k = \sigma_{k'}$.
El siguiente hecho que debemos verificar es que el conjunto de llegada de f es $Gal(E|F)$, es decir, cada σ_k es un elemento del grupo de Galois. Es fácil ver que los σ_k son automorfismos de $\mathbb{C}(x)$. Además si $r(x^n) \in F = \mathbb{C}(x^n)$, se tiene que, $\sigma_k(r(x^n)) = r((\zeta^k x)^n) = r(x^n)$, por lo que $\sigma_k \in Gal(E|F)$ para todo $k \in \mathbb{Z}_n$. Falta ver que f es un isomorfismo. Para esto, $f(k + k') = \sigma(\zeta^{k+k'} x) = \sigma_k \sigma_{k'}$. Para la inyectividad, veamos que, $ker(f) = 0$. En efecto, si $\sigma_k(x) = \mathrm{Id}(x)$ para todo x, implica que, $r(x) = r(\zeta^k x)$, así $k = 0$. En cuanto a la sobreyectividad, notemos que $\{1, x, x^2, \cdots, x^{n-1}\}$ es una base para $E|F$, de esa manera, por el Teorema 1.2.7 $|Gal(E|F)| = [E : F] = n$. Luego, por la inyectividad de f y el hecho de que $\mathbb{Z}_n$ tiene n elementos, sigue la sobreyectividad de f. Por el argumento anterior, tenemos que $Gal(E|F) \cong \mathbb{Z}_n$, como $\mathbb{Z}_n = \langle 1 \rangle$, tenemos que $Gal(E|F) = \langle f(1) \rangle$, con $f(1) = \sigma_1$, esto es:

$$\begin{aligned} \sigma_1 : \quad \mathbb{C}(x) &\to \mathbb{C}(x) \\ r(x) &\mapsto r(\zeta x) \end{aligned}$$

La condición inicial del teorema, es equivalente a que $N(f(x)) = 1$, así por el Teorema 90 de Hilbert, existe $g(x) \in \mathbb{C}(x)$, tal que $f(x) = \dfrac{f(x)}{\sigma_1(f(x))}$, esto es equivalente a $f(x) = \dfrac{g(x)}{g(\zeta x)}$ y obtenemos lo deseado.

□

Un ejemplo del teorema anterior queda garantizado a continuación.

Ejemplo 2.4.2. *Consideremos la función $f(x) = \zeta$. Lo primero que debemos ver es que $f(x)$ verifica las condiciones del Teorema 2.4.1. Lo anterior tiene validez, debido a que,*

$$f(x)f(\zeta x)\cdots f(\zeta^{n-1}x) = \zeta^n = 1$$

por lo que, mediante el Teorema 2.4.1 se garantiza la existencia de $g(x) \in \mathbb{C}(x)$, tal que $f(x) = \dfrac{g(x)}{g(\zeta x)}$. En este caso, tomando $g(x) = \dfrac{1}{x}$, se tiene el resultado.

Observación: El teorema anterior garantiza la existencia $g(x) \in \mathbb{C}(x)$ bajo las condiciones indicadas, sin embargo, no garantiza la unicidad, por ejemplo, en el ejemplo anterior la función, $g(x) = \dfrac{1}{cx}$, para todo $c \in \mathbb{R}$, también verifica las condiciones del teorema.

2.5. OTRAS APLICACIONES

Una de las cualidades del Teorema 90 de Hilbert, que lo convierten en tema de interés para muchos matemáticos es su amplia gama de aplicaciones no solo en el área de álgebra sino que, en diferentes áreas de la matemática. Por ejemplo, en geometría algebraica este teorema tiene diversas implicaciones desde el punto de vista algebraico, para muestra de ello, ver el articulo [6], donde se explora bajo otra perspectiva los alcances de este teorema. Además de esto, existen generalizaciones de este teorema a otros contextos, por ejemplo en [7], se puede encontrar una versión del Teorema 90 de Hilbert para el caso de acciones parciales. De esa manera, si el lector se interesa en el tema puede consultar cualquiera de los artículos anteriores.

---

[6] Schröer S. "Hilbert's Theorem 90 and algebraic spaces". En: *Journal of Pure and Applied Algebra.* (2002).

[7] PINEDO H. y ROCHA I. DOKUCHAEV M. PAQUES A. "Partial generalized crossed products and a seven-term exact sequence". En: *Journal of Algebra.* (2021).

Bibliografía

ARTIN Emil y Milgram, A.N. *Galois Theory*. Notre Dame Mathematical Lectures, New Jersey, 1971 (vid. págs. 8, 11, 32).

DOKUCHAEV M. PAQUES A., PINEDO H. y ROCHA I. "Partial generalized crossed products and a seven-term exact sequence". En: *Journal of Algebra.* (2021) (vid. pág. 49).

DUMMIT D.S y FOOTE, A.N. *Abstract Algebra.* John Wiley & Sons, Vermont, 2004 (vid. pág. 10).

GALLIAN, J.A. *Contemporary Abstract Algebra*. Cengage learning, Minnesota, 2010 (vid. pág. 10).

LEE, Seewoo. "Hilbert's theorem 90". En: *Berkeley University Library* (2018) (vid. pág. 8).

MILNE, J.S. *Fields and Galois Theory*. Princeton Mathematical Series, New Jersey, 2021 (vid. pág. 32).

S., Schröer. "Hilbert's Theorem 90 and algebraic spaces". En: *Journal of Pure and Applied Algebra.* (2002) (vid. pág. 49).