Departamento de Álgebra
Facultad de Matemáticas, Universidad de Sevilla

Teoría de Galois en cuerpos de característica positiva

Pedro Gómez de Terreros Oramas

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Prof. Manuel Jesús Soto Prieto

Índice

Resumen

El objetivo de este trabajo de fin de grado es extender la correspondencia de Galois, inicialmente concebida para extensiones de Galois (finitas, separables y normales), a un teorema sobre extensiones normales finitas. Este trabajo consta de 4 secciones. Se definen primero las nociones de característica y de cuerpo de descomposición, dando resultados ya conocidos sobre cuerpos finitos. En la sección 2 estudiaremos el concepto de separabilidad y luego lo aplicaremos a extensiones finitas normales. En la sección 3 demostraremos el teorema y luego se ilustrará su uso con varios ejemplos. Al final de esta sección lo compararemos con otro enfoque del mismo teorema descrito en la refencia [5]. Como adición, en la sección 4 se aplica el teorema a otros resultados que previamente habían sido demostrados únicamente para extensiones separables finitas.

Abstract

The purpose of this paper is to extend the scope of the Galois Correspondence Theorem, initially proved for Galois extentions, to finite normal field extensions. To that end, this work is divided in 4 sections. Firstly, we define the notion of characteristic of a field and other widely known concepts of field theory. Then we procced to section 2, where separability is described and applied to finite normal extensions. In section 3 we will prove the theorem, followed by some examples of its use. Then, it is compared to another version of the theorem, underlined in the reference [5]. In addition, in section 4 we will apply the theorem to some results which had previuosly been proven solely for separable finite extensions.

Introducción

En 1830, Évariste Galois descubrió que las soluciones de un polinomio se pueden expresar mediante raíces de números racionales si y solo si el grupo de permutaciones de las soluciones es soluble. Más adelante, cuando se publicaron sus resultados, se fue construyendo una serie de teoremas y teorías que llegaron ser la Teoría de Galois, que estudia la relación entre extensiones de cuerpos y teoría de grupos. La base fundamental de esta teoría es un teorema que utiliza métodos elementales, el Teorema de Correspondencia de Galois, que asocia los cuerpos intermedios de una extensión de cuerpos con el grupo de automorfismos de la extensión que dejen fijo al cuerpo base, que vienen dados por permutaciones del conjunto de raíces de un polinomio. El resultado se restringe a extensiones finitas con ciertas propiedades que aseguren que las raíces que se están añadiendo son todas distintas y que se encuentran todas en la extensión, las llamadas extensiones de Galois. Los matemáticos modernos han buscado formas de generalizar dicho resultado a todo tipo de extensiones de cuerpos. La solución a este planteamiento existe, y no es única, a lo largo del siglo XX y XXI se han desarrollado teorías para expandir los resultados de Galois más allá del cuerpo de los números racionales. Son variadas y utilizan métodos diferentes, como: topología, álgebras de Lie, análisis y teoría de categorías, por mencionar algunos. Todas tienen en común que se apoyan en objetos matemáticos más avanzados o distintos del álgebra elemental, incluso expandiendo la teoría más allá del estudio de los cuerpos. Un grado mayor de abstracción requiere un mayor nivel de complejidad, y por tanto exigen profundizar bastante para llegar a comprender sus demostraciones.

Este trabajo se centra en desarrollar un Teorema de Correspondencia de Galois sobre extensiones normales finitas, describiendo de forma explícita el cuerpo que se queda fijo por todo automorfismo del grupo de Galois de una extensión, haciendo uso de razonamientos elementales similares al teorema original. Este enfoque no es desconocido, es mencionado una nota en *Algebra* de Serge Lang [8] y se deja como ejercicio en *Algebra from the viewpoint of Galois Theory* de Siegfried Bosch [5], pero ambos no lo llegan a desarrollar, y la mayoría de textos optan por describir la correspondencia solo para extensiones de Galois, o utilizando otro método para demostrarla.

Como las extensiones finitas que no vienen incluidas en el teorema para extensiones de Galois son todas de característica positiva, haremos especial hincapié en estas a lo largo este texto. Por eso, en la primera sección, de conceptos previos, a parte de conceptos generales de teoría de cuerpos se detallan las propiedades de los cuerpos finitos.

Para poder demostrar el teorema, primero definiremos el concepto de separabilidad, primero sobre polinomios y después sobre extensiones, y propiedades y proposiciones sobre ellas. Luego definiremos la inseparabilidad pura de un elemento y vemos como interactúa esta propiedad con extensiones de cuerpos normales finitas y sus grupos de Galois, que nos facilitará estudiar el cuerpo fijo por los elementos de $Gal(K/k)$.

La mayoría de estos resultados provienen de las notas [2], con orden, y redacción modificados para su correcta comprensión. Las demostraciones están basadas en dichas notas, con referencia auxiliar de [1], [4] y [5].

Tras esto, en la sección 3 se formulará y se demostrará el Teorema de Correspondecia, y luego lo compararemos con la correspondencia de *Algebra* de Stephen Shatz y Jean Gallier [5],una instancia de este teorema muy similar, que por su perspectiva única se entrará en detalle.

Finalmente, en la última sección vamos a aplicar la correspondencia generalizada a un par de teoremas que utilizan la Correspondencia de Galois en su demostración, y ampliar su uso a todo tipo de extensiones normales finitas. Notablemente, vamos a expandir el Teorema de Galois sobre solubilidad por radicales, el precursor de toda esta teoría, para que incluya extensiones inseparables. En la literatura no está escrito tal resultado, más que una mención a su existencia como análogo a la versión separable en [8].

Para esto se necesitará utilizar las herramientas norma y traza de una extensión, y por ello se dejan propiedades y teoremas sobre estas, extraídos de la referencia [4], complementariamente en el apéndice como apoyo al lector.

1 Conceptos previos

1.1 Definiciones y propiedades de cuerpos

Definición. Sea un cuerpo K, existe un homomorfismo de anillos

$$\iota : \mathbb{Z} \longrightarrow K$$

$$n \longmapsto n$$

Todos los ideales de $\mathbb{Z}$ son principales, luego se tiene $ker(\iota) = \langle p \rangle$, con p un primo que se denomina ***característica*** del cuerpo K. Si el homomorfismo es inyectivo se dice que K tiene característica 0.

Observación. En un cuerpo de característica positiva p, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Definición. Sea Z un anillo, definimos el ***cuerpo de fracciones*** como el cociente del conjunto

$$Q(Z) = \left\{ \frac{a}{b} \;\middle|\; a, b \in Z, b \neq 0 \right\}.$$

por la relacion de equivalencia $\frac{a}{b} \sim \frac{c}{d}$ *si* $ad - bc = 0$.

Definición. Sean cuerpos $k \subset K$. Dado un polinomio $f(X) \in k[X]$ se dice que el elemento $\alpha \in K$ tal que $f(\alpha) = 0$, denotado cero o raíz del polinomio, es ***simple*** si $f(X) = (X - \alpha)g(X)$, con $g(X) \in K[X]$ coprimo con $(X - \alpha)$. De lo contrario, ocurre $f(X) = (X - \alpha)^k g(X)$ con $(X - \alpha) \nmid g(X)$ y α es una ***raíz múltiple*** de multiplicidad k.

Definición. Sea una extensión K/k. Los elementos $x_i \in K, i = 1, ..., n$ son ***algebraicamente independientes*** sobre k si para todo $f(X_1, ..., X_n) \in k[X_1, ..., X_n]$ se verfica que $f(x_1, ..., x_n) \neq 0$. Si existe algún f tal que $f(x_1, ..., x_n) = 0$, se denominan ***algebraicamente dependientes*** sobre k. Si $n = 1$, dicho elemento se se llama ***trascendente*** o ***algebraico*** respectivamente.

Definición. Se dirá que K es una ***extensión algebraica*** de un cuerpo k si todo elemento de K es algebraico sobre k. Si existe algún elemento transcendente, K/k se denomina ***extensión transcendente***.

Definición. Se denomina ***clausura algebraica*** $\overline{K}$ a la máxima extensión algebraica de un cuerpo K. Si $K = \overline{K}$ se dirá que K es ***algebraicamente cerrado***. Todo polinomio $f(X) \in K[X]$ tiene todas sus raíces en $\overline{K}$.

Definición. Sea K/k una extensión de cuerpos. Se denomina K_0 el conjunto de

elementos algebraicos de K sobre k. K_0 es un cuerpo y es la máxima extensión algebraica de k contenida en K.

Nota 1. Sea una extensión de cuerpos K/k y $\alpha \in K$ algebraico y $f(X) \in k[X]$ tal que $f(\alpha) = 0$. La función

$$\varphi : k[X] \to K$$
$$f(X) \mapsto f(\alpha)$$

induce un isomorfismo a un subanillo L. Cuando $f(X)$ es irreducible, L es un cuerpo, el mínimo cuerpo intermedio de K/k que contiene a α.

$$k[X]/ker(\varphi) \cong L$$

Definición. Sea $x \in K$ algebraico sobre k. Se llama ***polinomio mínimo*** de x sobre k al polinomio mónico irreducible $f(X) \in k[X]$ tal que $(f) = ker(\varphi)$.

Definición. Sea la extensión K/k. Si K es un k-espacio vectorial de dimensión finita, se dirá que K es una ***extensión finita*** de k y se denota $[K : k] = dim_k K$, que se llamará el grado de K sobre k. En caso contrario se dirá que la extensión es infinita.

Lema 1.1. *Si L es un cuerpo intermedio de K/k tales que L es una extensión finita de k y K es una extensión finita de L, K es una extensión finita de k y*

$$[K : k] = [K : L] \cdot [L : k].$$

Si $\{\omega_1, ..., \omega_n\}$ es una base de L/k y $\{\theta_1, ..., \theta_m\}$ es una base de K/L entonces los nm productos $\{\omega_i\theta_j\}$ forman una base de K/k.

Definición. Sean $k \subset K$ dos cuerpos. Se dirá que K es una extensión de k ***finitamente generada*** si existe un número finito de elementos $x_1, ..., x_n \in K$ tal que $K = k(x_1, ...x_n)$. Para $n = 1$, se dice que K/k es una ***extensión simple***, generada por el elemento x_1, llamado ***elemento primitivo*** de la extensión $k \subset K$.

Proposición 1.2. *Sean $k \subset K$ dos cuerpos, las condiciones son equivalentes:*

1. *K es una extensión finita de k.*

2. *K es una extensión algebraica finitamente generada de K.*

Definición. Sean K, K' dos cuerpos, ambos extensiones de un cuerpo k y sea $\varphi : K \longrightarrow K'$ un homomorfismo de cuerpos. Se dirá que φ es un k-homomorfismo de K en K' si para todo $\alpha \in k$, se verifica que $\varphi(\alpha) = \alpha$.

Definición. Sea k un cuerpo y $f_1, ..., f_n$ una familia de polinomios en $k[X]$. Se llama ***cuerpo de descomposición*** de dicha familia sobre k al cuerpo K que verifique las dos condiciones:

- Que todos los f_i se descompongan en factores lineales en $K[X]$, es decir :

$$f(X) = (X - x_1)(X - x_2)...(X - x_n).$$

- K está generada como extensión por $K = k(x_1, x_2, ..., x_n)$, las raíces de los $f_i(X)$.

Proposición 1.3. *Sea k un cuerpo, $f(X) \in k[X]$ un polinomio de grado positivo, K y K' cuerpos de descomposición de $f(X)$ sobre k. Existe un k-isomorfismo θ de K a K' que transforma raíces de $f(X)$ en raíces de $f(X)$.*

Definición. Sea k un cuerpo, K y K' extensiones de k y $x \in K$, $x' \in K'$ elementos algebraicos sobre k. Se dirá que x y x' son ***conjugados*** sobre k si tienen el mismo polinomio mínimo sobre k.

Corolario 1.4. *Sean $x \in K$ y $x' \in K'$ conjugados sobre k. Existe un k-isomorfismo de $k(x)$ a $k(x')$ que transforma x en x'.*

1.2 Estructura de cuerpos finitos

Definición. Un ***cuerpo finito*** K es un cuerpo con un número finito de elementos. Tiene característica positiva p. Sea $|K| = p^e = q$ con $e = dim_{\mathbb{Z}/\mathbb{Z}p}(K)$, se denota K como $\mathbb{F}_q$.

Teorema 1.5. *Teorema de clasificación de cuerpos finitos*

Sea un entero $e > 0$ y un número natural primo p, existe un cuerpo finito K con p^e elementos. Cualesquiera dos cuerpos finitos con el mismo número de elementos son isomorfos.

1.2.1 El endomorfismo de Frobenius

El endomorfismo auxiliar más útil sobre un cuerpo de característica positiva, que indica una serie de propiedades únicas, es el endomorfismo de Frobenius.

Definición. El ***endomorfismo de Frobenius*** es una función sobre un cuerpo K de característica $p > 0$, definida mediante:

$$\phi : K \to K$$

$$\phi(X) = X^p$$

El i-endomorfismo de Frobenius ϕ^i es la composición de ϕ consigo mismo i veces.

$$\phi^i(x) = x^{p^i}.$$

Definición. Sea K un cuerpo de característica p y $q = p^e$, denotamos K^q como el conjunto imagen del e-endomorfismo de Frobenius, $\phi^e(K)$. Igualmente, denotamos por $K^{1/q}$ el conjunto de elementos de $\overline{K}$ que, elevados a q, pertenecen al cuerpo K. Ambos conjuntos tienen estructura de cuerpo.

Definición. Sea K un cuerpo. Se dirá que es ***perfecto*** si es de característica $p = 0$ o si es de característica $p > 0$ y se cumple $K = K^p$.

Corolario 1.6. *El endomorfismo ϕ es un automorfismo si y solo si Kes un cuerpo perfecto.*

Proposición 1.7. *Las siguientes condiciones son equivalentes para un elemento $x \in K$:*

1. $\phi^i(x) = x$
2. *x es raíz de $X^{p^i} - X = 0$*

Proposición 1.8. *Todos los elementos de un cuerpo finito K de cardinal $q = p^e$ son raíces del polinomio $X^q - X$.*

Corolario 1.9. *Sobre un cuerpo finito K, ϕ es un automorfismo y por lo tanto todo cuerpo finito es perfecto.*

1.2.2 Extensiones

Teorema 1.10. *Sea K una extensión finita de $k = \mathbb{F}_p$ con p primo. Entonces $K = \mathbb{F}_{p^e}$, un cuerpo finito de característica p.*

Teorema 1.11. *Sea $K = \mathbb{F}_q$ un cuerpo finito de característica p con $q = p^e$. Sea $K' \subset K$ un subcuerpo de K. Entonces el número de elementos de K' es de la forma $p^{e'}$ donde $e'|e$. El subcuerpo K' es el conjunto de los elementos de K invariantes por el e'-automorfismo de Frobenius. Este es el único subcuerpo de $p^{e'}$ elementos de K.*

Teorema 1.12. *Sean $K' \subset K$ dos cuerpos finitos con $p^{e'}$ y p^e elementos respectivamente, y $e'u = e$. Se tiene que para $a \in K$ las siguientes condiciones son equivalentes:*

1. *K es el mínimo subcuerpo que contiene a a.*

2. *El polinomio mínimo de a es*

$$f(X) = \prod_{i=0}^{u-1} (X - \phi^{e'i}(a))$$

   y es de grado u.

3. *El polinomio mínimo de a genera a K/K' como extensión algebraica.*

4. *Una base de K como K'-espacio vectorial es*

$$\{1, a, a^2, ..., a^{u-1}\}$$

Corolario 1.13. *Siempre existe el elemento a que cumple las condiciones del teorema anterior y es un elemento primitivo de K/K'.*

Corolario 1.14. *Todas las extensiones de cuerpos finitos son cuerpos de descomposición.*

2 Extensiones normales finitas

2.1 Separabilidad

Definición. Sea k un cuerpo y $f(X) \in k[X]$ un polinomio irreducible, se dirá que $f(X)$ es ***separable*** si todas sus raíces son simples. Un polinomio arbitrario se dirá separable si todos sus factores irreducibles son separables. En caso contrario se dirá que f es inseparable.

Ejemplo 1. El polinomio X^2+1 tiene dos ceros distintos sobre $\mathbb{Q}$, i y $-i$. Por tanto, es separable. El mismo polinomio sobre $\mathbb{F}_2$ tiene una única raíz 1, que está repetida $(X+1)^2 = X^2+1$, pero como $X+1 \in \mathbb{F}_2[X]$, este polinomio es reducible y por lo tanto sigue siendo separable sobre $\mathbb{F}_2$.

La motivación al definir la separabilidad es describir la propiedad de que un polinomio se pueda escribir en factores lineales distintos, es decir, se pueda "separar" en factores. Esta es la propiedad de polinomios que va a resultar ser crucial a la hora de estudiar cuerpos de descomposición. Como veremos ahora, la separabilidad está íntimamente conectada a la característica del cuerpo al que pertenezca el polinomio.

2.1.1 Polinomios separables e inseparables

Lema 2.1. *Sean $k \subseteq K$ cuerpos y $\alpha \in K$ una raíz de un polinomio de grado positivo $f(X) \in k[X]$. Entonces α es simple si y solo si $f'(\alpha) \neq 0$.*

Nota 2. La definición de derivada de polinomios que se va a utilizar es la derivación formal, no la derivación analítica.

Sea $f(X) = \sum_{i=0}^{n} a_i X^n$. Se define la función $d(f(X)) = f'(X)$ como

$$f'(X) = a_1 + 2a_2X + ... + nX^{n-1}$$

Dicha función tiene las propiedades habituales de la derivación (regla de la cadena) y es compatible con anillos de polinomios $A[X]$ independientemente de su característica. Es posible definirla de forma analítica, pero para los resultados de este trabajo basta con esta definición. Con esto aclarado procedamos a la demostración del Lema.

Demostración: Suponiendo que α es simple, se tiene que $f(X) = (X-\alpha)g(X)$ con $g(X) \in K[X]$, que cumple $g(\alpha) \neq 0$. Entonces

$$f'(X) = g(X) + (X-\alpha)g(X) \Rightarrow f'(\alpha) = g(\alpha).$$

Como se tiene que $g(\alpha) \neq 0$ esto implica que $f'(\alpha) \neq 0$. Vemos la otra implicación. Supongamos que $f'(\alpha) \neq 0$. Si α no fuese simple, sería $f(X) = (X-\alpha)^2 g(X)$, luego

$$f'(X) = 2(X-\alpha)g(X) + (X-\alpha)^2 g(X), \;\; y$$
$$f(\alpha) = 0 + 0$$

Por lo que $(X-\alpha)^2$ divide $f(X)$ si y solo si $f'(\alpha) = 0$.

□

Proposición 2.2. *Sea $f(X)$ un polinomio irreducible sobre $k[X]$. Las condiciones siguientes son equivalentes:*

1. *$f(X)$ es separable sobre $k[X]$.*

2. *$f'(X) \neq 0$*

Demostración:
Supongamos $f(X)$ inseparable sobre $k[X]$. Es inmediato que por el lema anterior, al ser las raíces de $f(X)$ simples, existen valores para los que $f'(X) \neq 0$.

Ahora supongamos $f'(X) \neq 0$. Sea una raíz arbitraria α de $f(X)$. Entonces, $f(X)$ es un polinomio irreducible, por lo que es el polinomio mínimo que la tiene como raíz. Al ser $f'(X)$ de grado estrictamente menor que $f(X)$ y no nulo, $f'(\alpha) \neq 0$. Consecuentemente toda raíz es simple. □

El resultado anterior facilita una forma de identificar polinomios separables. Es suficiente encontrar un polinomio irreducible en k cuya derivada no sea idénticamente nula.

Ejemplo 2. En $\mathbb{F}_{11}((t))$, un cuerpo k de característica 11 , X^3+3X+2 es irreducible, y por consecuente, como su derivada $3X^2 + 3 \neq 0$, se tiene que es separable.

Cabe reiterar que este criterio no es generalizado, sino solo aplicable a polinomios irreducibles. Que un polinomio tenga derivada idénticamente 0 no implica que sea separable ni viceversa, ya que si el polinomio no es irreducible, para verificar si es separable hay que comprobar si sus factores irreducibles lo son.

Ejemplo 3. En $k = \mathbb{F}_{11}(t)$, el cuerpo de funciones racionales sobre $\mathbb{F}_{11}$, el polinomio $X^{33} + 3X^{11} + 2$ es separable a pesar de tener $f'(X) = 0$. Esto es porque se tiene que $X^{33} + 3X^{11} + 2 = (X^3 + 3X + 2)^{11}$ y hemos visto en el ejemplo anterior que $X^3 + 3X + 2$ es separable.

En el otro sentido,

$$g(X) = X^{13} + X^{12} + tX^{11} + tX^2 + tX + t^2 = (X^{11} + t)(X^2 + X + t)$$

es un polinomio en el que al menos un factor irreducible, $(X^{11}+t)$ es inseparable, al ser $11X^{10}=0$. Por lo tanto, $g(X)$ es inseparable, aunque $g(X)\neq 0$. De hecho, el grado de $g(X)$ ni siquiera es un múltiplo de 11.

Proposición 2.3. *Sea el anillo de polinomios $k[X]$ con k un cuerpo de característica 0. Se verifica que todos los polinomios son separables.*

Demostración: Sea $f(X)\in k[X]$ no constante con coeficicientes a_i $i=0,...,n$. Sin perdida de generalidad supongamos que $f(X)$ es irreducible. Si se prueba que todo $f(X)$ irreducible es separable, cualquier polinomio arbitrario también lo será.

$$f'(x)=0 \quad \forall\, x\in k \;\Leftrightarrow ia_i=0 \quad \forall\, i>0 \;\Leftrightarrow f(X)=c$$

por ser la $car(k)=0$. Entonces $f'(X)\neq 0$ para algún $x\in k$. Por la proposición 2.2 se tiene que $f(X)$ es separable.

□

Un polinomio irreducible no tiene una raíz múltiple a no ser que $f'(X)=0$, y la derivación se comporta de forma "correcta" en característica 0. Esto diferencia de forma inequívoca a los polinomios de característica 0 y los de característica positiva.

Ejemplo 4. El polinomio $X^9+X^6+X^3+2$ en característica 3 tiene derivada idénticamente nula, así que para ver si es separable o no debemos ver qué ocurre para sus factores irreducibles. En cambio, en característica 0 los factores irreducibles del polinomio deben ser separables ya que su derivada no podrá ser idénticamente 0 a no ser que sean una constante.

Proposición 2.4. *Sea $f(X)\in k[X]$ un polinomio con una raíz múltiple α e irreducible sobre k, un cuerpo con característica $p>0$. Entonces existe $e>0$ maximal y $g(X)\in k[X]$ tal que*

1. *$f(X)=g(X^{p^e})$, con $g(X)$ irreducible y separable.*

2. *El polinomio mínimo de α^{p^e} es separable sobre k. Cualquier cero β de f es una raiz p^e-ésima de un cero del polinomio g.*

Demostración:

1. El polinomio $f(X)$ es irreducible. Como α es múltiple, $f'(\alpha)=0$ y el polinomio mínimo debe ser de la forma
$$f(X)=\sum_{i=0}^{k} a_i X^{(ip)}$$
para que la derivada f' sea 0, por la condición de la Proposición 2.2. O sea, f es un polinomio en $k[X^p]$, con $p>0$. Mediante un cambio de variable

$Y_1 = X^p$ reescribimos $f(X) = f_1(X^p) = f_1(Y_1)$, donde $f_1(Y_1) \in k[Y_1]$. Si se verifica $f_1'(Y_1) = 0$, repetimos $f_1(Y_1) = f_2(Y_1^p) = f_2(Y_2)$ y volvemos a ver si la derivada es no nula. Continuamos este proceso hasta que encontremos f_i con derivada no idénticamente nula. Como $gr(f)$ es finito, esta sucesión de pasos debe ser finita. Entonces existe $e \in \mathbb{Z}_+$ tal que $f(X) = g(X^{p^e})$ con $g'(Y) \neq 0$.

