Universidad Nacional Autónoma de México

y

Universidad Michoacana de San Nicolás de Hidalgo

Posgrado Conjunto en Ciencias Matemáticas
UNAM-UMSNH

Bases Normales Óptimas sobre Campos Finitos

T E S I S

Que para obtener el grado de Maestro en Ciencias Matemáticas

Presenta:

Vither Franco Rojas Tarquino

Director: Doctor en Matemáticas Ernesto Vallejo Ruiz

Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México

---

Morelia, Michoacán - Febrero de 2014.

Lista de Símbolos.

$\mathbb{F}_q$	campo finito de q elementos
$\mathbb{F}_q^\star$	el grupo multiplicativo de los elementos no nulos de $\mathbb{F}_q$
$\mathbb{Q}$	el conjunto de números racionales
$\mid S \mid$	la cardinalidad (número de elementos) del conjunto finito S
$\mathcal{L}(F, K)$	el conjunto de aplicaciones K-lineales de F a K
$\varphi(a)$	la función de Euler en a
$\mathbb{Z}_n$	el anillo de enteros módulo n
$\mathbb{Z}_n^\star$	el grupo multiplicativo de las unidades del anillo $\mathbb{Z}_n$
$\overline{a}$	clase de congruencia del entero a
$\mid G \mid$	el orden del grupo finito G
$< g >$	el grupo cíclico generado por g
$Q_n(x)$	el n-ésimo polinomio ciclotómico
$K(\theta)$	la extensión de K obtenida adjuntando θ
$K^{(n)}$	el n-ésimo campo ciclotómico sobre K
$E^{(n)}$	el conjunto de las raíces n-ésimas de la unidad sobre K
$\mathrm{Tr}_{F/K}(\alpha)$	la traza de $\alpha \in F$ sobre K
$\Delta_{F/K}(\alpha_1, ..., \alpha_m)$	el discriminante de $\alpha_1, ..., \alpha_m \in F$ sobre K
$C_m(A, B)$	coordenada m del producto AB
$\mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q)$	el grupo de Galois de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$
$\{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$	grupo de Galois de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ ($\sigma_i(\alpha) = \alpha^{q^i}$ para todo $\alpha \in \mathbb{F}_{q^n}$)
$i \,\%n$	el residuo que queda de dividir i entre n
$\mathbf{C}_N$	complejidad de la base normal N.

Índice general

Resumen.

Consideremos el campo finito $\mathbb{F}_{q^n}$. Dicho campo puede verse como un espacio vectorial de dimensión n sobre $\mathbb{F}_q$, así, tiene una base formada por n elementos de $\mathbb{F}_{q^n}$. Una base de la forma $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}}\}$ con $\alpha \in \mathbb{F}_{q^n}$ se llama *base normal* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Cuando un elemento se identifica con su vector de coordenadas en esta base, su potencia q-ésima tiene el mismo vector pero rotado una posición a la derecha. La multiplicación con respecto a una base normal puede ser definida en términos de una cierta forma bilineal representada por una matriz, se define entonces la complejidad de esa base normal como el número de entradas distintas de cero en dicha matriz. Un argumento debido a Mullin *et al.* muestra que dicha matriz tiene al menos $2n-1$ entradas distintas de cero. Cuando tiene exactamente $2n-1$ entradas distintas de cero, la base normal se dice que es óptima. En esta tesina se explica y describe el escenario de las bases normales en campos finitos. Se prueba el Teorema de la Base Normal y se caracteriza a los elementos normales de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Se expone el argumento de Mullin *et al.*, se explican por un lado los criterios para construir bases normales óptimas y por otro lado su clasificación.

Las pruebas de los resultados fueron detalladas, los hechos que en las fuentes originales se dan por sentados se aislaron en lemas, los cuales fueron demostrados para conseguir pruebas claras. Se propone una formulación equivalente y alternativa al Teorema de S. Gao que permite construir bases normales óptimas y de baja complejidad, además se hacen observaciones aclaratorias en la forma de proposiciones, relativas a los objetos que participan en el enunciado de dicho Teorema.

Palabras clave: campos finitos, bases normales, complejidad de una base normal, bases normales óptimas.

Abstract.

Consider the finite field $\mathbb{F}_{q^n}$. This field can be viewed as a n-dimensional vector space over $\mathbb{F}_q$, thus, it has a basis formed by n elements of $\mathbb{F}_{q^n}$. A basis of the form $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}}\}$ with $\alpha \in \mathbb{F}_{q^n}$ is called normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. When an element is identified by its coordinate vector in this basis, its q-th power has the same vector, but shifted to the right one position. Multiplication with respect to a normal basis can be defined in terms of a certain bilinear form representated by a matrix. We define the complexity of that normal basis to be the number of nonzero entries in this matrix. An argument due to Mullin *et al.* shows that this matrix has at least $2n-1$ non zero entries. If it contains exactly $2n-1$ non zero entries, then the normal basis is said to be optimal. In this dissertation is explained and described the stage of normal bases in finite fields. Normal Bases Theorem is showed and the normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ were characterized. The argument due to Mullin *et al.* is exposed. On the one hand, the criteria for constructing optimal normal bases is analized, on the other hand the classification of all optimal normal bases is explained.

The proofs of results were detailed, the facts that are assumed true in original sources were isolated in lemas, which were shown for get clear proofs. An equivalent and alternative formulation is proposed of Theorem due S. Gao, which allows to construct optimal normal bases and low complexity normal bases. Finally, explanatory observations about the objects into the statement of this Theorem are made in the form of propositions.

Keywords: finite fields, normal bases, complexity of a normal basis, optimal normal bases.

Capítulo 1

Presentación.

1.1. Introducción.

Cada campo finito F es un espacio vectorial sobre cada uno de sus subcampos y por lo tanto tiene una base de espacio vectorial sobre cada uno de ellos. Hay varios tipos distintos de bases para campos finitos. Cada tipo de base facilita ciertos cálculos. Cuando se hace cálculos aritméticos en campos finitos, hay algunas operaciones importantes, como la adición, multiplicación, elevar a la potencia q-ésima y el cálculo de inversos multiplicativos.

Con algunas bases calcular inversos y q-potencias puede ser fácil, mientras que la multiplicación puede ser más complicada. Con otras bases, se puede calcular multiplicaciones rápidamente pagando el precio de tener cálculos de inversos y exponenciaciones más complicados.

Con las bases normales el cálculo de q-potencias es fácil, pues es equivalente a un desplazamiento cíclico de las coordenadas de un elemento en la base normal dada, mientras que la multiplicación es desde un punto de vista computacional más costosa.

En el presente trabajo nos enfocaremos en el estudio de las bases normales óptimas que son bases normales de complejidad mínima, es decir, aproximadamente hablando bases normales tales que la multiplicación puede realizarse con el menor número posible de ope-

raciones.

Comenzamos el trabajo haciendo una breve incursión hacia el escenario de las bases normales en campos finitos en general, probamos que siempre existe una base normal y damos un criterio computacionalmente aceptable para determinar si un conjunto candidato de elementos en una extensión finita es una base normal para dicha extensión. En el capítulo tres hacemos preciso el concepto de complejidad de una base normal. Probamos que hay una complejidad mínima posible la cual está relacionada con el grado de extensión del campo finito en cuestión con respecto a uno de sus subcampos. En segundo lugar probamos un resultado general que nos permite construir bases normales óptimas y bases normales de baja complejidad. Terminamos el capítulo probando que todas las bases normales óptimas pueden construirse usando dicho resultado.

1.2. Antecedentes.

El Teorema de la Base Normal (Teorema 2.2.2) fue probado inicialmente por K. Hensel en 1888. Posteriormente surgieron otras demostraciones.

En el año 2003 Cohen and Huczynska [3] dieron una prueba teórica que no requiere cálculos en computadora del llamado Teorema de la Base Normal Primitiva (Teorema 2.2.3).

El estudio de las base normales óptimas comienza con Mullin et. al. [10] donde se observan dos tipos de bases normales óptimas (Tipo I y Tipo II) y se dan criterios para construirlas. Dichas construcciones fueron generalizadas por Ash, Blake y Vanstone [2], posteriormente por Wassermann [12] y finalmente por S. Gao [5] para construir bases normales óptimas y de baja complejidad, haremos referencia a dicha construccion en el Teorema 3.2.10.

Fue S. Gao quien probó que cualquier base normal óptima de un campo finito debe ser equivalente a una base normal óptima de Tipo I o de Tipo II. Finalmente Gao y Lenstra [4] extendieron dicho resultado a cualquier extensión finita de Galois de un campo arbitrario. Presentamos una versión de éste resultado para campos finitos en el Teorema 3.3.9.

1.3. Objetivos.

Asumiremos que K, F son campos finitos con K subcampo de F.

Son tres los objetivos trazados para este trabajo:

(1) Explicar y describir el escenario de las bases normales en campos finitos. Nos enfocamos en dos aspectos:

- Probar el Teorema de la Base Normal.
- Caracterizar a los elementos normales de F sobre K.

(2) Determinar la complejidad mínima teórica de una base normal y dar criterios para construir bases normales óptimas.

(3) Clasificar todas las bases normales óptimas.

Todas las pruebas de los resultados se harán de una manera detallada, en muchos casos los hechos que son dados por sentado se aislarán en lemas previos al resultado, los cuales serán demostrados consiguiendo así una prueba clara.

Se proponen el Lema 3.2.9 y el Teorema 3.2.10 como formulaciones equivalentes al Lema 4.1.3 de [5] y Teorema 4.1.4 de [5] respectivamente.

Se harán observaciones aclaratorias en la forma de proposiciones (3.2.7 y 3.2.8) relativas a los objetos que participan en los enunciados del Lema 3.2.9 y el Teorema 3.2.10.

Capítulo 2

Bases Normales.

2.1. Introducción.

Consideremos el campo $\mathbb{F}_{q^n}$ donde n es un entero positivo y q es potencia positiva de algún primo. Se puede ver $\mathbb{F}_{q^n}$ como un espacio vectorial de dimensión n sobre $\mathbb{F}_q$, así tiene una base formada por n elementos de $\mathbb{F}_{q^n}$.

Si existe un elemento $\alpha \in \mathbb{F}_{q^n}$ tal que el conjunto $B = \{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}}\}$ es una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se dice que B es una *base normal* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y que α es un *elemento normal* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. La definición de una base normal puede verse también del modo siguiente: recordemos que el conjunto de todos los automorfismos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ (por un automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ entendemos un automorfismo de $\mathbb{F}_{q^n}$ que fija los elementos de $\mathbb{F}_q$) es $G = \{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$ donde $\sigma_i : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ esta dado por $\sigma_i(\alpha) = \alpha^{q^i}$ para todo $\alpha \in \mathbb{F}_{q^n}$, nótese que dicho conjunto, es decir G, es un grupo cíclico (bajo la composición de funciones) que esta generado por σ_1, este último se denomina *automorfismo de Frobenius* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, entonces $B = \{\sigma_0(\alpha), \sigma_1(\alpha), ..., \sigma_{n-1}(\alpha)\}$.

Por otra parte, si K es un subcampo de F, $\theta \in F$ es un elemento algebraico sobre K y $g(x)$ es el polinomio mínimo de θ sobre K ($g(x) \in K[x], g(\theta) = 0$) con grado $\deg g(x) = n$, entonces es bien sabido que

(i) $K(\theta) \cong \frac{K[x]}{(g(x))}$

(ii) La dimensión de $K(\theta)$ sobre K es n, i.e., $[K(\theta) : K] = n$

(iii) $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ es una base para $K(\theta)$ sobre K

(iv) Cada elemento de $K(\theta)$ es algebraico sobre K con grado un divisor de n.

La base dada en (iii) se llama *base polinómica*.
Las referencias que utilizaremos en este capítulo son [6] capítulo 2, sección 3 (ó [7] misma referencia) y [9] capítulo 1.

2.2. Existencia de Bases Normales.

En esta sección probaremos que toda extensión finita de un campo finito tiene una base normal, para ello recordaremos algunos hechos del algebra lineal.
Sean V un espacio vectorial de dimensión finita y $T : V \longrightarrow V$ un operador lineal, decimos que un polinomio $p(x)$ *anula* T si $p(T) = 0$. El único polinomio mónico de grado mínimo que anula T se denomina *polinomio mínimo* de T.
El *polinomio característico* de T es el determinante formal de $xI - T$. Un vector $v \in V$ es *cíclico para* T si $\{v, Tv, T^2v, ...\}$ genera V.

(AL-1) El grado del polinomio característico de T es igual a la dimensión de V.

(AL-2) El polinomio mínimo de T divide al polinomio característico de T.

(AL-3) Un operador lineal tiene un vector cíclico si y sólo si su polinomio característico es igual a su polinomio mínimo.

