Grupos de Galois de Campos Finitos

Pablo García Román

2010

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

"GRUPOS DE GALOIS DE CAMPOS FINITOS"

TÍTULO DE : MATEMÁTICO

PRESENTA: GARCÍA ROMÁN PABLO

2010

García
Román
Pablo
58-32-17-53
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas

Jurado

Dra.
Eugenia
O´Reilly
Regueiro

Dr.
Hugo Alberto
Rincón
Mejía

Dr.
José
Ríos
Montes

Dra.
Alejandro Javier
Díaz Barriga
Casales

Dr.
Alejandro
Alvarado
García

Grupos de Galois de Campos Finitos
31 p
2010

A mi Mamá

A Bety y Toña

A Yamili, Sarai y Abraham

A Ali

A mi familia

Índice general

Introducción

En el Renacimiento italiano se encuentra la fórmula para resolver la ecuación general de cuarto grado. Es una expresión en las que solamente intervienen los coeficientes de la ecuación y raíces hasta de exponente cuarto. Este resultado extiende lo que sucede con las ecuaciones de grado 2 y 3 (en cuya solución general hay raíces de exponentes 2 y 3 respectivamente). Acababa el siglo XVIII cuando Gauss $(1777-1855)$ presentó en 1799 su tesis doctoral en la que aparecía el *Teorema Fundamental del Álgebra* que establece de forma rigurosa que toda ecuación polinómica con coeficientes reales se puede descomponer de forma única como producto de factores de primero y segundo grados, y en consecuencia que toda ecuación de ese tipo tiene al menos una raíz (real o imaginaria). Este era un resultado general pero que no establecía el método efectivo de hallar esas raíces. Vistos los datos anteriores era una hipótesis razonable pensar que una ecuación de quinto grado tendría cinco soluciones reales o imaginarias, diferentes o repetidas; pero no se había encontrado la fórmula para encontrarlas, aunque, caso de que la hubiera, también era razonable suponer que contendría raíces de grado cinco. Y, generalizando un poco, que las de grado seis se resolverían con raíces sextas, las de grado siete con raíces de ese mismo grado y así sucesivamente. Era cuestión de ponerse a trabajar para encontrar la solución de la ecuación de quinto grado y después seguir. Se dedicaron a ello muchos grandes matemáticos de la época, como Lagrange $(1736-1813)$, Cauchy $(1789-1857)$ y sobre todo Ruffini $(1765-1822)$ que fue el que más avanzó hacia el resultado final, aunque no llegó a completarlo. Esa sería la labor de Abel $(1802-29)$ que en el año de 1823 (cuando tenía 21 años) obtuvo el resultado definitivo: la ecuación general de quinto grado no era soluble por radicales, ni de índice cinco ni de ningún otro. Con eso se daba un paso importante al cerrar el problema de la búsqueda de fórmulas de solución. Todavía quedaban otros aspectos importantes por abordar, en particular las condiciones que debían cumplir ecuaciones particulares para que sí se pudieran resolver. La forma en que Abel 'resolvió' el problema de la solución de la ecuación general de quinto grado demostrando su imposibilidad, fue la primera vez en la historia en que un problema tenía este final, y sería el inicio de una larga lista de demostraciones de imposibilidades. Hasta ese momento cuando un problema no se sabía

resolver se consideraba que era porque no se seguía el camino apropiado o porque no se tenían los instrumentos necesarios para resolverlo, pero se tenía el convencimiento de que antes o después se lograría resolver.

La contribución genial de Galois a la teoría de solución de ecuaciones fue la determinación de las condiciones en las que una ecuación es soluble por radicales, lo que da como consecuencia que para todo $n > 4$ haya ecuaciones polinómicas que no son solubles por radicales. En esencia el resultado de Galois sobre solubilidad por radicales de una ecuación tiene que ver con una serie de subgrupos (de un tipo especial llamados normales) del grupo de permutaciones, cada uno subgrupo del anterior, asociados a lo que llama Galois *resolventes* de la ecuación. Basten las pocas líneas anteriores para mostrar la aportación de Galois a la teoría de resolución de ecuaciones, que fue de tal calibre que acabó con el propio objeto del álgebra, pasando a partir de sus resultados a poner el acento en el estudio de las estructuras algebraicas. Así comienza lo que aún hoy se conoce como *Matemáticas modernas*, de las que la *Teoría de Galois* sigue siendo una parte plenamente vigente. El presente trabajo comienza introduciendo los resultados básicos de la teoría de anillos, necesarios para la teoría de Galois. El capitulo siguiente forma el cuerpo principal del trabajo, el cual esta dedicado a calcular los *Grupos de Galois de Campos Finitos*.

Pablo García Román

Capítulo 1

Preliminares

1.1. Definiciones

Todos los anillos considerados tienen 1 y casi todos serán conmutativos.

Definición 1.1.1. *Un subgrupo I de R que satisface $rI \subseteq I$, para todo $r \in R$ es un ideal izquierdo de R y uno que satisface $Ir \subseteq I$, para todo $r \in R$ es un ideal derecho de R. Un ideal que es derecho e izquierdo se llama ideal bilateral o simplemente ideal.*

Observación 1.1.2. *Cuando el anillo es conmutativo todo ideal es bilateral.*

Definición 1.1.3. *Un ideal I de un anillo R es propio si $I \neq R$, o de forma equivalente si $I \subsetneq R$*

Definición 1.1.4. *Un anillo conmutativo R en el cual no existen divisores de cero, es llamado un dominio entero, es decir, para $u, v \in R$, $uv = 0$ implica que $u = 0$ o $v = 0$.*

Definición 1.1.5. *Sea R un anillo. Un ideal máximo de R es un ideal $I \subsetneq R$ tal que para cualquier otro ideal M de R, con $I \subseteq M \subseteq R$ se tiene que $I = M$ o $M = R$.*

Teorema 1.1.6 (ver [**?**])**.** *Sea R un anillo conmutativo. Entonces I es un ideal máximo de R si y sólo si R/I es un campo.*

Definición 1.1.7. *Sea R un anillo conmutativo. Un ideal $I \subsetneq R$ se llama primo si siempre que $ab \in I$, se tiene que $a \in I$ o $b \in I$, para todas $a, b \in R$.*

Teorema 1.1.8 (ver [**?**])**.** *Sea R un anillo conmutativo. Un ideal $I \subsetneq R$ es primo si y sólo si R/I es un dominio entero.*

Definición 1.1.9. *Si R es un anillo conmutativo y $a \in R$, el ideal $\{ra : r \in R\}$ de todos los múltiplos de a es el ideal principal generado por a y es denotado por $\langle a \rangle$. Un ideal I de R es un ideal principal si $I = \langle a \rangle$, para algún $a \in R$.*

Proposición 1.1.10 (ver [?])**.** *Sea R un anillo conmutativo con cancelación y sean $a, b \in R$. Entonces $\langle a \rangle = \langle b \rangle$ si y sólo si $a = bc$, para algún elemento invertible $c \in R$.*

Para cualquier anillo R (no necesariamente conmutativo) con unidad, existe un importante homomorfismo de anillos $\eta : \mathbb{Z} \to R$ llamado el *homomorfismo unidad o característico*, el cual esta definido por

$$\eta(n) = n \cdot 1 = \begin{cases} 1 + 1 + \cdots + 1 (n - sumandos), & \text{n}> 0; \\ 0, & \text{n}= 0; \\ -(1 + 1 + \cdots + 1), & \text{n}< 0. \end{cases}$$

Ya que $0 \neq 1 \in R$, $Nuc(\eta)$ es un ideal propio de $\mathbb{Z}$ y usando los Teoremas de Isomorfismos vemos que existe un monomorfismo cociente $\bar{\eta} : \mathbb{Z}/Nuc(\eta) \to R$, el cual nos lleva a identificar el anillo cociente $\mathbb{Z}/Nuc(\eta)$ con la imagen $\eta\mathbb{Z} \subseteq R$ como un subanillo de R. Como $\mathbb{Z}$ es un dominio de ideales principales, existe un único entero no negativo $p \geq 0$ tal que $Nuc(\eta) = \langle p \rangle$; a tal p se le llama la *característica* de R y se le denota $car(R)$.