Además, $g(Y)$ tiene que ser irreducible porque en caso contrario $f(X)$ tampoco lo sería, ya que entonces se tendría

$$f(X) = g(X^{p^e}) = g(Y) = u(Y)v(Y) = u(X^{p^e})v(X^{p^e})$$

con $u(X^{p^e})$ y $v(X^{p^e})$ polinomios no constantes divisores de $f(X)$. Como $g(X)$ es irreducible sobre k y con derivada no nula, es separable por la Proposición 2.2.

2. Evaluando $f(X)$ en una raíz α resulta $f(\alpha) = g(\alpha^{p^e}) = 0$, luego α^{p^e} es una raíz de $g(X)$, un polinomio separable sobre k. El resto de raíces también verifica esto.

□

Definición. Sean $f(X)$ y $g(X)$ en las condiciones de la proposición anterior, n es el grado de f y n_0 el de g. Se tiene

$$n = n_0 p^e,$$

y n_0, p^e y e se denominan respectivamente ***factor separable*** del grado de $f(X)$ (o grado reducido de $f(X)$), ***factor inseparable*** del grado de $f(X)$ y ***exponente de inseparabilidad*** de $f(X)$.

Corolario 2.5. *Si k es de característica $p > 0$, entonces el polinomio irreducible $f(X) \in k[X]$ es separable si y solo si coinciden su grado y grado reducido.*

Proposición 2.6. *Si k es un cuerpo no perfecto con $car(k) = p > 0$ y $a \in k$ tal que $\sqrt[p]{a} \notin k$ entonces, para todo entero $e \geq 0$, el polinomio*

$$f(X) = X^{p^e} - a$$

es irreducible en $k[X]$. Recíprocamente, si para algún e dicho polinomio es irreducible, entonces $a \notin k^p$.

Demostración:

Sea $g(X) \in k[X]$ un factor irreducible de $f(X) = X^{p^e} - a$. Vamos a ver que $g(X)$ tiene que ser el único factor, y $g(X) = f(X)$. Sea una extensión K/k que contenga a un cero de $g(X)$, es decir, existe $x \in K$ con $g(x) = 0$. Además, se cumple que

$$g(x)l(x) = f(x) = x^{p^e} - a = 0.$$

Supongamos que existe un $h(X) \in k[X]$, coprimo con $g(X)$ y que divide a $f(X)$. Entonces existen $s(X), t(X) \in k[X]$, tal que $s(X)g(X) + t(X)h(X) = 1$ en $k[X]$. Ahora, f se puede descomponer en $K[X]$ de la forma:

$$f(X) = X^{p^e} - a = X^{p^e} - x^{p^e} = (X - x)^{p^e} = g(X)h(X)u(X)$$

Pero como $h(X)$ divide a $f(X)$, se tiene que $(X - x)|h(X)$, luego x es una raíz de $h(X)$, por lo que $1 = s(x)g(x)+t(x)h(x) = 0$, lo cual es una contradicción. Entonces no hay otro factor irreducible distinto de $g(X)$.

$$X^{p^e} - a = (g(X))^{p^{e'}},$$

donde $e' \geq 0$. como $\sqrt[p]{a} \notin k$, debe ser $e' = 0$, con lo que $f(X) = g(X)$ es irreducible.

□

Teorema 2.7. *Sea k un cuerpo. Las siguientes condiciones son equivalentes:*

1. *Todo polinomio irreducible $f(X) \in k[X]$ es separable o, lo que es lo mismo, todo polinomio de grado positivo es separable.*

2. *k es perfecto.*

Demostración:
Que (1) implica (2) es inmediato por la Proposición 2.6, pues si k no fuese perfecto, existirían polinomios irreducibles e inseparables.

Ahora veamos la otra implicación. Sea $f(X) \in k[X]$ un polinomio irreducible e inseparable. Entonces $f(X) \in k[X^p]$ por la Proposición 2.2 y se puede escribir como

$$f(X) = \sum_{i=0}^{n} a_i X^{ip}, \quad n > 0.$$

Como k es perfecto, existen $b_i \in k$ tal que $a_i = b_i^p$; por tanto,

$$f(X) = \sum_{i=0}^{n} b_i^p X^{ip} = \left(\sum_{i=0}^{n} b_i X^i \right)^p$$

lo que quiere decir que $f(X)$ es reducible, lo cual es una contradicción. Entonces $f(X) \notin k[X^p]$ y su derivada no es idénticamente nula a no ser que sea constante, por lo que es separable.

□

Aquí es donde se encuentra la diferencia entre cuerpos finitos y otros cuerpos de característica positiva. Los cuerpos finitos, al ser perfectos, tienen todos sus polinomios irreducibles separables, pues el automorfismo de Frobenius "no falla" en cuerpos perfectos.

Sin embargo, los $X^{p^e} - a$ de la Proposición 2.6 no son los únicos polinomios irreducibles inseparables. El siguiente lema describe como son de los polinomios irreducibles inseparables en función de los polinomios irreducibles separables de un cuerpo.

Lema 2.8. *Sea k un cuerpo no perfecto de característica p y $f(X) \in k[X]$ un polinomio arbitrario de la forma $f(X) = g(X^{p^e})$, con $g(X) \in k[X]$. Se tiene que $f(X)$ es irreducible sobre $k[X]$ si y solo si $g(X)$ es irreducible sobre $k[X]$, con $\sqrt[p]{a_i} \notin k$ para algún $a_i, i = 1...n$ siendo a_i los coeficientes de $g(X)$.*

Demostración: Si $f(X)$ es irreducible $g(X)$ es irreducible, esto es consecuencia directa de la Proposición 2.4. Veamos la otra implicación.

Sea $g(X)$ irreducible verificando la condición del enunciado, probemos que $f(X)$ es irreducible por reducción al absurdo. Supongamos que $f(X)$ fuese reducible. Siempre es posible escribir $f(X)$ de una de estas 2 formas:

1. Hay dos polinomios coprimos no constantes $v(X), u(X) \in k[X]$ tal que $f(X) = v(X)u(X)$.
2. Existe $h(X) \in k[X]$ irreducible tal que $f(X) = (h(X))^r$.

Si ocurre $f(X) = (h(X))^r$, se tiene que

$$f'(X) = r(h(X))^{r-1}h'(X) = 0.$$

Veamos el caso $p|r$. Como $r = 0$, se verifica la igualdad anterior. Sea $r = ps$

$$f(X) = g(X^{p^e}) = (h(X))^r = ((h(X))^s)^p.$$

Aquí, $h(X)^s$ es un polinomio en $k[X]$, que por lo tanto, tiene coeficientes $c_z \in k$, con $z = 0, ..., np^{e-1}$. Se denotan igualmente d_w los coeficientes de $(h(X)^s)^p$, que por estar en un cuerpo de característica p se cumple la igualdad

$$d_{zp} = (c_z)^p \quad \forall \ z = 0, ..., np^{e-1}.$$

Denotamos también b_j los coeficientes de $f(X)$. Ya que $f(X) = g(X^{p^e})$, se tiene que $a_i = b_{ip^e}$ y el resto de los b_j son nulos. Por estar en un cuerpo de característica p y por la igualdad anterior, todos los coeficientes de $h(X)^s$ son

$$d_{ip^e} = (c_{ip^{e-1}})^p = b_{ip^e} = a_i \quad \Rightarrow \quad c_{ip^{e-1}} = \sqrt[p]{a_i} \ \ \forall \ i$$

Pero eso quiere decir que todos los a_i tienen raíz p-ésima que pertenece a k, lo cual contradice la suposición del enunciado. Con que exista un solo a_i tal que $\sqrt[p]{a_i} \notin k$, se llega a una contradicción.

Si $p \nmid r$, se tiene que cumplir $h'(X) = 0$. Entonces, $h(X)$ es constante, y por lo tanto $f(X)$ irreducible, o $h(X)$ también es un polinomio en $k[X^p]$. Por ahora dejemos este caso en este paso, demostraremos la contradicción más adelante.

Ahora veamos el caso $f(X) = v(X)u(X)$ donde $u(X)$ y $v(X)$ son coprimos. El anillo $k[X]$ es un DIP, por lo que se cumple la identidad de Bezout para u y v coprimos. Existen $s(X), t(X) \in k[X]$ tal que

$$v(X)s(X) + u(X)t(X) = 1.$$

También se cumple la ecuación

$$f'(X) = v(X)u'(X) + v'(X)u(X) = 0.$$

Suponiendo que $v'(X) \neq 0$, lo multiplicamos en ambos miembros de la primera ecuación y sustituimos

$$\begin{aligned} 1 \cdot v'(X) &= v(X)s(X)v'(X) + u(X)t(X)v'(X) \\ &= v(X)s(X)v'(X) - v(X)t(X)u'(X) \\ &= v(X)\big(s(X)v'(X) - t(X)u'(X)\big) \end{aligned}$$

Nos queda que $v(X)$ divide a $v'(X)$, lo cual es un absurdo, pues $gr(v') < gr(v)$. Entonces $v'(X) = 0$, y eso implica $u'(X) = 0$ por darse $f'(X) = 0$, es decir, $u(X), v(X) \in k[X^p]$ o alguno de ellos es constante, pero esto último implicaría que $f(X)$ es irreducible.

Falta por demostrar $f(X) = g(X^{p^e}) = v(X)u(X)$ a con $f(X), v(X)$ y $u(X) \in k[X^p]$ y el otro caso no demostrado $f(X) = (h(X))^r$ con $p \nmid r$ y $h(X) \in k[X^p]$. Demostremos ambos casos mediante el caso general $f(X) = h(X)z(X)$, con $h(X), z(X) \in K[X^p]$ no necesariamente coprimos.

La situación ideal sería aquella en la que se tiene $h(X) \in k[X^{p^e}]$. Haciendo un cambio de variable $Y = X^{p^e}$ se tendría que

$$f(X) = g(X^{p^e}) = g(Y) = h(X)z(X) \;\; y \;\; h(X) = h_p(Y) \in K[Y]$$

$$\Rightarrow g(Y)/h_p(Y) = z_p(Y) \in K[Y],$$

y $g(Y)$ no es irreducible, lo cual es una contradicción.

No sabemos si está garantizado que dicha condición se verifique, pues que $h(X)z(X)$ pertenezca a $k[X^{p^e}]$ no implica que $h(X)$ y $z(X)$ también.

Sin embargo podemos aplicar este razonamiento a otro polinomio, $g_1(X)$ tal que $f(X) = g_1(X^p)$. Si g_1 es irreducible, se produciría una contradicción pues estaría dividido por un h_{p1} tal que $h_{p1}(X^p) = h(X)$, cuya existencia está asegurada porque $h(X) \in k[X^p]$.

$$f(X) = g_1(X^p) = h_{p1}(X^p)z_{p1}(X^p)$$

Haciendo un cambio de variable $Y_1 = X^p$

$$g(Y_1) = h_{p1}(Y_1)z_{p1}(Y_1)$$

Pero hemos supuesto que $g_1(Y_1)$ es un polinomio irreducible, así que este caso es absurdo.

Para ver que g_1 es irreducible, realizamos la demostración entera de este lema sobre g_1 tras un cambio de variable $Y_1 = X^p$, cuyo razonamiento es idéntico al caso inicial, ya que $g_1(Y_1)$ satisface que:

- Tiene derivada nula, $g_1(Y_1) = g(Y_1^{p^{e-1}})$.
- Su polinomio reducido $g(X)$ es irreducible y separable.
- Los coeficientes a_i no son potencias p-ésimas de un elemento de k.

Estas son todas las suposiciones del enunciado. Repetimos los razonamientos habiendo supuesto que g_1 es reducible, y acabamos con la misma situación que antes, $g_1(Y_1) = h_1(Y_1)z_1(Y_1)$ con $\quad h_1(Y_1), z_1(Y_1) \in k[Y_1^p]$. Le aplicamos otra vez el mismo razonamiento tomando $g_2(Y_1^p) = g_1(Y_1)$ y suponiendo que g_2 es irreducible. Se verifica que $h_1(Y_1) = h_{p2}(Y_1^p)$, y se toma otra vez un cambio de variable $Y_2 = Y_1^p$ para ver que se produce una contradicción sobre la suposición de irreductibilidad del polinomio g_2, y que por lo tanto g_1 es irreducible. Para demostrar que g_2 es irreducible, hacemos lo mismo que para g_1, y así consecutivamente hasta llegar al paso e, en el que $Y_e = Y_{e-1}^p$ es el cambio de variable. Al deshacer el cambio queda

$$g_e(Y_e) = g_e(Y_{e-1}^p) = g_{e-1}(Y_{e-1}) = \cdots = g_1(X^{p \cdot p^{e-1}}) = g(X^{p^e}) = g(Y_e)$$

Entonces $g_e(X) = g(X)$, el cual no tenemos que probar si es irreducible porque es una suposición del enunciado. Esto genera una cadena de implicaciones en las que como $g_i(X)$ es irreducible, $g_{i-1}(X)$ también es irreducible, hasta acabar en $f(X)$ irreducible.

□

Corolario 2.9. *Sea $f(X) \in k[X^{p^e}]$, si es reducible y su polinomio reducido es irreducible, se tiene que $f(X) = (h(X))^s$*

Este lema es una especie de generalización de la Proposición 2.4. La demostración de irreductibilidad de un polinomio inseparable sigue siendo consecuencia de saber si el polinomio reducido es irreducible o no, que no es fácil de por sí, pero reduce su complejidad, lo cual es importante al ver si un polinomio arbitrario es separable o no.

Ejemplo 5. El polinomio $X^9+X^6+X^3+2$ en $\mathbb{F}_3(t)[X]$ sí es separable, de la misma forma que lo es en $\mathbb{F}_3[X]$,

$$X^9 + X^6 + X^3 + 2 = (X^3 + X^2 + X + 2)^3$$

Por el contrario, el polinomio $X^9 + X^6 + X^3 + t$ no tiene factores irreducibles separables. Es irreducible inseparable, pues $X^3 + X^2 + X + t$ es irreducible, ya que si no por cuestiones grado debería tener un divisor de grado 1 $X - a$, pero no existe ningún $a \in \mathbb{F}_3(t)$ que sea raíz del polinomio.

Las computaciones necesarias determinar la separabilidad de un polinomio arbitrario se pueden refinar incluso más. Si bien no es tan fácil de aplicar como el criterio para polinomios irreducibles, este siguiente criterio puede resultar útil, especialmente si el grado del polinomio no es muy alto.

Lema 2.10. *Sea $f(X) \in K[X]$. Es inseparable si y solo si para el menor natural n tal que $f^{(n)}(X) = 0$ y $f^{(n-1)}(X) = u(X^{p^e})$, se verifica*

$$mcd(f^{(n-1)}(X), f(X)) \neq C$$

con $C \in K$ y $mcd(f^{(n-1)}(X), f(X))$ tiene un factor inseparable.

DEMOSTRACIÓN: Sea $f(X)$ inseparable. Se tiene que $f(X) = h(X)g(X)$, con $g(X)$ un factor separable y $h(X)$ un factor inseparable, de forma que $h(X) = u(X^{p^e})$.

$$f'(X) = h'(X)g(X) + g'(X)h(X) = 0 + g'(X)h(X) = g'(X)h(X),$$

y más generalmente,

$$f^{(i)}(X) = h(X)g^{(i)}(X)$$

Como el grado de las sucesivas derivadas va disminuyendo, en algún momento se tiene que $g^{(n)}(X) = 0$. Entonces $h(X)|f^{(i)}$ y si $h(X) = C$ entonces $f(X)$ es separable. □

Nota 3. En las condiciones del lema anterior, se tienen varios casos sobre la forma de $mcd(f^{(n-1)}(X), f(X))$. Al encontrarnos en característica p, se tienen varias opciones:

- $g^{(n-1)}(X)$ es constante, en cuyo caso $f^{(n-1)}(X)$ divide a $f(X)$ y es exactamente la parte inseparable.

- $g^{(n-1)}(X) \in K[X^p]$. En este caso este polinomio tiene dos factores distintos, $g(X) = u(X)z(X)$:

  - La potencia p^e-ésima $u(X) = (v(X))^{p^e}$ de un polinomio separable $v(X) \in K[X]$. Es separable al ser reducible en $K[X]$ con factores irreducibles separables, pero su derivada es nula, por lo que se queda $g'(X) = u(X)z'(X)$. El factor separable $u(X)$ con derivada nula también divide a $f(X)$ y se va a encontrar en el $mcd(f^{(n-1)}(X), f(X))$, pues $g^{(n-1)}(X) = u(X)z^{(n-1)}(X)$.

  -En característica positiva, los polinomios solo se pueden derivar hasta p veces antes de tener derivada nula. Los únicos elementos en común de $z^{(n-1)}(X)$ y $f(X)$ deben ser raíces múltiples por ser $z^{(n-1)}(X) \in K[X^p]$, bien separables o inseparables.

Ejemplo 6. Sobre $\mathbb{F}_3(t_1, t_2)[X]$, sea el polinomio $X^5+t_1t_2X^4+\frac{t_1}{t_1+1}X^3+t_1^5X^2+X+t_2$. Veamos si es inseparable derivando.

$$\begin{aligned} f'(X) &= 2X^4 + t_1t_2X^3 + 2t_1^5X + 1 \\ f''(X) &= 2X^3 + 2t_1^5 \\ f^{(3)}(X) &= 0. \end{aligned}$$

Como $X^3+t_1^5$ no es un divisor de $f(X)$, no hay ningún factor irreducible de $f(X)$ que sea inseparable, luego tiene que ser separable. No hace falta probar si este polinomio es irreducible por este método.

Proposición 2.11. *Sea k un cuerpo de característica $p > 0$, y $f(X) \in k[X]$ un polinomio irreducible de grado n. Sea n_0 el grado reducido de $f(X)$ y e su exponente de inseparabilidad. Entonces, para todo cuerpo de descomposición K de $f(X)$ sobre k se verifican las siguientes propiedades:*

1. *$f(X)$ posee exactamente n_0 raíces distintas en K.*

2. *La multiplicidad de cada una de ella es p^e.*

DEMOSTRACIÓN: Si $f(X)$ es separable, $n = n_0$, $e = 0$, pues todas las raíces son simples.

En caso de que $f(X)$ sea inseparable, k no es perfecto y

$$f(X) = \sum_{i=0}^{n_0} a_i X^{ip}$$

Hacemos el cambio de variable $f(X) = g(X^{p^e}) = g(Y)$. Puesto que $f(X)$ es irreducible, $g(Y)$ también lo es , y como es separable, todas sus raíces en cualquier cuerpo de descomposición son simples. Además, las raíces de $g(X)$ son potencias p-ésimas de las raíces de $f(X)$ por la Proposición 2.4.

Sea L' un cuerpo de descomposición de $g(Y)$ sobre k y sean y_i' las n_0 raíces de $g(Y)$ en L', que son distintas al ser $g(Y)$ separable. Consideramos la extensión L/L', con L el cuerpo de descomposición del polinomio:

$$h(X) = \prod_{i=1}^{n_0} h_i(X) = \prod_{i=1}^{n_0} (X^{p^e} - y_i')$$

Cada $h_i(X)$ tiene una única raíz, múltiple de orden p^e. Por ser L el cuerpo de descomposición de $h(X)$ sobre L' se tiene que $y_i \in L$, y como $(y_i)^{p^e} = y_i'$,

$$h_i(X) = (X - y_i)^{p^e}, \quad i = 1, ..., n_0.$$

En L tenemos que

$$g(Y) = \prod_{i=1}^{n_0} (Y - y_i'),$$

porque $L' \subset L$ y finalmente

$$f(X) = g(X^{p^e}) = \prod_{i=1}^{n_0} (X^{p^e} - y_i') = \prod_{i=1}^{n_0} (X - y_i)^{p^e}.$$

□

2.1.2 Extensiones separables y inseparables

De forma análoga a los polinomios, podemos definir el concepto de extensión separable.

Definición. Sea $\alpha \in K$ un elemento algebraico sobre k, K/k una extensión de cuerpos y $f(X) \in k[X]$ el polinomio mínimo de α; se dice que α es un ***elemento separable*** sobre k si es una raíz simple de dicho polinomio, es decir, f es separable. La extensión K/k es ***separable*** si todos sus elementos son separables sobre k. De lo contrario se denominará ***inseparable***.

Como nos estamos centrando en extensiones finitas, toda extensión separable con la que trabajemos es a su vez finita. Sin embargo, existen extensiones separables infinitas, como $\mathbb{C}/\mathbb{Q}$.

Proposición 2.12. *Sea $\alpha \in K$ inseparable sobre k. Entonces $char(p) > 0$. Los cuerpos con característica 0 solo tienen extensiones separables.*

Demostración: Por la Proposición 2.3, se tiene que todo polinomio es separable sobre un cuerpo k con $car(k) = 0$. Entonces, en cualquier extensión finita K/k, en la que ambos cuerpos tienen que tener característica 0; el polinomio mínimo $f(X) \in k[X]$ de $\alpha \in K$ es separable y por lo tanto α es simple.

□

Esto prueba que la inseparabilidad es una propiedad única de los cuerpos de característica positiva.

Proposición 2.13. *Toda extensión finita de un cuerpo perfecto k es separable.*

Demostración: Consecuencia directa de 2.7, pues todo polinomio $f(X)$ es separable. Por lo tanto toda extensión algebraica es separable.

□

Corolario 2.14. *Toda extensión finita de un cuerpo finito es separable.*

Como se mencionó antes, el endomorfismo de Frobenius es un automorfismo sobre $\mathbb{F}_{p^e}$, tenemos que todo $x^p = x$ y por lo tanto toda extensión finita es separable.

Proposición 2.15. *Sean $k \subset L \subset K$ cuerpos, donde K es una extensión separable de k; entonces K es separable sobre L.*

Demostración: Sea $x \in K$ y $f(X)$ su polinomio mínimo sobre k; $g(X)$ el polinomio

mínimo de x sobre L. En $L[X]$ se puede escribir

$$f(X) = h(X)g(X), \;\; h(X) \in L[X]$$

Si x fuese inseparable sobre L, se tiene que

$$g'(X) = 0 \Rightarrow f'(X) = h'(X)g(X) + h(X)g'(X) = h'(X)g(X)$$

por lo que $f'(x) = h'(x)g(x) = h'(x) \cdot 0 = 0$, que contradice que x sea separable sobre k por el Lema 2.1. Entonces $g'(X) \neq 0$ y x es separable sobre L. Como x es arbitrario, K/L es una extensión separable.

□

Corolario 2.16. *Sea una extensión algebraica inseparable K/k con característica p y $\alpha \in K$ un elemento inseparable de la extensión. Su polinomio mínimo $f(X) \in k[X^{p^e}]$ verifica $f(X) = g(X^{p^e})$ para un $e > 0$ maximal con $g(X) \in k[X]$ separable y además α^{p^e} es un elemento separable de la extensión y un cero de $g(X)$.*

Consecuencia directa de la Proposición 2.4.