Lema 2.2.1 [Lema de Artin, Lema 2.33 de [6]] Sean G un grupo y F un campo. Si $\psi_1, ..., \psi_m$ son homomorfismos distintos de G en $F^\star$ y $a_1, ..., a_m$ son elementos de F, no todos cero, entonces existe $g \in G$ tal que $a_1\psi_1(g) + ... + a_m\psi_m(g) \neq 0$.

Teorema 2.2.2 [Teorema de la Base Normal, Teorema 2.35 [6]] Para cada entero positivo n, existe una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Prueba. Afirmamos que $x^n - 1$ es el polinomio mínimo del automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ $\sigma : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$. En efecto, para cada $\alpha \in \mathbb{F}_{q^n}$ se tiene

$$(\sigma^n - I)(\alpha) = \sigma^n(\alpha) - I(\alpha) = \alpha^{q^n} - \alpha = 0.$$

Por otro lado, sea $p(x)$ un polinomio no nulo de grado menor que n, digamos,

$$p(x) = a_{n-1}x^{n-1} + ... + a_1x + a_0$$

el cual produce el operador

$$p(\sigma) = a_{n-1}\sigma^{n-1} + ... + a_1\sigma + a_0I$$

donde $I, \sigma, ..., \sigma^{n-1}$ son n automorfismos distintos, luego homomorfismos de $\mathbb{F}_{q^n}^\star$ en $\mathbb{F}_{q^n}^\star$, así por el lema 2.2.1, existe $\alpha \in \mathbb{F}_{q^n}^\star$ tal que $(p(\sigma))(\alpha) \neq 0$, por tanto $p(x)$ no anula σ. Ahora bien, sea $f(x)$ el polinomio característico de σ, por (AL-1) $\deg f(x) = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, además por (AL-2) $x^n - 1 \mid f(x)$ y ambos son mónicos, luego $x^n - 1 = f(x)$ y por (AL-3) σ tiene un vector cíclico, es decir, existe $\alpha \in \mathbb{F}_{q^n}$ tal que $\{\alpha, \sigma(\alpha), ..., \sigma^{n-1}(\alpha)\}$ genera $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y por tanto $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ es una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.□

Un elemento $\alpha \in \mathbb{F}_{q^n}$ es *normal primitivo* sobre $\mathbb{F}_q$ si es normal sobre $\mathbb{F}_q$ y tiene orden multiplicativo $q^n - 1$. Una base normal generada por un elemento normal primitivo se llama *base normal primitiva*. El teorema siguiente nos dice que el elemento que genera una base normal puede elegirse primitivo.

Teorema 2.2.3 [Teorema de la Base Normal Primitiva, [3]] Para cada entero positivo n, $\mathbb{F}_{q^n}$ tiene un elemento normal primitivo sobre $\mathbb{F}_q$.

2.3. Criterios para Independencia Lineal.

En esta sección presentaremos algunos criterios que nos permitirán decidir si un subconjunto $A \subseteq \mathbb{F}_{q^n}$ es linealmente independiente sobre $\mathbb{F}_q$. Nótese que si dichos criterios son aplicados a subconjuntos de $\mathbb{F}_{q^n}$ con n elementos nos dirán si dicho conjunto es una base sobre $\mathbb{F}_q$. En lo que sigue usaremos la notación siguiente: $K = \mathbb{F}_q$ y $F = \mathbb{F}_{q^n}$.

Definición 2.3.1 Sea $\alpha \in F$, la *traza* de α sobre K es

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + ... + \alpha^{q^{n-1}}.$$

Si K es el subcampo primo de F, la traza se llamara *traza absoluta*.
La traza define una función de F a F. Veremos en lo que sigue que $\mathrm{Im}\,\mathrm{Tr}_{F/K} = K$.

Lema 2.3.2 Para cada $\alpha \in F$, $\mathrm{Tr}_{F/K}(\alpha) \in K$.

Prueba. Sea $\alpha \in F$, para probar que $\mathrm{Tr}_{F/K}(\alpha) \in K$ será suficiente mostrar que $\mathrm{Tr}_{F/K}(\alpha)$ es fijado por el automorfismo de Frobenius de F sobre K, es decir, mostraremos que $(\mathrm{Tr}_{F/K}(\alpha))^q = \mathrm{Tr}_{F/K}(\alpha)$.

$$\begin{aligned}\big(\mathrm{Tr}_{F/K}(\alpha)\big)^q &= \left(\sum_{i=0}^{n-1} \alpha^{q^i}\right)^q = \sum_{i=0}^{n-1} \alpha^{q^{i+1}} \\ &= \sum_{i=0}^{n-2} \alpha^{q^{i+1}} + \alpha^{q^n} = \sum_{i=1}^{n-1} \alpha^{q^i} + \alpha \\ &= \sum_{i=0}^{n-1} \alpha^{q^i} = \mathrm{Tr}_{F/K}(\alpha).\end{aligned}$$

Teorema 2.3.3 La función traza tiene las siguientes propiedades:

1. La función traza $\mathrm{Tr}_{F/K} : F \longrightarrow K$ es una aplicación K-lineal sobreyectiva.

2. $\mathrm{Tr}_{F/K}(\alpha) = n\alpha$, para cada $\alpha \in K$

3. $\mathrm{Tr}_{F/K}(\alpha^{q^l}) = \mathrm{Tr}_{F/K}(\alpha)$, para cada $\alpha \in F$ y para cada entero positivo l.

Prueba. (1) Es fácil ver que la función $\mathrm{Tr}_{F/K} : F \longrightarrow K$ es una aplicación K-lineal. Así, $\mathrm{Im}\,\mathrm{Tr}_{F/K}$ es un subespacio de K, pero K tiene dimensión 1 sobre K, entonces $\mathrm{Im}\,\mathrm{Tr}_{F/K} \in \{\{0\}, K\}$ así basta probar que $\mathrm{Im}\,\mathrm{Tr}_{F/K} \neq \{0\}$. Nótese que $\ker \mathrm{Tr}_{F/K}$ está formado por las raíces del polinomio $\sum_{i=0}^{n-1} x^{q^i}$ que tiene grado q^{n-1} y por tanto tiene a lo más q^{n-1} raíces distintas pero F tiene q^n elementos, así existe $\alpha \in F$ tal que $\alpha \notin \ker \mathrm{Tr}_{F/K}$, es decir, $\mathrm{Tr}_{F/K}(\alpha) \neq 0$ y en consecuencia $\mathrm{Im}\,\mathrm{Tr}_{F/K} \neq \{0\}$.

(2) Sea $\alpha \in K$, basta notar que cada elemento de $\mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q)$ fija α.

(3) Sea $\alpha \in F$, sabemos que $\mathrm{Tr}_{F/K}(\alpha) \in K$ así

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha) &= \left(\mathrm{Tr}_{F/K}(\alpha)\right)^{q^l} = \left(\sum_{i=0}^{n-1} \alpha^{q^i}\right)^{q^l} \\ &= \sum_{i=0}^{n-1} (\alpha^{q^i})^{q^l} = \sum_{i=0}^{n-1} (\alpha^{q^l})^{q^i} \\ &= \mathrm{Tr}_{F/K}(\alpha^{q^l}).\end{aligned}$$

Lema 2.3.4 Para cada $\alpha \in K$, $\mid \mathrm{Tr}^{-1}_{F/K}(\alpha) \mid = q^{n-1}$.

Prueba. Sea $\alpha \in K$, como $\mathrm{Tr}_{F/K} : F \longrightarrow K$ es sobreyectiva existe $w \in F$ tal que $\mathrm{Tr}_{F/K}(w) = \alpha$. Ahora definimos la función $h : \ker \mathrm{Tr}_{F/K} \longrightarrow \mathrm{Tr}^{-1}_{F/K}(\alpha)$ por $h(\beta) = \beta + w$ $\forall \beta \in \ker \mathrm{Tr}_{F/K}$. Afirmamos que h es una biyección. En efecto, si $\beta_1, \beta_2 \in \ker \mathrm{Tr}_{F/K}$ son tales que $h(\beta_1) = h(\beta_2)$, es decir, $\beta_1 + w = \beta_2 + w$, entonces $\beta_1 = \beta_2$. Por tanto h es inyectiva.

Por otro lado, si $u \in \mathrm{Tr}^{-1}_{F/K}(\alpha)$, entonces $\mathrm{Tr}_{F/K}(u-w) = \mathrm{Tr}_{F/K}(u) - \mathrm{Tr}_{F/K}(w) = \alpha - \alpha = 0$ por tanto existe $\beta = u - w \in \ker \mathrm{Tr}_{F/K}$ tal que $h(\beta) = u$ y por tanto h es sobreyectiva.

Ahora veamos que $\ker \mathrm{Tr}_{F/K}$ tiene q^{n-1} elementos. Dado que $\mathrm{Tr}_{F/K} : F \longrightarrow K$ es una transformación lineal sobreyectiva se tiene que $F/\ker \mathrm{Tr}_{F/K} \cong K$ como espacios vectoriales y luego como grupos, por tanto $\mid K \mid = \frac{|F|}{|\ker \mathrm{Tr}_{F/K}|}$ así $\mid \ker \mathrm{Tr}_{F/K} \mid = \frac{|F|}{|K|} = \frac{q^n}{q} = q^{n-1}$.

Teorema 2.3.5 La función $\psi : F \longrightarrow \mathcal{L}(F, K)$ definida por $\psi(\beta)(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ $\forall \beta, \alpha \in F$ es un isomorfismo de K espacios vectoriales.

Prueba. Sea $\beta \in F$, $\psi(\beta) \in \mathcal{L}(F, K)$ pues es la composición de las aplicaciones $K-$lineales: $\alpha \mapsto \beta\alpha$ y $\mathrm{Tr}_{F/K}$.

Para ver la inyectividad, sean $\beta_1, \beta_2 \in F$ con $\beta_1 \neq \beta_2$ así $\beta_1 - \beta_2 \neq 0$ y como $\mid \ker \mathrm{Tr}_{F/K} \mid = q^{n-1} < q^n = \mid F \mid$ existe $r \in F$, tal que $\mathrm{Tr}_{F/K}(r) \neq 0$, sea entonces $\alpha = (\beta_1 - \beta_2)^{-1} r$ así $\psi(\beta_1)(\alpha) - \psi(\beta_2)(\alpha) = \mathrm{Tr}_{F/K}(\beta_1\alpha) - \mathrm{Tr}_{F/K}(\beta_2\alpha) = \mathrm{Tr}_{F/K}((\beta_1 - \beta_2)\alpha) = \mathrm{Tr}_{F/K}(r) \neq 0$,

por tanto $\psi(\beta_1) \neq \psi(\beta_2)$.

La sobreyectividad se sigue de $\mid \{\psi(\beta) : \beta \in F\} \mid = \mid F \mid = q^n$ y $\mid \mathcal{L}(F,K) \mid = q^n$ esto último viene del hecho siguiente: si $s \in \mathcal{L}(F,K)$ y $\{\alpha_0, ..., \alpha_{n-1}\}$ es una base de F sobre K, entonces s esta completamente determinado por $s(\alpha_0), ..., s(\alpha_{n-1}) \in K$ y es claro que hay q^n posibilidades para s. Finalmente, ψ es $K-$lineal por que la $\mathrm{Tr}_{F/K}$ es $K-$lineal.

Definición 2.3.6 Sea $\{\alpha_1, ..., \alpha_m\} \subseteq F$. Definimos el *discriminante* de dicho conjunto como el determinante siguiente:

$$\Delta_{F/K}(\alpha_1, ..., \alpha_m) = \det \begin{pmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{pmatrix}$$

Lema 2.3.7 Si $\{\alpha_1, ..., \alpha_n\} \subseteq F$ ($[F : K] = n$, entonces $\{\alpha_1, ..., \alpha_n\}$ es una base para F sobre K si y sólo si $\Delta_{F/K}(\alpha_1, ..., \alpha_n) \neq 0$.

