UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

BASES NORMALES EN CAMPOS FINITOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A :

GERARDO RUBÉN LÓPEZ HERNÁNDEZ

DIRECTOR DE TESIS:
DR. JUAN MORALES RODRÍGEZ
2016

Ciudad Universitaria, D. F.

1. Datos del alumno	1. Datos del alumno
Apellido paterno	López
Apellido materno	Hernández
Nombre(s)	Gerardo Rubén
Teléfono	26 42 00 45
Universidad Nacional Autónoma de México	Universidad Nacional Autónoma de México
Facultad de Ciencias	Facultad de Ciencias
Carrera	Matemáticas
Número de cuenta	405097515
2. Datos del tutor	2. Datos del tutor
Grado	Dr
Nombre(s)	Juan
Apellido paterno	Morales
Apellido materno	Rodríguez
3. Datos del sinodal 1	3. Datos del sinodal 1
Grado	Dra
Nombre(s)	Diana
Apellido paterno	Avella
Apellido materno	Alaminos
4. Datos del sinodal 2	4. Datos del sinodal 2
Grado	Dra
Nombre(s)	Bertha María
Apellido paterno	Tomé
Apellido materno	Arreola
5. Datos del sinodal 3	5. Datos del sinodal 3
Grado	Dra
Nombre(s)	María del Carmen Herendira
Apellido paterno	Goméz
Apellido materno	Laveaga
6. Datos del sinodal 4	6. Datos del sinodal 4
Grado	Mat
Nombre(s)	Ernesto
Apellido paterno	Mayorga
Apellido materno	Saucedo
7. Datos del trabajo escrito	7. Datos del trabajo escrito
Título	Bases normales en campos finitos
Subtitulo	
Número de páginas	33 pg
Año	2016

Dedicado

A Dios mi trabajo, por siempre socorrerme, amarme y perdonarme como solo el puede.

A mis padres Reynaldo López Pérez y Carmen Hernández Prieto, por ser mis estrellas referentes en este mundo.

A mi mujer Josefina Janeth Miranda Blancas y Quetzalli López Miranda, que son mi razón de superación en esta vida.

A mis hermanos Clara Mirella Hernández, Felipe Antonio López Hernández, Héctor Alejandro López Hernández y Rodrigo Gabriel Medina Hernández porque sin el amor de una familia seria muy difícil enfrentar la vida.

A Teodoro López Pérez, Alicia Montes de Oca, Juan José López Montes de Oca y Jóse Juan López Montes de Oca por que los amo mucho.

En memoría de Isabel Alicía López Montes de Oca, por haberme irradiado con su singular alegría de vivir y confiar en mi como un hermano mayor.

Agradecimientos

Al Doctor Juan Morales Rodriguéz por el gran apoyo y comprensión en momentos muy inciertos.

Al Doctor Octavio Paez Osuna por haberme brindado su mano para levantarme en situaciones muy difíciles que la vida da.

A mis amigos y personas que de una u otra forma me han ayudado para lograr este trabajo, José Roberto de la Vega Martínez, Bernardo Vargas Cárdenas, Edgar René Hernández Martínez, Manuel Díaz Díaz, Raul Bartolo, José Lino Samaniego Mendoza, Miguel Osorio Hernández, Graciela Gloria Ocampo Vázquez, Marcos Durán Tapía, José Sanchez Juárez, a la familia Mendez Bravo, a las secretarias de la facultad de ciencias por su gran ayuda y todas las personas que me faltaron nombrar, gracias.

Índice general

Introducción

Dado E un campo, el subcampo primo F de E es la intersección de todos los subcampos de E. En este caso se tiene que E es un espacio vectorial sobre F; si E es un campo finito con q elementos, su subcampo primo es isomorfo a $\mathbb{Z}_p$, para algún primo p, la dimensión de E sobre F es necesariamente finita, digamos que sea n, siendo E isomorfo a F^n y se tiene entonces que E consta de p^n elementos, esto es, si E es un campo finito y su subcampo primo es $\mathbb{Z}_p$, el cardinal q de E es $q = p^n$. Se prueba que para todo primo p y toda $n \geq 1$ existe un campo con p^n elementos y que si K y L son campos con p^n elementos, son isomorfos.
Si E es un campo finito y tiene p^n elementos, escribimos $E = GF(p^n)$. Los campos finitos se conocen como campos de Galois.
Sea $\mathscr{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}$ una base ordenada de $GF(p^n)$ sobre $GF(p)$, $v_1, v_2 \in GF(p^n)$ y

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

son los vectores de coordenadas de v_1 y v_2 con respecto de la base $\mathscr{B}$ respectivamente. Dado que E es un campo, tiene sentido considerar el producto $v_1 v_2$ en E. Surge entonces la siguiente pregunta: ¿como podemos expresar al vector de coordenadas de $v = v_1 v_2$ con respecto de la base $\mathscr{B}$ en términos de A y B?
Se tiene que

$$\begin{aligned} v = v_1 v_2 &= (\sum_{i=1}^{n} a_i \beta_i)(\sum_{j=1}^{n} b_j \beta_j) \\ &= \sum_{j=1}^{n} \sum_{i=1}^{n} a_i b_j \beta_i \beta_j. \end{aligned} \tag{1}$$

y supóngase que

$$\beta_i \beta_j = \sum_{k=1}^{n} d_{ij}^{(k)} \beta_k, \tag{2}$$

con $d_{ij}^{(k)} \in GF(p)$. De (1) y (2) se obtiene que

$$v = \sum_{k=1}^{n}(\sum_{j=1}^{n}\sum_{i=1}^{n} a_i b_j d_{ij}^{(k)})\beta_k. \tag{3}$$

Si

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

es el vector de coordenadas de v con respecto de la base $\mathscr{B}$, de (3) se obtiene que

$$c_k = \sum_{j=1}^{n}\sum_{i=1}^{n} a_i b_j d_{ij}^{(k)}, \text{ para } 1 \leq k \leq n. \tag{4}$$

Así podemos observar que

$$c_k = \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} \begin{pmatrix} d_{11}^{(k)} & \dots & d_{1n}^{(k)} \\ \vdots & & \vdots \\ d_{n1}^{(k)} & \dots & d_{nn}^{(k)} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}. \tag{5}$$

Si $D_k = [d_{ij}^{(k)}]$

$$c_k = [v_1]_{\mathscr{B}}^{t} D_k [v_2]_{\mathscr{B}}$$

La matriz D_k está determinada por la base $\mathscr{B}$. Es deseable encontrar una base apropiada $\mathscr{B}$ tal que los cálculos a realizar para obtener c_k, sean lo más sencillos posibles.
El objetivo principal de esta tesis es mostrar que si E es una extensión finita de un campo F, existen bases de E sobre F que cumplen con los requerimientos anteriores, (algunas de estas son llamadas bases normales). Bajo ciertas condiciones existen bases normales óptimas, que como dice su nombre optimizan los cálculos para encontrar el vector de coordenadas del producto de dos elementos de $GF(p^n)$.

Capítulo 1

Bases Normales

Después de definir el concepto de base normal y de dar un ejemplo, recordaremos algunas definiciones y resultados necesarios para demostrar que existe una base normal para todo campo de Galois sobre su subcampo primo.

Definición 1 *Sea $E = GF(p^n)$ y $F = GF(p)$, su subcampo primo. Una base $\{v_0, v_1, \ldots, v_{n-1}\}$ de E sobre F es normal si existe $\alpha \in E$ tal que $v_0 = \alpha, v_1 = \alpha^p, \ldots, v_{n-1} = \alpha^{p^{n-1}}$.*

Ejemplo. Sea $f(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$, $f(x)$ es irreducible en $\mathbb{Z}_2[x]$. Es conocido que existe $\alpha \in GF(2^5)$ tal que $f(\alpha) = 0$; si $\beta = \alpha^3$ y $\mathscr{N} = \{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}\} = \{\alpha^3, \alpha^3 + \alpha, \alpha^3 + \alpha^2 + \alpha, \alpha^4 + \alpha^3 + \alpha^2 + \alpha, 1\}$, se tiene que $\mathscr{N}$ es una base normal de $GF(2^5)$ sobre $GF(2)$.
Presentamos el teorema principal de este trabajo:

Teorema 1 *Para cualquier campo finito, existe una base normal de éste sobre su subcampo primo.*

Con la finalidad de presentar una demostración de este teorema, recordaremos algunos resultados necesarios.

Definición 2 *$p(x) \in F[x]$ es irreducible sobre F si $grd(p(x)) \geq 1$ y los únicos divisores de $p(x)$ en $F[x]$ son polinomios de grado cero o del mismo grado que $p(x)$.*

Definición 3 *Decimos que $f(x) \in F[x]$ es reducible sobre F si no es irreducible.*

Ejemplos:

(i) $x^2 - 2 \in \mathbb{Q}[x]$ es irreducible sobre $\mathbb{Q}$.

(ii) $x^2 + 1 \in \mathbb{R}[x]$ es irreducible sobre $\mathbb{R}$.

(iii) $x^2 + 1 \in \mathbb{C}[x]$ es reducible sobre $\mathbb{C}$.

(iv) $x^2 + 2x + 1$ en $F[x]$ es reducible sobre $F[x]$.

(v) Si $f(x) \in F[x]$ y $grd(f(x)) = 1$, $f(x)$ es irreducible.

Se tiene el siguiente importante hecho:

Teorema 2 *Si $f(x) \in F[x]$, con $grd(f(x)) \geq 1$, existen $a \in F$ y $p_1(x), p_2(x), \ldots, p_s(x) \in F[x]$ irreducibles mónicos tales que $f(x) = ap_1(x)p_2(x)\ldots p_s(x)$ con $s \geq 1$. La descomposición es única salvo el orden de los factores.*

Observacion 1. Sea F un campo. Si $f(x) \in F[x]$ y $grd(f(x)) \in \{2, 3\}$, entonces $f(x)$ es reducible sobre F si y sólo si $f(x)$ tiene una raíz en F.
Demostración. Supongamos que $f(x)$ es reducible, por lo cual $f(x) = g(x)h(x)$ con $grd(g(x)) < grd(f(x))$ y $grd(h(x)) < grd(f(x))$ y como el grado de $f(x)$ es dos o tres, uno de los polinomios $g(x)$ o $h(x)$ tiene grado uno y este tiene una raíz en F. Por consiguiente $f(x)$ tiene una raíz en F. La otra implicación es inmediata en virtud del teorema del factor. ■

Observacion 2. Un polinomio de grado mayor o igual a cuatro con coeficientes en el campo F puede ser reducible y no tener raíces en F, como el siguiente polinomio $f(x) = (x^2 + 1)(x^2 - 2) \in \mathbb{Q}[x]$, que es claramente reducible pero no tiene raíces en $\mathbb{Q}$.

Observacion 3. Sea $p(x) \in F[x]$ y $J := \{p(x)a(x) | a(x) \in F[x]\}$, se tiene que:

(i) $J \neq \emptyset$.