2.1.3 Elementos puramente inseparables

El dato crucial para distinguir qué elementos de una extensión normal finita van a ser separables es el concepto siguiente:

Definición. Sean $k \subset K$ cuerpos, el elemento $\alpha \in K$ es ***puramente inseparable*** sobre k si existe algún $e \geq 0$ tal que $\alpha^{p^e} \in k$, es decir el polinomio mínimo es de la forma $f(X) = X^{p^e} - a$, para algún $a \in k$.

Nota 4. El elemento $\alpha \in K$ pertenece a k si y solo si α es simultáneamente separable y puramente inseparable sobre k. Esto es porque cumple a la vez que $\alpha^{p^e} \in k$ y que su polinomio mínimo $f(X)$ tiene a α como raíz simple, es decir $f(X) = X - \alpha$.

Definición. Sea $k \subset K$ una extensión de cuerpos. Se dice que K es una ***extensión puramente inseparable*** de k si todos los elementos de K son puramente inseparables sobre k.

Nota 5. Para k con $car(k) = 0$ los elementos puramente inseparables son simplemente los de k.

Definición. Se denomina $k^{(*)}$ el conjunto $\{x \in K | x^{p^r} \in k$, para algún $r \geq 0\}$.

Propiedades 1. *Sean $k \subset L \subset K$ tres cuerpos de característica $p > 0$. Se verifican*

las siguientes propiedades:

1. *Si K/k es una extensión puramente inseparable, también lo es K/L.*

2. *Si K es puramente inseparable sobre L y L puramente inseparable sobre k, K es puramente inseparable sobre k.*

3. *$k^{(*)}$ es un cuerpo, de hecho es la máxima extensión puramente inseparable de k contenida en K.*

4. *Todo elemento de K puramente inseparable sobre $k^{(*)}$ pertenece a $k^{(*)}$.*

5. *Si $K = k(x_1, ..., x_n)$ es una extensión finitamente generada de k y para todo i x_i es puramente inseparable sobre k, entonces K es una extensión puramente inseparable de k.*

6. *Si el elemento primitivo x de una extensión simple $K = k(x)$ de k es puramente inseparable sobre k y e el menor entero tal que $x^{p^e} \in k$, entonces $[K : k] = p^e$.*

7. *Si K es una extensión puramente inseparable de k, entonces el grado de la extensión es una potencia de p.*

8. *Si un elemento $x \in K$ es a la vez separable y puramente inseparable sobre k, entonces $x \in k$. En particular, si k es perfecto, $k^{(*)} = k$.*

Demostración:

1. Sea $x \in K$, se verifica $x^{p^e} \in k$. Entonces $x^{p^e} \in L$ ya que $k \subset L$.
2. Sea $x \in K$. Por ser puramente inseparable sobre L y porque L/k es puramente inseparable existen $e, e' \geq 0$ naturales tal que $x^{p^e} \in L$ y $(x^{p^e})^{p^{e'}} \in k$ lo que implica que $x^{p^{e+e'}} \in k$ y x es puramente inseparable sobre k.
3. Trivialmente $k^{(*)}$ contiene a todos los elementos de k, que preservan la estructura de cuerpo. Ahora, si tenemos $x, y \in k^{(*)}$, por ser puramente inseparables sobre k, existen e y $e' \in \mathbb{N}$ tales que $x^{p^e}, y^{p^{e'}} \in k$. Entonces se cumple que $x+y \in k^{(*)}$ por

$$(x+y)^{p^{e+e'}} = x^{p^{e+e'}} + y^{p^{e+e'}} = (x^{p^e})^{p^{e'}} + (y^{p^{e'}})^{p^e} \in k$$

Además, existen opuestos, se tiene que $-x \in k^{(*)}$.
La multiplicación también está bien definida, pues $xy \in k^{(*)}$, ya que

$$(xy)^{p^{e+e'}} = (x^{p^e})^{p^{e'}} (y^{p^{e'}})^{p^e} \in k$$

Análogamente a la resta, la división está bien definida y existen inversos multiplicativos, simplemente para cualquier $x \in k^{(*)}$ se tiene que su inverso $1/x$

sobre K pertenece a $k^{(*)}$.

4. Sea un $x \in K$ puramente inseparable sobre $k^{(*)}$. Entonces también es puramente inseparable sobre k, pues $x^{p^e} \in k^{(*)}$ implica que $x^{p^{e+e'}} \in k$, y por lo tanto $x \in k^{(*)}$.

5. Sea $x \in K$. Si $x \in k$, es puramente inseparable sobre k. Si $x \notin k$, se puede expresar mediante una base de K como k-espacio vectorial de elementos puramente inseparables sobre k, por estar K/k finitamente generada por los x_i, elementos puramente inseparables. Esto implica que x también es puramente inseparable sobre k, por lo que todo elemento de K es puramente inseparable sobre k. Entonces K/k es una extensión puramente inseparable. De hecho $K = k^{(*)}$ ya que no existe ningún elemento de K sobre k que no esté en $k^{(*)}$, por definición de $k^{(*)}$ y de K.

6. $K = k(x)$ es una extensión de la forma $k[X]/(f(X))$, con polinomio mínimo f cuyas raíces que tienen multiplicidad p^e. El polinomio es de la forma $X^{p^e} - a$, que es mínimo por la condición de minimalidad de e; por lo que $[K : k] = p^e$.

7. Sea $K = k(x_1, ..., x_r)$, con x_i elementos puramente inseparables sobre k. Por la propiedad anterior, $[k(x_1) : k] = p^{e_1}$ y

$$[k(x_1, ..., x_i) : k(x_1, ..., x_{i-1})] = p^{e_i}, \quad i = 2, ..., r$$

entonces usando que $[K : k] = [K : L][L : k]$:

$$[K : k] = [K : k(x_1, ..., x_{r-1})] \cdots [k(x_1) : k] = p^{e_r} \cdots p^{e_1} = p^{e_r + \cdots + e_1}$$

8. Como vimos antes, elementos a la vez separables y puramente inseparables sobre k pertenecen a k. Si k es perfecto, está demostrado en el Teorema 2.7 que todo polinomio irreducible de grado positivo es separable y que todas sus extensiones son separables, así que $k^{(*)} = k$.

□

Proposición 2.17. *Sea K/k una extensión finita de cuerpos de característica $p > 0$. Las condiciones son equivalentes:*

1. *K es separable sobre k.*

2. *$k(K^p) = K$*

Demostración:
Supongamos que K es separable sobre k. Se tiene que $k(K^p) \subseteq K$. Falta demostrar $K \subseteq k(K^p)$. Sea $x \in K$, entonces $x^p \in K^p \subset k(K^p)$. Como x es puramente inseparable sobre K^p para $e = 1$, entonces también lo es sobre $k(K^p)$, pero como x es separable sobre k por suposición, también lo es sobre cualquier extensión de k, en particular $k(K^p)$. Entonces $x \in k(K^p)$ por la propiedad 8 anterior.

Ahora supongamos que $k(K^p) = K$. Sea $\{x_1, ..., x_n\}$ una base de K como k-espacio vectorial y sea $x \in K$. Como $x \in K^p$, se puede escribir de la forma

$$x = \sum_{i=1}^{r} a_i y_i^p, \;\; a_i \in k, y_i \in K$$

con $y_i \in K$, $y_i^p = x_i$. A su vez, y_i se puede expresar mediante la base x_i, y sustituyendo en la ecuación anterior

$$x = \sum_{i=1}^{r} a_i \sum_{j=1}^{n} (b_{ij} x_j)^p = \sum_{i=1}^{r} \sum_{j=1}^{n} a_i b_{ij}^p x_j^p$$

Esto prueba que los x_j^p son un sistema de generadores de K como espacio vectorial de k, y por tanto forman una base de K/k. En particular, dados elementos $\{z_1, ..., z_m\}$ de K linealmente independientes entonces $\{z_1^{p^e}, ..., z_m^{p^e}\}$ también son linealmente independientes para $e \in \mathbb{N}$.

Supongamos que existe $x \in K$ inseparable sobre k. Sea $f(X)$ su polinomio mínimo, n_0 su grado reducido y p^e su grado inseparable; se tiene que $n_0 < n$. Los elementos $\{1, x, ..., x^{n_0}\}$ son linealmente independientes sobre k, de lo contrario existiría un polinomio separable de grado n_0 con raíz x. Pero, $\{1, x^{p^e}, ..., x^{n_0 p^e}\}$ no son linealmente independientes sobre k pues $f(x)$ da una relación no trivial de dependencia. Se da una contradicción.

El elemento x tiene que ser necesariamente separable, por lo que K/k es una extensión separable.

□

Proposición 2.18. *Sean $k \subset L \subset K$ cuerpos. Si K una extensión algebraica separable de L y L una extensión algebraica separable de k, entonces K es una extensión separable de k.*

Demostración:
Si $p = 0$, resultado es inmediato al ser separables todas las extensiones de cuerpos por la Proposición 2.12.

Para $p > 0$, dadas $k \subset L \subset K$ extensiones de cuerpos, queremos ver que K/k es separable.
Si K/k es una extensión finita, L/k y K/L también son finitas y como $L^p \subset K^p$, se tiene que K/k es separable por la Proposición 2.17 ya que

$$K = L(K^p) = k(L^p)(K^p) = k(K^p).$$

Para extensiones infinitas, basta con observar que dado $x \in K$, su polinomio mínimo $f(X)$ sobre L es separable y tiene coeficientes en L, y dichos coeficientes son separables sobre k. Sea L' la extensión intermedia de L/k que contiene todos los coeficientes de f. $L'(x)/L'$ es separable por tener polinomio mínimo f y L'/k también

lo es por la Proposición 2.15. Ambas son extensiones finitas. Entonces aplicando la demostración para extensiones finitas, x es separable sobre k.

□

Proposición 2.19. *Sean $k \subset K$ dos cuerpos y $x_1, ..., x_n \in K$ separables sobre k. Entonces $k(x_1, ..., x_n)$ es separable sobre k.*

DEMOSTRACIÓN: Toda extensión en característica 0 es separable así que para $p = 0$ es inmediato. Asumimos $p > 0$ y se tiene la cadena de inclusiones:

$$k \subset k(x_1) \subset k(x_1)(x_2) \subset \cdots \subset k(x_1, ..., x_{n-1}) \cdots (x_n) \subseteq K$$

Basta con probar el caso $n = 1$ y luego aplicar sucesivamente la misma demostración a $(k(x_1) \cdots (x_{n-1}))(x_n)$ para todo $n > 1$. En dicho caso

$$k(k(x_1)^p) = k(x_1^p) \subseteq k(x_1)$$

y al ser separable sobre k, x_1 es tanto separable como puramente inseparable sobre $k(x_1)^p$. Asimismo todo $x \in k$ es simultáneamente separable y puramente inseparable sobre $k(x_1)^p$ lo que implica que $k(x_1) \subseteq k(x_1)^p$, luego $k(x_1) = k(x_1)^p$ y $k(x_1)$ es separable por la Proposición 2.17.

□

2.1.4 Clausura separable

Definición. El conjunto de elementos de K separables sobre k se denomina $k_{(*)}$ y es un subcuerpo de K que contiene a k. Es la máxima extensión intermedia separable de K/k . Recibe el nombre de **clausura separable**.

Nota 6. La demostración de que en efecto $k_{(*)}$ es un cuerpo es consecuencia inmediata de que la suma y producto de elementos separables es separable, y los elementos opuestos y inversos están bien definidos. Esto se da ya que si $a, b \in K$ son separables sobre k. La extensión $k(a, b)/k$ es separable por la Proposición 2.19 y $a+b \in k(a, b)$. Análogamente con la multiplicación $ab \in k(a, b)$.

Definición. Sea K/k una extensión de cuerpos, se define $[K : k]_s = [k_{(*)} : k]$ el **factor separable** de K/k.

Definición. Sea K/k una extensión de cuerpos, de define el **factor inseparable** de K/k como $[K : k]_i = [K : k_{(*)}]$.

Nota 7. En característica 0 las definiciones de factor inseparable y separable son redundantes ya que $K = k_{(*)}$ para todo K/k.

Teorema 2.20. *Sean $k \subset K$ dos cuerpos de característica $p > 0$ tales que K es una extensión finita de k. Se verifican las propiedades:*

1. *Existe un cuerpo intermedio $k_{(*)}$ tal que $k_{(*)}$ es separable sobre k y que K es puramente inseparable sobre $k_{(*)}$.*

2. *$[K : k] = [K : k]_s \cdot [K : k]_i$*

3. *$[K : k]_i$ es una potencia de p.*

4. *Si K es una extensión simple $k(x)$ de grado n, grado reducido n_0, y e exponente de inseparabilidad del polinomio mínimo de x sobre k, entonces $k_{(*)} = k(x^{p^e})$, $[K : k]_s = n_0$ y $[K : k]_i = p^e$*

Demostración:

1. Sea $k_{(*)}$ la clausura separable de K/k. Claramente es una extensión separable de k. Dado $x \in K$, existe $e \in \mathbb{N}$ tal que x^{p^e} separable sobre k, ya que todo elemento tiene una potencia p^e-ésima separable, por el Corolario 2.16. Entonces $x^{p^e} \in k_{(*)}$ para todo x, por lo que K es puramente inseparable sobre $k_{(*)}$.

2. Se tiene $k \subseteq k^{(*)} \subseteq K$, así que

$$[K : k] = [K : k_{(*)}][k_{(*)} : k] = [K : k]_i[K : k]_s$$

3. Como $K/k_{(*)}$ es puramente inseparable por el apartado 1, para algún $e \in \mathbb{N}$ se tiene la igualdad

$$[K : k]_i = [K : k_{(*)}] = p^e$$

4. $[K : k] = [k(x) : k] = n_0 \cdot x^{p^e}$. Si $k_{(*)} = k(x^{p^e})$, entonces $[K : k]_i = p^e$, y por lo tanto $[K : k]_s = n_0$ por los apartados anteriores. Veamos que en efecto $k_{(*)}$ es de esa forma.

   Por el Corolario 2.16, x^{p^e} es separable sobre k, por lo que $k(x^{p^e}) \subseteq k_{(*)}$. Ahora, dado un $y \in k_{(*)}$, se tiene que y es separable sobre $k(x^{p^e})$, porque y tiene que ser separable sobre toda extensión intermedia de $k_{(*)}/k$ por la Proposición 2.18. Pero además $y^{p^e} \in k(x^{p^e})$. Esto se observa expresando y como un elemento del k-espacio vectorial $k(x)$, y su potencia

$$y^{p^e} = \left(\sum_{i=0}^{n} a_i x^i \right)^{p^e} = \sum_{i=0}^{n} a_i^{p^e} x^{ip^e} \in k(x^{p^e})$$

   Entonces y es puramente inseparable sobre $k(x^{p^e})$ y por lo tanto $y \in k(x^{p^e})$, por lo que $k_{(*)} = k(x^{p^e})$.

□

Teorema 2.21. *Teorema del Elemento Primitivo (B.L. van der Waerden* [6]*)*

Sea $K = k(x_1, x_2, ..., x_n)$, $n > 1$, una extensión finita de k tal que los x_i $i > 1$ elementos son separables. Entonces existe un elemento primitivo ϑ tal que $k(\vartheta) = K$. Más aun, si k tiene infinitos elementos, existe un elemento primitivo de K/k tal que es una combinación lineal de los elementos $x_1, ..., x_n$ con coeficientes en k.

DEMOSTRACIÓN: Si $K = \mathbb{F}_{p^e}$ es un cuerpo finito, basta con tomar un elemento generador ϑ de $\mathbb{F}_{p^e}^*$ como grupo multiplicativo cíclico, y dicho elemento genera a todos los x_i.

Supongamos que k es infinito. Vamos a probar el teorema por inducción. Para $n = 1$ es inmediato, $K = k(x_1)$.
Caso $n = 2$. $K = k(x_1, x_2)$ donde x_2 es separable sobre k y sean $f_1(X)$, $f_2(X) \in k[X]$ los polinomios mínimos de x_1 y x_2 respectivamente. Sean $\{x_1 = x_{11}, ..., x_{1r}\}$ y $\{x_2 = x_{21}, ..., x_{2s}\}$ sus respectivos conjugados y sea L un cuerpo de descomposición del polinomio $f_1(X) \cdot f_2(X)$ sobre k. Consideremos la familia de ecuaciones lineales:

$$x_{1i} + x_{2j}X = x_{11} + x_{21}X, \;\; i = 1, ..., r, \quad j = 1, ..., s$$

Como x_2 es separable sobre k, todos sus conjugados son diferentes, por lo que cada una de las ecuaciones anteriores tiene solución única en L (L es un cuerpo así que tiene que existir esa solución por defecto). Elegimos un elemento $c \in k$ que no cumpla ninguna de estas ecuaciones, cuya existencia está asegurada por ser k infinito y que solo hay un numero finito de soluciones de las ecuaciones anteriores. Con esto, definimos $\vartheta = x_1 + cx_2 \in L$. Este es el elemento que queremos probar que tiene la propiedad de ser elemento primitivo.

Probemos que $k(x_1, x_2) = k(\vartheta)$. Claramente $k(\vartheta) \subseteq k(x_1, x_2)$. Para probar la otra inclusión consideremos los polinomios $f_2(X)$ y $f_1(\vartheta - cX) \in k(\vartheta)$. Estos polinomios tienen x_2 como raíz común, $f_2(x_2) = f_1(\vartheta - cx_2) = f_1(x_1) = 0$.

De hecho, es la única raíz que tienen en común, ya que eligiendo x_{2j} da para todo $j \neq 1$

$$\vartheta - cx_{2j} \neq x_{1i} \quad \forall i$$

debido a que los conjugados de x_2 son estrictamente distintos por ser separables sobre k y haber elegido c específicamente para que cx_2 no cumpla ninguna de las ecuaciones lineales.

La raíz x_2 es simple en f_2 y solo tiene en común con $f_1(\vartheta - cX)$ el factor $(X - x_2)$. Los coeficientes de máximo común divisor de estos polinomios debe estar contenido en $k(\vartheta)$, es decir $x_2 \in k(\vartheta)$, y a partir de esto deducimos que $\vartheta - cx_2 = x_1 \in k(\vartheta)$ y por lo tanto $k(x_1, x_2) \subseteq k(\vartheta)$.

A partir de aquí la demostración para el caso n, suponiendo que se cumple el resultado para $n-1$, es: $k(x_1, ..., x_n) = k(\vartheta)$ se concluye de reducir $k(x_1, ..., x_n)$ a $k(\alpha, x_n)$ y aplicar la misma demostración para $n = 2$.

□

Teorema 2.22. *Teorema del Elemento Primitivo (Versión de Ersnt Steinitz [5])*

Sea K/k una extensión finita, entonces $K = k(\alpha)$ si y solo si solo existen finitas extensiones intermedias $k \subseteq L \subseteq K$.

Demostración:
Sean $k \subseteq L \subseteq K = k(\alpha)$, $f(X) \in k[X]$ el polinomio mínimo de α sobre k y $g(X) \in L[X]$ su polinomio mínimo sobre L. Sabemos que $f(X)$ es irreducible en $k[X]$. Como $L(\alpha) = K = k(\alpha)$, se tiene

$$[k(\alpha) : L] = [L(\alpha) : L] = gr(g).$$

Sea L' el cuerpo obtenido al adjuntar a k los coeficientes $c_0, ..., c_{gr(g)}$ de $g(X)$. Se tiene que $L' \subseteq L$ y $g(X)$ es irreducible en L'. Por lo tanto

$$gr(g) = [L'(\alpha) : L'] = [k(\alpha) : L'] = [k(\alpha) : L][L : L'] = gr(g)[L : L'] \Rightarrow L = L'$$

Entonces L está únicamente determinado por $g(X)$. Sin embargo todo $g(X)$ es un factor de $f(X) \in K[X]$, y por lo tanto, al haber solo un número finito de factores del polinomio mínimo $f(X)$ se tiene que existen solo finitas extensiones intermedias de K/k.

Ahora veamos la otra implicación. Sea $K = k(x_1, ..., x_n)$ una extensión finita de k, podemos aplicar el razonamiento de existencia de un elemento primitivo inductivamente para K/k hasta encontrar un elemento ϑ que genere $K = k(\vartheta)$.

Para $n = 1$, es inmediato. $K = k(x_1)$. Para $n = 2$, sea K/k con un número finito de subextensiones intermedias.

Asumamos que el cuerpo es infinito, pues si es finito es trivial (la demostración es la misma que en la otra versión del teorema). Sea una función

$$\tau : \lambda \longmapsto k(x_1 + \lambda x_2)$$

con $\lambda \in k$. Se tiene que $k(x_1 + \lambda x_2) \subseteq k(x_1, x_2)$. Esta función está definida para todo $\lambda \in k$. Como solo existe un número finito de elementos en la imagen de la función, al ser k infinito existen $\lambda_1, \lambda_2 \in k$ distintos tal que $\tau(\lambda_1) = \tau(\lambda_2) = L$, lo que implica que $x_1 + \lambda_1 x_2,\ x_1 + \lambda_2 x_2 \in L$ y consecuentemente $(\lambda_1 - \lambda_2)x_2 \in L$. Por tanto,

$$\lambda_1 - \lambda_2 \neq 0 \Rightarrow x_2 \in L \Rightarrow k(x_1, x_2) \subseteq k(x_1 + \lambda_1 x_2)$$

Por tanto, tiene que $k(x_1, x_2) = k(x_1 + \lambda_1 x_2)$, luego $x_1 + \lambda_1 x_2$ es un elemento primitivo. Para $n - 1$, suponemos que se cumple el resultado. Veamos el caso n.

$$k(x_1, ...x_n) = k(x_1, ..., x_{n-1})(x_n) = k(\vartheta_{n-1})(x_n) = k(\vartheta_{n-1}, x_n)$$

Entonces se tiene el caso para $n = 2$, y se tiene que $\vartheta = \vartheta_{n-1} + \lambda x_n$ con es un elemento primitivo de $k(\vartheta_{n-1}, x_n)$, por lo que tenemos que $K = k(\vartheta)$, K tiene elemento primitivo.

□

El primer teorema del elemento primitivo es más útil para trabajar con extensiones finitamente generadas explícitamente, mientras que el segundo puede usarse para extensiones finitas cualquiera, a pesar de que el concepto de "solamente existe un número finito de extensiones intermedias" es a primera vista más complicado de probar.

Teorema 2.23. *Sea k un cuerpo de característica $p>0$. Sea $k^p \subset k$, si $[k : k^p] = p$, toda extensión finita de k posee un elemento primitivo.*

DEMOSTRACIÓN: Sea k con la condición del enunciado,

$$[k : k^p] = p \Rightarrow [k : k^{p^e}] = p^e \Rightarrow [k^{1/p^e} : k] = p^e.$$

Sea una extensión K/k finita tal que $k \subseteq k^{1/p^e} \subseteq K$. Como se trata de una extensión intermedia tenemos que $p^e | [K : k]$. Tomamos e maximal, que existe al ser finita K/k.

Ahora queremos probar que $K/k^{1/p^e}$ es separable. Sea x en K, con $f(X) \in k[X]$ su polinomio mínimo sobre k. Si x es separable sobre k, también lo es sobre k^{1/p^e}. Si existiese un elemento x inseparable sobre k^{1/p^e}, también lo sería sobre k. Entonces su polinomio mínimo irreducible sobre k es de la forma $f(X) = g(X^{p^{e'}})$ $e' \leq e$ por la Proposición 2.4 y la condición de maximalidad de e. Pero, en $k^{1/p^e}[X]$ se tiene que $f(X) = h(X)^{p^{e'}}$ pues dados los coeficientes a_i de $f(X)$, se tiene que $(a_i)^{1/p^{e'}} \in k^{1/p^e}$ para todo i. El polinomio $h(X)$ es separable sobre k, por lo que también es separable sobre k^{1/p^e}. Por tanto x es separable sobre k^{1/p^e}. Se cumple entonces que $K/k^{1/p^e}$ es separable.

