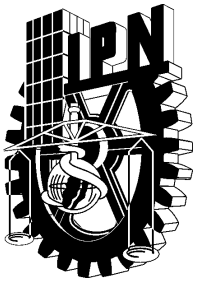

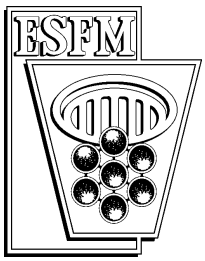

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

La Cerradura Normal de Algunas Extensiones de Kummer y la Estructura de su Grupo de Galois

T E S I S
QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN FÍSICA Y MATEMÁTICAS

P R E S E N T A

ALDO GUZMÁN SÁENZ

DIRECTOR DE TESIS
DR. PABLO LAM ESTRADA

México, D. F. **Febrero de 2008**

A mi familia.

Agradecimientos

Agradezco a mis padres, Sr. Sergio Guzmán Vargas y Sra. María Eugenia Sáenz Llamas, a mis hermanos y al resto de mi familia por todo el apoyo que me han brindado.

También agradezco a los miembros del Jurado, Dra. Myriam Rosalía Maldonado Ramírez, M. en C. María Elizabeth de la Cruz Santiago, M. en C. Abelardo Santaella Quintas y al Lic. Manuel Robles Bernal por las diversas observaciones y correcciones hechas durante la realización de este trabajo de tesis.

Un agradecimiento especial al Dr. Pablo Lam Estrada, Director de Tesis, por la ayuda y guía proporcionada para hacer la misma.

Índice general

Introducción

Sea p un número primo, y sea F un campo de característica distinta a p el cual contiene una ζ raíz p-ésima primitiva de la unidad. Consideraremos también una extensión K sobre F de Galois con grupo de Galois cíclico generado por σ de orden $q = p^n$. Hace más de 70 años, A. A. Albert ([2], [3]) estudió la posibilidad de encontrar extensiones de K que fueran cíclicas de grado p^{n+1} sobre F. La presencia de ζ en F implica que cualquier extensión cíclica L de grado p sobre K es de la forma $K(\sqrt[p]{a})$, para algún $a \in K$. Albert demostró que L es de Galois sobre F si y sólo si $\sigma(a)/a = b^p$, para algún $b \in K$, y observó que la norma $N_{K/F}(b)$ es una raíz p-ésima de la unidad. Su resultado principal fue que el grupo de Galois de L sobre F es cíclico si esta raíz p-ésima de la unidad es no trivial. Si es trivial, entonces el grupo de Galois de L sobre F es el producto de grupos cíclicos de orden q y p.

En este trabajo de tesis se desarrollarán los resultados que generalizan el caso en el que se toma una extensión arbitraria $K(\sqrt[p]{a})$ y se toma a L como la cerradura normal de $K(\sqrt[p]{a})$ sobre F. El resultado principal (Teorema 3.2.1) es determinar la estructura del grupo $\mathrm{Gal}(L/K)$ completamente, partiendo únicamente de la información de K. Para esto, definiremos una sucesión de elementos de K dada como sigue: Dado un elemento arbitrario $a \in K$, definimos $a_0 := a$ y $a_{i+1} := \sigma(a_i)/(a_i)$, para cada $i > 0$. Entonces, el grado de L sobre K estará determinado por el primer s tal que $a_s = b^p$, con $b \in K$. Veremos que $s \leq q$ y que para cada grado posible, salvo el mayor ($s = q$), habrá exactamente dos tipos de grupos de Galois que se pueden dar; de la sucesión definida, construiremos una raíz p-ésima de la unidad que es trivial en un caso y no trivial en el otro.

Para poder demostrar el resultado principal, desarrollamos algunos resultados que serán útiles para nuestro propósito. La tesis está dividida de tres capítulos. En el Capítulo 1 presentamos los resultados de álgebra lineal que serán aplicados para la obtención de la cerradura normal L de la extensión $K(\sqrt[p]{a})/F$; básicamente está dirigido a los subespacios invariantes y subespacios cíclicos. Pero, además, en este capítulo explicamos la estructura que deberán de tener aquellos grupos que están caracterizados por una clase del segundo grupo de cohomología, y que será de importancia para entender uno de los grupos de Galois que se nos presentarán.

Los resultados que son objeto de estudio en este trabajo se encuentran en el Capítulo 2, como son algunos resultados de la Teoría de Galois Finita, extensiones cíclicas, Teoría de Kummer y resultados sobre extensiones radicales, en general. Por supuesto, la Teoría de Kummer es esencial en nuestro trabajo, ya que la extensión de L/K será una extensión de Kummer. Sin embargo, varios de los resultados de extensiones radicales que presentamos no serán usados en el desarrollo del trabajo, pero muestran la diversidad de situaciones que se pueden presentar en las mismas.

Finalmente, en el Capítulo 3 presentamos el desarrollo de nuestro resultado principal en el que se caracteriza el grupo de Galois de la extensión L/F.

Notación

$\dim(V)$	La dimensión de V
$\mathrm{gr}f$	El grado del polinomio f
$T \rtimes A$	El producto semidirecto de T con A
$C(\alpha, T)$	El T-subespacio cíclico generado por α
$M(\alpha; T)$	El T-anulador de α
$Z^2(T, A)$	El conjunto de las 2-cociclos $T \times T \longrightarrow A$
$B^2(T, A)$	El conjunto de las 2-cofronteras $T \times T \longrightarrow A$
$H^2(T, A)$	El segundo grupo de cohomología de T con coeficientes en A
E/F	Extensión de campos, con E conteniendo a F
$\mathrm{Gal}(E/F)$	El grupo de Galois de la extensión E/F
$[E : F]$	El grado de la extensión E/F
$[E : F]_s$	El grado de separabilidad de la extensión E/F
$\mathrm{Hom}(G, \langle\zeta_n\rangle)$	El conjunto de homomorfismos de G a $\langle\zeta_n\rangle$
$H^{\perp}$	El ortogonal de H
G^*	El conjunto de homomorfismos del grupo G a $\mathbb{C}^*$
F^*	El conjunto de unidades del campo F
$\overline{F}$	La cerradura algebraica de F
$\mathrm{tor}(G)$	El subgrupo de torsión de G
$\square$	Fin de una demostración

Capítulo 1

Preliminares

1.1. Subespacios invariantes

En esta sección, asumiremos la siguiente notación: V es un espacio vectorial sobre un campo F.

Definición 1.1.1. *Sean T un operador lineal sobre V y W un subespacio de V. Decimos que W es **invariante bajo** T si, para cada vector α en W, el vector $T(\alpha)$ está en W, es decir, si $T(W)$ está contenido en W.*

Si T es un operador lineal sobre V, entonces V es invariante bajo T. También lo es el subespacio cero. La imagen de T y el espacio nulo de T son invariantes bajo T. En general, sean T un operador lineal sobre V y U cualquier operador lineal sobre V que conmuta con T, es decir, $TU = UT$. Sean W la imagen de U y N el espacio nulo de U. Entonces, W y N son invariantes bajo T. En efecto, si α está en la imagen de U, digamos $\alpha = U(\beta)$, entonces $T(\alpha) = T(U(\beta)) = U(T(\beta))$, así que $T(\alpha)$ está en la imagen de U. Por otro lado, si α está en N, entonces $U(T(\alpha)) = T(U(\alpha)) = T(0) = 0$; por lo tanto, $T(\alpha)$ está en N.

Un tipo de operador que conmuta con T son los operadores $U = g(T)$, donde g es un polinomio con coeficientes en los escalares. Por ejemplo, podemos tener $U = T - cI$, donde c es un valor característico de T. Vemos que este ejemplo incluye el hecho de que el espacio de vectores característicos de T asociados con el valor característico c es invariante bajo T.

Ejemplo 1.1.2. Sea T el operador lineal en $\mathbb{R}^2$ representado en la base ordenada estándar por la matriz

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Entonces los únicos subespacios de $\mathbb{R}^2$ invariantes bajo T son $\mathbb{R}^2$ y el subespacio cero. Cualquier otro subespacio invariante no necesariamente tendrá dimensión 1. Pero si W es el subespacio generado por algún vector α no cero, el hecho de que W es invariante bajo T quiere decir que α es un vector característico, pero A no tiene valores característicos.

Cuando el subespacio W es invariante bajo el operador T, entonces T induce un operador lineal T_W sobre el espacio W. El operador lineal T_W es la restricción de T a W, es decir, T_W está dado por $T_W(\alpha) = T(\alpha)$, para α en W. Pero T_W es un objeto muy distinto de T pues su dominio es W, no V.

Cuando V es de dimensión finita, existe una interpretación del hecho de que W sea invariante bajo T. Supongamos que elegimos una base ordenada $\mathfrak{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ para V tal que $\mathfrak{B}' = \{\alpha_1, \ldots, \alpha_r\}$ es una base ordenada para W ($r = \dim(W)$). Sea $A = [a_{ij}] = [T]_{\mathfrak{B}}$; así que

$$T(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i,$$

para cada $j = 1, \ldots, n$.

Pero como W es invariante bajo T, el vector $T(\alpha_j)$ pertenece a W para $j \leq r$. De manera que

$$T(\alpha_j) = \sum_{i=1}^{r} a_{ij}\alpha_i, \tag{1.1.1}$$

para cada $j = 1, \ldots, r$.

En otras palabras, $a_{ij} = 0$ si $j \leq r$ e $i > r$.

En términos matriciales, A tiene la siguiente forma en bloques:

$$A = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix}, \tag{1.1.2}$$

donde B es una matriz $r \times r$, C es una matriz $r \times (n-r)$ y D es una matriz $(n-r) \times (n-r)$. De acuerdo a (1.1.1), la matriz B es precisamente la matriz del operador inducido T respecto a la base ordenada $\mathfrak{B}'$.

Proposición 1.1.3. *Conservando las notaciones anteriores, sea W un subespacio invariante bajo T. El polinomio característico para el operador restringido T_W divide al polinomio característico de T, y el polinomio mínimo de T_W divide al polinomio mínimo de T.*

Demostración. Tenemos

$$A = \begin{bmatrix} B & C \\ 0 & D \end{bmatrix},$$

donde $A = [T]_{\mathfrak{B}}$ y $B = [T_W]_{\mathfrak{B}'}$. Con la forma de la matriz se tiene

$$\det(xI - A) = \det(xI - B)\det(xI - D).$$

Esto prueba la afirmación sobre polinomios característicos. Notemos que usamos I para representar matrices identidades de tres diferentes tamaños.

Por otro lado, la k-ésima potencia de A tiene la siguiente forma en bloques

$$A^k = \begin{bmatrix} B^k & C_k \\ 0 & D^k \end{bmatrix},$$

donde C_k es alguna matriz $(r \times (n-r))$. Por lo tanto, cualquier polinomio que anula a A también anula a B. Así, el polinomio mínimo de B divide al polinomio mínimo de A.

□

Proposición 1.1.4. *Sean W un subespacio de un espacio vectorial V y T un operador lineal de V. Entonces, W es invariante bajo T si y sólo si W es invariante bajo todo polinomio en T.*

Demostración. Supóngase que W es invariante bajo T. Si β está en W, entonces $T(\beta)$ está en W. En consecuencia, $T(T\beta) = T^2(\beta)$ está en W. Por inducción, tenemos que $T^k(\beta)$ está en W para cada $k \geq 0$. Por lo tanto, se tiene que $f(T)(\beta)$ está en W para todo polinomio f, es decir, W es invariante bajo todo polinomio en T.

Recprocamente, si W es invariante bajo todo polinomio en T, tenemos en particular que W es invariante bajo T.

□

Corolario 1.1.5. *El subespacio W es invariante bajo T si y sólo si lo es bajo $T - I$.*

Demostración. Se sigue inmediatamente de la Proposición 1.1.4

□

1.2. Subespacios cíclicos

Supongamos que V es un espacio vectorial sobre un campo F de dimensión finita, y sea T un operador lineal fijo (pero arbitrario) sobre V. Si α es cualquier vector en V, existe un subespacio de V que es invariante bajo T y que contiene a α. Este subespacio puede ser definido como la intersección de todos los espacios T-invariantes que contienen a α. Sin embargo, es más útil verlo de la siguiente manera: si W es cualquier subespacio de V invariante bajo T que contiene a α, entonces W debe contener al vector $T(\alpha)$; por lo que debe contener a $T(T(\alpha)) = T^2(\alpha)$, $T(T^2(\alpha)) = T^3(\alpha)$, etc. En otras palabras, W debe contener $g(T)(\alpha)$ para cualquier polinomio g sobre F. El conjunto de todos los vectores de la forma $g(T)(\alpha)$, con g en $F[X]$, es claramente invariante bajo T, y es por lo tanto el menor subespacio invariante que contiene a α.

Definición 1.2.1. *Si α es cualquier vector en V. El T-**subespacio cíclico generado por** α es el subespacio $C(\alpha;T)$ de todos los vectores de la forma $g(T)(\alpha)$, con g en $F[X]$. Si $C(\alpha;T) = V$, entonces decimos que α es un **vector cíclico para** T.*

Otra manera de describir al subespacio $C(\alpha;T)$, es diciendo que $C(\alpha;T)$ es el subespacio generado por los vectores $T^k(\alpha)$, con $k \geq 0$; as, α es un vector cíclico para T si y sólo si estos vectores generan V. En general, es posible que el operador T no tenga vectores cíclicos.

Observación 1.2.2. Para cualquier operador lineal T, el T-subespacio cíclico generado por el vector cero es el subespacio cero. El espacio $C(\alpha;T)$ es de dimensión uno si y sólo si α es un vector característico para T. Para el operador identidad, todo vector no cero genera un subespacio cíclico uno-dimensional; así, si $\dim(V) > 1$, el operador identidad no tiene un vector cíclico. Un ejemplo de un operador que tiene un vector cíclico es el operador lineal T en F^2 el cual es representado en el orden estándar por la matriz

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Aquí, un vector cíclico es el vector canónico ϵ_1; pero, si $\beta = (a,b)$ entonces, con $g(X) = a + bX$, tenemos que $\beta = g(T)\epsilon_1$. Para este mismo operador T, el subespacio cíclico generado por ϵ_2 es el espacio uno-dimensional generado por ϵ_2, porque ϵ_2 es un vector característico de T.

Para cualesquier T y α, analizaremos brevemente las combinaciones lineales de la forma

$$c_0\alpha + c_1T(\alpha) + \cdots + c_kT^k(\alpha) = 0,$$

entre los vectores $T^j(\alpha)$; esto es, estaremos analizando las combinaciones $g(T)(\alpha) = c_0\alpha + c_1T\alpha + \cdots + c_kT^k\alpha$ que tiene la propiedad de $g(T)(\alpha) = 0$. El conjunto de todos los polinomios g en $F[X]$ tales que $g(T)(\alpha) = 0$ es claramente un ideal de $F[X]$ distinto de cero, ya que este contiene al polinimio mínimo p del operador T, es decir, se tiene que $p(T)(\alpha) = 0$ para cualquier α en V.

Definición 1.2.3. *Si α es cualquier vector en V, el T-**anulador** de α es el ideal $M(\alpha;T)$ en $F[X]$ consistente de todos los polinomios g sobre F tales que $g(T)(\alpha) = 0$. El único polinomio mónico p_α que genera este ideal será llamado también el T-**anulador** de α.*

Como señalamos arriba, el T-anulador p_α divide al polinomio mínimo del operador T. Notemos que $gr(p_\alpha) > 0$ excepto cuando α es el vector cero.

Teorema 1.2.4. *Sean α cualquier vector no cero en V y p_α el T-anulador de α. Entonces,*

(*i*) *El grado de p_α es igual a la dimensión del subespacio cíclico $C(\alpha;T)$.*

(*ii*) *Si el grado de p_α es k, entonces los vectores $\alpha, T(\alpha), T^2(\alpha), \ldots, T^{k-1}(\alpha)$ forman una base de $C(\alpha;T)$.*

(*iii*) *Si U es el operador lineal en $C(\alpha;T)$ inducido por T, entonces el polinomio mínimo para U es p_α.*

Demostración. Sea g cualquier polinomio sobre el campo F. Escribimos, a través del algoritmo de la división,

$$g = p_\alpha q + r,$$

donde $r = 0$ $\text{gr}(r) < gr(p_\alpha) = k$. El polinomio $p_\alpha q$ está en el T-anulador de α. Así

$$g(T)(\alpha) = r(T)(\alpha).$$

Puesto que $r = 0$ ó $\text{gr}(r) < k$, el vector $r(T)(\alpha)$ es una combinación lineal de los vectores $\alpha, T(\alpha), \ldots, T^{k-1}(\alpha)$ y, como $g(T)(\alpha)$ es un vector típico en $C(\alpha;T)$, esto muestra que estos k vectores generan $C(\alpha;T)$. Estos vectores son ciertamente

linealmente independientes, porque cualquier combinación lineal no trivial entre ellos nos daría un polinomio no cero g tal que $g(T)(\alpha) = 0$ y $\text{gr}(g) < \text{gr}(p_\alpha)$, lo que es absurdo. Esto prueba (i) y (ii).

Por otro lado, sea U el operador lineal en $C(\alpha; T)$ obtenido por restricción de T al subespacio $C(\alpha; T)$. Si g es cualquier polinomio sobre F, entonces

$$\begin{aligned} p_\alpha(U)(g(T)(\alpha)) &= p_\alpha(T)(g(T)(\alpha)) \\ &= g(T)(p_\alpha(T)(\alpha)) \\ &= g(T)(0) \\ &= 0. \end{aligned}$$

De esta manera, el operador $p_\alpha(U)$ mapea cada vector de $C(\alpha; T)$ al 0, es decir, es el operador cero en $C(\alpha; T)$. Más aún, si h es un polinomio de grado menor que k, no podemos tener $h(U) = 0$, porque entonces $h(U)(\alpha) = h(T)(\alpha) = 0$, contradiciendo la definición de p_α. Esto prueba que p_α es el polinomio mínimo de U.

□

Una consecuencia particular del teorema anterior es la siguiente: Si α fuera un vector cíclico para T, entonces el polinomio mínimo para T debe tener grado igual a la dimensión del espacio V; por lo tanto, el Teorema de Cayley-Hamilton [[4], Teorema 4, Sección 6.3, Capítulo 6] nos dice que el polinomio mínimo para T es el polinomio característico para T.