Prueba. $\Rightarrow$) Supongamos que $\{\alpha_1, ..., \alpha_n\}$ es una base para F sobre K. Mostraremos que $\Delta_{F/K}(\alpha_1, ..., \alpha_n) \neq 0$ mostrando que las columnas de la matriz A que aparece en la definición del discriminante son linealmente independientes. Sean $C_1, C_2, ..., C_n$ las columnas de la matriz A y supongase que $d_1C_1 + d_2C_2 + ... + d_nC_n = 0$ para ciertos $d_1, ..., d_n \in K$ así para cada $j \in \{1, ..., n\}$ tendremos

$$d_1\mathrm{Tr}_{F/K}(\alpha_j\alpha_1) + ... + d_n\mathrm{Tr}_{F/K}(\alpha_j\alpha_n) = 0$$

ahora como $\mathrm{Tr}_{F/K}$ es K-lineal tenemos

$$\mathrm{Tr}_{F/K}((d_1\alpha_1 + ... + d_n\alpha_n)\alpha_j) = 0.$$

Sea $\beta = d_1\alpha_1 + ... + d_n\alpha_n$ y sea $\alpha \in F$, entonces $\alpha = \sum_{j=1}^{n} h_j\alpha_j$ con $h_j \in K$ y

$$\mathrm{Tr}_{F/K}(\beta\alpha) = \mathrm{Tr}_{F/K}(\beta\sum_{j=1}^{n} h_j\alpha_j) = \mathrm{Tr}_{F/K}(\sum_{j=1}^{n} h_j\beta\alpha_j)$$
$$= \sum_{j=1}^{n} h_j\mathrm{Tr}_{F/K}(\beta\alpha_j) = 0.$$

Ahora bien, si $\beta \neq 0$ la aplicación $f : F \longrightarrow F$ dada por $f(\alpha) = \beta\alpha$ para todo $\alpha \in F$ es inyectiva por tanto biyectiva, así hay q^n elementos en $\ker \mathrm{Tr}_{F/K}$ lo cual es imposible por 2.3.4. Por tanto $\beta = 0$ y así $d_i = 0$ para todo $i \in \{1, ..., n\}$.
$\Leftarrow$) Supongamos que $\Delta_{F/K}(\alpha_1, ..., \alpha_n) \neq 0$ y $d_1\alpha_1 + ... + d_n\alpha_n = 0$ para ciertos $d_1, ..., d_n \in K$, entonces para cada $j \in \{1, ..., n\}$ se tiene

$$d_1\alpha_j\alpha_1 + ... + d_n\alpha_j\alpha_n = 0,$$

aplicando la traza tenemos

$$d_1\mathrm{Tr}_{F/K}(\alpha_j\alpha_1) + ... + d_n\mathrm{Tr}_{F/K}(\alpha_j\alpha_n) = 0$$

lo cual nos da la combinación $d_1C_1 + ... + d_nC_n = 0$ y como las columnas son linealmente independientes se tiene $d_1 = ... = d_n = 0$ y por tanto $\{\alpha_1, ..., \alpha_n\}$ es linealmente independiente y así una base.

Teorema 2.3.8 Sea $B = \{\alpha_1, ..., \alpha_n\} \subseteq F$ ($[F : K] = n$). B es una base para F sobre K si y sólo si

$$\det \begin{pmatrix} \alpha_1 & \cdots & \cdots & \alpha_n \\ \alpha_1^q & \cdots & \cdots & \alpha_n^q \\ \vdots & & & \vdots \\ \alpha_1^{q^{n-1}} & \cdots & \cdots & \alpha_n^{q^{n-1}} \end{pmatrix} \neq 0.$$

Prueba. Sea A la matriz dada por $A_{ij} = \alpha_j^{q^{i-1}}$ entonces

$$\begin{aligned}(A^TA)_{ij} &= \sum_{l=1}^{n}(A^T)_{il}A_{lj} = \sum_{l=1}^{n} A_{li}A_{lj} \\ &= \sum_{l=1}^{n} \alpha_i^{q^{l-1}}\alpha_j^{q^{l-1}} = \sum_{l=0}^{n-1} \alpha_i^{q^l}\alpha_j^{q^l} \\ &= \sum_{l=0}^{n-1}(\alpha_i\alpha_j)^{q^l} = \mathrm{Tr}_{F/K}(\alpha_i\alpha_j).\end{aligned}$$

Así $A^TA = D$ donde D es la matriz que aparece en la definición de discriminante, luego

$$\begin{aligned}\Delta_{F/K}(\alpha_1, ..., \alpha_n) &= \det(D) = \det(A^TA) \\ &= \det(A^T)\det(A) = (\det(A))^2.\end{aligned}$$

De donde es claro que $\Delta_{F/K}(\alpha_1, ..., \alpha_n) = 0$ si y sólo si $\det(A) = 0$, así por el Lema 2.3.7 B es una base para F sobre K si y sólo si $\det(A) \neq 0$.

Lema 2.3.9 Sea F un campo cualquiera y $a_0, a_1, ..., a_{n-1} \in F$. La matriz circulante de $n \times n$

$$c[a_0, a_1, ..., a_{n-1}] = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

es ***no*** singular si y sólo si $\text{mcd}(\sum_{i=0}^{n-1} a_i x^i, x^n - 1) = 1$.

Prueba. Sea A la matriz de $n \times n$ siguiente

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}, \text{ como } A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ \vdots \\ x_n \\ x_1 \end{pmatrix}$$

y como la columna j de AB es A por la columna j de B se sigue que $c[a_0, a_1, ..., a_{n-1}] = \sum_{i=0}^{n-1} a_i A^i = f(A)$ donde $f(x) = \sum_{i=0}^{n-1} a_i x^i \in F[x]$. Por otro lado, como el operador lineal $T : F^n \longrightarrow F^n$ dado por $T(X) = AX$ tiene como vector cíclico a e_n (n-ésimo vector de la base canónica de F^n sobre F) y

$$\det(xI - A) = \det \begin{pmatrix} x & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & -1 \\ -1 & 0 & \cdots & 0 & x \end{pmatrix} = x^n - 1.$$

(haciendo el desarrollo por cofactores a lo largo de la primera columna), el polinomio mínimo de A es $x^n - 1$.

$\Leftarrow$) Si $\text{mcd}(f(x), x^n - 1) = 1$, entonces existen $a(x)$, $b(x)$ en $F[x]$ tales que $a(x)f(x) + b(x)(x^n - 1) = 1$, así $a(A)f(A) = I_n$, luego $f(A)$ es invertible y por tanto $c[a_0, a_1, ..., a_{n-1}]$ es no singular.

$\Rightarrow$) Si $\text{mcd}(f(x), x^n - 1) = d(x) \neq 1$, entonces $\deg d(x) \geq 1$ y $f(x) = d(x)g(x)$, $x^n - 1 = d(x)h(x)$ para ciertos $g(x), h(x)$ en $F[x]$ con $h(x) \neq 0$. Ahora bien, como $n = \deg(x^n - 1) = \deg d(x) + \deg h(x) > \deg h(x)$ se tiene que $h(A) \neq 0$. Pero $d(A)h(A) = A^n - I_n = 0$ luego $d(A)$ es singular y por tanto $f(A) = d(A)g(A)$ es singular.

Observación 1 Si $\text{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q) = \{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$ e $i, j \in \{0, 1, ..., n-1\}$, entonces $\sigma_i \circ \sigma_j = \sigma_{(i+j)\,\%n}$ donde $(i+j)\,\%n$ es el resto de dividir $i+j$ entre n, además si denotamos α^{q^i} por α_i, entonces $\sigma_j(\alpha_i) = \alpha_{(i+j)\,\%n}$.

Usaremos la observación anterior y la notación allí presente en la demostración del teorema siguiente.

Teorema 2.3.10 Sea $\alpha \in \mathbb{F}_{q^n}$, α es un elemento normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si y sólo si $\text{mcd}(\alpha + \alpha^q x + ... + \alpha^{q^{n-1}} x^{n-1}, x^n - 1) = 1$.

Prueba. Por definición, α es un elemento normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si y sólo si $\{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ es una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ lo cual es equivalente por 2.3.8 a que

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_0 \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_{n-2} & \alpha_{n-1} & \alpha_0 & \cdots & \alpha_{n-3} \\ \alpha_{n-1} & \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} \end{pmatrix} \text{ sea no singular}$$

pero dicha matriz es no singular si y sólo si

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} \\ \alpha_{n-2} & \alpha_{n-1} & \alpha_0 & \cdots & \alpha_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_0 \end{pmatrix} \text{ es no singular (pues solo reordenamos las filas)}$$

lo cual ocurre si y sólo si $c[\alpha_0, \alpha_1, ..., \alpha_{n-1}]$ es no singular.

Finalmente, usando 2.3.9 vemos que $c[\alpha_0, \alpha_1, ..., \alpha_{n-1}]$ es no singular si y sólo si $\text{mcd}(\alpha_0 + \alpha_1 x + ... + \alpha_{n-1}x^{n-1}, x^n - 1) = 1$.

Observación 2 Este teorema es una herramienta importante a la hora de determinar si un elemento es normal o no. Nótese que calcular un máximo comun divisor en $F[x]$ con $F = \mathbb{F}_{q^n}$ requiere por lo general menos operaciones que calcular un determinante, como es el caso del Teorema 2.3.8.

Capítulo 3

Bases Normales Óptimas.

3.1. Complejidad de una Base Normal.

Consideremos el campo $\mathbb{F}_{q^n}$, el cual es una extensión de grado n sobre $\mathbb{F}_q$. Sea $\mathcal{B} = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Si $A, B \in \mathbb{F}_{q^n}$, entonces se expresan de modo único como combinación lineal de los elementos de $\mathcal{B}$.

$$A = \sum_{i=0}^{n-1} a_i \alpha_i \ \text{ con } a_i \in \mathbb{F}_q$$
$$B = \sum_{j=0}^{n-1} b_j \alpha_j \ \text{ con } b_j \in \mathbb{F}_q.$$

Una pregunta natural es: dado $l \in \{0, 1, ..., n-1\}$, ¿cuál es la coordenada l de $A + B$ y cuál la coordenada l de AB ?.

En el caso de la suma la respuesta es inmediata la coordenada l de $A + B$ es $a_l + b_l$. En el caso de la multiplicación la respuesta requiere algunos cálculos, veamos

$$\begin{aligned} AB &= \left(\sum_{i=0}^{n-1} a_i \alpha_i \right) \left(\sum_{j=0}^{n-1} b_j \alpha_j \right) \\ &= \sum_{i=0}^{n-1} \left(a_i \alpha_i \sum_{j=0}^{n-1} b_j \alpha_j \right) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \alpha_i \alpha_j. \end{aligned}$$

Ahora bien, $\alpha_i\alpha_j \in \mathbb{F}_{q^n}$ por tanto se puede escribir como combinación lineal de los elementos de $\mathcal{B}$, así

$$\alpha_i\alpha_j = \sum_{l=0}^{n-1} t_{ij}^{(l)}\alpha_l \quad \text{para todo } i,j \in \{0,1,...,n-1\}$$

sustituyendo se tiene:

$$\begin{aligned}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_ib_j\left(\sum_{l=0}^{n-1} t_{ij}^{(l)}\alpha_l\right) &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{l=0}^{n-1} a_ib_jt_{ij}^{(l)}\alpha_l \\ &= \sum_{l=0}^{n-1}\left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_ib_jt_{ij}^{(l)}\right)\alpha_l.\end{aligned}$$

Así vemos que la coordenada l de AB, la cual denotamos por $C_l(A,B)$, es

$$C_l(A,B) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_it_{ij}^{(l)}b_j \quad \text{y}$$
$$AB = \sum_{l=0}^{n-1} C_l(A,B)\alpha_l.$$

Nótese que para cada $l \in \{0,1,...,n-1\}$ tenemos la matriz $(t_{ij}^{(l)})$, luego podemos ver a C_l como una forma bilineal (identificando A y B con sus vectores de coordenadas) dada por $C_l(A,B) = A(t_{ij}^{(l)})B^T$.

Las referencias que utilizaremos en este capítulo son [10], [8], [5] y [6].

EL interés en las bases normales surge en parte por un método para multiplicar que Massey y Omura proponen en [8]. A continuacion enunciamos y probamos una formulación de dicho metodo.

Proposición 3.1.1 (Massey - Omura, [8]) Sea $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Si $A, B \in \mathbb{F}_{q^n}$ y $m \in \{0,1,...,n-1\}$, entonces $C_m(A,B) = C_0(\sigma_m^{-1}(A), \sigma_m^{-1}(B))$.

Prueba. Sean $A = \sum_{i=0}^{n-1} a_i\alpha_i$, $B = \sum_{j=0}^{n-1} b_j\alpha_j$, como $\sigma_m^{-1} \in \mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q)$ se tiene:

$$\begin{aligned}\sigma_m^{-1}(A)\sigma_m^{-1}(B) = \sigma_m^{-1}(AB) &= \sigma_m^{-1}(\sum_{l=0}^{n-1} C_l(A,B)\alpha_l) \\ &= \sum_{l=0}^{n-1} C_l(A,B)\sigma_m^{-1}(\alpha_l) = \sum_{l=0}^{n-1} C_l(A,B)\alpha_{(l-m)\,\%n} \\ &= C_m(A,B)\alpha_0 + ...\end{aligned}$$

Por otra parte

$$\begin{aligned}\sigma_m^{-1}(A)\sigma_m^{-1}(B) &= \sum_{l=0}^{n-1} C_l(\sigma_m^{-1}(A), \sigma_m^{-1}(B))\alpha_l \\ &= C_0(\sigma_m^{-1}(A), \sigma_m^{-1}(B))\alpha_0 + ...\end{aligned}$$

Así $C_m(A,B) = C_0(\sigma_m^{-1}(A), \sigma_m^{-1}(B))$.□

Cabe hacer algunas observaciones:

1. Sabemos que la matriz $(t_{ij}^{(0)})$ determina la forma bilineal C_0 y por la Proposición 3.1.1 C_0 determina C_m para cada $m \in \{0, 1, ..., n-1\}$.

