Teoría de Galois

Miguel González
mgonzalez.contacto@gmail.com
miguelgg.com

Enero de 2021

$$G = \mathrm{Gal}(E/L) \longleftrightarrow L = E^G/K$$

Revisado en 2022
Apuntes de la asignatura impartida por Ana Bravo
en la Universidad Autónoma de Madrid en Enero de 2021.

Acerca de este documento

Estos apuntes son una versión revisada de los de la asignatura Teoría de Galois del grado en matemáticas, tomados en Enero de 2021 por Miguel González. La asignatura fue impartida por Ana Bravo. A los apuntes originales se les ha añadido esta página, una imagen de portada, y breves párrafos explicativos en las zonas menos completas. Asimismo se han revisado las erratas y completado los contenidos faltantes.

Este documento es:

- Una recopilación ordenada y directa de las definiciones y resultados más importantes del tema en cuestión, al nivel de los estudios de grado.
- Una colección de demostraciones completas de dichos resultados (salvo en los casos más básicos).
- Una *guía* para revisar de manera rápida las ideas que se han adquirido previamente, o para consultar enunciados puntuales que puedan no haberse comprendido en su totalidad.

Este documento NO es:

- Un libro de texto de la asignatura.
- Una colección de ejercicios para practicar los conceptos adquiridos.
- Un listado de ejemplos para ilustrar las ideas tratadas. A pesar de ello, en ocasiones se incluyen ejemplos puntuales que puedan ser de especial interés o curiosidad, pero se intentan reducir al mínimo en virtud del primer punto de la lista anterior.

Sobre Teoría de Galois

En esta asignatura se desarrolla la teoría de anillos y teoría de cuerpos y extensiones de cuerpos necesaria para establecer el Teorema Fundamental de la Teoría de Galois, que establece una correspondencia entre ciertas extensiones de un cuerpo y ciertos subgrupos de un grupo, permitiendo estudiar la estructura de los cuerpos a través de la teoría de grupos.

Esta teoría desemboca en multitud de aplicaciones, en problemas clásicos inclusive, como la irresolubilidad por radicales de ciertos polinomios de grado superior a 4, o la imposibilidad de la cuadratura del círculo, entre otros.

Requisitos previos

1. Conocimientos de álgebra lineal.
2. Conocimientos de estructuras algebraicas, sobre todo de teoría de grupos (se revisará la teoría de anillos y cuerpos).

Índice

1. Introducción. Teoría de Anillos. 3
1.1. Anillos de polinomios . . . 4
1.2. Ideales en un anillo . . . 4
1.3. Anillo cociente . . . 5
1.4. Homomorfismos de anillos . . . 6
1.5. Ideales primos y maximales . . . 7
1.5.1. Ideales primos y maximales en $K[X]$ . . . 8

2. Extensiones de cuerpos 10

3. Extensiones de Galois 12
3.1. El grupo de Galois de una extensión . . . 13
3.2. Extensiones normales . . . 14
3.3. Separabilidad . . . 15
3.4. Cuerpos finitos . . . 17

4. El Teorema Fundamental 19
4.1. Subcuerpos intermedios y subgrupos del grupo de Galois . . . 20
4.2. El Teorema Fundamental . . . 23

5. Resolución por radicales 25

1. Introducción. Teoría de Anillos.

El objetivo global de este documento es demostrar el **Teorema de Galois**. La teoría que se va a desarrollar para llegar a ese objetivo resultará notablemente potente y de gran interés. El Teorema de Galois establece que, para ecuaciones polinómicas $a_n x^n + \cdots + a_1 x + a_0 = 0$, $a_n \neq 0$, no existen expresiones **generales** (para todas las ecuaciones simultáneamente fijado el n) con sumas, restas, productos, cocientes y radicales que proporcionen los valores solución de x si $n \geq 5$.

Para comenzar a comprender cómo se va a enfocar el problema, supongamos por el momento que los $a_i \in \mathbb{Q}$. Sabemos que va a haber n raíces, no necesariamente racionales. Consideramos el menor cuerpo que contiene a las raíces y a $\mathbb{Q}$. La teoría de Galois asociará a este cuerpo especial un grupo finito, cuyas propiedades revelarán si las raíces pueden obtenerse mediante una fórmula con las características ya mencionadas.

Con el fin de llegar hasta ese objetivo, repasaremos los conceptos de teoría de anillos:

Definición 1. Un **anillo** es un conjunto R no vacío dotado de dos operadores, $+ : R \times R \to R$, y $\cdot : R \times R \to R$, tales que $(R, +)$ es un grupo abeliano, $\cdot$ es asociativa, y se verifica que $\forall a, b, c \in \mathbb{R}$ se tiene $a(b + c) = ab + ac$, es decir, la propiedad distributiva que vincula ambas operaciones.

Si además $(R, \cdot)$ tiene un elemento neutro (conocido como *identidad*), entonces se dice que *el anillo tiene unidad*. Asimismo, si $\cdot$ es conmutativa, entonces R es un **anillo conmutativo**.

A partir de este momento se asume que los anillos son conmutativos y con unidad. Se denotará por 0 el neutro de la suma, 1 la identidad del producto, $-a$ el opuesto de la suma, y a^{-1} el opuesto del producto (denominado *inverso*) en caso de que exista. Asimismo, denotaremos na el resultado de operar n veces al elemento a con la operación suma, y a^n para lo mismo con el operador producto.

Definición 2. Un anillo $(R, +, \cdot)$ es un **cuerpo** si $(R \backslash \{0\}, \cdot)$ es un grupo abeliano, es decir, si todo elemento no nulo de R tiene inverso multiplicativo.

Sabemos que si consideramos el anillo $\mathbb{Z}_n$, cuando n es primo, se trata de un cuerpo. En estos casos se suele denotar por $\mathbb{F}_n$, al igual que cuando se considera como grupo se denotaba C_n al ser el cíclico.

Definición 3. Sea R un anillo. Un elemento $a \in R$, $a \neq 0$ es un **divisor de cero** si $\exists b \in R$, $b \neq 0$ tal que $ab = 0$.

Por ejemplo, en $\mathbb{Z}_6$, tenemos que $2 \cdot 3 = 0$. Ambos son por tanto divisores de cero.

Definición 4. Si R no tiene divisores de cero, se dice que es un **dominio de integridad**.

Definición 5. Sea R un anillo. Se dice que un elemento $a \in R$ divide a otro $b \in R$, si $\exists c \in R$ tal que $ac = b$. Se denota por $a \mid b$.

Definición 6. Se dice que $S \subset R$ es un subanillo si $(S, +, \cdot)$ es un anillo conmutativo y con unidad. Obsérvese que esto equivale a que sea no vacío y cerrado a la suma y producto, así como contener al 1.

Por ejemplo, $\mathbb{Z} \subset \mathbb{C}$ es un subanillo. Nos podemos plantear qué ocurre si consideramos un elemento de $\mathbb{C}$, como $i \in \mathbb{C}$, y preguntarse cuál es el subanillo de $\mathbb{C}$ más pequeño que contiene tanto a $\mathbb{Z}$ como a i. Esto lo denotaremos $\mathbb{Z}[i]$. Que este anillo exista, en general para cualquier subanillo $S \subset R$ y elementos $\{a_1, \ldots, a_k\} \subset R$, puede justificarse considerando todos los subanillos de R que contienen a S y a los elementos a_i, que existen (por lo menos R cumple eso), e intersecando todos. Como la intersección de subanillos es un subanillo, se obtiene tal subanillo más pequeño que los contiene.

Vamos a tratar de construir un subanillo de este tipo, por ejemplo $Q[\sqrt{2}, \sqrt[3]{3}]$. Un elemento de este anillo deberá tener la forma $a_0 + a_{10}\sqrt{2} + a_{01}\sqrt[3]{3} + a_{11}\sqrt{2}\sqrt[3]{3} + \cdots + a_{ij}\sqrt{2}^i\sqrt[3]{3}^j$, para unos $a_{ij} \in \mathbb{Q}$. Es decir, debe obtenerse mediante sumas y productos de elementos de $\mathbb{Q}$ y ambas raíces (no aparecen potencias de racionales ni sumas de racionales porque dan lugar a nuevos racioneales). Es fácil ver que realmente $0 \leq i \leq 1$ y $0 \leq j \leq 2$, dado que sucesivas potencias se convierten en racionales.

Otra idea que puede plantearse es, dado un subanillo de un cuerpo, como $\mathbb{Q} \subset \mathbb{R}$, obtener el **subcuerpo más pequeño** que contiene a $\mathbb{Q}$ y a algún elemento como $\sqrt{2}$. Su existencia se justifica con un argumento de intersecciones como antes, y se denota $\mathbb{Q}(\sqrt{2})$. Evidentemente, $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. Vamos a tratar de construir $\mathbb{Q}(\sqrt{2})$. Comenzamos por añadir los inversos de $\mathbb{Q}[\sqrt{2}]$ y hacer las combinaciones lineales necesarias. Estos inversos son de la forma $\frac{1}{a+b\sqrt{2}}$, luego los elementos de $\mathbb{Q}(\sqrt{2})$ tienen la forma $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ para $a, b, c, d \in \mathbb{Q}$. Simplificando esa expresión se comprueba que coincide con $\mathbb{Q}[\sqrt{2}]$, y este hecho será de importancia próximamente.

1.1. Anillos de polinomios

Motivados por lo anterior, vamos a considerar un elemento indeterminado X y construir los anillos de polinomios de esta manera:

Definición 7. Sea R un anillo. Construimos el **anillo de polinomios** $R[X] = \{a_0 + a_1X + \cdots + a_nX^n, a_i \in R, n \in \mathbb{N}\}$, con la suma y producto de polinomios habituales. Para polinomios no nulos, el coeficiente de la mayor potencia no nulo se denomina **coeficiente director**, y tal potencia n se denomina **grado** del polinomio (denotado por $gr(p)$, $deg(p)$). Si el coeficiente director es la unidad 1, se dice que el polinomio es **mónico**.

Recordemos que dados polinomios no nulos $p = \sum a_iX^i$, $q = \sum b_jX^j$, se tiene $gr(pq) = gr(p) + gr(q)$ **siempre que** R **sea un dominio** (para evitar que pueda anularse el coeficiente de $X^{gr(p)+gr(q)}$, que es $a_{gr(p)}b_{gr(q)}$). En general se da que $gr(pq) \leq gr(p) + gr(q)$. De aquí se deduce también que si R es un dominio, las unidades de $R[X]$ han de tener forzosamente grado 0, dado que si $pq = 1$, entonces $gr(pq) = 0$, luego $gr(p) + gr(q) = 0$, únicamente posible si ambos grados son cero. Por tanto las unidades de $R[X]$ son las mismas que las de R. Si R es cuerpo, entonces son todos los elementos de grado 0 de $R[X]$. Obsérvese que $R[X]$, por tanto, **nunca puede ser un cuerpo** (si R es dominio).

Asimismo podemos definir $K(X)$ análogamente como $\{\frac{p(X)}{q(X)} : p(X), q(X) \in K[X], q(X) \neq 0\}$, insipirados por los conceptos anteriores. Es decir, el *cuerpo más pequeño que contiene* a K y a X. Las operaciones son las usuales y estableciendo que $\frac{P}{Q} = \frac{R}{S}$ siempre que $PS = RQ$ (esto se hace interpretando $K(X)$ como un cociente de $K \times K$ bajo esa relación de equivalencia).

1.2. Ideales en un anillo

Definición 8. Sea R un anillo. Un **ideal** de R es un subconjunto no vacío $I \subset R$, que verifica:

1. $(I, +)$ es subgrupo de $(R, +)$.
2. $\forall r \in R$, $a \in I$, se tiene que $ra \in I$. (Absorción)

Observación 1. Dado $I \subset R$, $I \neq \emptyset$, se tiene que I es ideal si y solo si

1. $\forall a, b \in I$, se tiene $a + b \in I$.
2. $\forall r \in R$, $a \in I$, se tiene que $ra \in I$. (Absorción)

Esto sigue de que el hecho de que I sea subgrupo de R equivale a que si $a, b \in R$, entonces $a - b \in R$, y gracias a la segunda propiedad, esto equivale a que $a + b \in R$, puesto que si $a - b \in R$, entonces $(a - (-b)) \in R$ puesto que $-b = (-1)b \in R$, entonces $a + b \in R$. Del mismo modo se revierte esta implicación.

En todo anillo R se tiene por lo menos el ideal R, y también $\{0\}$. Si un ideal no es el total, se denomina **propio**.

Observación 2. Sea R un anillo, $I, J \subset R$ ideales. Entonces $I \cap J$ es ideal. No obstante, $I \cup J$ no lo es necesariamente.

Se comprueba de inmediato.

Observación 3. Si K es un cuerpo, solo contiene como ideales a $\{0\}$ y a K. El recíproco es cierto también.

Razón. Dado un ideal no trivial, tomamos $a \neq 0$. Entonces $aa^{-1} = 1$ está en el ideal, y dado $k \in K$, se tiene que $1k = k$ también. Para el recíproco, dado $k \in K$ no nulo, consideramos el ideal $\{ak : a \in K\}$ (es fácil verificar que es ideal). Este ideal no es $\{0\}$ luego ha de ser igual a K. Como $1 \in K$, debe darse que $\exists a \in K$ tal que $ak = 1$. □

Definición 9. Sea $\{r_i\}_{i \in I}$ una familia de elementos del anillo R. Se dice que el **ideal generado** por esa familia es el más pequeño que los contiene. Se denota $\langle r_i \rangle_{i \in I}$.

Este ideal existe argumentando, como anteriormente, que ha de ser la intersección de todos los ideales que contienen a esa familia (hay al menos uno: R). Podemos encontrar una construcción explícita:

Proposición 1. *Se tiene que* $\langle r_i \rangle_{i \in I} = \{a_1 r_1 + \cdots + a_k r_k : k \in \mathbb{N}, r_1, \ldots, r_k \in \{r_i\}_{i \in I}\}$*, es decir, son las combinaciones lineales de cantidades finitas de elementos.*

Definición 10. Un ideal I es principal si $I = \langle a \rangle$ para cierto $a \in R$.