Corolario 1.2.5. *Sean T un operador lineal sobre V y α un vector no cero de V tal que existe un $m \in \mathbb{N}$ tal que $T^m(\alpha) = 0$. Sea s el mínimo entero positivo tal que $T^s(\alpha) = 0$. Entonces, el anulador p_α de α tiene grado $s - 1$ y los vectores $\alpha, T(\alpha), \ldots, T^{s-1}(\alpha)$ forman una base del subespacio cíclico $C(\alpha; T)$.*

Demostración. Estamos suponiendo que $T^s(\alpha) = 0$ pero $T^{s-1}(\alpha) \neq 0$. Luego, es claro que el conjunto $\{\alpha, T(\alpha), \ldots, T^{s-1}(\alpha)\}$ genera al subespacio cíclico $C(\alpha; T)$ generado por α. Así que la dimensión del subespacio $C(\alpha; T)$ es menor o igual que $s-1$. Además, dicha dimensión debe de ser $s-1$, ya que el conjunto formado por los vectores $\alpha, T(\alpha), \ldots, T^{s-1}(\alpha)$ es linealmente independiente. En efecto, consideremos la ecuación $a_0\alpha + a_1T(\alpha) + \cdots + a_{s-1}T^{s-1}(\alpha) = 0$; aplicando T^{s-1} a ambos miembros, tenemos que $a_0T^{s-1}(\alpha) = 0$, con lo cual $a_0 = 0$. Luego, la ecuación se reduce a que $a_1T(\alpha) + \cdots + a_{s-1}T^{s-1}(\alpha) = 0$; aplicando T^{s-2} a la última ecuación, obtenemos que $a_1T^{s-1}(\alpha) = 0$, con lo cual $a_1 = 0$. Siguiendo con el proceso, tendremos que $a_0 = \cdots = a_{s-1} = 0$. Por lo tanto, el corolario se sigue del Teorema 1.2.4.

□

Definición 1.2.6. *Sea T un operador lineal sobre V. Se dice que T es* ***nilpotente*** *si existe un $n \in \mathbb{N}$ tal que $T^n = 0$.*

De acuerdo con la definición anterior, el Corolario 1.2.5 se puede enunciar de la siguiente forma.

Corolario 1.2.7. *Sean T un operador lineal sobre V nilpotente y α un vector no cero de V. Sea s el mínimo entero no negativo tal que $T^s(\alpha) = 0$. Entonces, el anulador p_α de α tiene grado $s-1$ y los vectores $\alpha, T(\alpha), \ldots, T^{s-1}(\alpha)$ forman una base del subespacio cíclico $C(\alpha; T)$.*

□

1.3. Extensiones de grupo

En esta sección trataremos de presentar la interpretación del segundo grupo de cohomología el cual será usado para establecer una de las estructuras del grupo de Galois de nuestro resultado principal. Para mayor información se puede consultar [7].

No desarrollaremos los conceptos y propiedades de la cohomología de grupos, el propósito es aclarar las partes esenciales que utilizaremos del segundo grupo de cohomología.

Sean G un grupo, A un subgrupo abeliano normal de G y $T = G/A$, y sea $\pi : G \longrightarrow T$ el epimorfismo canónico. Sea $s : T \longrightarrow G$ una sección de π (es decir, $\pi \circ s = \mathrm{id}_T$), satisfaciendo la relación $s([1]) = 1$. Notemos que s no es necesariamente un homomorfismo; pero si lo es, entonces tenemos que $G \cong T \ltimes A$. El propósito de esta sección es determinar la estructura del grupo G cuando la sección s no es un homomorfismo.

Así que, con la notación anterior, suponemos que s no es homomorfismo. Podemos escribir, para cada $\lambda, \mu \in T$

$$s(\lambda)s(\mu) = f(\lambda, \mu)s(\lambda\mu), \tag{1.3.1}$$

para algún $f(\lambda, \mu) \in A$, ya que

$$\begin{aligned}\pi(s(\lambda)s(\mu)s(\lambda\mu)^{-1}) &= \pi(s(\lambda))\pi(s(\mu))\pi(s(\lambda\mu)^{-1}) \\ &= \lambda\mu(\lambda\mu)^{-1} \\ &= 1;\end{aligned}$$

luego $f(\lambda,\mu) = s(\lambda)s(\mu)s(\lambda\mu)^{-1} \in ker(\pi) = A$. La ecuación (1.3.1) permite definir una acción de grupos, del grupo T en el grupo abeliano A, definida por conjugación a través de la sección s, es decir,

$$\lambda a := s(\lambda)as(\lambda)^{-1},$$

para cada $\lambda \in T$ y para cada $a \in A$. Además, para cada $\lambda, \mu, \nu \in T$, se tiene lo siguiente:

$$\begin{aligned}(s(\lambda)s(\mu))s(\nu) &= (f(\lambda,\mu)s(\lambda\mu))s(\nu) \\ &= f(\lambda,\mu)(s(\lambda\mu)s(\nu)) \\ &= f(\lambda,\mu)f(\lambda\mu,\nu)s(\lambda\mu\nu) \qquad (1.3.2)\end{aligned}$$

y

$$\begin{aligned}s(\lambda)(s(\mu)s(\nu)) &= s(\lambda)(f(\mu,\nu)s(\mu\nu)) \\ &= s(\lambda)f(\mu,\nu)s(\lambda)^{-1}s(\lambda)s(\mu\nu) \\ &= s(\lambda)f(\mu,\nu)s(\lambda)^{-1}f(\lambda,\mu\nu)s(\lambda\mu\nu) \\ &= (\lambda f(\mu,\nu))f(\lambda,\mu\nu)s(\lambda\mu\nu). \qquad (1.3.3)\end{aligned}$$

Usando notación aditiva para el grupo abeliano A e igualando relaciones (1.3.2) y (1.3.3), y cancelando $s(\lambda\mu\nu)$, tenemos que

$$\lambda f(\mu,\nu) - f(\lambda\mu,\nu) + f(\lambda,\mu\nu) - f(\lambda,\mu) = 0. \qquad (1.3.4)$$

Una función $f : T \times T \longrightarrow A$ es llamada un 2-**cociclo** (o un **conjunto de factores**) si satisface la ecuación (1.3.4). Decimos que un 2-cociclo f es **normalizado** si $f(\lambda,\mu) = 0$ cuando $\lambda = 1$ o $\mu = 1$. Usando la ecuación (1.3.4), tenemos que f es normalizado si y sólo si $f(1,1) = 0$. Así que, puesto que $s(1) = 1$, dado un grupo G y un subgrupo abeliano normal A de G, con $T = G/A$, tenemos un 2-cociclo normalizado $f : T \times T \longrightarrow A$ cuya definición depende de la elección de la sección $s : T \longrightarrow G$.

Sea s' otra sección. Entonces, para cualquier $\lambda \in T$, $s'(\lambda) = h(\lambda)s(\lambda)$ para algún $h(\lambda) \in A$, por lo que tenemos una función $h : T \longrightarrow A$ que relaciona la secciones s y s'. Notemos que $h(1) = 0$. La función h es llamada 1-**cocadena**. Luego, si f' es el 2-cociclo definido por la sección s', al aplicar la ecuación (1.3.1), tenemos que

$$f'(\lambda, \mu) = h(\lambda) + \lambda h(\mu) - h(\lambda\mu) + f(\lambda, \mu) \tag{1.3.5}$$

Para una 1-cocadena $h : T \longrightarrow A$, la función $\partial h : T \times T \longrightarrow A$ definido por $\partial h(\lambda, \mu) = \lambda h(\mu) - h(\lambda\mu) + h(\lambda)$ es un 2-cociclo; es un tipo especial de 2-cociclo, llamada **2-cofrontera**. El conjunto de los 2-cociclos $T \times T \longrightarrow A$ es un grupo abeliano, denotado por $Z^2(T, A)$, con la operación punto a punto en A.

El conjunto de las 2-cofronteras es un subgrupo de $Z^2(T, A)$, denotado por $B^2(T, A)$. El grupo cociente $Z^2(T, A)/B^2(T, A)$ es llamado el **segundo grupo de cohomología de T con coeficientes en A**, y es denotado por $H^2(T, A)$. Dado cualquier 2-cociclo f, existe un 2-cociclo normalizado $\overline{f}$ tal que tienen la misma clase; de hecho, si $h : T \longrightarrow A$ es tal que $h(\lambda) = \lambda f(1, 1)$, entonces $\overline{f} = f - \partial h$ es normalizado.

Resumiendo, tenemos que si A es un es un subgrupo abeliano normal de un grupo G y $T = G/A$, entonces A es un T-módulo y existe, a través de la elección de una sección $s : T \longrightarrow G$, un elemento $f \in Z^2(T, A)$ normalizado cuya clase en $H^2(T, A)$ es independiente de s. De manera recíproca, dado un grupo T, un T-módulo A y una clase $[f] \in H^2(T, A)$, existe un grupo G conteniendo a A como un subgrupo abeliano normal, con $T \cong G/A$, tal que la clase $[f]$ ocurre como antes.

Sea $f \in Z^2(T, A)$ un representante normalizado de $[f]$. Consideramos $G(f) = T \times A$ y definimos una operación binaria como sigue: Para $(\lambda, a), (\mu, b) \in G(f)$, definimos

$$(\lambda, a)(\mu, b) = (\lambda\mu, a + \lambda b + f(\lambda, \mu)).$$

Notemos que si $f = 0$ entonces tenemos de nuevo el producto semidirecto. Pero, en general, tenemos que $(1, 0)$ es el elemento identidad, pues elegimos f normalizado. También tenemos que cada elemento tiene su inverso. Falta verificar que la operación es asociativa. Así pues, tenemos que

$$\begin{aligned} (\lambda, a)((\mu, b)(\nu, c)) &= (\lambda, a)(\mu\nu, b + \mu c + f(\mu, \nu)) \\ &= (\lambda\mu\nu, a + \lambda b + \lambda\mu c + \lambda f(\mu, \nu) + f(\lambda, \mu\nu)) \end{aligned}$$

y

$$\begin{aligned} ((\lambda, a)(\mu, b))(\nu, c) &= (\lambda\mu, a + \lambda b + f(\lambda, \mu))(\nu, c) \\ &= (\lambda\mu\nu, a + \lambda b + f(\lambda, \mu) + \lambda\mu c + f(\lambda\mu, c). \end{aligned}$$

Luego, la asociatividad es equivalente a la condición de que f sea un 2-cociclo. Por lo tanto, $G(f)$ es un grupo.

Por otro lado, supongamos que f y f' son dos 2-cociclos normalizados que representan a $[f]$. Entonces, los grupos $G(f)$ y $G(f')$, construidos como arriba, son isomorfos; de hecho, si $f' = f + \partial h$, con h una 1-cocadena que podemos suponer que satisface la relación $h(1) = 0$ (recordemos que A es escrito aditivamente), entonces la función $G(f) \longrightarrow G(f')$ dada por la correspondencia $(\lambda, a) \longmapsto (\lambda, a + h(\lambda))$ es un isomorfismo.

Sean T un grupo, A un T-módulo y G un grupo tales que A es subgrupo abeliano normal de G y $T \cong G/A$. Si f es un 2-cociclo normalizado con coeficientes en A, dado por la elección de una sección $s : T \longrightarrow G$, entonces se tiene que $G \cong G(f)$.

Con los resultados anteriores, tenemos el siguiente:

Teorema 1.3.1. *Sean T un grupo y A un T-módulo. Entonces, el grupo $H^2(T, A)$ parametriza, salvo isomorfismo, todos los grupos G que tienen a A como subgrupo abeliano normal y a T como el cociente correspondiente.*

□

Capítulo 2

Teoría de Kummer y extensiones radicales

En este capítulo desarrollaremos la Teoría de Kummer que es esencial para la demostración de nuestro teorema principal (Teorema 3.2.1).

2.1. Definiciones y resultados preliminares

Definición 2.1.1. *Sea E/F una extensión de campos. Decimos que E/F es* ***abeliana*** (*resp.* ***cíclica***) *si E/F es una extensión de Galois y su grupo de Galois,* $\mathrm{Gal}(E/F)$*, es abeliano* (*resp. cíclico*)*.*

Lema 2.1.2. *Sea F un campo de característica $p > 0$ y sea E/F una extensión algebraica. Si F_s es la cerradura separable de F en E, entonces F_s/F es separable y E/F_s es puramente inseparable.*

Demostración. F_s/F es separable por la definición de F_s. Si K es la cerradura separable de F_s en E, entonces K/F es separable. Por lo tanto $K = F_s$ y por lo tanto E/F_s es puramente inseparable. □

Lema 2.1.3. *Sea F un campo de característica $p > 0$ y sea E/F una extensión finita. Entonces,*

(*i*) *E/F es puramente inseparable si y sólo si $[E : F]_s = 1$. En particular, si E/F es puramente inseparable, entonces $[E : F]$ es una potencia de p.*

(*ii*) $[E : F]_s = [F_s : F]$, *con* F_s *la cerradura separable de* F *en* E.

Demostración.

(*i*) Inmediata.

(*ii*) E/F_s es puramente inseparable, luego $[E : F_s]_s = 1$. Como

$$[E : F]_s = [F_s : F]_s[E : F_s]_s \text{ y } [F_s : F]_s = [F_s : F],$$

se tiene que $[E : F]_s = [F_s : F]$. Como se quería.

□

Lema 2.1.4. *Sean* p *primo impar,* $n = p^k$, F *un campo con característica distinta de* p *y* F_n. *Entonces* F_n/F *es cíclica. Si* $p = 2$ *y* $k \geq 3$, *entonces* F_n/F *es cíclica o* $\mathrm{Gal}(F_n/F)$ *es el producto directo de un grupo cíclico de orden 2 y otro de orden* 2^{t-2} *con* $t \leq k$.

Lema 2.1.5. *Sea* E/F *una extensión normal, y sea* K *un campo intermedio tal que* K/F *es normal. Entonces*

$$\frac{\mathrm{Gal}(E/F)}{\mathrm{Gal}(E/K)} \cong \mathrm{Gal}(K/F).$$

Demostración. Como K/F es normal, la restricción de cualquier $\sigma \in \mathrm{Gal}(E/F)$ a K es un automorfismo de K, es decir, $\sigma|_K \in \mathrm{Gal}(K/F)$. Luego, la correspondencia $\sigma \longmapsto \sigma|_K$ de $\mathrm{Gal}(E/F)$ en $\mathrm{Gal}(K/F)$ es un epimorfismo tal que su núcleo es $\mathrm{Gal}(E/K)$. Aplicando el Primer Teorema de Isomorfismo de grupos, se tiene el resultado.

□

Lema 2.1.6. *Sean* E/F *y* K/F *extensiones finitas de campos, con* E/F *Galois, y supóngase que* E *y* K *son subcampos de un campo común. Entonces* EK/K *y* $E/(E \cap K)$ *son extensiones de Galois con grupos de Galois isomorfos.*

Demostración. Las extensiones EK/K y $E/(E \cap K)$ son obviamente normales y separables, es decir, son de Galois. Si $\sigma \in \mathrm{Gal}(EK/K)$, entonces $\sigma|_E$ es un F-homomorfismo $E \longrightarrow EK$, luego es un elemento de $\mathrm{Gal}(E/F)$, pues E/F es normal. La correspondencia $\sigma \longmapsto \sigma|_E$ de $\mathrm{Gal}(EK/K)$ en $\mathrm{Gal}(E/F)$ claramente es un homomorfismo. Si $\sigma|_E$ es la identidad, entonces σ debe ser la identidad en EK, pues

también deja fijo a los elementos de K. Por lo tanto, el homomorfismo dado es inyectivo. Sea S su imagen. Entonces, los elementos de S dejan fijo a $E \cap K$ y, de manera recíproca, si un elemento $\lambda \in E$ es dejado fijo por los elementos de S, tenemos que λ queda fijo bajo los elementos de $\mathrm{Gal}(EK/K)$; así que, $\lambda \in K$ y $\lambda \in E \cap K$. Luego, $E \cap K$ es el campo fijo de S. En consecuencia, $S = \mathrm{Gal}(E/E \cap K)$. Por lo tanto, los grupos son isomorfos. □

2.2. Extensiones cíclicas

Teorema 2.2.1. *Sea E/F una extensión de campos con F conteniendo una raíz n-ésima primitiva de la unidad, donde n es primo relativo con la característica de F. Entonces,*

(*i*) *E/F es cíclica de grado un divisor de n si y sólo si $E = F(\lambda)$, para alguna λ tal que $\lambda^n \in F$.*

(*ii*) *El polinomio irreducible sobre F de cualquier $\lambda \in E$, con $\lambda^n \in F$, es $X^d - \lambda^d$ con $d|n$.*

Demostración.

(*i*) Supongamos que E/F es cíclica de grado d divisor de n. Entonces, el grupo $\mathrm{Gal}(E/F)$ es generado por un elemento de orden d, digamos σ. Sea δ una raíz d-ésima primitiva de la unidad en F. Luego $\sigma(\lambda) = \delta\lambda$, para algún $\lambda \in E$ distinto de cero. El polinomio irreducible de λ sobre F tiene d raíces distintas: $\lambda, \sigma(\lambda) = \delta\lambda, \ldots, \sigma^{d-1}(\lambda) = \delta^{d-1}\lambda$. Por lo tanto, $E = F(\lambda)$. Más aún,

$$\sigma(\lambda^d) = \sigma(\lambda)^d = (\delta\lambda)^d = \lambda^d,$$

así $\lambda^d \in F$ y $\lambda^n \in F$.

De manera recíproca, supongamos que $E = F(\lambda)$, para algún $\lambda \in E$ tal que $\lambda^n \in F$. Sea ϵ una raíz n-ésima primitiva de la unidad. Entonces

$$X^n - \lambda^n = \prod_{i=1}^{n} (X - \lambda\epsilon^i)$$

y por lo tanto E es el campo de descomposición del polinomio $X^n - \lambda^n \in F[X]$. Como $X^n - \lambda^n$ tiene n raíces distintas, se tiene que E/F es de Galois. Tenemos el homomorfismo inyectivo

$$\mathrm{Gal}(E/F) \longrightarrow \langle \epsilon \rangle$$

que manda cada $\sigma \in \mathrm{Gal}(E/F)$ a $a_\sigma \in \langle \epsilon \rangle$, donde $\sigma(\lambda) = \lambda a_\sigma$. Luego, el grupo $\mathrm{Gal}(E/F)$ es cíclico de orden un divisor de n.

(*ii*) Sea $\lambda \in E$ tal que $\lambda^n \in F$ y sea $K = F(\lambda)$. Entonces, por (*i*), K/F es cíclica de grado d divisor de n y $\lambda^d \in F$. Por lo tanto $X^d - \lambda^d$ es el polinomio irreducible de λ sobre F.

□

Corolario 2.2.2. *Sea E/F una extensión de campos de grado n, donde F contiene una raíz n-ésima primitiva de la unidad, con n primo relativo a la característica. Entonces, la extensión E/F es cíclica si y sólo si $E = F(\lambda)$ para algún $\lambda \in E$ tal que $X^n - \lambda^n$ es el polinomio irreducible de λ sobre F.*

Demostración. Es consecuencia inmediata del Teorema 2.2.1.