(ii) Si α, $\beta \in J$, $\alpha - \beta \in J$.

(iii) Si $b(x) \in F[x]$, y $\alpha \in J$ entonces $\alpha b(x) \in J$.

Al conjunto J lo denotaremos como $(p(x))$.
Se define $f(x) + J := \{f(x) + g(x) | g(x) \in J\}$ y $F[x]/J := \{f(x) + J | f(x) \in F[x]\}$. Se tiene que $f(x) + J = g(x) + J$ si y solo si $f(x) - g(x) \in J$.

Lema 1 $F[x]/J = \{r(x) + J | r(x) \in F[x], grd(r(x)) < grd(p(x))\}$.

Demostración. Por el algoritmo de la división, si $f(x) \in F[x]$, existen únicos $q(x)$ y $r(x) \in F[x]$ con $grd(r(x)) < grd(p(x))$ tales que $f(x) = p(x)q(x) + r(x)$ y por consiguiente $f(x) + J = r(x) + J$, lo que implica que
$F[x]/J = \{r(x) + J | r(x) \in F[x], grd(r(x)) < grd(p(x))\}$. ■

Observación 4. En el caso que $p(x) \in F[x]$ sea irreducible, $F[x]/J$ es un campo con las siguientes operaciones $(f(x) + J) + (g(x) + J) = (f(x) + g(x)) + J$ y
$(f(x) + J)(g(x) + J) = f(x)g(x) + J$, con idénticos aditivo y multiplicativo $0 + J$ y $1 + J$ respectivamente.

Definición 4 *Sean F y F' campos con idénticos multiplicativos 1 y $1'$ respectivamente. Un homomorfismo de F en F' es una función no cero $\varphi : F \to F'$ tal que*
$\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ *y* $\varphi(1) = 1'$.

Definición 5 *Sean F y F' campos, un isomorfismo de F en F' es un homomorfismo biyectivo entre ellos.*

Sea $p(x) \in F[x]$ irreducible y $J = (p(x))$, si consideramos la función $\varphi : F \to F[x]/J$ tal que $\varphi(a) = a + J$, se tiene que φ es un homomorfismo inyectivo y de esta manera se puede pensar a F como un subcampo de $F[x]/J$.

Teorema 3 *Si $p(x) \in F[x]$ es irreducible sobre F, existe un campo E que contiene como subcampo a F en donde $p(x)$ tiene una raíz.*

Demostración. Si $grd(p(x)) = 1$, $E = F$. Si $p(x)$ es irreducible sobre F y $grd(p(x)) > 1$, $p(x)$ no tiene raíces en F. Sin embargo, si a $p(x) = a_0 + a_1x + \cdots + a_sx^s$ lo consideramos como un polinomio con coeficientes en $F[x]/J$ con $J = (p(x))$, esto es,
$p(x) = (a_0 + J) + (a_1 + J)x + \cdots + (a_s + J)x^s$, se observa que $\alpha = x + J \in F[x]/J$ es una raíz de $p(x)$ ya que

$$\begin{aligned} p(\alpha) =& (a_0 + J) + (a_1 + J)(x + J) + \cdots + (a_s + J)(x + J)^s \\ =& (a_0 + a_1x + \cdots + a_sx^s) + J \\ =& p(x) + J = J. \blacksquare \end{aligned}$$

Corolario 1 **(Teorema de Kronecker)** *Si $f(x) \in F[x]$, con $grd(f(x)) \geq 1$, existe un campo E que contiene a F como subcampo donde $f(x)$ tiene una raíz.*

Demostración. Si $f(x) = ap_1(x)p_2(x)\cdots p_r(x)$ es la descomposición del teorema 2 como producto de polinomios mónicos irreducibles y $E = F[x]/(p_1(x))$, E contiene a F y $\alpha = x + (p_1(x))$ es una raíz de $p_1(x)$ y por consiguiente α es una raíz de $f(x)$.

Corolario 2 *Si $f(x) \in F[x]$ es mónico de grado $s \geq 1$, existe un campo Σ que contiene a F como subcampo tal que $f(x) = c(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_s)$ con $c \in F$ y $\alpha_1, \alpha_2, \ldots, \alpha_s \in \Sigma$.*

Demostración. Por inducción sobre el grado de $f(x)$. Si $grd(f(x)) = 1$, es inmediato. Supongamos que $grd(f(x)) > 1$. Por el teorema de Kronecker existe un campo E que contiene a F y donde $f(x)$ tiene una raíz α; $f(x) = c(x - \alpha)h(x)$ con $h(x) \in E[x]$. Como el $grd(h(x)) < grd(f(x))$, por hipótesis de inducción existe un campo Σ que contiene a E como subcampo tal que $h(x)$ se descompone como producto de polinomios de grado uno con coeficientes en Σ; es decir $h(x) = (x - \alpha_2)(x - \alpha_3)\cdots(x - \alpha_s)$ y Σ resulta ser el campo buscado. $\blacksquare$

Definición 6 *Decimos que un campo E es una extensión del campo F y escribimos $E : F$ si existe un homomorfismo $\sigma : F \to E$.*

Ejemplos de extensiones: $\mathbb{R}$ es una extensión de $\mathbb{Q}$ y $\mathbb{C}$ es una extensión de $\mathbb{R}$.

Definición 7 *Sea $p(x) \in F[x]$ irreducible, $p(x)$ es separable si $p(x)$ no tiene raíces repetidas.*

Definición 8 *Si $f(x) \in F[x]$ y $f(x) = \alpha p_1(x)p_2(x)\dots p_s(x)$ es la descomposición en polinomios irreducibles sobre F, $f(x)$ es separable si $p_i(x)$ es separable para cada i, $1 \leq i \leq s$.*

Definición 9 *Si E es una extensión de F, se dice que $\alpha \in E$ es algebraico sobre F si existe un polinomio $f(x) \in F[x]$ diferente del polinomio cero tal que $f(\alpha) = 0$.*

Definición 10 *Si $E : F$ y $\alpha \in E$ es algebraico sobre F, al polinomio $p(x) \in F[x]$ que se anula en α, de grado mínimo y mónico se le llama el polinomio mínimo de α sobre F.*

Observacion 5. Sea $E : F$ una extensión de campos, $\alpha \in E$ algebraico sobre F y $p(x)$ el polinomio mínimo de α sobre F, entonces $p(x)$ es irreducible sobre F.

Demostración Si $p(x) = g(x)h(x)$ con $g(x)$, $h(x) \in F[x]$, se tiene que $g(\alpha) = 0$ o $h(\alpha) = 0$ y como $grd(g(x)) \leq grd(p(x))$ y $grd(h(x)) \leq grd(p(x))$ se tiene que $grd(g(x)) = grd(p(x))$ o $grd(h(x)) = grd(p(x))$, es decir, $p(x)$ es irreducible. ■

Observacion 6. Si E es un campo, la intersección de una familia no vacía de subcampos de E es un subcampo.
Demostración. Sea $\{E_l\}$ una familia no vacía de subcampos de E y $K = \cap E_l$ la intersección de todos ellos.
Se tiene que $K \neq \emptyset$ pues todos los E_l contienen a la identidad aditiva y multiplicativa.
Si $a, b \in K$, $a, b \in E_l$ para todo E_l, por lo que $a + b$, ab, $-a \in E_l$ lo que implica que $a + b, ab, -a \in K$. Si $a \in K$ con $a \neq 0$, por el mismo argumento, a^{-1} está en K. ■

Definición 11 *Sea E una extensión del campo F y S un subconjunto de E. La intersección de todos los subcampos de E que contienen a F y S se llama el subcampo generado por F y S, y se denota por $F(S)$.*

De aquí en adelante en lugar de escribir $F(\{\alpha\})$ escribiremos $F(\alpha)$.
A partir de resultados elementales se prueba lo siguiente.

Lema 2 *Sea $E : F$ y $\alpha \in E$. Se tiene que $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} | f(x), g(x) \in F[x], g(\alpha) \neq 0\}$.*

Teorema 4 *Sea $E : F$ una extensión de campos, $\alpha \in E$ algebraico sobre F y $p(x) \in F[x]$ el polinomio mínimo de α sobre F. Se tiene que*
$F(\alpha) = \{f(\alpha) | f(x) \in F[x], grd(f(x)) < grd(p(x))\}$.

Demostración. Sea $M = \{f(\alpha)|f(x) \in F[x], grd(f(x)) < grd(p(x))\}$. Es claro que $M \subset F(\alpha)$.
Por otro lado, si $y \in F(\alpha)$, $y = f(\alpha)/g(\alpha)$ con $f(x), g(x) \in F[x]$ y $g(\alpha) \neq 0$. Como $p(x)$ no divide a $g(x)$, entonces se tiene que $(p(x), g(x)) = 1$ y $1 = p(x)a(x) + g(x)b(x)$ con $a(x), b(x) \in F[x]$. Luego $f(x)/g(x) = \frac{f(x)p(x)a(x)+f(x)g(x)b(x)}{g(x)} = \frac{f(x)p(x)a(x)}{g(x)} + f(x)b(x)$.
Además por otro lado, $f(x)b(x) = p(x)q(x) + r(x)$ con $grd(r(x)) < grd(p(x))$. Por lo tanto $f(\alpha)/g(\alpha) = r(\alpha) \in M$. ■

Teorema 5 *Si $E : F$ es una extensión de campos, $\alpha \in E$ es algebraico sobre F y $p(x) \in F[x]$ es el polinomio mínimo de α sobre F, existe un isomorfismo φ de $F(\alpha)$ en $F[x]/(p(x))$ tal que $\varphi(\alpha) = x + (p(x))$.*

Demostracion. Como $F(\alpha) = \{f(\alpha)|f(x) \in F[x], grd(f(x)) < grd(p(x))\}$ y $F[x]/(p(x)) = \{r(x) + (p(x))|r(x) \in F[x], grd(r(x)) < grd(p(x))\}$, si definimos $\varphi : F(\alpha) \to F[x]/(p(x))$ como $\varphi((f(\alpha)) = f(x) + (p(x))$, no es difícil ver que φ es un isomorfismo y que $\varphi(\alpha) = x + (p(x))$. ■

Teorema 6 *Sea $E : F$ una extensión, $\alpha \in E$ algebraico sobre F, $p(x)$ el polinomio mínimo de α sobre F y $grd(p(x)) = n$. Se tiene que $F(\alpha)$ es un espacio vectorial de dimensión n sobre F.*

Demostración. Del teorema 4 se sigue que $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ genera a $F(\alpha)$ sobre F. Cualquier polinomio diferente de cero de grado menor al de $p(x)$ evaluado en α no se anula, por lo que el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es linealmente independiente y tiene n elementos por lo tanto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F. ■

Definición 12 *Si $E : F$ es una extensión de campos, el grado de $E : F$ es la dimensión de E sobre F como espacio vectorial y lo denotaremos por $[E : F]$. En el caso de que $[E : F]$ sea finito se dice que la extensión es finita, en caso contrario decimos que es infinita.*