Teorema 1. *Si K es un cuerpo, entonces en $K[X]$ todos los ideales son principales (y entonces se denomina **dominio de ideales principales**).*

Demostración. Sea $I \subset K[X]$ un ideal distinto del trivial (el trivial es principal). Entonces $\exists p \in I$ tal que $p \neq 0$. Sea $\Lambda = \{\deg p(x) : p(x) \in I\} \subset \mathbb{N}$, que es no vacío al haber un polinomio no nulo en I. Sea entonces $n = \min \Lambda$, y $q(x) \in I$ alguno con grado n. Se afirma entonces que $I = \langle q \rangle$. Para comprobarlo, sea $s \in I$. Como K es cuerpo, podemos aplicar la división euclídea: $s(x) = q(x)c(x) + r(x)$ con $\deg r < \deg q = n$, o bien $r = 0$. Pero como $r = s - qc$, y $q, s \in I$, ha de darse que $r \in I$, pero por minimalidad del n ha de ser forzosamente que $r = 0$, luego $s = qc$, por tanto $I \subset \langle q \rangle$, y hemos acabado (dado que claramente $\langle q \rangle \subset I$). □

Obsérvese que entonces todos los ideales son de la forma $\langle p(x) \rangle$, pero resulta que si $k \in K$ no nulo, entonces $\langle p(x) \rangle = \langle kp(x) \rangle$. Si establecemos un coeficiente principal, entonces cada ideal de $K[X]$ es generado por un único elemento con ese coeficiente principal (en general se toma el mónico).

1.3. Anillo cociente

Sea R un anillo y sea $I \subset R$ un ideal. Se define en R la relación de equivalencia $a \sim b \iff a - b \in I$. Como R es conmutativo, entonces $I \lhd R$ y podemos considerar como grupo el cociente R/I con la suma heredada de R. La pregunta razonable es si puede ser también un anillo heredando el producto ($\overline{a}\overline{b} = \overline{ab}$). Lo más importante para responder a esta pregunta es si la operación está bien definida, puesto que en ese caso las propiedades de anillo se heredan automáticamente. Consideramos $\overline{a}$ y $\overline{b}$. Cualquier otro elemento de esas clases puede escribirse como $a + i$ o $b + j$ dados $i, j \in I$. Tenemos que comprobar entonces que $\overline{(a+i)(b+j)} = \overline{ab}$. Pero como en R se tiene que $(a+i)(b+j) = ab + aj + bi + ij$. Por definición de ideal, tenemos entonces que $aj + bi + ij \in I$, luego se tiene lo que se quería. Este suceso es el que motiva la definición de ideal, de hecho.

1.4. Homomorfismos de anillos

Definición 11. Sean R,T anillos. Un **homomorfismo de anillos** $f : R \to T$ es una función tal que, $\forall r, r' \in R$:

1. $f(r + r') = f(r) + f(r')$
2. $f(rr') = f(r)f(r')$
3. $f(1) = 1$

Por ejemplo, $f : \mathbb{Z} \to R$, siendo R arbitrario, si ha de ser un homomorfismo, debe ser que $f(1) = 1$, pero entonces si $n > 0$, $f(n) = 1_R + 1_R + \cdots + 1_R = n \cdot 1_R$, forzando el valor de f en todos los enteros positivos. Asimismo $f(-n) = -f(n)$ luego está forzado también. Existe, por tanto, y es único (es fácil comprobar que cumple la propiedad del producto).

Otro ejemplo de importancia es el paso al cociente. Dado $I \subset \mathbb{R}$ ideal, consideramos $\pi : R \to R/I$ dado por $\pi(a) = \overline{a} \in R/I$.

Finalmente, supongamos que R es un anillo. Consideramos de nuevo el $f : \mathbb{Z} \to R$ único. Si $p \in \mathbb{Z}$ es primo y $f(p) = 0$, se tiene $g : R \to R$ dado por $g(a) = a^p$ es homomorfismo y se conoce como **morfismo de Fröbenius**.

Proposición 2 (Propiedades de los homomorfismos)**.** *Sea $f : R \to T$ homomorfismo de anillos.*

1. *Si $S \subset R$ es subanillo, también lo es $f(S) \subset T$.*
2. *Si $J \subset T$ es ideal, entonces $f^{-1}(J) \subset R$ es ideal.*
3. *Si f es sobreyectivo, y $I \subset R$ es ideal, entonces $f(I) \subset T$ es ideal.*
4. *$Nuc(f) \subset R$ es un ideal.*
5. *f es inyectivo $\iff$ $Nuc(f) = \{0\}$.*

Demostración. Para 1, sabemos que como f es homomorfismo de grupos, $f(S)$ es subgrupo. Asimismo, como $1 \in S$, entonces $1 \in f(S)$, y si $a, b \in f(S)$, con $a = f(s_1)$, $b = f(s_2)$, se tiene que $ab = f(s_1 s_2) \in f(S)$. Para 2, sabemos que $f^{-1}(J)$ es subgrupo. Ahora, dado $a \in f^{-1}(J)$, con $f(a) = j \in J$, y dado $r \in R$, tenemos que $f(ra) = f(r)j \in J$, luego $ra \in f^{-1}(J)$ y es ideal. Para 3, sabemos que $f(I)$ es subgrupo. Dado $a \in f(I)$, $t \in T$, escribamos $a = f(i)$ para $i \in I$, y $t = f(r)$ para $r \in R$, dado que f es sobreyectivo. Tenemos entonces que $at = f(ir) \in f(I)$ por ser $ir \in I$ al ser ideal. Para 4, sabemos que $Nuc(f)$ es subgrupo. Dado $n \in Nuc(f)$ y $r \in r$, se tiene que $rn \in Nuc(f)$ puesto que $f(rn) = f(r)f(n) = f(r)0 = 0$. Para 5, como f es homomorfismo de grupos si consideramos solo $(R, +)$ y $(T, +)$, y ese enunciado es válido para homomorfismos de grupos, se tiene. □

Corolario. Sea $f : K \to T$ homomorfismo de anillos, y supongamos que K es cuerpo. Entonces f es inyectiva, dado que $Nuc(f)$ debe ser $\{0\}$ (si fuese todo K, no se daría $f(1) = 1$).

Observación 4. Si $f : R \to T$ es homomorfismo de anillos biyectivo, entonces su inversa $f^{-1} : T \to R$ es también homomorfismo de anillos. En ese caso se denomina *isomorfismo*.

Demostración. Ya sabemos que f^{-1} es homomorfismo de grupos. Asimismo, dados $a, b \in T$, digamos con $f(r_1) = a$, $f(r_2) = b$, entonces se tiene que $f^{-1}(a)f^{-1}(b) = r_1 r_2$, pero además como $f(r_1 r_2) = f(r_1)f(r_2) = ab$, se tiene que $f^{-1}(ab) = r_1 r_2$, luego son iguales. Asimismo, como $f(1) = 1$, entonces $f^{-1}(1) = 1$. □

Teorema 2 (De isomorfía)**.** *Sea $f : R \to T$ un homomorfismo de anillos cualquiera. Entonces $\exists \overline{f} : R/Nuc(f) \to T$, homomorfismo, tal que $f = \overline{f} \circ \pi$, dada por definición como $\overline{f}(\overline{a}) = f(a)$. Asimismo, se tiene que $\overline{f}$ es inyectiva y, por tanto, hay un isomorfismo entre $R/Nuc(f)$ y $f(R)$.*

Demostración. Basta con ver que esa $\overline{f}$ está bien definida, dado que las propiedades de homomorfismo siguen de forma natural de su definición (se heredan de f). Se tiene que si $\overline{a} = \overline{b}$, entonces $a = b + n$ con $n \in Nuc(f)$, luego $f(a) = f(b+n)$ y por tanto $f(a) = f(b) + f(n) = f(b) + 0 = f(b)$, luego efectivamente la imagen no depende del representante. Para ver que $\overline{f}$ es inyectiva, si $\overline{f}(a) = 0$, es porque $f(a) = 0$ luego $a \in Nuc(f)$, y por tanto $\overline{a} = \overline{0}$. Es decir, $Nuc(\overline{(f)}) = \{\overline{0}\}$. □

Definición 12. Sea R un anillo cualquiera. Consideramos el homomorfismo $f : \mathbb{Z} \to R$ único. Sabemos que $Nuc(f) \subset \mathbb{Z}$ es un ideal, y por tanto $Nuc(f) = k\mathbb{Z}$ para cierto $k \in \mathbb{N}$. Entonces se tiene que hay una copia de $\mathbb{Z}/k\mathbb{Z}$ en R, usando el primer teorema de isomorfía (se trata de $f(\mathbb{Z})$). Se define la **característica de** R como $char(R) = k$.

Otro modo análogo de entender la característica de R es como el orden de 1_R considerando R como grupo aditivo, siendo 0 si este orden no es finito.

Proposición 3. *Sea A un anillo y sea $I \subset A$ un ideal. Existe una identificación biyectiva entre el retículo de ideales de A/I y el subretículo de ideales de A que contienen a I. Esta identificación viene dada por π^{-1} (es decir, tomar la preimagen del ideal por π da el ideal asociado), es biyectiva y preserva las inclusiones.*

Demostración. Dado $\overline{J} \in A/I$ ideal, veamos que $J = \pi^{-1}(\overline{J})$ es un ideal de A que contiene al núcleo. Como $0 \in \overline{J}$, está claro que $Nuc(\pi) \subset J$. Para ver que es un ideal, construimos la aplicación $\tilde{\pi} : A/I \to (A/I)/\overline{J}$, y entonces $Nuc(\tilde{\pi} \circ \pi) = \pi^{-1}(\overline{J})$ luego es ideal. Si $\overline{J} \subset \overline{J}'$, se tiene $\pi^{-1}(\overline{J}) \subset \pi^{-1}(\overline{J}')$, preservando además la inclusión estricta si lo fuese, al ser sobreyectivo. Finalmente hay que ver que dado un ideal $J \subset A$ tal que $I \subset J$, existe un ideal de A/I que va a parar a él. Se afirma que tal ideal es J/I. Está claro que $J \subset \pi^{-1}(J/I)$, dado que si $a \in J$, entonces $\pi(a) \in J/I$ por definición de J/I. Para la inclusión opuesta, dado $b \in \pi^{-1}(J/I)$, se tiene que la clase $b + I \in J/I$, es decir, $\exists a \in J$ tal que $b + I = a + I$, de donde $b - a \in I$ luego $b = a + i$, con $i \in I$, $a \in J$, lo que indica que $b \in J$ y hemos acabado. □

1.5. Ideales primos y maximales

Definición 13. Se dice que en un anillo R un ideal $I \subsetneq R$ es **primo** si $ab \in I \implies a \in I$ o bien $b \in I$.

Por ejemplo en $\mathbb{Z}$, el ideal $\langle k \rangle$ es primo si y solo si k es primo o 0. Esto es así porque si $ab = km$ para cierto m, entonces k divide a ab y si k es primo, entonces $k \mid a$ o $k \mid b$ luego a o b están en $\langle k \rangle$. Además $\langle 0 \rangle$ es primo porque $\mathbb{Z}$ es dominio.

Observación 5. Un anillo R es dominio de integridad si y solo si $\langle 0 \rangle$ es primo.

Proposición 4. *Un ideal $I \subset R$ es primo si y solo si R/I es dominio de integridad.*

Demostración. $I \subset R$ es primo equivale a que $ab \in I \implies a \in I$ o $b \in I$, que equivale a que $\overline{ab} = 0 \implies \overline{a} = 0$ o $\overline{b} = 0$ en el cociente, y esto último equivale a que R/I sea dominio. □

Definición 14. Se dice que un ideal $I \subsetneq R$ es **maximal** si cuando $\exists J \subset R$ ideal con $I \subset J$, se tiene que $J = I$ o bien $J = R$.

Como la biyección entre retículos de ideales de R/I y R (en R solo los que contienen a I) preserva las inclusiones, entonces también preserva el concepto de maximalidad. Por ello:

Proposición 5. *Un ideal $I \subset R$ es maximal si y solo si R/I es un cuerpo.*

Demostración. Como hemos apuntado antes, que I sea maximal equivale a que R/I solo tiene 2 ideales dado que $\pi(I)$ en R/I es maximal si y solo si I lo es, y esto equivale a que R/I solo tenga al total y al $\langle 0\rangle$ como ideales o, lo que es lo mismo, que sea un cuerpo. □

Observación 6. Todo ideal maximal es primo.

1.5.1. Ideales primos y maximales en $K[X]$

Vamos a estudiar cómo son los ideales primos y maximales en el dominio de ideales principales $K[X]$, con K cuerpo.

Observación 7. Si $I, J \subset K[X]$ son ideales, $I = \langle p(x)\rangle$, $J = \langle q(x)\rangle$, se tiene que $I \subset J \iff q(x)|p(x)$, dado que esto equivale a que $p(x) = s(x)q(x)$ para cierto $s(x)$.

Definición 15. En un anillo R se dice que un elemento no unidad $a \in R$ es **irreducible** si cada vez que $a = bc$ se tiene que b o c son unidades de R.

Por ejemplo, en $K[X]$ cuerpo, todo polinomio de grado 1 es irreducible, dado que si tal polinomio p se escribiese como $p = qr$, ha de ser que el grado de uno de ellos sea 0 luego ese es unidad.

Asimismo, si $p(x) \in K[x]$ no es irreducible, entonces existen dos polinomios q, s de grado menor tal que $p = qs$.

Definición 16. Se dice que un elemento no unidad $a \in R$ es **primo** si cada vez que $a|bc$ entonces $a|b$ o $a|c$. Equivalentemente, a es primo si $\langle a\rangle$ es primo.

Observación 8. Todo elemento primo es irreducible en un dominio.

Esto es así porque si tal elemento $a \in R$ se escribe como $a = bc$, entonces ha de darse que $a|b$, por ejemplo, luego $b = ak$ para cierto $k \in R$, y entonces $a = (ak)c$, luego $(kc - 1)a = 0$, y al estar en un dominio, $kc = 1$ y c es unidad.