2. Sabemos que $\mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q)$ es generado por σ_1, así, si identificamos A con su vector de coordenadas, es decir, $A = (a_0, a_1, ..., a_{n-1})$ tenemos $\sigma_1(A) = (a_{n-1}, a_0, ..., a_{n-2})$ y por tanto $\sigma_m(A)$ se obtiene rotando ciclicamente m posiciones a la derecha, las coordenadas de A y por consiguiente $\sigma_m^{-1}(A)$ se obtiene haciendo dicha rotación cíclica m posiciones a la izquierda.

A continuación probaremos que las matrices $(t_{ij}^{(0)})$, $(t_{ij}^{(1)})$, ..., $(t_{ij}^{(n-1)})$ tienen todas las mismas entradas, pero en un orden distinto. Asumimos que $\{\alpha_0, ..., \alpha_{n-1}\}$ es una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Teorema 3.1.2 Para cada $m \in \{1, ..., n-1\}$ las matrices $(t_{ij}^{(m)})$ y $(t_{ij}^{(0)})$ tienen las mismas entradas, pero acomodadas de forma distinta. En particular el número de entradas distintas de cero en cada una de las matrices $(t_{ij}^{(l)})$ es el mismo.

Prueba. Sean $i, j \in \{0, 1, ..., n-1\}$, ya vimos que $\alpha_i \alpha_j = \sum_{l=0}^{n-1} t_{ij}^{(l)} \alpha_l$ donde $t_{ij}^{(l)} \in \mathbb{F}_q$ para todo $l \in \{0, 1, ..., n-1\}$. Sea $m \in \{0, 1, ..., n-1\}$, entonces

$$\begin{aligned}
\alpha_{(i-m)\,\%n} \alpha_{(j-m)\,\%n} &= \sigma_m^{-1}(\alpha_i)\sigma_m^{-1}(\alpha_j) = \sigma_m^{-1}(\alpha_i \alpha_j) \\
&= \sum_{l=0}^{n-1} t_{ij}^{(l)} \sigma_m^{-1}(\alpha_l) = \sum_{l=0}^{n-1} t_{ij}^{(l)} \alpha_{(l-m)\,\%n} \\
&= t_{ij}^{(m)} \alpha_0 + ...
\end{aligned}$$

Por otro lado

$$\begin{aligned}
\alpha_{(i-m)\,\%n} \alpha_{(j-m)\,\%n} &= \sum_{l=0}^{n-1} t_{(i-m)\,\%n\,(j-m)\,\%n}^{(l)} \alpha_l \\
&= t_{(i-m)\,\%n\,(j-m)\,\%n}^{(0)} \alpha_0 + ...
\end{aligned}$$

Por tanto

$$t_{ij}^{(m)} = t_{(i-m)\,\%n\,(j-m)\,\%n}^{(0)}. \tag{3.1}$$

Finalmente, si $R_n = \{0, 1, ..., n-1\}$, entonces la aplicación $f : R_n \times R_n \longrightarrow R_n \times R_n$ dada por $f(i, j) = ((i-m)\,\%n, (j-m)\,\%n)$ tiene inversa $g : R_n \times R_n \longrightarrow R_n \times R_n$ dada por $g(i, j) = ((i+m)\,\%n, (j+m)\,\%n)$ por tanto es una biyección.

Definición 3.1.3 Sea $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ donde $\alpha_i = \alpha^{q^i}$ para $i \in \{0, 1, ..., n-1\}$. Definimos la *complejidad* de la base normal N, denotada por $\mathbf{C}_N$, como el número de entradas distintas de cero en la matriz $(t_{ij}^{(0)})$.

Nótese que si $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ es una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, entonces

$$\alpha \alpha_i = \alpha_0 \alpha_i = \sum_{j=0}^{n-1} t_{0i}^{(j)} \alpha_j \quad \forall i \in \{0, 1, ..., n-1\}.$$

Definimos entonces T como la matriz de tamaño $n \times n$ con entradas $T_{ij} = t_{0i}^{(j)}$. La matriz T se llamará *tabla de multiplicación* de la base normal N.

Lema 3.1.4 Con la notación del párrafo anterior.

(i) Las matrices T y $(t_{ij}^{(0)})$ tienen el mismo número de entradas distintas de cero.

(ii) $\sum_{i=0}^{n-1} T_{ij} = 0$ para cada $1 \leq j \leq n-1$ y $\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} T_{i0}$.

(iii) Las filas de T son linealmente independientes.

Prueba. (i) Si $R_n = \{0, 1, ..., n-1\}$ e $i, j \in R_n$, entonces por 3.1 se tiene $T_{ij} = t_{0i}^{(j)} = t_{(-j)\,\%n\;(i-j)\,\%n}^{(0)}$. Ahora la aplicación $f : R_n \times R_n \longrightarrow R_n \times R_n$ dada por $f(i,j) = ((-j)\,\%n, (i-j)\,\%n)$ tiene como inversa a la función $\psi : R_n \times R_n \longrightarrow R_n \times R_n$ dada por $\psi(u,v) = ((v-u)\,\%n, (-u)\,\%n)$ por tanto f es una biyección.
(ii)

$$\begin{aligned}\mathrm{Tr}(\alpha)\alpha_0 = \alpha_0\mathrm{Tr}(\alpha) = \alpha_0 \sum_{i=0}^{n-1} \alpha_i = \sum_{i=0}^{n-1} \alpha_0\alpha_i \\ = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} t_{0i}^{(j)}\alpha_j = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} t_{0i}^{(j)}\right)\alpha_j \\ = \left(\sum_{i=0}^{n-1} t_{0i}^{(0)}\right)\alpha_0 + \sum_{j=1}^{n-1}\left(\sum_{i=0}^{n-1} t_{0i}^{(j)}\right)\alpha_j.\end{aligned}$$

De donde $\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} t_{0i}^{(0)} = \sum_{i=0}^{n-1} T_{i0}$ y $0 = \sum_{i=0}^{n-1} t_{0i}^{(j)} = \sum_{i=0}^{n-1} T_{ij}$ para todo $j \in \{1, ..., n-1\}$.
(iii) Notemos que

$$\begin{pmatrix} \alpha_0\alpha_0 \\ \alpha_0\alpha_1 \\ \vdots \\ \alpha_0\alpha_{n-1} \end{pmatrix} = \begin{pmatrix} \sum_{j=0}^{n-1} t_{00}^{(j)}\ \alpha_j \\ \sum_{j=0}^{n-1} t_{01}^{(j)}\ \alpha_j \\ \vdots \\ \sum_{j=0}^{n-1} t_{0\,n-1}^{(j)}\alpha_j \end{pmatrix} = \begin{pmatrix} t_{00}^{(0)}\alpha_0 & + & t_{00}^{(1)}\alpha_1 & + & \cdots & + & t_{00}^{(n-1)}\alpha_{n-1} \\ t_{01}^{(0)}\alpha_0 & + & t_{01}^{(1)}\alpha_1 & + & \cdots & + & t_{01}^{(n-1)}\alpha_{n-1} \\ \vdots & & \vdots & & & & \vdots \\ t_{0\,n-1}^{(0)}\alpha_0 & + & t_{0\,n-1}^{(1)}\alpha_1 & + & \cdots & + & t_{0\,n-1}^{(n-1)}\alpha_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} t_{00}^{(0)} & t_{00}^{(1)} & \cdots & t_{00}^{(n-1)} \\ t_{01}^{(0)} & t_{01}^{(1)} & \cdots & t_{01}^{(n-1)} \\ \vdots & \vdots & & \vdots \\ t_{0\,n-1}^{(0)} & t_{0\,n-1}^{(1)} & \cdots & t_{0\,n-1}^{(n-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} T_{00} & T_{01} & \cdots & T_{0\,n-1} \\ T_{10} & T_{11} & \cdots & T_{1\,n-1} \\ \vdots & \vdots & & \vdots \\ T_{n-1\,0} & T_{n-1\,1} & \cdots & T_{n-1\,n-1} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}$$

Ahora como $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ es una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, se tiene que el conjunto $\{\alpha_0\alpha_0, \alpha_0\alpha_1, ..., \alpha_0\alpha_{n-1}\}$ es también una base, así sus vectores de coordenadas en la base N (que son las filas de T) también forman una base de $(\mathbb{F}_q)^n$, por tanto son linealmente

independientes.

Teorema 3.1.5 [Teorema 2.1, [10]] Para cada base normal N de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se tiene que $\mathbf{C}_N \geq 2n-1$.

Prueba. Sea N una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, por (i) del Lema 3.1.4 $\mathbf{C}_N$ puede calcularse a partir de T. Por (iii) las filas y por tanto las columnas de T son linealmente independientes, así en cada columna hay almenos una entrada distinta de cero. Por (ii) cada una de las columnas $1, 2, ..., n-1$ suma cero, luego en cada una de ellas debe haber al menos dos entradas distintas de cero habiendo en total al menos $2(n-1)+1 = 2n-1$ entradas distintas de cero.

Definición 3.1.6 Sea $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Decimos que N es una *base normal óptima* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si tiene complejidad $2n-1$.

3.2. Construcción de Bases Normales Óptimas.

Antes de presentar y probar los resultados que nos permitirán construir bases normales óptimas y algunas bases normales de baja complejidad haremos una breve incursión hacia el escenario de los polinomios y campos ciclotómicos, asi como de las raíces de la unidad sobre un campo arbitrario. La referencia principal para dicha incursión es [6] (capítulo 2, sección 4).

3.2.1. Raíces de la Unidad y Polinomios Ciclotómicos.

Definición 3.2.1 Sean n un entero positivo y K un campo. El campo de descomposición del polinomio $x^n - 1 \in K[x]$ sobre K, se denotará por $K^{(n)}$ y se llama el *n-ésimo campo ciclotómico* sobre K. Definimos $E^{(n)} = \{z \in K^{(n)} : z \text{ es raíz de } x^n - 1\}$. $E^{(n)}$ se llama el conjunto de la *raíces n-ésimas de la unidad* sobre K. Nótese que $E^{(n)} \subseteq K^{(n)} \backslash \{0\}$.

A partir de ahora y durante toda esta subsección p denotará la característica del campo de coeficientes del polinomio $x^n - 1$, es decir, $p = car(K)$ (permitimos en esta subsección que p sea cero).

Teorema 3.2.2 (i) Si $p \nmid n$, entonces $E^{(n)}$ es un grupo cíclico de orden n (con respecto a la multiplicación en $K^{(n)}$).
(ii) Si $p \mid n$, escribimos $n = p^e m$ con m, e enteros positivos y $p \nmid m$, entonces $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ y las raíces de $x^n - 1$ en $K^{(n)}$ son los m elementos de $E^{(m)}$ cada uno con multiplicidad p^e.

Definición 3.2.3 Asumimos que $p \nmid n$. Una raíz n-ésima *primitiva* de la unidad sobre K, es cualquier generador del grupo cíclico $E^{(n)}$. Hay $\varphi(n)$ de tales raíces. Si $E^{(n)} =< w >$, definimos el *n-ésimo polinomio ciclotómico* sobre K, como

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{mcd}(s,n)=1}}^{n} (x - w^s).$$

Nótese que el grado de $Q_n(x)$ es $\varphi(n)$.

Teorema 3.2.4 Si $p \nmid n$, entonces

(i) $x^n - 1 = \prod_{d|n} Q_d(x)$.

(ii) Los coeficientes de $Q_n(x)$ están todos en el subcampo primo de K. Si el subcampo primo de K es $\mathbb{Q}$, entonces los coeficientes de $Q_n(x)$ son enteros.

Teorema 3.2.5 (i) $K^{(n)}$ es una extensión algebraica simple de K.

(ii) Si $K = \mathbb{Q}$, entonces $Q_n(x)$ es irreducible sobre K y $[K^{(n)} : K] = \varphi(n)$.

(iii) Si $K = \mathbb{F}_q$ y $\bar{q} \in \mathbb{Z}_n^\star$, entonces $Q_n(x)$ se factoriza como el producto de $\frac{\varphi(n)}{d}$ polinomios en $K[x]$ todos ellos distintos, mónicos, irreducibles y de grado d, donde $d = \text{ord}(\bar{q})$ en $\mathbb{Z}_n^\star$, además $K^{(n)}$ es el campo de descomposición de cada uno de dichos factores sobre K y $[K^{(n)} : K] = d$.