Observacion 7. Si $E : F$ es finita y $\alpha \in E$, se tiene que α es algebraico sobre F.
Demostración. Supóngase que $[E : F] = n$. La lista $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n$ de elementos de E es linealmente dependiente, por lo cual existe una combinación lineal de la lista igual a cero con no todos los escalares cero. Lo que implica que existe $f(x) \in F[x]$, $f \neq 0$, tal que $f(\alpha) = 0$, esto es, que α es algebraico sobre F. ■

Teorema 7 *Sean $K : F$ y $E : K$ extensiones finitas de campos. Se tiene que $[E : F] = [E : K][K : F]$.*

Demostración. Sea $\mathscr{B}_1 = \{\beta_1, \beta_2, \ldots \beta_r\}$ base de K sobre F y $\mathscr{B}_2 = \{\alpha_1, \alpha_2, \ldots \alpha_s\}$ base de E sobre K, no es difícil hacer ver que $\mathscr{B}_3 = \{\beta_i\alpha_j : \beta_i \in \mathscr{B}_1 \text{ y } \alpha_j \in \mathscr{B}_2\}$ es base de E sobre F. ■

Definición 13 *Sea $f(x) \in F[x]$ de grado mayor o igual a uno. Un campo de descomposición de $f(x)$ sobre F, es una extensión E de F tal que $f(x)$ es producto de polinomios de grado uno en $E[x]$ y si K es un subcampo propio de E que contiene F, $f(x)$ no es producto de polinomios de grado uno con coeficientes en K.*

Ejemplo. Sea $x^2 - 2 \in \mathbb{Q}[x]$. $E = \mathbb{Q}(\sqrt{2})$ es un campo de descomposición de $x^2 - 2$ sobre $\mathbb{Q}$.

Teorema 8 *Sea $f(x) \in F[x]$, con $grd(f(x)) \geq 1$, si E es una extension de F y $f(x)$ se descompone como producto de polinomios de grado uno con coeficientes en E, existe un campo de descomposición de f sobre F contenido en E.*

Demostración Sea Σ la intersección de todos los subcampos K de E que contienen a F y $f(x)$ es producto de polinomios de grado uno en $K[x]$. No es complicado ver que Σ es un campo de descomposición de $f(x)$ sobre F. ■

Lema 3 *Sean F y F' campos y σ un isomorfismo de F en F'. Si se define $\sigma^* : F[x] \to F'[x]$ como $\sigma^*(\sum_{i=1}^{s} a_i x^i) = \sum_{i=1}^{s} \sigma(a_i)x^i$, se tiene que σ^* es un isomorfismo de $F[x]$ en $F'[x]$.*

Demostración. Se sigue de la definicion de σ^* que esta es homomorfismo. Se verá que σ^* es biyectiva.
Sean $f(x), g(x) \in F[x]$, con $f(x) = \sum_{i=0}^{s} a_i x^i$ y $g(x) = \sum_{i=0}^{s} b_i x^i$, tal que
$\sigma^*(f(x)) = \sigma^*(g(x))$.
Se tiene que $\sum_{i=0}^{s} \sigma(a_i)x^i = \sum_{i=0}^{s} \sigma(b_i)x^i$ lo que implica que $\sigma(a_i) = \sigma(b_i)$ para todo $i = 0, 1, \ldots s$ y como σ es inyectivo, tenemos que $f(x) = g(x)$.
Ahora veamos que σ^* es sobre.
Sea $g(x) \in F'[x]$, $g(x) = \sum_{i=1}^{s} b_i x^i$. Como σ es isomorfismo de F en F', σ es sobre por lo que cada $b_i = \sigma(a_i)$ para algún $a_i \in F$. Por lo tanto existe $f(x) \in F[x]$ tal que $\sigma^*(f(x)) = g(x)$, a saber $f(x) = \sum_{i=1}^{s} a_i x^i$. ■

Notación. Con las condiciones del lema 3, para cada $f(x) \in F[x]$, en lugar de $\sigma^*(f(x))$ se escribirá $f^*(x)$.

Lema 4 *Sean $E : F$ y $E' : F'$ extensiones de campos, σ un isomorfismo de F en F', $p(x) \in F[x]$ irreducible sobre F, $\alpha \in E$ una raíz de $p(x)$ y $\beta \in E'$ una raíz de $p^*(x)$. Entonces existe un único isomorfismo $\widehat{\sigma} : F(\alpha) \to F'(\beta)$ tal que $\widehat{\sigma}(a) = \sigma(a)$ para todo $a \in F$ y $\widehat{\sigma}(\alpha) = \beta$.*

Demostración. Como $p(x)$ es irreducible sobre F, $p^*(x)$ es irreducible sobre F', $p(x)$ es el polinomio mínimo de α sobre F y $p^*(x)$ es el polinomio mínimo de β sobre F'.
Sea $\widehat{\sigma} : F(\alpha) \to F'(\beta)$ dada por $\widehat{\sigma}(f(\alpha)) = (\sigma^* f)(\beta)$. $\widehat{\sigma}$ es un isomorfismo, que $\widehat{\sigma}(\alpha) = \beta$.

Veamos ahora la unicidad de $\widehat{\sigma}$. Supongamos que φ es un isomorfismo de $F(\alpha)$ en $F'(\beta)$ con $\varphi(a) = \sigma(a)$ para toda $a \in F$ y $\varphi(\alpha) = \beta$, si $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{s-1}\alpha^{s-1}$,

$$\begin{aligned}\varphi(f(\alpha)) &= \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + \cdots + \varphi(a_{s-1})\varphi(\alpha)^{s-1} \\ &= \varphi(a_0) + \varphi(a_1)\beta + \cdots + \varphi(a_{s-1})\beta^{s-1} \\ &= \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{s-1})\beta^{s-1} \\ &= \widehat{\sigma}(f(\alpha)).\end{aligned}$$

Por lo tanto $\varphi = \widehat{\sigma}$. ■

Teorema 9 *Si σ es un isomorfismo entre los campos F y F', $f(x) \in F[x]$, con $grd(f(x)) \geq 1$, E es campo de descomposición de $f(x)$ sobre F y E' es campo de descomposición de $f^*(x)$ sobre F', se tiene que*

(i) Existe un isomorfismo $\widetilde{\sigma} : E \to E'$ que extiende a σ.

(ii) Si $f(x)$ es separable, para cada isomorfismo $\sigma : F \to F'$, existen exactamente $[E : F]$ isomorfismos como en (i).

Demostración de (i). Se procede por inducción sobre $[E : F]$. Si $[E : F] = 1$, entonces $E = F$ y $f(x)$ es un producto de factores lineales en $F[x]$; de esto se sigue que $f^*(x)$ es también un producto de factores lineales en $F'[x]$, así $E' = F'$. Por lo tanto se cumple (i) con $\widetilde{\sigma} = \sigma$.
Supongamos que $[E : F] > 1$. Existe $p(x) \in F[x]$ un factor irreducible de $f(x)$ con grado $d > 1$. Sea $\alpha \in E$ una raíz de $p(x)$ y si $\beta \in E'$ una raíz de $p^*(x)$, por el lema 4 existe un único isomorfismo $\widehat{\sigma}$ isomorfismo de $F(\alpha)$ en $F'(\beta)$ que extiende a σ. Si además $E = F(\alpha)$, se tiene que $E' = F(\alpha)$ y entonces se cumple (i) con $\widetilde{\sigma} = \widehat{\sigma}$.
Supongamos que $F(\alpha)$ es un subcampo propio de E. Por lo que $1 < [E : F(\alpha)] < [E : F]$. Ahora, E es campo de descomposición de $f(x)$ sobre $F(\alpha)$, así como E' es un campo de descomposición de $f^*(x)$ sobre $F'(\beta)$. Por hipótesis de inducción existe $\widetilde{\sigma}$ que extiende a $\widehat{\sigma}$ y como $\widehat{\sigma}$ extiende a σ entonces $\widetilde{\sigma}$ extiende a σ.
Demostración de (ii). Si $[E : F] = 1$, $E = F$ y F es campo de descomposición de $f(x)$ sobre F. Consecuentemente $E' = F'$, F' es campo de descomposición de $f^*(x)$ sobre F' y $\widetilde{\sigma} = \sigma$ es la única extensión de σ y por lo tanto se cumple (ii).
Si $[E : F] > 1$, $f(x)$ tiene un factor irreducible $p(x)$ con $grd(p(x)) = d > 1$. Si $\alpha \in E$ es una raíz de $p(x)$, en virtud del lema 4, para cada $\beta \in E'$ raíz de $p^*(x)$, existen exactamente d extensiones de σ de este tipo, ya que $p^*(x)$ es separable sobre F'.
Por hipótesis de inducción, cada σ_β se puede extender a un isomorfismo de E en E' de $\frac{[E:F]}{d}$ formas diferentes y por consiguiente σ se puede extender de $(\frac{[E:F]}{d})d$ maneras diferentes de la forma indicada.
Para terminar la demostración del teorema es necesario hacer ver que $\widetilde{\sigma} : E \to E'$ es una extensión de σ, $\widetilde{\sigma}$ es una de las extensiones de σ que se obtiene como en el párrafo anterior.

Si $\widetilde{\sigma}$ lo restringimos a $F(\alpha)$, se obtiene un isomorfismo de $F(\alpha)$ en $F'(\widetilde{\sigma}(\alpha))$ y $\widetilde{\sigma}(\alpha)$ es una raíz de $p^*(x)$. Por lo tanto existe un isomorfismo de $F(\alpha)$ en $F'(\sigma(\alpha))$ que extiende a σ, pero $\widetilde{\sigma}|_{F(\alpha)} = \sigma_{\widetilde{\sigma}(\alpha)}$ es decir es una de las extensiones mencionadas anteriormente. ■

Corolario 3 *Si E y E' son campos de descomposición de $f(x) \in F[x]$ sobre F, se tiene que E y E' son isomorfos.*

Demostración. Es consecuencia inmediata del inciso (i) del teorema 9, considerando $F = F'$ y $\sigma = Id$. ■

Definición 14 *Sea F un campo y $f(x) \in F[x]$ con $f(x) = \sum_{i=0}^{n} a_i x^i$. El polinomio derivada de $f(x)$ es el polinomio $f'(x) = \sum_{i=0}^{n-1}(i+1)a_{(i+1)}x^i$.*

Teorema 10 *Sea F un campo, $f(x) \in F[x]$ y $f'(x) \in F[x]$ el polinomio derivada de $f(x)$. $f(x)$ no tiene raíces repetidas si y sólo si el máximo común divisor de $f(x)$ y $f'(x)$ es uno.*

Demostración. Sea E un campo de descomposición de $f(x)$ sobre F, y $d(x)$, el máximo común divisor de f y f'. Supóngase que $d(x) \neq 1$ y sea α raíz de $d(x)$. Entonces α es raíz común de $f(x)$ y $f'(x)$, por lo que, si α es raíz de multiplicidad $k \geq 1$ de $f'(x)$, se tiene que α es de multiplicidad $k+1$ de $f(x)$, y como $k+1 \geq 2$, se tiene que $f(x)$ tiene raíces repetidas. Supongamos ahora que $f(x)$ tiene una raíz repetida en alguna extensión de F. Entonces $f(x) = (x-\alpha)^k g(x)$ con $k > 1$ y $f'(x) = (x-\alpha)^k g'(x) + k(x-\alpha)^{k-1}g(x)$, lo que implica que $(x-\alpha)$ divide a $f'(x)$ y por consiguiente $(x-\alpha)$ divide a $(f(x), f'(x))$ y $(f(x), f'(x)) \neq 1$. ■

Ahora demostraremos el siguiente resultado.