Teorema 3. *Sea $I = \langle p(x)\rangle \subset K[X]$. Entonces I es maximal si y solo si p es irreducible.*

Demostración. Supongamos que I es maximal. Si p no fuese irreducible, entonces hay $q, r \in K[X]$ tales que $p = qr$ y ninguno es unidad. Pero entonces $I \subset \langle q\rangle$ y $\langle q\rangle \subsetneq K[X]$ al no ser q una unidad, luego $I = \langle q\rangle$ al ser maximal. Esto no puede ocurrir porque se tendría que $q = pk$ para cierto $k \in K[X]$, cosa que no puede pasar porque $gr(q) < gr(p)$. Por otro lado, si p es irreducible pero I no es maximal, entonces hay un J tal que $I \subsetneq J \subsetneq K[X]$. Como estamos en un dominio de ideales principales, pongamos $J = \langle q(x)\rangle$ para cierto $q \in K[X]$. Entonces tendríamos que $p = qr$ para cierto $r \in K[X]$. Como q no es unidad, dado que no genera el total, habría de darse que r es unidad, es decir, que $q = pr^{-1}$, pero esto afirmaría que $I = J$, cosa que no pasa. □

Como **corolario**, todo irreducible en $K[X]$ ha de ser primo también, dado que si p es irreducible, $\langle p\rangle$ es maximal y por tanto primo. Es decir, en $K[X]$, los primos y los irreducibles coinciden. (Obsérvese que la única condición que hemos necesitado para esta afirmación es que $K[X]$ sea un dominio de ideales principales).

Teorema 4. *En $K[X]$, todo polinomio de grado mayor o igual que 1 (es decir, no unidad) puede escribirse de manera única como producto de irreducibles, salvo producto por unidades. Los dominios que cumplen esta propiedad se denominan **dominios de factorización única**.*

Demostración. Por inducción en el grado del polinomio. Sea $p \in K[X]$. Si $gr(p) = 1$, sabemos entonces que es irreducible. Ahora, supongamos que el teorema es válido para polinomios de grado inferior a $gr(p) = n > 1$. Si $p(x)$ es irreducible hemos acabado. Si no, por definición, se tienen dos polinomios q, r, de grado menor que n, con $p = qr$. Como, por hipótesis, cada uno puede ponerse como producto de irreducibles, p también. Falta ver que esas expresiones son únicas. Supongamos que $p(x) = q_1 q_2 \dots q_m = s_1 s_2 \dots s_l$,

siendo los $q_i, s_j \in K[X]$ irreducibles. Como q_1 es irreducible, por el corolario previo consecuencia de ser $K[X]$ un dominio de ideales principales, ha de ser que q_1 sea primo, y como divide a $p = s_1 \dots s_l$, entonces $\exists j$ tal que $q_1 | s_j$. Pero, como s_j es irreducible, ha de ser que $q_1 u = s_j$, para cierta unidad $u \in K$. Podemos entonces reordenar para que $j = 1$, y entonces se tendría que $q_1 q_2 \dots q_m = u q_1 s_2 \dots s_l$, y, cancelando, $q_2 \dots q_m = u s_2 \dots s_l$. Repitiendo este argumento de manera iterativa, se concluye que cada q es un s, salvo a lo sumo una unidad (y ha de ser $m = l$ dado que, de otro modo, se llegaría a que $1 = us(x)$, para cierto elemento s no unidad). □

Obsérvese una vez más que solo hemos utilizado de $K[X]$ que es un dominio de ideales principales (para usar que todo irreducible es primo). Es decir, que ser un dominio de ideales principales basta para ser un dominio de factorización única.

2. Extensiones de cuerpos

Definición 17. Sea K un cuerpo. Se dice que otro cuerpo E es una **extensión** de K si $K \subset E$, y las operaciones suma y producto en K son las de E restringidas, es decir, K es un subcuerpo de E. Se denota E/K.

En ocasiones, por abuso del lenguaje, diremos que E es una extensión de K si contiene un subcuerpo isomorfo a K.

Por ejemplo, $\mathbb{C}$ es una extensión de $\mathbb{Q}$. Asimismo, otra extensión de $\mathbb{Q}$ es $\mathbb{Q}[X]/\langle x^3-3\rangle$. Está claro que está contenido, a través de la cadena inyectiva $\mathbb{Q} \to \mathbb{Q}[X] \to \mathbb{Q}[X]/\langle x^3-3\rangle$ (es inyectiva porque $\mathbb{Q}$ es cuerpo). Asimismo, es un cuerpo al ser x^3-3 irreducible en $Q[X]$. La inclusión es estricta puesto que, por ejemplo $\overline{x} \in \mathbb{Q}[X]/\langle x^3-3\rangle$ pero no está en el subcuerpo $\mathbb{Q}$ porque $x-q$ nunca es divisible por x^3-3 si $q \in \mathbb{Q}$. Otra manera de verlo es que $\overline{x}^3 = 3$, pero no hay elemento en $\mathbb{Q}$ que verifique tal cosa.

Las extensiones nos interesan dado que una ecuación polinómica con coeficientes en un cuerpo puede no tener las raíces en ese mismo cuerpo. Así podremos considerar un cuerpo algo más grande que sí las tenga:

Definición 18. Sea E/K una extensión de cuerpos. Se dice que un elemento $\alpha \in E$ es **algebraico sobre** K si $\exists p(x) \in K[X]$, $p(x) \neq 0$, con $p(\alpha) = 0$. En caso contrario, se dice que α es **transcendente**.

Por ejemplo, $i, \sqrt{2} \in \mathbb{C}$ son algebraicos sobre $\mathbb{Q}$. Números transcendentes, por ejemplo, son π o e.

Definición 19. Una extensión E/K es algebraica si todo elemento de E es algebraico en K.

Por ejemplo, $\mathbb{C}/\mathbb{R}$ es algebraica. Esto es porque dado $z \in \mathbb{C}$, el polinomio $(x-z)(x-\overline{z}) \in \mathbb{R}[X]$ lo tiene como raíz. Otro ejemplo menos claro es $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$. A continuación profundizaremos en las extensiones de cuerpos para poder dar una explicación acerca de esta extensión.

Teorema 5 (Del Polinomio Mínimo)**.** *Sea E/K extensión de cuerpos y $\alpha \in E$ un elemento algebraico sobre K.*

1. *Existe un único $p(x) \in K[X]$, mónico y de grado mínimo, tal que $p(\alpha) = 0$.*
2. *Tal polinomio es irreducible sobre K.*
3. *Dado cualquier otro $q(x) \in K[X]$ con $q(\alpha) = 0$, entonces $p(x)|q(x)$.*

Demostración. Sea $\Lambda = \{s \in K[X] : s(\alpha) = 0\}$. Este conjunto es no vacío porque al menos $0 \in \Lambda$, y de hecho es un ideal, dado que si $s_1, s_2 \in \Lambda$, $s_1(\alpha) + s_2(\alpha) = 0 + 0 = 0$, y además $r(x)s_1(x) = r(\alpha)s_1(\alpha) = r(\alpha)0 = 0$. Como es un ideal de $K[X]$, ha de ser principal, y como α es algebraico, es distinto del trivial, es decir, $K[X] = \langle p(x)\rangle$ para cierto $p(x)$ no nulo y de grado mínimo en Λ. Dicho $p(x)$ puede tomarse mónico multiplicando por el inverso de su coeficiente director. Ha de ser único dado que cualquier otro con este grado se obtiene multiplicando a p por un elemento distinto de 0 y 1 en K, luego dejaría de ser mónico. Esto demuestra 1 y 3. Para ver que p es irreducible, si no lo fuese, se tendría $p = st$ con los grados de s y t menores que el de p, pero entonces $0 = p(\alpha) = s(\alpha)t(\alpha)$, y como K es en particular dominio de integridad, alguno de ellos se anula en α, contradiciendo la minimalidad en el grado de p. □

A ese polinomio p lo denominaremos **polinomio mínimo de α sobre K**. Se denota por $p_{\alpha,K}(x)$. Obsérvese que si encontramos un polinomio irreducible y mónico en K que se anula en α, ya es el polinomio mínimo. (Si hubiese otro de menor grado lo dividiría y ya no sería irreducible).

Teorema 6 (Algebraico-Transcendente)**.** *Sea E/K una extensión de cuerpos y $\alpha \in E$. Entonces:*

1. *Si α es transcendente sobre K, se tiene que $K \subset K[\alpha] \subsetneq K(\alpha)$, y además $K[\alpha] \simeq K[X]$.*

2. *Si α es algebraico sobre K, entonces $K \subset K[\alpha] = K(\alpha)$, y además $K[\alpha] \simeq K[X]/\langle p_{\alpha,K}(x)\rangle$.*

Demostración. Consideramos la extensión E/K y $\alpha \in E$. Construimos el homomorfismo $f : K[X] \to K[\alpha] \subset E$, dado por $f(p(x)) = p(\alpha)$. Tal homomorfismo es sobreyectivo, dado que todo elemento de $K[\alpha]$ es de la forma $\sum k_i\alpha^i$, luego el polinomio $\sum k_iX^i$ va a parar a ese elemento. Ahora, si α es transcendente, $Nuc(f) = \{0\}$ y por tanto $K[X] \simeq K[\alpha]$ por el primer teorema de isomorfía. Si α es algebraico, sabemos que $Nuc(f) = \langle p_{\alpha,K}(x)\rangle$, luego del mismo modo se tiene que $K[\alpha] \simeq K[X]/\langle p_{\alpha,K}(x)\rangle$. Para ver que $K[\alpha] \subsetneq K(\alpha)$ en el caso transcendente, basta con observar que $K[X]$ no es un cuerpo, luego $K[\alpha]$ tampoco. En el caso algebraico, como $p_{\alpha,K}(x)$ es irreducible, entonces $K[X]/\langle p_{\alpha,K}(x)\rangle$ es cuerpo, y por tanto coincide con $K(\alpha)$. □

Como corolario, si α es algebraico sobre K en E/K, entonces $K[\alpha]$ es un K-espacio vectorial de dimensión igual a $gr(p_{\alpha,K}(x))$. En primer lugar, como $K \subset K[X]/\langle p_{\alpha,K}(x)\rangle \simeq K[\alpha]$, entonces $K[\alpha]$ es un K-espacio vectorial (es inmediato ver que se cumplen las propiedades de K-espacio vectorial en un cuerpo que contiene a K). Asimismo, sabemos que todo elemento de $K[X]/\langle p_{\alpha,K}(x)\rangle$ puede expresarse de la forma $\overline{\sum_{i=0}^{gr(p_{\alpha,K}(x))} k_ix^i}$, por el algoritmo de la división. Es decir, si $n = gr(p_{\alpha,K}(x))$, el conjunto $\{\overline{1}, \ldots, \overline{x^{n-1}}\}$ genera ese cociente como K-espacio vectorial. Además es claramente una base, dado que para escalares no nulos $\{k_i\}$, tenemos que $\overline{\sum k_ix^i}$ no puede ser nulo, dado que en ese caso el polinomio no nulo $\sum k_ix^i$ sería múltiplo de $p_{\alpha,K}(x)$, que es de grado superior.

Definición 20. Dada la extensión E/K, se define el **grado de la extensión** como la dimensión de E como K-espacio vectorial. Se denota por $[E : K]$

Teorema 7 (Transitividad de grados)**.** *Sean E/K y F/E dos extensiones finitas de cuerpos (es decir, el grado de cada extensión es finito).*
Entonces, se tiene que F/K es finita, y:

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

Demostración. Sea $\{\alpha_1, \ldots, a_n\}$ base en F/E, y $\{\beta_1, \ldots, \beta_m\}$ base de E/K. Basta probar que $\{a_i\beta_j, 1 \leq i \leq n, 1 \leq j \leq m\}$ es base de F/K. Observemos que todo elemento $\gamma = F$ admite la escritura $\gamma = a_1\alpha_1 + \cdots + a_n\alpha_n$, para escalares $\{a_i\} \subset E$ y a su vez, como, cada $a_i \in E$, se tiene $a_i = \sum_k b_{i_k}\beta_k$, luego se tiene que $\gamma = \sum_i \sum_k b_{i_k}\beta_k\alpha_i$, y por tanto ese conjunto genera F con coeficientes en K.

Asimismo, supongamos que existen escalares $\{a_{ij}\} \subset K$, tales que $\sum a_{ij}\alpha_i\beta_j = 0$. Pero entonces, por independencia lineal de los α_i, podemos factorizar: $0 = a_{ij}\alpha_i\beta_j = \sum_i[(\sum_j a_{ij}\beta_j)]\alpha_i$. Como cada uno de esos coeficientes está en E, y los α_i son base de F como E-espacio, ha de darse que cada $\sum_j a_{ij}\beta_j = 0$. Finalmente, por lo tanto, al ser los β_j base, sigue que todos los $a_{ij} = 0$. □

Teorema 8. *Si E/K es finita, es decir $[E : K] < \infty$, entonces E/K es algebraica, es decir, todo $a \in E$ es algebraico en K.*

Demostración. Sea $m = [E : K]$. Tomamos los elementos de E siguientes: $\{1, a, a^2, \ldots, a^m\}$. Como hay $m+1$ de ellos, no pueden ser linealmente independientes sobre K, luego tenemos coeficientes $\{k_i\} \subset K$ no todos nulos con $k_0+k_1a+k_2a^2+\cdots+k_ma^m = 0$, luego a anula al polinomio $p(x) = \sum_{i=0}^m k_ix^i \subset K[X]$. □

Asimismo, si en E hay elementos transcendentes sobre K, se tiene que $[E : K] = \infty$.

Proposición 6. *Si F/E es algebraica, y E/K también, entonces F/K es algebraica.*

Dado $\beta \in F$, sabemos que $\exists p(x) \in E[X]$ no nulo que verifica $p(\beta) = 0$. Pongamos $p(x) = \sum_0^n b_ix^i$, con cada coeficiente $b_i \in E$, y por tanto cada b_i es algebraico sobre K. Sea $L = K(b_0, b_1, \ldots, b_n) \subset E$.