□

Teorema 2.2.3. (Artin-Schreir). *Sea F un campo de característica $p > 0$ y sea E/F una extensión de campos. Entonces,*

(*i*) *E/F es cíclica de grado p si y sólo si $E = F(\lambda)$ para algún $\lambda \in E$ tal que $\lambda^p - \lambda \in F$ y $\lambda \notin F$.*

(*ii*) *El polinomio irreducible sobre F de cualquier $\lambda \in E$ tal que $\lambda^p - \lambda \in F$ y $\lambda \notin F$ es*

$$X^p - X - (\lambda^p - \lambda).$$

(*iii*) *Para cualquier $a \in F$, el polinomio $X^p - X - a$ es irreducible ó se factoriza en p factores lineales sobre F.*

Demostración. Notemos primero que si $a \in F$ y α es raíz del polinomio $X^p - X - a$, entonces $\alpha + i$ es también raíz para $i = 0, 1, \ldots, p-1$, pues

$$(\alpha + i)^p = \alpha^p + i^p = \alpha^p + i.$$

Así, $X^p - X - a$ se factoriza en p factores lineales distintos sobre $F(\alpha)$ y, por lo tanto, $F(\alpha)/F$ es de Galois.

Supongamos ahora que $E = F(\lambda)$ para algún $\lambda \in E$ tal que $\lambda^p - \lambda \in F$ y $\lambda \notin F$. Como λ es una raíz de $X^p - X - (\lambda^p - \lambda)$, E/F es de Galois. Dado $\sigma \in \mathrm{Gal}(E/F)$, existe un único $i_\sigma \in \{0, 1, \ldots, p-1\}$ tal que $\sigma(\lambda) = \lambda + i_\sigma$. Consideremos la función:

$$\begin{array}{ccc} \mathrm{Gal}(E/F) & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \sigma & \longmapsto & i_\sigma + p\mathbb{Z}, \end{array}$$

que en efecto está bien definida por la unicidad de i_σ; además, es un homomorfismo inyectivo. Como $\mathbb{Z}/p\mathbb{Z}$ es cíclico de orden p y $E \neq F$, concluimos que $\mathrm{Gal}(E/F)$ es cíclico de orden p. Luego E/F es cíclica de grado p y $X^p - X - (\lambda^p - \lambda)$ es el polinomio mínimo de λ sobre F. Esto prueba (ii) y una dirección de (i).
Recíprocamente, supongamos que E/F es cíclica de grado p. Sea σ un generador de $\mathrm{Gal}(E/F)$ de orden p. Para algún $\lambda \in F$ se tiene que $\sigma(\lambda) = \lambda + 1$. Luego $\sigma(\lambda^p) = \lambda^p + 1$ y $\sigma(\lambda^p - \lambda) = (\lambda^p + 1) - (\lambda + 1) = \lambda^p - \lambda$, por lo que $\lambda^p - \lambda \in F$. Pero $\lambda \notin F$ pues $\sigma(\lambda) \neq \lambda$. Luego $E = F(\lambda)$, probando (i).
Para probar (iii), necesitamos verificar que si ninguna raíz de $X^p - X - a$ está en F, entonces $f(X) = X^p - X - a$ es irreducible sobre F. Supongamos que $f(X)$ no es irreducible sobre F, tenemos así que

$$f(X) = g(X)h(X),$$

con $g(X), h(X) \in F[X]$ y $1 \leq \mathrm{gr}(g) < p$. Como

$$f(X) = \prod_{i=0}^{p-1}(X - \alpha - i),$$

con α raíz de $f(X)$, tenemos que $g(X)$ es el producto de $X - \alpha - i$ para algunos enteros $i \in \{0, \ldots, p-1\}$. Si $d = \mathrm{gr}(g)$, entonces el coeficiente de X^{d-1} es una suma de términos $-(\alpha + i)$ tomados sobre d enteros i. Luego es igual a $-da + j$ para algún entero j. Pero $d \neq 0 \in F$, y como los coeficientes de $g(X)$ están en F, $\alpha \in F$, lo que es una contradicción.

□

2.3. Teoría de Kummer

Sean F un campo y n un entero positivo. Una extensión de Galois E/F es de **exponente** n si el exponente de $\mathrm{Gal}(E/F)$ divide a n, es decir, si $\sigma^n = 1$ para todo $\sigma \in \mathrm{Gal}(E/F)$. Por extensión de **Kummer de exponente** n entenderemos una extensión abeliana E/F de exponente finito n, donde F contiene una raíz n-ésima primitiva de la unidad. Se sigue que para cualquier extensión de este tipo, la característica de F no divide a n.

A lo largo de esta discusión, el campo base F estará fijo, y toda extensión algebraica sobre F estará contenida en una cerradura algebraica $\bar{F}$ fija de F. Además, asumimos que F contiene una raíz n-ésima primitiva de la unidad, la cual será denotada por ζ_n. En cualquier campo, ζ_n denotará una raíz n-ésima primitiva de la unidad cuando ésta exista. Nuestro objetivo en esta sección es clasificar todas las extensiones finitas de Kummer E/F de exponente n. Así pues, si E/F es una extensión finita de Kummer de exponente n, denotaremos por $G = \mathrm{Gal}(E/F)$.

Sea G un grupo abeliano finito. Escribimos

$$\mathrm{Hom}(G, \langle\zeta_n\rangle) = \{\chi : G \longrightarrow \langle\zeta_n\rangle \mid \chi \text{ es un homomorfismo}\}.$$

Entonces $\mathrm{Hom}(G, \langle\zeta_n\rangle)$ es un grupo bajo la multiplicación de valores, es decir,

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g),$$

para cada $\chi_1, \chi_2 \in \mathrm{Hom}(G, \langle\zeta_n\rangle)$ y para cada $g \in G$.

Por otro lado, el conjunto G^* de todos los homomorfismos de G a $\mathbb{C}^*$ es también un grupo bajo la multiplicación de valores, llamado el **dual de** G. Los elementos del grupo G^* son llamados **caracteres de G**. Si el exponente de G divide a n, entonces la imagen de cualquier caracter $\chi \in G^*$ está contenido en el grupo cíclico de raíces n-ésimas de la unidad de $\mathbb{C}^*$. Así que

$$\mathrm{Hom}(G, \mathbb{C}^*) = \mathrm{Hom}(G, \langle\zeta_n\rangle),$$

donde aquí ζ_n es una raíz n-ésima primitiva de la unidad en $\mathbb{C}^*$.

Dado un subgrupo H de G, se define el **ortogonal de** H como:

$$H^\perp = \{\chi \in G^* \mid \chi(h) = 1 \text{ para todo } h \in H\}.$$

Claramente tenemos un isomorfismo natural tal que

$$H^\perp \cong (G/H)^*.$$

Lema 2.3.1. *Si G es un grupo abeliano finito, entonces $G \cong G^*$ (de manera no canónica) y $G^{**} \cong G$ (canónicamente).*

Demostración. Es fácil verificar que $(G_1 \times G_2)^* \cong G_1^* \times G_2^*$. Por lo tanto, de acuerdo con la descomposición cíclica de los grupos abelianos finitos, basta probar que $G \cong G^*$, con G cíclico con orden n. Sea g un generador de G y sea $\chi : G \longrightarrow \mathbb{C}^*$ un homomorfismo. Entonces $\chi(g)^n = 1$, es decir, $\chi(g)$ es una raíz n-ésima de la unidad. Sea ζ_n una raíz n-ésima primitiva de la unidad en $\mathbb{C}$, y sea $\psi : G^* \longrightarrow \langle \zeta_n \rangle$ dada por $\psi(\chi) = \chi(g)$. Es obvio que ψ es un homomorfismo inyectivo. Y como para algún $k \geq 1$, $\chi(g) = \zeta_n^k$, tenemos que cada elemento de $\langle \zeta_n \rangle$ genera un elemento de G^*; en consecuencia, ψ también es suprayectiva. Así pues, $G \cong G^*$.

Por otro lado, para cada $g \in G$ y para cada $\chi \in G^*$, definimos $\psi_g(\chi) = \chi(g)$. Entonces $\psi_g \in G^{**}$ y la correspondencia $g \longrightarrow \psi_g$ determina un homomorfismo de G a G^{**}. Si $\chi(g) = 1$ para todo $\chi \in G^*$ y $H = \langle g \rangle$, entonces

$$G^* = H^\perp \cong (G/H)^*.$$

Por lo tanto, de lo anterior, se tiene que $G \cong G/H$, lo cual implica que $H = 1$. Así, $g = 1$ y el mapeo determinado por la correspondencia $g \longrightarrow \psi_g$ es inyectivo. Como $|G| = |G^*| = |G^{**}|$, se sigue que éste debe de ser un isomorfismo.

□

Ahora retomamos nuestra discusión de extensiones de Kummer E/F de exponente n fijo. Seguimos denotando a ζ_n como una raíz n-ésima primitiva de la unidad en F.

Usaremos el símbolo $\sqrt[n]{a}$, con $a \in F$, para denotar cualquier elemento $\lambda \in \bar{F}$ tal que $\lambda^n = a$. $\sqrt[n]{a}$ es llamada una **raíz n-ésima de** a. Hay exactamente n elementos de tales raíces n-ésimas de a, a saber, $\zeta_n^i \lambda$, $0 \leq i \leq n-1$. Observamos que el campo $F(\lambda)$ es el mismo sin importar cual sea la n-ésima raíz λ de a seleccionada. Siempre supondremos que $\sqrt[n]{a}$ es fija. Denotaremos este campo por $F(\sqrt[n]{a})$.

Denotamos por $(F^*)^n$ al subgrupo de F^* que consiste de todas las n-potencias de elementos de F^*. Si H es un subgrupo de F^* conteniendo a $(F^*)^n$, denotamos por F_H la composición de todos los campos $F(\sqrt[n]{a})$ con $a \in H$, y es caracterizado de manera única por H como un subcampo de $\bar{F}$. Notemos también que F_H es el campo de descomposición de la familia de polinomios

$$X^n - a, \text{ donde } a \in H.$$

Lema 2.3.2.

(*i*) *Para cualquier subgrupo H de F^* conteniendo $(F^*)^n$, F_H/F es una extensión de Kummer de exponente n.*

(*ii*) *Si E/F es una extensión de Kummer de exponente n, entonces $E = F_H$ con $H = (E^*)^n \cap F^*$.*

(*iii*) *E/F es una extensión de Kummer de exponente m si y sólo si F contiene una raíz m-ésima primitiva de la unidad y E es el campo de descomposición de una familia de polinomios de la forma $X^m - a$, con $a \in F$.*

Demostración.

(*i*) Por el Teorema 2.2.1(*i*), $F(\sqrt[n]{a})/F$ es una extensión cíclica de grado un divisor de n. Por lo tanto, para cualquier $\sigma \in \mathrm{Gal}(F_H/F)$, la restricción de σ^n de $F(\sqrt[n]{a})$ es 1.

Así pues, $\sigma^n = 1$, ya que F_H es generado por todos los elementos de forma $\sqrt[n]{a}$, con $a \in H$. Más aún, F_H/F es una extensión abeliana, pues es la composición de extensiones cíclicas.

(*ii*) Claramente, $F_H \subseteq E$. Más aún, E/F es la composición de sus subextensiones finitas de E'/F. Como el grupo abeliano finito $\mathrm{Gal}(E'/F)$ es el producto directo de grupos cíclicos, y cada uno de los cuales puede ser visto como el grupo de Galois de una subextensión cíclica de E'/F, concluimos que E'/F (y por lo tanto E/F) es la composición de sus subextensiones cíclicas.

Supóngase que K/F es una subextensión cíclica de E/F. Entonces $\mathrm{Gal}(K/F)$ es de orden un divisor de n, así que, por el Teorema 2.2.1(*i*), $K = F(\sqrt[n]{a})$, para algún $a \in (E^*)^n \cap F^* = H$. Por lo tanto, $K \subseteq F_H$ y así $E \subseteq F_H$, como se quería.

(*iii*) Supóngase que F contiene una raíz m-ésima primitiva de la unidad. Si E es el campo de descomposición de una familia de polinomios de la forma $X^m - a$, con $a \in F$, entonces E es el compuesto de campos $F(\sqrt[m]{a})$. De aquí que, por el argumento de (*i*), E/F es una extensión de Kummer de exponente m. La recíproca es cierta en virtud de (*ii*).

□

Lema 2.3.3. *Sea E/F una extensión de Kummer de exponente n y sea*

$$H = (E^*)^n \cap F^*.$$

Entonces, para cualquier $a \in H$, el mapeo

$$\begin{array}{rccc} \chi_a & : & \mathrm{Gal}(E/F) & \longrightarrow & \langle \zeta_n \rangle \\ & & \sigma & \longmapsto & \dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{array}$$

es un homomorfismo que no depende de la elección de $\sqrt[n]{a}$*, y cuyo núcleo es el grupo* $\mathrm{Gal}(E/F(\sqrt[n]{a}))$*. En particular, la extensión* $F(\sqrt[n]{a})/F$ *es una extensión cíclica de grado un divisor de* n*.*

Demostración. Sea λ una raíz n-ésima fija a en F tal que $\lambda\zeta_n^i$, $0 \leq i \leq n-1$, son todas las raíces n-ésimas distintas de a. Entonces, para $\sqrt[n]{a} = \lambda\zeta_n^i$, tenemos

$$\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \frac{\sigma(\lambda)\zeta_n^i}{\lambda\zeta_n^i} = \frac{\sigma(\lambda)}{\lambda}$$

probando que χ_a es independiente de la elección de $\sqrt[n]{a}$. Más aún, dados $\sigma_1, \sigma_2 \in \mathrm{Gal}(E/F)$, tenemos $\sigma_i(\lambda)/\lambda = \zeta_n^{k_i}$, para algún $k_i \geq 1$, y

$$\chi_a(\sigma_1\sigma_2) = \frac{(\sigma_1\sigma_2)(\lambda)}{\lambda} = \frac{\sigma_1(\lambda\zeta_n^{k_2})}{\lambda} = \zeta_n^{k_1+k_2} = \chi_a(\sigma_1)\chi_a(\sigma_2).$$

Finalmente, es claro que $\mathrm{Ker}(\chi_a) = \mathrm{Gal}(E/F(\sqrt[n]{a}))$, y que la extensión $F(\sqrt[n]{a})/F$ es cíclica de grado un divisor de n debido al Teorema Fundamental de la Teoría de Galois Finita.

□

Los homomorfismos χ_a en el Lema 2.3.3 serán referidos como los **caracteres de Kummer de** $\mathrm{Gal}(E/F)$ **correspondientes a** a. Lo que uno entiende comúnmente bajo el nombre de Teoría de Kummer es el resultado del siguiente.

Teorema 2.3.4. *Sea* F *un campo conteniendo una raíz* n*-ésima primitiva de la unidad.*

(*i*) *El mapeo determinado por la correspondencia* $H \longrightarrow F_H$ *es una biyección entre el conjunto de subgrupos de* F^* *conteniendo* $(F^*)^n$ *y las extensiones de Kummer de* F *de exponente* n*. La inversa de este mapeo está dado por la correspondencia* $E \longmapsto (E^*)^n \cap F^*$*.*

(*ii*) *Si* E/F *es una extensión finita de Kummer de exponente* n *y* $H = (E^*)^n \cap F^*$*, entonces el mapeo*

$$\begin{aligned} H/(F^*)^n &\longrightarrow \mathrm{Hom}(\mathrm{Gal}(E/F), \langle\zeta_n\rangle) \\ a(F^*)^n &\longmapsto \chi_a \end{aligned}$$

es un isomorfismo. En particular, $H/(F^*)^n$ *es finito y*

$$\mathrm{Gal}(E/F) \cong H/(F^*)^n \text{ y } [E:F] = |H/(F^*)^n|.$$

Demostración. Sea $G = \mathrm{Gal}(E/F)$. Si $a, b \in H$ y $\alpha^n = a$, $\beta^n = b$, entonces

$$(\alpha\beta)^n = ab$$

y por lo tanto

$$\sigma(\alpha\beta)/\alpha\beta = (\sigma(\alpha)/\alpha)(\sigma(\beta)/\beta), \text{ para todo } \sigma \in G.$$

Si $a = \lambda^n$, con $\lambda \in F^*$, entonces $\chi_a(\sigma) = \sigma(\lambda)/\lambda = 1$, para toda $\sigma \in G$. Por lo tanto el mapeo en (ii) es un homomorfismo. Supóngase que $a \in H$ es tal que $\chi_a = 1$, es decir, $\sigma(\alpha) = \alpha$ para toda $\sigma \in G$, donde $\alpha^n = a$. Por el Lema 2.3.2(ii), $E = F_H$ y $F(\alpha)$ es un subcampo de E. Si α no está en F, existe un automorfismo de $F(\alpha)$ sobre F el cual no es la identidad. Extendemos este automorfismo de E y lo denotamos por σ_0. Entonces $\sigma_0(\alpha) \neq \alpha$, contradicción. Así tenemos una sucesión exacta.

$$1 \longrightarrow H/(F^*)^n \longrightarrow \mathrm{Hom}(G, \langle\zeta_n\rangle). \tag{2.3.1}$$

Note que el mapeo $G \longrightarrow \mathrm{Hom}(H/(F^*)^n, \langle\zeta_n\rangle)$, dada por la correspondencia $\sigma \longmapsto f_\sigma$, donde $f_\sigma(a(F^*)^n) = \chi_a(\sigma)$, es un homomorfismo. Si $\chi_a(\sigma) = 1$, para todo $a \in H$, entonces para todo generador α de E, con $\alpha^n = a \in H$, tenemos $\sigma(\alpha) = \alpha$ y por lo tanto $\sigma = 1$. Así tenemos una sucesión exacta.

$$1 \longrightarrow G \longrightarrow \mathrm{Hom}(H/(F^*)^n, \langle\zeta_n\rangle). \tag{2.3.2}$$

Aplicando el primer isomorfismo del Lema 2.3.2, se sigue de (2.3.1), (2.3.2) y del hecho de que E/F es finita, que $H/(F^*)^n$ es finito y, si este es el caso, entonces $G \cong H/(F^*)^n$.

Para completar la prueba de (ii), necesitamos sólo verificar que el mapeo dado es suprayectivo. Pero, por lo anterior, esto es cierto debido a que la extensión E/F es finita.