Lema 1.1.11 (ver [?])**.** *Si R es un dominio entero, su característica, $car(R)$ es un primo.*

Observación 1.1.12. *Cuando se habla de una anillo con unidad R, podemos considerar que contiene un subanillo de la forma $\mathbb{Z}/\langle car(R) \rangle$, como el homomorfismo cociente $\bar{\eta} : \mathbb{Z}/\langle car(R) \rangle \longrightarrow R$ da un isomorfismo $\mathbb{Z}/\langle car(R) \rangle \longrightarrow Im(\eta)$, esto nos permite identificar dichos anillos. En particular cada dominio entero contiene como un subanillo a $\mathbb{Z} = \mathbb{Z}/\langle 0 \rangle$, si $car(R) = 0$ o $\mathbb{Z}/\langle p \rangle$, si $p = car(R) > 0$. Este subanillo es llamado algunas veces el subanillo característico de R. Cuando consideramos dominios enteros, los anillos $\mathbb{Z}$ y $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}/\langle p \rangle$, para $p > 0$ un primo, son llamados anillos primos.*

Para el anillo de polinomios $k[x]$, donde k es un campo tenemos los siguientes resultados.

Teorema 1.1.13 (ver [?])**.** *$p(x) \in k[x]$ es irreducible si y sólo si $\langle p(x) \rangle$ es ideal máximo.*

Corolario 1.1.14 (ver [?])**.** *El número de raíces distintas de un polinomio no constante $f(x) \in k[x]$ es a lo más $grad(f(x))$.*

1.2. Campos

Definición 1.2.1. *Sean K y k campos. Se dice que K que es una extensión de k, si k es subcampo de K.*

Notación 1.2.2. *Si K es una extensión de k, usaremos la notación K/k.*

Recordemos que si k y K son campos, todo morfismo de campos $\phi : k \to K$ (por definición, $\phi(1) = 1$) es inyectivo, ya que $Nuc(\phi) \subseteq k$ es un ideal y como k es campo sus únicos ideales son el 0 y el total, y como $\phi(1) = 1 \neq 0$, entonces $Nuc(\phi) = 0$.

En realidad se puede dar la definición 1.2.1. de una manera mas general:

Definición 1.2.3. *Sean K y k campos. K es una extensión de k si existe un monomorfismo de k en K.*

Observación 1.2.4. *Dada una extensión K/k, podemos ver a K como espacio vectorial sobre k y como tal, tiene una dimensión.*

Definición 1.2.5. *Sea K extensión de k, a la dimensión de K sobre k se le llama el grado de K sobre k y es denotada por $[K : k] = dim_k K$.*

Definición 1.2.6. *Una extensión K de k es una extensión finita de k si $[K : k]$ es finito.*

Definición 1.2.7. *Dadas dos extensiones K/k y L/K, decimos que K/k es una subextensión de L/K y algunas veces escribiremos $K/k \leq L/K$.*

Teorema 1.2.8 (ver [?])**.** *Sea L extensión finita de K y sea K extensión finita de k, entonces L es extensión finita de k y $[L : k] = [L : K][K : k]$.*

Definición 1.2.9. *Sea K extensión de k y sea $S \subseteq K$ un subconjunto. Sea $\mathcal{A}$ la familia de subcampos de K que contienen a k y a S. Esta familia de subcampos de K es no vacía ya que $K \in \mathcal{A}$. El subcampo $k(S) = \bigcap_{E \in \mathcal{A}} E$ se llama el campo obtenido al adjuntar S a k.*

Claramente $k \subseteq k(S) \subseteq K$ y $k(S)$ es el menor subcampo de K que contiene a k y a S. Si $S = \{a_1, ..., a_n\} \subseteq K$ es un conjunto finito, usaremos la notación

$$k(\{a_1, ..., a_n\}) = k(a_1, ..., a_n).$$

En particular, si $S = \{a\} \subseteq K$, diremos que $k(a)$ es una *extensión simple* de k. Comenzamos describiendo internamente estas extensiones simples.

Proposición 1.2.10 (ver [?])**.** *Sean K extensión de k y $a \in K$. Sea $k(a)/k$ la extensión simple obtenida al adjuntar a a k. Entonces,*

$$k(a) = \left\{ \tfrac{f(a)}{g(a)} : f(x), g(x) \in k[x] \quad y \quad g(a) \neq 0 \right\}$$

Una vez obtenida esta descripción interna de las extensiones simples, comenzaremos con su clasificación.

Definición 1.2.11. *Sea K extensión de k. Un elemento $a \in K$ se llama algebraico sobre k, si existe $0 \neq f(x) \in k[x]$ tal que $f(a) = 0$. Si a no es algebraico sobre k, decimos que a es trascendente sobre k.*

Definición 1.2.12. *Sea K extensión de k. Decimos que K es extensión algebraica de k si todo elemento de K es algebraico sobre k.*

Teorema 1.2.13 (ver [?])**.** *Toda extensión finita de k es algebraica.*

Consideremos ahora un elemento $a \in K$ algebraico sobre k. Por definición existe un polinomio

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in k[x]$$

con $a_n \neq 0$ tal que $f(a) = 0$. Si ahora dividimos $f(x)$ por a_n, se obtiene un polinomio

$$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in k[x]$$

con $b_j = a_j/a_n \in k$ y claramente $g(a) = 0$. Así, si $a \in K$ es algebraico sobre k, entonces a es raíz de un polinomio mónico no constante en $k[x]$. Ahora, si $a \in K$ es algebraico sobre k, del conjunto de polinomios mónicos de $k[x]$ del cual a es raíz, por el principio del buen orden en $\mathbb{N}$, existe uno de menor grado. Denotemos a este polinomio por $p(x) \in k[x]$.

Teorema 1.2.14 (ver [?])**.** *El polinomio mónico de menor grado $p(x) \in k[x]$ del cual $a \in K$ es raíz, es único. Más aún, $p(x)$ es irreducible en $k[x]$ y $p(x)$ divide a cualquier otro polinomio $q(x) \in k[x]$ del cual a es raíz.*

Notación 1.2.15. *A $p(x)$ se le llama el polinomio irreducible de a y se le denota $Irr(a, k)$.*

Definición 1.2.16. *Sea K una extensión finita de k. Un elemento $u \in K$ para el cual $K = k(u)$ es llamado un elemento primitivo para la extensión K/k.*

Más adelante veremos que cuando $car(k) = 0$, cada extensión finita K/k tiene un elemento primitivo.