Está claro que β es algebraico en L. Como L/K es ahora una extensión finita, y asimismo $L(\beta)/L$ es finita, tenemos que $L(\beta)/K$ es finita y por tanto todo elemento de $L(\beta)$ es algebraico en K, en particular β. □

Proposición 7. *Sea E/K extensión de cuerpos. Entonces, el conjunto de elementos de E algebraicos sobre K es un cuerpo.*

Demostración. Sea $L \subset E$ el conjunto de elementos algebraicos de E sobre K. Claramente $L \neq \emptyset$ dado que al menos $K \subset L$. Sean $\alpha, \beta \in L$. Véase que $K(\alpha, \beta)$ es algebraica dado que es finita. Por lo tanto todo elemento de $K(\alpha, \beta)$ es algebraico, incluyendo $\alpha + \beta$, $\alpha\beta$, y α^{-1} si α es no nulo. Por lo tanto, como todos esos elementos también son algebraicos, se tiene que L es un cuerpo. □

Definición 21. Dada una extensión E/K, el conjunto de elementos de E algebraicos sobre K se denomina **clausura algebraica** de K en E y se denota $\overline{K}$.

Definición 22. Dada la extensión E/K, se dice que E es **simple** si $E = K(a)$ para cierto elemento $a \in E$.

3. Extensiones de Galois

Definición 23. Sea E/K una extensión de cuerpos. Se dice que $p(x)$ **descompone** en E si puede escribirse como producto de polinomios de grado 1 en $E[X]$. Es decir, que $p(x)$ tiene todas sus raíces en E.

Definición 24. Se dice que E es un **cuerpo de descomposición** de $p(x) \in K[X]$ sobre K si $p(x)$ descompone en E pero no lo hace en ningún subcuerpo propio de E que contenga a K.

Por ejemplo, $x^2 - 7 \in \mathbb{Q}[X]$ tiene como un cuerpo de descomposición al $\mathbb{Q}(\sqrt{7})$. Si lo miramos como un polinomio en $\mathbb{R}[X]$, entonces el propio $\mathbb{R}$ es cuerpo de descomposición. Vemos así que la noción depende del cuerpo sobre el que se considere.

Teorema 9 (Existencia de cuerpos de descomposición)**.** *Sea K un cuerpo y $p(x) \in K[x]$ no nulo. Entonces, existe un cuerpo de descomposición E de p sobre K. Además, $[E : K] \leq n!$, con $n = \deg p$.*

Demostración. Por inducción en $n = \deg p$. Si $n = 1$, entonces $E = K$ sirve y cumple la cota del grado. Ahora, supongamos que el teorema vale para todo polinomio con grado menor que n. Supongamos que $p(x) \in K[x]$ tiene grado n. Si $p(x)$ es reducible en $K[X]$, es decir, $p = qr$ con $\deg q, \deg r < n$. Por hipótesis de inducción en $q(x) \in K[X]$, encontramos un cuerpo de descomposición E_1/K de q sobre K. Por hipótesis, $[E_1 : K] \leq (\deg q)!$. Ahora aplicamos la hipótesis a r sobre E_1, obteniendo E_2/E_1 de descomposición de r sobre E_1, y $[E_2 : E_1] \leq (\deg r)! = (n - \deg q)!$. De esta manera, E_2/K es cuerpo de descomposición de p sobre K, y $[E_2 : K] \leq (\deg q)!(n - \deg q)! \leq n!$.

Si, por otra parte, p es irreducible sobre K, tenemos que $E = K[T]/\langle p(T) \rangle$ es un cuerpo con E/K y donde p tiene una raíz (T). Asimismo, $[E : K] = n$ por ser el grado de p, y podemos poner $(X - T)s(x) = p(x)$ con $s \in E[x]$, y $\deg s = n - 1$. Por la hipótesis de inducción, tenemos un cuerpo L/E de descomposición de s en E, con $[L : E] \leq (n-1)!$, y por tanto L/K es de descomposición de p y $[L : K] \leq n(n-1)! = n!$. □

Observación 9. Dado un polinomio $q(x) \in \mathbb{F}_p[X]$, si tenemos una raíz $r \in E/\mathbb{F}_p$, entonces r^p es asimismo raíz. Esto es porque por el teorema de Fermat, los coeficientes de q se fijan al elevar a la p, y además por tener E característica p, elevar a la p es homomorfismo.

Observación 10. Si $charE = p$, con E un cuerpo, entonces $Fr : E \to E$ el homomorfismo de Frobenius es inyectivo (por ser E cuerpo) y si E es finito, será asimismo sobreyectivo, y por tanto un automorfismo.

A continuación vamos a demostrar que el cuerpo de descomposición es único para un polinomio y un cuerpo dados. Para ello, primero:

Lema 1. *Sean K, K' dos cuerpos y $\varphi : K \to K'$ un isomorfismo. Sea $p(x) \in K[x]$ un polinomio $p(x) = \sum_{j=0}^{n} a_j x^j$ irreducible sobre K. Sea α una raíz de p en alguna extensión E/K. Definimos $\varphi(p(x)) = \sum_{j=0}^{n} \varphi(a_j)x^j \in K'[x]$, y sea β una raíz de $\varphi(p(x))$ en alguna extensión E' de K'.*
En ese caso, φ puede extenderse a un isomorfismo entre $K(\alpha)$ y $K'(\beta)$.

Demostración. Sabemos que $K(\alpha) \simeq K[x]/\langle p(x)\rangle$. Podemos extender φ de manera natural a $\tilde{\varphi} : K[x] \to K'[x]$ actuando sobre los coeficientes, de tal manera que $\varphi(p(x)) := \tilde{\varphi}(p(x))$ es irreducible, y por tanto $K'(\beta) \simeq K'[x]/\langle \varphi(p(x))\rangle$. Consideramos la cadena sobreyectiva $\gamma : K[x] \to K'[x] \to K'[x]/\langle \tilde{\varphi}(p(x))\rangle$, dada por $\gamma = \pi \circ \tilde{\varphi}$. Obsérvese asimismo que $p(x) \in Nuc(\gamma)$, y al ser irreducible, y por ser $K[x]$ de ideales principales, ha de darse que $Nuc(\gamma) = \langle p(x)\rangle$. Aplicando el primer teorema de isomorfía, sigue que $\overline{\gamma}$ dado por $\overline{\gamma}(\overline{q(x)}) = \gamma(q(x))$ es un isomorfismo entre $K(\alpha)$ y $K'(\beta)$. Este isomorfismo, si $k \in K$, verifica que $\overline{\gamma}(\overline{k}) = \gamma(k) = \pi(\varphi(k)) = \overline{\varphi(k)}$ luego en efecto extiende a φ. □

Obsérvese asimismo que este isomorfismo extendido, digamos $\overline{\varphi}$, verifica que $\overline{\varphi}(\alpha) = \beta$, dado que $\alpha \to \overline{x} \to \overline{x} \to \beta$.

Asimismo, si $p(x)$ es irreducible en K y tenemos dos raíces α, β en alguna extensión E/K, el lema garantiza que $K(\alpha) \simeq K(\beta)$.

Teorema 10 (Teorema General de Unicidad de Cuerpos de Descomposición)**.** *Sea $\varphi : K \to K'$ un isomorfismo de cuerpos. Sea $p(x) \in K[x]$. Sea E/K un cuerpo de descomposición de p sobre K. Sea E'/K' un cuerpo de descomposición de $\varphi(p(x))$ sobre K'. Entonces φ puede extenderse a un isomorfismo entre E y E'.*

Demostración. Por inducción en el grado de $p(x)$. Si $gr(p) = 1$, entonces tiene una raíz en K y el único cuerpo de descomposición que hay es K, dado que ya lo es, y toda extensión no trivial lo contiene. Asimismo, $\varphi(p)$ es de grado 1 y, por lo mismo, el único cuerpo de descomposición sobre K' de ese polinomio es el propio K'. Así, la única posibilidad es $E = K$ y $E' = K'$, y el isomorfismo es φ.

Ahora supongamos que el teorema vale para polinomios de grado menor que n. Sea $p(x) \in K[x]$ de grado n. Si no es irreducible, ponemos $p(x) = s(x)r(x)$, ambos con grado menor, y en tal caso el teorema se deduce de la hipótesis de inducción aplicada a s y a r (extendiendo primero al cuerpo de descomposición de s sobre K y luego al de r sobre esa extensión). Si $p(x)$ es irreducible sobre K, y E, E' son los de la hipótesis, y $\alpha \in E$, $\beta \in E'$ raíces de p en E y $\varphi(p)$ en E'. Por el lema previo, sigue que $K(\alpha) \simeq K'(\beta)$ a través de una extensión de φ. Como en $K(\alpha)[x]$ tenemos que $p(x) = (x - \alpha)\tilde{p}(x)$, podemos utilizar la hipótesis de inducción en $K(\alpha)$ y $K'(\beta)$, y el polinomio $\tilde{p}$, y este nuevo isomorfismo. □

En particular, si $K = K'$ y partimos de φ, entonces siempre hay una extensión de E en E que lleva una raíz de α en otra β del polinomio en cuestión. (Haciendo primero la extensión $K(\alpha) \to K(\beta)$), que es la que finalmente se extiende por la hipótesis de inducción.

Teorema 11 (Unicidad de cuerpos de descomposición)**.** *Sean E, E' dos cuerpos de descomposición sobre K del polinomio $p(x) \in K[x]$. Entonces $\exists \sigma : E \to E'$ isomorfismo que fija los elementos de K (también denominado K-isomorfismo).*

Demostración. Sigue del teorema general, poniendo $K = K'$ y φ la identidad. □

3.1. El grupo de Galois de una extensión

Definición 25. Sea F/K una extensión de cuerpos. Se define el siguiente conjunto:

$$Gal(F/K) := \{\varphi : F \to F \text{ automorfismos}, \varphi(r) = r \ \forall r \in K\} \subset Aut(F)$$

Y es inmediato ver que $Gal(F/K)$ con la composición es un grupo. Esto se conoce como el **grupo de Galois de la extensión**.

Sea E/K una extensión donde E es el cuerpo de descomposición de $p(x) \in K[x]$ sobre K. Si $a_1, \ldots, a_r \in E$ son raíces de $p(x)$, es decir, $E = K(a_1, \ldots, a_r)$, y tomamos $\varphi \in Gal(E/K)$, se tiene que $\varphi(p(a_i)) = \varphi(p)(\varphi(a_i)) = p(\varphi(a_i)) = 0$. Luego los elementos de $Gal(E/K)$ mandan raíces de p en otras raíces de p.

Es decir, φ obligatoriamente fija K y permuta las raíces a_i, y el comportamiento ya está definido a través de esto. Podemos interpretar, entonces $Gal(E/K) < S_r$, es decir, es un subgrupo del grupo de permutaciones de r elementos. La identificación se realiza mandando cada automorfismo a la permutación correspondiente que efectúa en las raíces.

Observación 11. Por ejemplo, vamos a calcular $Gal(\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q})$, siendo ξ una raíz cúbica de la unidad distinta de 1. Es decir, estamos considerando el cuerpo de descomposición de $x^3 - 2$, luego el grupo de Galois será subgrupo en S_3.

Si $\varphi : \mathbb{Q}(\sqrt[3]{2}, \xi) \to \mathbb{Q}(\sqrt[3]{2}, \xi)$ es automorfismo, dado que fija $\mathbb{Q}$ por ser el subcuerpo primo, solo tenemos que ver a donde van $\sqrt[3]{2}$ y ξ. No pueden elegirse arbitrariamente, dado que $\varphi^3(\sqrt[3]{2}) - 2 = 0$ y $\varphi^3(\xi) - 1 = 0$, no pudiendo ser $\varphi(\xi) = 1$ porque es inyectiva.

Consideramos primero $id : \mathbb{Q} \to \mathbb{Q}$. Por el lema de extensión aplicado al polinomio $x^2 + x + 1$ que es irreducible por ser el 3-ciclotómico, se tiene que tanto la extensión dada por $\xi \to \xi$ como la dada por $\xi \to \xi^2 = \bar{\xi}$ son isomorfismos entre $\mathbb{Q}(\xi)$ y $\mathbb{Q}(\xi)$.

Podemos volver a aplicar el lema porque $x^3 - 2$ es irreducible en $\mathbb{Q}(\xi)$, por un argumento de comprobación de grados (si no lo fuese, el grado del cuerpo más grande en $\mathbb{Q}$ no sería divisible por 3, pero sí lo es). De esta manera, cualquiera de los isomorfismos encontrados previamente pueden extenderse a $\mathbb{Q}(\xi, \sqrt[3]{2})$ mediante $\sqrt[3]{2} \to \sqrt[3]{2}$, $\sqrt[3]{2} \to \sqrt[3]{2}\xi$ y $\sqrt[3]{2} \to \sqrt[3]{2}\xi^2$.

Esto nos da 6 automorfismos distintos, y además son todos los posibles por las restricciones que hemos puesto al inicio: $\varphi^3(\sqrt[3]{2}) - 2 = 0$ y $\varphi^3(\xi) - 1 = 0$. Es decir, **en este caso**, todas las elecciones sensatas dan lugar a automorfismos.

Por tanto, finalmente, $Gal(\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}) = S_3$.

3.2. Extensiones normales

Definición 26. Sea E/K una extensión algebraica. Se dice que es **normal** si cada vez que $q(x) \in K[x]$ tiene una raíz en E, entonces tiene todas sus raíces en E.

Por ejemplo, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal, porque $x^3 - 2$ no tiene todas sus raíces en $\mathbb{Q}(\sqrt[3]{2})$.