Teorema 11 **(Pequeño Teorema de Fermat)** *Si $a \in \mathbb{Z}_p$, se tiene que $a^p = a$.*

Demostración. Sea $a \neq 0$, como $\mathbb{Z}_p - \{0\}$ es un grupo multiplicativo de orden $p-1$, $a^{p-1} = 1$ y $a^p = a$.
Si $a = 0$, es claro que $a^p = a$. ■

Teorema 12 *Si $m = p^n$ con p un primo, $n \geq 1$, existen campos con m elementos.*

Demostración. Sea $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, E un campo en donde $f(x)$ se descompone como producto de factores de grado uno y $K = \{\alpha \in E | \alpha \text{ es raíz de } f(x)\}$. Se tiene que $\mathbb{Z}_p \subset K$ en virtud del pequeño teorema de Fermat, K tiene p^n elementos porque $f(x)$ no tiene raíces repetidas debido al teorema 10 y K resulta ser un subcampo de E. ■

Observemos que un campo E con p^n elementos es campo de descomposición de $f(x) = x^{p^n} - x$ sobre F, con F el subcampo primo de E:
Si $a \in E - \{0\}$, $a^{p^n-1} = 1$, así $a^{p^n} = a$, por lo que α es raíz de $f(x) = x^{p^n} - x \in F[x]$.
Por otro lado $0^{p^n} - 0 = 0$ lo que implica que todo elemento de E es raíz de $f(x)$ y por consiguiente E es campo de descomposición de $f(x)$ sobre F.
También se tiene el siguiente resultado.

Teorema 13 *Si p es un primo, $n \in \mathbb{Z}$, $n \geq 1$, E y E' campos con p^n elementos, se tiene que E y E' son isomorfos.*

Demostración. Como E y E' son campos de descomposición de $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ sobre $\mathbb{Z}_p$, se sigue que son isomorfos. ■

Definición 15 *Si E es un campo, un automorfismo de E es un isomorfismo de E en E.*

Se tiene que el conjunto $aut(E)$ formado por todos los automorfismos del campo E, es un grupo con la operación composición de funciones.
Sea $E : F$ una extensión de campos. Es fácil hacer ver que

$$Gal(E : F) := \{\sigma \in aut(E) \quad | \quad \sigma(a) = a \text{ para toda } a \in F\}$$

es un subgrupo de $aut(E)$.

Definición 16 *Si $E : F$ es una extensión de campos, a $Gal(E : F)$ se le llama el grupo de Galois de $E : F$.*

Observacion 8. Si $\sigma \in Gal(E : F)$, σ es un operador lineal de E sobre F.

Lema 5 *Si $\sigma : GF(p^n) \to GF(p^n)$ es tal que $\sigma(a) = a^p$, $\sigma \in Gal(GF(p^n) : GF(p))$.*

Demostración. $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$, $\sigma(a + b) = (a + b)^p = a^p + b^p$ porque $GF(p^n)$ es de característica p, es fácil ver que σ es inyectiva y en consecuencia dado que el conjunto $GF(p^n)$ es finito es un automorfismo. En virtud del teorema (pequeño) de Fermat se tiene que $\sigma \in Gal(GF(p^n) : GF(p))$. ■

Definición 17 *Al automorfismo σ del lema anterior se le llama el automorfismo de Frobenius de $GF(p^n)$.*

Teorema 14 *Si $f(x) \in F[x]$ es separable y E es el campo de descomposición de $f(x)$ sobre F, se tiene que $Gal(E : F)$ es de orden $[E : F]$.*

Demostración. Es una consecuencia inmediata del inciso (ii) del teorema 9 al considerar $F = F'$, $E = E'$ y $\sigma = Id$. ■

Lema 6 *La dimensión de $GF(p^n)$ sobre $GF(p)$ es n, es decir $[GF(p^n) : GF(p)] = n$.*

Demostración. Como $GF(p^n)$ es finito, $[GF(p^n) : GF(p)]$ es finita, digamos que sea s. $GF(p^n)$ es isomorfo a $(GF(p))^s$, y como $GF(p)$ tiene p elementos, $(GF(P))^s$ tiene p^s, por consiguiente $p^n = p^s$ y $n = s$. ■

Recordemos la siguiente caracterización de los grupos cíclicos finitos.
Un grupo finito es cíclico si y solo si para cada divisor del orden del grupo, este tiene a lo más un subgrupo de ese orden.
Usando la caracterización anterior, se prueba el siguiente resultado.

Teorema 15 *Si F es un campo y G es un subgrupo finito del grupo multiplicativo F, G es cíclico.*

Demostración. Sea m un divisor del orden de G, si H y K son dos subgrupos diferentes de orden m, $H \cup K$ tiene más de m elementos y todos ellos son raíces del polinomio $x^m - 1$, lo que es imposible, por que un polinomio de grado m, con coeficientes en un campo, tiene a lo más m raíces en el campo, de donde se sigue que G es cíclico.

Teorema 16 *Para todo $n \geq 1$, existe un polinomio irreducible de grado n sobre el campo $F = GF(p)$.*

Demostración. Como el grupo multiplicativo H de $GF(p^n)$ es cíclico, si α es un generador de H, se tiene que $GF(p^n) = H \cup \{0\} = F(\alpha)$. Como $[F(\alpha) : F] = grd(p(x))$ con $p(x)$ el polinomio mínimo de α sobre F, que es irreducible sobre F, y ya que $n = [GF(p^n) : GF(p)]$ se sigue que $p(x)$ es de grado n. ■

Teorema 17 *Si $E = GF(p^n)$, el grupo de Galois $G = Gal(E : F)$ es un grupo cíclico de orden n y el automorfismo de Frobenius es un generador.*

Demostración. $E = F(\alpha)$, con α un generador de $E - \{0\}$. Si $p(x) \in F[x]$, es el polinomio mínimo de α y con $grd(p(x)) = n$, E contiene a lo más n raíces de $p(x)$.
Si $\varphi \in G$, $h \in E - \{0\}$, $h = \alpha^k$ para alguna $k \in \mathbb{Z}$, $\varphi(h) = \varphi(\alpha^k) = \varphi(\alpha)^k$, lo que implica que φ esta determinado por $\varphi(\alpha)$.
Como α es raíz de $p(x)$, $\varphi(\alpha)$ también es raíz de $p(x)$, por lo tanto $|G| \leq n$.
Si σ es el automorfismo de Frobenius de $E : F$, $< \sigma > \leq G$. Si probamos que el orden de σ es n, se tendría que $G =< \sigma >$, que es lo que se quiere demostrar.
Como $\sigma(a) = a^p$, $\sigma^k(a) = a^{p^k}$ para toda $a \in E$, en particular $\sigma^n(a) = a^{p^n}$. Como cada elemento de E es raíz de $x^{p^n} - x$, se tiene que $\sigma^n(a) = a^{p^n} = a$ para toda $a \in E$, es decir $\sigma^n = Id$.
Si l es el orden de σ y $l < n$, $\sigma^l = Id$. Entonces, para toda $a \in E$, $a = \sigma^l(a) = a^{p^l}$, lo que implica que el polinomio $g(x) = x^{p^l} - x$ de grado $p^l < p^n$ tiene más raíces que su grado, lo que es una contradicción por lo tanto el orden de σ es n. ■

Notacion. Si F es un campo, $M_n(F)$ es el conjunto de todas las matrices de $n \times n$ con entradas en el campo F.
Observacion 9. Si $A \in M_n(F)$, entonces como $F \subset F[x]$, se tiene que $A \in M_n(F[x])$.

Definición 18 *Si $A \in M_n(F)$, la matriz caracteristíca de A, es la matriz $xI - A \in M_n(F[x])$.*

Definición 19 *Si $A \in M_n(F)$, el polinomio característico de A es el determinante de $xI - A$.*

Observacion 10. Si $A \in M_n(F)$, de la definición de determinante se sigue que el polinomio característico de A es un polinomio $p(x)$ de la forma

$$x^n - (a_{11} + a_{22} + \cdots + a_{nn})x^{n-1} + g(x)$$

con $g(x) \in F[x]$ de grado menor que $n-1$ y con término constante igual a $(-1)^n det(A)$.

$$p(x) = |xI - A| = x^n - (a_{11} + a_{22} + \cdots + a_{nn})x^{n-1} + \cdots + (-1)^n det(A).$$

Definición 20 *Sea F un campo, $f(x) = a_s x^s + a_{s-1}x^{s-1} + \cdots + a_1 x + a_0 \in F[x]$ y $A \in M_n(F)$. Definimos $f(A)$ como:*
$f(A) = a_s A^s + a_{s-1}A^{s-1} + \cdots + a_1 A + a_0 I$.

Definición 21 *Si $A \in M_n(F)$ y $f(x) \in F[x]$, se dice que f anula a A si $f(A)$ es la matriz cero y escribimos $f(A) = 0$.*

Teorema 18 *Si F es un campo y $B \in M_n(F)$, existe un polinomio no cero $f(x)$ con coeficientes en F tal que f anula a B.*

Demostración. Si B es diferente de la matriz cero se tiene que la lista de matrices $I, B, B^2, \ldots, B^{n^2}$ es linealmente dependiente sobre F porque la dimensión de $M_n(F)$ es n^2. Entonces existen $\alpha_0, \alpha_1, \ldots, \alpha_{n^2} \in F$ no todos cero tales que $\alpha_0 I + \alpha_1 B + \ldots, +\alpha_{n^2} B^{n^2} = 0$ lo que nos dice que el polinomio $f(x) = \alpha_0 + \alpha_1 x + \ldots, +\alpha_{n^2} x^{n^2}$, que es diferente de cero, anula a B. ■

Definición 22 *Si $B \in M_n(F)$, al polinomio $m(x) \in F[x]$ de grado mínimo y mónico que anula a B se le llama el polinomio mínimo de B sobre F.*

Observacion 11. Sean $f(x) \in F[x]$, $B \in M_n(F)$ y $m(x) \in F[x]$ el polinomio mínimo de B. Si $f(B) = 0$ entonces $m(x)$ divide a $f(x)$.
Demostración. Por el algoritmo de la división tenemos que $f(x) = m(x)q(x) + r(x)$; con $q(x), r(x) \in F[x]$ y $gr(r(x)) < gr(f(x))$. Como $0 = f(B) = m(B)q(B) + r(B) = r(B)$ y $m(x)$ es el polinomio mínimo de B, se sigue que $r(x) = 0$. ■