Teorema 1.2.17 (ver [?])**.** *Sea K extensión de k y sea $a \in K$ algebraico sobre k. Entonces $k(a) = \{r(a) : r(x) \in k[x], grado(r(x)) < grado(Irr(a, k))\}$, donde $r(a) = s(a) \Leftrightarrow r(x) = s(x)$. Esto es, cada elemento β de $k(a)$ se expresa de manera única como $\beta = r(a)$, con $grado(r(x)) < grado(Irr(a, k))$.*

Corolario 1.2.18 (ver [?])**.** *Sean K extensión de k y $a \in K$. Si a es algebraico sobre k, entonces $k(a)$ es una extensión finita de k y por lo tanto algebraica. De hecho $[k(a) : k] = grad(Irr(a, k))$.*

Corolario 1.2.19 (ver [?]). *Sea K extensión de k y supongamos que $a_1, ..., a_n \in K$ son algebraicos sobre k. Entonces $k(a_1, ...a_n)$ es una extensión finita de k y por lo tanto algebraica.*

Corolario 1.2.20 (ver [?]). *Sea K extensión de k y sean $a, b \in K$ algebraicos sobre k. Entonces $a+b, a-b, a\cdot b, \frac{a}{b}$ con $b \neq 0$ son algebraicos sobre k.*

Proposición 1.2.21 (ver [?]). *Sean L/K y K/k extensiones algebraicas. Entonces la extensión L/k es algebraica.*

Definición 1.2.22. *Para una extensión L/K, sea*

$$L^{alg} = \{a \in L : a \ \ es \ \ algebraico \ \ sobre \ \ K\} \subseteq L.$$

Proposición 1.2.23 (ver [?]). *Para una extensión L/K, L^{alg} es un subcampo que contiene a K y L^{alg}/K es algebraica.*

El estudio de los *automorfismos* de un campo, es fundamental en la Teoría de Galois.

Definición 1.2.24. *Sean K, L extensiones de k. Un isomorfismo $\sigma : K \longrightarrow L$ es llamado un $k-isomorfismo$, si $\sigma(a) = a$, para toda $a \in k$. Si existe un $k-isomorfismo$ de K en L, se dice que K y L son $k-isomorfos$.*

Definición 1.2.25. *Sea K una extensión de k y sean $a, b \in K$, los cuales son algebraicos sobre k. Si $Irr(a,k) = Irr(b,k)$, diremos que a y b son conjugados sobre k o son k-conjugados.*

Teorema 1.2.26. *Sea K extensión de k y sean $a, b \in K$ conjugados sobre k. Entonces $k(a)$ y $k(b)$ son k-isomorfos. De hecho, existe un k-isomorfismo $\sigma : k(a) \longrightarrow k(b)$ tal que $\sigma(a) = b$.*

Teorema 1.2.27 (ver [?]). *Sea $p(x) \in k[x]$ un polinomio irreducible no constante. Si K y L son extensiones de k las cuales contienen raíces a y b de $p(x)$ respectivamente, entonces existe un k-isomorfismo $\varphi : k(a) \longrightarrow k(b)$ tal que $\varphi(a) = b$.*

1.3. Campos de Descomposición y el Teorema de Kronecker

Sea K campo y sea $f(x) \in K[x]$.

Definición 1.3.1. *Si E es una extensión de K, donde $f(x)$ se puede factorizar como producto de factores lineales, decimos que $f(x)$ se descompone en $E[x]$. Así si $f(x)$ se descompone en $E[x]$ tenemos $f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$, donde $a_i \in E, i = 1, ..., n$.*

Por supuesto, si tenemos un campo como E, entonces las distintas raíces $a_1, a_2, ..., a_n$ de $f(x)$ en E, generan un subcampo $K(a_1, a_2, ..., a_n) \leq E$ el cual es el subcampo más pequeño de E para el cual $f(x)$ se factoriza en factores lineales en $E[x]$.

Teorema 1.3.2. *(Teorema de Kronecker: primera versión)[ver [?]]. Sean k un campo y $f(x) \in k[x]$ un polinomio de grado positivo. Entonces existe una extensión finita K/k para la cual, $f(x)$ tiene una raíz en K.*

Teorema 1.3.3. *(Teorema de Kronecker: segunda versión)[ver [?]]. Sean k un campo y $f(x) \in k[x]$ un polinomio de grado positivo. Entonces existe una extensión finita K/k la cual es un campo de descomposición de $f(x)$ sobre k.*

Proposición 1.3.4 (ver [?])**.** *Sean F extensión de K y $f(x) \in K[x]$. Si $E_1, E_2 \leq F$ son subcampos de descomposición para $f(x)$ sobre K, entonces $E_1 = E_2$.*

1.4. Monomorfismos entre extensiones

Definición 1.4.1. *Para extensiones F/K y L/K, sea $Mono_K(L, F)$ el conjunto de todos los monomorfismos $L \longrightarrow F$, los cuales fijan a los elementos de K, de la misma manera sea $Aut_K(F)$ el conjunto de todos los automorfismos de F los cuales fijan a los elementos de K.*

Observación 1.4.2. *Siempre tenemos que $Aut_K(F) \subseteq Mono_K(F, F)$ y $Mono_K(F, F)$ es cerrado bajo composición pero no es siempre un grupo, ya que los elementos no son necesariamente invertibles. Si F es extensión finita de K, entonces tenemos $Mono_K(F, F) = Aut_K(F)$, ya que cada transformación $K-$lineal inyectiva es suprayectiva y de este modo invertible.*

Definición 1.4.3. *Sea F/K una extensión y $f(x) \in K[x]$. Sea*

$$Roots(f, F) = \{a \in F : f(a) = 0\},$$

el conjunto de raíces de $f(x)$ en F. Este conjunto es siempre finito y puede también ser vacío (esto sucede cuando $f(x)$ no tiene raíces en F).

Supongamos que $p(x)$ es un polinomio irreducible, del cual podemos también suponer es mónico y sea F extensión de K. Entonces si $t \in F$ es una raíz de $p(x)$, el homomorfismo evaluación $\varepsilon_t : K[x] \longrightarrow F$ lo factoriza a través del monomorfismo cociente $\tilde{\varepsilon}_t : K[x]/\langle p(x)\rangle \longrightarrow F$ cuya imagen es $K(t) \leq F$. Por supuesto, existe sólo uno de tales monomorfismos para cada una de las raíces de $p(x)$ en F. Si fijamos una raíz como t_0 e

identificamos $K[x]/\langle p(x)\rangle$ con $K(t_0)$ via $\tilde{\varepsilon}_{t_0}$, entonces cada raíz de $p(x)$ en F da lugar a un monomorfismo $\varphi_t = \tilde{\varepsilon}_t \circ \tilde{\varepsilon}_{t_0}^{-1} : K(t_0) \longrightarrow F$, para el cual $\varphi_t(t_0) = t$.

Note que si $\varphi : K[x]/\langle p(x)\rangle \longrightarrow F$ es cualquier homomorfismo que extiende la función identidad sobre K, entonces la clase $x + p(x)$ debe ser enviada por φ a una raíz de $p(x)$ en F, por lo tanto cada uno de esos homomorfismos surge de esta manera. Esta discusión se resume en el siguiente resultado.

Proposición 1.4.4 (ver [?])**.** *Sea F extensión de K. Sea $p(x) \in K[x]$ un polinomio irreducible tal que $p(t_0) = 0$, con $t_0 \in F$. Entonces existe una biyección*

$$Roots(p, F) \leftrightarrow Mono_K(K(t_0), F)$$

dado por $t \leftrightarrow \varphi_t$, donde $\varphi_t : K(t_0) \to F$ cumple $\varphi_t(t_0) = t$.