Proposición 8. *Si E/K tiene grado 2, entonces es normal.*

Demostración. Sea $p \in K[x]$ irreducible con una raíz $\alpha \in E$. Escribimos $p(x) = (x - \alpha)r(x)$, con $r(x) \in E[x]$. Veamos que $r(x)$ tiene grado 1 porque $p(x)$ tiene grado 2, dado que $K \subset K(\alpha) \subset E$ y se tiene que $gr(p) = [K(\alpha) : K] \leq [E : K] = 2$. Pero entonces la otra raíz de p es la raíz de r que está en E. □

Teorema 12 (Caracterización de extensiones normales finitas)**.** *Sea E/K finita. Entonces E/K es normal $\iff$ E es cuerpo de descomposición de algún polinomio sobre K.*

Demostración. Para $\implies$, supongamos que E/K es normal. Como además es finita, ponemos $E = K(a_1, \ldots, a_n)$ y consideramos $p(x) = \Pi_1^n p_{a_i,K}(x)$ el producto de cada polinomio mínimo. Como cada uno de ellos es irreducible y tiene una raíz en E por ser normal, entonces tienen todas sus raíces en E y por tanto p también. Asimismo, por construcción, E es el cuerpo más pequeño que contiene a K y a todas las raíces de $p(x)$, luego es el de descomposición.

Para el recíproco, supongamos que E/K es un cuerpo de descomposición de $q \in K[x]$. Sea $p(x) \in K[x]$ irreducible con raíz $\theta \in E$. Vamos a ver que entonces todas las raíces están en E. Sea M el cuerpo de descomposición de $p(x)$ sobre E, y sea $\theta' \in M$ otra raíz de p. Tenemos las inclusiones $K \subset K(\theta) \subset$

$E(\theta) = E \subset M$, pero también $K \subset K(\theta') \subset E(\theta') \subset M$. Se afirma que $[E(\theta') : E] = 1$, y habremos acabado.

Si $r_1, \ldots, r_n \in E$ son las raíces de q, podemos pensar $E = K(r_1, \ldots, r_n)$ al ser su cuerpo de descomposición. Tenemos que $[E(\theta') : K] = [E(\theta') : K(\theta')][K(\theta') : K] = [E(\theta') : E][E : K]$. Veamos que $[E(\theta') : K(\theta')] = [E(\theta) : K(\theta)]$.

Se tiene que $E(\theta')$ es el cuerpo de descomposición de $q(x)$ sobre $K(\theta')$, porque contiene a las raíces de q y a $K(\theta')$ y es el más pequeño. Es decir, por el teorema general de extensión de isomorfismos de cuerpos de descomposición, podemos extender $\varphi : K(\theta') \to K(\theta)$ a un isomorfismo entre $E(\theta')$ y $E(\theta) = E$.

Entonces, $[E(\theta') : K(\theta')][K(\theta') : K] = [E(\theta) : K(\theta)][K(\theta) : K] = [E(\theta) : K] = [E : K]$ y hemos acabado. □

Observación 12. Supongamos que E/K es normal y finita, y se tiene $K \subset L \subset E$. Entonces E/L es normal, pero L/K no tiene por qué. Esto es porque E es cuerpo de descomposición de algún $p \in K[x]$, pero en particular $p \in L[x]$ luego E/L es normal al ser E de descomposición sobre L. No obstante, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$, siendo el más grande el cuerpo de descomposición de $x^3 - 2$, pero $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal, por ejemplo por culpa del $x^3 - 2$.

3.3. Separabilidad

El objetivo es determinar cuándo un polinomio irreducible sobre K tiene raíces múltiples en su cuerpo de descomposición, dado que en ese caso se simplifica mucho el grupo de Galois.

Definición 27. Sea $p(x) \in K[x]$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$. Se define su **derivada formal** como el polinomio $p'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$.

Esta noción cumple las propiedades habituales de suma y producto. Asimismo, si $p'(x) \neq 0$, entonces $\deg p' < \deg p$.

Definición 28. Sea $a \in E$ una raíz de $p(x) \in K[x]$, donde E es una extensión de K. Se dice que a es **raíz múltiple** de p si $p(x) = (x-a)^m \cdot q(x)$ con $m > 1$, $q(x) \in E[x]$ coprimo con $x - a$.

Teorema 13. *Sea $p(x) \in K[x]$. Se tiene que p tiene una raíz múltiple en una extensión E/K $\iff$ $\deg mcd(p, p') \geq 1$ en $K[x]$, es decir, si y solo si p, p' no son coprimos en $K[x]$.*

Demostración. Supongamos que $a \in E$ es raíz múltiple de $p(x)$. Entonces, en ese cuerpo, $p(x) = (x-a)^s q(x)$, con $s > 1$, $q \in E[x]$. Se tiene entonces que $p'(x) = s(x-a)^{s-1} q(x) + (x-a)^s q'(x)$. Supongamos que p y p' son coprimos en $K[x]$. Se sigue entonces que $\exists u, v \in K[x]$ con $pu + p'v = 1$. Evaluando ahora en $a \in E$, se llega a que $0 = 1$, luego ha de ser que p y p' no sean coprimos.

Para el recíproco, si $\deg mcd(p, p') \geq 1$, denotamos $h = mcd(p, p')$. Escribimos $p = hq$, $p' = hs$ para ciertos $q, s \in K[x]$. Consideramos E/K una extensión tal que $a \in E$ es raíz de h. Vamos a comprobar que en ese caso a es raíz múltiple de p. Se tiene que $p(a) = p'(a) = 0$, y que en $E[x]$ se tiene $p(x) = (x-a)\hat{p}(x)$. Por lo tanto, $p'(x) = \hat{p}(x) + (x-a)\hat{p}'(x)$. Se sigue entonces que $\hat{p}(a) + 0 = 0$, evaluando en a. Es decir, $\hat{p}(a) = 0$ luego ha de darse que $(x-a) | \hat{p}(x)$ y por tanto $p(x) = (x-a)^2 \hat{\hat{p}}(x)$ y hemos acabado. □

Observación 13. Si $char(K) = 0$, se tiene que $\deg p' = n - 1$. Esto es así porque si $n = \deg(p)$, entonces el coeficiente de x^{n-1} en p' es $n a_n$, siendo $a_n \neq 0$ el coeficiente de grado n en p, luego, como la característica es 0, sigue que $n a_n \neq 0$.

Proposición 9. *Si $char(K) = 0$, entonces un polinomio irreducible sobre $K[x]$ **no** tiene raíces múltiples en su cuerpo de descomposición.*

Demostración. Por lo observado anteriormente, se tiene que tal polinomio p verifica que $mcd(p, p') = 1$ puesto que $\deg p' < \deg p$, $p' \neq 0$, y p es irreducible. □

Observación 14. Si $char(K) = q > 0$, puede suceder que el grado de p' sea menor que $n-1$, e incluso que $p'(x) = 0$, si y solo si $p(x) = a_0 + a_q x^q + a_{2_q} x^{2q} + \cdots + a_{mq} x^{mq}$. En ese caso, $mcd(p, p') = p$, incluso aunque p sea irreducible, y por tanto no puede afirmarse en este caso que todo irreducible no tiene raíces múltiples en el cuerpo de descomposición. (En los casos en los que $p' \neq 0$, sí puede afirmarse)

Observación 15. Asimismo, si $char(K) = q > 0$, y el polinomio es de la forma $p(x) = b_0^q + b_q^q x^q + \cdots + b_{mq}^q x^{mq}$, es decir, no solo su derivada se anula sino que además todos sus coeficientes son potencias de q. Entonces, por el homomorfismo de Frobenius, sigue que $p(x) = (b_0 + b_q x + \cdots + b_{mq} x^m)^q$, y p no es irreducible.

Definición 29. Se dice que K es **perfecto** si:

- $char(K) = 0$, o bien
- $char(K) = p$ y $Fr : K \to K$, el homomorfismo de Frobenius, es isomorfismo (es decir, todo $a \in K$ tiene un b tal que $b^p = a$).

Por ejemplo, $\mathbb{Q}, \mathbb{R}$ son perfectos dado que su característica es nula, pero también lo son otros como $\mathbb{F}_p$, gracias al pequeño teorema de Fermat.

Observación 16. Por todo lo discutido anteriormente, si K es un cuerpo perfecto y $p(x) \in K[x]$ es irreducible, entonces $p(x)$ no tiene raíces múltiples en su cuerpo de descomposición.

Proposición 10. *Si K es finito, entonces es perfecto.*

Demostración. Si $char(K) = p > 0$, el homomorfismo de Frobenius $Fr : K \to K$ es inyectivo (su núcleo es el 0), luego es un automorfismo. □

Un ejemplo de cuerpo no perfecto es $\mathbb{F}_2(t^2)$.

Definición 30. Sea K un cuerpo.

1. Sea $p(x) \in K[x]$ irreducible. Se dice que p es un **separable** sobre K si todas sus raíces en el cuerpo de descomposición son simples, es decir, no tiene raíces múltiples.
2. Si E/K y $\alpha \in E$ es algebraico, se dice que α es un **elemento separable** sobre K si $p_{\alpha,K}(x)$ lo es.
3. Se dice que una extensión E/K es una **extensión separable** sobre K si todo elemento $\alpha \in E$ es separable sobre K.
4. Se dice que $q(x) \in K[x]$ (no necesariamente irreducible) es un **polinomio separable** sobre K si todos sus factores irreducibles lo son.

En particular, todo polinomio de coeficientes en un cuerpo perfecto es separable y por tanto toda extensión sobre un cuerpo perfecto es separable. Si el cuerpo K no es perfecto, puede haber extensiones separables y no separables. Por ejemplo, si $K = \mathbb{F}_2(t^2)$, la extensión $\mathbb{F}_2(t)$ no es separable pero la extensión $\mathbb{F}_2(t)[x]/\langle x^2 + x + 1 \rangle$ lo es.

Teorema 14. *Sea $p(x) \in K[x]$ irreducible y E/K cuerpo de descomposición. Entonces todas las raíces de $p(x)$ tienen la misma multiplicidad, es decir $p(x) = a \cdot \Pi(x - a_i)^m$ para un $m \geq 1$ y los $a, a_1, \ldots, a_s \in E$.*

Demostración. Si K es perfecto ya sabemos que $m = 1$. En caso contrario, supongamos que $p(x) = a \cdot \Pi(x - a_i)^{m_i}$. Sin perder generalidad, suponemos que $m_1 \geq m_2$. Por el lema de extensión, sabemos que $\exists \gamma \in Gal(E/K)$ con $\gamma(a_1) = a_2$. Como K se fija por γ, sigue que $\gamma(p(x)) = p(x)$, y asimismo $\gamma(p(x)) = a \cdot \Pi(x - \gamma(a_i))^{m_i}$, y ahora aparece a_1 con exponente m_2 y a_2 con exponente m_1, luego $m_2 \geq m_1$ y por tanto vale la igualdad. Para el resto de multiplicidades igual. □

Definición 31. Sea E/K una extensión algebraica. Sea B un cuerpo intermedio, es decir $K \subset B \subset E$. Se dice que otro cuerpo intermedio L es **conjugado** de B si hay un $\gamma \in Gal(E/K)$ con $\gamma(B) = L$.

Esto es una relación de equivalencia.

Teorema 15. *Sea E/K una extensión normal y sea B subcuerpo con $K \subset B \subset E$. Equivalen:*

1. *B no tiene conjugados distintos de B.*
2. *Dado $\gamma \in Gal(E/K)$, se tiene $\gamma|_B \in Gal(B/K)$.*
3. *B/K es normal.*

Demostración. $1 \implies 2$ se tiene porque $\gamma(B) = B$, al no tener B conjugados, y por tanto $\gamma|_B : B \to B$ y es entonces automorfismo (y sigue fijando K).

Para $2 \implies 3$, supongamos que todo $\gamma \in Gal(E/K)$ verifica que $\gamma|_B$ está en $Gal(B/K)$. Sea $p(x) \in K[x]$ irreducible con una raíz $\alpha \in B$. Tenemos que ver que si $\beta \in E$ es raíz de p, entonces está en B. Sabemos por los teoremas de extensión que hay un $\gamma_0 \in Gal(E/K)$ tal que $\gamma_0(\alpha) = \beta$, luego, como $\gamma_0|_B \in Gal(B/K)$, sigue que $\beta \in B$.

Para $3 \implies 1$, supongamos que hay un $\gamma \in Gal(E/K)$ con $\gamma(B) \neq B$. Entonces, hay un $\alpha \in B$ con $\gamma(\alpha) \notin B$. El polinomio $p_{\alpha,K}(x)$ tiene al α y al $\gamma(\alpha)$ como raíces, luego no están todas en B, lo que indica que B/K no es normal. □

Definición 32. Se dice que la extensión E/K es **Galois** si es normal, finita y separable.

3.4. Cuerpos finitos

Sea K un cuerpo con $|K| = m < \infty$. Tomamos $f : \mathbb{Z} \to K$ el único homomorfismo entre esos cuerpos. f no puede ser inyectivo porque K es finito, luego el teorema de isomorfía asegura que $\mathbb{Z}/\ker(f) \simeq f(\mathbb{Z}) \subset K$, es decir, para cierto $p \in \mathbb{N}, \mathbb{Z}/p\mathbb{Z} \subset K$, y además p ha de ser primo porque si no K tendría divisores de cero. Por tanto, K tiene un subcuerpo isomorfo a $\mathbb{Z}/p\mathbb{Z}$, y este es su **subcuerpo primo**, es decir, el cuerpo más pequeño contenido en K (si hubiese otro más pequeño tendría característica divisora de p, luego es p también, luego contiene a este), y $charK = p$.

Asimismo, puede pensarse que K es un espacio vectorial sobre $\mathbb{F}_p$, de dimensión $[K : \mathbb{F}_p] = l$, luego K **tiene** p^l elementos.

Proposición 11. *Sea K un cuerpo con p^n elementos. K es el cuerpo de descomposición de $p(x) = x^{p^n} - x$ sobre $\mathbb{F}_p$.*

Demostración. Como mucho puede tener p^n raíces en K, y además, derivando, se sigue que $p'(x) = p^n x^{p^n-1} - 1 = -1$. Luego $mcd(p, p') = 1$. Por lo tanto, $p(x)$ tiene exactamente p^n raíces simples (distintas) en su cuerpo de descomposición.