Ejemplo 1 Sean r un primo distinto de p y l un entero positivo, entonces

$$Q_{r^l}(x) = 1 + \sum_{i=1}^{r-1} x^{i(r^{l-1})}$$

pues por el Teorema 3.2.4

$$Q_{r^l}(x) = \frac{x^{r^l} - 1}{Q_1(x)Q_r(x)...Q_{r^{l-1}}(x)} = \frac{x^{r^l} - 1}{x^{r^{l-1}} - 1}.$$

Finalmente como un corolario de 3.2.5 tenemos.

Teorema 3.2.6 Si $\bar{q} \in \mathbb{Z}_n^\star$, entonces $Q_n(x)$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $\text{ord}(\bar{q}) = \varphi(n)$.

3.2.2. Construcción de Bases Normales Óptimas.

Para comenzar se hará algunas observaciones (en la forma de proposiciones) relativas a los objetos que participan en el enunciado del teorema principal de esta sección.

Proposición 3.2.7 Sean n, k enteros positivos y $\mathbb{F}_q$ un campo finito. Si $nk+1$ es primo y $\bar{q} \in \mathbb{Z}_{nk+1}^\star$, entonces

1. $E^{(nk+1)} \subseteq \mathbb{F}_q^{(nk+1)} \subseteq \mathbb{F}_{q^{nk}}$.

2. $E^{(nk+1)}$ es el único subgrupo de $\mathbb{F}_{q^{nk}}^\star$ de orden $nk+1$.

3. En $E^{(nk+1)} \setminus \{1\}$ todas son raíces primitivas.

Prueba. 1) Dado que la característica de $\mathbb{F}_q$ no divide a $nk+1$ se tiene por 3.2.2 que $E^{(nk+1)} \subseteq \mathbb{F}_q^{(nk+1)}$ es un grupo cíclico de $nk+1$ elementos. Por otro lado, por 3.2.5 se tiene que $[\mathbb{F}_q^{(nk+1)} : \mathbb{F}_q] = \text{ord}(\bar{q})$ en $\mathbb{Z}_{nk+1}^\star$, así, si $d = \text{ord}(\bar{q})$, entonces $d \mid nk$, luego $\mathbb{F}_q^{(nk+1)} = \mathbb{F}_{q^d}$ es un subcampo de $\mathbb{F}_{q^{nk}}$, por tanto $E^{(nk+1)} \subseteq \mathbb{F}_q^{(nk+1)} \subseteq \mathbb{F}_{q^{nk}}$.
2) Nótese que como $nk+1$ es primo $|\mathbb{Z}_{nk+1}^\star| = nk$ así $\bar{q}^{\,nk} = \bar{1}$ de donde $q^{nk} \equiv 1 (\text{mod } nk+1)$, luego $nk+1 \mid q^{nk} - 1$, es decir, $nk+1 \mid |\mathbb{F}_{q^{nk}}^\star|$ y como $\mathbb{F}_{q^{nk}}^\star$ es cíclico, existe un único $H \leqslant \mathbb{F}_{q^{nk}}^\star$ tal que $|H| = nk+1$. Ahora bien, si $r \in H$, entonces $r^{nk+1} = 1$, así $r^{nk+1} - 1 = 0$, es decir, r es raíz de $x^{nk+1} - 1 \in \mathbb{F}_q[x]$ luego $r \in E^{(nk+1)}$, con lo que se tiene $H \subseteq E^{(nk+1)}$

y como $|H| = nk+1 = |E^{(nk+1)}|$ se tiene $H = E^{(nk+1)}$.
3) Finalmente, como $|H| = nk+1$ es primo y H es cíclico, cada uno de sus nk elementos distintos de 1 lo generan, por tanto todos los elementos de $E^{(nk+1)} \setminus \{1\}$ son raíces $(nk+1)$-ésimas primitivas de la unidad.

Proposición 3.2.8 Sean n, k enteros positivos. Si $nk+1$ es primo, entonces

1. $E^{(k)} \subseteq \mathbb{Z}_{nk+1}^{(k)} = \mathbb{Z}_{nk+1} (= \mathbb{F}_{nk+1})$.

2. $E^{(k)}$ es el único subgrupo de $\mathbb{Z}_{nk+1}^{\star}$ de orden k.

3. En $E^{(k)}$, $\varphi(k)$ son raíces primitivas.

Prueba. 1) Como $\text{car}(\mathbb{Z}_{nk+1}) = nk+1$ no divide a k, por 3.2.2 $E^{(k)}$ es un grupo cíclico de orden k, además $E^{(k)} \subseteq \mathbb{Z}_{nk+1}^{(k)}$. Por otra parte, usando 3.2.5 se tiene $[\mathbb{Z}_{nk+1}^{(k)} : \mathbb{Z}_{nk+1}] = \text{ord}(\overline{nk+1})$ en $\mathbb{Z}_k^{\star}$, es decir, $[\mathbb{Z}_{nk+1}^{(k)} : \mathbb{Z}_{nk+1}] = \text{ord}(\bar{1}) = 1$, por tanto $\mathbb{Z}_{nk+1}^{(k)} = \mathbb{Z}_{nk+1}$, así $E^{(k)} \subseteq \mathbb{Z}_{nk+1}$.
2) Como $k \mid nk$ y $nk = |\mathbb{Z}_{nk+1}^{\star}|$, entonces existe un único subgrupo cíclico $L \leqslant \mathbb{Z}_{nk+1}^{\star}$ de orden k. Ahora bien, si $s \in L$, entonces $s^k = 1$ luego $s^k - 1 = 0$, es decir, $s \in E^{(k)}$, así $L \subseteq E^{(k)}$ y como $|L| = k = |E^{(k)}|$ se tiene $L = E^{(k)}$.
3) Se sigue del hecho que $E^{(k)} = L$ tiene $\varphi(k)$ generadores.

Lema 3.2.9 Sean n, k, q enteros positivos. Si $nk+1$ es primo, $\bar{q} \in \mathbb{Z}_{nk+1}^{\star} =< g >$ donde $\bar{q} = g^h$ con $\text{mcd}(h, n) = 1$ y $\overline{\tau}$ es una raíz k-ésima primitiva de la unidad en $\mathbb{Z}_{nk+1}$, entonces cada elemento $r \in \mathbb{Z}_{nk+1}^{\star}$ puede ser escrito de modo único en la forma $r = \overline{\tau}^{\,i}\, \overline{q}^{\,j}$ con $0 \leq i \leq k-1$ y $0 \leq j \leq n-1$.

Prueba. Como $\overline{\tau} \in \mathbb{Z}_{nk+1}^{\star}$ y $\text{ord}(\overline{\tau}) = k$ se tiene que $\overline{\tau} = (g^{\frac{nk}{k}})^l$ para algún $1 \leq l \leq k$ con $\text{mcd}(l, k) = 1$. Sean $0 \leq i, s \leq k-1$ y $0 \leq j, t \leq n-1$ tales que $\overline{\tau}^{\,i}\, \overline{q}^{\,j} = \overline{\tau}^{\,s}\, \overline{q}^{\,t}$ en $\mathbb{Z}_{nk+1}^{\star}$, así $\overline{\tau}^{\,i-s} = \overline{q}^{\,t-j}$, es decir, $(g^{nl})^{i-s} = (g^h)^{t-j}$ por lo tanto

$$nl(i-s) \equiv h(t-j) (\text{mod } nk) \quad (\star)$$

así $nl(i-s) \equiv h(t-j)(\text{mod } n)$ y $nl(i-s) \equiv 0(\text{mod } n)$ de donde $h(t-j) \equiv 0(\text{mod } n)$ y como $\text{mcd}(h,n) = 1$ se tiene $(t-j) \equiv 0(\text{mod } n)$ lo cual implica que $t = j$. Sustituyendo esto último en $(\star)$ se tiene $nl(i-s) \equiv 0(\text{mod } nk)$ así $l(i-s) \equiv 0(\text{mod } k)$. Ahora, como $\text{mcd}(l,k) = 1$ concluimos que $(i-s) \equiv 0(\text{mod } k)$ lo cual implica que $i = s$ y por tanto hemos probado que si $(i,j) \neq (s,t)$, entonces $\overline{\tau}^{\,i}\,\overline{q}^{\,j} \neq \overline{\tau}^{\,s}\,\overline{q}^{\,t}$ y como hay nk de tales elementos en $\mathbb{Z}^{\star}_{nk+1}$ se sigue la conclusión del Lema.

Observaciones. Se harán tres observaciones relativas al Lema precedente y al Teorema siguiente. Asumiremos que n, k, q son enteros positivos tales que $nk+1$ es primo y $\overline{q} \in \mathbb{Z}^{\star}_{nk+1}$. Denotamos por Gen al conjunto de generadores de $\mathbb{Z}^{\star}_{nk+1}$, es decir, $Gen = \{x \mid \mathbb{Z}^{\star}_{nk+1} =< x >\}$.

OBS.1: Si existe $g \in Gen$ tal que $\overline{q} = g^h$ con $\text{mcd}(h,n) = 1$, entonces para cada $x \in Gen$ existe ℓ tal que $\overline{q} = x^{\ell}$ con $\text{mcd}(\ell, n) = 1$.

En efecto, supongamos que $g \in Gen$ tal que $\overline{q} = g^h$ con $\text{mcd}(h,n) = 1$. Sea $x \in Gen$, entonces existe ℓ tal que $\overline{q} = x^{\ell}$ y como $x \in \mathbb{Z}^{\star}_{nk+1}$, existe s tal que $x = g^s$ luego $g^h = \overline{q} = x^{\ell} = (g^s)^{\ell} = g^{s\ell}$ así $h \equiv s\ell(\text{mod } nk)$ de donde $h \equiv s\ell(\text{mod } n)$ y como $\text{mcd}(h,n) = 1$ se tiene que $\text{mcd}(s\ell, n) = 1$ lo cual implica que $\text{mcd}(\ell, n) = 1$.

OBS.2: Si $g \in Gen$, entonces los enunciados siguientes son equivalentes.

(a) Existe h tal que $\overline{q} = g^h$ y $\text{mcd}(h,n) = 1$.

(b) $\text{mcd}(\frac{nk}{o(\overline{q})}, n) = 1$, donde $o(\overline{q})$ es el orden de $\overline{q}$.

En efecto, veamos que (a)⇒(b), por hipótesis existe h tal que $\overline{q} = g^h$ y $\text{mcd}(h,n) = 1$, así $o(\overline{q}) = \frac{nk}{\text{mcd}(h,nk)}$, luego $\text{mcd}(\frac{nk}{o(\overline{q})}, n) = \text{mcd}(\text{mcd}(h,nk), n) = \text{mcd}(h, \text{mcd}(nk,n)) = \text{mcd}(h,n) = 1$.

(b)⇒(a) Como $g \in Gen$, existe h tal que $\overline{q} = g^h$, así $o(\overline{q}) = \frac{nk}{\text{mcd}(h,nk)}$, luego $1 = \text{mcd}(\frac{nk}{o(\overline{q})}, n) = \text{mcd}(\text{mcd}(h,nk), n) = \text{mcd}(h, \text{mcd}(nk,n)) = \text{mcd}(h,n)$.

OBS.3: De (OBS.1) es claro que no puede ocurrir que el logaritmo de $\overline{q}$ con respecto a un generador sea coprimo a n y su logaritmo con respecto a otro generador no lo sea.

De (OBS.2) se sigue que el Lema 3.2.9 y el Teorema 3.2.10 que se han propuesto son equivalentes al Lema 4.1.3 de [5] y Teorema 4.1.4 de [5] respectivamente.

Teorema 3.2.10 Sean n, k enteros positivos y $q = p^l$ con p primo y l entero positivo. Si $nk+1$ es primo, $\bar{q} \in \mathbb{Z}^{\star}_{nk+1} =< g >$ donde $\bar{q} = g^h$ con $\text{mcd}(h, n) = 1$ y $\overline{\tau}$ es una raíz k-ésima primitiva de la unidad en $\mathbb{Z}_{nk+1}$ y β es una raíz $(nk+1)$-ésima primitiva de la unidad en $\mathbb{F}_{q^{nk}}$, entonces $\alpha = \sum_{i=0}^{k-1} \beta^{\tau^i}$ genera una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ con complejidad a lo más $(k+1)n - k$ si $p \nmid k$ y a lo más $kn - 1$ si $p \mid k$.