Proposición 1.4.5 (ver [?])**.** *Sean F/K y L/K extensiones.*

1. *Para $p(x) \in K[x]$, cada monomorfismo $\alpha \in Mono_K(L, F)$ restringe a una función $\alpha_p : Roots(p, L) \longrightarrow Roots(p, F)$ la cual es inyectiva.*

2. *Si $\alpha \in Mono_K(L, L)$, entonces $\alpha_p : Roots(p, L) \longrightarrow Roots(p, L)$ es una biyección.*

1.5. Cerraduras Algebraicas

Definición 1.5.1. *Un campo K es algebraicamente cerrado, si no tiene extensiones algebraicas propias.*

Definición 1.5.2. *Sea K un campo. Una extensión F de K es llamada una cerradura algebraica de K, si F es algebraica sobre K y algebraicamente cerrada.*

Notación 1.5.3. *Escribimos $\bar{K}$ o $K^{alg\ \ cl}$, para referirnos a la cerradura algebraica de K.*

Teorema 1.5.4 (ver [?])**.** *Sea K un campo.*

1. *Existe una cerradura algebraica de K*

2. *Sean F_1 y F_2 cerraduras algebraicas de K. Entonces existe un isomorfismo $\varphi : F_1 \longrightarrow F_2$ el cual fija los elementos de K.*

Por lo tanto las cerraduras algebraicas son esencialmente únicas.

Existen algunas consecuencias inmediatas del Teorema 1.5.4. $E_1 \doteq E_2$ indica que para extensiones E_1/K y E_2/K existe un $K-$isomorfismo, $E_1 \longrightarrow E_2$.

Proposición 1.5.5 (ver [?]). *Sea K un campo.*

1. *Si L/K es una extensión algebraica, entonces $\bar{L} \doteq \bar{K}$.*
2. *Si L/K es una extensión, entonces también lo es $\bar{L}/K$ y $(\bar{L})^{alg} \doteq \bar{K}$.*

Existe un resultado más fuerte que el Teorema 1.5.4.(2), el *Teorema de Extensión de Monomorfismos*.

Teorema 1.5.6. *(Teorema de Extensión de Monomorfismos)[ver [?]] Sea M/K una extensión algebraica y $L/K \leq M/K$. Supongamos que $\varphi_0 : L \longrightarrow K$ es un $K-$monomorfismo. Entonces φ_0 se extiende a un monomorfismo $\varphi : M \longrightarrow \bar{K}$.*

Definición 1.5.7. *Sean $u, v \in \bar{K}$. Entonces v es conjugado para u sobre K o es un conjugado de u sobre K si existe un monomorfismo $\varphi : \bar{K} \longrightarrow \bar{K}$, para el cual $v = \varphi(u)$.*

Lema 1.5.8 (ver [?]). *Sea $p(x) = Irr(u, K)$, si $u, v \in \bar{K}$, entonces v es conjugado para u sobre K si y sólo si $p(v) = 0$.*

1.6. Multiplicidad de raíces y Separabilidad

Sea K un campo. Supongamos que $f(x) \in K[x]$ y $u \in K$ es una raíz de $f(x)$, es decir, $f(u) = 0$. Entonces podemos factorizar a $f(x)$ como $f(x) = (x - u)f_1(x)$, para algún $f_1(x) \in K[x]$.

Definición 1.6.1. *Si $f_1(u) = 0$, entonces u es una raíz multiple de $f(x)$. Si $f_1(u) \neq 0$, entonces u es una raíz simple de $f(x)$.*

Necesitamos entender más claramente cuando un polinomio irreducible tiene una raíz multiple. Consideremos la *derivada formal* en $K[x]$, es decir, la función $\partial : K[x] \longrightarrow K[x]$ dada por

$$\partial(f(x)) = f'(x) = a_1 + 2a_2x + \cdots + da_dx^{d-1},$$

donde $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$, con $a_j \in K$.

Proposición 1.6.2. *La derivada formal $\partial : K[x] \longrightarrow K[x]$ tiene las siguientes propiedades.*

1. *∂ es $K-$lineal.*
2. *∂ es una derivación, es decir, para $f(x), g(x) \in K[x]$,*

$$\partial(f(x)g(x)) = \partial(f(x))g(x) + f(x)\partial(g(x)).$$

3. *Si* $car(K) = 0$, *entonces* $Nuc(\partial) = K$ *y* ∂ *es suprayectiva.*

4. *Si* $car(K) = p$, *entonces*

$$Nuc(\partial) = \{h(x^p) : h(x) \in K[x]\}$$

y $Im(\partial)$ *es generada por los monomios* x^k, *con* $p \nmid (k+1)$.

Proposición 1.6.3 (ver [?]). *Sea* L *extensión de* K *y* $f(x) \in K[x]$ *tal que* $f(u) = 0$, *para algún* $u \in L$. *Entonces* u *es una raíz multiple de* $f(x)$ *si y sólo si* $f(x)$ *y* $f'(x)$ *tienen un factor común de grado positivo en* $K[x]$, *el cual se anula en* u.

Corolario 1.6.4 (ver [?]). *Si* $f(x)$ *es irreducible en* $K[x]$, *entonces una raíz* u *es multiple si y sólo si* $f'(u) = 0$. *En particular, esto puede ocurrir si* $car(K) > 0$.

Corolario 1.6.5 (ver [?]). *Si* $car(K) = 0$ *y* $f(x)$ *es irreducible en* $K[x]$, *entonces cada raíz de* $f(x)$ *es simple.*

Definición 1.6.6. *Un polinomio irreducible* $p(x) \in K[x]$ *es separable sobre* K *si cada raíz de* $p(x)$ *en una extensión* L/K *es simple. Por el Corolario 1.6.4, esto es equivalente a pedir que* $p'(u) \neq 0$, *para cada raíz* u *de* $p(x)$. *Si* $u \in L$ *es una raíz multiple de* $p(x)$, *entonces la multiplicidad de* u *en* $p(x)$ *es el máximo* m *tal que* $p(x) = (x-u)^m q(x)$, *para algún* $q(x) \in L[x]$.

Proposición 1.6.7 (ver [?]). *Sea* K *un campo y sea* $\bar{K}$ *una cerradura algebraica. Si el polinomio irreducible* $p(x) \in K[x]$ *tiene raíces distintas* $u_1, ..., u_k \in \bar{K}$, *entonces las multiplicidades de las* u_j *son iguales. Por lo tanto en* $\bar{K}$,

$$p(x) = c(x-u_1)^m \cdots (x-u_k)^m,$$

donde $c \in K$ *y* $m \geq 1$.

Corolario 1.6.8 (ver [?]). *Sea* K *un campo y sea* $\bar{K}$ *una cerradura algebraica. Si el polinomio irreducible* $p(x) \in K[x]$ *tiene raíces distintas* $u_1, ..., u_k \in \bar{K}$ *las cuales son todas simples, entonces en* $\bar{K}[x]$,

$$p(x) = c(x-u_1) \cdots (x-u_k),$$

donde $c \in K$ *y* $k = grad(p(x))$.

Corolario 1.6.9 (ver [?]). *Sea* K *un campo y sea* $u \in \bar{K}$. *Entonces el número de conjugados distintos de* u *es*

$$\frac{grad(Irr(u,K))}{m},$$

donde m es la multiplicidad de u en $Irr(u,K)$.

Definición 1.6.10. *Sea L extensión de K. Un elemento $u \in L$ algebraico sobre K es separable sobre K, si $Irr(u,K) \in K[x]$ es separable sobre K.*

Definición 1.6.11. *Una extensión algebraica L/K es llamada separable, si cada elemento de L es separable sobre K.*

Definición 1.6.12. *Sea L extensión finita de K. El grado separable de L sobre K se define como*

$$(L:K) = |Mono_K(L, \bar{K})|.$$

Lema 1.6.13 (ver [**?**])**.** *Para una extensión finita simple $K(u)/K$,*

$$(K(u):K) = |Roots(Irr(u,K), \bar{K})|.$$

Si $K(u)/K$ es separable, entonces $[K(u):K] = (K(u):K)$.