Para probar (i), es suficiente, por el Lema 2.3.2(i), (ii), mostrar que $F_{H_1} \subseteq F_{H_2}$ implica $H_1 \subseteq H_2$, para cualesquiera subgrupos H_1, H_2 de F^* conteniendo a $(F^*)^n$. Si $b \in H_1$, entonces $F(\sqrt[n]{b}) \subseteq F_{H_2}$ y $F(\sqrt[n]{b})$ está contenido en una subextensión finitamente generada de F_{H_2}. Luego, podemos asumir que $H_2/(F^*)$ es finitamente generada, por lo tanto finito. Sea H_3 un subgrupo de F^* generado por H_2 y b. Entonces, $F_{H_2} = F_{H_3}$ y, por lo que vimos anteriormente, el grado de este campo sobre F es precisamente

$$|H_2/(F^*)^n| \text{ o } |H_3/(F^*)^n|.$$

Por lo tanto $H_2 = H_3$, con $b \in H_2$ y de aquí que $H_1 \subseteq H_2$, como afirmamos.

□

Ahora probaremos algunas consecuencias importantes.

Corolario 2.3.5. *Sea E/F una extensión finita de Kummer de exponente n, sea $G = \mathrm{Gal}(E/F)$ y sea $\sqrt[n]{F^*}$ que denota al subgrupo E^* que consiste de todas las raíces n-ésimas de elementos en F^*. Entonces:*

$$G \cong \sqrt[n]{F^*}/F^* \cong (\sqrt[n]{F^*})^n/(F^*)^n.$$

Demostración. Sea $H = (E^*)^n \cap F^*$. Entonces $H = (\sqrt[n]{F^*})^n$ y así el mapeo

$$\begin{array}{ccc} \sqrt[n]{F^*} & \longrightarrow & H/(F^*)^n \\ x & \longmapsto & x^n(F^*)^n \end{array}$$

es un homormofismo suprayectivo de grupos; su núcleo es F^* ya que F contiene una raíz n-ésimas primitiva de la unidad. Así, por el Teorema 2.3.4(ii),

$$\sqrt[n]{F^*}/F^* \cong H/(F^*)^n \cong G$$

y el resultado se tiene.

□

Corolario 2.3.6. *Sea p un primo y sea F un campo conteniendo una raíz p-ésima primitiva de la unidad. Supóngase que α es un elemento de una extensión de campo de F tal que $\alpha^p \in F$. Si $\beta \in F(\alpha)$ es tal que $\beta^p \in F$, entonces para algún $k \in \mathbb{Z}$ y para algún $a \in F$, $\beta = \alpha^k a$.*

Demostración. La afirmación es obvia en el caso $\alpha \in F$. Supóngase que $\alpha \notin F$. Así $\alpha^p \notin F^p$, pues F contiene todas las raíces p-ésimas de la unidad. Esto implica que $[F(\alpha) : F] = p$. Así que, $F(\alpha)/F$ es una extensión de Kummer de exponente p y $F(\alpha) = F_H$, donde $H = \langle \alpha^p \rangle (F^*)^p$. Si $\beta \in F$, entonces $\beta = \alpha^p(\alpha^{-p}\beta)$ y $\alpha^{-p}\beta \in F$. Podemos por tanto suponer que $\beta \notin F$. Luego, $F(\alpha) = F(\beta)$ y $F(\beta) = F_{H_1}$, donde $H_1 = \langle \beta^p \rangle (F^*)^p$. Por el Teorema 2.3.4($i$), $H = H_1$ y de aquí que

$$\beta^p = \alpha^{pk} c^p, \text{ para algún } k \in \mathbb{Z},\ c \in F^*.$$

Tomando raíz p-ésima, obtenemos que $\beta = \alpha^k a$, para algún $a \in F$. □

Es útil saber que se puede prescindir de la condición de que F contenga una raíz p-ésima primitiva de la unidad. Así tenemos más generalmente lo siguiente:

Corolario 2.3.7. *Sea p un primo y sea F un campo con característica distinta de p. Supóngase que α es un elemento de una extensión del campo F tal que $\alpha^p \in F - F^p$. Si $\beta \in F(\alpha)$ es tal que $\beta^p \in F$, entonces $\beta = \alpha^k a$, para algún $k \in \mathbb{Z}$ y algún $a \in F$.*

Demostración. Como $\alpha^p \notin F^p$, tenemos $[F(\alpha) : F] = p$. Sea ζ una raíz p-ésima primitiva de la unidad sobre F. El grado $[F(\zeta) : F] \leq p-1$; por lo tanto, puesto que los grados $[F(\alpha) : F]$ y $[F(\zeta) : F]$ son primos relativos, se tiene que $F(\alpha) \cap F(\zeta) = F$. Consideremos $F(\zeta)(\alpha)$ sobre $F(\zeta)$. Entonces, $\alpha^p \in F(\zeta)$, $\beta^p \in F(\zeta)$, y $F(\zeta)$ contiene a ζ.

Aplicando el Corolario 2.3.6, concluimos que $\beta = \alpha^k a$ para algún $k \in \mathbb{Z}$ y algún $a \in F(\zeta)$. Pero

$$a = \beta\alpha^{-k} \in F(\zeta) \cap F(\alpha) = F,$$

lo que concluye la demostración.

□

Por la **extensión de Kummer maximal de F de exponente** n entendemos el compuesto de todas las extensiones de Kummer de F de exponente n. Es claro que dicha extensión es la más grande extensión de Kummer de F de exponente n.

Corolario 2.3.8. *Sea E la extensión maximal de Kummer de F de exponente n. Entonces*

$$\mathrm{Hom}(\mathrm{Gal}(E/F), \langle \zeta_n \rangle) \cong F^*/(F^*)^n.$$

Demostración. Debido al Teorema 2.3.4, es suficiente verificar que $(E^*)^n \cap F^* = F^*$.

Así, dado $\lambda \in F^*$ y $a = \sqrt[n]{\lambda}$, tenemos que $a \in E$, ya que $F(a)/F$ es una extensión de Kummer de exponente n. Por lo tanto $\lambda = a^n \in (E^*)^n \cap F^*$ como se requería.

□

2.4. Extensiones radicales y resultados relacionados

Sea E/F una extensión de campos. Escribimos $\mathrm{tor}(E^*/F^*)$ para el subgrupo torsión del grupo cociente E^*/F^*. Decimos que E/F es una **extensión radical** si E es de la forma

$$E = F(\lambda_1, \ldots, \lambda_m), \tag{2.4.1}$$

con

$$\lambda_i^{n_i} \in F(\lambda_1, \ldots, \lambda_{i-1}) \quad (1 \leq i \leq m), \tag{2.4.2}$$

para algún $n_i \in \mathbb{N}$. Es claro que cualquier extensión radical es una extensión finita. El caso $m = 1$, es decir, que E es de la forma $E = F(\lambda)$, con $\lambda^n \in F$ para algún $n \geq 1$, es de particular importancia. Nos referiremos a tales extensiones E/F como **extensiones radicales simples**. Así, si E/F es una extensión radical que satisface (2.4.1) y (2.4.2), entonces

$$F \subseteq F(\lambda_1) \subseteq F(\lambda_1, \lambda_2) \subseteq \cdots \subseteq F(\lambda_1, \ldots, \lambda_m) = E$$

y cada extensión $F(\lambda_1, \ldots, \lambda_i)/F(\lambda_1, \ldots, \lambda_{i-1})$ es una extensión radical simple. Una **extensión radical irreducible** es una extensión radical simple de la forma $F(\lambda)/F$ tal que $\lambda^n \in F$, con $n = [F(\lambda) : F]$. Luego, E/F es una extensión radical irreducible si y sólo si E es de la forma $E = F(\lambda)$, donde λ es una raíz de un binomial irreducible sobre F de la forma $X^n - a$, con $a \in F$.

Dicho de otra manera, una extensión finita E/F es una extensión radical irreducible si y sólo si $E = F(\lambda)$, para algún $\lambda \in E^*$ tal que el orden de λF^* en E^*/F^* es igual al grado de λ sobre F.

Lema 2.4.1. *Sea E/F una extensión de campos de grado n, con F conteniendo una raíz n-ésima primitiva de la unidad. Entonces E/F es radical irreducible si y sólo si E/F es cíclica.*

Demostración. Se sigue inmediatamente del Corolario 2.2.2.

□

Para analizar las extensiones radicales irreducibles de un campo F, debemos investigar bajo qué condiciones el polinomio $X^n - a$ es irreducible sobre F, para cualquier $a \in F$ dado. La siguiente observación muestra que podemos suponer que n es una potencia de un primo.

Lema 2.4.2. *Sean F cualquier campo, a un elemento de F, y m y n enteros positivos primos relativos. Entonces $X^{mn} - a$ es irreducible sobre F si y sólo si $X^m - a$ y $X^n - a$ son irreducibles sobre F.*

Demostración. Como $X^{mn}-a=(X^m)^n-a=(X^n)^m-a$, si $X^{mn}-a$ es irreducible, entonces también X^m-a y X^n-a lo son. De manera recíproca, supongamos que X^m-a y X^n-a son ambos irreducibles sobre F. Sea E el campo de descomposición de $X^{mn}-a$ y sea $\lambda \in F$ una raíz de $X^{mn}-a$. Entonces λ^n es una raíz de X^m-a y λ^m es una raíz de X^n-a, así que

$$[F(\lambda^m):F]=n \quad \text{y} \quad [F(\lambda^n):F]=m.$$

Por lo tanto, n y m dividen a $[F(\lambda):F]$ y, de aquí que, nm divide $[F(\lambda):F]$, pues $(n,m)=1$. Pero λ es una raíz de $X^{nm}-a$, así que $[F(\lambda):F]\leq nm$. Esto demuestra que $[F(\lambda):F]=mn$ y, por lo tanto, $X^{mn}-a$ es irreducible sobre F.

□

Procederemos a analizar el caso de potencia de un primo. Primero investigaremos el caso primo.

Lema 2.4.3. *Sean p un primo y a un elemento del campo F. Entonces X^p-a es irreducible sobre F si y sólo si $a\notin F^p$.*

Demostración. Si $a=\mu^p$, para algún $\mu\in F$, entonces μ es una raíz de X^p-a y por lo tanto X^p-a no es irreducible. De manera recíproca, supongamos que $a\notin F^p$. Procederemos por contradicción y denotaremos por f un factor irreducible de X^p-a de grado k, $1\leq k<p$. Sea c el término constante de f. Todas las raíces de X^p-a (en algún campo de descomposición) tienen la forma $\zeta_p u$, donde u es una raíz fija y ζ_p es una raíz p-ésima de la unidad. Como $\pm c$ es producto de k de esas raíces, tenemos que $\pm c=\delta u^k$, con $\delta^p=1$. Como $(k,p)=1$, existen enteros r y s tales que $rk+sp=1$. Luego,

$$u=u^{rk}u^{sp}=(\pm c/\delta)^r a^s.$$

Por lo tanto $u\delta^r$ está en F. Pero $a=(u\delta^r)^p$, contradicción.

□

Lema 2.4.4. *Sean p un primo, a un elemento del campo F y X^p-a irreducible sobre F. Si λ es una raíz de X^p-a, entonces*

(*i*) *Si p es impar, o si $p=2$ y la característica de F es 2, entonces $\lambda\notin F(\lambda)^p$.*

(*ii*) *Si $p=2$ y la característica de F es distinta de 2, entonces $\lambda\in F(\lambda)^2$ si y sólo si $a\in -4F^4$.*

Demostración.

(i) Supongamos, por el contrario, que $\lambda = \omega^p$ para algún $\omega \in F(\lambda)$. El caso en el que la característica de F es p es directo: pues ω es un polinomio en λ y las p-ésimas potencias son tomadas término a término, tenemos $\omega^p \in F$, lo cual es imposible, por el Lema 2.3.3. Ahora supongamos que la característica de F es distinta de p y adjuntemos una p-ésima raíz primitiva de la unidad a F, digamos ζ_p. El campo resultante E es el campo de descomposición de $X^p - a$ sobre F y por lo tanto E/F es una extensión normal. Cualquier automorfismo de E/F manda λ a algún $\zeta_p^i\lambda$, $0 \leq i \leq p-1$, y para todo $i \in \{0, 1, \ldots, p-1\}$ hay un automorfismo f_i que manda λ a $\zeta_p^i\lambda$. Pongamos $\omega_i = f_i(\omega)$. Entonces $\zeta_p^i\lambda = \omega_i^p$. El elemento ω está en $F(\lambda)$ pero no en F, por lo tanto su polinomio irreducible (digamos f) sobre F tiene grado p y tiene p raíces en E distintas. Si ω' es cualesquiera de esas raíces, entonces existe un automorfismo ψ de E/F que manda ω a ω'. Si $\psi(\lambda) = \zeta_p^j\lambda$, tenemos $\psi(\omega) = \omega_j$. Por lo tanto, los elementos $\omega_0, \omega_1, \ldots, \omega_{p-1}$ son todas las raíces de f lo cual implica que $z = \omega_0\omega_1 \cdots \omega_{p-1} \in F$. Ahora multiplicamos juntas las ecuaciónes $\zeta_p^i\lambda = \omega_i^p$, para obtener

$$\mu\lambda^p = \mu a = z^p,$$

donde $\mu = 1 \cdot \zeta_p \cdot \zeta_p^2 \cdots \zeta_p^{p-1}$. Si p es impar, $\mu = 1$, y tenemos una contradicción $a = z^p$, probando (i).

(ii) Supongamos que $\lambda = \omega^2$, con $\omega = \alpha + \beta\lambda$ ($\alpha, \beta \in F$). De $\lambda = (\alpha + \beta\lambda)^2$ obtenemos las ecuaciones $\alpha^2 + \beta^2\alpha = 0$, $2\alpha\beta = 1$. Eliminando β, encontramos $\alpha = -4\alpha^4 \in -4F^4$. De manera recíproca, si $a = -4\alpha^4$, $\alpha \in F$, tomamos $\beta = (1/2)\alpha$ para tener que $\lambda = (\alpha + \beta\lambda)^2$.

□

Ahora estamos listos para considerar el caso de una potencia de un primo (el caso primo será omitido por el Lema 2.4.3)

Lema 2.4.5. *Sean F un campo arbitrario, $n \geq 2$ un entero positivo y p un primo. Denotemos por a un elemento arbitrario en F. Entonces,*

(i) *Si p es impar, ó $p = 2$ y la característica de F es 2, entonces $X^{p^n} - a$ es irreducible sobre F si y sólo si $a \notin F^p$.*

(ii) *Si $p = 2$ y la característica de F es distinta de 2, entonces $X^{2^n} - a$ es irreducible sobre F si y sólo si $a \notin F^2$ y $a \notin -4F^4$.*

Demostración.

(*i*) Si $a = \mu^p$, para algún $\mu \in F$, entonces $X^{p^n} - a = X^{p^n} - \mu^p$ es divisible por $X^{p^{n-1}} - \mu$. De manera recíproca supongamos que $a \notin F^p$. Sea λ una raíz de $X^{p^n} - a$ y sea $\mu = \lambda^{p^{n-1}}$. Entonces μ es una raíz de $X^p - a$; por lo tanto, por el Lema 2.4.3,

$$[F(\mu) : F] = p.$$

Afirmamos que λ tiene grado p^{n-1} sobre $F(\mu)$; si esto ocurre, se seguirá que λ tiene grado p^n sobre F y $X^{p^n} - a$ es irreducible sobre F. El que λ tiene grado p^{n-1} sobre $F(\mu)$ es cierto por inducción sobre n, considerando $\mu \notin F(\mu)^p$. La conclusión deseada es, por tanto, una consecuencia del Lema 2.4.4(*i*).

(*ii*) Si $a \in F^2$, entonces obviamente $X^{2^n} - a$ es reducible. Ahora supongamos que $a \in -4F^4$ y escribamos $a = -4\alpha^4$, $\alpha \in F$ e $Y = X^{2^{n-2}}$. Entonces

$$X^{2^n} - a = Y^4 + 4\alpha^4 = (Y^2 + 2\alpha Y + 2\alpha^2)(Y^2 - 2\alpha Y + 2\alpha^2).$$

De manera recíproca, supongamos que $a \notin F^2$ y $a \notin -4F^4$. Como $a \notin -4F^4$, se sigue que $-4a$ no es una cuarta potencia en F. De nuevo, tomamos λ una raíz de $X^{2^n} - a$ y $\mu = \lambda^{2^{n-1}}$. Puesto que, $a \notin F^2$ y μ es una raíz de $X^2 - a$, tenemos que $[F(\mu) : F] = 2$, por el Lema 2.4.3. Debemos mostrar que $[F(\lambda) : F(\mu)] = 2^{n-1}$. Para $n = 2$ esto es cierto si μ no es un cuadrado en $F(\mu)$, y para $n > 2$ esto es cierto por inducción sobre n, probando que μ no es un cuadrado en $F(\mu)$ y -4μ no es una cuarta potencia en $F(\mu)$. En el último caso, $-\mu$ es un cuadrado en $F(\mu)$. Así que basta mostrar que ni μ ni $-\mu$ son cuadrados en F. Estas dos afirmaciones son equivalentes pues la correspondencia $\mu \longmapsto -\mu$ induce un automorfismo en $F(\mu)$ a F. Por tanto, aplicando el Lema 2.4.4(*ii*), se sigue el resultado.

□

Usando los resultados anteriores, ahora deducimos el siguente resultado.

Teorema 2.4.6. *Sean F un campo arbitrario, $n \geq 1$ y $a \in F$. Entonces $X^n - a$ es irreducible sobre F si y sólo si $a \notin F^p$, para todo primo p divisor de n y $a \notin -4F^4$ siempre que $4|n$.*

Demostración. Si p^s es la máxima potencia de un primo p divisor de n y si $a \in F^p$, entonces $X^{p^s} - a$ es reducible, por los Lemas 2.4.3 y 2.4.5. Por tanto $X^n - a$ es reducible, por el Lema 2.4.2. Si $4|n$ y $a = -4\lambda^4$, $\lambda \in F$, entonces

$$X^n - a = X^n + 4\lambda^4 = (X^{n/2} - 2\lambda X^{n/4} + 2\lambda^2)(X^{n/2} + 2\lambda X^{n/4} + 2\lambda^2).$$

De manera recíproca, asumamos que $a \notin F^p$, para todo primo p divisor de n y $a \notin -4F^4$ siempre que $4|n$. Sea p^s la máxima potencia de un primo p divisor de n. Por el Lema 2.4.2, es suficiente mostrar que $X^{p^s} - a$ es irreducible. La conclusión deseada es, por tanto, una consecuencia de los Lemas 2.4.5 y 2.4.3.

□

Nuestro siguiente objetivo es probar que si E/F es una extensión radical, entonces para cualquier campo intermedio K, $\mathrm{Gal}(K/F)$ es soluble. Tenemos las siguientes observaciones preliminares.