Prueba. (1) En primer lugar probaremos que $\alpha \in \mathbb{F}_{q^n}$. Como $\overline{q} \in \mathbb{Z}^{\star}_{nk+1}$, entonces $(\overline{q})^{nk} = \bar{1}$, así $((\overline{q})^n)^k - \bar{1} = \bar{0}$, por tanto $\overline{q}^n$ es una raíz k-ésima de la unidad en $\mathbb{Z}_{nk+1}$, luego $\overline{q}^n = \overline{\tau}^s$ para algún $0 \leq s \leq k-1$, es decir, $q^n \equiv \tau^s (\text{mod } nk+1)$. Así $\beta^{q^n} = \beta^{\tau^s}$ $(\star)$.
Por otra parte, para cada $i \in \{0, 1, ..., k-1\}$ se tiene $(s+i) \equiv (s+i)\,\%k (\text{mod } k)$, así $\overline{\tau}^{s+i} = \overline{\tau}^{(s+i)\,\%k}$ en $\mathbb{Z}_{nk+1}$, luego $\tau^{s+i} \equiv \tau^{(s+i)\,\%k} (\text{mod } nk+1)$ de donde $\beta^{\tau^{s+i}} = \beta^{\tau^{(s+i)\,\%k}}$ $(\star\star)$.
También nótese que si $R_k = \{0, 1, ..., k-1\}$, la función $f : R_k \longrightarrow R_k$ dada por $f(i) = (i+s)\,\%k$ es una permutación de R_k, luego

$$\sum_{i=0}^{k-1} \beta^{\tau^i} = \sum_{i=0}^{k-1} \beta^{\tau^{f(i)}} = \sum_{i=0}^{k-1} \beta^{\tau^{(i+s)\,\%k}} \quad (\star\star\star).$$

Finalmente aplicando $(\star)$, $(\star\star)$ y $(\star\star\star)$ se tiene

$$\begin{aligned} \alpha^{q^n} &= (\sum_{i=0}^{k-1} \beta^{\tau^i})^{q^n} = \sum_{i=0}^{k-1} (\beta^{q^n})^{\tau^i} \\ &= \sum_{i=0}^{k-1} \beta^{\tau^s \tau^i} = \sum_{i=0}^{k-1} \beta^{\tau^{(s+i)\,\%k}} = \alpha. \end{aligned}$$

(2) En segundo lugar probaremos que $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ es linealmente independiente sobre $\mathbb{F}_q$.
Sean $\lambda_0, \lambda_1, ..., \lambda_{n-1}$ en $\mathbb{F}_q$ tales que $\sum_{i=0}^{n-1} \lambda_i \alpha^{q^i} = 0$, entonces $0 = \sum_{i=0}^{n-1} \lambda_i (\sum_{j=0}^{k-1} \beta^{\tau^j q^i}) = \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} \lambda_i \beta^{\tau^j q^i} = \bigstar$.
Ahora, por el lema anterior $\mathbb{Z}^{\star}_{nk+1} = \{\overline{1}, \overline{2}, ..., \overline{nk}\} = \{\overline{\tau^j q^i} \mid 0 \leq j \leq k-1, 0 \leq i \leq n-1\}$, luego para cada $\delta \in \{1, ..., nk\}$, $\delta \equiv \tau^j q^i (\text{mod } nk+1)$ para exactamente un par $(j, i) \in \{0, 1, ..., k-1\} \times \{0, 1, ..., n-1\}$ así $\beta^{\delta} = \beta^{\tau^j q^i}$, por tanto
$\bigstar = \sum_{\delta=1}^{nk} u_\delta \beta^{\delta} = \sum_{\delta=0}^{nk-1} u_{\delta+1} \beta^{\delta} \beta = \beta (\sum_{\delta=0}^{nk-1} u_{\delta+1} \beta^{\delta})$.
Sea $f(x) = \sum_{\delta=0}^{nk-1} u_{\delta+1} x^{\delta} \in \mathbb{F}_q[x]$, (nótese que β es una raíz de $f(x)$). Sea $1 \leq r \leq nk$ fijo,

entonces nuevamente por el Lema anterior $r \equiv \tau^v q^w (\text{mod } nk+1)$ por tanto $\beta^r = \beta^{\tau^v q^w}$. Ahora bien, como $xf(x) = \sum_{\delta=1}^{nk} u_\delta x^\delta$ se tiene

$$\begin{aligned}
\beta^r f(\beta^r) &= \sum_{\delta=1}^{nk} u_\delta (\beta^r)^\delta = \sum_{i=0}^{n-1} \lambda_i (\sum_{j=0}^{k-1} (\beta^r)^{\tau^j q^i} \\
&= \sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} (\beta^{\tau^v q^w})^{\tau^j q^i} \right) = \sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} \beta^{\tau^{(v+j)\,\%k} q^i q^w} \right) \\
&= \sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} \beta^{\tau^{(v+j)\,\%k} q^i} \right)^{q^w} = \left(\sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^{(v+j)\,\%k} q^i} \right)^{q^w} \\
&= \left(\sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} \beta^{\tau^{(v+j)\,\%k}} \right)^{q^i} \right)^{q^w} = \left(\sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} \right)^{q^w} = 0.
\end{aligned}$$

Por tanto, para cada $r \in \{1, ..., nk\}$, β^r es raíz de $f(x)$ que tiene grado a lo más $nk-1$, luego $f(x) \neq 0$ no es posible, así $f(x) = 0$ de donde $u_{\delta+1} = 0 \ \forall \delta \in \{0, 1, ..., nk-1\}$, lo cual implica que $\lambda_0 = ... = \lambda_{n-1} = 0$.

(3) Finalmente calculamos la complejidad de esta base. Sea $0 \leq i \leq n-1$.

$$\begin{aligned}
\alpha \alpha^{q^i} &= \left(\sum_{j=0}^{k-1} \beta^{\tau^j} \right) \left(\sum_{l=0}^{k-1} \beta^{\tau^l} \right)^{q^i} = \sum_{j=0}^{k-1} \left(\beta^{\tau^j} \left(\sum_{l=0}^{k-1} \beta^{\tau^l} \right)^{q^i} \right) \\
&= \sum_{j=0}^{k-1} \left(\beta^{\tau^j} \left(\sum_{s=0}^{k-1} \beta^{\tau^{j+s}} \right)^{q^i} \right) = \sum_{j=0}^{k-1} \sum_{s=0}^{k-1} \beta^{\tau^j} \beta^{\tau^{j+s} q^i} \\
&= \sum_{j=0}^{k-1} \sum_{s=0}^{k-1} \beta^{\tau^j (1+\tau^s q^i)} = \sum_{s=0}^{k-1} \left(\sum_{j=0}^{k-1} \beta^{\tau^j (1+\tau^s q^i)} \right).
\end{aligned}$$

Por el Lema anterior existe un único par (s_0, i_0) con $0 \leq s_0 \leq k-1$ y $0 \leq i_0 \leq n-1$ tal que $\tau^{s_0} q^{i_0} \equiv nk (\text{mod } nk+1)$ y como $nk \equiv -1 (\text{mod } nk+1)$ se tiene $1+\tau^{s_0} q^{i_0} \equiv 0 (\text{mod } nk+1)$. Sea $(s, i) \in \{0, 1, ..., k-1\} \times \{0, 1, ..., n-1\}$.

► Si $(s, i) \neq (s_0, i_0)$, entonces $\overline{1+\tau^s q^i} \in \mathbb{Z}_{nk+1}^\star$, luego existen w, l tales que $1 + \tau^s q^i \equiv$

$\tau^w q^l (\text{mod } nk+1)$. Así

$$\sum_{j=0}^{k-1} \beta^{\tau^j(1+\tau^s q^i)} = \sum_{j=0}^{k-1} \beta^{\tau^j \tau^w q^l} = \left(\sum_{j=0}^{k-1} \beta^{\tau^{j+w}} \right)^{q^l}$$
$$= \left(\sum_{j=0}^{k-1} \beta^{\tau^j} \right)^{q^l} = \alpha^{q^l}.$$

► Si $(s,i) = (s_0, i_0)$, entonces $\sum_{j=0}^{k-1} \beta^{\tau^j(1+\tau^{s_0} q^{i_0})} = k$ ($k = 0$ si $p \mid k$).

Así, para todo $i \neq i_0$ se tiene que $\alpha\alpha^{q^i}$ es una suma de a lo más k elementos de la base, por tanto la complejidad de la base es a lo más $(n-1)k + n = n(k+1) - k$, si $p \nmid k$.
Si $p \mid k$, entonces también se tiene en el caso de $i \neq i_0$ a lo más $(n-1)k$ elementos del campo base en las filas distintas de i_0, pero si $i = i_0$, $\alpha\alpha^{q^i}$ será a lo más una suma de $k-1$ elementos de la base, habiendo en total a lo más $(n-1)k + k - 1 = nk - 1$.
Los dos corolarios que siguen se corresponden con las construcciones de bases normales óptimas descubiertas por Mullin *et al.* [10].

Corolario 3.2.11 Sean n un entero positivo, $q = p^\ell$ con p primo y ℓ entero positivo. Si $n+1$ es primo con $\mathbb{Z}_{n+1}^\star =< \overline{q} >$ y β es una raíz $(n+1)$-ésima primitiva de la unidad en $\mathbb{F}_{q^n}$, entonces β genera una base normal óptima de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Prueba. Hágase $k = 1$, en el Teorema 3.2.10 y use el Teorema 3.1.5.

Definición 3.2.12 Sea r un primo y $\mathcal{R}_r = \{x^2 \mid x \in \mathbb{Z}_r^\star\}$. Se llama *residuo cuadrático* modulo r a cualquier elemento de $\mathcal{R}_r$.

Observación. Sea n un entero positivo. Se sigue inmediatamente de la definición que, si $2n+1$ es primo y $\mathbb{Z}_{2n+1}^\star =< g >$, entonces $\mathcal{R}_{2n+1} = \{g^{2\ell} \mid 0 \leq \ell \leq n-1\}$ y por tanto $\mathcal{R}_{2n+1}$ es un subgrupo de $\mathbb{Z}_{2n+1}^\star$ de orden n.
Para otras propiedades de los residuos cuadráticos puede verse [1]. Usaremos la observación anterior en la prueba del corolario siguiente.

Corolario 3.2.13 Sea n un entero positivo. Si $2n+1$ es primo y se verifica una de las dos condiciones siguientes:

(1) $\mathbb{Z}^{\star}_{2n+1} =< \overline{2} >$ o

(2) $2n+1 \equiv 3(mod\, 4)$ y $\overline{2}$ genera a los residuos cuadráticos en $\mathbb{Z}_{2n+1}$

y β es una raíz $(2n+1)$-ésima primitiva de la unidad en $\mathbb{F}_{2^{2n}}$, entonces $\alpha = \beta + \beta^{-1}$ genera una base normal óptima de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_2$.

Prueba. Haciendo $k = 2$, $q = 2$ en el Teorema 3.2.10 se obtiene el enunciado siguiente:
"Si $2n+1$ es primo, $\overline{2} \in \mathbb{Z}^{\star}_{2n+1} =< g >$ donde $\overline{2} = g^h$ con $\text{mcd}(h, n) = 1$ y β es una raíz $(2n+1)$-ésima primitiva de la unidad en $\mathbb{F}_{2^{2n}}$, entonces $\alpha = \beta + \beta^{-1}$ genera una base normal óptima de $\mathbb{F}_{2^n}$ sobre $\mathbb{F}_2$."
Así basta probar que existe un generador g tal que $\overline{2} = g^h$ con $\text{mcd}(h, n) = 1$.
Si ocurre (1), entonces existen $g = \overline{2}$ y $h = 1$ tal que $\text{mcd}(h, n) = 1$. Por otra parte, si $2n+1 \equiv 3(mod\, 4)$, entonces n es impar y como $\overline{2}$ genera a los residuos cuadráticos, se sigue que $\overline{2}$ tiene orden n luego si g es cualqier generador, se tiene $\overline{2} = (g^{\frac{2n}{n}})^{\ell}$ para algún entero positivo ℓ con $\text{mcd}(\ell, n) = 1$, así existe $h = 2\ell$ y como $\text{mcd}(2, n) = 1$ se tiene $\text{mcd}(h, n) = 1$.

Definición 3.2.14 Las bases normales óptimas que se construyen usando el Corolario 3.2.11 se llaman bases normales óptimas de Tipo I y las que se construyen usando el Corolario 3.2.13 se llaman bases normales óptimas de Tipo II.

3.3. Determinación de Todas las Bases Normales Óptimas.

En esta sección probaremos que toda base normal óptima de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ es equivalente (en un sentido que se explicará en breve) a una base normal óptima de Tipo I o Tipo II, es decir, a una base normal óptima que se construye usando ya sea el Corolario 3.2.11 o el Corolario 3.2.13.
Comenzaremos con algunos resultados preliminares.

Definición 3.3.1 Sean $\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ y $\mathcal{C} = \{\beta_1, \beta_2, ..., \beta_n\}$ bases de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Decimos que $\mathcal{C}$ es una *base dual* de $\mathcal{B}$ si $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i\beta_j) = \delta_{ij}$ para todo $i, j \in \{1, ..., n\}$.