Sea una extensión intermedia arbitraria L de K/k y k^{1/p^s} la $1/p$-extensión de k maximal contenida en L. $L/k^{1/p^s}$ es separable. Para cada $s = 1, ..., e$ existe una extensión puramente inseparable $k^{1/p^s}/k$, y para cada L de K/k con s maximal, hay finitas extensiones intermedias en $L/k^{1/p^s}$ al ser una extensión separable. Entonces existe una cantidad finita de extensiones intermedias de K/k y por el Teorema del Elemento Primitivo, $K = k(\alpha)$. □

Corolario 2.24. *Todas las extensiones finitas de $\mathbb{F}_p(t)$ tienen elemento primitivo, pues $[\mathbb{F}_p(t) : \mathbb{F}_p(t^p) = (\mathbb{F}_p(t))^p] = p$.*

2.2 Extensiones normales finitas

2.2.1 Extensiones normales

Definición. Sean $k \subset K$ cuerpos, se dirá que K/k es una ***extensión normal*** si es una extensión algebraica tal que para todo $\alpha \in K$, K contiene al cuerpo de descomposición de su polinomio mínimo $f(X) \in k[X]$ sobre k.

Teorema 2.25. *Sea K una extensión finita de k, las condiciones siguientes son equivalentes:*

1. *K es una extensión normal de k.*

2. *K es un cuerpo de descomposición de un cierto polinomio $f(X) \in k[X]$.*

Demostración:
Sea K/k normal. Al ser K/k finita, se tiene $K = k(x_1, ..., x_n)$. Sea $f_i(X) \in k[X]$ el polinomio mínimo de x_i sobre k. Al ser K/k normal, contiene todas las raíces de $f_i(X)$ para todo i. Entonces las raíces del polinomio

$$f(X) = \prod_{i=1}^{n} f_i(X)$$

están todas en K y además f es el mínimo polinomio que contiene todas dichas raíces, por lo que $K = k[X]/(f(X))$ y es un cuerpo de descomposición de $f(X)$ sobre k.

Veamos la otra implicación. Sea $f(X) \in k[X]$ el polinomio cuyo cuerpo de descomposición es K. Sea $g(X) \in k[X]$ un polinomio irreducible que posee una raíz $\alpha \in K$ y sea K' su cuerpo de descomposición sobre K. Dado $\beta \in K'$ un conjugado de α, existe un k-isomorfismo $\sigma : k(\alpha) \longrightarrow k(\beta)$ que lleva α a β. La inclusión de las raíces $x_1, ..., x_n$ de $f(X)$ a $k(\alpha)$ y $k(\beta)$ generan respectivamente

$$K = k(\alpha)(x_1, ..., x_n) \qquad y \qquad K(\beta) = k(\beta)(x_1, ..., x_n)$$

Ambos son cuerpos de descomposición de $f(X)$, ya que hemos incluido todas sus raíces. Entonces σ se puede extender a un k-isomorfismo τ:$K \longrightarrow K(\beta)$. Esta función τ permuta el conjunto de las raíces de $f(X)$, y como generan a K, estas raíces de $f(X)$ también generan a β, por lo que $K(\beta) = K$.

□

Corolario 2.26. *Sean $k \subset L \subset K$ cuerpos tal que K es una extensión normal de k. Entonces K es una extensión normal de L.*

Nota 8. Como todos los cuerpos finitos son cuerpos de descomposición, son todos

normales sobre cualquier subcuerpo. Por la misma razón, toda extensión de un cuerpo k que contenga a $\mathbb{F}_p$ que sea de la forma $K = k(\mathbb{F}_{p^e})$ es normal.

Proposición 2.27. [5] *Sea L/k una extensión finita de cuerpos. Existe una extensión K de L tal que K/k es una extensión normal finita y si L' es otra extensión normal $L \subset L' \subseteq K$ entonces $L' = K$. Este cuerpo se llama la* ***clausura normal*** *de L/k y está únicamente determinado salvo isomorfismos, y lo denotaremos $Nr_{L/k}$.*

Demostración:
Sea $L = k(\alpha_1, ..., \alpha_n)$, con α_i elementos en L. Sea $f_i(X)$ el polinomio mínimo de α_i sobre k y $f(X) = \prod_{i=1}^{n} f_i(X)$. Denotamos K el cuerpo de descomposición de f. Es una extensión normal de k, y contiene a L. Este es el cuerpo que denominaremos clausura normal de L/k.

Ahora, si se diese que $L = k(\alpha_1, ..., \alpha_n) \subseteq L' \subset K$ con L'/L normal, L' contendría a todos los elementos α_i lo que implica que también contendría a todos sus conjugados. Tales elementos son los generadores de K sobre k, por lo que $K \subseteq L'$ pero entonces $K = L'$. La extensión K es la mínima extensión normal de L pues no existe ninguna extensión intermedia normal sobre L.

□

Adjuntar elementos algebraicos a un cuerpo genera extensiones, pero para construir extensiones normales hay que asegurarse de que todos los conjugados de los elementos que se están adjuntando se pueden generar también en la extensión. Si no, hace falta extender dicha extensión a su clausura normal. Esto es cierto incluso para cuerpos en característica 0.

Ejemplo 7. Sea $\mathbb{Q}$, la extensión finita $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ no es normal ya que le faltan las otras dos raíces del polinomio mínimo $X^3 - 5$ de $\sqrt[3]{5}$. Al adjuntar a $\mathbb{Q}(\sqrt[3]{5})$ la raíz compleja de la unidad $e^{2\pi i/3}$, se generan las otras dos raices del polinomio, $e^{2\pi i/3}\sqrt[3]{5}$ y $e^{4\pi i/3}\sqrt[3]{5}$. Esto resulta en la clausura normal de $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$.

Análogamente en característica positiva, la extensión $\mathbb{F}_2(t^{1/3})/\mathbb{F}_2(t)$ tampoco es normal, pues el polinomio mínimo de $t^{1/3}$ es $f(X) = X^3 + t$, que tiene 3 raíces distintas al ser separable, de las que $t^{1/3}$ es solo una raíz, y en $\mathbb{F}_2(t^{1/3})$ no hay ninguna otra. Por lo tanto no es un cuerpo de descomposición de $f(X)$. Para construir la clausura normal se le adjuntan las otras dos raíces. Sean las raíces de $X^3 + 1$, que son 1, α y $\alpha + 1$, con $\alpha^2 + \alpha + 1 = 0$. Los elementos $t^{1/3}$, $\alpha t^{1/3}$ y $(\alpha + 1)t^{1/3}$ son raíces de $f(X)$, así que $Nr_{\mathbb{F}_2(t^{1/3})/\mathbb{F}_2(t)} = \mathbb{F}_2(t^{1/3}, \alpha) = \mathbb{F}_4(t^{1/2})$. .

2.2.2 Grupos de Galois

Definición. Sea $Gal(K/k)$ el conjunto de todos los k-automorfismos de K. La composición de aplicaciones sobre $Gal(K/k)$ determina una estructura de grupo, que se denomina el ***grupo de Galois*** de K sobre k.

Proposición 2.28. *Sean una extensión normal K/k y elementos $x, y \in K$. Las condiciones son equivalentes :*

1. *x e y son conjugados sobre k.*

2. *Existe $\sigma \in Gal(K/k)$ tal que $\sigma(x) = y$*

Demostración:
Supongamos que x e y son conjugados. Existe un isomorfismo

$$\tau : k(x) \longmapsto k(y)$$

tal que $\tau(x) = y$. Además K es un cuerpo de descomposición de $k(x)$ y $k(y)$. Por tanto τ se puede ampliar a un k-automorfismo σ de K, y por definición $\sigma \in Gal(K/k)$.

Para la otra implicación, si $f(X)$ es el polinomio mínimo de x en $k[X]$,

$$0 = \sigma(f(x)) = f(\sigma(x)) = f(y)$$

Entonces x e y son conjugados.

□

Definición. Sea un subgrupo $\mathcal{G} \subset Gal(K/k)$, y sea

$$F(\mathcal{G}) = \{x \in K \mid \sigma(x) = x \ \ \forall \sigma \in \mathcal{G}\}$$

$F(\mathcal{G})$ se llamará el ***cuerpo fijo de Galois***.

El conjunto $F(\mathcal{G})$ es un subcuerpo de K. Ya que $\sigma(x) = x$ para todo σ si $x \in k$, $k \subseteq F(\mathcal{G}) \subseteq K$. Además, como los elementos de $F(\mathcal{G})$ quedan fijos mediante automorfismos, la suma y producto con inversos están cerrados en $F(\mathcal{G})$.

Teorema 2.29. *Sea K/k normal finita y un elemento $x \in K$. Las siguientes condiciones son equivalentes:*

1. *x es puramente inseparable sobre k.*

2. *x coincide con todos sus conjugados sobre k.*

3. *$x \in F(Gal(K/k))$.*

Demostración:
Primero, probemos la equivalencia de (1) y (2). Sea $x \in K$ algebraico con $f(X)$ su polinomio mínimo sobre k, que tiene grado n, grado reducido n_0 y exponente de inseparabilidad e. Por la Proposición 2.11 el número de conjugados de x sobre en K

es n_0. El elemento x es puramente inseparable si y solo si $n_0 = 1$, que ocurre si y solo si coincide con todos sus conjugados, no hay otra raíz de $f(X)$ distinta de x.

Veamos que (2) implica (3). Si x coincide con todos sus conjugados, es un elemento fijo, es decir, $\sigma(x) = x$ para todo σ ya que los σ llevan elementos a sus conjugados sobre k por la Proposición 2.28.

Finalmente, demostremos que (3) implica (2). Sea $x \in F(Gal(K/k))$, entonces por definición de cuerpo fijo se cumple que

$$\sigma(x) = x \ \forall \ \sigma \in Gal(K/k).$$

Si existiese un conjugado y distinto de x, existiría un $\sigma' \in Gal(K/k)$ tal que $\sigma'(x) = y$, pero entonces $x \notin F(Gal(K/k))$. Luego no existe ningún conjugado distinto de x. □

Corolario 2.30. *$F(Gal(K/k)) = k^{(*)}$. En particular, si K es separable sobre k, $F(Gal(K/k)) = k$.*

Esto es consecuencia directa de la proposición anterior y que todos los elementos puramente inseparables sobre k están en $k^{(*)}$. Esto prueba que $k^{(*)}$ es el cuerpo deseado que queda fijo bajo todos los automorfismos de $Gal(K/k)$, y sobre el que basaremos la correspondencia. Si K/k es separable $k^{(*)} = k$ así que se da el segundo resultado.

Teorema 2.31. *Sea K/k una extensión normal y finita. Se verifican las siguientes propiedades:*

1. *$k_{(*)}$ es una extensión normal separable de k.*
2. *K es una extensión normal separable de $k^{(*)}$.*
3. *$k_{(*)}(k^{(*)}) = k^{(*)}(k_{(*)}) = K$*
4. *$[K : k^{(*)}] = [K : k]_s$*
5. *$[k^{(*)} : k] = [K : k]_i$*

Demostración:

1. Por definición de $k_{(*)}$, todos los elementos $x \in k_{(*)}$ son separables sobre k, así que es una extensión separable de k.

   Sea $f(X)$ el polinomio mínimo de un $x \in K$ separable sobre k. Como K/k es normal, todas las raíces de $f(X)$ están en K. Además, $f(X)$ es separable sobre k por lo que todas sus raíces son separables, y consecuentemente también pertenecen a $k_{(*)}$.

2. Como $k^{(*)}$ es un cuerpo intermedio de la extensión normal K/k, se tiene por la Proposición 2.26 que $K/k^{(*)}$ es una extensión normal. Basta con probar la separabilidad de $K/k^{(*)}$. Sea $x_1 \in K$ y $\{x_1, ..., x_n\}$ sus conjugados distintos. Consideremos el polinomio

$$f(X) = (X - x_1)...(X - x_n).$$

Al ser K/k normal, todos los conjugados de x_1 están en K, luego $f(X) \in K[X]$. Sea $\sigma \in Gal(K/k)$. Para todo x_i, dicho σ lleva x_i a uno sus conjugados, es decir, es una permutación del conjunto $\{x_1, ..., x_n\}$ por la Proposición 2.28. La ampliación σ' de σ a $K[X]$ mantiene $f(X)$ fijo, es decir, $\sigma'(f(X)) = f(X)$. Esto demuestra que los coeficientes de $f(X)$ son invariantes sobre automorfismos de $Gal(K/k)$, y por lo tanto este polinomio también pertenece a $k^{(*)}[X]$ gracias al corolario 2.30.

Por otra parte, sea $g(X) \in k^{(*)}[X]$ tal que $g(x_1) = 0$. Existe $\sigma_i \in Gal(K/k)$ tal que $\sigma_i(x_1) = x_i$ para cada $i = 1...n$:

$$\sigma_i(g(x_1)) = g(\sigma_i(x_1)) = g(x_i) = 0$$

Entonces todos los conjugados distintos son raíces de $g(X)$ y se cumple que $gr(g(X)) \geq gr(f(X))$, implicando que $f(X)$ es irreducible sobre $k^{(*)}[X]$. Por lo tanto, x_i es separable sobre $k^{(*)}$ para todo i, ya que su polinomio mínimo tiene todas sus raíces simples, luego $K/k^{(*)}$ es separable .

3. Veamos que $k_{(*)}(k^{(*)}) = k^{(*)}(k_{(*)}) = K$. Sean dos conjuntos S y E y un cuerpo L, se cumple la igualdad $L(S)(E) = L(E)(S)$. Eligiendo $S = k^{(*)}$, $E = k_{(*)}$ y $L = k$ la igualdad es $k_{(*)}(k^{(*)}) = k^{(*)}(k_{(*)})$ es inmediata.

Por definición $k^{(*)}$ y $k_{(*)}$ están contenidos en K así que $k_{(*)}(k^{(*)}) \subseteq K$, queda probar la inclusión inversa. Sea $x \in K$ y sea $g(X)$ su polinomio mínimo sobre $k_{(*)}$. La extensión $K/k_{(*)}$ es puramente inseparable por el Teorema 2.20. Entonces todo $x \in K$ también es puramente inseparable sobre $k^{(*)}(k_{(*)})$.

Por el apartado anterior, todo $x \in K$ también será separable sobre $k^{(*)}(k_{(*)})$, al ser separable sobre $k^{(*)}$.

Entonces x es simultáneamente separable y puramente inseparable, por lo que $x \in k^{(*)}(k_{(*)})$ por la Nota 4, así que $K = k_{(*)}(k^{(*)}) = k^{(*)}(k_{(*)})$.

4. El cuerpo $k_{(*)}$ es separable sobre k, por lo tanto, por el Teorema del Elemento Primitivo 2.21, existe $x \in k_{(*)}$ tal que x genera $k_{(*)}$ como extensión simple $k(x)$. Entonces,

$$K = k^{(*)}(k_{(*)}) = k^{(*)}(k(x)) = k^{(*)}(x).$$

Por lo tanto, x también es el elemento primitivo de K sobre $k^{(*)}$.

Sea $f(X) \in k$ su polinomio mínimo sobre k, y sea $g(X) \in k^{(*)}[X]$ tal que $g(x) = 0$. Si y es un conjugado de x sobre k, existe un automorfismo $\sigma \in Gal(K/k)$ que lleva x a y, y entonces:

$$0 = \sigma(0) = \sigma(g(x)) = g(\sigma(x)) = g(y)$$

por lo que $X - y$ divide a $g(X)$ en $K[X]$. Esto se puede aplicar a cada conjugado, por lo que todos los son raíces de $g(X)$, así que $gr(g(X)) \geq gr(f(X))$, lo que implica que $f(X)$ es irreducible en $k^{(*)}[X]$. Entonces, como $K = k^{(*)}(x)$ y $k_{(*)} = k(x)$ con el mismo polinomio mínimo, $[K : k^{(*)}] = [k_{(*)} : k] = [K : k]_s$.

5. Por el apartado anterior, la propiedad 2 del Teorema 2.20 y las propiedades de multiplicidad del grado de las extensiones tenemos

$$[K : k] = [K : k_{(*)}][k_{(*)} : k] = [K : k^{(*)}][k^{(*)} : k] = [K : k]_s[K : k]_i \Rightarrow$$

$$[K : k^{(*)}][K : k]_i = [K : k^{(*)}][k^{(*)} : k] \Rightarrow [k^{(*)} : k] = [K : k]_i$$

□

Ejemplo 8. Sea $X^{98} + (\frac{t+1}{t^3})X^{49} + t \in \mathbb{F}_7(t)[X]$. Sea K su cuerpo de descomposición sobre $\mathbb{F}_7(t)$. Este polinomio irreducible es inseparable. Por el Teorema anterior, sabemos que $k \subset k^{(*)} \subset K$ es una extensión intermedia de grado 49, pues el factor de inseparabilidad de f es $7^2 = 49$, y que su grado reducido es 2 por lo que $[K : k]_s = 2$, así que como cuerpo de descomposición de $k^{(*)}$, K es una extensión simple.

No todas las extensiones finitamente generadas por un elemento algebraico son necesariamente normales, como se ha visto en ejemplos anteriores. La condiciones para que al adjuntar una raíz a un cuerpo k, se puedan construir las otras raíces, no solo dependen de la existencia de elementos en k que las puedan generar sino también de la separabilidad de la extensión. Las propiedades anteriores pueden utilizarse como indicador de si una extensión que posee elementos inseparables es normal o no, pues son condiciones necesarias de normalidad. Veamos un ejemplo.

Ejemplo 9. En $\mathbb{F}_p(t_1, t_2) = k$, tenemos el polinomio $f(X) = X^{2p} + t_1X^p + t_2 \in K[X]$. Sea $K = k(\alpha)$ la extensión de k al adjuntar una raíz α de $f(X)$. Veamos que este polinomio es irreducible.

Sea $g(X) = X^2 + t_1X + t_2$. Veamos que es irreducible sobre k. Si existiesen $h(X), v(X) \in k[X]$ tal que $h(X)v(X) = g(X)$ se tendría

$$g(X) = h(X)v(X) = (X - a)(X - b)$$

Por razones de grado, queda $a + b = t_1$ y $ab = t_2$. Al ser t_1 y t_2 trascendentes e independientes, este sistema de ecuaciones carece de solución en k. Por lo tanto $g(X)$ es irreducible sobre k, y por el Lema 2.8 $f(X)$ también lo es.

Entonces $f(X)$ es un polinomio inseparable porque $f'(X) = 0$. Veamos ahora que ninguno de los elementos de K es puramente inseparable sobre k. Suponemos que existe un β puramente inseparable, luego $\beta^{p^e} \in k$. Si $f(X)$ fuese irreducible sobre

$k(\beta)$, entonces sería el mínimo polinomio de α, y $[K : k(\beta)] = 2p$, pero se tiene que $[K : k] = 2p$ al ser irreducible sobre k, por lo que $k(\beta) = k$ o $f(X)$ no es irreducible sobre $k(\beta)$.

Si $f(X)$ no es irreducible, se tiene que tener que $f(X) = (h(X))^p$ en dicha extensión intermedia. Entonces, los elementos $\sqrt[p]{t_1}$ y $\sqrt[p]{t_2} \in k(\beta)$, así que $k(\sqrt[p]{t_1}, \sqrt[p]{t_2}) \subset k(\beta)$, pero $[k(\sqrt[p]{t_1}, \sqrt[p]{t_2}) : k] = p^2$, lo cual es una contradicción para $p \neq 2$ pues $[K : k] = 2p$. En el caso $p = 2$, se tiene $p^2 = 2p = 4$, la contención de cuerpos $k(\sqrt[p]{t_1}, \sqrt[p]{t_2}) \subseteq K$ implica que K/k sería puramente inseparable, pero esta extensión también añade elementos separables, las raíces de $g(X)$, lo cual es un absurdo. Así que no existe β puramente inseparable, sin embargo la extensión es inseparable. Pero, por la propiedad 2 anterior, si K/k fuese normal, se tendría que $K/k^{(*)}$ sería separable. Ya que $k = k^{(*)}$, y K/k es inseparable, no puede ser normal.

La distinción que posee esta extensión es que combina elementos trascendentes independientes, que al ser independientes impiden una separación del polinomio, a no ser que estén ambas raíces en la extensión. La forma de computar su clausura normal pasa a ser cuestión de encontrar su cuerpo de descomposición, adjuntando ambas raíces distintas de $f(X)$, y se tiene que $[Nr_{K/k} : k] \geq 2p^2$.

La inseparabilidad y la inseparabilidad pura no son lo mismo, tanto en el contexto de un elemento como el de una extensión, y existen extensiones inseparables que no contienen ningún elemento puramente inseparable que no pertenezca al cuerpo base. Sin embargo, para extensiones normales inseparables, $k^{(*)}$ siempre es distinto de k, precisamente por el Teorema 2.31.

Teorema 2.32. *El grupo de Galois de una extensión normal finita de cuerpos K/k es un grupo finito de orden igual a $[K : k]_s$.*

Demostración: K es una extensión normal separable de $k^{(*)}$ por la propiedad anterior 2. Además $Gal(K/k^{(*)}) \subseteq Gal(K/k)$ y por el Corolario 2.30

$$F(Gal(K/k^{(*)})) = F(Gal(K/k)) = k^{(*)}.$$

Entonces

$$\forall\ \sigma,\ \ \sigma \in Gal(K/k^{(*)}) \Rightarrow Gal(K/k) \subseteq Gal(K/k^{(*)}) \Rightarrow Gal(K/k) = Gal(K/k^{(*)}).$$

Puesto que $[K : k^{(*)}] = [K : k]_s$, basta con probar que $Gal(K/k^{(*)})$ es de orden $[K : k^{(*)}]$.

Sea α un elemento primitivo de $K/k^{(*)}$, se tiene que $K = k^{(*)}(\alpha)$. Denotados α_i sus conjugados sobre $k^{(*)}$ con $i = 1, ..., n$ todos distintos, puesto que α es separable sobre $k^{(*)}$, se tiene que $[K : k^{(*)}] = n$.

Todo $\sigma \in Gal(K/k^{(*)})$ transforma $\alpha = \alpha_1$ en un conjugado suyo, y recíprocamente para todo $1 \leq i \leq n$, existe un $\sigma \in Gal(K/k^{(*)})$ tal que $\sigma(\alpha) = \alpha_i$. Estos σ son todos distintos al ser automorfismos de una extensión separable. Así que hay justamente n automorfismos distintos. Entonces

$$[k^{(*)}(\alpha) : k^{(*)}] = n = |Gal(K/k^{(*)})| = |Gal(K/k)|$$

□

Este teorema se puede aplicar tanto como a $k^{(*)}$ como a cualquier extensión intermedia K' de $K/k^{(*)}$, que nos da que los $Gal(K/K')$ son subgrupos de orden $[K : K']$ de $Gal(K/k)$. Este hecho es una base importante de la correspondencia, encontrar y ver como son los subgrupos de $Gal(K/k)$, su orden y su relación con las extensiones.

Nota 9. Tanto la notación $k^{(*)}$ como $k_{(*)}$ conllevan un cierto abuso de lenguaje, pues solo hacen referencia al cuerpo base de la extensión K/k a la que pertenecen. En la mayoría de este trabajo, como solo hay una extensión a la que se refieren estos cuerpos intermedios, se ha hecho implícito el cuerpo K en el que se encuentran y se utiliza esta notación. Sin embargo, en el próximo resultado se utilizan los conjuntos $\{x \in K|$ separable sobre $k\}$ y $\{x \in L|$ separable sobre $k\}$ de dos extensiones distintas K/k y L/k en un mismo contexto. Para distinguirlos, se utilizará la notación $k_{(*),K}$ y $k_{(*),L}$ para hacer explícita de cual es dicho conjunto la máxima extensión separable.