Cualquier extensión finita se puede construir por una sucesión de extensiones simples

$$K(u_1)/K, K(u_1,u_2)/K(u_1), ..., L = K(u_1, ..., u_k)/K(u_1, ..., u_{k-1}).$$

Así podemos usar lo siguiente para calcular $(L:K) = (K(u_1, ..., u_k):K)$.

Proposición 1.6.14 (ver [**?**])**.** *Sean L/K y M/L extensiones finitas. Entonces $(M:K) = (M:L)(L:K)$.*

Corolario 1.6.15 (ver [**?**])**.** *Sea L extensión finita de K. Entonces $(L:K)|[L:K]$.*

Proposición 1.6.16 (ver [**?**])**.** *Sea L extensión finita de K. Entonces L/K es separable si y sólo si $(L:K) = [L:K]$.*

Proposición 1.6.17 (ver [**?**])**.** *Sean L/K y M/L extensiones finitas. Entonces M/K es separable si y sólo si L/K y M/L son separables.*

1.7. El Teorema del Elemento Primitivo

Teorema 1.7.1. *(Teorema del Elemento Primitivo)[ver [**?**]] Sea L extensión finita separable de K. Entonces L tiene un elemento primitivo.*

Corolario 1.7.2 (ver [**?**])**.** *Sea L/K una extensión finita separable de un campo de característica 0. Entonces L tiene un elemento primitivo*

Proposición 1.7.3 (ver [?]). *Sea $u \in \bar{K}$ un elemento separable sobre K. Entonces*

$$Irr(u, K) = (x - \alpha_1(u)) \cdots (x - \alpha_d(u)),$$

donde $\alpha_1, ..., \alpha_d$ son los elementos de $Mono_K(K(u), \bar{K})$. En particular, el polinomio

$$(x - \alpha_1(u)) \cdots (x - \alpha_d(u)) \in \bar{K}$$

está en $K[x]$ y es irreducible.

1.8. Extensiones Normales y Campos de Descomposición

Sea $\bar{K}$ una cerradura algebraica para el campo K y sea $E/K \leq \bar{K}/K$ una extensión finita. Si $\varphi \in Mono_K(E, \bar{K})$, entonces por la Observación 1.4.2 tenemos que $\varphi(E) = E$ si y sólo si $\varphi(E) \leq E$.

Definición 1.8.1. *Una extensión E de K se dice que es una extensión normal de K, si $\varphi(E) = E$, para cada $\varphi \in Mono_K(E, \bar{K})$.*

Observación 1.8.2. *Si E/K es una extensión normal entonces siempre que un polinomio irreducible $p(x) \in K[x]$ tiene una raíz en E, se descompone en E ya que por el Lema 1.5.8 cada par de raíces de $p(x)$ son conjugados sobre K y una puede ser enviada a la otra por un monomorfismo $\bar{K} \longrightarrow \bar{K}$, el cual debe enviar E en el mismo.*

Teorema 1.8.3 (ver [?]). *Una extensión finita E/K es normal si y sólo si es un campo de descomposición sobre K, para algún polinomio $f(x) \in K[x]$.*

Corolario 1.8.4 (ver [?]). *Sean E/L y L/K extensiones finitas. Si E/K es normal, entonces E/L es normal.*

Capítulo 2

Extensiones de Galois y la Correspondencia de Galois

En este capítulo estudiaremos la estructura de las *extensiones de Galois* y sus *grupos de Galois asociados*, en particular explicaremos como estos están relacionados por la *Correspondencia de Galois*. En todo el capítulo, sea K un campo.

2.1. Extensiones de Galois

Definición 2.1.1. *Una extensión finita E de K es una extensión de Galois (finita) si es normal y separable.*

De la sección 1.6 sabemos que para una extensión de Galois E/K, $[E : K] = (E : K)$ y también cada monomorfismo $\varphi \in Mono_K(E, \bar{K})$ manda E en sí mismo, por lo tanto restringe a un automorfismo de E el cual será denotado $\varphi|_E$.

Dado que cada monomorfismo $\alpha \in Mono_K(E, \bar{K})$, es también un elemento de $Aut_K(E)$,por el Teorema de Extensión de Monomorfismos 1.5.6, tenemos que cada automorfismo $\alpha \in Mono_K(E, \bar{K})$ se extiende a un monomorfismo $E \longrightarrow \bar{K}$ que fija a los elementos de K. De este modo existe una biyección

$$Mono_K(E, \bar{K}) \leftrightarrow Aut_K(E)$$

y tenemos

$$|Aut_K(E)| = (E : K) = [E : K].$$

Definición 2.1.2. *Para una extensión finita de Galois E/K, el grupo*

$$Gal(E/K) = Aut_K(E)$$

es llamado el Grupo de Galois de la extensión o el Grupo de Galois de E sobre K. Los elementos de $Gal(E/K)$ son llamados automorfismos de E/K.

Por lo dicho anteriormente tenemos que:

$$|Gal(E/K)| = (E : K) = [E : K].$$

También podemos reformular la noción de conjugación introducida en la Definición 1.5.7.

Definición 2.1.3. *Sean E extensión finita de Galois de K y $u, v \in E$. Entonces v es conjugado para u sobre K, si existe $\varphi \in Gal(E/K)$, para el cual $v = \varphi(u)$; también se dice que v es un conjugado de u sobre K.*

Sea E extensión finita de Galois de K. Sabemos que E es un campo de descomposición para algún polinomio sobre K, ya que E es normal sobre K. También sabemos que E es una extensión simple de K, ya que E es separable sobre K. Con frecuencia es conveniente utilizar estos hechos para interpretar elementos del grupo de Galois como permutaciones de las raíces de algún polinomio el cual se descompone sobre E.

Resumiremos las propiedades de los grupos de Galois, para ello recordaremos algunas nociones de la teoría de grupos [ver [4]].

Definición 2.1.4. *Sea G un grupo y X un conjunto. Una acción de G en X, es una transformación $* : X \times G \longrightarrow X$, tal que*

- *$xe = x$ para toda $x \in X$ y $e \in G$ es el elemento identidad.*
- *$x(g_1 g_2) = (x_1 g_1) g_2$, para toda $x \in X$, para toda $g_1, g_2 \in G$.*

Una acción de un grupo G en un conjunto X es transitiva si para cada par de elementos $x, y \in X$, existe un elemento $g \in G$ tal que $y = xg$.
La acción es fiel o efectiva si para cada elemento $h \in G$, $h \neq e$, existe un elemento $z \in X$ tal que $zh \neq z$.

Teorema 2.1.5 (ver [7])**.** *Sea E extensión finita de Galois de K. Supongamos que E es el campo de descomposición de un polinomio irreducible separable de grado n, $f(x) \in K[x]$. Entonces se cumple lo siguiente:*

1. *$Gal(E/K)$ actúa transitivamente y fielmente en $Roots(f, E)$*
2. *$Gal(E/K)$ puede ser identificado con un subgrupo del grupo de permutaciones de $Roots(f, E)$. Si ordenamos las raíces $u_1, ..., u_n$, entonces $Gal(E/K)$ puede ser identificado con un subgrupo de S_n.*

3. $|Gal(E/K)|$ *divide a* $n!$ *y es divisible por* n*.*

Dada una extensión de Galois E/K, estudiaremos subextensiones $L/K \leq E/K$ y subgrupos $\Gamma \leq Gal(E/K)$, enfocándonos en la relación entre este tipo de objetos.