Sea $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, con $\alpha_i = \alpha^{q^i}$ para cada $i \in \{0, 1, ..., n-1\}$ y $\alpha \in \mathbb{F}_{q^n}$. Sea

$$\alpha\alpha_i = \sum_{j=0}^{n-1} T_{ij}\alpha_j \quad \text{para } i \in \{0, 1, ..., n-1\},\ T_{ij} \in \mathbb{F}_q. \tag{3.2}$$

Es sabido, que a cada base normal le corresponde una única base dual la cual es también normal (Teorema 2.2.7 de [5]). Sea $M = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$ con $\beta_i = \beta^{q^i}$ para cada $i \in \{0, 1, ..., n-1\}$ la base dual de N y sea

$$\alpha\beta_i = \sum_{j=0}^{n-1} D_{ij}\beta_j \quad \text{para } i \in \{0, 1, ..., n-1\},\ D_{ij} \in \mathbb{F}_q.$$

Sean $T = (T_{ij})$ y $D = (D_{ij})$. Afirmamos que

(i) D es la transpuesta de T.

(ii) Para todo $i, j \in \{0, 1, ..., n-1\}$ se tiene $T_{ij} = T_{(-i)\,\%n\,(j-i)\,\%n}$ y

$$D_{ij} = D_{(i-j)\,\%n\,(-j)\,\%n} \tag{3.3}$$

(i) En efecto, sea $k \in \{0, 1, ..., n-1\}$ y considerando la Traza de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se tiene

$$\begin{aligned}\mathrm{Tr}(\alpha\alpha_i\beta_k) = \mathrm{Tr}((\alpha\alpha_i)\beta_k) &= \mathrm{Tr}(\sum_{j=0}^{n-1} T_{ij}\alpha_j\beta_k) \\ &= \sum_{j=0}^{n-1} T_{ij}\mathrm{Tr}(\alpha_j\beta_k) = \sum_{j=0}^{n-1} T_{ij}\delta_{jk} = T_{ik}.\end{aligned}$$

$$\begin{aligned}\mathrm{Tr}(\alpha\alpha_i\beta_k) = \mathrm{Tr}((\alpha\beta_k)\alpha_i) &= \mathrm{Tr}(\sum_{j=0}^{n-1} D_{kj}\beta_j\alpha_i) \\ &= \sum_{j=0}^{n-1} D_{kj}\mathrm{Tr}(\alpha_i\beta_j) = \sum_{j=0}^{n-1} D_{kj}\delta_{ij} = D_{ki}.\end{aligned}$$

Es decir $T_{ik} = D_{ki}$.

(ii) Sean $\mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q) = \{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$ e $i \in \{0, 1, ..., n-1\}$ aplicamos σ_i^{-1} a (3.2) teniendo en cuenta que $\sigma_i^{-1} = \sigma_{(-i)\,\%n}$

$$\sigma_i^{-1}(\alpha\alpha_i) = \sigma_i^{-1}(\alpha)\sigma_i^{-1}(\alpha_i) = \alpha_{(-i)\,\%n}\alpha = \alpha\alpha_{(-i)\,\%n} \text{ y}$$

$$\sigma_i^{-1}(\sum_{j=0}^{n-1} T_{ij}\alpha_j) = \sum_{j=0}^{n-1} T_{ij}\sigma_i^{-1}(\alpha_j) = \sum_{j=0}^{n-1} T_{ij}\alpha_{(j-i)\,\%n}$$

Así
$$\alpha\alpha_{(-i)\,\%n} = \sum_{j=0}^{n-1} T_{ij}\alpha_{(j-i)\,\%n} \tag{3.4}$$

pero
$$\alpha\alpha_{(-i)\,\%n} = \sum_{\ell=0}^{n-1} T_{(-i)\,\%n\;\ell}\alpha_\ell \tag{3.5}$$

El sumando j de 3.4 es $T_{ij}\alpha_{(j-i)\,\%n}$ y el sumando correspondiente a $\ell = (j-i)\,\%n$ en 3.5 es $T_{(-i)\,\%n\;(j-i)\,\%n}\alpha_{(j-i)\,\%n}$. Por tanto

$$T_{ij} = T_{(-i)\,\%n\;(j-i)\,\%n}.$$

Así $D_{ij} = T_{ji} = T_{(-j)\,\%n\;(i-j)\,\%n} = D_{(i-j)\,\%n\;(-j)\,\%n}$.

Lema 3.3.2 Sea $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

1. Para cada $b \in \mathbb{F}_q^\star$, $bN := \{b\alpha, b\alpha^q, ..., b\alpha^{q^{n-1}}\}$ es una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ generada por $\beta = b\alpha$ y tal que $\mathbf{C}_N = \mathbf{C}_{bN}$.

2. Si $M = \{\beta, \beta^q, ..., \beta^{q^{n-1}}\}$ es la base dual (normal) de N, entonces $\mathrm{Tr}(\alpha)\mathrm{Tr}(\beta) = 1$, donde $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

3. Si $G = \{1\} \cup N$ y para cada $x \in G$ se tiene que $\alpha x \in G$, entonces $G \leqslant \mathbb{F}_{q^n}^\star$.

Prueba. (1) Sea $b \in \mathbb{F}_q^\star$, como N es una base, claramente bN es una base. Sea $\mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q) = \{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$, entonces

$$\begin{aligned} bN &= \{b\sigma_0(\alpha), b\sigma_1(\alpha), ..., b\sigma_{n-1}(\alpha)\} \\ &= \{\sigma_0(b\alpha), \sigma_1(b\alpha), ..., \sigma_{n-1}(b\alpha)\} \\ &= \{\sigma_0(\beta), \sigma_1(\beta), ..., \sigma_{n-1}(\beta)\} \text{ con } \beta = b\alpha. \end{aligned}$$

Por tanto, bN es una base normal generada por β. Por otro lado $\beta^{q^i} = \sigma_i(\beta) = \sigma_i(b\alpha) = b\sigma_i(\alpha) = b\alpha^{q^i}$ para cada $i \in \{0, 1, ..., n-1\}$. Así

$$\begin{aligned} \beta\beta^{q^i} &= (b\alpha)(b\alpha^{q^i}) = b^2(\alpha\alpha^{q^i}) = b^2\sum_{j=0}^{n-1} T_{ij}\alpha^{q^j} \\ &= \sum_{j=0}^{n-1}(bT_{ij})(b\alpha^{q^j}) = \sum_{j=0}^{n-1}(bT_{ij})\beta^{q^j} \qquad 0 \leqslant i \leqslant n-1. \end{aligned}$$

Luego si S es ta tabla de multiplicación de la base bN y T la tabla correspondiente a N se tiene $S = bT$ de donde $\mathbf{C}_N = \mathbf{C}_{bN}$.

(2) Usaremos que Tr es $\mathbb{F}_q$-lineal.

$$\begin{aligned}\mathrm{Tr}(\alpha)\mathrm{Tr}(\beta) &= \mathrm{Tr}(\beta)\mathrm{Tr}(\alpha) = \mathrm{Tr}(\mathrm{Tr}(\beta)\alpha)\\ &= \mathrm{Tr}(\alpha\sum_{i=0}^{n-1}\beta^{q^i}) = \mathrm{Tr}(\sum_{i=0}^{n-1}\alpha_0\beta_i)\\ &= \sum_{i=0}^{n-1}\mathrm{Tr}(\alpha_0\beta_i) = \sum_{i=0}^{n-1}\delta_{0\,i} = 1.\end{aligned}$$

(3) Si $x \in G$ y $\ell \in \{0, 1, ..., n-1\}$, entonces $\sigma_\ell(x) \in G$. En efecto, como $x \in G$ se tiene $x = 1$ o $x = \alpha_i$ para algún $i \in \{0, 1, ..., n-1\}$. Si $x = 1$, entonces $\sigma_\ell(x) = \sigma_\ell(1) = 1 \in G$. Si $x = \alpha_i$, entonces $\sigma_\ell(x) = \sigma_\ell(\alpha_i) = \alpha_{(i+\ell)\,\%n} \in G$. Ahora bien, sean $u, v \in G$. Tenemos dos casos:

Caso 1. $u = 1$ o $v = 1$. En este caso uv es o bien u, o bien v, así $uv \in G$.

Caso 2. $u \neq 1$ y $v \neq 1$. En este caso, $u = \alpha_i$ y $v = \alpha_j$ para ciertos $i, j \in \{0, 1, ..., n-1\}$ así $uv = \alpha_i\alpha_j = \sigma_i(\alpha)\sigma_i(\sigma_i^{-1}(\alpha_j)) = \sigma_i(\alpha\sigma_i^{-1}(\alpha_j)) = \sigma_i(\alpha\alpha_{(j-i)\,\%n}) \in G$.

Definición 3.3.3 Sean N y M bases normales de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Diremos que N y M son *equivalentes* si existe $a \in \mathbb{F}_q^\star$ tal que $M = aN$.

Observación 3 Se sigue del Lema 3.3.2 que todas las bases normales equivalentes tienen la misma complejidad.

Lema 3.3.4 Toda base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ es equivalente a una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ generada por un elemento de traza igual a -1.

Prueba. Sea N una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ generada por $\alpha \in \mathbb{F}_{q^n}$. Así $\mathrm{Tr}(\alpha) \neq 0$ (pues N es linealmente independiente) luego $b = \mathrm{Tr}(\alpha) \in \mathbb{F}_q^\star$, de donde por 3.3.2 $M = (-1)b^{-1}N$ es una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ generada por $\beta = (-1)b^{-1}\alpha$, además
$\mathrm{Tr}(\beta) = (-1)b^{-1}\mathrm{Tr}(\alpha) = -1$.

Lema 3.3.5 Sean $p(x) \in \mathbb{F}_q[x]$ y $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Si α es una raíz de $p(x)$, entonces $\prod_{i=0}^{n-1}(x - \alpha^{q^i}) \mid p(x)$.

Prueba. Sean $\mathrm{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q) = \{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$ y $\ell \in \{0, 1, ..., n-1\}$. Por hipótesis, $0 = p(\alpha)$, así $0 = \sigma_\ell(p(\alpha)) = p(\sigma_\ell(\alpha))$, es decir, $\sigma_\ell(\alpha)$ es también una raíz de $p(x)$, por tanto cada elemento de N es una raíz de $p(x)$, de donde concluimos que $\prod_{i=0}^{n-1}(x - \alpha^{q^i}) \mid p(x)$.

Lema 3.3.6 Sea $f(x) = 1 + x + ... + x^n \in \mathbb{F}_q[x]$. Si $f(x)$ es irreducible en $\mathbb{F}_q[x]$, entonces $n+1$ es primo.

Prueba. Sea $p = \mathrm{car}(\mathbb{F}_q)$.

Paso 1: Si $p \nmid n+1$ y $n+1$ es compuesto. entonces $f(x)$ es reducible.

En efecto, como $n+1$ es compuesto existe un primo $r \neq p$ con $1 < r < n+1$ tal que $r \mid n+1$ y como $\prod_{d|n+1} Q_d(x) = x^{n+1} - 1 = (x-1)(1 + x + ... + x^n)$ se tiene $Q_r(x)Q_1(x) \mid (x-1)(1+x+...+x^n)$ de donde $Q_r(x) \mid (1+x+...+x^n)$ con $1 \leq \deg(Q_r(x)) = r - 1 < n$, por tanto $f(x)$ es reducible.

Paso 2: Si $p \mid n+1$ y $n > 1$, entonces $f(x)$ es reducible.

En efecto, como $p \mid n+1$, entonces $n+1 = pt$ para algún t entero positivo. Por otro lado

$$f(x) = 1 + x + ... + x^n = \frac{x^{n+1} - 1}{x - 1} = \frac{(x^t)^p - 1^p}{x - 1}$$
$$= \frac{(x^t - 1)^p}{x - 1} = (x-1)^{p-1}(1 + x + ... + x^{t-1})^p.$$

Ahora bien, como $n > 1$ se tiene $pt = n + 1 > 2$. Si $p = 2$ y $t = 1$, entonces $pt = 2$ es una contradicción, así $p > 2$ o $t > 1$.

Si $p > 2$, entonces $p - 1 \geq 2$ luego $(x-1)^2 \mid f(x)$, así $f(x)$ es reducible. Si $t > 1$, entonces $t - 1 \geq 1$, así $(1 + x + ... + x^{t-1})^p$ no es constante luego $f(x)$ es reducible.

Paso 3: Ahora probamos el Lema. Si $n = 1$, entonces $n + 1$ es primo. Así supongase que $n > 1$. Si $p \mid n+1$, entonces $f(x)$ es reducible por el Paso 2, lo cual es una contradicción. Por tanto $p \nmid n+1$ y como $f(x)$ es irreducible se tiene por el Paso 1 que $n+1$ es primo.

Teorema 3.3.7 [Teorema 3.33, [6]] Sea $\alpha \in \mathbb{F}_{q^n}$. Si el grado de α sobre $\mathbb{F}_q$ es d y $g(x) \in \mathbb{F}_q[x]$ es el polinomio mínimo de α sobre $\mathbb{F}_q$. Entonces

(i) $g(x)$ es irreducible sobre $\mathbb{F}_q$ y su grado d divide n.