Proposición 2.33. [4] *Sea una extensión finita K/k y un cuerpo intermedio L de esta, se tiene que*

$$[K : k]_s = [K : L]_s \cdot [L : k]_s$$

Demostración:
Se tiene la igualdad

$$[K : k]_s = [k_{(*),K} : k] = [k_{(*),K} : k_{(*),L}] \cdot [k_{(*),L}, k] = [k_{(*),K} : k_{(*),L}][L : k]_s.$$

Por lo tanto, para que se verifique la igualdad del enunciado se tiene que cumplir que

$$[k_{(*),K} : k_{(*),L}] = [K : L]_s = [L_{(*),K} : L].$$

Denotamos $E = k_{(*),L}$ y $F = k_{(*),K}$. Sea $S = \{\, x \mid \, x \in L, x$ inseparable sobre $k\}$.

Primero probemos que $E(S) = L$ y que $F(S) = L_{(*),K}$. La primera igualdad se cumple por definición de E y S. Para la segunda, probamos la doble inclusión. Se tiene que $F(S) \subseteq L_{(*),K}$ ya que $F \subseteq L_{(*),K}$ y $S \subseteq L_{(*),K}$. Sea $x \in L_{(*),K}$, si x es separable sobre k, $x \in F$. Si x es inseparable sobre k, x^{p^e} es separable sobre k para algún $e > 0$, luego $x^{p^e} \in F(S)$ y por lo tanto x es puramente inseparable sobre $F(S)$. Además, como es separable sobre L y $L \in F(S)$, x es simultáneamente separable e inseparable sobre $F(S)$ y entonces $x \in F(S)$. Todo $x \in F(S)$ y se tiene la otra inclusión.

Ahora, probemos que $[F : E] = [F(S) : E(S)]$. La extensión F/E es separable por lo que por el Teorema del Elemento Primitivo $F = E(\alpha)$ con $\alpha \in F$. La igualdad queda como $[E(\alpha) : E] = [E(S)(\alpha) : E(S)]$, que se cumple si los polinomios mínimos de α sobre E y sobre $E(S)$ son del mismo grado. Sea $f(X)$ el polinomio mínimo de α sobre E. Como α es separable también lo son sus conjugados y no hay conjugados suyos

que estén en $E(S)$ y no en E pues $E(S)/E$ es una extensión puramente inseparable. Si $f(X)$ fuese reducible en $E(S)$, existiría $h(X) \in E(S)[X]$ que dividiese a $f(X)$, y que tendría que ser de la forma $h(X) = (X - \alpha_1) \cdots (X - \alpha_j)$ con α_i con $i = 1, ..., j$ ciertos conjugados de α. Los coeficientes de $h(X)$ tienen que estar en $E(S)$. Sin embargo, la suma y producto de elementos separables es separable, y se observa que los coeficientes de $h(X)$ son sumas y productos de conjundos de α, por lo que son separables. Como $h(X) \notin E[X]$, hay coeficientes que no están en E, el cuerpo base en una extensión puramente inseparable $E(S)/E$, lo cual es una contradicción. Recíprocamente, no puede ocurrir que el polinomio mínimo $g(X) \in E(S)[X]$ de α sobre $E(S)$ sea de mayor grado que $f(X)$ pues $f(X) \in E(S)[X]$ y entonces $g(X)$ no sería el polinomio mínimo de α. Entonces $gr(g) = gr(f)$, se cumple la igualdad y consecuentemente también

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

□

Lema 2.34. *Sea K/k una extensión normal finita. Denotados G' un subgrupo de $Gal(K/k)$ y $K' = F(G')$, se verifican las siguientes propiedades:*

1. $k^{(*)} \subseteq K' \subseteq K$

2. $[K : K'] \leq |G'|$

Demostración:

1. La demostración de este apartado es inmediata ya que todo automorfismo de $Gal(K/k)$ deja $k^{(*)}$ fijo por el corolario 2.30.

2. El primer apartado implica que K' es un cuerpo intermedio de la extensión $K/k^{(*)}$, que es separable y normal por el segundo apartado del Teorema 2.31. Esto implica que K/K' es una extensión separable y normal por las Proposiciones 2.26 y 2.15. Aplicando el Teorema del Elemento Primitivo 2.21, podemos encontrar α tal que $K = K'(\alpha)$. Denotamos $\sigma_i \in G'$ los elementos de G', con $id_k = \sigma_1$. Definimos el polinomio:

$$f(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha)).$$

Se tiene que $f(\alpha) = 0$ pues $\sigma_1(\alpha) = \alpha$. Como $G' \in Gal(K/k)$ es un subgrupo, $\sigma_j G' = G'$. Sea σ'_j la ampliación de σ_j a $K[X]$,

$$\sigma'_j(f(X)) = \prod_{i=1}^{n} (X - \sigma_i\sigma_j(x)) = f(X).$$

Luego, $f(X) \in K'[X]$ y como su grado es n se tiene $[K : K'] \leq |G'|$. □

3 Teorema de Galois sobre extensiones finitas normales

3.1 La correspondencia de Galois

Definición. Denotamos $\mathcal{I}(K:k) = \{L \mid k^{(*)} \subseteq L \subseteq K, L \text{ un cuerpo}\}$, el conjunto de las extensiones intermedias de la extensión $K/k^{(*)}$ y $\mathcal{S}(Gal(K/k))$, el conjunto de subgrupos del grupo de Galois $Gal(K/k)$ de una extensión K/k.

Con todas las propiedades anteriores y términos bien definidos podemos finalmente establecer una correspondencia entre los subgrupos de Galois de una extensión normal finita K/k y las extensiones intermedias de $K/k^{(*)}$.

Teorema 3.1. [2] *Teorema fundamental de la correspondencia de Galois*

Sea K/k una extensión normal y finita. Las funciones Φ y Φ' definidas como

$$\Phi : \mathcal{I}(K:k) \to \mathcal{S}(Gal(K/k)) \qquad \Phi' : \mathcal{S}(Gal(K/k)) \to \mathcal{I}(K:k^{(*)})$$
$$\Phi(K') = Gal(K/K') \qquad \Phi'(G') = F(G')$$

son biyecciones inversas una de la otra. Además, si $K' \in \mathcal{I}(K:k)$, entonces K' es una extensión normal de k si y solo si $\Phi(K')$ es un subgrupo normal de $Gal(K/k)$ y, en tal caso

$$Gal(K'/k) \cong {}^{Gal(K/k)}\!/_{\Phi(K')}$$

Demostración:
Sea $K' \in \mathcal{I}(K:k^{(*)})$. Al ser K separable sobre K' por la Proposición 2.15, por serlo $K/k^{(*)}$, se tiene que

$$(K')^{(*)} = F(Gal(K/K')) = K',$$

que da

$$\Phi'(\Phi(K')) = \Phi'(Gal(K/K')) = F(Gal(K/K')) = K'.$$

Para la otra composición, dado $G' \subseteq Gal(K/k)$ tenemos

$$\Phi(\Phi'(G')) = \Phi(F(G')) = Gal(K/F(G'))$$

Se tiene que $G' \subseteq Gal(K/F(G'))$. Si n es el orden de G', por el Lema 2.34,

$$[K:F(G')] = |Gal(K/F(G'))| \leq n$$

$$\Rightarrow Gal(K/F(G')) \subseteq G' \Rightarrow G' = Gal(K/F(G')).$$

Por lo tanto se da que Φ y Φ' son funciones inversas entre si.

La extensión K'/k es normal si y solo si para todo $x \in K'$ se verifica que los conjugados de x pertenecen a K'. Esta propiedad se refleja en el grupo de Galois $Gal(K/K')$ como subgrupo de $Gal(K/k)$. Dados $x \in K'$, $\sigma' \in Gal(K/K')$ y $\sigma \in Gal(K/k)$ arbitrarios. Al dejar σ' fijo a x y a sus conjugados, se tiene que

$$\sigma'\sigma(x) = \sigma(x) \Rightarrow \sigma^{-1}\sigma'\sigma(x) = x$$

es decir, $\sigma^{-1}\sigma'\sigma \in Gal(K/K')$ y el subgrupo $Gal(K/K') = \Phi(K')$ es un subgrupo normal de $Gal(K/k)$.

Por último, demostremos el isomorfismo de $Gal(K'/k)$ al cociente. Supongamos que K/K' es normal. En tal caso, se puede definir la restricción de un automorfismo $\sigma \in Gal(K/k)$ a K', y la denotamos $\sigma_{K'}$. Puesto que K/K' es normal, la restricción es un k-automorfismo de K', ya que lleva conjugados a conjugados y k permanece fijo al ser un k-morfismo. Sea

$$\varphi : {}^{Gal(K/k)}\!\diagup_{\Phi(K')} \to Gal(K'/k)$$

$$\varphi([\sigma]) = \sigma_{K'}$$

Esta función es un homomorfismo. Veamos que es una biyección. Para la inyectividad, suponemos que existen σ, σ' distintos tal que $\sigma_{K'} = \sigma'_{K'}$. Entonces

$$\sigma'\sigma^{-1} = \sigma'' \in Gal(K/k) \ \ con \ \ \sigma''_{K'} = id_{K'},$$
$$\varphi(\sigma'\sigma^{-1}) = \varphi(\sigma'') \Rightarrow \varphi(\sigma') = \varphi(\sigma) \Rightarrow \sigma' = \sigma.$$

Veamos ahora que es sobreyectiva. Al ser K una extensión normal de k, es el cuerpo de descomposición de un polinomio $f(X)$ sobre k. Pero entonces las raíces de $f(X)$ también generan K como cuerpo de descomposición sobre K'. Por lo tanto, todo k-automorfismo de K' se puede ampliar a un k-automorfismo de K por la Proposición 1.3. Esto implica que todo elemento de la imagen de φ tiene preimagen.

Entonces, tenemos que φ es inyectiva y sobreyectiva, es decir, biyectiva, por lo tanto es un isomorfismo. Con esto acaba la demostración. □

Nota 10. Las extensiones de Galois, extensiones separables,normales y finitas, también están incluidas en este teorema más generalizado. En tal caso se tiene que la extensión puramente inseparable es trivial $k^{(*)} = k$ y todos los cuerpos intermedios de K/k son separables sobre k.

3.2 Ejemplos

Las extensiones algebraicas finitas de $\mathbb{F}_p(t)$ son las extensiones más fáciles de manejar, y como hemos visto antes, las menos complicadas de computar sus polinomios, así que nos centramos en ejemplos de esta forma.

Ejemplo 10. Tenemos $f(X) = (X^2+X+1)(X^2+t) = X^4+X^3+(t+1)X^2+tX+t \in \mathbb{F}_2(t)[X]$. A pesar de ser un polinomio con $f'(X) \neq 0$ como tiene un componente inseparable $X^2 + t$, cuya derivada es 0, el polinomio es inseparable. Una extensión de $\mathbb{F}_2(t)$ como cuerpo de descomposición de $f(X)$ nos va a dar una cadena de extensiones de esta forma:

$$\mathbb{F}_2(t) \subset \mathbb{F}_2(t^{1/2}) \subset \mathbb{F}_4(t^{1/2})$$

En este caso $k^{(*)} = \mathbb{F}_2(t^{1/2})$, la extensión sobre la que observamos los cuerpos intermedios de la correspondencia. Esto es porque $f(X)$, al estar ya descompuesto en partes irreducibles, nos da tanto el factor de separabilidad y inseparabilidad de forma inmediata. Dada α la raíz tal que $\alpha^2 + t = 0$, esto implica que $\alpha^2 \in \mathbb{F}_2(t)$, por lo que es una extensión puramente inseparable, además, $n_0 = 1$ y $p^e = 2$. El otro componente, que da la raíz β y su conjugado, es separable, pero no se encuentra en el cuerpo base, así que no es un elemento puramente separable. Por lo tanto, al aplicar la correspondencia de Galois esto queda bien delineado.

$$Gal(K/k) = Gal(K/k^{(*)}) = Gal(\mathbb{F}_2(t^{1/2}))(\beta)/\mathbb{F}_2(t^{1/2}) \cong C_2$$

Como $K/k^{(*)}$ no tiene cuerpos intermedios, este grupo no tiene subgrupos. De hecho, es un grupo cíclico de orden primo.

Este ejemplo es muy simple, pero cementa qué parte es la más importante a la hora de calcular estos cuerpos de descomposición, saber cuáles son sus componentes irreducibles para poder diferenciar si es una extensión separable o no, y cómo es la forma de $k^{(*)}$.

Ejemplo 11. Sea $k = \mathbb{F}_7(t)$, el polinomio $X^{21} + X^7 + t$ y α una raíz de dicho polinomio. Este polinomio es irreducible pues su polinomio reducido $X^3 + X + t$ es irreducible, y $(a_0)^{1/p} = (t)^{1/p} \notin k$. Sea $\mathbb{F}_7(t)(\alpha)$. Se cumple $\mathbb{F}_7(t)(\alpha) = \mathbb{F}_7(\alpha)$ pues t se puede expresar en función de α y $\mathbb{F}_7$, $t = 6(\alpha^{21} + \alpha^7)$. Antes de poder aplicar el Teorema de correspondencia, hay que verificar que la extensión es normal. Si $\mathbb{F}_7(\alpha)/\mathbb{F}_7(t)$ fuese normal, todos los conjugados de α están en la extensión y $f(X)$ tendría que descomponerse en factores lineales. Se tiene que $f(X) = (h(X))^7 = (X^3 + X + 6(\alpha^3 + \alpha))^7$. Sea $X^3 + X + 6(\alpha^3 + \alpha)/(X - \alpha) = X^2 + \alpha X + (\alpha^2 + 1)$, y sea β un conjugado disntinto de α. Se tendría que este polinomio es reducible si $\beta \in \mathbb{F}_7(\alpha)$. La fórmula de una ecuación cuadrática implica que si $\beta \in \mathbb{F}_7(\alpha)$ entonces $2\sqrt{\alpha^2 - 1} \in \mathbb{F}_7(\alpha)$ lo cual no es cierto. Entonces $\beta \notin \mathbb{F}_7(\alpha)$ y el cuerpo de descomposición $K = (\alpha, \beta)$ será una extensión de grado 42. Una vez distinguidas las raíces se utiliza la correspondencia de Galois para computar las extensiones intermedias mediante $Gal(K/k)$.

Primero computemos $Gal(K/k)$. Se tiene $Gal(K/k) = Gal(K/k^{(*)})$, y como $t^{1/7} \in k^{(*)}$ y $[k^{(*)} : k] = 7$ se tiene que $k^{(*)} = \mathbb{F}_7(t^{1/7})$. Denotamos $\sigma_1 = id$. Construyamos el resto de automorfismos. Todo $\sigma \in Gal(K/k)$ lleva una raíz de $f(X)$ a un conjugado. Designadas dos raíces α y β, la otra raíz es $\gamma = \frac{t^{1/7}}{\alpha\beta}$.

Sea σ_2 un k-endomorfismo de K. Supongamos que $\sigma_2(\beta) = \frac{t^{1/7}}{\alpha\beta}$ y que $\sigma_2(\alpha) = \alpha$. Entonces se tiene que $\sigma_2(\frac{t^{1/7}}{\alpha\beta}) = \frac{t^{1/7}}{\alpha t^{1/7}/\alpha\beta} = \beta$, por lo que es un automorfismo de $Gal(K/k)$.

Sea σ_3 un k-endomorfismo de K que deja fijo a β. Si $\sigma_3(\alpha) = \frac{t^{1/7}}{\alpha\beta}$ entonces $\sigma_3(\gamma) = \sigma_3(\frac{t^{1/7}}{\alpha\beta}) = \alpha$ y también es un automorfismo.

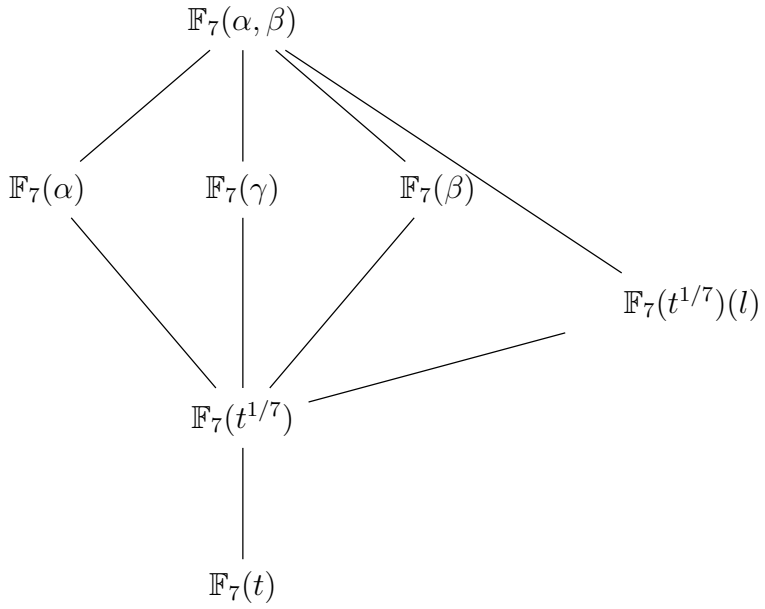
Denotamos σ_4 el k-endomorfismo que lleva α a β y viceversa. La raíz γ queda fija al estar en función de α, β y un elemento de $k^{(*)}$ y es un automorfismo.

Como $Gal(K/k)$ es un grupo, $\sigma_2\sigma_4$, $\sigma_3\sigma_4 \in Gal(K/k)$, y son automorfismos distintos a los otros, así que $\sigma_5 = \sigma_2\sigma_4$ y $\sigma_6 = \sigma_3\sigma_4$.

σ_2	σ_3	σ_4	σ_5	σ_6
$\alpha \mapsto \alpha$	$\alpha \mapsto \gamma$	$\alpha \mapsto \beta$	$\alpha \mapsto \beta$	$\alpha \mapsto \gamma$
$\beta \mapsto \gamma$	$\beta \mapsto \beta$	$\beta \mapsto \alpha$	$\beta \mapsto \gamma$	$\beta \mapsto \alpha$
$\gamma \mapsto \beta$	$\gamma \mapsto \alpha$	$\gamma \mapsto \gamma$	$\gamma \mapsto \alpha$	$\gamma \mapsto \beta$

Con esto queda explícitamente definido $Gal(K/k)$. Se puede ver inmediatamente que $Gal(K/k) = S_3$, pues tiene 3 subgrupos de grado 2, propiedad que C_6, el otro grupo de orden 6, no verifica.

Se pueden definir explícitamente las extensiones intermedias no triviales de $K/k^{(*)}$, que tienen que ser 4, correspondiendo a los subgrupos $\{\sigma_1, \sigma_2\}$,$\{\sigma_1, \sigma_3\}$,$\{\sigma_1, \sigma_4\}$, y $\{\sigma_1, \sigma_5, \sigma_6\}$. Los tres primeros cuerpos intermedios tienen elementos fijos denotados explícitamente, una de las 3 raíces, y por lo tanto generan la extensión intermedia al adjuntarlos a $k^{(*)}$. Para el último subgrupo, sea el elemento $l = (\alpha-\beta)(\alpha-\gamma)(\gamma-\beta)$. Se tiene que $l \notin k^{(*)}$ pues $\sigma_2(l) = \sigma_3(l) = \sigma_4(l) = -(\alpha-\beta)(\alpha-\gamma)(\gamma-\beta) = -l$. Sin embargo, $\sigma_5(l) = \sigma_6(l) = l$, por lo tanto $l \in F(\{\sigma_1, \sigma_5, \sigma_6\})$. Como el grado de l es 2, es el elemento primitivo de la extensión sobre $k^{(*)}$. Les aplicamos Φ' y nos queda el diagrama:

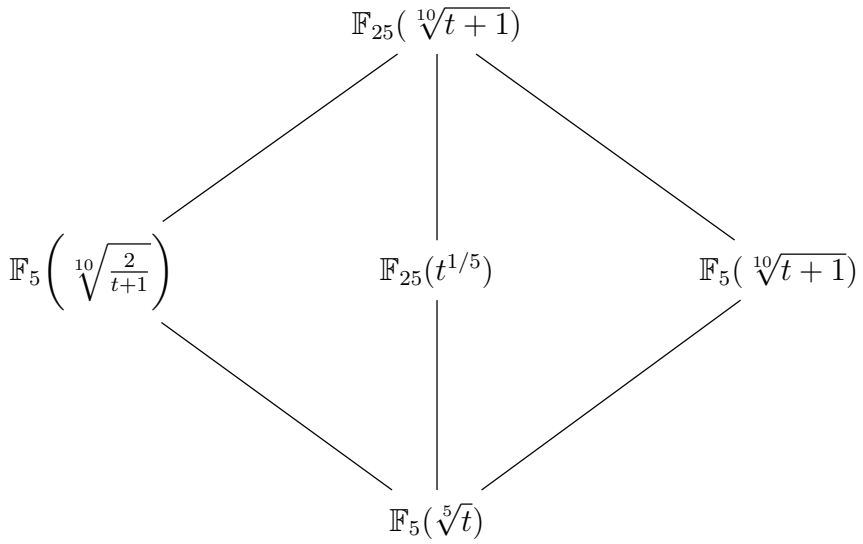


Con esto quedan diferenciadas las extensiones intermedias. Como el único subgrupo normal es $\{\sigma_1, \sigma_5, \sigma_6\}$, su cuerpo fijo es la única extensión intermedia normal.

Ejemplo 12. Añadimos elementos $\sqrt[10]{\frac{2}{t+1}}$ y $\sqrt[10]{t+1}$ al cuerpo $\mathbb{F}_5(t)$ mediante el polinomio $(X^{10}+t+1)(X^{10}+\frac{2}{t+1}) = X^{20}+(\frac{t^2+2t+3}{t+1})X^{10}+2$. Se tiene que $\sqrt{2} = \sqrt[10]{\frac{2}{t+1}}\cdot\sqrt[10]{t+1} \in K$, que es un elemento primitivo de $\mathbb{F}_{25}$. Luego, la forma de K es

$$\mathbb{F}_5(t) \subset \mathbb{F}_5\left(\sqrt[10]{\frac{2}{t+1}}, \sqrt[10]{\frac{t+1}{1}}, t\right) \cong \mathbb{F}_{25}\big(\sqrt[10]{t+1}, t\big)$$

Se comprueba inmediatamente por las Proposiciones 2.33 y 2.20 que $[K:k]_s = 4$ y $[K:k]_i = 5$, con $k^{(*)} = \mathbb{F}_5(t^{1/5})$. Los cuerpos intermedios son suficientemente simples como para ser computados explícitamente, basta con adjuntar a $k^{(*)}$ solo uno de los 2 elementos para obtener dos extensiones intermedias distintas $K_1 = \mathbb{F}_5\left(\sqrt[10]{\frac{2}{t+1}}\right)$ y $K_2 = \mathbb{F}_5(\sqrt[10]{t+1})$, y la última extensión está generada por el producto de los dos elementos, $\sqrt[10]{2} = \sqrt{\sqrt[5]{2}} = \sqrt{2}$, luego se tiene que $K_3 = \mathbb{F}_{25}(\sqrt[5]{t})$. No existe ninguna otra extensión intermedia de $K/k^{(*)}$ pues K_1, K_2 y K_3 son las únicas 3 extensiones intermedias de grado 2 y es el único grado posible que puede tener una extensión no trivial de $K/k^{(*)}$. Queda el diagrama:



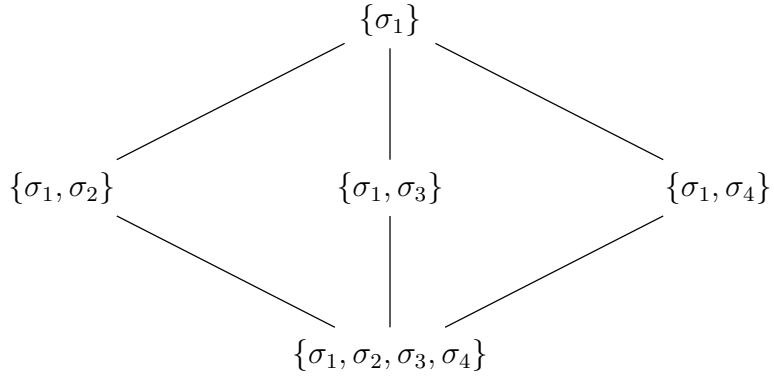
Ahora le podemos aplicar Φ del Teorema 3.1 para ver cómo se comporta $Gal(K/k)$.