Lema 2.4.7. *Sean E/F una extensión de campos y $E_1/F, \ldots, E_n/F$ subextensiones radicales de E/F. Entonces $(E_1E_2\cdots E_n)/F$ es una extensión radical.*

Demostración. Es suficiente tratar el caso $n = 2$. Sean $E_1 = F(\lambda_1, \ldots, \lambda_m)$ y $E_2 = F(\mu_1, \ldots, \mu_k)$ tales que E_1/F y E_2/F son extensiones radicales. Entonces

$$E_1E_2 = F(\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_k)$$

mostrando que E_1E_2/F es una extensión radical. □

Lema 2.4.8. *Sea $F \subseteq K \subseteq E$ una torre de campos.*

(*i*) *Si E/F es radical, entonces también lo es E/K.*

(*ii*) *Si K/F es radical y E es la cerradura normal de K sobre F, entonces E/F es radical.*

Demostración.

(*i*) Si $E = F(\lambda_1, \ldots, \lambda_m)$, con $\lambda_i^{n_i} \in F(\lambda_1, \ldots, \lambda_{i-1})$, $1 \leq i \leq m$, entonces $E = K(\lambda_1, \ldots, \lambda_m)$, con $\lambda_i^{n_i} \in K(\lambda_1, \ldots, \lambda_{i-1})$, como se quería.

(*ii*) Como K/F es finito, podemos escribir $K = F(a_1, \ldots, a_s)$, donde a_i es una raíz de un polinomio irreducible $f_i(X)$ sobre F, $1 \leq i \leq s$. Si λ_i es cualquier raíz de $f_i(X)$, entonces $F(\lambda_1, \ldots, \lambda_s)$ es F-isomorfo a K y, por tanto, $F(\lambda_1, \ldots, \lambda_s)/F$ es radical. Como K es el compuesto de un número finito de campos de la forma $F(\lambda_1, \ldots, \lambda_s)$, la afirmación se sigue en virtud del Lema 2.4.7.

□

Lema 2.4.9.

(*i*) *Sean p un primo y E el campo de descomposición de $X^p - 1$ sobre F. Entonces* $\mathrm{Gal}(E/F)$ *es cíclico.*

(*ii*) *Si F es un campo en el que $X^n - 1$ se descompone en factores lineales, a un elemento arbitraro de F y E el campo de descomposición de $X^n - a$ sobre F, entonces* $\mathrm{Gal}(E/F)$ *es cíclico.*

Demostración.

(*i*) Si la característica de F es p, entonces $E = F$ y no hay nada que probar. Si la característica de F no es p, entonces $E = F(\zeta)$, donde ζ es una raíz p-ésima primitiva de la unidad, es decir, la extensión $F(\zeta)/F$ es una extensión ciclotómica. Por tanto, $\mathrm{Gal}(E/F)$ es isomorfo a un subgrupo del grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$; así $\mathrm{Gal}(E/F)$ es cíclico.

(*ii*) Si u es una raíz de $X^n - a$, entonces la raíz general tiene la forma εu donde $\varepsilon^n = 1$ y también ε está en F. Se sigue que $E = F(u)$, y que un automorfismo de E/F es determinado por su valor en u. Ahora, todos los elementos ε, con $\varepsilon^n = 1$ forman un grupo cíclico, digamos generado por ζ_n. Si $\sigma \in \mathrm{Gal}(E/F)$, entonces $\sigma(u) = \zeta_n^{i_\sigma} u$, para algún $i_\sigma \geq 1$. El mapeo $\mathrm{Gal}(E/F) \longrightarrow \langle \zeta_n \rangle$ dado por $\sigma \longmapsto \zeta_n^{i_\sigma}$ es obviamente un homomorfismo inyectivo, y así tenemos el resultado.

□

Ahora estamos listos para probar:

Teorema 2.4.10. *Si E/F es una extensión radical, entonces para cualquier campo intermedio K,* $\mathrm{Gal}(K/F)$ *es soluble.*

Demostración. Sean K un campo intermedio y K_0 el subcampo fijo de $\mathrm{Gal}(K/F)$. Entonces K/K_0 es de Galois y $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/K_0)$. Como, por el Lema 2.4.8(i), E/K_0 es radical, podemos suponer $K = K_0$, es decir, K/F es de Galois. Si L denota la cerradura normal de E sobre F, entonces por el Lema 2.4.8(ii), L/F es radical. De esta manera, podemos suponer también que E/F es normal. Por tanto $\mathrm{Gal}(K/F)$ es una imagen homomorfa de $\mathrm{Gal}(E/F)$ (Lema 2.1.5), y sólo falta verificar que $\mathrm{Gal}(E/F)$ es soluble.

Sea $E = F(\lambda_1, \ldots, \lambda_n)$ tal que E/F es una extensión radical. Insertando de ser necesario más $\lambda' s$, podemos hacer que en cada caso una potencia de λ_i esté en

$F(\lambda_1, \ldots, \lambda_{i-1})$. Procedamos por inducción sobre n. Por hipótesis, $\lambda_1^p \in F$ para algún p primo. Sea E_0 el campo de descomposición de $X^p - 1$ sobre E y sea E_1 un subcampo de E_0 generado por F y las raíces de $X^p - 1$. Como obviamente E_0/F es normal, $\mathrm{Gal}(E/F)$ es una imagen homomorfa de $\mathrm{Gal}(E_0/F)$, así sólo necesitamos probar que $\mathrm{Gal}(E_0/F)$ es soluble.

La extensión E_1/F es obviamente de Galois y por tanto cíclica, por el Lema 2.4.9(i). Como

$$\mathrm{Gal}(E_0/F)/\mathrm{Gal}(E_0/E_1) \cong \mathrm{Gal}(E_1/F),$$

es suficiente probar que $\mathrm{Gal}(E_0/E_1)$ es soluble. Ahora $E_0 = E_1(\lambda_1, \ldots, \lambda_n)$, pues E_0 es generado sobre F por los $\lambda' s$ y las raíces de $X^p - 1$, y esas últimas están en E_1. Sea $G = \mathrm{Gal}(E_0/E_1)$ y sea $H = \mathrm{Gal}(E_0/E_1(\lambda_1))$. Puesto que $X^p - 1$ se factoriza completamente en E_1, $E_1(\lambda_1)$ es un campo de descomposición de $X^p - \lambda_1^p$ sobre E_1 y por tanto $E_1(\lambda)/E_1$ es normal. Más aún, por el Lema 2.4.9(ii), $\mathrm{Gal}(E_1(\lambda_1)/E_1)$ es cíclico. Pero E/F es normal y radical, por tanto E_0/E_1 debe ser normal. Se sigue, por el Lema 2.1.5, que $H \lhd G$ y G/H es cíclico. Para probar que G es soluble, queda por probar que H es soluble. Esto se sigue de la hipótesis inductiva, pues $E_0/E_1(\lambda_1)$ es una extensión radical generada por $n-1$ elementos, los $\lambda_2, \ldots, \lambda_n$. Así que el teorema es cierto.

□

Sea F un campo y sea $f(X) \in F[X]$. Definimos el **grupo de Galois** de $f(X)$ como el grupo de Galois de un campo de descomposición de $f(X)$ sobre F.

Corolario 2.4.11. *Sean F un campo arbitrario y $f(X)$ un polinomio irreducible sobre F. Si existe una extensión radical E/F que contenga una raíz de $f(X)$, entonces el grupo de Galois de $f(X)$ sobre F es soluble.*

Demostración. Sea E_0 la cerradura normal de E sobre F. Por el Lema 2.4.7, E_0/F es radical y por tanto podemos suponer que E/F es normal. Por lo tanto E contiene un campo de descomposición K de $f(X)$ sobre F y, por el Teorema 2.4.10, $\mathrm{Gal}(K/F)$ es soluble.

□

Nuestro siguiente resultado nos da un recíproco parcial del Teorema 2.4.10.

Teorema 2.4.12. *Sean F un campo de característica 0 y E/F una extensión normal finita, con grupo de Galois G soluble. Entonces E puede ser encajado en una extensión radical de F.*

Demostración. Procederemos por inducción sobre $[E : F]$. Como G es soluble, este contiene un subgrupo normal H de índice p primo. Sea K un campo de descomposición de $X^p - 1$ sobre E. Entonces K/F es normal y, como $\mathrm{Gal}(K/E)$ es cíclico (Lema 2.4.9(i)), el grupo $\mathrm{Gal}(K/F)$ es soluble. Sea L el subcampo de K obtenido al adjuntar las raíces de $X^p - 1$ a F. Entonces K/L también es normal. Como L/F es una extensión radical, verificaremos que K puede ser encajado en una extensión radical de L.

Para esto, primero mostramos que $\mathrm{Gal}(K/L)$ es isomorfo a un subgrupo de G. En efecto, consideremos el mapeo

$$\begin{array}{ccc} \mathrm{Gal}(K/L) & \longrightarrow & \mathrm{Gal}(E/F) \\ \sigma & \longmapsto & \sigma|_E \end{array}$$

Entonces, este mapeo es un homomorfismo, el cual es inyectivo, pues $\sigma|_E = \text{identidad}$ implica que σ deja fijos a los elementos de L y de E y por lo tanto $\sigma = 1$.

Si $\mathrm{Gal}(K/L)$ es isomorfo a un subgrupo propio de G entonces, por nuestra hipótesis de inducción, K puede ser encajado en una extensión radical de L. De aquí que, podemos suponer que $\mathrm{Gal}(K/L) \cong G$. Sea T un campo intermedio correpondiente a H. Entonces $[T : L] = p$, T es normal sobre L, y L contiene una raíz p-ésima primitiva de 1. Puesto que T/L es cíclica de grado p, se sigue del Lema 2.4.1 que T/L es una extensión radical. Ahora K/T es normal con grupo de Galois soluble H. Por inducción, K puede ser encajado en una extensión radical de T. Por tanto K puede ser encajado en una extensión radical de L, como se requería.

□

Sean F un campo y $f(X)$ un polinomio de grado positivo sobre F. Entonces la ecuación

$$f(X) = 0$$

se dice que es **soluble por radicales sobre** F si cada raíz de $f(X)$ está en una extensión radical de F. Por el Lema 2.4.7, esto es equivalente a la condición de que un campo de descomposición de $f(X)$ sobre F pueda ser encajado en una extensión radical de F.

Corolario 2.4.13. (Criterio de Galois). Una ecuación $f(X) = 0$ es soluble por radicales sobre un campo F de característica 0 si y sólo si el grupo de Galois de $f(X)$ es soluble.

Demostración. Basta aplicar los Teoremas 2.4.12 y 2.4.10.

□

Nuestro siguiente objetivo es dar algunas aplicaciones del Teorema 2.4.6, los cuales aseguran la existencia de extensiones de grado grande.

Lema 2.4.14. *Sean F un campo de característica $p > 0$, $a \in F$ y $X^p - X - a$ irreducible sobre F. Si λ es una raíz de $X^p - X - a$, entonces $X^p - X - a\lambda^{p-1}$ es irreducible sobre $F(\lambda)$.*

Demostración. Procedamos por contradicción, supongamos que $X^p - X - a\lambda^{p-1}$ es reducible. Entonces, por el Teorema de Artin-Schreir (Teorema 2.2.3(*iii*)), tiene una raíz μ en $F(\lambda)$. Escribimos

$$\mu = a_0 + a_1\lambda + \cdots + a_{p-1}\lambda^{p-1}$$

con $a_i \in F$. Entonces, como $\lambda^p = \lambda + a$, tenemos

$$\begin{aligned} \mu^p &= a_0^p + a_1^p\lambda^p + \cdots + a_{p-1}^p\lambda^{p(p-1)} \\ &= a_0^p + a_1^p(\lambda + a) + \cdots + a_{p-1}^p(\lambda + a)^{p-1}. \end{aligned} \tag{2.4.3}$$

Por otro lado,

$$\mu^p = \mu + a\lambda^{p-1} = a_0 + a_1\lambda + \cdots + (a_{p-1} + a)\lambda^{p-1}. \tag{2.4.4}$$

Igualando los coeficientes de λ^{p-1} en (2.4.3) y (2.4.4), obtenemos $a_{p-1}^p = a_{p-1} + a$, lo que contradice la irreducibilidad de $X^p - X - a$ sobre F. □

Ahora estamos listos para probar el siguiente resultado.

Teorema 2.4.15. *Sean F un campo y p o bien un primo impar ó $p = 2$ y $\mathrm{car}(F) = 2$. Si F tiene una extensión con grado divisible por p, entonces para cada $n \geq 1$, F tiene una extensión de grado divisible por p^n.*

Demostración. Si la característica de F es p y F no es perfecto, entonces $\lambda \notin F^p$ para algún $\lambda \in F$, por tanto, por el Teorema 2.4.6, $X^{p^n} - \lambda$ es irreducible para todo $n \geq 1$. De aquí que, si la característica de F es p, podemos suponer que F es perfecto.

Sea E/F una extensión de campos con $p|[E:F]$ y sea K la cerradura separable de F en E. Si la característica de F es p, entonces $K = E$, pues estamos suponiendo que F es perfecto. Si la característica de F es q y $q = 0$, entonces $K = E$, pues cualquier extensión algebraica de un campo de característica cero es separable. Finalmente, si la característica de F es $q > 0$ y $q \neq p$ entonces, por las Proposiciones 2.1.2 y 2.1.3(i), $[E : K]$ es una potencia de q, así que p divide a $[K : F]$. Así podemos suponer que E/F es separable. Tomando la cerradura normal de E, podemos más aún asumir que E/F es Galois. Aplicando la Teoría de Galois Finita y la existencia de un elemento de orden p en $\mathrm{Gal}(E/F)$, suponemos que E/F es una extensión de Galois de grado p.

Si la característica de F es p entonces, por el Teorema 2.2.3, $E = F(\lambda)$, con λ una raíz de un polinomio irreducible sobre F de la forma $X^p - X - a$. Por lo tanto, por el Lema 2.4.14, existe una extensión de F de grado p^2 y el proceso puede ser repetido para obtener la extensión de grado p^n para cualquier n.

Supongamos ahora que la característica de F es distinta de p y sea K un campo de descomposición de $X^p - 1$ sobre E. Si T es obtenido de F adjuntándole una raíz p-ésima primitiva de la unidad, entonces K/T es de Galois donde el grupo de Galois es cíclico de orden p. Por el Lema 2.4.1, $K = T(\lambda)$ con λ una raíz de un polinomio irreducible $X^p - a$, para algún $a \in F$. Por tanto $a \notin F^p$ y, por el Teorema 2.4.6, $X^{p^n} - a$ es irreducible sobre F, para cualquier $n \geq 1$. Esto completa la prueba del teorema.

□

Teorema 2.4.16. *Sea F un campo teniendo una extensión de grado divisible por 4. Entonces, para cualquier $n \geq 2$, F tiene una extensión de grado divisible por 2^n.*

Demostración. Si la característica de F es 2, entonces la afirmación es cierta al aplicar el Teorema 2.4.15. Así que, supongamos que la característica de F es distinta de 2. Por el argumento en el Teorema 2.4.15, podemos suponer que la extensión dada E de F es tal que E/F es de Galois, con $[E : F] = 4$. Consideremos el campo $E(i)$, con $i^2 = -1$. Entonces $E(i)/F(i)$ es Galois de grado 2 o 4. En cualquier caso, $E(i)$ contiene una extensión cuadrática de $F(i)$ y, por lo tanto, $F(i)$ contiene un elemento a sin raíces cuadráticas en $F(i)$. Más aún, $-4a$ no puede tener una raíz cuarta en $F(i)$, pues si la tuviera $-a$ es un cuadrado y también a. Aplicando el Lema 2.4.5(ii), concluimos que $F(i)$ tiene una extensión de grado 2^n para toda $n \geq 2$.

□

Para los siguientes resultados, necesitamos introducir la noción de un campo ordenado. Sea R un anillo conmutativo con identidad. Decimos que R es un **anillo ordenado** si existe un orden total $>$ de R tal que

(*a*) $x > x',\ y > y' \Rightarrow x + y > x' + y'$;

(*b*) $x > 0,\ y > 0 \Rightarrow xy > 0$.

Cuando hablemos del orden de R, escribiremos $x \geq y$ para establecer que $x > y$ o $x = y$, y usaremos $<, \leq$ para el orden opuesto. Un elemento $x \in R$ se dice que es **positivo** ó **negativo** si $x > 0$ ó $x < 0$, respectivamente.

En cualquier anillo R, un **cono** es un subconjunto P conteniendo al 1 pero no al 0 y es cerrado bajo la adición y la multiplicación.

Lema 2.4.17. *Sea R un anillo conmutativo con identidad ordenado.*

(*i*) *El conjunto P de elementos positivos de R es un cono, y $R = P \cup -P \cup \{0\}$ (unión disjunta), donde $-P = \{-x \mid x \in P\}$.*

(*ii*) *Cada cono P de un anillo conmutativo con identidad S tal que $S = P \cup -P \cup \{0\}$ define un orden en S tomando $x > y$ si y sólo si $x - y \in P$.*

(*iii*) *R es un dominio entero de característica 0, y el cuadrado de cualquier elemento no cero de R es positivo.*

Demostración. La demostración de (*i*) y (*ii*) es directa. Veamos (*iii*): Dados $x, y \in R$, $x, y \neq 0$, si $x, y > 0$, entonces $xy > 0$. Similarmente, si $x, y < 0$, entonces $-x, -y > 0$ y así $xy = (-x)(-y) > 0$. Si x y y tienen signos opuestos, digamos que $x > 0 > y$, entonces $xy < 0$. En cada caso $xy \neq 0$, luego R es un dominio entero. En particular, si $x = y$, entonces los últimos dos casos no pueden ocurrir y $x^2 > 0$. Por último, notemos que $1^2 = 1 > 0$ y que $1, 1 + 1, \ldots$ todos son > 0, por tanto la característica de R es 0.

□

El conjunto P del Lema 2.4.17 es llamado **cono positivo** de R.

Teorema 2.4.18. *Sea F un campo que tiene una extensión cuadrática pero no una extensión de grado 4. Entonces F es un campo ordenado en el cual cada elemento positivo tiene una raíz cuadrada.*

Demostración. Sea P el subconjunto de F de todos los cuadrados no cero. Entonces P es obviamente cerrado bajo multiplicación. Así, de acuerdo con el Lema 2.4.17(*ii*), nos falta verificar que P es cerrado bajo la adición y que para cualquier $0 \neq a \in F$, o bien a ó $-a$ es un cuadrado, pero no ambos.

Debido al Teorema 2.4.15, tenemos que la característica de F no es 2. Por lo tanto, de acuerdo con el Lema 2.4.5(iii), para cada $a \in F$ o bien a es un cuadrado ó $-4a$ es una cuarta potencia; de otra manera $X^4 - a$ sería irreducible sobre F y nos daría una extensión de grado 4. En particular, o bien a ó $-a$ es un cuadrado. Si -1 es un cuadrado, entonces cualquier elemento en F sería un cuadrado, y no existirían extensiones cuadráticas de F. Así, para cualquier $0 \neq a \in F$, o bien a ó $-a$ es un cuadrado, pero no ambos.