2.2. Subgrupos del grupo de Galois y su campo fijo.

Sea E/K una extensión de Galois y supongamos que $\Gamma \leq Gal(E/K)$. Consideremos el subconjunto de elementos de E fijados por Γ,

$$E^{\Gamma} = \{u \in E | \forall \gamma \in \Gamma, \gamma(u) = u\}.$$

Lema 2.2.1 (ver [3])**.** $E^{\Gamma} \leq E$ *es un subcampo de* E *que contiene a* K*.*

Definición 2.2.2. $E^{\Gamma} \leq E$ *es el campo fijo de* Γ*.*

Por la Proposición 1.6.17, las extensiones E/E^{Γ} y E^{Γ}/K son separables. E/E^{Γ} también es normal, de esta manera E/E^{Γ} es una extensión de Galois; identificaremos su grupo de Galois. Observemos que

$$[E : E^{\Gamma}] = (E : E^{\Gamma}) = |Gal(E/E^{\Gamma})|.$$

Ahora cada elemento de $Gal(E/E^{\Gamma})$ es también un elemento de $Gal(E/K)$ y $Gal(E/E^{\Gamma}) \leq Gal(E/K)$.
Por definición $\Gamma \leq Gal(E/E^{\Gamma})$, así el Teorema de Lagrange implica que $|\Gamma|$ divide a $|Gal(E/E^{\Gamma})|$. De hecho tenemos

Proposición 2.2.3 (ver [7])**.** *Para* $\Gamma \leq Gal(E/K)$*, tenemos* $Gal(E/E^{\Gamma}) = \Gamma$ *y las ecuaciones*

$$[E : E^{\Gamma}] = |Gal(E/E^{\Gamma})| = |\Gamma|,\ [E^{\Gamma} : K] = \frac{Gal(E/K)}{|\Gamma|}.$$

2.3. Subcampos de Extensiones de Galois y grupos relativos de Galois.

Sea E/K una extension de Galois y supongamos que $L/K \leq E/K$, es decir, $K \leq L \leq E$. Entonces E/L es también una extension de Galois cuyo grupo de Galois $Gal(E/L)$ es algunas veces llamado el *grupo relativo de Galois* de la pareja de extensiones E/K y L/K.

Lema 2.3.1 (ver [7])**.** *El grupo relativo de Galois de* $L/K \leq E/K$ *es un subgrupo de* $Gal(E/K)$*, es decir,* $Gal(E/L) \leq Gal(E/K)$ *y su orden es* $|Gal(E/L)| = [E : L]$*.*

Proposición 2.3.2 (ver [7]). *Sean $L/K \leq E/K$ extensiones. Entonces $L = E^{Gal(E/L)}$.*

El siguiente resultado explica la conexión entre los dos usos de la palabra *normal*, los cuales se derivan de su uso en la teoría de Galois.

Proposición 2.3.3 (ver [3]). *Sea E una extensión finita de Galois de K y $L/K \leq E/K$.*

1. *El grupo relativo de Galois $Gal(E/L)$ de $L/K \leq E/K$ es un subgrupo normal de $Gal(E/K)$ si y sólo si L/K es una extensión normal.*

2. *Si L es extensión normal de K y por lo tanto una extensión de Galois, entonces existe un isomorfismo de grupos*

$$Gal(E/K)/Gal(E/L) \longrightarrow Gal(L/K), \text{ dado por } \alpha Gal(E/L) \mapsto \alpha|_L.$$

Ahora ya estamos listos para enunciar nuestro resultado central que describe la *Correspondencia de Galois* asociada con una extensión de Galois finita. Para una extensión de Galois finita, sean

$$\begin{aligned} S(E/K) &= \text{ el conjunto de todos los subgrupos de } Gal(E/K); \\ F(E/K) &= \text{ el conjunto de todas las subextensiones } L/K \text{ de } E/K. \end{aligned}$$

Cada uno de estos conjuntos esta ordenado por la inclusión. Como cada subgrupo de un grupo finito es un subconjunto finito de un conjunto finito, $S(E/K)$ es también un conjunto finito. Definimos dos funciones por

$$\begin{aligned} \Phi_{E/K} : F(E/K) \longrightarrow S(E/K);\ \Phi_{E/K}(L) = Gal(E/L), \\ \Theta_{E/K} : S(E/K) \longrightarrow F(E/K);\ \Theta_{E/K}(\Gamma) = E^{\Gamma}. \end{aligned}$$

Teorema 2.3.4. *(Teorema Fundamental de la Teoría de Galois)[ver [7]]. Sea E extensión finita de Galois de K. Entonces las funciones $\Phi_{E/K}$ y $\Theta_{E/K}$ son biyecciones mutuamente inversas las cuales invierten el orden de la inclusión.*

$$\mathrm{F}(E/K) \rightleftarrows \mathrm{S}(E/K)$$

Bajo esta correspondencia subextensiones normales de E/K corresponden a subgrupos normales de $Gal(E/K)$ y viceversa.

Corolario 2.3.5. *Sea E una extensión finita de Galois de K. Entonces sólo hay un número finito de subextensiones $L/K \leq E/K$.*

2.4. Extensiones de Galois para campos de característica positiva

Supongamos que K es un campo y digamos que $car(K) = p$. Podemos ver K como una extensión de campo de $\mathbb{F}_p$.

Lema 2.4.1. *Sea F un campo finito con q elementos y sea V un $F-$espacio vectorial. Entonces $dim_F V < \infty$ si y sólo si V es finito y en este caso $|V| = q^{dim_F V}$.*

Demostración. $\Rightarrow$) Si $d = dim_F V < \infty$, entonces para una base $v_1, ..., v_d$ podemos expresar cada elemento $v \in V$ de manera única en la forma $v = t_1 v_1 + \cdots + t_d v_d$, donde $t_1, ..., t_d \in F$. Claramente existen exactamente q^d de tales expresiones, de este modo $|V| = q^d$.
$\Leftarrow$) Si V es finito, entonces cualquier base tiene un número finito de elementos, así $dim_F V < \infty$. ■

Corolario 2.4.2. *Sea F un campo finito y E/F una extensión. Entonces E es finito si y sólo si E/F es finita y entonces $|E| = |F|^{[E:F]}$.*

Corolario 2.4.3. *Sea K un campo finito. Entonces $K/\mathbb{F}_p$ es finita y $|K| = p^{[K:\mathbb{F}_p]}$.*

En lo que sigue mostraremos que para cada potencia p^d existe un campo finito con p^d elementos. Comenzamos con la cerradura algebraica $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ y consideremos el polinomio

$$\Theta_{p^d}(x) = x^{p^d} - x \in \mathbb{F}_p[x].$$

Observemos que $\Theta'_{p^d}(x) = -1$, por lo tanto, por la Proposición 1.6.3, cada raíz de $\Theta_{p^d}(x)$ en $\overline{\mathbb{F}}_p$ es simple. Por lo tanto por el Corolario 1.1.14, $\Theta_{p^d}(x)$ debe tener exactamente p^d raíces distintas en $\overline{\mathbb{F}}_p$, digamos $0, u_1, ..., u_{p^d-1}$.

Entonces en $\overline{\mathbb{F}}_p[x]$ tenemos

$$x^{p^d} - x = x(x - u_1) \cdots (x - u_{p^d-1}),$$

y cada raíz es separable sobre $\mathbb{F}_p$. Sea

$$\mathbb{F}_{p^d} = \{u \in \overline{\mathbb{F}}_p | \Theta_{p^d}(u) = 0\} \subseteq \overline{\mathbb{F}}_p,\ \mathbb{F}^0_{p^d} = \{u \in \mathbb{F}_{p^d} | u \neq 0\}.$$

Observación 2.4.4. $u \in \mathbb{F}^0_{p^d} \Leftrightarrow u \neq 0$ y $\Theta_{p^d}(u) = 0 \Leftrightarrow \frac{u^{p^d}}{u} = 1 \Leftrightarrow u^{p^d-1} = 1$.