$\Phi(K_1) = Gal(K/K_1) = \{\sigma_1, \sigma_2\}$, con σ_2 un automorfismo que deja fijo $\sqrt[10]{\frac{2}{t+1}}$. Sin embargo, no deja fijo a $\mathbb{F}_{25}$ pues $\sqrt{2} \notin K_1$, e igualmente con la raíz de $(X^{10}+t+1)$. Consecuentemente $\sigma_2(\sqrt{2}) = -\sqrt{2}$ y $\sigma_2(\sqrt[10]{t+1}) = -\sqrt[10]{t+1}$.

$\Phi(K_2) = Gal(K/K_2) = \{\sigma_1, \sigma_4\}$ con σ_4 el automorfismo que deja fijo $\sqrt[10]{t+1}$, y por lo tanto $\sigma_4\big(\sqrt[10]{\frac{2}{t+1}}\big) = -\sqrt[10]{\frac{2}{t+1}}$. Entonces se tiene que $\sigma_4(\sqrt[10]{2}) = -\sqrt[10]{2}$.

$\Phi(K_3) = Gal(K/K_3) = \{id, \sigma_3 = \sigma_2\sigma_4\}$. Como hemos descrito anteriormente a σ_2 y σ_4 se tiene que $\sigma_3(\sqrt{2}) = \sigma_2\sigma_4(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2}$. luego se deja fijo a $\mathbb{F}_{25}$.

$Gal(K/k) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ es el grupo de Klein de 4 elementos, que es abeliano, luego las extensiones intermedias son normales. Este resultado es consistente con la construcción de la extensión pues se añade un par de elementos x, y tal que xy es un elemento de orden 2 distinto, una característica identificativa de la presentación del grupo de Klein.



El cuerpo de las series formales sobre un cuerpo base k, denotado $k((t))$, es el cuerpo de fracciones de $k[[t]]$, el anillo de series formales de potencias. En él, extensiones finitas $k(t)(x_1;...,x_n)$ de $k(t)$ inducen extensiones finitas $f((t))(x_1,...,x_n)$ de $k((t))$, pues si $f(X) \in k(t)[X]$ también se tiene que $f(X) \in k((t))[X]$. También existen extensiones algebraicas añadiendo sucesiones infinitas que anulan un cierto polinomio, pero encontrar y distinguir las propiedades de sucesiones de ese tipo queda fuera del ámbito de este trabajo.

Ejemplo 13. Sea la extensión generada por las raíces del polinomio $X^{12} - t^{12}$ sobre el cuerpo base $k = \mathbb{F}_3((t^{12}))$. Este cuerpo es de característica 3, por lo que $f(X)$ tiene derivada nula. Los elementos que estamos añadiendo son los conjugados de t, la raíz duodécima de t^{12}. Como $n_0 = 4$ tiene que haber 4 conjugados distintos, $2^2 = 1$ y además $\sqrt{2} \neq 1$ en característica 3, entonces las raíces de $f(X)$ son $\{t, 2t, \sqrt{2}t, 2\sqrt{2}t\}$. El cuerpo $\mathbb{F}_9$ contiene las raíces cuartas de la unidad $1, 2, \sqrt[2]{2}, 2\sqrt[2]{2}$ necesarias para descomponer $f(X)$ en factores lineales, por lo que están en K y $K = \mathbb{F}_9((t))$. Por el lema multiplicativo, sabemos que $[K : k] = 24$.

Examinando rápidamente los elementos de la extensión K/k vemos que los elementos puramente inseparables están generados por t^4, por ser $car(k) = 3$ todo $(a + bt^4 + cbt^8)^3 = a^3 + b^3t^{12} + c^3t^{24} \in k$ con $a, b, c \in k$. Por lo tanto, se tiene que $k^{(*)} = \mathbb{F}_3((t^4))$. El polinomio $f(X)$ en $k^{(*)}$ es reducible y sus componentes irreducibles son separables. $f(X) = (X^{12} - t^{12}) = (X^4 - t^4)^3$. Entonces se tiene que $[K : k]_s = 8$ y que $[K : k]_i = 3$. La extensión es normal y le podemos aplicar la correspondencia de Galois.

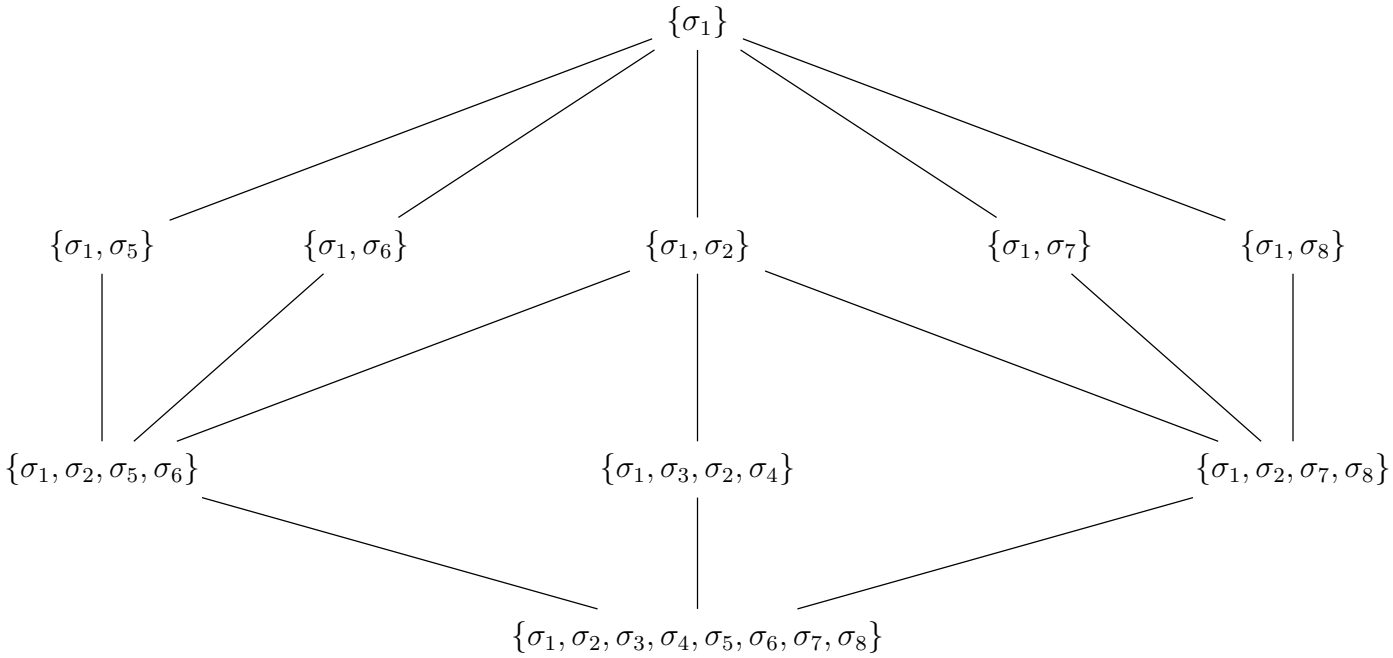
Tras un examen no riguroso del problema, se podría suponer que las extensiones intermedias son $\mathbb{F}_3((t))$, $\mathbb{F}_9((t^2))$, $\mathbb{F}_9((t^2))$ y $\mathbb{F}_3((t^2))$. Sin embargo, utilizando la correspondencia de Galois al describir los automorfismos de $Gal(K/k)$, se pueden observar si existen otros cuerpos intermedios. El calculo explícito de los automorfismos en este caso se puede realizar como en ejemplos anteriores, escogiendo morfismos tales que los conjugados vayan unos a otros y ver cuáles son todas las posibilidades de automorfismos de esa forma.

σ_1		σ_2		σ_3	
	$t \mapsto t$		$t \mapsto 2t$		$t \mapsto \sqrt{2}t$
$\sqrt{2} \mapsto \sqrt{2}$	$2t \mapsto 2t$	$\sqrt{2} \mapsto \sqrt{2}$	$2t \mapsto t$	$\sqrt{2} \mapsto \sqrt{2}$	$2t \mapsto 2\sqrt{2}t$
$2\sqrt{2} \mapsto 2\sqrt{2}$	$\sqrt{2}t \mapsto \sqrt{2}t$	$2\sqrt{2} \mapsto 2\sqrt{2}$	$\sqrt{2}t \mapsto 2\sqrt{2}t$	$2\sqrt{2} \mapsto 2\sqrt{2}$	$\sqrt{2}t \mapsto 2t$
	$2\sqrt{2}t \mapsto 2\sqrt{2}t$		$2\sqrt{2}t \mapsto \sqrt{2}t$		$2\sqrt{2}t \mapsto t$

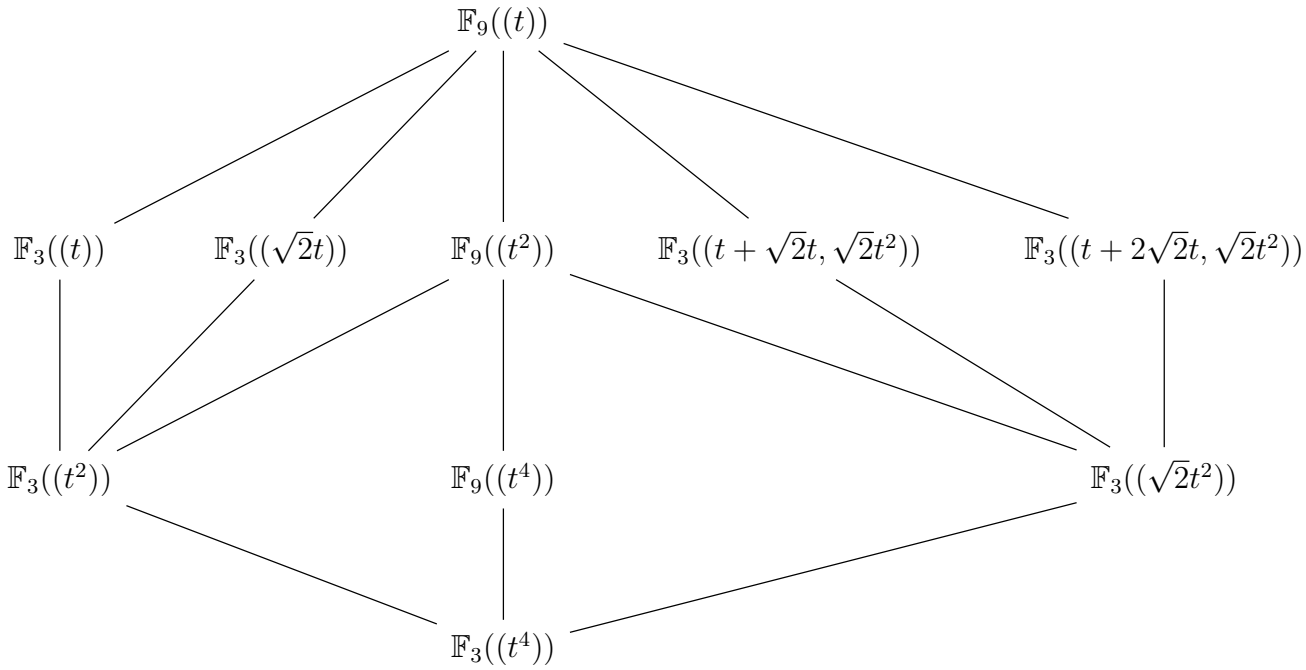
$$\begin{array}{ccc} \sigma_3 & & \\ & t \mapsto 2\sqrt{2}t & \\ \sqrt{2} \mapsto \sqrt{2} & 2t \mapsto 2\sqrt{2}t & \\ 2\sqrt{2} \mapsto 2\sqrt{2} & \sqrt{2}t \mapsto t & \\ & 2\sqrt{2}t \mapsto 2t & \end{array} \qquad \begin{array}{ccc} \sigma_4 & & \\ & t \mapsto t & \\ \sqrt{2} \mapsto 2\sqrt{2} & 2t \mapsto 2t & \\ 2\sqrt{2} \mapsto \sqrt{2} & \sqrt{2}t \mapsto 2\sqrt{2}t & \\ & 2\sqrt{2}t \mapsto \sqrt{2}t & \end{array} \qquad \begin{array}{ccc} \sigma_5 & & \\ & t \mapsto 2t & \\ \sqrt{2} \mapsto 2\sqrt{2} & 2t \mapsto t & \\ 2\sqrt{2} \mapsto \sqrt{2} & \sqrt{2}t \mapsto \sqrt{2}t & \\ & 2\sqrt{2}t \mapsto 2\sqrt{2}t & \end{array}$$

$$\begin{array}{ccc} \sigma_7 & & \\ & t \mapsto \sqrt{2}t & \\ \sqrt{2} \mapsto 2\sqrt{2} & 2t \mapsto 2\sqrt{2}t & \\ 2\sqrt{2} \mapsto \sqrt{2} & \sqrt{2}t \mapsto t & \\ & 2\sqrt{2}t \mapsto 2t & \end{array} \qquad \begin{array}{ccc} \sigma_8 & & \\ & t \mapsto 2\sqrt{2}t & \\ \sqrt{2} \mapsto 2\sqrt{2} & 2t \mapsto \sqrt{2}t & \\ 2\sqrt{2} \mapsto \sqrt{2} & \sqrt{2}t \mapsto 2t & \\ & 2\sqrt{2}t \mapsto t & \end{array}$$

Una vez calculados, para establecer la correspondencia se buscan los subgrupos de $Gal(K/k)$. Con estos explícitos se comprueba fácilmente que se verifican $\sigma_2^2 = \sigma_5^2 = \sigma_6^2 = \sigma_7^2 = \sigma_8^2 = \sigma_1 = id$, por lo que hay 5 subgrupos de orden 2. Además $\sigma_2\sigma_5 = \sigma_6$, luego $\{\sigma_1, \sigma_2, \sigma_5, \sigma_6\}$ es un grupo de Klein. Asimismo, $\sigma_7\sigma_8 = \sigma_2$ y $\{\sigma_1, \sigma_2, \sigma_7, \sigma_8\}$ es otro grupo de Klein. Por otra parte, $\sigma_3^2 = \sigma_2$, $\sigma_3^3 = \sigma_4$ y $\sigma_3^4 = \sigma_1 = id$, luego $\{\sigma_1, \sigma_3, \sigma_2, \sigma_4\}$ es un grupo cíclico. No hay otros subrupos de orden 4. En efecto, estos son todos los subgrupos del grupo $C_4 \times C_2$, que tiene que ser $Gal(K/k)$.



Ahora podemos calcular explícitamente los cuerpos intermedios aplicando Φ', fijándonos en que elementos se quedan fijos. Aquellos subgrupos que dejan fijo $\sqrt{2}$ dejan fijo $\mathbb{F}_9$. Si un subgrupo deja fijo $t^2 = t \cdot t$ es porque t se queda fijo o $t \to 2t$, luego $t^2 \to 4t^2 = t^2$. Un elemento que deja fijo el subgrupo $\{\sigma_1, \sigma_7, \sigma_2, \sigma_8\}$ es $\sqrt{2}t^2$, $\sigma_2(\sqrt{2}t^2) = \sigma_7(\sqrt{2}t^2) = \sigma_8(\sqrt{2}t^2) = 2 \cdot 2\sqrt{2}t^2$. Los automorfismos σ_7 y σ_8 dejan fijo $t + \sqrt{2}t$ y $t + 2\sqrt{2}t$ respectivamente, así que podemos denotarlos como generadores de los subgrupos de orden 2 que generan. Entonces, el diagrama de extensiones intermedias es:



3.3 Otra versión de la correspondencia de Galois sobre extensiones finitas normales

Como ya se ha dicho en la introducción, existen diferentes teoremas de correspondencia que extienden la correspondencia de Galois a extensiones no necesariamente de Galois.

De estos teoremas, el de [5] de Stephen Shatz y Jean Gallier se acerca más a la simpleza y resultados del Teorema 3.1. De hecho es un teorema equivalente, es decir, se puede derivar un resultado del otro. Para ello primero define las clases de equivalencia de Galois, que son clases sobre el conjunto de extensiones intermedias de K/k tal que $L' \in [L]$ si $L'^{(*)} = L^{(*)}$. Esto añade cierta complicación para ver que las clases de equivalencia están bien definidas como tal y utilizar sus propiedades en la demostración del teorema. El teorema formulado queda así:

Teorema 3.2. *Sea K/k una extensión normal finita. Sea $G' \subset Gal(K/k)$ y $[L]$ con $k \subset L \subset K$ un cuerpo intermedio. Entonces las funciones*

$$\Phi([L]) = Gal(K/L) \qquad \Phi'(G') = [F(G')]$$

son inversas y establecen una correspondencia biyectiva entre subgrupos de Galois y las clases de Galois de extensiones intermedias.

Además $Gal(K/L) \triangleleft Gal(K/k)$ si y solo si $L^{(*)}$ es una extensión normal de k, lo cual ocurre si y solo si $L_{(*)}$ es una extensión normal de k. Cuando ocurre esto último, se tiene una sucesión exacta canónica

$$0 \to Gal(K/L) \to Gal(K/k) \to Gal(L^{(*)}/k) \to 0.$$

Como se puede ver, la correspondencia sobre $k^{(*)}$ es una instancia especifica de esta versión en la que solo se fija en los cuerpos intermedios de $K/k^{(*)}$, así que las clases de Galois solo tienen un elemento.

Asimismo, se puede inferir esta versión de la correspondencia de la versión formulada al principio de la sección.

Un esquema de la demostración es: Se le aplica la correspondencia de Galois a k, que da una biyección entre K' intermedios de $K/k^{(*)}$ y $Gal(K/K')$. Sea L un cuerpo intermedio de K/k arbitrario. Se observa que la clase de equivalencia de Galois tiene un representante $L^{(*)}$ entre $k^{(*)}$ y K, y que todo cuerpo intermedio entre K y $k^{(*)}$ pertenece a una clase única, pues $K/k^{(*)}$ es separable, luego $(K')^{(*)} = K'$. Esto quiere decir que sobre la extensión K/k si se tuviesen 2 distintas clases $[D]$ y $[L]$ los correspondientes subgrupos de Galois no pueden ser el mismo, y dos subgrupos distintos de $Gal(K/k)$ no pueden tener la misma clase asociada. Entonces, la biyección de Φ y Φ' se mantiene al tomar clases de equivalencia en vez de cuerpos intermedios de $K/k^{(*)}$, pues el representante de cada clase es una extensión intermedia de $K/k^{(*)}$.

La secuencia exacta se tiene de que $Gal(K/L) \subset Gal(K/k)$ y que siempre $k^{(*)} \subset L^{(*)}$, por lo que se le puede aplicar la condición de normalidad para el Teorema 3.1 sobre K/k y se tiene que $Gal(L^{(*)}/k) \cong Gal(K/k)/\Phi(L^{(*)})$ si y solo si $L^{(*)}$ es normal. Poner esta relación como una secuencia exacta es lo mismo que poner dicho cociente.

□

Ejemplo 14. Partiendo del último ejemplo anterior, podemos saber el grupo de Galois de la extensión $\mathbb{F}_9((t))/\mathbb{F}_3((t^6))$, pues $\mathbb{F}_3((t^6)) \in [\mathbb{F}_3((t^2))]$. Entonces,

$$Gal(\mathbb{F}_9((t))/\mathbb{F}_3((t^6))) = Gal(\mathbb{F}_9((t))/\mathbb{F}_3((t^2))) = \{\sigma_1, \sigma_2, \sigma_5, \sigma_6\}.$$

Igualmente para $\mathbb{F}_9((t^{12}))$,

$$Gal(\mathbb{F}_9((t))/\mathbb{F}_9((t^{12}))) = Gal(\mathbb{F}_9((t))/\mathbb{F}_9((t^4))) = \{\sigma_1, \sigma_3, \sigma_2, \sigma_4\}.$$

Se puede calcular entonces el grupo de Galois de toda extensión intermedia K/K' de K/k.

La ventaja de de la correspondencia de S.G. es que se agrupan en clases de equivalencia extensiones intermedias, dejando claro cuáles cuerpos intermedios cualesquiera tienen grupos de Galois iguales. Además, si resultase más fácil calcular la máxima extensión puramente inseparable de algún L intermedio en vez de $k^{(*)}$, ayudaría a resolver el resto de la correspondencia. La desventaja esta es que saber la clase de equivalencia a la que pertenece cada extensión intermedia, si se sabe encontrar dicha extensión intermedia, es una computación ligeramente complicada si el cuerpo base tiene extensiones inseparables. No hay una distinción muy significativa a la hora de computar la correspondencia entre los dos teoremas, al fin y al cabo son teoremas equivalentes. Pero la forma en la que enfocan las extensiones intermedias da una interesante perspectiva que el otro tal vez no refleja de forma tan evidente, por lo que merece la pena conocer ambas formulaciones ya que se complementan.

4 Consecuencias del teorema de correspondencia de Galois

Como complemento al trabajo, en esta sección se estudian varios resultados que existen para extensiones separables finitas, que se pueden extender a extensiones finitas mediante el Teorema de Correspondencia 3.1.

4.1 Teorema de irracionalidades naturales

Teorema 4.1. [5] *Sea K/k una extensión normal finita y $k \subset k'$ una extensión arbitraria de k. Sea $K' = K(k')$. Entonces:*

1. *K'/k' es una extensión normal finita.*

2. *La función $\tau : \sigma \mapsto \sigma_{|K}$ da una inyección canónica $Gal(K'/k') \hookrightarrow Gal(K/k)$, con imagen $Gal(K/(K \cap k'))$.*

Demostración:

1. Tenemos $k \subset k' \subset k'(K)$, y $K = k(x_1, ..., x_n)$, por lo que $k' \subset k'(k(x_1, ..., x_n)) = k'(x_1, ..., x_n) = K'$. Entonces K'/k' es una extensión normal finitamente generada.

2. Sea $\sigma \in Gal(K'/k')$. Definamos la restricción natural $\sigma_{|K}$ y veamos que τ está bien definida. Sea $\sigma(K) = \{\sigma(x) \mid x \in K\}$, se tiene que $\sigma(K) \subseteq K'$. Sea $a \in k'$, si $k \subset k(a) \subset K$ se tiene por el Teorema 2.26 que $K/k(a)$ es normal por ser K/k normal. Si $a \notin K$, una transformación σ_a entre conjugados de a deja fijo a K, al ser K/k normal. Por lo tanto $\sigma(K) = K$, ya que si σ llevase una raíz de K'/k' fuera de K no sería normal. Ya que σ fija k', también fija k al estar contenido en él. Entonces $\sigma_{|K} \in Gal(K/k)$.