Asimismo, $K^* = K \setminus \{0\}$ es un grupo abeliano con $p^n - 1$ elementos. Así, si $\alpha \in K^*$, entonces $\alpha^{p^n-1} = 1$ y por tanto $\alpha^{p^n} = \alpha$, es decir, todos los elementos de K son raíces de $p(x)$ y hemos acabado, porque en K hay justo p^n raíces distintas de $p(x)$ (es decir, descompone y no puede ser menor). □

Como consecuencia inmediata:

Teorema 16. *Todos los cuerpos de p^n elementos son isomorfos.*

Demostración. Todos ellos son cuerpos de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$, y sabemos que ese cuerpo de descomposición es único salvo isomorfismo. □

Así, a tal cuerpo lo denotaremos $\mathbb{F}_{p^n}$. Como corolario, $\mathbb{F}_{p^n}/\mathbb{F}_p$ es normal. De hecho:

Observación 17. Si E/F es una extensión de cuerpos finitos (E y F son finitos), entonces E/F es normal.

Esto es porque se tienen las cadenas $\mathbb{F}_p \subset F \subset E$, luego $|E| = p^l$ y por tanto E es extensión normal de $\mathbb{F}_p$ y entonces también lo es de F porque $x^{p^l} - x$ también está en $F[x]$.

Nos planteamos ahora si $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ para $d < n$, en el sentido de si un cuerpo de p^n elementos puede contener a uno de p^d. Claramente, si $d \nmid n$ no puede cumplirse, puesto que $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{F}_p]$, es decir, que $n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]d$. El recíproco, de hecho, es cierto:

Teorema 17. *Si $|E : \mathbb{F}_p| = n$, es decir, si $E \simeq \mathbb{F}_{p^n}$, entonces para todo $d|n$, se tiene un subcuerpo en E isomorfo a $\mathbb{F}_{p^d}$.*

Demostración. Escribimos $n = ds$ con $s \in \mathbb{N}$. Asimismo, los elementos de E se caracterizan por ser las distintas raíces de $x^{p^n} - x$. Basta entonces probar que si α es raíz de $x^{p^d} - x$, entonces también lo es de $x^{p^n} - x$, pero esto es así porque $x^{p^d} - x | x^{p^n} - x$ (puede comprobarse), luego todo elemento de $\mathbb{F}_{p^d}$ está en E. □

Teorema 18. *Si E es un cuerpo finito con p^n elementos, entonces $(E^*, \cdot)$ es un grupo cíclico.*

Demostración. Por el teorema de clasificación de grupos abelianos finitos, $E^* \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$, donde podemos organizarlo para que cada $d_i | d_{i+1}$. Se afirma que en este caso $t = 1$. Si $t \geq 2$, como $d_1 | d_2$, tomamos un $l > 1$ con $l | d_1$ y $l | d_2$. Tomamos $\alpha \in C_{d_1}$ de orden l, y $\beta \in C_{d_2}$ de orden l. Tomamos en E^* el elemento $\hat{\alpha} = (\alpha, 0, 0, \ldots, 0)$ y $\hat{\beta} = (0, \beta, 0, \ldots, 0)$. Claramente $A := \langle \hat{\alpha} \rangle \neq \left\langle \hat{\beta} \right\rangle =: B$, además de que $|A| = |B| = l$, y todo elemento x de A o de B verifica que $x^l - 1 = 0$, de tal manera que ese polinomio tendría más de l raíces, cosa que en un cuerpo no sucede. □

Por lo tanto, **la extensión $E/\mathbb{F}_p$ es simple, es decir $E = \mathbb{F}_p[\theta]$,** donde θ es un generador del E^*.

Proposición 12. *Dado $n \in \mathbb{N}$, $\exists p(x) \in \mathbb{F}_p[X]$ de grado n, irreducible.*

Demostración. Por lo visto anteriormente, se tiene que $\mathbb{F}_{p^n} \simeq \mathbb{F}_p(\theta)$, luego $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X] / \langle p_{\theta, \mathbb{F}_p}(x) \rangle$, luego entonces dicho polinomio $p_{\theta, \mathbb{F}_p}(x)$ tiene grado n y es irreducible. □

Teorema 19 (Del elemento primitivo)**.** *Si E/K es una extensión finita y separable, entonces es simple, es decir, $E = K(\alpha)$.*

4. El Teorema Fundamental

El objetivo es ver que si E/K es una extensión Galois, el retículo de subgrupos de $Gal(E/K)$ está en correspondencia biyectiva con el retículo de cuerpos intermedios de la extensión. Para ello, primero:

Teorema 20. *Sea $\varphi : K \to \tilde{K}$ un isomorfismo, y $\hat{\varphi} : K[x] \to \tilde{K}[x]$ la extensión natural a los anillos de polinomios. Sea E/K el cuerpo de descomposición de $p(x)$ sobre K y sea $\tilde{E}$ el cuerpo de descomposición de $\hat{\varphi}(p(x))$ sobre $\tilde{K}$. Entonces:*

1. *φ se extiende a un isomorfismo entre E y $\tilde{E}$.*
2. *Existen a lo sumo $|E : K|$ tales extensiones distintas.*
3. *Si $p(x)$ es separable sobre K, existen precisamente $|E : K|$ tales extensiones.*
4. *Si φ se puede extender de precisamente $|E : K|$ maneras distintas, entonces $p(x)$ es separable sobre K.*

Demostración. La parte 1 ya se ha demostrado en el teorema 10. Por inducción en el grado de $|E : K|$. Si $|E : K| = 1$, entonces $E = K$ y no hay nada que probar. Supongamos ahora que el punto 2 es válido para $|E : K| < n$, y supongamos que $|E : K| = n$. Ponemos $p(x) = q_1(x) \dots q_s(x)$ los factores irreducibles en $K[x]$, y como el grado de la extensión no es 1, podemos suponer que $\deg q_1 > 1$. Tomamos α una raíz de $q_1(x)$ en E.

Observamos que $\hat{\varphi}(p(x)) = \hat{\varphi}(q_1(x)) \dots \hat{\varphi}(q_s(x))$ siendo estos irreducibles en $\tilde{K}$. Denotamos $\hat{\varphi}(q_i) \equiv \hat{q}_i$. Dado $\beta \in \tilde{E}$ raíz de $\hat{q}_1(x)$, por el lema de extensión, puede extenderse φ a φ_1 entre $K(\alpha)$ y $\tilde{K}(\beta)$, de tal modo que $\varphi_1(\alpha) = \beta$.

Por hipótesis de inducción, puede extenderse φ_1 a $\psi_1 : E \to \tilde{E}$ de como mucho $|E : K(\alpha)| < n$ maneras. Basta ver cuántas elecciones de φ_1 hay, pero hay tantas como raíces de $q_1(x)$, es decir, como mucho $\deg q_1 = |K(\alpha) : K|$. Por tanto a lo sumo hay $|K(\alpha) : K||E : K(\alpha)| = |E : K|$ extensiones. Esas son todas dado que una raíz de q_1 debe ir en una raíz de $\hat{q}_1$ obligatoriamente, o si no no sería un isomorfismo.

La parte 3 se prueba de la misma manera, por inducción con el mismo argumento pero observando que al ser p separable, entonces todas las raíces de q_1 son distintas, de tal manera que hay precisamente $|K(\alpha) : K|$ elecciones para φ_1.

Asimismo, para la parte 4, si hay raíces múltiples, hay estrictamente menos de $|K(\alpha) : K|$ elecciones de raíces de q_1, y por lo tanto no se alcanzan todas las extensiones. □

Por lo tanto:

Observación 18. Si E/K es Galois, como en particular es separable, entonces $|Gal(E/K)| = |E : K|$.

Proposición 13. *Se tiene que $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq C_p$, generado por el automorfismo de Fröbenius.*

Demostración. Sabemos que $Fr \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ y que $|Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$ por el teorema previo. Lo único que hay que ver es que el orden de ese automorfismo es justamente n. Sea $\Theta \in \mathbb{F}_{p^n}^*$ un generador del grupo multiplicativo cíclico. Se tiene entonces que el menor exponente r para el que $\Theta^r = 1$ es $r = p^n - 1$, luego el menor exponente para el que $\Theta^r = \Theta$ es $r = p^n$. Es decir, que Fr^k con $k < n$ **no** es la identidad, puesto que $Fr^k(\Theta) = \Theta^{p^k} \neq \Theta$, de tal modo que se tiene lo que se quería. □

Proposición 14. *Sea L/K una extensión y $\alpha \in L$ algebraico sobre K. Entonces $K(\alpha)$ es separable sobre $K \iff \alpha$ es separable sobre K.*

Demostración. $\implies$ es trivial. Para $\impliedby$, tomamos $\beta \in K(\alpha)$. Tenemos que ver que $p_{\beta,K}(x)$ es separable sobre K. Como $p_{\alpha,K}(x)$ es separable, sea E el cuerpo de descomposición de ese polinomio. Se tiene entonces que $|Gal(E/K)| = |E : K|$ por separabilidad. Como E/K es normal, $p_{\beta,K}(x)$ descompone

en E y en particular E es el cuerpo de descomposición de $p(x) = p_{\beta,K}(x)p_{\alpha,K}(x)$, luego volvemos a fijarnos en el teorema anterior para ver que como $|Gal(E/K)| = |E : K|$, $p(x)$ ha de ser separable, y en particular $p_{\beta,K}(x)$ también. □

Como consecuencia inductiva:

Teorema 21. *Sea E/K una extensión y sean $\alpha_1, \ldots, \alpha_s \in E$ separables. Entonces la extensión $K(\alpha_1, \ldots, \alpha_s)$ es separable.*

4.1. Subcuerpos intermedios y subgrupos del grupo de Galois

Supongamos que tenemos una extensión E/K y un cuerpo intermedio $K \subset B \subset E$. Si consideramos un automorfismo de E que fija B, ha de fijar asimismo K, de tal manera que $Gal(E/B) \leq Gal(E/K)$.

Teorema 22. *Sea E/K una extensión Galois, y B un cuerpo intermedio.*

1. *$Gal(E/B) \leq Gal/(E/K)$*
2. *Si B/K es normal, entonces $Gal(E/B) \trianglelefteq Gal(E/K)$, y se tiene $Gal(B/K) \simeq Gal(E/K)/Gal(E/B)$.*

Demostración. El punto 1 ya se ha comentado al comienzo de la sección. Para el punto 2, supongamos que B/K es normal. Sabemos que en ese caso si $\varphi \in Gal(E/K)$, se tiene que $\varphi|_B \in Gal(B/K)$, de tal manera que $\pi : Gal(E/K) \to Gal(B/K)$ con $\pi(\varphi) = \varphi|_B$ está bien definida y es de hecho un homomorfismo de grupos, puesto que es lo mismo restringir antes de componer que después. Asimismo, es sobreyectiva dado que si tenemos un $f \in Gal(B/K)$, es decir, $f : B \to B$, como E/K es normal (y por tanto E/B), podemos aplicar el teorema general de extensión a cuerpos de descomposición para obtener un $\varphi \in Gal(E/K)$ que extiende a f.

Se tiene del primer teorema de isomorfía entonces que $Gal(B/K) \simeq Gal(E/K)/\ker(\pi)$. Falta para concluir ver que $\ker(\pi) = Gal(E/B)$, pero esto es así porque $\varphi \in \ker(\pi) \iff \varphi|_B = Id \iff \varphi(b) = b \; \forall b \in B \iff \varphi \in Gal(E/B)$. □

Observación 19 (Ejemplo). Consideremos la cadena $\mathbb{F}_p \subset \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ con $d \mid n$. Sabemos que $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq C_n$ y que $Gal(\mathbb{F}_{p^d}/\mathbb{F}_p)$, y además $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) \trianglelefteq Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ al ser una extensión normal. Como la extensión $|\mathbb{F}_{p^n} : \mathbb{F}_{p^d}|$ es separable y de grado $\frac{n}{d}$, ha de ser que $|Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})| = \frac{n}{d}$, y por tanto es $\langle Fr^d \rangle$ si Fr es el Frobenius de $\mathbb{F}_{p^n}$.

Definición 33. Sea E/K una extensión algebraica. Dado un subgrupo $H < Gal(E/K)$, se define el **subcuerpo fijo** $E^H = \{\alpha \in E : \forall \varphi \in H, \varphi(\alpha) = \alpha\}$.

Es inmediato comprobar que E^H es un cuerpo y que $K \subset E^H \subset E$.

Definición 34. Sea E/K una extensión algebraica. Si $K \subset L \subset K$, siendo L un cuerpo intermedio, definimos $Gal(E/K)^L = \{\varphi \in Gal(E/K) : \forall \alpha \in L, \varphi(\alpha) = \alpha\}$.

Se comprueba que $Gal(E/K)^L < Gal(E/K)$.

Observación 20. Si $H < Gal(E/K)$, se tiene que $H \subset Gal(E/K)^{E^H}$. Esto es así porque $Gal(E/K)^{E^H}$ son los elementos de $Gal(E/K)$ que fijan E^H, y los elementos de H lo hacen, al menos.

Observación 21. Si $K \subset L \subset E$, se tiene que $L \subset E^{Gal(E/K)^L}$. Esto es así porque $E^{Gal(E/K)^L}$ son los elementos de E que quedan fijos por $Gal(E/K)^L$, y por definición, L al menos se queda fijo.

Veamos ahora que, sin ninguna condición adicional sobre E/K, estas asociaciones pueden no ser inversas, es decir, las igualdades pueden no darse en las dos observaciones previas. Tomamos $E = \mathbb{Q}(\sqrt[3]{2})$ y $G = Gal(E/\mathbb{Q}) = \{id\}$. Esto nos indica que $E^G = E$, no obstante si nos fijamos en $\mathbb{Q}$, vemos que $\mathbb{Q} \subset E^{Gal(E/\mathbb{Q})^{\mathbb{Q}}} = E$, luego no vale la igualdad. El problema es que hay 2 subcuerpos, E y $\mathbb{Q}$, que se

fijan por esos automorfismos. Este problema ha surgido porque faltaban raíces de X^3-2, luego el grupo de galois no estaba todo lo completo posible.

Puede verse algo similar en $E=\mathbb{F}_3(t)[w]/\langle w^3-t\rangle$, que es normal por ser cuerpo de descomposición, pero no es separable, luego se tiene el problema de que $G=Gal(E/\mathbb{F}_3(t))=\{id\}$ y sucede lo de antes.