Proposición 2.4.5. *Para cada $d \geq 1$, $\mathbb{F}_{p^d}$ es un subcampo finito de $\overline{\mathbb{F}}_p$ con p^d elementos y $\mathbb{F}^0_{p^d} = \mathbb{F}^*_{p^d} = (\mathbb{F}_{p^d} \setminus \{0\})$. Además $\mathbb{F}_{p^d}/\mathbb{F}_p$ es campo de descomposición separable.*

Demostración. Hay que ver que $\mathbb{F}_{p^d}$ es subcampo de $\overline{\mathbb{F}}_p$, por lo anterior ya tenemos que $\mathbb{F}_{p^d} \subseteq \overline{\mathbb{F}}_p$. Ahora sean $u, v \in \mathbb{F}_{p^d}$, entonces

$(u+v)^{p^d} - (u+v) = u^{p^d} + v^{p^d} - u - v = (u^{p^d} - u) + (v^{p^d} - v) = 0$, por lo tanto $u+v \in \mathbb{F}_{p^d}$

$(uv)^{p^d} - uv = u^{p^d} v^{p^d} - uv = uv - uv = 0$, por lo tanto $uv \in \mathbb{F}_{p^d}$, por lo tanto $\mathbb{F}_{p^d} < \overline{\mathbb{F}}_p$ y $|\mathbb{F}_{p^d}| = p^d$ y $\mathbb{F}^0_{p^d} = \mathbb{F}^*_{p^d}$.

■

Definición 2.4.6. *El campo finito $\mathbb{F}_{p^d} \leq \overline{\mathbb{F}}_p$ es llamado el campo de Galois de orden p^d.*

Usaremos $GF(p^d)$ para denotar a tales campos. Si $d = 1$, $GF(p) = \mathbb{F}_p$ y $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$.

Proposición 2.4.7. *Sea $d \geq 1$.*

1. *$\mathbb{F}_{p^d} \leq \overline{\mathbb{F}}_p$ es el campo de descomposición de $x^{p^d} - x$ y $x^{p^d-1} - x$ sobre $\mathbb{F}_p$.*
2. *$\mathbb{F}_{p^d} \leq \overline{\mathbb{F}}_p$ es el único subcampo con p^d elementos.*
3. *Si F es un campo con p^d elementos, entonces existe un monomorfismo $\varphi : F \longrightarrow \overline{\mathbb{F}}_p$, con $Im(\varphi) = \mathbb{F}_{p^d}$ y por lo tanto $F \cong \mathbb{F}_{p^d}$.*

Demostración.

1. $\mathbb{F}_p$ es campo de descomposición de $x^{p^d} - x$ por lo anterior y los elementos de $\mathbb{F}^0_{p^d} = \mathbb{F}^*_{p^d} \subset \mathbb{F}_{p^d}$ son las raíces de $x^{p^d-1} - 1$.

2. Supongamos que $F \leq \overline{\mathbb{F}}_p$ y $|F| = p^d$. Tomamos $F^* = F \setminus \{0\}$ el cual es un grupo abeliano bajo la multiplicación, con $p^d - 1$ elementos. Por el Teorema de Lagrange, $\forall a \in F^*$, $o(a) | p^d - 1$, por lo tanto $\forall a \in F^*$, $a^{p^d-1} = 1$, es decir, $a^{p^d} = a$, entonces a es raíz de $\Theta_{p^d}(x)$, lo que implica que $F^* \subset \mathbb{F}_{p^d}$, entonces $F \subset \mathbb{F}_{p^d}$ y $|F| = |\mathbb{F}_{p^d}| = p^d$.

$$\therefore F = \mathbb{F}_{p^d}.$$

■

Corolario 2.4.8. *Sea K un campo finito de característica p. Entonces $K/\mathbb{F}_p$ es una extensión finita de Galois.*

Proposición 2.4.9. *Sean $\mathbb{F}_{p^m}$ y $\mathbb{F}_{p^n}$ dos campos de Galois de característica p. Entonces $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$ si y sólo si $m|n$.*

Demostración. $\Rightarrow$) Si $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$, entonces por el Corolario 2.4.2,

$$p^n = (p^m)^{[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]} = p^{m[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]},$$

así $m|n$.
$\Leftarrow$) Si $m|n$, escribimos $n = mk$, donde $k \geq 1$. Entonces para $u \in \mathbb{F}_{p^m}$ tenemos que $u^{p^m} = u$, así

$$u^{p^n} = u^{p^{mk}} = (u^{p^m})^{p^{m(k-1)}} = u^{p^{m(k-1)}} = \cdots = u^{p^m} = u.$$

Por lo tanto $u \in \mathbb{F}_{p^n}$ y por lo tanto $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$. ■

Teorema 2.4.10. *La cerradura algebraica de $\mathbb{F}_p$ es la unión de todos los campos de Galois de característica p,*

$$\overline{\mathbb{F}}_p = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$$

Además cada elemento $u \in \overline{\mathbb{F}}_p$ es separable sobre $\mathbb{F}_p$.

Demostración. Sea $u \in \overline{\mathbb{F}}_{p^n}$. Entonces u es algebraico sobre $\mathbb{F}_p$ y la extensión $\mathbb{F}_p(u)/\mathbb{F}_p$ es finita. Por lo tanto por el Corolario 2.4.2, $\mathbb{F}_p(u) \leq \overline{\mathbb{F}}_p$ es un campo finito. La Proposición 2.4.9 implica que $\mathbb{F}_p(u) = \mathbb{F}_{p^n}$, para alguna n. La separabilidad la obtenemos por el Corolario 2.4.8. ■

Proposición 2.4.11. *El grupo de unidades $\mathbb{F}^*_{p^d}$ en $\mathbb{F}_{p^d}$ es cíclico.*

Este resultado es un caso especial de un resultado más general acerca de campos arbitrarios. Para la siguiente Proposición recordemos que si G es un grupo Abeliano, entonces el *exponente* de G denotado $exp(G)$, es el mínimo común múltiplo de los órdenes de los elementos de G. Por un resultado de la teoría de grupos, existe un elemento de G cuyo orden es $exp(G)$. De este hecho se tiene que G es cíclico si y sólo si $|G| = exp(G)$.

Proposición 2.4.12. *Sea K un campo. Entonces cada subgrupo finito $G \leq K^*$ es cíclico.*

Demostración. Sea $n = |G|$ y $m = exp(G)$. Entonces $m|n$ por el teorema de Lagrange. Si $g \in G$, entonces $g^m = 1$, así cada elemento de G es una raíz del polinomio $x^m - 1$. Este polinomio tiene a lo más m raíces en el campo K. Sin embargo, $x^m - 1$ tiene al menos a los elementos de G como raíces, así $n \leq m$. Por lo tanto, $exp(G) = |G|$, de este modo G es cíclico. ■

Definición 2.4.13. *Un elemento $u \in \mathbb{F}^*_{p^d}$ es llamado una raíz primitiva, si es una raíz primitiva $(p^d - 1)$-ésima de la unidad, es decir, su orden en el grupo $\mathbb{F}^*_{p^d}$ es $(p^d - 1)$, por lo tanto $\langle w\rangle = \mathbb{F}^*_{p^d}$.*

Proposición 2.4.14. *La extensión de Galois $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ es simple.*

Demostración. Por la Proposición 2.4.11 $\mathbb{F}_{p^{nd}}$ tiene una raíz primitiva w. Entonces w genera a $\mathbb{F}^*_{p^{nd}}$ cíclico de orden $p^{nd} - 1$. $\mathbb{F}_{p^{nd}}$ sobre $\mathbb{F}_{p^d}$ tiene una base de potencias de w. Por lo tanto $\mathbb{F}_{p^{nd}} = \mathbb{F}_{p^d}(w)$. ■

2.5. Grupos de Galois de extensiones finitas y mapeos de Frobenius

Tomemos una extensión de campos de Galois $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$. Tenemos

$$|Gal(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})| = |Aut_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^{nd}})| = [\mathbb{F}_{p^{nd}} : \mathbb{F}_{p^d}] = n$$

Introducimos un elemento importante del grupo de Galois $Gal(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$.