   Veamos la inyectividad de τ. Se tiene que $k'(x_1, ..., x_n) = K'$. Si $\sigma_{|K} = id_K$, tenemos $\sigma_{|K}(x_i) = x_i$ para todo i. Además por suposición $\sigma_{k'} = id_{k'}$, y entonces σ fija K'. Por lo tanto $\sigma = id \in Gal(K'/k')$. La preimagen de la identidad de $Gal(K/k)$ es únicamente la identidad de Gal y consecuentemente es inyectiva.

   Sea $H = K \cap k'$ y $G' = im(\tau)$. Se tiene que $G' \cong Gal(K'/k')$ al ser inyectivo τ. Como $H \subseteq k'$ esto implica que G' deja fijo a H, luego $G' \subset Gal((K/H))$.

   Sea $L = F(G')$. Se verifica que $L = L^{(*)}$ por el Corolario 2.30. Queremos demostrar que $H^{(*)} = L^{(*)}$. Una primera inclusión se tiene ya que $H \subset F(G') = L$. Veamos la segunda inclusión $L \subset H^{(*)}$.

   Sea $x \in L$. Entonces $x \in K$ por definición de cuerpo fijo. Además $F(G') \subseteq F(Gal(K'/k'))$. Entonces por 2.30 $x \in k'$ y por lo tanto $x^{p^e} \in k'$ para algún e por ser L puramente inseparable. Además $x^{p^e} \in K$ por el mismo razonamiento. Entonces $x^{p^e} \in k' \cap K = H$. Esto implica que $L = L^{(*)} \subseteq H^{(*)}$. Con esto, queda

$L^{(*)} = H^{(*)}$ y se verifica la igualdad

$$Gal(K/H) = Gal(K/H^{(*)}) = Gal(K/L) = Gal(K/F(G')) = im(\tau)$$

Por el Teorema de Correspondencia de Galois 3.1.

□

Este teorema tiene utilidad tanto más adelante como de por sí, pues asocia grupos de Galois de extensiones no intermedias entre sí, identificando $Gal(K'/k')$ con $Gal(K/K \cap k')$.

4.2 Solubilidad de extensiones

4.2.1 Raíces n-ésimas

Definición. Un cuerpo de descomposición K del polinomio $f(X) = X^n - 1 \in k[X]$ sobre k en se llama un ***cuerpo de raíces n-ésimas de la unidad*** de k.

Nota 11. Sobre un cuerpo de característica $p > 0$, el concepto de raíces n-ésimas de la unidad no tiene utilidad sobre los $n = mp$ múltiplos de p. En tal caso las raíces que se están añadiendo no son n-raíces, ya que $(X^n - 1) = (X^m - 1)^p$. Por consecuente, las p-raíces de la unidad no triviales no existen, y en tal caso $K = k$.

Nota 12. Como ilustran los teoremas 1.12 y 1.5, toda extensión de un cuerpo finito se puede ver como la adjunción de las raíces de $X^{p^e-1}-1$, que son raíces de la unidad. Las raíces de la unidad sobre un cuerpo de característica positiva se encuentran en las sucesivas extensiones de los cuerpos finitos, similarmente a como funcionan las extensiones ciclotómicas sobre los racionales.

Proposición 4.2. *Sea $n = p_1^{r_1}...p_s^{r_s}$ la descomposición en factores primos de n en factores primos y sea G el conjunto de raíces n-ésimas de la unidad de k en K.Se verifican las siguiente propiedades:*

1. *La multiplicación de K induce sobre G una estructura de grupo.*

2. *G es un grupo cíclico.*

Demostración: Para esta demostración asumimos n coprimo con $car(k)$ sin pérdida de generalidad.

1. Está claro que sea $a, b \in G$ se tiene $a^n \cdot b^n = (ab)^{(n)} = 1$, por lo que $ab \in G$ y que la operación es asociativa, es la multiplicación. Le existencia de un elemento inverso es inmediato. Sea $\varepsilon \in G$, puesto que $G \subset K^* = K - \{0\}$, y como K es

un cuerpo existe $1/\varepsilon \in K^*$ inverso de ε y se tiene que

$$(1)^n = \left(\frac{\varepsilon}{\varepsilon}\right)^n = \frac{\varepsilon^n}{\varepsilon^n} = \left(\frac{1}{\varepsilon}\right)^n$$

Entonces $1/\varepsilon \in G$ y G es un grupo.

2. Sea i un entero $1 \leq i \leq s$. El polinomio $X^{n/p_i} - 1$ tiene como mucho n/p_i n-raíces de la unidad. Como $n/p_i < n$, debe existir un elemento $\varepsilon \in G$ que no sea raíz de $X^{n/p_i} - 1$, por tanto $\varepsilon^{n/p_i} \neq 1$. Definamos $\theta_i = \varepsilon^{n/p_i^{r_i}}$. Se tiene que $\theta_i^{p_i^{r_i}} = \varepsilon_i^n = 1$. El orden de θ_i es un divisor de $p_i^{r_i}$, pero como $\theta_i^{p_i^{r_i-1}} = \varepsilon_i^{n/p_i} \neq 1$. Ahora sea $\theta = \theta_1 \cdots \theta_s$, el orden de θ es producto del orden de los factores, y por lo tanto es de orden n y es un generador de G como grupo cíclico.

□

Definición. Sea k un cuerpo de característica p, y el polinomio $f(X) = X^n - a \in k[X]$. Su cuerpo de descomposición sobre k se llama ***cuerpo de raíces n-ésimas de a*** sobre k.

Teorema 4.3. [4] *Sea un cuerpo k que contenga una n-raíz de la unidad. Una extensión que adjunte una raíz α de $X^n - a$, con $car(k) \nmid n$, es una extensión cíclica separable y satisface que $[K : k] = d$ con $d|n$. Existe $c^d = a$ y $X^d - c^d \in k[X]$ es el polinomio mínimo de la extensión. Recíprocamente, toda extensión cíclica separable de grado n es de la forma $K = k(\alpha)$, y su polinomio mínimo sobre k es de la forma $f(X) = X^n - a \in k^[X]$.*

Para la demostración de este teorema y el siguiente se utilizan resultados sobre la traza y la norma de una de extensión, $tr_{K/k}$ y $N_{K/k}$, conceptos que vienen explicados en detalle en el Apéndice.

Demostración: Sea K/k una extensión cíclica separable de grado n. Sea ζ un elemento de k tal que $\zeta^n = 1$. Entonces, $N_{K/k}(\zeta^{-1}) = (\zeta^{-1})^n = 1$ por el Lema A.2. Por el Teorema 90 de Hilbert multiplicativo A.8(véase apéndice), existe $c \in K^*$ tal que $\sigma(c) = \zeta c$ con $\sigma \in Gal(K/k)$, un elemento que genera el grupo de Galois. Tenemos que para todo $i = 1, ..., n$

$$\sigma^i(c) = \zeta^i c.$$

Estos valores son conjugados de c. Los conjugados $\zeta^i c$ tienen que ser distintos al ser la extensión K/k separable, y c es de grado al menos n. De hecho, $K = k(c)$ ya que $k(c) \subset K$ y $[K : k] = n$. Ahora calculemos el polinomio mínimo de c.

$$\sigma(c^n) = \sigma(c)^n = \zeta^n c^n = c^n$$

Esto implica que $c^n \in k$ Entonces el polinomio mínimo es $X^n - c^n$, ya que c es una raíz del polinomio y su grado es idéntico al grado de c.

Recíprocamente, sea $K = k(\alpha)$ con α una raíz de $f(X) = X^n - a$. Al ser n coprimo con $car(k)$ se tiene que la derivada de $f(X)$ no es nula. Si el polinomio es irreducible,

esto implica que tiene que ser separable. Sea $d = [K : k] = |Gal(K/k)|$. Por el teorema de Lagrange, $d|n$. Si $d = n$, se tiene que $f(X)$ es irreducible. Si $d \neq n$, esto implica que $p \nmid d$, por lo que al ser α separable, su polinomio mínimo tiene que ser de grado d. Dado un $\zeta \in G$, con G el grupo multiplicativo de n-raíces de la unidad, $\zeta\alpha$ es solución de $f(X)$, y definiendo $\sigma(\alpha) = \zeta\alpha$ podemos asociar los $\sigma \in Gal(K/k)$ con elementos del grupo G de raíces n-ésimas. Por la Proposición 4.2, como $Gal(K/k) \subseteq G$, $Gal(K/k)$ es un grupo cíclico, y por lo tanto se tiene que

$$\sigma(\alpha^d) = \sigma(\alpha)^d = \zeta^d\alpha^d = \alpha^d = c$$

luego $c \in k$ al quedarse fijo por σ. Entonces el polinomio mínimo tiene que ser $f(X) = (X^d) - c$.

□

Varios ejemplos realizados anteriormente con raíces de la unidad, como Ejemplo 10 y Ejemplo 12 son parte este fenómeno, en el que la existencia de la raíz n-ésima asegura que una extensión con $f(X) = X^n - a$ sea normal y cíclica. Por eso en el Ejemplo 13 al cuerpo intermedio de K/k que contiene la raíz de la unidad X^2-1 tiene consecuentemente un grupo cíclico al extenderse a K, $Gal(\mathbb{F}_9((t))/\mathbb{F}_9((t^{12}))) = C_4$.

También existen extensiones cíclicas de grado p en cuerpos de característica p positiva, que tienen asociados unos polinomios específicos. El nombre distintivo de estas extensiones y estos polinomios viene dado por los matemáticos que primero estudiaron estas extensiones y desarrollaron su teoría.

Definición. Una extensión K/k que es un cuerpo de descomposición del polinomio X^p-X-c con $c \neq a^p-a \in k$ para cualquier $a \in k$ se llama una ***extensión de Artin-Schreier***, y el polinomio de descomposición se llama análogamente ***polinomio de Artin-Schreier***.

Teorema 4.4. *Teorema de Artin-Schreier.* [4]

Sea $f(X) \in k[X]$ un polinomio de Artin-Schreier. Es irreducible, separable y la extensión de Artin-Schreier K/k asociada es cíclica. Recíprocamente, si existe una extensión separable de grado $p = car(k)$, se tiene que su polinomio mínimo es un dicho polinomio.

Demostración: El polinomio $X^p - X - c$ tiene derivada no nula y es de grado p. Si es irreducible debe ser separable. Si no, si existiese un polinomio inseparable que lo dividiese, este polinomio tendría que ser de la forma $X^p + b \in k[X]$, pero no existe ningún elemento que cumpla esa condición, por lo que $f(X)$ es separable. Veamos que en efecto es irreducible.
Sea a una raíz, el resto de raíces distintas son de la forma $a + i$ con $i = 0, ..., p - 1$, ya que

$$(a+i)^p = (a+i) + c = a^p - a + c = 0.$$

Sobre K, $f(X)$ tiene factorización en factores lineales

$$\sum_{i=0}^{p-1}(X - (a+i)).$$

Supongamos que $f(X)$ es reducible. Por lo tanto, existe algún $g(X) \in k[X]$ tal que $g(X)|f(X)$ y que debe ser un producto de algunos de estos factores en $K[X]$. Sea $d = gr(g)$. El coeficiente g_{d-1} de $g(X)$ es de la forma $-da + j$ para algún $j \in \mathbb{F}_p$. Pero al ser d y p coprimos y que $g_{d-1} = -da + j \in k$, esto implicaría que $a \in k$, lo cual contradice la condición del coeficiente de la definición. Luego, $f(x)$ tiene que ser irreducible. Además, $|Gal(K/k)| = p$ es primo por lo que el grupo es cíclico.

Recíprocamente, sea una extensión finita normal separable K/k de grado $[K : k] = p$. Al ser separable, todas las raíces son distintas y el grado del polinomio mínimo del elemento primitivo α es p, y $[K : k] = |Gal(K/k)|$, por lo que $Gal(K/k)$ es un grupo de orden p. Por el Teorema de Lagrange, $Gal(K/k)$ es un grupo cíclico. Al ser $car(k) = p$, $f(X)$ no es de la forma $X^p - a$, ya que este polinomio es reducible o inseparable. Como $Gal(K/k)$ es un grupo cíclico, una base de este grupo es $(\sigma^0, \sigma^1, ..., \sigma^{p-1})$ para algún $\sigma \in Gal(K/K)$. Sea $x \in K$, representando x dada una base de K como k-espacio vectorial

$$x = x_1\alpha^0 + ...x_{p-1}\alpha^{p-1}.$$

Se tiene que $tr_{K/k}(-1) = 0$ por el Lema A.2 ya que $-1 \in k$. Por tanto, por el teorema 90 de Hilbert A.9, existe a tal que $\sigma(a) - a = 1$, ya que . Esto implica que

$$\sigma^i(a) = a + i$$

y todos estos elementos son distintos, por lo que el grado de a es al menos p, y por tanto es un elemento primitivo de la extensión, $K = k(a)$.

$$\sigma(a^p - a) = \sigma(a^p) - \sigma(a) = (a+i)^p - (a+i) = a^p - a$$

Definimos $c := a^p - a \in k$, que queda fijo por σ, y a es un cero del polinomio $X^p - X - c \in k[X]$. Como el grado de a es mayor o igual a p, tenemos que este es el polinomio mínimo de a, y por lo tanto esta extensión está generada por un polinomio de Artin-Schreier.

□

Ejemplo 15. Tenemos $X^{13} - X - 1 \in \mathbb{F}_{13}[X]$. Se puede comprobar que ningún $a \in \mathbb{F}_{13}$ satisface $X^{13} - X = 1$, pues $a^{13} = a$. Entonces por el teorema anterior, este polinomio es irreducible y dada una raíz suya, el resto de sus raíces son $\alpha + i$ con $i = 1, ..., 12$. El cuerpo de descomposición del polinomio es $\mathbb{F}_{13}(\alpha)$, se tiene que $Gal(\mathbb{F}_{13}(\alpha)/\mathbb{F}_{13}) = C_{13}$ y su grado es $[\mathbb{F}_{13}(\alpha) : \mathbb{F}_{13}] = 13$.

4.2.2 Solubilidad de extensiones finitas normales

Definición. Decimos que una extensión E/k es ***radical*** si se genera añadiendo elementos que sean raíces m-ésimas , es decir,

$$k = E_0 \subset E_1 \subset \cdots \subset E_n = E$$

donde $E_{i+1} = E_i(\alpha_{i+1})$ con $\alpha_{i+1}^{m_i} \in E_i$

La propiedad de ser radical es muy útil, pues ayuda a poder expresar los ceros de un polinomio mediante radicales, es decir, mediante expresiones con suma, multiplicación, división y raíces. En característica 0, Galois demuestra que estas extensiones son exactamente aquellas que generan un grupo de Galois con extensiones intermedias con grupos cíclicos abelianos. Este es el denominado Teorema de Galois de solubilidad. Dicha propiedad de grupos es la llamada:

Definición. Un grupo es ***soluble*** si existe una cadena de subgrupos

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

donde $G_i \triangleleft G_{i+1}$, y el grupo cociente G_{i+1}/G_i es abeliano.

Dicha cadena de subgrupos se llama una serie abeliana normal.

Definición. Una extensión finita K/k se dice soluble (Galois) si K admite una extensión de Galois E con grupo de Galois soluble.

Definición. Se dice que un polinomio $f(X) \in k[x]$ es soluble por radicales si la extensión K como cuerpo de descomposición de $f(X)$ es radical.

Esta definición hace que el Teorema de Galois de solubilidad falle en característica positiva, pues surgen dos inconsistencias al aplicarlo sobre estas. Como ya hemos visto antes, los polinomios de Artin-Schreier generan extensiones cíclicas pero no son radicales, así que no estarían incluidos a pesar de tener grupo soluble. Además, para su demostración, se asume que la extensión es separable y se utiliza esta propiedad para demostrar dicho teorema con la Correspondencia de Galois separable, así que no se puede aplicar a extensiones inseparables. Por ello, para demostrar un análogo en característica positiva, la definición de extensión soluble por radicales se extiende generalmente para admitir la primera excepción, pero se restringe para no incluir extensiones inseparables, y que sigan siendo extensiones de Galois.

Definición. Una extensión finita K/k de característica 0 se denomina ***soluble por radicales*** si K admite una extensión E que tiene una cadena de extensiones

$$k = E_0 \subset E_1 \subset \cdots \subset E_n = E$$

tal que en cada caso E_{i+1} se obtiene de E_i adjuntando una raíz del polinomio $X^n - a$ en el caso $car(k) = 0$.

Una extensión finita K/k de característica $p > 0$ se llama soluble por radicales a k si admite una extensión E con una cadena de extensiones tal que las extensiones E_{i+1}/E_i adjuntan elementos con polinomios mínimos de la forma

- $X^n - a$, con $a \in E_i$ y $p \nmid n$.
- $X^p - X - a$, con $a \in K$ tal que dicho polinomio sea irreducible.

Consecuentemente, con esta definición, toda extensión K/k soluble por radicales es separable y normal pues las extensiones intermedias son separables y normales. Con esta restricción ninguna extensión inseparable es soluble por radicales. Entonces, se puede realizar una demostración análoga del resultado en característica 0, ya que se puede usar la correspondencia de Galois para extensiones normales separables y queda un teorema de solubilidad de extensiones de Galois con característica arbitraria.

La motivación tras la definición de solubilidad por radicales es la cuestión de desmostrar si se puede resolver la ecuación $f(X) = 0$ mediante una formula de radicales. Como existen extensiones radicales inseparables, tiene sentido reformular esta noción para que incluya extensiones inseparables que se puedan resolver por radicales.

En este apartado vamos a basarnos en el apartado de solubilidad por radicales de *Algebra from the viewpoint of Galois Theory* de Siegfried Bosch [4], aplicando el Teorema de Correspondencia 3.1 para extender el concepto de solubilidad por radicales y solubilidad de extensiones a extensiones inseparables y poder demostrar el Teorema de Galois para extensiones normales finitas, para lo cual utilizaremos la siguiente definición de solubilidad.

Definición. Una extensión finita K/k de característica 0 se denomina ***soluble por radicales*** si K admite una extensión E que tiene una cadena de extensiones

$$k = E_0 \subset E_1 \subset \cdots \subset E_n = E$$

tal que en cada caso, E_{i+1} se obtiene de E_i adjuntando una raíz de $X^n - a$ en el caso $car(k) = 0$, es decir, la extensión es radical.

Una extensión finita K/k de característica $p > 0$ se denomina soluble por radicales si K admite una extensión E que tiene una cadena de extensiones, tal que las extensiones E_{i+1}/E_i adjuntan una raíz de un polinomio de la forma

- $X^n - a$, $a \in E_i$, es decir, la extensión es radical.
- $X^p - X - a$ irreducible con $a \in K$.

Definición. Una extensión finita K/k se dice ***soluble*** si K admite una extensión

normal E con grupo de Galois soluble.

La afirmación de que extensiones puramente inseparables son solubles es consistente con la definición de extensión soluble, pues toda extensión puramente inseparable puede tener una extensión normal con grupo de Galois soluble.

Nota 13. Sean dos cuerpos K y F con la misma característica p, se denota la unión de cuerpos $KF = K(F) = F(K)$.

Lema 4.5. *Sea una extensión finita soluble L/k y F una extensión de cuerpos arbitraria de k. Entonces, LF es soluble sobre F.*

DEMOSTRACIÓN: Sea L/k con un grupo de Galois soluble. Por el teorema de irracionalidades naturales 4.1, eligiendo $K = L'$ siendo L' la clausura normal de L, $k' = F$, $k = k$ y $K' = FL' = F(L')$, vemos que $Gal(FL'/F) \cong Gal(L'/L' \cap F) \subset Gal(L'/k)$. Todo subgrupo no trivial de un grupo soluble es soluble, por lo que por ser $Gal(L'/k)$ soluble se tiene que $Gal(FL'/F)$ también lo es, es decir, como L'/k es una extensión soluble, se tiene que LF/F es soluble. Si $Gal(FL'/F)$ fuese el grupo trivial, como FL/F es una extensión finita, es una extensión puramente inseparable y existen extensiones de esta con grupo soluble.

□

Lema 4.6. *Sean los cuerpos $k \subset E \subset K$. La extensión K/k es soluble, si y solo si E/k y K/E son solubles.*

DEMOSTRACIÓN: Si K/k es soluble, podemos suponer K/k normal y $Gal(K/k)$ soluble. Escogiendo $F = K$ y $L = E$ se tiene inmediatamente del lema anterior que $Gal(K/E) \subset Gal(K/k)$ y un subgrupo de un grupo soluble es soluble o el grupo trivial. Si $Gal(K/E)$ es el grupo trivial, K/E es puramente inseparable y se puede extender a una extensión normal finita F/E con grupo soluble. Por otra parte, E/k se puede extender a K/k, que tiene grupo de Galois soluble y es normal.

Supongamos que K/E y E/k son solubles. Entonces K/k es una extensión finita. Sea K' la clausura normal de K. Se tiene que K'/E es normal. Además por ser E/k y K/E solubles podemos suponer que $E = Nr_{E^{(*)}/k} \subset K'$ y suponemos que $Gal(E/k)$ y $Gal(K'/E)$ son solubles sin pérdida de generalidad. Sea la restricción

$$\tau : Gal(K'/k) \to Gal(E/k)$$

Como K' y E son normales, por el Teorema 3.1 se verifica que $im(\tau) \cong Gal(E/k)$ y que τ es un homomorfismo de grupos, por lo que se tiene que $im(\tau)$ es un subgrupo de $Gal(K'/k)$. Por otra parte, $ker(\tau) \cong Gal(K'/E)$ ya que los elementos que van al ker cumplen $\sigma(E) = E$, habiendo escogido E normal. Por ser τ un homomorfismo de grupos cuya imagen es un subgrupo normal de $Gal(K'/k)$, se tiene que $Gal(K'/k) = ker(\tau)im(\tau)$. Pero un grupo G es soluble y si solo si dado un subgrupo normal H, H y G/H son solubles. Por lo tanto $Gal(K'/k)$ es soluble y consecuentemente K/k

es soluble. □

Lema 4.7. *Sea una extensión finita soluble por radicales L/k y F una extensión de cuerpos arbitraria de k. Entonces, la composición de cuerpos FL es soluble por radicales sobre F.*

Demostración: Sea una cadena de extensiones solubles por radicales

$$k = E_0 \subset E_1 \subset ... \subset E_n = L'$$

con $L \subseteq L'$. Entonces, la cadena de extensiones

$$k(F) = F = E_0F \subset E_1(F) = EF_1 \subset ... \subset E_n(F) = FE_n = FL'$$

también es soluble por radicales, ya que para extender FE_i a FE_{i+1} basta con adjuntar las raíces del polinomio mínimo de la extensión E_{i+1}/E_i, que es soluble por radicales. Entonces FL también es soluble por radicales.