Definición 23 *Sea $A \in M_n(F)$. A_{ij} es la matriz de $(n-1) \times (n-1)$ que se obtiene de A eliminando el renglón i y la columna j de A.*

Se recuerda que el determinante de $A = (a_{ij})$ es
$(-1)^{i+1}a_{i1}det(A_{i1}) + (-1)^{i+2}a_{i2}det(A_{i2}) + \cdots + (-1)^{i+j}a_{ij}det(A_{ij}) + \cdots + (-1)^{i+n}a_{in}det(A_{in})$,
y que el cofactor de a_{ij} es $(-1)^{i+j}det(A_{ij})$, y se denota por a'_{ij}, por lo que

$$det(A) = a_{i1}a'_{i1} + a_{i2}a'_{i2} + \cdots + a_{ij}a'_{ij} + \cdots + a_{in}a'_{in}$$

Definición 24 *Si $A \in M_n(F)$, la matriz de cofactores de A es la matriz $C = (c_{ij}) \in M_n(F)$ con $c_{ij} = a'_{ij}$*

Definición 25 *La matriz adjunta de A es la matriz transpuesta de C y se denota por $adj(A)$.*

Teorema 19 *Si $A \in M_n(F)$ se tiene que $A(adj(A)) = det(A)I_n = adj(A)A$.*

Demostración. El elemento (i, j) de $A(adj(A))$ es el producto del renglón i de A con la columna j de $adj(A)$, es decir,

$$\begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix} \begin{pmatrix} a'_{j1} \\ a'_{j2} \\ \vdots \\ a'_{jn} \end{pmatrix} = a_{i1}a'_{j1} + a_{i2}a'_{j2} + \cdots + a_{in}a'_{jn}.$$

Si $j = i$, esta expresión es el determinante de A; y si $j \neq i$, es el determinante de una matriz con dos renglones iguales.
Luego,

$$A(adj(A)) = \begin{pmatrix} det(A) & 0 & \dots & 0 \\ 0 & det(A) & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & det(A) \end{pmatrix} = det(A)I.$$

Análogamente, $adj(A)A = det(A)$. ■

Teorema 20 **(Cayley - Hamilton)** *Si $A \in M_n(F)$, y $p(x) \in F[x]$ es su polinomio característico, entonces $p(A) = 0$.*

Demostración. Sea $B = (b_{ij})$ la matriz adjunta de $xI - A$. Cada b_{ij} es un polinomio de grado menor o igual a $n - 1$, con coeficientes en F de la forma
$b_{ij} = c_{ij}^{(0)} + c_{ij}^{(1)}x + \cdots + c_{ij}^{(n-1)}x^{n-1}$ y sea $B^{(k)} = (c_{ij}^{(k)}) \in M_n(F)$ para $1 \leq k \leq n - 1$. Se tiene que $B = B^{(0)} + xB^{(1)} + \cdots + x^{n-1}B^{(n-1)}$, que se puede ver como elpolinomio
$B = B^{(0)} + B^{(1)}x + \cdots + B^{(n-1)}x^{n-1}$ dando el siguiente isomorfismo
$\varphi : M_n(F[x]) \to M_n(F)[x]$ dado por $\varphi(x^iA) = Ax^i$.
Por el teorema 19 tenemos que $B(xI - A) = |xI - A|I = p(x)I$.
Si $p(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$, $(B^{(0)} + xB^{(1)} + \cdots + x^{n-1}B^{(n-1)})(xI - A)$
$= B(xI - A) = |xI - A|I = p(x)I = (a_0 + xa_1 + \cdots + x^{n-1}a_{n-1} + x^n)I$
$= a_0I + (a_1x)I + \cdots + (a_{n-1}x^{n-1}I) + x^nI$, de donde se obtiene que

$$-B^{(0)}A + (B^{(0)} - B^{(1)}A)x + (B^{(1)} - B^{(2)}A)x^2 + \cdots + (B^{(n-2)} - B^{(n-1)}A)x^{n-1} + B^{(n-1)}x^n$$

$$= a_0 I + (a_1 I)x + \cdots + (a_{n-1} I)x^{n-1} + Ix^n$$

y en consecuencia

$$\begin{aligned} -B^{(0)}A &= a_0 I \\ B^{(0)} - B^{(1)}A &= a_1 I \\ B^{(1)} - B^{(2)}A &= a_2 I \\ &\vdots \\ B^{(n-2)} - B^{(n-1)}A &= a_{n-1} I \\ B^{(n-1)} &= I \end{aligned}$$

lo que implica que

$$\begin{aligned} -B^{(0)}A &= a_0 I \\ B^{(0)}A - B^{(1)}A^2 &= a_1 A \\ B^{(1)}A^2 - B^{(2)}A^3 &= a_2 A^2 \\ &\vdots \\ B^{(n-2)}A^{n-1} - B^{(n-1)}A^n &= a_{n-1} A^{n-1} \\ B^{(n-1)}A^n &= A^n \end{aligned}$$

de lo anterior tenemos que

$$\begin{aligned} p(A) &= a_0 + a_1 A + \cdots + a_{n-1}A^{n-1} + A^n \\ &= -B^{(0)}A + (B^{(0)}A - B^{(1)}A^2) + (B^{(1)}A^2 - B^{(2)}A^3) + \cdots + (B^{(n-2)}A^{n-1} - B^{(n-1)}A^n) + B^{(n-1)}A^n \\ &= (-B^{(0)}A + B^{(0)}A) + (-B^{(1)}A^2 + B^{(1)}A^2) + \cdots + (-B^{(n-1)}A^n + B^{(n-1)}A^n) = 0. \blacksquare \end{aligned}$$

Corolario 4 *El polinomio mínimo de una matriz A divide al polinomio característico de A.*

Definición 26 *Sean V un espacio vectorial sobre el campo F, T un operador lineal de V y $f(x) = a_0 + a_1 x + \cdots + a_s x^s \in F[x]$. Se define $f(T)$ como el operador lineal $a_0 I + a_1 T + a_2 T^2 + \cdots + a_s T^s$.*

Definición 27 *Con la notación del párrafo anterior, si $v \in V$ se define $f \cdot v = f(T)v$.*

Es fácil verificar que si $f, g \in F[x]$, T un operador lineal de V, $u, v \in V$ y $\alpha \in F$ se tiene que $f \cdot (u + v) = f \cdot u + f \cdot v$, $(f + g) \cdot u = f \cdot u + g \cdot u$, $(fg) \cdot u = f \cdot (g \cdot u)$ y que $\alpha(f \cdot u) = (\alpha f) \cdot u = f \cdot (\alpha u)$.

Observacion 12. Si V es un espacio vectorial sobre el campo F, T un operador lineal de V y $v \in V$, se tiene que el conjunto $Z(v;T) = \{g \cdot v | g \in F[x]\}$ es un subespacio de V. A este subespacio se le llama el $T-$subespacio cíclico de V generado por v.

Definición 28 *Sean V un espacio vectorial sobre el campo F, T un operador lineal en V y $v \in V$. Si el $T-$subespacio cíclico de V generado por v es todo V, se dice que v es un vector cíclico de T.*

Definición 29 *Si V es un espacio vectorial sobre el campo F, T un operador lineal en V y $v \in V$, al conjunto $M(v;T) := \{f \in F[x] | f \cdot v = 0\}$ se le llama el T-anulador de v.*

Lema 7 *Si V es un espacio vectorial sobre el campo F y T un operador lineal en V se tiene que*

(i) $0 \in M(v;T)$.

(ii) Si $f, g \in M(v;T)$ *entonces* $f + g \in M(v;T)$.

(iii) Si $f \in M(v;T)$ *y* $h \in F[x]$ *entonces* $hf \in M(v;T)$.

Demostración.
(i) $0 \cdot v = 0(T)v = 0$.
(ii) Como $f, g \in M(v;T)$ y $(f+g) \cdot v = f \cdot v + g \cdot v$, entonces
$(f+g) \cdot v = f \cdot v + g \cdot v = 0 + 0 = 0$ por lo tanto $f + g \in M(v;T)$.
(iii) Como $f \in M(v;T)$, $(gf)(x) = g(x)f(x)$ y $(gf) \cdot v = g(f \cdot v)$, entonces
$(gf) \cdot v = g \cdot (f \cdot v) = g \cdot 0 = 0$ por lo tanto $gf \in M(v;T)$. ■

Observacion 13. Si V es un espacio vectorial sobre el campo F de dimensión finita y $v \in V$, se tiene que $M(v;T) \neq \{0\}$, ya que el polinomio mínimo de T está en $M(v;T)$.

Definición 30 *Al polinomio mónico de grado mínimo que está en $M(v;T)$ también se le llama el T-anulador de v y se denota por p_v.*

Lema 8 *Si $M(v;T) \neq \{0\}$ y $f(x) \in M(v;T)$, se tiene que p_v divide a $f(x)$.*

Demostración. Por el algoritmo de la división se tiene que $f(x) = q(x)p_v(x) + r(x)$ con $grd(r(x)) < grd(p_v(x))$, así $0 = f \cdot v = (qp_v + r) \cdot v = q \cdot vp_v \cdot v + r \cdot v = r \cdot v$, lo que implica que $r(x) = 0$ y por lo tanto p_v divide a $f(x)$. ■

Observacion 14. $Z(v;T) = \{r \cdot v | grd(r(x)) < grd(p_v(x))\}$.
Demostración. Es suficiente probar que $Z(v;T) \subset \{r \cdot v | grd(r(x)) < grd(p_v(x))\}$. Sea $u \in Z(v;T)$, por lo cual $u = f \cdot v$ con $f(x) \in F[x]$. Por el algoritmo de la división se tiene que $f(x) = p_v(x)q(x) + r(x)$ con $q(x), r(x) \in F[x]$ y $grd(r(x)) < grd(p_v(x))$, por lo tanto $f \cdot v = qp_v \cdot v + r \cdot v = q \cdot (p \cdot v) + r \cdot v = q \cdot 0 + r \cdot v = r \cdot v$ ■

Observacion 15. Si $p_v(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k$, el conjunto $\mathscr{B} = \{v, Tv, T^2v, \ldots, T^{k-1}v\}$ es una base de $Z(v;T)$.
Demostración. Sea $u \in Z(v;T)$, $u = r \cdot v$ con $r \in F[x]$ y $s = grd(r) < k$. Si $r(x) = c_0 + c_1x + \cdots + c_sx^s$, $u = (c_0I + c_1T + \cdots + c_sT^s)v = c_0v + c_1T(v) + \ldots + c_sT^s(v)$ por lo que $\mathscr{B}$ genera a $Z(v;T)$. Si $\mathscr{B}$ fuera linealmente dependiente, existiría un polinomio r no cero de grado menor que s tal que $r \cdot v = 0$, lo que es una contradicción porque p_v es el $T-$anulador de v y es de grado s. ■

Lema 9 *$Z(v;T)$ es invariante bajo T.*

Demostración. Sea $u \in Z(v;T)$, $u = r \cdot v = a_0v + a_1T(v) + \cdots + a_{k-1}T^{k-1}(v)$, $T(u) = a_0T(v) + a_1T^2(v) + \cdots + a_{k-1}T^k(v) \in Z(v;T)$. ■
Observacion 16. Como $Z(v;T)$ es T-invariante, la restricción U de T a $Z(v;T)$ es un operador lineal de $Z(v;T)$.