Definición 2.5.1. *El mapeo (relativo) de Frobenius para la extensión $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ es la función: $F_d : \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ dado por $F_d(t) = t^{p^d}$.*

Proposición 2.5.2. *El mapeo de Frobenius $F_d : \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ es un automorfismo de $\mathbb{F}_{p^{nd}}$ que fija a $\mathbb{F}_{p^d}$, entonces $F_d \in Gal(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$ y su orden es n, por lo tanto $Gal(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle F_d \rangle$.*

Demostración. Sean $u, v \in \mathbb{F}_{p^{nd}}$,

$$F_d(u+v) = (u+v)^{p^d} = u^{p^d} + v^{p^d} = F_d(u) + F_d(v),$$
$$F_d(uv) = (uv)^{p^d} = u^{p^d} v^{p^d},$$

así F_d es un homomorfismo de anillos. Sea $u \in \mathbb{F}_{p^d}$, entonces $F_d(u) = u^{p^d} = u$, por lo tanto F_d fija a $\mathbb{F}_{p^d}$. Para ver que F_d es un automorfismo, sea $w \in \mathbb{F}_{p^d}$, entonces $F_d^n(w) = F_d \circ F_d \circ \cdots \circ F_d(w) = F_d \circ \cdots \circ F_d(w^{p^d}) = F_d \circ \cdots \circ F_d((w^{p^d})^{p^d}) = F_d \circ \cdots \circ F_d(w^{p^{2d}}) = w^{p^{nd}} = w$, para todo $w \in \mathbb{F}_{p^{nd}}$ por lo tanto $F_d^n = id$, entonces $o(F_d)|n$. Sea z generador de $(\mathbb{F}_{p^{nd}})^*$, entonces el $o(z) = p^{nd} - 1$. Supongamos también que el orden de F_d es k, con $k < n$, entonces $F_d^k = id$, entonces $F_d^k(z) = z^{p^{kd}} = z$, $k < n$, entonces $o(z)|p^{kd} - 1$, pero $o(z) = p^{nd} - 1$ y $o(z)|(p^{kd}, p^{nd} - 1)$ lo cual es una contradicción, entonces $o(z) = p^{nd} - 1 > p^{kd} - 1$, por lo tanto el orden de F_d es n y tiene inverso $F_d^{-1} = F_d^{n-1}$. ■

Para $d \geq 1$, tomemos la función

$$F_d : \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p, \text{ dada por } F_d(t) = t^{p^d}.$$

Proposición 2.5.3. *Sea $d \geq 1$.*

1. *$F_d : \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$ es un automorfismo de $\overline{\mathbb{F}}_p$ que fija a $\mathbb{F}_{p^d}$. Además para $u \in \overline{\mathbb{F}}_p$, $F_d(u) = u$ si y sólo si $u \in \mathbb{F}_{p^d}$.*
2. *La restricción $F_d|_{\mathbb{F}_{p^{nd}}}$, es el mapeo relativo de Frobenius $F_d : \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$.*
3. *Si $k \geq 1$, $F_d^k = F_{kd}$. Por lo tanto en $Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_{p^d})$, F_d tiene orden infinito, así $Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$ es infinito.*

Demostración. 1. $F_d : \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p \in Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$. Sean $u, v \in \overline{\mathbb{F}}_p$, entonces

$$F_d(u+v) = (u+v)^{p^d} = u^{p^d} + v^{p^d} = F_d(u) + F_d(v),$$
$$F_d(uv) = (uv)^{p^d} = u^{p^d} v^{p^d}.$$

por lo tanto $F_p \in Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$. Por otro lado si $u \in \mathbb{F}_{p^d}$, $F_d(u) = u^{p^d} = u$. Supongamos que $F_d(x) = x$, $x \in \overline{\mathbb{F}}_p$, dado que $x^{p^d} = x$, si $x = 0$, entonces $x \in \mathbb{F}_{p^d}$, por otra parte si $x \neq 0$, entonces $x^{p^d-1} = 1$ y así $x \in \mathbb{F}_{p^d}$.

2. Sea $u \in \overline{\mathbb{F}}_p$, entonces $F_d^k(u) = F_d \circ \cdots \circ F_d(u) = u^{p^{kd}}$...(1). Por otra parte $F_{kd} = u^{p^{kd}}$...(2). Por lo tanto de (1) y (2) tenemos que $F_d^k = F_{kd}$. Ahora supongamos que F_d en $Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$ tienen orden finito digamos n. Entonces $F_d^n = F_{nd} = id$. Sea w raíz primitiva en $\mathbb{F}_{p^{nd}} \subset \overline{\mathbb{F}}_p$, con $m > n$, entonces $o(w) = p^{md} - 1$, aplicamos $F_d^n = F_{nd} = id$ y tenemos $F_d^n(w) = w^{p^{nd}} = w$, entonces $o(w) | p^{nd} - 1$, lo cual es una contradicción, ya que $o(w) = p^{md} - 1$, con $m > n$. Por lo tanto el orden de F_d en $Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$ es infinito y así $Aut_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$ es infinito.

■

Definición 2.5.4. *El mapeo de Frobenius F_1 es llamado el* mapeo absoluto de Frobenius, *ya que es un elemento de los grupos $Aut_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ y $Aut_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ para cada $n \geq 1$.*

Observación 2.5.5. *$Gal(\mathbb{F}_{p^{nd}} : \mathbb{F}_{p^d}) = \langle F_d \rangle$, tiene un subgrupo cíclico para cada $k|n$ que es $\langle F_d^k \rangle$, de orden n/k.*

Proposición 2.5.6. *Para cada $k|n$, el subcampo fijo de $\langle F_d^k \rangle$ en $\mathbb{F}_{p^{nd}}$ es $\mathbb{F}_{p^{nd}}^{\langle F_d^k \rangle} = \mathbb{F}_{p^{dk}}$.*

Demostración. Sabemos que $\mathbb{F}_{p^d} \leq \mathbb{F}_{p^{nd}}^{\langle F_d^k \rangle} \leq \mathbb{F}_{p^{nd}}$. Sea $0 \neq u \in \mathbb{F}_{p^{nd}}$, $F_d^k(u) = u^{p^{kd}} = u$ si y sólo si $u \in \mathbb{F}_{p^{kd}}$. ■

Bibliografía

[1] Morandi, Patrick, *Field and Galois Theory*, Springer-Verlag, Inc, New York, 1996.

[2] Stewart, Ian, *Galois Theory*, Chapman y Hall/CRC mathematics.

[3] Zaldivar, Felipe, *Teoría de Galois*, Anthropos, Barcelona, 1996.

[4] Rotman, Joseph J, *An Introduction to the Theory of Groups*, Springer-Verlag, Inc, New York, 1995.

[5] Fraleigh, John B, *A first course in Abstract Algebra*, Addison-Wesley.

[6] McCarthy, Paul Joseph, *Algebraic extensions of fields*, Dover, New York, 1976.

[7] Baker, Andrew, *An Introduction to Galois Theory*, Department of Mathematics, University of Glasgow, 2008.