Vemos que tanto la falta de separabilidad como la de normalidad son problemáticas, porque no se obtienen todos los automorfismos necesarios para establecer una biyección.

Lema 2 (Dedekind)**.** *Sean K y L dos cuerpos. El conjunto $Hom(K,L)\cup\{0\}$, es decir, los homomorfismos de K en L al que le añadimos la función nula, es un L-espacio vectorial.*

Se tiene que si tomamos una cantidad arbitraria $\gamma_1,\dots,\gamma_n : K\to L$ de homomorfismos distintos no nulos, son linealmente independientes.

Demostración. Por inducción. Si $n=1$ es inmediato. Si suponemos que vale para todo $k<n$, sean $\{\gamma_j\}_1^n$ homomorfismos distintos no nulos, y escalares λ_j con $\sum\lambda_j\gamma_j=0$. Como $\gamma_1\neq\gamma_n$, hay un $k\in K$ donde difieren. Obsérvese que también $\sum\gamma_n(k)\lambda_j\gamma_j=0$. Si evaluamos la primera combinación lineal en xk, para x arbitrario, se obtiene que $0=\sum\lambda_j\gamma_j(xk)=\sum\lambda_j\gamma_j(x)\gamma_j(k)$, y si evaluamos la segunda en x, se obtiene que $\sum\gamma_n(k)\lambda_j\gamma_j(x)=0$.

Restando ambos resultados, y notando que el último se cancela, $0=\sum_{j=1}^{n-1}\lambda_j\gamma_j(x)\cdot[\gamma_n(k)-\gamma_j(k)]$. Como x era arbitrario, sigue que $0=\sum_{j=1}^{n-1}\lambda_j\gamma_j\cdot[\gamma_n(k)-\gamma_j(k)]$. Sigue por hipótesis de inducción que $\lambda_j\cdot[\gamma_n(k)-\gamma_j(k)]=0$ en todo $j\in\{1,\dots,n-1\}$. Como $\gamma_1(k)\neq\gamma_n(k)$, sigue que $\lambda_1=0$, de tal manera que lo que tenemos en realidad es que $\sum_{j=2}^{n}\lambda_j\gamma_j=0$, y por hipótesis de inducción todos los $\lambda_j=0$ y hemos acabado. □

Lema 3 (Artin)**.** *Sea E un cuerpo y $G=\{\gamma_1,\dots,\gamma_n\}\subset Aut(E)$, distintos. Se tiene que $|E:E^G|\geq|G|$.*

Asimismo, si G es un subgrupo de $Aut(E)$, se sigue que $|E:E^G|=|G|$.

Demostración. Comenzamos por la primera parte. Supóngase que $|E:E^G|:=r<|G|=n$. Sea $\{\alpha_1,\dots,\alpha_r\}$ una base de E/E^G. Construimos este sistema:

$$\begin{cases}\gamma_1(\alpha_1)x_1+\cdots+\gamma_n(\alpha_1)x_n=0\\ \gamma_1(\alpha_2)x_1+\cdots+\gamma_n(\alpha_2)x_n=0\\ \vdots\\ \gamma_1(\alpha_r)x_1+\cdots+\gamma_n(\alpha_r)x_n=0\end{cases}$$

Como $r<n$ el sistema admite una solución no trivial, digamos $(a_1,\dots,a_n)$, en E^n. Tomamos $\beta\in E$ arbitrario con $\beta=\sum_1^r b_i\alpha_i$, los $b_i\in E^G$, y consideramos el siguiente sistema, que admite la misma solución $(a_1,\dots,a_n)$:

$$\begin{cases}b_1\gamma_1(\alpha_1)x_1+\cdots+b_1\gamma_n(\alpha_1)x_n=0\\ b_2\gamma_1(\alpha_2)x_1+\cdots+b_2\gamma_n(\alpha_2)x_n=0\\ \vdots\\ b_r\gamma_1(\alpha_r)x_1+\cdots+b_r\gamma_n(\alpha_r)x_n=0\end{cases}$$

Como los $b_i\in E^G$, se sigue que $\gamma_i(b_j)=b_j$, luego podemos reescribirlo como:

$$\begin{cases}\gamma_1(b_1\alpha_1)x_1+\cdots+\gamma_n(b_1\alpha_1)x_n=0\\ \gamma_1(b_2\alpha_2)x_1+\cdots+\gamma_n(b_2\alpha_2)x_n=0\\ \vdots\\ \gamma_1(b_r\alpha_r)x_1+\cdots+\gamma_n(b_r\alpha_r)x_n=0\end{cases}$$

Sumando las ecuaciones, sigue que $\gamma_1(\sum b_j\alpha_j)x_1+\cdots+\gamma_n(\sum b_j\alpha_j)x_n = 0$, es decir, que $\sum_1^n \gamma_j(\beta)x_j = 0$. Ahora podemos evaluar esta expresión en los a_j, que verifican el sistema, para obtener que $\sum_1^n \gamma_j(\beta)a_j = 0$, lo que entra en contradicción con que los γ_j sean independientes según el Lema de Dedekind.

Para la segunda parte, basta con demostrar que $|E : E^G| \leq |G|$. Supongamos que $|E : E^G| > |G| = n$. Entonces, podemos tomar $\{w_1, \ldots, w_{n+1}\} \subset E$ linealmente independientes, y considerar el sistema:

$$\begin{cases} \gamma_1(w_1)x_1 + \cdots + \gamma_1(w_{n+1})x_{n+1} = 0 \\ \vdots \\ \gamma_n(w_1)x_1 + \cdots + \gamma_n(w_{n+1})x_{n+1} = 0 \end{cases}$$

Como $n+1 > n$, el sistema admite una solución no trivial, que suponemos (reordenado si hace falta) de la forma $(a_1, \ldots, a_k, 0, \ldots, 0)$, en la que los a_j son no nulos y k es el menor con esa propiedad (es decir, no hay otra solución con más de $n-k$ coordenadas nulas). Asimismo, podemos suponer $k > 1$, dado que si $k = 1$ se tiene que $\gamma_1(w_1)a_1 = 0$ de donde, como γ_1 es automorfismo y $w_1 \neq 0$, ha de darse que $a_1 = 0$ también. De igual manera, puede ponerse $a_r = 1$ multiplicando en caso contrario la solución por a_r^{-1} para obtener otra. Finalmente, no todos los $a_j \in E^G$, dado que en caso contrario, la fila del sistema que tiene $\gamma_i = Id$ (existe por ser G grupo), verifica que $w_1a_1 + \cdots + w_ra_r = 0$, contradiciendo que los w_j sean linealmente independientes sobre E^G. Sin pérdida de generalidad, ponemos que $a_1 \notin E^G$.

Como $a_1 \notin E^G$, tomamos el γ_k que no lo fija, y reescribimos el sistema evaluado en la solución:

$$\begin{cases} \gamma_1(w_1)a_1 + \cdots + w_r = 0 \\ \vdots \\ \gamma_n(w_1)a_1 + \cdots + w_r = 0 \end{cases} \tag{1}$$

Y le aplicamos γ_k:

$$\begin{cases} \gamma_k(\gamma_1(w_1))\gamma_k(a_1) + \cdots + \gamma_k(\gamma_1(w_r)) = 0 \\ \vdots \\ \gamma_k(\gamma_n(w_1))\gamma_k(a_1) + \cdots + \gamma_k(\gamma_n(w_r)) = 0 \end{cases}$$

Como G es subgrupo, $\gamma_k \circ G = G$, de tal manera que el sistema es solo una reordenación de este:

$$\begin{cases} \gamma_1(w_1)\gamma_k(a_1) + \cdots + \gamma_1(w_r) = 0 \\ \vdots \\ \gamma_n(w_1)\gamma_k(a_1) + \cdots + \gamma_n(w_r) = 0 \end{cases}$$

Restamos este sistema al sistema (1) y obtenemos:

$$\begin{cases} \gamma_1(w_1)(a_1 - \gamma_k(a_1)) + \cdots + \gamma_1(w_{r-1})(a_{r-1} - \gamma_k(a_{r-1})) = 0 \\ \vdots \\ \gamma_n(w_1)(a_1 - \gamma_k(a_1)) + \cdots + \gamma_1(w_{r-1})(a_{r-1} - \gamma_k(a_{r-1})) = 0 \end{cases}$$

De tal modo que el $(a_1 - \gamma_k(a_1), \ldots, a_{r_1} - \gamma_k(a_{r-1}), 0, \ldots, 0)$ es una solución del sistema original, es no trivial porque $\gamma_k(a_1) \neq a_1$, y sin embargo tiene más coordenadas nulas que la original, lo que es una contradicción y hemos acabado. □

Teorema 23. *Sea E/K una extensión finita con grupo de Galois $G = Gal(E/K)$. Equivalen:*

1. $K = E^G$

2. E/K es Galois

3. E es cuerpo de descomposición de un polinomio separable sobre K.

Demostración. Para 1 $\implies$ 2. Supongamos que $K = E^G$. Veamos que si $p(x) \in K[x]$ es irreducible con $\deg p \geq 2$, con una raíz en E, entonces $p(x)$ descompone en raíces distintas en E. Sea $\alpha \in E \setminus K$ la raíz de $p(x)$ que conocemos, fuera de K. Consideramos $\Lambda = \{\gamma(\alpha) : \gamma \in G\}$. Se tiene que $|\Lambda| > 1$, puesto que si siempre obtuviésemos $\gamma(\alpha) = \alpha$, entonces $\alpha \in E^G = K$, lo cual no ocurre. Pongamos que $\Lambda = \{\alpha_1, \ldots, \alpha_s\}$. Se afirma que el polinomio $q(x) = (x - \alpha_1) \ldots (x - \alpha_s)$ está en $K[x]$. Observemos que existen automorfismos γ_j tales que $q(x) = (x - \gamma_1(x)) \ldots (x - \gamma_s(x))$. Si tomamos ahora $\varphi \in G$ y lo aplicamos a $q(x)$, tenemos $\varphi(q(x)) = (x - \varphi(\gamma_1(x))) \ldots (x - \varphi(\gamma_s(x))) = q(x)$. Eso sucede porque $\varphi \circ \gamma_j \in G$, luego $\varphi \circ \gamma_j(\alpha) = \alpha_k$ para cierto k, y no se repiten por ser φ automorfismo. Es decir, que todos los coeficientes de $q(x)$ se fijan por $\varphi \in G$ arbitrario, luego están en $E^G = K$. Como $p(x)$ y $q(x)$ tienen una raíz común, α, ha de ser que $mcd_{K[x]}(p, q) \neq 1$, y como $p(x)$ es irreducible, entonces $p(x)|q(x)$, y como $q(x)$ descompone en E, en raíces distintas, entonces $p(x)$ también, como se quería.

La parte 2 $\implies$ 3 es inmediata por lo que ya hemos visto acerca de extensiones normales finitas.

Para 3 $\implies$ 1, queremos ver que si E/K es el cuerpo de descomposición de un polinomio separable sobre K, entonces $K = E^G$. Sabemos que $K \subset E^G$. Por el teorema de extensión de isomorfismos en el caso separable, sigue que $|E : E^G| \leq |E : K| = |Gal(E/K)|$, pero como G es un grupo, usamos el teorema de Artin y se obtiene que $|E : E^G| = |Gal(E/K)|$, luego todo son igualdades y entonces $|E : K| = |E : E^G|$, de donde $E^G = K$. □

Teorema 24. *Sea E/K una extensión y $G = Gal(E/K)$. Sea R el retículo de subgrupos de G y F el retículo de cuerpos intermedios de E/K. La asociación $f : R \to F$ dada por $f(H) = E^H$ es inyectiva.*

Demostración. Sean H,N subgrupos de G distintos. Supongamos que $E^H = E^N$. Sea $\gamma \in N \setminus H$. Como E^H y E^N son iguales, entonces E^H se fija por γ, y podemos entonces poner que $E^H \subset E^{H \cup \{\gamma\}}$, y por el teorema de Artin, $|H| = |E : E^H| \geq |E : E^{H \cup \{\gamma\}}| \geq |H| + 1$, lo que es una contradicción. Se repite ahora lo mismo si hay algún $\gamma \in H \setminus N$ para concluir que son iguales. □

Teorema 25. *Sea E/K una extensión Galois, B un cuerpo intermedio $K \subset B \subset E$ y $\varphi \in Gal(E/K)$. Se tiene que $Gal(E/\varphi(B)) = \varphi \cdot Gal(E/B) \cdot \varphi^{-1}$.*

Demostración. Sea $H = Gal(E/B)$. Como E/K es Galois, E/B también y entonces $|H| = |E : B|$, pero se tiene también que $|E : B| = |E : \varphi(B)|$ al ser B y $\varphi(B)$ isomorfos (por φ). Es decir, $|\varphi H \varphi^{-1}| = |H| = |E : B| = |E : \varphi(B)|$. Vamos a ver que todos los elementos de $\varphi H \varphi^{-1}$ fijan $\varphi(B)$, es decir, que $\varphi(B) \subset E^{\varphi H \varphi^{-1}}$ para concluir que $\varphi H \varphi^{-1} \subset Gal(E/\varphi(B))$. Sea entonces $\beta = \varphi(\alpha) \in \varphi(B)$ y $h \in Gal(E/B)$. Se tiene que $\varphi \circ h \circ \varphi^{-1}(\beta) = \varphi \circ h(\alpha) = \varphi(\alpha) = \beta$, y se tiene la inclusión. Entonces sabemos que $|H| = |\varphi H \varphi^{-1}| = |E : E^{\varphi H \varphi^{-1}}| \leq |E : \varphi(B)| = |H|$, luego ha de ser que $E^{\varphi H \varphi^{-1}} = \varphi(B)$. □

4.2. El Teorema Fundamental

Con todo esto, podemos finalmente enunciar el teorema principal:

Teorema 26 (Teorema Fundamental de la Teoría de Galois)**.** *Sea E/K una extensión Galois de grado n y sea $G = Gal(E/K)$. Entonces:*