□

Lema 4.8. *Sean cuerpos $k \subset L \subset K$. La extensión K/k es soluble por radicales si y solo si L/k y K/L son solubles por radicales.*

Demostración: Sean L/k y K/L solubles por radicales. Sin perdida de generalidad asumimos que admiten una cadena de extensiones intermedias solubles por radicales. Se concatenan sus respectivas cadenas de extensiones intermedias para generar una cadena de extensiones entre K y k que sea soluble por radicales.

$$k = L_0 \subset L_1 \subset ... \subset L_n = L = F_0 \subset F_1 \subset ... \subset F_s = K$$

Recíprocamente, sea K/k soluble por radicales. Si L/k es soluble por radicales, K/L también lo es, basta con adjuntar a L todas las raíces de las extensiones intermedias radicales de K/k. Ahora, por definición, L/k admite una extensión K soluble por radicales luego es soluble por radicales. □

Proposición 4.9. *Toda extensión finita puramente inseparable K/k es radical, por lo tanto, soluble por radicales.*

Demostración: Sea $K = k(x_1, ..., x_n)$ una extensión finita. Al ser puramente inseparable, todos los elementos $x \in K$ cumplen que $x^{p^e} \in k$ para algún $e \in \mathbb{N}$. Esto incluye a los generadores x_i con $i = 1...n$, por lo que K es el cuerpo de descomposición del polinomio $f(X) = \prod_{i=1}^{n} X^{p^e} - x_i^{p^e}$. Además, se tiene una cadena de extensiones radicales añadiendo un x_i en cada escalón.

$$k \subset k(x_1) \subset k(x_1, x_2)... \subset k(x_1, ..., x_n) = K$$

□

Teorema 4.10. *Una extensión K/k finita es soluble por radicales si y solo si es soluble.*

DEMOSTRACIÓN: Probemos primero el caso para extensiones de Galois, es decir, extensiones normales finitas y separables.

Supongamos que K/k es soluble. Sea F la extensión de k generada al adjuntar una raíz m-ésima de la unidad, con m el producto de primos $q|[K : k]$ coprimos con $car(k)$. Por definición, F/k es soluble por radicales.

Veamos que FK/F es soluble por radicales. Por el lema 4.5 FK/F es soluble, es decir,

$$Gal(F/F) = 1 = G_0 \subset G_1 \subset ... \subset G_n = Gal(FK/K)$$

Por el Teorema de Correspondencia de Galois, hay una biyección entre estos subgrupos y una cadena de extensiones intermedias entre KF y $F^{(*)} = F$, al ser separable.

$$F = F_0 \subset F_1 \subset ... \subset F_n = FK$$

En cada caso F_{i+1}/F_i es una extensión cíclica de un orden p_i. Si $p_i \neq car(k)$, se trata de una extensión radical por el Teorema 4.3 y que F contiene todas las m raíces de la unidad, y si $p_i = car(k)$, por el teorema de Artin-Schreier se tiene que la extensión tiene que ser de la forma $F_i(\alpha) = F_{i+1}$ con α que satisface $X^{p_i} - X - a \in F_i[X]$. En ambos casos son solubles por radicales y por lo tanto FK/K es soluble por radicales. Esto implica que FK/k es soluble por radicales, ya que FK/F y F/k son solubles por radicales. Pero entonces, K/k es soluble por radicales pues se puede extender a una extensión soluble por radicales.

Ahora supongamos que K/k es soluble por radicales. Existe una cadena de extensiones

$$k = K_0 \subset K_1 \subset ... \subset K_n$$

tal que $K \subseteq K_n$ y en cada caso K_{i+1}/K_i es de la forma indicada para extensiones solubles por radicales separables. Supongamos $K = K_n$ sin pérdida de generalidad. Basta con probar que todas estas extensiones intermedias son solubles y por el Lema 4.6 también lo será K/k. Las extensiones de raíces de la unidad y de Artin-Schreier tienen grupo de Galois cíclico y abeliano por el Teorema 4.3 y el Teorema de Artin-Schreier 4.4 respectivamente. En ambos casos, dichas extensiones son solubles. El caso que falta es el caso $X^n - c$, con $p \nmid n$ en el caso que la n raíz de la únidad no está en k. Para ello, consideremos una extensión F/k que esté generada por una n-raíz de la unidad de k. Entonces F/k es soluble al ser cíclica abeliana, y FK/F también lo será. Pero entonces FK/k también lo es, y por lo tanto K/k también.

Ahora supongamos que K/k es una extensión finita arbitraria. Sin pérdida de generalidad, supongamos que K es normal.

Se tiene que $Gal(K/k) = Gal(K/k^{(*)})$. Por el Teorema de Correspondencia de Galois, existe una biyección entre extensiones intermedias de $K/k^{(*)}$ y subgrupos de $Gal(K/k)$. Veamos que si $Gal(K/k)$ es soluble, K/k es soluble por radicales. Al ser $Gal(K/k)$ soluble, existe una cadena de extensiones

$$k^{(*)} \subset E_1 \subset \cdots \subset E_n = K$$

la cual es soluble por radicales, cosa que ya hemos probado para el caso separable. Como $K/k^{(*)}$ es soluble por radicales y $k^{(*)}/k$ también por la Proposición 4.9, se tiene que K/k es soluble por radicales por el Lema 4.8.
Entonces se tiene que

$$k = k_0^{(*)} \subset k_1^{(*)} ... \subset k_n^{(*)} = k^{(*)} \subset E_1 \cdots \subset E_n = K$$

Ahora veamos la otra implicación. Sea K/k soluble por radicales. Podemos suponer que admite una cadena de extensiones solubles por radicales sin perdida de generalidad. Sea dicha cadena

$$k = E_0 \subset E_1 \cdots E_{n-1} \subset E_n = K,$$

donde $E_{i+1} = E_i(\alpha_{i+1})$, con $(\alpha_{i+1})_i^m = a_i$ con $a_i \in E_i$ o α_i, raíz de un polinomio de Artin-Schreier.

Utilizando el Lema 4.7, tomemos $F = k^{(*)}$ y $L = K$. Como $L/k = K/k$ es soluble por radicales, $FL/F = K/k^{(*)}$ también. Entonces existe una cadena soluble por radicales entre $k^{(*)}$ y K

$$k(F) = k^{(*)} \subset E_1(k^{(*)}) \subset ... \subset E_n(k^{(*)}) = FL = K$$

Entonces, por el teorema de correspondencia de Galois, tenemos que hay una cadena de subgrupos de $Gal(K/k^{(*)})$, que ya hemos probado para el caso separable que es soluble. Y por lo tanto $Gal(K/k^{(*)}) = Gal(K/k)$ es soluble.

□

Ejemplo 16. Generalizaciones de ecuaciones ya conocidas como la ecuaciones de segundo grado, tercer grado y cuarto grado nos dan ecuaciones generales $f(X^{p^e})$. Por ejemplo, $X^{2p}+aX^p+b$, donde la solución es la p^e raíz de la ecuación X^2+aX+b, cuya solución en un cuerpo de característica distinta de 2 es

$$\frac{-a \pm \sqrt{a^2+4b}}{2}$$

Así podemos calcular explícitamente las raíces del polinomio del ejemplo 9 en $\mathbb{F}_p[t_1, t_2]$, que será

$$\sqrt[p]{\frac{-t_1 \pm \sqrt{t_1^2+4t_2}}{2}}$$

Evidentemente la solución de este ejemplo ya era conocida anteriormente, pues solo hacía falta hacer un cambio de variable, pero la sutileza que añade el teorema 4.10 es que el grupo de Galois sigue siendo soluble, lo cual no es un resultado trivial. Para polinomios que mezclen factores irreducibles separables e inseparables, en los cuales no se puede hacer un cambio de variable a primera vista para ver si su polinomio reducido es soluble por radicales y resolverlo, el grupo de Galois de su cuerpo de descomposición nos sigue indicando si dicho polinomio es soluble por radicales.

Específicamente, todos los ejemplos de la sección 3 son solubles por radicales: el Ejemplo 10 es una extensión de Artin Schreier más un elemento puramente inseparable, Ejemplo 12 tiene $Gal(K/k) = K_4$ que es abeliano y por lo tanto soluble, Ejemplo 11 tiene un grupo de Galois S_3, que es soluble a pesar de no ser abeliano, y en el Ejemplo 13 $Gal(K/k) = C_4 \times C_2$ también es soluble. De hecho, todo polinomio con grupo de Galois de orden menor que 60 será soluble por radicales, pues A_5 es el menor grupo finito no soluble.

Conclusión

El Teorema de Correspondencia 3.1 es una ampliación natural del teorema de de Correspondencia para extensiones de Galois. Si bien la tendencia a favorecer la utilización única de extensiones de Galois está justificada en la influencia del estudio de las extensiones de números racionales, estudiar la Teoría de Galois desde un punto de vista más general a través de la separabilidad proporciona claridad sobre lo que está ocurriendo con la biyección, y no se pierde ni la simplicidad ni la elegancia del resultado original.

Su aplicación a extensiones normales finitas resulta análogo a las extensiones de Galois. En consecuencia, es capaz de extender resultados clásicos a todo tipo de extensiones normales finitas sin necesidad de utilizar una base matemática más compleja, como hemos visto con la solubilidad, que siguen teniendo grupo de Galois no necesariamente trivial, lo que proporciona una cantidad de información sustancial. Otros resultados seguidos de la Correspondencia de Galois también se podrán extender de forma similar, con la debida precisión. Una continuación posible de este trabajo sería estudiar cuáles de ellos se pueden ampliar.

A Apéndice

A.1 Caracteres de grupos

Definición. Sea G un grupo y K un cuerpo. Un K-carácter de G es un homomorfismo de grupos $\chi : G \longrightarrow K^*$.

Proposición A.1. *Caracteres distintos de un grupo G sobre K son linealmente independientes sobre el K-espacio vectorial $Map(G, K)$ de funciones de G a K.*

Demostración: Deducimos por reducción al absurdo. Suponemos que existe $n \in \mathbb{N}$, el mínimo valor tal que caracteres distintos χ_i con $i = 1, ..., n$ son linealmente dependientes sobre G. Se tiene que $n \geq 2$ pues χ no puede ser la función nula. Sea

$$\chi(e) = a\chi_1(e) + ... + a_n\chi_n(e) = 0 \quad \forall\, e \in G$$

con coeficientes $a_i \in K$ no nulos. Ahora evaluamos la función para gh, con $g, h \in G$, eligiendo g con la propiedad $\chi_1(g) \neq \chi_2(g)$, que existe ya que las funciones son distintas.

$$\chi(gh) = a\chi_1(gh) + ... + a_n\chi_n(gh) = a\chi_1(g)\chi(h) + ... + a_n\chi_n(g)\chi_n(h) = 0$$

Como h es un valor arbitrario se tiene que se cumple la ecuación para todo $h \in G$. Entonces tenemos

$$\chi_1(g)\chi(h) - \chi(gh) = a_2(\chi_1(g) - \chi_2(g))\chi_2 + ... + a_n(\chi_1(g) - \chi_n(g))\chi_n = 0$$

Sin embargo, en esta diferencia, que no es trivialmente 0 ya que $a_2(\chi_1(g) - \chi_2(g)) \neq 0$ se tienen solo $n - 1$ caracteres, lo cual implicaría que existe una base dependiente de $n - 1$ caracteres, contradiciendo que n es minimal.

□

A.2 Norma y traza

Definición. Sea K/k una extensión finita de cuerpos. Para $a \in K$, definimos el endomorfismo de K como un k-espacio vectorial

$$\varphi_a : K \to K$$

$$x \mapsto ax$$

φ_a como endomorfismo de un espacio vectorial tiene una matriz característica A_{φ_a}.

Definimos

$$tr_{K/k}(a) := traza(\varphi_a)$$

$$N_{K/k}(a) := det(\varphi_a)$$

como la ***traza*** y la ***norma*** de la extensión K/k respectivamente.

Nota 14. La traza y la norma son homomorfismos de k-espacio vectorial y grupo multiplicativo respectivamente.

Lema A.2. *Sea una extensión finita K/k con $n = [K : k]$ y $a \in K$.*

1. *Si $a \in k$ se tiene $tr_{K/k}(a) = na$.*

2. *Si $a \in k$ se tiene $N_{K/k}(a) = a^n$.*

3. *Si $K = k(a)$ y $f(X) = \sum_{i=0}^{n} c_i X^i$ su polinomio mínimo. Se tiene*

$$tr_{K/k}(a) = -c_{n-1} \qquad\qquad N_{K/k}(a) = (-1)^n c_0$$

Demostración:

1. La matriz característica de φ_a es D, una matriz diagonal con todos los $d_{ii} = a$, por lo que $tr_{K/k}(a) = traza(D) = a + a + ... + a = an$.
2. Análogamente a la demostración anterior, $N_{K/k}(a) = det(D) = a^n$.
3. Sea a tal que $K = k(a)$. El polinomio mínimo $p(X)$ del endomorfismo φ_a coincide de polinomio mínimo de a. Entonces, como $p(X)$ es el polinomio característico del endomorfismo se satisfacen las igualdades $tr_{K/k}(a) = traza(\varphi_a) = -c_{n-1}$ y $N_{K/k}(a) = det(\varphi_a) = (-1)^n c_0$.

□

Lema A.3. *Sea $a \in K$, una extensión finita K/k y sea $r = [K : k(a)]$. Se tiene*

$$tr_{K/k}(a) = r \cdot tr_{k(a)/k}(a)$$

$$N_{K/k}(a) = (N_{k(a)/k}(a))^r$$

Demostración: Sea una k-base vectorial $\{x_1, ..., x_s\}$ de $k(a)$ y una $k(a)$-base vectorial de K $\{y_1, ..., y_r\}$. Los productos $x_i y_j$ forman una k-base de K. Sea $A \in K^{s \times s}$ la matriz característica de φ_a de $K(a)/k$ con dicha base vectorial. Entonces, la matriz característica de φ_a sobre K/k con la base vectorial $x_i y_j$ es de la forma

$$C = \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix}$$

con r cajas A. Entonces se tiene

$$tr_{K/k}(a) = traza(C) = r \cdot traza(A) = r \cdot tr_{k(a)/k}(a)$$

$$N_{K/k}(a) = det(C) = (det(A))^r = (N_{k(a)/k}(a))^r$$

□

Proposición A.4. *Sea K/k una extensión finita de grado $[K : k] = n_0 p^e$, con factor de separabilidad n_0. Sean $\sigma_1, ..., \sigma_n$ los elementos de $Gal(K/k)$, se cumplen las siguientes formulas para todo $a \in K$*

$$tr_{K/k}(a) = p^e \sum_{i=1}^{n_0} \sigma_i(a)$$

$$N_{K/k}(a) = \left(\prod_{i=1}^{n_0} \sigma_i(a) \right)^{p^e}$$

DEMOSTRACIÓN: Supongamos $a \in k$. Para todo i se da $\sigma_i(a) = a$. Como consecuencia del lema anterior tenemos

$$tr_{K/k}(a) = [K : k] \cdot a = p^e(n_0 a) = p^e \sum_{i=1}^{n_0} \sigma_i(a)$$

$$N_{K/k}(a) = a^{n_0 p^e} = (a^{n_0})^{p^e} = \left(\prod_{i=1}^{n_0} \sigma_i(a) \right)^{p^e}$$

.

Ahora supongamos que existe a tal que $K = k(a)$. Podemos aplicar el lema A.2 otra vez y vemos que el polinomio mínimo irreducible admite la factorización por la Proposición 2.11:

$$\sum_{i=1}^{n_0} (X - \sigma_i(a))^{p^e}$$

Entonces,

$$tr_{K/k}(a) = -c_1 = p^e \sum_{i=1}^{n_0} \sigma_i(a)$$

$$N_{K/k}(a) = (-1)^n c_n = (-1)^n (-1)^n \left(\prod_{i=1}^{n_0} \sigma_i(a) \right)^{p^e}$$

Ahora sea $a \in K$ arbitrario. Consideremos la cadena de extensiones $k \subset k(a) \subset K$. Utilizamos el lema A.3, que da

$$tr_{K/k}(a) = [K : k(a)] tr_{k(a)/k}(a) = tr_{k(a)/k}([K : k(a)]a) = tr_{k(a)/k}(tr_{K/k(a)}(a))$$

$$N_{K/k(a)}(a) = (N_{k(a)/k}(a))^{[K:k(a)]} = N_{k(a)/k}(a^{[K:k(a)]}) = N_{k(a)/k}(N_{K/k(a)}(a))$$

Denotando las formulas del enunciado como

$$tr'_{K/k}(a) = p^e \sum_{i=1}^{n_0} \sigma_i(a)$$

$$N'_{K/k}(a) = \left(\prod_{i=1}^{n_0} \sigma_i(a) \right)^{p^e}$$

y utilizando el caso anterior, que ya tenemos demostrado que son iguales a $tr_{k(a)/a}(a)$ y $N_{k(a)/k}$, y las ecuaciones

$$tr_{K/k}(a) = tr_{k(a)/k}(tr_{K/k(a)}(a)) = tr'_{k(a)/k}(tr'_{K/k(a)}(a))$$

$$N_{K/k(a)}(a) = N_{k(a)/k}(N_{K/k(a)}(a)) = N'_{k(a)/k}(N'_{K/k(a)}(a))$$

Falta demostrar la transitividad de las formulas como una función de a, es decir, queremos probar que dada una extensión intermedia $k \subset L \subset K$

$$tr'_{K/k}(a) = tr'_{L/k} \circ tr'_{K/L}$$

$$N'_{K/k}(a) = N'_{L/k} \circ N'_{K/L}$$

Entonces, tendremos la igualdad.

Se tiene por la formula de la multiplicación y por la Proposición 2.33 que

$$[K : k] = [K : L][L : k] = [K : L]_i[K : L]_s[L : k]_i[L : k]_s = p^{e_1+e_2}[K : k]_s$$

Sea $\sigma_i \in Gal(L/k)$ y $\tau_j \in Gal(K/L)$, se tiene que una base de $Gal(K/k)$ es de la forma $\sigma'_i \circ \tau_j$, con σ'_i la extensión de σ_i a la clausura algebraica $\overline{K}$. Una explicación a fondo de este hecho es consecuencia del teorema 3.6/9 de la referencia [4]. Entonces la transitividad se da inmediatamente.

□

Corolario A.5. *Se tiene que $tr_{K/k}(a) = 0$ si la extensión es inseparable.*

Corolario A.6. *La traza y norma de la extensión son funciones transitivas, es decir, para una extensión finita $k \subset L \subset K$*

$$tr_{K/k}(a) = tr_{L/k} \circ tr_{K/L}$$

$$N_{K/k}(a) = N_{L/k} \circ N_{K/L}$$

Corolario A.7. *Sea una extensión finita separable normal. Entonces, la traza y la norma de la extensión son compatibles con los k-automorfismos de $Gal(K/k)$, es decir:*

$$tr_{K/k}(a) = tr_{K/k}(\sigma(a))$$

$$N_{K/k}(a) = N_{K/k}(\sigma(a))$$

para todo $a \in K$, $\sigma \in Gal(K/k)$.

Teorema A.8. *Nonagésimo teorema de Hilbert (versión multiplicativa). Sea K/k un una extensión separable cíclica y sea $\sigma \in Gal(K/k)$ un elemento generador de la misma. Entonces, para $b \in K$ las condiciones son equivalentes:*

1. $N_{K/k}(b) = 1$

2. *existe $a \in K^*$ tal que $b = a \cdot \sigma(a)^{-1}$*

Demostración:
Sea $b \in K$ tal que $N_{K/k}(b) = 1$. Dados $n = [K : k]$ y la función

$$\begin{gathered} \varphi : L \longrightarrow L \\ a \longmapsto \sigma^0(a) + b\sigma(a) + b\sigma(b)\sigma^2(a) + ... + b\sigma(b)...\sigma^{n-2}(b)\sigma^{n-1}(a) \end{gathered}$$

debe existir un elemento c tal que $\varphi(c) \neq 0$ por la independencia lineal de los caracteres de $Gal(K/k)$.

Por la separabilidad de la extensión y la formula de la Proposición A.4 se verifica que $N_{K/k}(b) = \sigma(b) \cdot ... \cdot \sigma^{n-1}(b)$, tenemos que $b \cdot \sigma(\varphi(c)) = N_{K/k}(b) \cdot \varphi(c) = \varphi(c)$. Despejando b nos queda la igualdad deseada.

Veamos la otra implicación. Si $b = a \cdot \sigma(a)^{-1}$ para algún $a \in K^*$, tenemos por A.7

$$N_{K/k}(b) = N_{K/k}(a\sigma^{-1}(a)) = N_{K/k}(a)N_{K/k}(\sigma^{-1}(a)) = \frac{N_{K/k}(a)}{N_{K/k}(\sigma(a))} = 1.$$

□

Teorema A.9. *Teorema 90 de Hilbert (versión aditiva). Sea K/k una extensión cíclica finita separable y $\sigma \in Gal(K/k)$ un elemento generador del grupo. Se cumplen las condiciones equivalentes, para algún $b \in K$:*

1. $tr_{K/k}(b) = 0$

2. *Existe $a \in K$ tal que $b = a - \sigma(a)$*

Demostración:
Si $b = a - \sigma(a)$ para algún a, se tiene

$$tr_{K/k}(b) = tr_{K/k}(a - \sigma(a)) = tr_{K/k}(a) - tr_{K/k}(\sigma(a)) = 0$$

Ahora, sea b con $tr_{K/k}(b) = 0$ y sea $n = [K : k]$. La traza no es una función idénticamente nula por A.1 y A.4, así que existe $y \in K$ tal que $tr_{K/k}(y) \neq 0$. Definimos un elemento a tal que

$$a(tr_{K/k}(y)) = b \cdot \sigma(y) + (b + \sigma(b)) \cdot \sigma^2(y) + ... + (b + \sigma(b)... + \sigma^{n-2}(b))\sigma^{n-1}(y)$$

El elemento $a \in K$ ya que es la división de dos elementos no nulos de K. Aplicando σ a dicha multiplicación y como K/k es separable, $tr_{K/k}(y)$ queda fijo bajo

automorfismos por la Proposición A.4 y el Corolario A.7, nos queda

$$\begin{aligned}\sigma(a(tr_{K/k}(y))) &= \sigma(a)tr_{K/k}(y)\\ &= \sigma(b)\cdot\sigma^2(y) + (\sigma(b)+\sigma^2(b))\cdot\sigma^3(c) + ... + \sigma(b + ... + \sigma^{n-2}(b))\sigma^n(y)\end{aligned}$$

Ahora, teniendo en cuenta que $\sigma^n = id$ y que $tr_{K/k}(b) = 0$, se puede sustituir en la ecuación :

$$\begin{aligned}(a-\sigma(a))tr_{K/k}(y) &= b\sigma(y) + b\sigma^2(y) + ... + b\sigma^{n-1}(y) - (\sigma(b) + ... + \sigma^{n-1}(b))\sigma^n(y)\\ &= b\cdot(\sigma(y) + ... + \sigma^{n-1}(y)) - (-\sigma^n(b))y\\ &= b\cdot(\sigma(y) + ... + \sigma^{n-1}(y) + y)\\ &= b\cdot tr_{K/k}(y)\end{aligned}$$

Por lo que $(a - \sigma(a)) = b$

□

Bibliografía

Referencias

[1] Emil Artin, *Galois Theory*, Dover Books, second edition 1964.

[2] Manuel Jesús Soto Prieto, Notas privadas

[3] Nicolas Bourbaki, *Algèbre Chapitre 5-7*, Springer,2006.

[4] Siegfried Bosch, *Algebra from the viewpoint of Galois Theory*, Birkhäuser, 2018.

[5] Stephen Shatz and Jean Gallier, *Algebra*, University of Pennsilvania, 2017.

[6] B.L. van der Waerden, *Algebra volume I*, Springer, 2003.

[7] Steven Roman, *Field Theory*, Second edition, Springer, 2006.

[8] Serge Lang, *Algebra*, Springer, Third edition, 2002.