Por lo antes mencionado, nos falta verificar que la suma de dos cuadrados es un cuadrado. Para este fin, construyamos el campo $F(i)$, con $i^2 = -1$. En $F(i)$ todo elemento debe ser un cuadrado, pues de otra manera sería una extensión cuadrática de $F(i)$ y por lo tanto una extensión de F de grado 4. Aplicando el hecho de que $a + bi$ es un cuadrado en $F(i)$, tenemos que $a^2 + b^2$ es un cuadrado en F, como se quería. □

Corolario 2.4.19. (Artin-Schreir). *Sea E/F una extensión finita de campos, con E algebraicamente cerrado pero F no algebraicamente cerrado. Entonces F es un campo ordenado y $E = F(i)$, con $i^2 = -1$.*

Demostración. Por hipótesis, E es la cerradura algebraica de F. Por lo que el grado de cualquier extensión finita de F está acotada por $[E : F]$. Se sigue, de los Teoremas 2.4.15 y 2.4.16, que $[E : F] = 2$. Luego, por el Teorema 2.4.18, F es un campo ordenado en el cual todo elemento positivo tiene una raíz cuadrada, y E debe ser $F(i)$.

□

Como un resultado preliminar para el teorema que sigue, probamos el siguiente:

Lema 2.4.20. *Sea F un campo tal que para algún primo p cualquier extensión finita no trivial de F tiene grado divisible por p. Entonces cualquier extensión finita de F tiene grado una potencia de p.*

Demostración. Sea E/F una extensión finita de campos. Si la característica de F es q, con $q > 0$ y $q \neq p$, entonces F es perfecto. En efecto, pues si no, de acuerdo al Lema 2.4.3, F tiene una extensión de grado q. Si la característica de F es p y K es la cerradura separable de F en E, entonces $[E : K]$ es una potencia de p (Proposiciones 2.1.2 y 2.1.3). Así podemos suponer que E/F es separable. Más aún, considerando la cerradura normal de E sobre F, podemos asumir que E/F es de Galois. Sea P un p-subgrupo de Sylow de $\mathrm{Gal}(E/F)$, y sea K el subcampo correspondiente. Entonces $[K : F] = [G : P]$ es primo relativo con p. Por nuestra hipótesis, esto implica $K = F$. Así $[E : F]$ es una potencia de p, como se quería.

□

Teorema 2.4.21. *Sea F un campo ordenado donde todo elemento positivo tiene una raíz cuadrada. Supóngase también que cualquier polinomio de grado impar sobre F tiene una raíz en F. Entonces $F(i)$, con $i^2 = -1$, es algebraicamente cerrado.*

Demostración. Por hipótesis, F no tiene extensiones finitas no triviales de grado impar. Por el Lema 2.4.20, tenemos que el grado de cualquier extensión finita de F es potencia de 2. Afirmamos que la única extensión finita no trivial de F es $F(i)$, que claramente nos dará el resultado. Sean E/F una extensión finita y $G = \mathrm{Gal}(E/F)$. Por el Lema 2.4.17, la característica de F es 0 y así E/F es separable. Pasando a la cerradura normal de E, podemos suponer que E/F es de Galois. Sabemos que el orden de G es una potencia de 2. Si $[E : F] > 2$, entonces G tiene un subgrupo de índice 4 el cual, a su vez, está contenido en un subgrupo de índice 2. Esto nos da una torre de campos $F \subset F_1 \subset F_2$, con $[F_1 : F] = [F_2 : F_1] = 2$. Puesto que $F(i)$ es la única extensión cuadrática de F, tenemos que $F_1 = F(i)$, lo que implica que todo elemento en F_1 es un cuadrado, luego F_2 no puede existir, lo que es una contradicción.

□

Sea E/F una extensión de campos y sea M un subgrupo de E^* tal que F^*M/F^* es finito. ¿Cuándo se da el caso que $|F^*M/F^*| = [F(M) : F]$? La respuesta a esta pregunta se tiene en el siguiente resultado:

Teorema 2.4.22. (Kneser). *Sea E/F una extensión de campos separable y sea M un subgrupo de E^* tal que F^*M/F^* es finito. Supongamos que para todo p primo impar, cada raíz p-ésima de 1 que está en F^*M también está en F y que $i = \sqrt{-1} \in F$ si $1 \pm i \in F^*$. Entonces*

$$|F^*M/F^*| = [F(M) : F].$$

Demostración. Primero observemos que $F(M)$ consiste de todas las combinaciones lineales de F^*M sobre F. Por lo tanto, podemos tomar una cantidad finita de elementos $x_1, \ldots, x_n$ en F^*M los cuales sean una F-base de $F(M)$. Entonces $x_1F^*, \ldots, x_nF^*$ son elementos distintos de F^*M/F^* y así

$$[F(M) : F] \leq |F^*M/F^*|. \tag{2.4.5}$$

Supongamos que el resultado es cierto para todo los subgrupos de Sylow de F^*M/F^*. Si N/F^* es un p-subgrupo Sylow de F^*M/F^* de orden p^t, entonces

$$p^t = [F(N) : F] \big| [F(M) : F]$$

y así $|F^*M/F^*| \leq [F(M) : F]$. Por (2.4.5), podemos suponer que F^*M/F^* es un p-grupo.

Tomemos una cadena de subgrupos

$$F^* = N_0 \subset N_1 \subset \cdots \subset N_t = F^*M,$$

con $[N_s : N_{s-1}] = p$, $1 \leq s \leq t$. Mostramos, por inducción sobre s, que

$$[F(N_s) : F(N_{s-1})] = p \tag{2.4.6}$$

y que un elemento de $F(N_s)$ (respectivamente, $F(N_s) \cap F^*M$ si $p = 2$ e $i \in F(N_s)$), cuya p-ésima potencia está en N_s, está en N_s. Supongamos que la declaración se cumple para $s-1$. Si $a \in N_s$ es tal que aN_{s-i} genera a N_s/N_{s-1}, entonces a es una raíz del polinomio $f(X) = X^p - a^p$ con coeficientes en $F(N_{s-1})$. Por lo tanto, si f es irreducible, entonces se tiene (2.4.6). Si f es reducible, entonces f tiene una raíz, digamos b, en $F(N_{s-1})$, por el Lema 2.4.3. Por tanto, $b = a\varepsilon$ con $\varepsilon^p = 1$ y $b^p = a^p \in N_{s-1}$. Por la hipótesis inductiva, $b \in F(N_{s-1})$, por lo que $\varepsilon \in N_s \subset F^*M$, lo que implica, por hipótesis, que $\varepsilon \in F$. Se sigue que $a \in N_{s-1}$, contradiciendo la suposición de que aN_{s-1} es de orden $p > 1$. Esto establece (2.4.6).

Ahora supongamos que $c \in F(N_s)$ satisface $c^p \in N_s$ (y $c \in F^*M$, cuando $p = 2$ e $i \in F(N_s)$). Entonces $c^p = a^q d$, con $0 \leq q \leq p$ y $d \in N_{s-1}$. Deseamos probar que $c \in N_s$. Esto se logrará probando el caso $q = 0$ y mostrando que el caso $q > 0$ no puede ocurrir.

Supongamos que $q = 0$, así que $c^p \in N_{s-1}$. Como E/F es separable, también $F(N_s)/F(N_{s-1})$ lo es. Por (2.4.6), existe un $F(N_{s-1})$-homomorfismo h de $F(N_s)$ en la cerradura normal de $F(N_s)/F(N_{s-1})$ tal que $h(a) \neq a$. Puesto que $h(a^p) = a^p = h(a)^p$, tenemos $h(a) = a\zeta_p$ con ζ_p una raíz p-ésima primitiva de 1. Similarmente, $h(c^p) = c^p = h(c)^p$ y también $h(c) = c\epsilon^r$, para algún $0 \leq r \leq p-1$.

Esto implica que $h(a^{-r}c) = a^{-r}c$ y por tanto $a^{-r}c = b \in F(N_{s-1})$. Más aún, $b^p = (a^p)^{-r}c^p \in N_{s-1}$ (y $b \in F^*M$ si $c \in F^*M$) lo que prueba, por inducción, que $b \in N_{s-1}$ y de aquí que $c \in N_s$.

Ahora supongamos que $q > 0$ y denotemos por N la norma de $F(N_s)$ sobre $F(N_{s-1})$. Ya que $N(a) = (-1)^{p-1}a^p$, tenemos que

$$((-1)^{p-1}a^p)^q = N(c)^p d^{-p}.$$

Para p impar, a^p es entonces una p-ésima potencia de un elemento en $F(N_{s-1})$, lo cual contradice (2.4.6). En el caso de que $p = 2$, tenemos que $-a^2 = \lambda^2$ con $\lambda \in F(N_{s-1})$ que nos dice que $i \in F(N_s)$, $i \notin F(N_{s-1})$ y $c^2 = ad = \pm i\lambda d$. Escribimos

$$c = g + it, \text{ con } g, t \in F(N_{s-1}).$$

Entonces, $c^2 = (g^2 - t^2) + 2gti = \pm i\lambda d$ lo cual implica que $g^2 = t^2$ y por lo tanto $c = (1 \pm i)g$. Concluimos que

$$g^4 = -c^4/4 \in N_{s-1},$$

lo que nos asegura, aplicando dos veces la hipótesis inductiva, que $g \in N_{s-1}$. Pero entonces $1 \pm i \in F^*M$ y también, por hipótesis, $i \in F \subseteq F(N_{s-1})$. Esta contradicción completa la demostración del teorema.

□

Regresando a las extensiones radicales, investigaremos las condiciones bajo las cuales el grupo de Galois de un binomio de la forma $X^n - a$ es abeliano.

Teorema 2.4.23. (Schinzel). *Sean F un campo, n un entero positivo no divisible por la característica de F y m el número de raíces n-ésimas de la unidad contenidas en F. Entonces, dado $a \in F$, el grupo de Galois de $X^n - a$ es abeliano si y sólo si $a^m = \lambda^n$, para algún $\lambda \in F$.*

Demostración. Para cualquier entero t no divisible por la característica de F, sea ζ_t una raíz t-ésima primitiva de la unidad sobre F. Sea F^{ab} la extensión abeliana maximal de F. Si $a^m = \lambda^n$, para algún $\lambda \in F$, entonces $\sqrt[n]{a} = \zeta_n^j \sqrt[m]{\lambda}$, $0 \leq j \leq n-1$. Como F contiene una raíz m-ésima primitiva de la unidad, $\sqrt[m]{\lambda} \in F^{ab}$ en virtud del Lema 2.3.2(*iii*). Así $\sqrt[n]{a} \in F^{ab}$ y $F(\sqrt[n]{a}, \zeta_n)/F$ es abeliano.

De manera recíproca, supongamos que el grupo de Galois de $X^n - a$ es abeliano. Sea k el máximo divisor de n tal que $a^m = \lambda^k$, para algún $\lambda \in F$. Sólo necesitamos verificar que $k = n$. Obviamente $k \leq n$ y $m|k$. Procedamos por contradicción, supongamos que $k < n$. Fijemos un primo p que divide a n/k y denotemos por p^s la máxima potencia de p que divide a m. Ponemos

$$t = p^{s+1}k/m, \quad L = F(\zeta_{p^{s+1}}) \text{ y } E = F(\sqrt[p^{s+1}]{\lambda}).$$

Entonces

$$E \subseteq F(\sqrt[t]{a}, \zeta_{tm}) \subseteq F^{ab},$$

pues, por hipótesis, $\sqrt[n]{a} \in F^{ab}$. Por definición de k, $[E : F] = p^{s+1}$. Así $\zeta_{p^{s+1}} \in E$ y $F \subseteq L \subseteq E$. Además, como $p^{s+1}|n$ y p^s es la máxima potencia de p que divide a m, tenemos $\zeta_{p^s} \in F$, pero $\zeta_{p^{s+1}} \notin F$. Ahora, discutiremos dos casos. Supongamos primero que $s = 0$. Entonces $[L : F]$ divide a $p - 1$. Luego, $L = F$ y $\zeta_p \in F$, contradicción. Ahora, supongamos que $s \geq 1$. Tenemos $[E : L] < p^{s+1}$ y $E = L(\sqrt[p^{s+1}]{\lambda})$. Luego $\lambda = \lambda_1^p$, para algún $\lambda_1 \in L$, en virtud del Lema 2.4.3. Así $F(\sqrt[p]{\lambda}) \subseteq L = F(\sqrt[p]{\zeta_{p^s}})$ y, por el Corolario 2.3.6, tenemos $\lambda = \zeta_{p^s}^j \lambda_2^p$, para algún $j \geq 0$ y algún $\lambda_2 \in F$. Pero entonces $a^m = \lambda_2^{p^k}$, con $p^k|n$, contradiciendo la definición de k.

□

Ahora damos una fórmula para obtener el grado del campo de descomposición de un binomio irreducible. En lo que sigue, para cualquier $n \geq 1$ no divisible por la característica de un campo F, escribimos ζ_n para una n-ésima raíz primitiva de la unidad sobre F.

Como paso preliminar, primero probaremos el siguiente lema:

Lema 2.4.24. *Sean F un campo, $n \geq 1$ un entero no divisible por la característica de F y $X^n - a \in F[X]$ irreducible sobre F con raíz λ. Sea*

$$r = \max\{k \mid k|n \text{ y } \zeta_k \in F(\lambda)\}.$$

Si E es cualquier campo tal que $F(\zeta_r) \subseteq E \subseteq F(\lambda)$, entonces

$$E = F(\lambda^s), \text{ donde } s = [F(\lambda) : E].$$

Demostración. Sea $f(X)$ el polinomio irreducible de λ sobre E. Como λ es una raíz de $X^n - a$, tenemos que $f(X)|(X^n - a)$. Luego, toda raíz de $f(X)$ es de la forma $\zeta_n^i \lambda$, para algún i, y por lo tanto

$$f(X) = \prod_{j=1}^{s} (X - \zeta_n^{i_j} \lambda).$$

Si $d = \sum_{j=1}^{s} i_j$, entonces

$$\prod_{j=1}^{s} \zeta_n^{i_j} \lambda = \zeta_n^d \lambda^s \in E \subseteq F(\lambda).$$

También $\lambda^s \in F(\lambda)$ y por lo tanto $\zeta_n^d \in F(\lambda)$. Entonces, por la definición de r, $\zeta_n^d \in F(\zeta_r) \subseteq E$ y así $\lambda^s \in E$. Ahora, $s = [F(\lambda) : E]$ y $[F(\lambda) : F(\lambda^s)] \leq s$, ya que λ es una raíz de $X^s - \lambda^s$ sobre $F(\lambda^s)$. Por lo tanto, tenemos que $E = F(\lambda^s)$.

□

Ahora estamos listos para probar:

Teorema 2.4.25. (Darbi-Gay-Velez) *Sean F un campo de característica $p \geq 0$, n un entero positivo y m definido por: $m = n$ si la característica de F es 0 y $n = mp^k$ con $(m, p) = 1$ si la característica de F es $p > 0$. Supongamos que $X^n - a \in F[X]$ es irreducible sobre F y λ una raíz, definimos el entero s como*

$$s = \max\{t \mid t|m \text{ y } \lambda^{m/t} \in F(\zeta_m)\}.$$

Si E es el campo de descomposición de $X^n - a$ sobre F, entonces

$$[E : F] = \frac{n[F(\zeta_m) : F]}{s}.$$

Demostración. Primero reducimos el caso general al caso $m = n$, es decir, $car(F) \nmid n$. Así que, supongamos que la característica de F es $p > 0$. Entonces

$$E = F(\lambda, \zeta_m) = F(\lambda^{p^k}, \lambda^m, \zeta_m),$$

el cual es a su vez el compuesto de la extensión separable $F(\lambda^{p^k}, \zeta_m)/F$ y una extensión puramente inseparable $F(\lambda^m)/F$. Por el Lema 2.4.2, tanto $X^m - a$ como $X^{p^k} - a$ son irreducibles sobre F. Como λ^m es una raíz de $X^{p^k} - a$, tenemos que $[F(\lambda^m) : F] = p^k$. Por tanto,

$$[E : F] = p^k[F(\lambda^{p^k}, \zeta_m) : F].$$

Así, si el resultado se cumple para $X^m - a$ (cuyo campo de descomposición es $F(\lambda^{p^k}, \zeta_m)$), entonces

$$[E : F] = \frac{p^k m[F(\zeta_m) : F]}{s} = \frac{n[F(\zeta_m) : F]}{s}.$$

De aquí que, podemos suponer que $m = n$ y que la característica de F no divide a n.

Pongamos $L = F(\zeta_n) \cap F(\lambda)$ y $s' = [L : F]$. Ya que $X^n - a$ es irreducible,

$$[F(\lambda) : F] = n.$$

Por otra lado, de la Proposición 2.1.6

$$[E : F(\lambda)] = [F(\zeta_n, \lambda) : F(\lambda)] = [F(\zeta_n) : L].$$

Se sigue que

$$[E : F] = \frac{n[F(\zeta_n) : F]}{s'}$$

y debemos mostrar que $s = s'$.

Por la definición de r en el Lema 2.4.24,

$$F(\zeta_r) \subseteq F(\zeta_n) \cap F(\lambda) = L \subseteq F(\lambda)$$

y por tanto, por el Lema 2.4.24, $L = F(\lambda^q)$, para $q = [F(\lambda) : L]$. Como $[F(\lambda) : F] = n$, tenemos que

$$[L : F] = \frac{n}{q} = s'.$$

Esto prueba que $\lambda^q \in F(\zeta_n)$ y $q = n/s'$. Por tanto, de la definición de s, $s \geq s'$. Por otro lado, como $\lambda^{n/s} \in F(\zeta_n) \cap F(\lambda) = L$, tenemos que

$$[F(\lambda) : L] = q \leq \frac{n}{s},$$

de donde $s' \geq s$, como se requería.

□

Sea E/F una extensión radical simple, digamos $E = F(\lambda)$, con $\lambda \in E^*$ y una potencia de λ en F^*. Entonces obviamente tenemos

$$(\langle\lambda\rangle \mathrm{tor}(E^*)F^*)/F^* \subseteq \mathrm{tor}(E^*/F^*).$$

Por lo tanto, es natural investigar las circunstancias bajo las cuales la igualdad se cumple.