1. *$|Gal(E/K)| = n$.*
2. *Las funciones f y g dadas por $f(H) = E^H$ para todo $H < Gal(E/K)$, y $g(L) = Gal(E/L)$ para todo $L \subset E$ cuerpo, son inversas entre sí, y dan lugar a una correspondencia biyectiva entre los subgrupos de $Gal(E/K)$ y los subcuerpos intermedios de E/K.*

3. *Esa correspondencia revierte las inclusiones, es decir, si* $H < G < Gal(E/K)$*, entonces* $E^G \subset E^H$*, y si* $K \subset L \subset M \subset E$*, entonces* $Gal(E/M) \subset Gal(E/L)$*.*

4. *Si* L *es un cuerpo intermedio, entonces* $|E : L| = |Gal(E/L)|$ *y* $|L : K| = \frac{|G|}{|Gal(E/L)|}$*.*

5. *Si* L *es un cuerpo intermedio, se sigue que* L *es normal (sobre* K*)* $\iff$ $Gal(E/L) \trianglelefteq Gal(E/K)$*.*

6. *Si* B/K *es normal,* $Gal(B/K) \simeq Gal(E/K)/Gal(E/B)$*.*

Demostración. El punto 1 ya se ha demostrado anteriormente. Para 2, sea $H < Gal(E/K)$. Se tiene que $g(f(H)) = Gal(E/E^H)$. Es evidente que $H \subset Gal(E/E^H)$, puesto que $Gal(E/E^H)$ son los automorfismos de E que fijan el subcuerpo fijo por H, es decir, por lo menos H. Para ver que vale la igualdad, observamos primero que E/E^H es Galois al tenerse la cadena $K \subset E^K \subset E$, y entonces $|E : E^H| = |Gal(E/E^H)| \geq |H|$, pero por el Teorema de Artin, $|E : E^H| = |H|$, luego todo son igualdades y se sigue que $|Gal(E/E^H)| = |H|$ y por tanto los grupos coinciden. Dado ahora un subcuerpo intermedio L, se tiene que $f(g(L)) = E^{Gal(E/L)}$. De nuevo, $L \subset E^{Gal(E/L)}$, dado que todos los elementos de L, por lo menos, se fijan a través de $Gal(E/L)$. Como E/L es Galois, se tiene que $|Gal(E/L)| = |E : L| \geq |E : E^{Gal(E/L)}| = |Gal(E/L)|$, donde la última igualdad sigue del teorema de Artin, y entonces todo son igualdades y por lo tanto $|E : L| = |E : E^{Gal(E/L)}|$ y entonces $L = E^{Gal(E/L)}$.

El punto 3 es inmediato por construcción. El punto 4 sigue de que E/L es Galois, aplicando el punto 1. Para la segunda expresión, se usa la transitividad de los grados. Para el punto 5, ya se vio la implicación $\implies$. Para la opuesta, sean $H = Gal(E/L)$ y $G = Gal(E/K)$, y supongamos que $H \trianglelefteq G$. Dado $\varphi \in Gal(E/K)$, se afirma que $\varphi(L) = L$, lo que demuestra que L/K es normal. Para ver esto, si $\varphi(L) \neq L$, usando el Teorema 25, se sigue que $Gal(E/\varphi(L)) = \varphi Gal(E/L)\varphi^{-1} = Gal(E/L)$ por normalidad de $Gal(E/L)$, contradiciendo el punto 2 (la inyectividad de g). El punto 6 ya se demostró con anterioridad. □

5. Resolución por radicales

En esta sección vamos a ver una de las principales aplicaciones de la teoría de Galois, que es establecer cuándo se pueden obtener ecuaciones generales con radicales en los coeficientes de un polinomio para obtener sus raíces.

Definición 35. Se dice que una extensión finita L/K es **radical** si existe una cadena de cuerpos $K = L_0 \subset L_1 \subset \cdots \subset L_n$ de tal modo que:

1. $L \subset L_n$
2. Para todo $i \in \{1, 2, \ldots, n\}$, se tiene $L_i = L_{i-1}(\alpha_i)$, donde $\alpha_i^{m_i} \in L_{i-1}$, para cierto $m_i \in \mathbb{N}$.

La idea es que si el cuerpo de descomposición de $p(x) \in \mathbb{K}[x]$ sobre K es radical, las raíces pueden expresarse como sumas, restas, multiplicaciones, divisiones y raíces de los elementos de K. El objetivo ahora es ver cuándo se da este caso, mirando al grupo de Galois.

Observación 22. Vamos a comenzar por el ejemplo más sencillo: K de característica 0, y $a \in K$, y consideramos el polinomio $p(x) = x^n - a$.

1. Si en K están las raíces n-ésimas de 1, es decir, n elementos ξ_j con $\xi_j^n - 1 = 0$, y dado un $b \in E$ una raíz de $x^n - a$, entonces se cumple que $E = K(b)$ dado que las n raíces son las de la forma $b\xi_j$. En este caso, se afirma que el grupo de galois $Gal(E/K)$ es abeliano. Dados $\varphi_1, \varphi_2 \in Gal(E/K)$, se tiene $\varphi_1(b) = b\xi_j$, y $\varphi_2(b) = b\xi_i$, donde $\xi_j = \xi^j$ y $\xi_i = \xi^i$ para cierta raíz de la unidad ξ, y entonces es inmediato que $\varphi_1(\varphi_2(b)) = b\xi^{i+j} = \varphi_2(\varphi_1(b))$, dado que los ξ se fijan al estar en K.

2. En caso contrario, si K no tiene raíces n-ésimas primitivas de la unidad, no tiene por qué ser abeliano. Basta con fijarse en $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$, cuyo grupo de Galois era S_3. En este caso tenemos las cadenas:

   $$K \subset K(\xi) \subset K(\xi, b)$$

   Donde $K(\xi)/K$ es Galois al ser el cuerpo de descomposición de $x^n - 1$ y tener K característica 0. Se tiene que $Gal(K(\xi)/K)$ sí es abeliano, al estar en el caso anterior. Por otro lado, $Gal(K(\xi, b)/K(\xi))$ también, puesto que volvemos a estar en el caso anterior.

   Como $K(\xi)/K$ es normal, entonces se tiene la cadena $\{Id\} \trianglelefteq Gal(K(\xi, b)/K(\xi)) \trianglelefteq Gal(K(\xi, b)/K)$, donde además se tiene que el cociente de cada grupo por el previo es abeliano: $Gal(K(\xi, b)/K(\xi))/\{Id\} \simeq Gal(K(\xi, b)/K(\xi))$, que era abeliano, y $Gal(K(\xi, b)/K)/Gal(K(\xi, b)/K(\xi)) \simeq Gal(K(\xi)/K)$, que también lo era.

Definición 36. Sea G un grupo finito. Se dice que G es **soluble** si existe en G una cadena de subgrupos normales:

$$\{id\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$$

tales que H_i/H_{i-1} es abeliano para todos los $i \in \{1, \ldots, s\}$.

Por ejemplo, todos los abelianos son solubles para la cadena trivial. Asimismo, los diédricos D_n son solubles, gracias a la cadena $\{id\} \trianglelefteq \langle r \rangle \trianglelefteq D_n$, siendo r una rotación primitiva, dado que $\langle r \rangle$ es cíclico y por tanto abeliano, y $D_n/\langle r \rangle \simeq C_2$. Un ejemplo de grupo no soluble es A_5, dado que no es abeliano ni tiene subgrupos normales no triviales.

Teorema 27. *Sea K un cuerpo de característica 0 y E el cuerpo de descomposición de $x^n - a \in K[x]$. Entonces $Gal(E/K)$ es soluble.*

Sigue de la observación previa.

Definición 37. Un grupo G es **simple** si no tiene subgrupos normales no triviales.

Por ejemplo, C_p para p primo es simple, y A_5 también. A_4, C_4 o D_3 no lo son.

Definición 38. Sea G un grupo finito. Una cadena de subgrupos:

$$\{Id\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

Es una **cadena de composición** si las inclusiones son estrictas y cada cociente G_{i+1}/G_i es simple.

Es decir, es la cadena más larga posible de subgrupos normales. Por ejemplo, $\{0\} \trianglelefteq C_2 \times C_2$ no es de composición pese a ser subgrupos normales, pero $\{0\} \trianglelefteq \langle(1,0)\rangle \trianglelefteq C_2 \times C_2$ sí. Otra es $\{Id\} \trianglelefteq A_5 \trianglelefteq S_5$.

Con esto, puede enunciarse una nueva definición de grupo soluble, equivalente a la primera:

Definición 39. Sea G un grupo finito. Se dice que G es **soluble** si tiene una cadena de composición:

$$\{Id\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

en la que cada cociente $G_{i+1}/G_i \simeq C_{p_i}$ para algún primo p_i.

Teorema 28. *Sea G un grupo finito.*

1. *Si G es soluble, todo $H \leq G$ es soluble.*
2. *Si $H \trianglelefteq G$, entonces G es soluble $\iff$ H y G/H son solubles.*

Por ejemplo, sabemos ya que A_5 no es soluble, y $A_5 < S_n$ $\forall n \geq 5$, de tal modo que ningún S_n con $n \geq 5$ es soluble.

Teorema 29 (Gran Teorema de Galois, parte I)**.** *Sea K un cuerpo con $charK = 0$. Sea $p(x) \in K[x]$ sea L su cuerpo de descomposición sobre K. Si $p(x)$ es resoluble por radicales (es decir, si L/K es radical), se tiene que $Gal(L/K)$ es soluble.*

Demostración. Escribimos $L = K(r_1, \ldots, r_s)$, siendo r_i las raíces de p, y sabemos que $K \subset K(a_1) \subset K(a_1, a_2) \subset \cdots \subset K(a_1, \ldots, a_n)$ donde $a_i^{m_i} \in K(a_1, \ldots, a_{i-1})$, y se tiene que $L \subset K(a_1, \ldots, a_n)$. Vamos a probar el teorema por inducción en el número de generadores de la extensión sobre el cuerpo.

Si $n = 1$, tenemos que $L \subset K(a_1)$ con $a_1^m \in K$. para cierto m. Sea M el cuerpo de descomposición de $x^m - a_1^m$. Tenemos que $K \subset L \subset K(a_1) \subset M$. Vimos anteriormente que $Gal(M/K)$ es soluble, pero $Gal(L/K) \simeq Gal(M/K)/Gal(M/L)$, luego es soluble al ser cociente de un soluble (propiedad 2 del teorema previo).

Supongamos ahora que el resultado vale para menos de n generadores, y veamos que se cumple para n. Tenemos $K \subset L(r_1, \ldots, r_s) \subset K(a_1, \ldots, a_n)$. Sea M el cuerpo de descomposición de $x^{m_1} - a^{m_1}$ sobre L, y sea E el cuerpo de descomposición de $x^{m_1} - a^{m_1}$ sobre K. Tenemos las cadenas $K \subset E \subset M$ y $E \subset L \subset M$. Se tiene asimismo que $M \subset E(a_2, \ldots, a_n)$, luego por hipótesis de inducción aplicada a $E \subset M$, $Gal(M/E)$ es soluble, y por el caso base aplicado a E y K se tiene que $Gal(E/K)$ es soluble, de tal manera que como $Gal(M/K)/Gal(M/E) \simeq Gal(E/K)$ y tanto $Gal(M/E)$ como $Gal(E/K)$ son solubles, entonces $Gal(M/K)$ es soluble.

Queda finalmente ver que $Gal(L/K)$ es soluble, pero ese es isomorfo a $Gal(M/K)/Gal(M/L)$ donde ambos son solubles, luego hemos acabado. □

Como corolario, si el cuerpo de descomposición E de $p(x) \in K[x]$ verifica que $Gal(E/K)$ no es soluble, no se pueden obtener todas las raíces de $p(x)$ mediante radicales.

Observación 23 (Polinomio cuyas raíces no pueden expresarse por radicales). Consideramos por ejemplo el $3x^5 - 15x + 5 \in \mathbb{Q}[x]$. Se puede analizar que es irreducible en $\mathbb{Q}$ por Eisenstein, y que por Bolzano en $(-2, 1), (0, 1)$ y $(1, 2)$ tiene al menos tres raíces reales, que resultan ser únicas por Rolle. Es decir, tiene 3 raíces reales y 2 raíces complejas no reales, conjugadas. Como $\deg p(x) = 5$, si E es su cuerpo de descomposición, se tiene $Gal(E/\mathbb{Q}) < S_5$. Tenemos que $\mathbb{Q} \subset \mathbb{Q}(x)/\langle p(x)\rangle \subset E$, siendo la primera extensión de grado 5, y por lo tanto $5 \mid |Gal(E/\mathbb{Q})|$, luego, como 5 es primo, ha de haber un elemento $\gamma \in Gal(E/\mathbb{Q})$ de orden 5 (un 5-ciclo). Asimismo, hay un τ que manda la raíz compleja que tiene en su conjugada, dado que si α es esa raíz, $(x-\alpha)(x-\bar{\alpha})$ es irreducible en $\mathbb{R}$ y por tanto en $\mathbb{Q}$. Puede probarse que γ y τ generan todo S_5, de tal manera que $Gal(E/\mathbb{Q}) = S_5$ y por lo tanto no es soluble, luego por el gran teorema $E/\mathbb{Q}$ no es radical.

Teorema 30 (Gran Teorema de Galois, parte II)**.** *Si E/K es Galois y $charK = 0$, entonces E/K es radical si y solo si $Gal(E/K)$ es soluble.*

Observación 24 (Sobre la Realizabilidad). Otra pregunta relevante en la teoría de Galois es qué grupos pueden obtenerse como grupos de Galois de un polinomio. En 1956, Shafarevich prueba que todo grupo soluble es realizable (es decir, es grupo de Galois de un polinomio).

Otro resultado relevante es de Osada, que demuestra que $Gal(x^n - x - 1/\mathbb{Q}) \simeq S_n$ para $n \geq 2$, luego todos los grupos simétricos son realizables.

Observación 25. Hermite demostró que para $n = 5$, la solución general de la ecuación (que no existe con radicales) se puede expresar en términos de las llamadas **funciones modulares**.