Teorema 21 *Con la notación usada en los párrafos anteriores, p_v es el polinomio mínimo de U.*

Demostración. Sea $z \in Z(v;T)$, $z = r \cdot v$ y $p_v(U)z = p_v(U)(r \cdot v) = p_v(T) \cdot r \cdot v = (p_vr) \cdot v = rp_v \cdot v = r \cdot (p_vv) = 0$, lo que quiere decir que p_v anula a U. Ahora, si $0 = f(U)$, $f(U)v = f(T)v = 0$, lo que implica que p_v divide a $f(x)$, por lo tanto p_v es el polinomio minímo de U. ■

Corolario 5 *Si V es un espacio vectorial de dimensión finita sobre el campo F, T un operador lineal en V y $v \in V$ un vector cíclico de T, se tiene que el polinomio mínimo de T coincide con p_v y p_v es el polinomio característico de T.*

Demostración. Como $V = Z(v : T)$, por el teorema 21 p_v es el polinomio mínimo de T. Además, $dim(V) = grd(p_v)$ y si $p(x)$ es el polinomio caraterístico de T, $grd(p(x)) = grd(p_v)$ y por lo tanto $p(x) = p_v(x)$. ■
La propiedad anterior caracteriza a los operadores lineales sobre un espacio vectorial de dimensión finita que tienen un vector cíclico de T.

Teorema 22 *Sea T un operador lineal de un espacio vectorial V de dimensión finita sobre el campo F. Se tiene que existe $v \in V$ tal que $Z(v,T) = V$ si y sólo si el polinomio mínimo de T y el polinomio característico de T coinciden.*

Demostración. Por el corolario anterior, si V tiene un vector cíclico de T, los polinomios mínimo y característico de T coinciden. La otra implicación puede consultarse en [1].

Definición 31 *Si G es un grupo y E es un campo, un carácter de G en E es un homomorfismo $\varphi : G \to E^*$, con E^* el grupo multiplicativo de E.*

Cada carácter de un grupo G en E se puede pensar como un elemento del espacio vectorial de funciones de G en E.

Definición 32 *Se dice que un conjunto $\{\sigma_1, \ldots, \sigma_n\}$ de caracteres de un grupo G en un campo E es linealmente independiente si es linealmente independiente en el espacio de funciones de G en E.*

Lema 10 **(Lema de Dedekind).** *Todo conjunto $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ de caracteres distintos de un grupo G en un campo E es linealmente independiente.*

Demostración. Por inducción sobre n. Si $n = 1$, como σ_1 es un caracter σ_1 no es cero, así $\{\sigma_1\}$ es linealmente independiente.
Sea $n > 1$ y supongamos que

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_{n-1}\sigma_{n-1}(x) + a_n\sigma_n(x) = 0. \text{ para toda } x \in G \tag{1.1}$$

con al menos una $a_i \neq 0$. Entonces $a_1 \neq 0$, ya que de otra forma, por hipótesis de inducción, toda a_i sería igual a cero, lo que contradice que los a_i no son todos cero.
Como $\sigma_1 \neq \sigma_n$, existe $y \in G$ tal que $\sigma_1(y) \neq \sigma_n(y)$. Multiplicando la ecuación (6) por $\sigma_n(y)$ obtenemos:

$$(a_1\sigma_n(y))\sigma_1(x) + (a_2(\sigma_n(y))\sigma_2(x) + \ldots + (a_n\sigma_n(y))\sigma_n(x) = 0 \tag{1.2}$$

luego

$$a_1\sigma_n(y)\sigma_1(x) + a_2\sigma_n(y)\sigma_2(x) + \ldots + a_n\sigma_n(y)\sigma_n(x) = 0 \tag{1.3}$$

para toda $x \in G$.

Por otro lado, evaluando la ecuación (6) en xy, se obtiene:

$$a_1\sigma_1(xy) + a_2\sigma_2(xy) + \ldots + a_n\sigma_n(xy) = 0 \tag{1.4}$$

$$a_1\sigma_1(x)\sigma_1(y) + a_2\sigma_2(x)\sigma_2(y) + \ldots + a_n\sigma_n(x)\sigma_n(y) = 0 \tag{1.5}$$

Así de (8) y (10) tenemos que

$$a_1(\sigma_n(y) - \sigma_1(y))\sigma_1(x) + \ldots + a_{n-1}(\sigma_n(y) - \sigma_{n-1}(y))\sigma_{n-1}(x) = 0, \tag{1.6}$$

por inducción se tiene que $a_i(\sigma_n(y) - \sigma_i(y)) = 0$ para toda $1 \leq i \leq n-1$ en (11), en particular $a_1[\sigma_n(y) - \sigma_1(y)] = 0$, puesto que $a_1 \neq 0$ implica que $\sigma_n(y) = \sigma_1(y)$ y esto contradice que son diferentes, así todos los a_i son cero . ■

Corolario 6 *Todo conjunto $\beta = \{\sigma_1, \ldots, \sigma_n\}$ de automorfismos de un campo F diferentes, es linealmente independiente.*

Demostración. Un automorfismo de un campo F restringido al grupo multiplicativo F^* es un carácter, por lo que β es linealmente independiente. ■
Con lo anterior ya se tiene lo necesario para demostrar el teorema 1.

Teorema 1. *Sea $E = GF(p^n)$ y $F = GF(p)$, entonces existe una base normal de E sobre F.*
Demostración. Si $G = Gal(E : F)$, se tiene que $G =< \sigma >$, con σ el automorfismo de Frobenius y el orden de σ es n. Como $\sigma^n = Id$, se tiene que σ es anulado por el polinomio $f(x) = x^n - 1 \in F[x]$. Dado que Id, σ, ..., σ^{n-1} son linealmente independientes, no existe un polinomio $g(x) \in F[x]$ no cero de grado menor que n tal que $g(\sigma) = 0$, por lo que $f(x) = x^n - 1$ es el polinomio mínimo de σ sobre F.
Como el polinomio característico de σ es de grado n y es dividido por el polinomio mínimo, se tiene que $f(x) = x^n - 1$ es el polinomio característico de σ, por lo que existe $v \in F$ tal que $\beta = \{v, \sigma(v), \sigma^2(v), \ldots, \sigma^{n-1}(v)\}$ es base de E en virtud del teorema 19, lo que implica que $\beta = \{v, v^p, \ldots, v^{p^{n-1}}\}$ es una base normal de E sobre F. ■

Ahora podemos generalizar la definición de base normal y dar un corolario del teorema anterior.

Definición 33 *Si $E : F$ es una extension finita de grado n, se dice que $E : F$ tiene una base normal si existe $v \in E$ y $\varphi \in Gal(E : F)$ tal que $\{v, \varphi(v), \varphi^2(v), \ldots, \varphi^{n-1}(v)\}$ es base de E sobre F y $\varphi^n(v) = v$.*

Corolario 7 *Si E es una extensión finita de un campo finito F, existe una base normal de E sobre F.*

Demostración. Si K es el subcampo primo de F, $K < F < E$. El grado de F sobre K y el grado de E sobre K son m y n respectivamente, se tiene que el grado de E sobre F es $\frac{n}{m} = s$. $|E| = p^n$ y $|F| = p^m$ con p la característica de K.
E es campo de descomposición del polinomio separable $f(x) = x^{p^n} - x$ sobre K, por lo que $E : K$ es de Galois. El grupo de Galois de $F : K$ es un grupo cíclico de orden n. Pongamos que $G =< \varphi >$. Como $Gal(E : F) < Gal(E : K)$, $Gal(E : F)$ es cíclico y
$|Gal(E : F)| = [E : F]$ porque $[E : F]$ es de Galois y $n = [E : K] = [E : F][F : K]$, luego $Gal(E : F) =< \varphi^m >$.
El polinomio mínimo de φ^m sobre F es $h(x) = x^s - 1$, ya que $x^n - 1$ es el polinomio mínimo de φ sobre K. Como $[E : F] = s$, se tiene que $h(x)$ es también el polinomio característico de φ^m sobre F, lo que implica que $E : F$ tiene una base normal. ■

Capítulo 2

Propiedades de bases normales

Observacion 17. Si E es una extensión finita de un campo finito F, σ es el automorfismo de Frobenius de E sobre $GF(p)$, $Gal(E:F) =< \tau >$, con $\tau = \sigma^m$, y
$\mathscr{N} = \{v, \tau(v), \tau^2(v), \ldots, \tau^{l-1}(v)\}$ una base normal de E sobre F, se tiene que si

$$X = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_l \end{pmatrix}$$

es el vector de coordenadas de $w \in E$ con respecto a la base $\mathscr{N}$, el vector de coordenadas de $\tau^j(w)$ con respecto a la base $\mathscr{N}$ es

$$\begin{pmatrix} a_{l-(j-1)} \\ \vdots \\ a_l \\ a_1 \\ a_2 \\ \vdots \\ a_{l-j} \end{pmatrix}$$

$1 \leq j \leq l-1$.

Demostración. Si A es la matriz que representa a τ con respecto a la base $\mathscr{N}$ se tiene que

$$A = [\tau]_{\mathscr{N}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & & & \cdots & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ I_{l-1} & 0 \end{pmatrix}$$

por lo que

$$A^2 = [\tau^2]_{\mathscr{N}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & & & \cdots & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & I_2 \\ I_{l-2} & 0 \end{pmatrix}$$

y

$$A^j = [\tau^j]_{\mathscr{N}} = \begin{pmatrix} 0 & I_j \\ I_{l-j} & 0 \end{pmatrix} \text{ para cada } 1 \leq j \leq l-1.$$

Si $w \in E$ y X es el vector de coordenadas de w con respecto a la base $\mathscr{N}$

$$X = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{l-3} \\ a_{l-2} \\ a_{l-1} \\ a_l \end{pmatrix}.$$

por lo que

$$[\tau^j]_{\mathscr{N}}[w]_{\mathscr{N}} = A^j X = \begin{pmatrix} O & I_j \\ I_{l-j} & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{l-3} \\ a_{l-2} \\ a_{l-1} \\ a_l \end{pmatrix} = \begin{pmatrix} a_{l-(j-1)} \\ \vdots \\ a_l \\ a_1 \\ a_2 \\ \vdots \\ a_{l-j} \end{pmatrix}.\blacksquare$$

Sea $E = GF(p^n)$ una extensión de un campo F, por el corolario 8 E admite una base normal $\mathscr{N}$ de E sobre F. Si $a, b \in E$, el producto de a con b está en E y los coeficientes del vector que representa al producto de a con b se obtienen con la igualdad (5) de la introducción. Lo que se hará en esta parte es calcular el número máximo de ceros en la matriz $(d_{ij}^{(k)})$ con respecto a una base normal.