Teorema 2.4.26. (May). *Sean p un primo y E/F una extensión de campos, con la característica de F distinta de p. Supóngase que $E = F(\lambda)$, donde $\lambda^p \in F - F^p$. Si $p = 2$, supongamos además que $E \neq F(i)$ $(i^2 = -1)$. Entonces*

$$\mathrm{tor}(E^*/F^*) = (\langle\lambda\rangle \mathrm{tor}(E^*)F^*)/F^*.$$

Demostración. Debido al Lema 2.4.3, $X^p - \lambda^p$ es irreducible sobre F y por tanto $[E : F] = p$. Sea $\mu \in E^*$ un elemento de orden una potencia de un primo módulo F^*. Primero supongamos que el orden es q^r, para algún primo $q \neq p$, y sea $\mu^{q^r} = \gamma \in F^*$. Si N es la norma de E en F, entonces $N(\mu)^{q^r} = \gamma^p$, por tanto $\gamma = \gamma_1^{q^r}$, para algún $\gamma_1 \in F^*$. Se sigue que $\mu = \gamma_1\varepsilon$, para alguna raíz de la unidad $\varepsilon \in F^*$, lo que demuestra que $\mu F^* \in \mathrm{tor}(E^*)F^*$.

Ahora supongamos que μ tiene orden p^r módulo F^*, y sea $\mu^{p^r} = \gamma \in F^*$. Afirmamos que $\gamma \notin F^p$. Supongamos que sí y escribamos $\gamma = \gamma_1^p$, para algún $\gamma_1 \in F^*$. Sea ζ_p un raíz p-ésima primitiva de la unidad. Entonces

$$\mu^{p^{r-1}} = \gamma_1\zeta_p^m, \text{ para algún } m \in \mathbb{Z}.$$

Debemos tener $p \nmid m$, porque si no el orden de μ módulo F^* sería menos que p^r. Por la misma razón, debemos tener que $\zeta_p \notin F^*$. Se sigue que

$$E \supseteq F(\zeta_p) \supseteq F,$$

con $[F(\zeta_p) : F] > 1$. Pero $[E : F] = p$ y $[F(\zeta_p) : F]$ divide a $p-1$. Esta contradicción prueba nuestra afirmación.

Salvo cuando $p = 2$, $r > 1$ e $i \notin F$, tenemos que $[F(\mu) : F] = p^r$ en virtud de los Lemas 2.4.5 y 2.4.3, y así $r = 1$. Consideremos el caso excepcional, es decir, supongamos que $p = 2$, $r > 1$, $i \notin F$ y $[F(\mu) : F] < 2^r$. Bajo estas circunstancias sabemos, por el Lema 2.4.5, que $\gamma = -4\delta^4$, para algún $\delta \in F$. De la relación

$$\mu^{2^r} = -4\delta^4,$$

vemos que $i \in E$ y por tanto $E = F(i)$. Como este caso es excluido en la hipótesis, retornaremos a la situación donde

$$\mu^p = \gamma \quad \text{y} \quad [F(\mu) : F] = p.$$

Entonces tenemos

$$F(\mu) = E = F(\lambda).$$

Por tanto, por el Corolario 2.3.7, $\mu = \lambda^k a$, para algún $k \in \mathbb{Z}$ y algún $a \in F$. Así, $\mu F^* \in \langle\lambda\rangle F^*$ y el resultado se tiene.

□

Volvemos al estudio del campo $F(\alpha)$, donde α es raíz de un polinomio irreducible $X^p - a \in F[X]$. Como una aplicación sencilla del Corolario 2.3.7, primero mostraremos que adjuntando dos p-ésima raíces "genuinamente distintas" obtenemos una extensión de grado p^2.

Teorema 2.4.27. *Sean p un primo y F un campo con característica distinta de p. Si α y β son raíces de los polinomios irreducibles $X^p - a$ y $X^p - b$ sobre F, respectivamente, entonces*

$$[F(\alpha, \beta) : F] = p^2$$

a menos que $b = c^p a^k$, para algún $k \in \mathbb{Z}$ y para algún $c \in F$.

Demostración. Si el polinomio $X^p - b$ permanece irreducible sobre $F(\alpha)$, entonces $[F(\alpha, \beta) : F] = p^2$. Si es reducible sobre $F(\alpha)$, entonces tiene una raíz γ en $F(\alpha)$. (Lema 2.4.3.) Como $\gamma^p = b \in F$, se sigue del Corolario 2.3.7 que $\gamma = ca^k$, para algún $k \in \mathbb{Z}$, y para algún $c \in F$. Elevando esta ecuación a la p-ésima potencia, obtenemos que $b = c^p a^k$.

□

Supongamos que α y β son raíces de los polinomios irreducibles $X^p - a$ y $X^p - b$ sobre F, respectivamente. ¿Qué podemos decir acerca del grado de $\alpha + \beta$, si $[F(\alpha, \beta) : F] = p^2$? Para contestar esta pregunta, primero probaremos el siguiente lema:

Lema 2.4.28. *Sean E/F una extensión de Galois finita y α y β dos elementos de E de grado m y n sobre F, respectivamente, tales que*

$$[F(\alpha, \beta) : F] = mn.$$

(*i*) *Para cualesquiera conjugados α_i de α y β_i de β, existe $\sigma \in \mathrm{Gal}(E/F)$ tal que*

$$\sigma(\alpha) = \alpha_i \quad y \quad \sigma(\beta) = \beta_j.$$

(*ii*) *Si ninguna de las diferencia de dos conjugados de* α *es igual a la diferencia de conjugados de* β*, entonces*

$$F(\alpha, \beta) = F(\alpha + \beta).$$

Demostración.

(*i*) Como E/F es una extensión de Galois finita, tenemos que existe $\theta \in \mathrm{Gal}(E/F)$ tal que $\theta(\alpha_i) = \alpha$. Escribimos $\theta(\beta_j) = \beta_k$, para algún conjugado β_k de β. Afirmamos que existe $\theta_1 \in \mathrm{Gal}(E/F)$ tal que $\theta_1(\alpha) = \alpha$ y $\theta_1(\beta_k) = \beta$; si se comprueba la afirmación, se tendrá lo deseado al tomar $\sigma = (\theta_1\theta)^{-1}$.

Sean $\beta_1, \ldots, \beta_n$ todos los conjugados de β sobre F. Nuestra hipótesis implica que el grado de β sobre $F(\alpha)$ es todavía n, así que las raíces de su polinomio irreducible sobre $F(\alpha)$ son $\beta_1, \ldots, \beta_n$. Puesto que $E/F(\alpha)$ es de Galois, el automorfismo requerido existe.

(*ii*) Sean $\alpha_1, \ldots, \alpha_m$ todos los conjugados de α sobre F. Entonces, por (i), todos los

$$\alpha_i + \beta_j \qquad (1 \leq i \leq m,\ \ 1 \leq j \leq n)$$

son todos los conjugados de $\alpha + \beta$. Si dos son iguales, entonces la diferencia de dos conjugados de α sería igual a la diferencia de dos conjugados de β. Así, por hipótesis, todos los $\alpha_i + \beta_j$ son distintos, probando que el grado de $\alpha + \beta$ es mn. Por lo tanto, $F(\alpha + \beta) = F(\alpha, \beta)$.

□

Terminamos esta sección con el siguiente resultado:

Teorema 2.4.29. *Sean* F *un campo y* p *un primo distinto de la característica de* F*. Sean* α *y* β *raíces de los polinomios irreducibles de la forma* $X^p - a$ *y* $X^p - b$ *sobre* F*, respectivamente. Si* $[F(\alpha, \beta) : F] = p^2$*, entonces* $F(\alpha + \beta) = F(\alpha, \beta)$*, es decir,* $\alpha + \beta$ *tiene grado* p^2 *sobre* F*.*

Demostración. Puesto que la característica de F es distinta de p, α y β son separables sobre F. Por lo tanto, existe una extensión finita de Galois E/F, con $\alpha, \beta \in E$. Debido al Lema 2.4.28, basta verificar que ninguna diferencia de dos conjugados de α es igual a una diferencia de dos conjugados de β. Ahora, la diferencia de dos conjugados de α tiene la forma $(\zeta_p^i - \zeta_p^j)\alpha$, donde ζ_p es una raíz p-ésima primitiva de la unidad. De aquí que, si una diferencia de dos conjugados de α es igual a una diferencia de dos conjugados de β, entonces $\alpha/\beta \in F(\zeta_p)$. Pero $[F(\zeta_p) : F] \leq p-1$, donde

el grado de α/β sobre F divide a $p^2 = [F(\alpha, \beta) : F]$. Así $\alpha/\beta \in F$, contradiciendo que $[F(\alpha, \beta) : F] = p^2$.

□

Capítulo 3

La cerradura normal de algunas extensiones de Kummer

En este capítulo, demostraremos nuestro resultado principal y, para ello, usaremos la Teoría de Kummer más rudimentaria, es decir, consideraremos p un número primo y K un campo de característica distinta de p conteniendo una ζ raíz p-ésima primitiva de la unidad. Entonces, adjuntando varias raíces p-ésimas de K, una extensión finita de Galois con grupo de Galois abeliano y anulado por p, y recíprocamente toda extensión de Galois de este tipo se obtiene de esta manera. Así que extensiones de este tipo corresponden a subgrupos finitos $N/(K^*)^p$ de $K^*/(K^*)^p$; las raíces p-ésimas de los elementos de N que generan al cociente dan una extensión $L = K(\sqrt[p]{N})$. Así pues, el grupo de Galois de la extensión L/K es isomorfo a $N/(K^*)^p$.

De acuerdo con el Teorema 2.3.4, tenemos una función de pareo (**pareo de Kummer**)

$$\begin{aligned} \phi: \quad N/(K^*)^p \times \mathrm{Gal}(L/K) \quad &\longrightarrow \qquad \langle\zeta\rangle \\ (a(K^*)^p, \tau) \qquad &\longmapsto \quad \tau(\sqrt[p]{a})/\sqrt[p]{a}. \end{aligned}$$

Esta función de pareo es bi-multiplicativa, y considerando a los grupos involucrados como espacios vectoriales sobre el campo finito $\mathbb{F}_p$ de p elementos, tenemos que este pareo es no-degenerado. Así, el grupo $\mathrm{Gal}(L/K)$ (como espacio vectorial) es isomorfo al espacio dual de $N/(K^*)^p$.

Notemos que si el campo K considerado arriba es extensión de un campo F, entonces tenemos claramente que el campo L, extensión de Kummer sobre K, es de Galois sobre F si y sólo si todo F-conjugado de los elementos de N están también en N. Esto quiere decir que el grupo $\mathrm{Gal}(K/F)$ actúa en el grupo $K^*/(K^*)^p$, y las extensiones de Kummer que son de Galois sobre F son aquellas que provienen de

grupos $N/(K^*)^p$ los cuales son invariantes bajo esta acción. En este caso, el grupo abeliano elemental $\mathrm{Gal}(L/K)$ es un subgrupo normal de $\mathrm{Gal}(L/F)$ y, en consecuencia, el grupo $\mathrm{Gal}(K/F)$ actúa en el grupo $\mathrm{Gal}(L/K)$ por conjugación en elementos de $\mathrm{Gal}(L/K)$. Notemos que no estamos suponiendo que ζ sea elemento de F; si no lo es, entonces dicha acción puede ser una acción de grupo sobre $\langle\zeta\rangle$. Además, el pareo de Kummer es consistente con la acción de $\mathrm{Gal}(K/F)$ sobre los tres grupos involucrados. En efecto, sea σ un elemento de $\mathrm{Gal}(K/F)$, y sea σ_1 una extensión de σ a L; entonces $\sigma_1 \in \mathrm{Gal}(L/F)$. Si $a \in N$ y $\tau \in \mathrm{Gal}(L/K)$, entonces tenemos que $\sigma_1(\sqrt[p]{a})^p = \sigma(a)$, y

$$\begin{aligned}\phi(\sigma(a)(E^*)^p, \sigma_1\tau\sigma_1^{-1}) &= (\sigma_1\tau\sigma_1^{-1})(\sigma_1(\sqrt[p]{a}))/\sigma_1(\sqrt[p]{a}) \\ &= \sigma(\tau(\sqrt[p]{a})/\sqrt[p]{a}).\end{aligned}$$

3.1. El grado de la extensión

Fijaremos la notación que utilizaremos en lo que resta de este capítulo. p será un número primo fijo, y F es un campo de característica distinta de p el cual contiene a ζ, una raíz p-ésima primitiva de unidad. Sea K una extensión de Galois cíclica de F con grupo de Galois $\langle\sigma\rangle$ de orden $q = p^n$.

Dado $a \in K$, consideraremos la extensión $K(\sqrt[p]{a})$ de K, y sea L la cerradura normal de $K(\sqrt[p]{a})$ sobre F. El objetivo es determinar la estructura del grupo $\mathrm{Gal}(L/F)$.

Teorema 3.1.1. *Sean $\zeta \in F$ y K/F una extensión de Galois con grupo de Galois $\langle\sigma\rangle$ de orden $q = p^n$. Se tiene lo siguiente:*

(*i*) *Para cualquier $a \in K$, definimos la sucesión de elementos tomando $a_0 = a$ y $a_{i+1} = \sigma(a_i)/a_i$. Entonces a_q es siempre una potencia de p.*

(*ii*) *Sea a_s el primer elemento en la sucesión que es una potencia de p. Entonces, la cerradura normal L de $K(\sqrt[p]{a})$ sobre F tiene grado p^s sobre K y está dada por $L = K(\sqrt[p]{a_0}, \ldots, \sqrt[p]{a_{s-1}})$.*

(*iii*) *Los únicos subcampos de L que contienen a K y que son de Galois sobre F son los de la forma $K(\sqrt[p]{a_r}, \ldots, \sqrt[p]{a_{s-1}})$.*

Demostración.

(*i*) Sea S el operador lineal dada por la acción de σ en el espacio vectorial $K^*/(K^*)^p$ con escalares en el campo finito $\mathbb{F}_p$. Para hacer más expresiva la demostración, usaremos notación aditiva, con la suma de elementos en el espacio vectorial dada por $\overline{a}+\overline{b} := \overline{ab}$, con $a, b \in K^*$, y la multiplicación escalar como $n \cdot \overline{a} := \overline{a}^{\,n}$. Como $\sigma^q = 1$, el polinomio mínimo de este operador lineal en cualquier espacio invariante divide a $X^q - 1$. Pero este espacio vectorial tiene característica p, luego se satisface que $X^q - 1 = (X-1)^q$ y, por lo tanto, el operador lineal $S - I$ es nilpotente de orden a lo más q. Es decir, existe un $n \in \mathbb{N}$, $n \leq q$, tal que $(S-I)^n = 0 = \langle (K^*)^p \rangle$. Puesto que $(S-I)^i(\overline{a}) = \overline{a_i}$, se tiene que $\overline{a_q} = 0 = (K^*)^p$. Por lo tanto $a_q \in (K^*)^p$.

(*ii*) Si consideramos a un vector $\overline{a} \in K^*/(K^*)^p$, tenemos que los elementos $\overline{a}$, $(S-I)\overline{a} = \overline{a_1}, \ldots, (S-I)^{s-1}\overline{a} = \overline{a_{s-1}}$ forman un conjunto linealmente independiente que generan al subespacio cíclico $C(\overline{a}, S-I)$ del espacio vectorial $K^*/(K^*)^p$ (Corolario 1.2.7), el cual sabemos que es invariante bajo $S - I$. Notemos que el subespacio $C(\overline{a}, S-I)$ es de la forma $N/(K^*)^p$, donde N es el subgrupo de K^* generado por los elementos $a_0, \ldots, a_{s-1}$ junto con $(K^*)^p$. Puesto que el subespacio $C(\overline{a}, S-I) = N/(K^*)^p$ es invariante bajo $S - I$ si y sólo si es invariante bajo S (Corolario 1.1.5), tenemos que, al aplicar la Teoría de Kummer, la extensión $L = K(\sqrt[p]{a_0}, \sqrt[p]{a_1}, \ldots, \sqrt[p]{a_{s-1}})$ es la cerradura normal de $K(\sqrt[p]{a})$ sobre F. además, si $N = \langle a_1, \ldots, a_{s-1} \rangle (K^*)^p$, entonces $|N/(K^*)^p| = p^s$, y se tiene que $[L : K] = p^s$ (Teorema 2.3.4).

(*iii*) El subespacio generado por los vectores $\overline{a_0}, \overline{a_1}, \ldots, \overline{a_{s-1}}$ no tiene subespacios invariantes bajo la acción de σ, excepto aquellos que son generados por los vectores $\overline{a_r}, \overline{a_{r+1}}, \ldots, \overline{a_{s-1}}$ y, por lo tanto, son los únicos subcampos de L que son Galois sobre F, los cuales son de la forma $K(\sqrt[p]{a_r}, \ldots, \sqrt[p]{a_{s-1}})$.

□

3.2. La estructura del grupo de Galois

Conservaremos las notaciones e hipótesis del Teorema 3.1.1.

Teorema 3.2.1. *Sean $G = \mathrm{Gal}(L/F)$ y $A = \mathrm{Gal}(L/K)$, donde $A \cong (\mathbb{Z}/p\mathbb{Z})^s$ y $G/A \cong \langle \sigma \rangle$. Sea $\{\tau_0, \ldots, \tau_{s-1}\} \subseteq A$ la base dual de $\{a_0, \ldots, a_{s-1}\}$ bajo el pareo de la Teoría de Kummer. Entonces,*

(*i*) *La acción de σ fija a τ_0 y mapea cada τ_i en $(\tau_i\tau_{i-2}\cdots)(\tau_{i-1}\tau_{i-3}\cdots)^{-1}$ para $i > 0$.*

(*ii*) *Si $s = q$, entonces G es único salvo isomorfismo, y es el producto semidirecto $A \rtimes \langle\sigma\rangle$.*

(*iii*) *Si $s < q$, hay exactamente dos posibles tipos de isomorfismos para G, el producto semidirecto $A \rtimes \langle\sigma\rangle$ y uno más.*

Demostración.

(*i*) Tenemos que $\sigma(a_i) = a_{i+1}a_i$, para cada $i \geq 0$. En el espacio vectorial $K^*/(K^*)^p$, tenemos entonces que $S(\overline{a_i}) = \overline{a_i} + \overline{a_{i+1}}$. En particular se tiene que $S(\overline{a_{s-1}}) = \overline{a_{s-1}}$. Por lo que la matriz asociada a este operador lineal es de la forma

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 1 & 1 & \dots & \dots & \dots & \vdots \\ 0 & 1 & \ddots & \dots & \dots & \vdots \\ \vdots & \vdots & \dots & \ddots & \dots & \vdots \\ \vdots & \vdots & \dots & \dots & 1 & 0 \\ 0 & 0 & \dots & \dots & 1 & 1 \end{bmatrix}$$

Tomando la transpuesta de la inversa de la matriz anterior tenemos

$$\begin{bmatrix} 1 & -1 & \dots & \dots & (-1)^{s-1} \\ 0 & 1 & \dots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -1 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

Por lo que, pasando a la notación multiplicativa de nuevo, tenemos que $S^*(\tau_0) = \tau_0$ y $S^*(\tau_i) = (\tau_i\tau_{i-2}\dots)(\tau_{i-1}\tau_{i-3}\dots)^{-1}$, para $i > 0$.