Definición 34 *Si E es un campo y G es un subconjunto no vacío del grupo de automorfismos de E, al conjunto $\{\alpha \in E | \sigma(\alpha) = \alpha$ para todo $\sigma \in G\}$ se le denota como E^G.*

Observacion 18 E^G es un subcampo de E y es conocido como el subcampo fijo por G.
Demostración. Sean $a, b \in E^G$. Se tiene que para $\sigma \in G$, $\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$, $\sigma(ab) = \sigma(a)\sigma(b) = ab$. Finalmente, si $a \in E^G$ y $\sigma \in G$,
$1 = \sigma(1) = \sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1}) = a\sigma(a^{-1})$, esto implica que $\sigma(a^{-1}) = a^{-1}$, por lo tanto E^G es un subcampo de E. ■

Lema 11 *Si $G = \{\sigma_1, \ldots, \sigma_n\}$ es un subconjunto de los automorfismos de E, se tiene que*

$$[E : E^G] \geq n.$$

Demostración. Supongamos que $[E : E^G] = r < n$; sea $\{\alpha_1, \ldots, \alpha_r\}$ una base de E sobre E^G. Consideremos el siguiente sistema de r ecuaciones lineales con n indeterminadas con coeficientes en E.

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n &= 0 \\ \sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n &= 0 \\ &\vdots \\ \sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n &= 0 \end{aligned} \tag{2.1}$$

Puesto que $r < n$, el sistema tiene una solución no trivial $(s_1, \ldots, s_n)$, por lo que

$$\begin{aligned} \sigma_1(\alpha_1)s_1 + \cdots + \sigma_n(\alpha_1)s_n &= 0 \\ \sigma_1(\alpha_2)s_1 + \cdots + \sigma_n(\alpha_2)s_n &= 0 \\ &\vdots \\ \sigma_1(\alpha_r)s_1 + \cdots + \sigma_n(\alpha_r)s_n &= 0 \end{aligned} \tag{2.2}$$

Sea $b \in E$, $b = \sum_i^r b_i\alpha_i$ con $b_i \in E^G$. Para todo $\sigma \in G$, $\sigma(b) = \sum_{i=1}^r b_i\sigma(\alpha_i)$.
De (2.3) obtenemos;

$$\begin{aligned} b_1\sigma_1(\alpha_1)s_1 + \cdots + b_1\sigma_n(\alpha_1)s_n &= 0 \\ b_2\sigma_1(\alpha_2)s_1 + \cdots + b_2\sigma_n(\alpha_2)s_n &= 0 \\ &\vdots \\ b_r\sigma_1(\alpha_r)s_1 + \cdots + b_r\sigma_n(\alpha_r)s_n &= 0 \end{aligned} \tag{2.3}$$

de donde obtenemos $s_1(b_1\sigma_1(\alpha_1) + \cdots + b_r\sigma_1(\alpha_r)) + \cdots + s_n(b_1\sigma_n(\alpha_1) + \cdots + b_r\sigma_n(\alpha_r)) = 0$, esto es, $s_1\sigma_1(b) + \cdots + s_n\sigma_n(b) = 0$, y como b es un elemento arbitrario en E, tenemos que $s_1\sigma_1 + s_2\sigma_2 + \cdots + s_n\sigma_n = 0$, lo que es una contradicción, ya que $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, en virtud del lema de Dedekind, es linealmente independiente. Por lo tanto $[E : E^G] \geq n$. ■

Teorema 23 **(Lema de Artin).** *Si $G = \{\sigma_1, \ldots, \sigma_n\}$ es un subgrupo de $Aut(E)$, se tiene que*

$$[E : E^G] = |G|.$$

Demostración. Sea $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ subgrupo de $Aut(G)$, con $\sigma_1 = Id$. Supongamos que $[E : E^G] > n$.
Sean $w_1, w_2, \ldots, w_n, w_{n+1} \in E$ linealmente independientes sobre E^G. Considerese el siguiente sistema de n ecuaciones lineales en $n+1$ indeterminadas con coeficientes en E.

$$\begin{aligned} w_1x_1 + w_2x_2 + \cdots + w_{n+1}x_{n+1} &= 0 \\ \sigma_2(w_1)x_1 + \sigma_2(w_2)x_2 + \cdots + \sigma_2(w_{n_1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(w_1)x_1 + \sigma_n(w_2)x_2 + \cdots + \sigma_n(w_{n+1})x_{n+1} &= 0 \end{aligned} \tag{2.4}$$

Sea $S = (y_1, y_2, \ldots, y_n, y_{n+1}) \in E^{n+1}$ una solución no trivial del sistema con el mínimo número de componentes no cero.
Supongamos que la última componente no cero es y_l , $R = y_l^{-1}S$ es también una solución al sistema con su componente l igual a uno, es decir $R = (y_1', y_2', \ldots, y_{l-1}', 1, 0, \ldots, 0)$; como $y_1'w_1 + y_2'w_2 + \cdots + y_{l-1}'w_{l-1} + w_l = 0$, algún $y_k \notin E^G$ para alguna $1 \leq k \leq l-1$, por lo que existe $\sigma \in G$ tal que $\sigma(y_k') \neq y_k'$.
Como R es solución del sistema (15), para cada $1 \leq j \leq n$, se tiene que
$\sigma_j(w_1)y_1' + \sigma_j(w_2)y_2' + \cdots + \sigma_j(w_{l-1})y_{l-1}' + \sigma_j(w_l) = 0$, de donde para cada $\sigma \in G$
$\sigma(\sigma_j(w_1)y_1' + \sigma_j(w_2)y_2' + \cdots + \sigma_j(w_{l-1})y_{l-1}' + \sigma_j(w_l)) = 0$ y
$(\sigma\sigma_j)(w_1)\sigma(y_1') + (\sigma\sigma_j)(w_2)\sigma(y_2') + \cdots + (\sigma\sigma_j(w_{l-1})\sigma(y_{l-1}') + (\sigma\sigma_j)(w_l) = 0$
para toda $j = 1, 2, \ldots, n$, así $(\sigma(y_1'), \sigma(y_2'), \ldots, \sigma(y_{l-1}'), 1, 0, \ldots, 0)$ es solución de (15), por lo que $T = R - (\sigma(y_1'), \sigma(y_2'), \ldots, \sigma(y_{l-1}'), 1, 0, \ldots, 0) =$
$(y_1' - \sigma(y_1'), y_2' - \sigma(y_2'), \ldots, y_l' - \sigma(y_{l-1}'), 0, 0, \ldots, 0)$ es una solución no trivial de (15) por que

$y'_k - \sigma(y'_k) \neq 0$ y tiene menos elementos no cero que R y que S, lo que es una contradicción. Por lo tanto $[E : E^G] \leq n$. ■

Teorema 24 *Las siguientes condiciones son equivalentes para una extension finita $E : F$ con grupo de Galois $G = Gal(E : F)$.*

(i) $F = E^G$.

(ii) *Todo polinomio irreducible $p(x)$ de $F[x]$ con una raíz en E es separable y todas sus raíces están en E, esto es, $p(x)$ se descompone como producto de factores lineales sobre E.*

(iii) *E es un campo de descomposición de algún polinomio separable $f(x) \in F[x]$.*

Demostración (i) implica (ii). Sean $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, $p(x) \in F[x]$ irreducible con una raíz $\alpha \in E$, $\alpha_1, \alpha_2, \ldots, \alpha_r \in E$ los diferentes elementos de la lista $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ y $g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r) \in E[x]$. Observemos que $g(x) \in E[x]$ no tiene raíces repetidas y cada coeficiente de $g(x)$ es dejado fijo por cada elemento de G, es decir, que cada coeficiente esta en $E^G = F$, por lo que $g(x) \in F[x]$.
Como G es un grupo, $\alpha \in E$ es una raíz común de $g(x)$ y $p(x)$, lo que implica que $(g(x), p(x)) \neq 1$ y como $p(x)$ es irreducible sobre $F[x]$, se tiene que $p(x)$ divide a $g(x)$, lo que implica que $p(x)$ se descompone como producto de factores lineales diferentes sobre E.
(ii) implica (iii): $E : F$ es una extensión finita, por lo que $E = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ y cada $\alpha_i \in E$ es algebraico sobre F.
Sea $p_i(x) \in F[x]$ el polinomio mínimo de α_i. Si $g(x) = p_1(x)p_2(x) \cdots p_r(x) \in F[x]$ y K es el campo de descomposición de $g(x)$ sobre F,
$K = F(\alpha_1, \alpha_2, \ldots, \alpha_r, \ldots) \subset E = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ por lo tanto $K = E$ y E resulta ser campo de descomposición de $g(x) \in F[x]$, que es separable.
(iii) implica (i). Si $G = Gal(E : F)$, $|G| = [E : F]$ por el teorema 14. Por otro lado, en virtud del lema de Artin, $|G| = [E : E^G]$; como $F \subset E^G \subset E$, se tiene que $[E : F] = [E : E^G][E^G : F]$, lo que implica que $[E^G : F] = 1$ y por lo tanto $E^G = F$. ■

Lema 12 *Sea $E : F$ una extensión finita de grado m de un campo finito F, τ un generador de $Gal(E : F)$, $G = \{1, \tau, \tau^2, \ldots, \tau^m\}$. $Tr : E \to E$ es la función tal que $Tr(v) = \sum_{i=1}^{m} \tau^i(v)$. Se tiene que $Tr(v) \in F$ para toda $v \in E$.*

Demostración. Para ver que $\sum_{i=1}^{m} \tau^i(v) \in F$ es suficiente probar que $\tau(\sum_{i=1}^{m} \tau^i(v)) = \sum_{i=1}^{m} \tau^i(v)$, pero $\tau(\sum_{i=1}^{m} \tau^i(v)) = \sum_{i=1}^{m} \tau(\tau^i(v)) = \sum_{i=1}^{m} \tau^i(v)$. ■

Definición 35 *La función anterior Tr se llama la traza de E sobre F.*

Observacion 19. Sea E una extensión normal de F, la función traza es un funcional lineal de E sobre F.

Demostración. La traza es suma de transformaciones lineales y por lo tanto es lineal. ■

En el siguiente teorema, dada una base normal, se dará una cota superior para el número máximo de ceros en la matriz D_k que aparece en (5) dada una base normal.