(*ii*) Supongamos ahora que $s = q$, y consideremos $\sigma_1 \in G$ tal que $\sigma_1|_K = \sigma$. Tenemos entonces que la acción de σ en A está dada por la conjugación con σ_1, es decir, que $\sigma\phi = \sigma_1\phi\sigma_1^{-1}$, para todo $\phi \in A$. Por un lado, cualquier elemento $\psi \in G$ puede ser escrito de la forma $\tau\sigma_1^i$, para algún $\tau \in A$ y $0 \leq i < q$. En efecto, como la cantidad de elementos en G es qp^s, se tiene que éstos son exactamente los de la forma $\tau\sigma_1^i$ (variando los τ en A y $0 \leq i < q$), lo que nos darán también qp^s elementos. Para verificar esto, basta con establecer que $\tau\sigma_1^j \neq \tau'\sigma_1^l$ si $\tau \neq \tau'$ o $j \neq l$. Si $\tau\sigma_1^j = \tau'\sigma_1^l$, con $0 \leq l \leq j < q$, entonces $\tau^{-1}\tau' = \sigma_1^{j-l}$, con lo cual $\sigma^{j-l} = \tau^{-1}\tau'|_K = id_K$, es decir, $j = l$, lo cual implica que $\tau = \tau'$. Así, tenemos que $G = A\langle\sigma_1\rangle$. Ahora bien, $\sigma_1^q \in A$, pues $\sigma^q = 1$;

además es dejado fijo por la acción de σ, por lo que es una potencia de τ_0. Por último, si $\sigma_1^q = 1$, entonces $\langle\sigma_1\rangle \cong \langle\sigma\rangle$ y $G \cong A \rtimes \langle\sigma\rangle$. Si no, podemos elegir otra extensión $\tau\sigma_1$ de σ tal que $(\tau\sigma_1)^q = 1$. En efecto, observemos primero que

$$\begin{aligned}(\tau\sigma_1)^q &= (\tau\sigma_1)\cdots(\tau\sigma_1) \quad (q \text{ veces}) \\ &= \tau(\sigma_1\tau\sigma_1^{-1})(\sigma_1^2\tau\sigma_1^{-2})\cdots(\sigma_1^{q-1}\tau\sigma_1^{-(q-1)})\sigma_1^q.\end{aligned}$$

Pasando esto a notación aditiva, y tomando en cuenta que estamos trabajamos sobre un campo de característica p, tenemos

$$(\tau\sigma_1)^q = \left((I + S + \cdots + S^{q-1})\tau\right)\sigma_1^q = \left((S - I)^{q-1}\tau\right)\sigma_1^q. \tag{3.2.1}$$

En particular, para τ_{q-1} tenemos

$$(\tau_{q-1}\sigma_1)^q = 1,$$

pues $(S - I)^r\tau_s = 1$, si $r > s$. Por lo tanto $G = A \rtimes \langle\sigma_1\rangle$.

(iii) Si suponemos que $s < q$, entonces, por la ecuación (3.2.1), todas las extensiones de σ tienen la misma q-ésima potencia. Si alguna de esas potencias, y por lo tanto todas, es la identidad, entonces tendremos de nuevo el producto semidirecto. En caso contrario, podemos tener algún $\tau_0^k \neq 1$, y la relación $\sigma_1^q \neq 1$ nos determina un nuevo grupo G, distinto del producto semidirecto. Más aún, si elegimos otro generador del grupo cíclico $\langle\sigma\rangle$, σ^e, con $(e, p) = 1$, debemos de reemplazar τ_0^k por τ_0^{ek} y, entonces, los grupos que inducen son isomorfos. Finalmente, los casos con σ_1^q no trivial y σ_1^q trivial nos proporcionan grupos no isomorfos entre sí, ya que el producto semidirecto tiene elementos de orden a lo más $q = p^n$ y el otro tiene un elemento de orden p^{n+1}. Cuando no es el producto semidirecto, una de clase en $H^2(\langle\sigma\rangle, A)$ determina la estructura de G (Teorema 1.3.1).

□

Notemos que en la demostración del teorema anterior, cuando el grupo G no es el producto semidirecto, entonces la aplicación del Teorema 1.3.1 está dado con $T = \langle\sigma\rangle \cong G/A$, y la sección s de T en G está dada por extensiones fijas a L de los elemento de T.

Teorema 3.2.2. *Supóngase que* $1 \leq s < q$. *Sean* $d \in K$ *tal que* $d^p = a_{q-1}$, $e(k) = \binom{q}{k}/p$ *y*

$$c = \left(\prod_{k=1}^{q-1} a_k^{e(k)}\right) \cdot \left(\frac{\sigma(d)}{d}\right)$$

Entonces $c^p = 1$, *y el grupo* $G = \mathrm{Gal}(L/F)$ *es el producto semidirecto si y slo si* $c = 1$.

Demostración. De acuerdo con la definición de los a_i, podemos elegir las raíces p-ésimas w_i de tal manera que satisfagan la relación $w_{i+1} = \sigma(w_i)/w_i$. Tenemos además

$$\begin{aligned} X^q &= ((X-1)+1))^q \\ &= \sum_{k=1}^{q} \binom{q}{k} (X-1)^{q-k} 1^k. \end{aligned}$$

Pasando a la notación multiplicativa y evaluando en las raíces tenemos

$$\sigma_1^q(w_0) = \prod_{k=0}^{q} w_k^{\binom{q}{k}}.$$

Por lo tanto

$$\sigma_1^q(w_0)/w_0 = \prod_{k=1}^{q} w_k^{pe(k)}.$$

Denotemos esta cantidad por c_1. Tenemos $w_0^p = a_0$ y $\sigma_1^q(a_0) = \sigma^q(a_0) = a_0$, por lo que $c_1^p = 1$. Para $k < q$, reemplazamos $w_k^{pe(k)}$ por $a_k^{e(k)} \in K$. Por hipótesis, tenemos que $d^q = a_{q-1}$, luego $w_{q-1} = d\zeta^s$, para algún s. Como $\zeta \in F$, tenemos $w_q = \sigma_1(w_{q-1})/w_{q-1} = \sigma(d)/d$. En consecuencia, $c_1 = c$. Además, sabemos por el Teorema 3.2.1 que $\sigma_1^q = \tau_0^k$, por lo que es trivial si y sólo si su acción sobre w_0 es trivial. Por lo tanto, G es producto semidirecto si y sólo si $c = 1$

□

Observación 3.2.3. Cuando $s < q - 1$, es posible reescribir la fórmula para c y expresar todos sus factores a partir de $k = s$ en términos de las p-ésimas raíces de a_s, las cuales por definición están en K. Ssupóngase en particular que $s = 1$, y escribimos $a_1 = b^p$. Por conveniencia, de nuevo podemos utilizar la notación aditiva, tratando a K^* como un $\mathbb{Z}[\sigma]$-módulo. Por ejemplo, $\sigma(b)/b$ es el resultado de aplicar $\sigma - 1$ a b. Para $i \geq 1$, se obtuvo w_i como resultado de aplicar $(\sigma - 1)^i$ a b. En

particular, hasta una potencia irreducible de ζ, obtenemos a d como el resultado de aplicar $(\sigma-1)^{q-2}$ a b y, por lo tanto, $\sigma(d)/d$ es el resultado de aplicar $(\sigma-1)^{q-1}$ a b. Así que, c es obtenido de aplicar a b la operación

$$\sum_{k=1}^{q-1}\binom{q}{k}(\sigma-1)^{k-1}+(\sigma-1)^{q-1}=\frac{(\sigma^q-1)}{\sigma-1}=\sum_{k=0}^{q-1}\sigma^k.$$

En K^*, esto significa que c es el producto de todos los conjugados de b. Así, en este caso, el teorema se reduce al resultado de Albert.

Finalizamos nuestro trabajo de tesis con el siguiente:

Ejemplo 3.2.4. Denotaremos por ζ_n a una raíz n-ésima primitiva de la unidad en $\mathbb{C}$. Sean p un número primo y F la p-ésima extensión ciclotómica sobre $\mathbb{Q}$, es decir, $F=\mathbb{Q}(\zeta_p)$. Entonces, la extensión $F/\mathbb{Q}$ es de grado $\varphi(p)=p-1$, donde φ es la función de Euler.

Por otro lado, sean l un número primo y $K=F(\sqrt[p]{l}\,)=\mathbb{Q}(\zeta_p,\sqrt[p]{l}\,)$, donde $\sqrt[p]{l}\in\mathbb{R}$. Tenemos que K es la cerradura normal de la extensión $\mathbb{Q}(\sqrt[p]{l}\,)/\mathbb{Q}$. Puesto que el polinomio X^p-l es irreducible sobre $\mathbb{Q}$, por el Criterio de Eisenstein, tenemos que $[\mathbb{Q}(\sqrt[p]{l}\,):\mathbb{Q}]=p$. Luego, la extensión $K/\mathbb{Q}$ es de grado $p(p-1)$ y, en consecuencia, la extensión K/F es de grado p. Por lo tanto, el polinomio X^p-l se mantiene irreducible sobre F. Más aún, por el Teorema 2.3.4, tenemos que la extensión K/F es una extensión de Kummer de exponente p y, de aquí que, es una extensión cíclica de grado p.

Denotemos por $a:=\sqrt[p]{l}$, y sea σ un generador de $\mathrm{Gal}(K/F)$, o sea, $\mathrm{Gal}(K/F)=\langle\sigma\rangle$. Puesto que los conjugados de a sobre F son $a,\ \zeta_p a,\ \zeta_p^2 a,\ldots,\ \zeta_p^{p-1}a$, y σ está completamente determinado por su acción sobre a, donde $\sigma(a)=\zeta_p^i a$ para algún $i\in\{1,\ldots,p-1\}$, tenemos que $(i,p)=1$, al ser σ de orden p. Como el grupo cíclico $\langle\sigma\rangle$ tiene $\varphi(p)=p-1$ generadores, podemos elegir σ tal que $\sigma(a)=\zeta_p a$.

De acuerdo con las notaciones y el enunciado del Teorema 3.1.1, elegimos el elemento $a\in K$ de arriba para tener la sucesión $a_0=a$ y $a_{i+1}=\sigma(a_i)/a_i$, para $i\geq 0$. Notemos que en nuestro caso $q=p$. Así que, a_p es siempre una p-ésima potencia de K. Sea a_s el primer elemento de la sucesión el cual es una p-ésima potencia de K. Más precisamente, tenemos que $a_0=\sqrt[p]{l}$, $a_1=\zeta_p$ y $a_i=1$, para cada $i\geq 2$; es decir, $s=2$. En efecto, si ζ_p fuera una p-ésima potencia de K, entonces existiría $\alpha\in K$ tal que $\alpha^p=\zeta_p$, con lo cual α sería una p^2-ésima raíz primitiva de la unidad contenida en K; así que $\alpha=\zeta_{p^2}$. Puesto que las extensiones $K/\mathbb{Q}$ y $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ tienen el mismo grado, con $\mathbb{Q}(\zeta_{p^2})\subseteq K$, tendremos que necesariamente $K=\mathbb{Q}(\zeta_{p^2})$. Notemos que

la extensión $\mathbb{Q}(\sqrt[p]{l}\ )/\mathbb{Q}$ es de Galois si $p = 2$, y no lo es para $p > 2$. Así pues, para $p = 2$ tendremos que $\mathbb{Q}(\sqrt[p]{l}\ ) = K = \mathbb{Q}(\zeta_{p^2}) = \mathbb{Q}(\zeta_4)$, lo cual es absurdo pues $\sqrt[p]{l} \in \mathbb{R}$; mientras que para $p > 2$ se tendría que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{l}\ ) \subseteq K = \mathbb{Q}(\zeta_{p^2})$, luego la extensión $\mathbb{Q}(\sqrt[p]{l}\ )/\mathbb{Q}$ sería de abeliana, lo cual también es absurdo.

De acuerdo con el Teorema 3.1.1(ii), $L = K(\sqrt[p^2]{l},\ \zeta_{p^2})$ es la cerradura normal de $K(\sqrt[p^2]{l}\ )$ sobre F la cual es de grado p^2. También, de acuerdo con las notaciones del Teorema 3.2.1, tenemos que $A = \mathrm{Gal}(L/K) \cong C_p \times C_p$, donde C_p es el grupo cíclico de p elementos y $G/A \cong \langle\sigma\rangle$, donde $G = \mathrm{Gal}(L/F)$. Luego, para $p = 2$ tenemos que G es el producto semidirecto de A y $\langle\sigma\rangle$, ya que $s = 2 = p = q$. Para $p > 2$ tendremos que $s = 2 < p = q$, y G no es el producto semidirecto de A y $\langle\sigma\rangle$. Para probar nuestra afirmación, aplicaremos el Teorema 3.2.2. Así que, definimos

$$c = \left(\prod_{k=1}^{q-1} a_k^{e(k)}\right) \cdot \left(\frac{\sigma(d)}{d}\right) = \zeta_p \neq 1,$$

ya que el elemento $d \in K$ satisface que $d^p = a_{p-1} = 1$ y $\sigma(d)/d = 1$; además de que $a_1 = \zeta_p$, $a_i = 1$, para cada $2 \leq i \leq p-1$ y $e(1) = 1$. Por lo tanto, por el Teorema 3.2.2, para $p > 2$ tenemos que G no es el producto semidirecto de A y $\langle\sigma\rangle$.

Para $p > 2$, caractericemos al grupo G bajo isomorfismo. Para esto, aplicamos los resultados de la Sección 1.3 del Capítulo 1. Notemos que en dicha sección tenemos las mismas notaciones que nuestro ejemplo. Así que, $T = G/A \cong \langle\sigma\rangle$ y π es el epimorfismo de G en T dado por restricción al campo K. Si expresamos a $T = \{1,\ \sigma,\ \sigma^2, \ldots,\ \sigma^{p-1}\}$, entonces definimos la sección s de T en G dada por $s(\sigma^i) = \sigma_1^i$, para cada $0 \leq i \leq p-1$, donde σ_1 es una extensión fija de σ; por ejemplo, podemos tomar σ_1 que esté determinada por las relaciones $\sigma_1(\sqrt[p^2]{l}\ ) = \zeta_{p^2}\sqrt[p^2]{l}$ y $\sigma_1(\zeta_{p^2}) = \zeta_{p^2}$. Notemos que σ tiene exactamente p^2 extensiones. Además, dicha sección satisface que $s(1) = 1$. Para cada $0 \leq i \leq p-1$ y $0 \leq j \leq p-1$ arbitrarios, sean $k_{ij},\ t_{ij} \in \mathbb{Z}$ tales que $0 \leq k_{ij} \leq p-1$ y $i + j = k_{ij} + pt_{ij}$. Definimos f de $T \times T$ en A dada por $f(\sigma^i, \sigma^j) := \sigma_1^{pt_{ij}}$, para cada $0 \leq i \leq p-1$ y $0 \leq j \leq p-1$. Entonces, tenemos que

$$\begin{aligned} s(\sigma^i)s(\sigma^j) &= \sigma_1^i\sigma_1^j = \sigma_1^{i+j} = \sigma_1^{pt_{ij}}\sigma_1^{k_{ij}} = \sigma_1^{pt_{ij}}s(\sigma^{k_{ij}}) \\ &= f(\sigma^i, \sigma^j)s(\sigma^i\sigma^j), \end{aligned}$$

para cada $0 \leq i \leq p-1$ y $0 \leq j \leq p-1$. Así, f es un conjunto de factores el cual está normalizado, ya que $k_{11} = 0$, $t_{11} = 0$ y $f(1,1) = 1$. Luego, $G(f) = T \times A$ es un grupo con operación

$$(\sigma^i, \tau)(\sigma^j, \tau') = (\sigma^{i+j}, \tau\sigma^i\tau' f(\sigma^i, \sigma^j)).$$

Por lo tanto, $G \cong G(f)$. Observemos que, en efecto, $f \neq 1$ y G no es el producto semidirecto de A y $\langle\sigma\rangle$ (pues, como $k_{p-1,p-1} = p-2$ y $t_{p-1,p-1} = 1$, tenemos que $f(\sigma^{p-1}, \sigma^{p-1}) = \sigma_1^p \neq 1$).

Conclusiones

En matemáticas se nos presentan muchos resultados que, después de varios años, admiten una generalización. En nuestro trabajo de tesis, una generalización a un resultado de A. A. Albert ha sido estudiado, después de más de 70 años de su aparición. W. C. Waterhouse nos muestra que algunas de generalizaciones son posibles utilizando herramienta sencilla, como es la aplicación de los subespcios invariantes y los subespacios cíclicos, para obtener la cerradura normal de ciertas extensiones de Kummer (Teorema 3.1.1); pero también, aplicando herramienta más sofisticada, se pudo determinar de manera completa el grupo de Galois a través de una clase de conjuntos de factores de un Segundo Grupo de Cohomología (Teorema 3.2.1). Una sencilla verificación, nos muestra el tipo de grupo que debería de ser el grupo de Galois de la cerradura normal de la extensión de Kummer en consideración (Teorema 3.2.2) que, por supuesto, no siempre ha de ser el producto semidirecto como lo muestra nuestro Ejemplo 3.2.4.

El problema inverso de la Teoría de Galois Finita consiste en que dado G un grupo finito, se pueda encontrar una extensión de Galois L/F teniendo como grupo de Galois a G. Es probable que, las cerraduras normales de las extensiones de Kummer tratadas en este trabajo, se puedan encontrar ejemplos de extensiones de Galois de grado $p^s q$ con grupo de Galois finito G teniendo un p-subgrupo abeliano elemental normal A y G/A cíclico de orden q.

Bibliografía

[1] Albert, A. A., *On normal Kummer fields over a non-modular field*, Trans. Amer. Math. Soc., Vol. **36**, 1934, pp. 885-892.

[2] _____ , *On cyclic fields*, Trans. Amer. Math. Soc., Vol. **37**, 1935, pp. 452-462.

[3] _____ , *Modern Higher Algebra*, University of Chicago Press, Chicago, 1937.

[4] Hoffman, K., y R. Kunze, *Algebra Lineal*, Prentice-Hall Hispanoamericana, S. A., 1971.

[5] Hungerford, T. W., *Algebra*, Springer-Verlag New York Inc., 1974.

[6] Karpilovski, G., *Field Theory: Classical Foundations and Multiplicative Groups*, Marcel Dekker, Inc., 1988.

[7] Villa-Salvador, G. D., *Introducción a la Teoría de las Funciones Algebraicas*, Fondo de Cultura Económica, 2003.

[8] Waterhouse, W. C., *The normal closure of certain Kummer extensions*, Canad. Math. Bull., Vol. **37** (1), 1984, pp. 133-139.

Índice alfabético