Teorema 25 *Sea E una extensión de grado l de un campo finito F, si $\mathscr{N}$ es una base normal de E sobre F, se tiene que el número máximo de ceros en la matriz D_k de la ecuación* (5) *que aparece en la introducción, es menor o igual a $(l-1)^2$.*

Demostración. Si $\mathscr{N}$ es una base normal de E sobre F, $\mathscr{N} = \{v, \tau(v), \tau^2(v), \ldots, \tau^{l-1}(v)\}$, para algún $v \in E$ y τ un generador de $Gal(E:F)$. En virtud de la ecuación (2) que aparece en la introducción, se tiene que $v = \beta_1, \tau(v) = \beta_2, \tau^2(v) = \beta_3, \ldots, \tau^{l-1}(v) = \beta_l$, por lo que

$$\begin{array}{lllllll} vv = & vv = & d_{11}^{(1)}v & +d_{11}^{(2)}\tau(v) & +d_{11}^{(3)}\tau^2(v) & +\ldots+d_{11}^{(l)}\tau^{l-1}(v) \\ \tau(v)v = & v\tau(v) = & d_{12}^{(1)}v & +d_{12}^{(2)}\tau(v) & +d_{12}^{(3)}\tau^2(v) & +\ldots+d_{12}^{(l)}\tau^{l-1}(v) \\ \vdots & & & & \vdots & \\ \tau^{l-1}(v)v = & v\tau^{l-1}(v) = & d_{1l}^{(1)}v & +d_{1l}^{(2)}\tau(v) & +d_{1l}^{(3)}\tau^2(v) & +\ldots+d_{1l}^{(l)}\tau^{l-1}(v) \end{array} \tag{2.5}$$

de donde se obtiene que

$$Tr(v)v = (\sum_{j=1}^{l} d_{1j}^{(1)})v + (\sum_{j=1}^{l} d_{1j}^{(2)})\tau(v) + (\sum_{j=1}^{l} d_{1j}^{(3)})\tau^2(v) + \cdots + (\sum_{j=1}^{l} d_{1j}^{(l)})\tau^{l-1}(v). \tag{2.6}$$

Como $Tr(v) \in F$ y $Tr(v) \neq 0$, porque $\mathscr{N}$ es base de E sobre F, se tiene que
$\sum_{j=1}^{l} d_{1j}^{(1)} = Tr(v)$ y $\sum_{j=1}^{l} d_{1j}^{(k)} = 0$ para toda $2 \leq k \leq l$, en (2.6).
Por otro lado, $\mathscr{B}_1 = \{vv, v\tau(v), v\tau^2(v), \ldots, v\tau^{l-1}(v)\}$ es base de E sobre F ya que $\mathscr{N}$ es base de E. En virtud de (2.5), la matriz

$$A_1 = \begin{pmatrix} d_{11}^{(1)} & d_{12}^{(1)} & d_{13}^{(1)} & \cdots & d_{1m}^{(1)} \\ d_{11}^{(2)} & d_{12}^{(2)} & d_{13}^{(2)} & \cdots & d_{1m}^{(2)} \\ d_{11}^{(3)} & d_{12}^{(3)} & d_{13}^{(3)} & \cdots & d_{1m}^{(3)} \\ \vdots & & & & \vdots \\ d_{11}^{(m)} & d_{12}^{(m)} & d_{13}^{(m)} & \cdots & d_{1m}^{(m)} \end{pmatrix}$$

es la matriz cambio de base $\mathscr{B}_1$ a la base $\mathscr{N}$. Puesto que las columnas de A_1 son linealmente independientes, ninguna es cero y al sumar las columnas de A_1 se obtiene la matriz

$$B_1 = \begin{pmatrix} \sum_{j=1}^{l} d_{1j}^{(1)} \\ \sum_{j=1}^{l} d_{1j}^{(2)} \\ \sum_{j=1}^{l} d_{1j}^{(3)} \\ \vdots \\ \sum_{j=1}^{l} d_{1j}^{(l)} \end{pmatrix} \in F^l. \tag{2.7}$$

Se observa que B_1 es el vector de coordenadas de $Tr(v)v$ con respecto a la base $\mathscr{N}$, que aparece en (2.6). De lo anterior se tiene que el número de $d_{1j}^{(1)}$ iguales a cero en $\sum_{j=1}^{l} d_{1j}^{(1)}$ es a lo más $l-1$, y en las sumas $\sum_{j=1}^{m} d_{1j}^{(2)}$, $\sum_{j=1}^{l} d_{1j}^{(3)}$, ..., $\sum_{j=1} d_{ij}^{(l)}$ es a lo mas $l-2$ ceros, lo que implica que en A_1 hay a lo más $(l-1)^2 = (l-1) + (l-1)(l-2) = (l-1)(l-1)$ ceros. Si para $0 \leq i \leq l-1$, $\mathscr{B}_{i+1} = \{\tau^i(v)v, \tau^i(v)\tau(v), \tau^i(v)\tau^2(v), \ldots, \tau^i(v)\tau^{l-1}(v)\}$, $\mathscr{B}_{i+1}$ también es base de E, y la matriz

$$A_{i+1} = \begin{pmatrix} d_{(i+1)1}^{(1)} & d_{(i+1)2}^{(1)} & d_{(i+1)3}^{(1)} & \cdots & d_{(i+1)l}^{(1)} \\ d_{(i+1)1}^{(2)} & d_{(i+1)2}^{(2)} & d_{(i+1)3}^{(2)} & \cdots & d_{(i+1)l}^{(2)} \\ d_{(i+1)1}^{(3)} & d_{(i+1)2}^{(3)} & d_{(i+1)3}^{(3)} & \cdots & d_{(i+1)l}^{(3)} \\ \vdots & & & & \vdots \\ d_{(i+1)1}^{(l)} & d_{(i+1)2}^{(l)} & d_{(i+1)3}^{(l)} & \cdots & d_{(i+1)l}^{(l)} \end{pmatrix}$$

es la matriz de cambio de base $\mathscr{B}_{i+1}$ a la base $\mathscr{N}$. Si $B_{i+1} \in F^l$ es la matriz que se obtiene de sumar las columnas de A_{i+1}, se observa en forma análoga que A_{i+1} tiene a lo mas $(l-1)^2$ entradas cero. En virtud de que $\tau^i(Tr(v)v) = Tr(v)\tau^i(v)$, A_{i+1} y A_1 tienen los mismos renglones, pero en diferente orden y el primer renglón de A_1 es el rengón $i+1$ de la matriz A_{i+1}.
Por último se obsérva que el renglón k de A_{i+1} es el renglón $i+1$ de D_k y por lo arriba mencionado, se tiene que todas las matrices D_k tienen el mismo número de entradas ceros y son a lo más $(l-1)^2$, para toda $1 \leq k \leq n$. ■

Definición 36 *Sea E una extensión de grado l de un campo finito F. Decimos que una base normal de E sobre F es óptima, si el número máximo de entradas ceros en D_k es igual a $(l-1)^2$, para toda $1 \leq k \leq l$.*

Ejemplo. Sea $E = GF(2^5)$ y $F = GF(2)$. Si consideramos a $f(x) = x^5 + x^2 + 1$, se tiene que $f(x)$ es irreducible sobre F y su campo de descomposición es E.

Sea $\alpha \in E$ una raíz de $f(x)$ y $v = \alpha^3$, se tiene que $\mathscr{N} = \{v, v^2, v^4, v^8, v^{16}\}$ es una base normal de E sobre F.

En la siguiente tabla podemos ver a los productos de los elementos de la base normal $\mathscr{N}$ expresados como combinación lineal de los elementos de $\mathscr{N}$.

v^{2^i}	v^{2^j}	v	v^2	v^4	v^8	v^{16}
v	v	0	1	0	0	0
v	v^2	0	1	1	1	0
v	v^4	1	1	1	0	1
v	v^8	1	0	1	1	1
v	v^{16}	1	1	1	0	0
v^2	v	0	1	1	1	0
v^2	v^2	0	0	1	0	0
v^2	v^4	0	0	1	1	1
v^2	v^8	1	1	1	1	0
v^2	v^{16}	1	1	0	1	1
v^4	v	1	1	1	0	1
v^4	v^2	0	0	1	1	1
v^4	v^4	0	0	0	1	0
v^4	v^8	1	0	0	1	1
v^4	v^{16}	0	1	1	1	1
v^8	v	1	0	1	1	1
v^8	v^2	1	1	1	1	0
v^8	v^4	1	0	0	1	1
v^8	v^8	0	0	0	0	1
v^8	v^{16}	1	1	0	0	1
v^{16}	v	1	1	1	0	0
v^{16}	v^2	1	1	0	1	1
v^{16}	v^4	0	1	1	1	1
v^{16}	v^8	1	1	0	0	1
v^{16}	v^{16}	1	0	0	0	0

Como podemos observar en las columnas de los productos de la tabla anterior, el número de elementos no cero de los $d_{ij}^{(k)}$ es 15.

Ejemplo. Sea α raíz de $f(x) = x^5 + x^2 + 1$, como en el ejemplo anterior y sea $v = \alpha^5$, se tiene que $\mathscr{N} = \{v, v^2, v^4, v^8, v^{16}\}$ es de nuevo una base normal de E sobre F, por la misma razón que en el ejemplo anterior.

En la siguiente tabla podemos observar los productos de los elementos de la base normal $\mathscr{N}$ expresados en términos de la misma base.

v^{2^i}	v^{2^j}	v	v^2	v^4	v^8	v^{16}
v	v	0	1	0	0	0
v	v^2	1	0	0	1	0
v	v^4	0	0	0	1	1
v	v^8	0	1	1	0	1
v	v^{16}	0	0	1	0	1
v^2	v	1	0	0	1	0
v^2	v^2	0	0	1	0	0
v^2	v^4	0	1	0	0	1
v^2	v^8	1	0	0	0	1
v^2	v^{16}	0	0	1	1	0
v^4	v	0	0	0	1	1
v^4	v^2	0	1	0	0	1
v^4	v^4	0	0	0	1	0
v^4	v^8	1	0	1	0	0
v^4	v^{16}	1	1	0	0	0
v^8	v	0	1	1	0	0
v^8	v^2	1	0	0	0	1
v^8	v^4	1	0	1	0	0
v^8	v^8	0	0	0	0	1
v^8	v^{16}	0	1	0	1	0
v^{16}	v	0	0	1	0	1
v^{16}	v^2	0	0	1	1	0
v^{16}	v^4	1	1	0	0	0
v^{16}	v^8	0	1	0	1	0
v^{16}	v^{16}	1	0	0	0	0

Se puede observar que el número de elementos no cero de los $d_{ij}^{(k)}$ es 9, es decir que la matriz D_k representada respecto a la base $\mathscr{N}$, tiene $m^2 - 2m + 1 = 16$ de los $d_{ij}^{(k)} = 0$. Por lo que es una base normal óptima de E sobre F.

Bibliografía

[1] Hoffman K. y Kunze R., *Álgebra lineal*, Prentice Hall, México, 1973.

[2] Lidl R.y Niederreiter H., *Introducction to finite fields and their applications.*, Cambridge University Press, Cambridge, 1986.

[3] Moullin R. C., Onyszchuk I. M. ,Vastone S. A. y Wilson R. M., *Optimal Normal Bases in $GF(p^n)$*, Vol. 22, Discrete Applied Mathematics, North Holland, 1988-1989, pag. 149-161.

[4] Rotman J., *Galois Theory (second edition).*, Springer., Urbana Illinois., 1998.