(ii) Si $f(x) \in \mathbb{F}_q[x]$, entonces $f(\alpha) = 0$ si y sólo si $g(x) \mid f(x)$

(iii) Si $f(x) \in \mathbb{F}_q[x]$ es mónico, irreducible y $f(\alpha) = 0$, entonces $f(x) = g(x)$

(iv) $g(x)$ divide a $x^{q^d} - x$ y a $x^{q^n} - x$.

(v) Las raíces de $g(x)$ son $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$ y $g(x)$ es el polinomio mínimo sobre $\mathbb{F}_q$ de todos estos elementos.

Teorema 3.3.8 [Corolario 3.47, [6]] Sean $f(x)$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado n y ℓ un entero positivo. Entonces $f(x)$ es irreducible sobre $\mathbb{F}_{q^\ell}$ si y sólo si $\text{mcd}(\ell, n) = 1$.

A continuación probamos una versión del Teorema 4.2.1 de [5] .

Teorema 3.3.9 Sea N una base normal óptima de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ generada por $\alpha \in \mathbb{F}_{q^n}$ con $\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -1$, entonces una de la dos condiciones siguientes se verifica:

(i) $n + 1$ es primo, $\mathbb{Z}^\star_{n+1} =< \overline{q} >$ y α es una raíz (n+1)-ésima primitiva de la unidad.

(ii) **(a)** $q = 2^v$ para algún entero positivo v tal que $\text{mcd}(v, n) = 1$,

(b) $2n + 1$ es primo, $\overline{2}$ y $\overline{-1}$ generan el grupo multiplicativo $\mathbb{Z}^\star_{2n+1}$ y

(c) $-\alpha = z + z^{-1}$ donde z es una raíz $(2n + 1)$-ésima primitiva de la unidad.

Prueba. Asumiremos la notación dada en el inicio de esta sección. Se sigue del Lema 3.1.4 que cada fila de la matriz D tiene exactamente dos entradas distintas de cero las cuales son inversos aditivos, excepto la primera fila, la cual tiene exactamente una entrada diferente de cero igual a -1, es decir, para cada $i \neq 0$ $\alpha\beta_i = a\beta_k - a\beta_\ell$ para algún $a \in \mathbb{F}^\star_q$, $0 \leq k, \ell \leq n - 1$ y

$$\alpha\beta_0 = -\beta_m \tag{3.6}$$

para algún $m \in \{0, 1, ..., n - 1\}$.

Si $m = 0$, entonces $\alpha = -1 \in \mathbb{F}_q$, luego $n = 1$. Así, si $q = 2^t$ se cumple (ii) y si $q = p^t$ con $p > 2$, se cumple (i). Asumiremos por tanto que $m > 0$. Sean $\text{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q) = \{\sigma_0, \sigma_1, ..., \sigma_{n-1}\}$ y $R_n = \{0, 1, ..., n - 1\}$.

Caso 1: $(2m)\,\%n = 0$.

Aplicamos σ_m a 3.6, así $\alpha_m\beta_m = \sigma_m(\alpha)\sigma_m(\beta_0) = -\sigma_m(\beta_m) = -\beta_{(2m)\,\%n} = -\beta_0 = \beta_m/\alpha$

de donde $\alpha\alpha_m = \alpha_m\alpha_0 = 1 = -Tr(\alpha) = -\sum_{\ell=0}^{n-1}\alpha_\ell = \sum_{\ell=0}^{n-1}(-1)\alpha_\ell$.

Así la fila m de T es $(-1,-1,...,-1)$ luego la columna m de D es $(-1,-1,...,-1)^t$, es decir, $D_{im} = -1$ para todo $i \in R_n$. Así podemos definir la función $\psi : R_n \setminus \{0\} \longrightarrow R_n \setminus \{m\}$ por $\psi(i) = i^\star$ para todo $i \in R_n \setminus \{0\}$ donde $i^\star$ es el índice de columna donde aparece el único otro elemento no nulo de la fila i en D. Así $\alpha\beta_i = \beta_{i^\star} - \beta_m$ para todo $i \in R_n \setminus \{0\}$. Ahora, si $i^\star = j^\star$, entonces $\beta_{i^\star} - \beta_m = \beta_{j^\star} - \beta_m$, es decir $\alpha\beta_i = \alpha\beta_j$ de donde $\beta_i = \beta_j$ y por tanto $i = j$, asi hemos probado que si $i \neq j$, entonces $i^\star \neq j^\star$, es decir que ψ es inyectiva y por tanto biyectiva. Así $\alpha\alpha_{i^\star} = \alpha_i$ para todo $i^\star \in R_n \setminus \{m\}$ y $\alpha\alpha_m = 1$. Luego $G = \{1\} \cup \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ es cerrado bajo la multiplicación por α, así por el Lema 3.3.2 $G \leqslant \mathbb{F}_{q^n}^\star$ de orden $n+1$, así $\alpha^{n+1} = 1$ y como $\alpha \neq 1$ se tiene que α es raíz de $f(x) = 1 + x + ... + x^n \in \mathbb{F}_q[x]$ luego el polinomio mínimo de α, $m_\alpha(x)$, divide $f(x)$ y por el Lema 3.3.5 se tiene $m_\alpha(x) = f(x)$, así $f(x)$ es irreducible y por el Lema 3.3.6 $n+1$ es primo. Luego $f(x) = Q_{n+1}(x)$, por tanto usando el Teorema 3.2.6 $\overline{q}$ genera $\mathbb{Z}_{n+1}^\star$, además el orden de α es $n+1$, por tanto α es una raíz $(n+1)$-ésima primitiva de la unidad, verificándose (i).

Caso 2: $(2m)\,\%n \neq 0$.

Así $m \in \{1, ..., n-1\}$. Por 3.6 se tiene que $D_{0\,m} = -1$ y $D_{0\,i} = 0$ para todo $i \neq m$. Ahora bien, si $i = (-m)\,\%n$, entonces $m = (-i)\,\%n$ luego por 3.3 $D_{i\,i} = D_{0\,(-i)\,\%n} = D_{0\,m} = -1$. También si $i \neq (-m)\,\%n$, entonces $m \neq (-i)\,\%n$ luego por 3.3 $D_{i\,i} = D_{0\,(-i)\,\%n} = 0$, es decir, en la diagonal principal de D existe exactamente un elemento no nulo.

Por tanto $\alpha\beta_{(-m)\,\%n}$ tiene un sumando $-\beta_{(-m)\,\%n}$. Como $(-m)\,\%n > 0$, existe $\ell \in \{0, 1, ..., n-1\}$ tal que

$$\alpha\beta_{(-m)\,\%n} = \beta_\ell - \beta_{(-m)\,\%n} \tag{3.7}$$

donde $\ell \neq (-m)\,\%n$. Nótese que

$$\alpha_m(\alpha\beta_0) = \alpha_m(-\beta_m) = -\sigma_m(\alpha\beta_0) = -\sigma_m(-\beta_m) = \sigma_m(\beta_m) = \beta_{(2m)\,\%n}$$

Por otro lado por 3.7

$$\begin{aligned}\alpha(\alpha_m\beta_0) &= \alpha(\sigma_m(\alpha)\sigma_m(\sigma_m^{-1}(\beta_0))) = \alpha\sigma_m(\alpha\beta_{(-m)\,\%n})\\ &= \alpha\sigma_m(\beta_\ell - \beta_{(-m)\,\%n}) = \alpha(\beta_{(m+\ell)\,\%n} - \beta_0)\\ &= \alpha\beta_{(m+\ell)\,\%n} - \alpha\beta_0) = \alpha\beta_{(m+\ell)\,\%n} + \beta_m.\end{aligned}$$

Así obtenemos

$$\alpha\beta_{(m+\ell)\,\%n} = \beta_{(2m)\,\%n} - \beta_m \tag{3.8}$$

Ahora calculamos $\alpha\alpha_\ell\beta_{(-m)\,\%n}$ de dos maneras.

Primero, nótese por 3.7 que $1 = D_{(-m)\,\%n\ \ell} = D_{(-m-\ell)\,\%n\,(-\ell)\,\%n}$ y como $\ell \neq (-m)\,\%n$ implica que $(-m-\ell)\,\%n \neq 0$ se tiene $\alpha\beta_{(-m-\ell)\,\%n} = \beta_{(-\ell)\,\%n} - \beta_j$ para algún $j \notin \{(-\ell)\,\%n, (-m-\ell)\,\%n\}$ de donde $(j+\ell)\,\%n \notin \{0, (-m)\,\%n\}$ (si $j = (-m-\ell)\,\%n$, entonces $D_{j\,j} = -1$, así $j = (-m)\,\%n$, es decir, $(-m-\ell)\,\%n = (-m)\,\%n$ de donde $\ell = 0$ y por 3.8 $D_{m\,m} = -1$ lo cual implica que $m = (-m)\,\%n$ de donde $(2m)\,\%n = 0$ lo cual es una contradicción).

Por una parte

$$\begin{aligned}\alpha_\ell(\alpha\beta_{(-m)\,\%n}) &= \alpha_\ell(\beta_\ell - \beta_{(-m)\,\%n}) = \alpha_\ell(\beta_\ell - \sigma_m^{-1}(\beta))\\ &= \sigma_\ell(\alpha)\sigma_\ell(\beta - \sigma_\ell^{-1}\circ\sigma_m^{-1}(\beta)) = \sigma_\ell(\alpha(\beta - \sigma_{(-\ell-m)\,\%n}(\beta)))\\ &= \sigma_\ell(\alpha\beta_0 - \alpha\beta_{(-m-\ell)\,\%n}) = \sigma_\ell(-\beta_m - \beta_{(-\ell)\,\%n} + \beta_j)\\ &= -\beta_{(m+\ell)\,\%n} - \beta_0 + \beta_{(j+\ell)\,\%n}.\end{aligned}$$

Por otra parte

$$\begin{aligned}\alpha(\alpha_\ell\beta_{(-m)\,\%n}) &= \alpha\sigma_\ell(\alpha\sigma_\ell^{-1}(\beta_{(-m)\,\%n})) = \alpha\sigma_\ell(\alpha\sigma_\ell^{-1}\circ\sigma_m^{-1}(\beta))\\ &= \alpha\sigma_\ell(\alpha\sigma_{(-\ell-m)\,\%n}(\beta)) = \alpha\sigma_\ell(\alpha\beta_{(-m-\ell)\,\%n})\\ &= \alpha\sigma_\ell(\beta_{(-\ell)\,\%n} - \beta_j) = \alpha(\beta_0 - \beta_{(j+\ell)\,\%n})\\ &= \alpha\beta_0 - \alpha\beta_{(j+\ell)\,\%n} = -\beta_m - \alpha\beta_{(j+\ell)\,\%n}.\end{aligned}$$

Así $-\beta_{(m+\ell)\,\%n} - \beta_0 + \beta_{(j+\ell)\,\%n} = -\beta_m - \alpha\beta_{(j+\ell)\,\%n}$ luego

$$\alpha\beta_{(j+\ell)\,\%n} = -\beta_{(j+\ell)\,\%n} + \beta_0 + \beta_{(m+\ell)\,\%n} - \beta_m.$$

Ahora bien como $(j+\ell)\,\%n \neq (-m)\,\%n$, el coeficiente de $\beta_{(j+\ell)\,\%n}$ es cero en la expansión de $\alpha\beta_{(j+\ell)\,\%n}$. Así $-\beta_{(j+\ell)\,\%n}$ debe cancelarse con uno de los últimos dos terminos. No se cancela con β_0, pues si así fuese tendríamos $\beta_0 = \beta_{(j+\ell)\,\%n}$ de donde $(j+\ell)\,\%n = 0$ lo cual no es posible.

Si $-\beta_{(j+\ell)\,\%n} + \beta_{(m+\ell)\,\%n} = 0$, entonces $(m+\ell)\,\%n = (j+\ell)\,\%n$, así $\alpha\beta_{(m+\ell)\,\%n} = \beta_0 - \beta_m$, pero por 3.8 $\alpha\beta_{(m+\ell)\,\%n} = \beta_{(2m)\,\%n} - \beta_m$ luego $\beta_{(2m)\,\%n} = \beta_0$ de donde $(2m)\,\%n = 0$ lo cual es una contradicción. Por tanto $-\beta_{(j+\ell)\,\%n} - \beta_m = 0$ y $\alpha\beta_{(j+\ell)\,\%n} = \beta_0 + \beta_{(m+\ell)\,\%n}$.

En la primera igualdad $m \neq (j+\ell)\,\%n$ no es posible por independencia lineal, así $m = (j+\ell)\,\%n$, luego $-2\beta_m = 0$ de donde $2 = 0$ y por tanto la característica de $\mathbb{F}_q$ es 2 y

$$\alpha\beta_m = \beta_{(m+\ell)\,\%n} + \beta_0. \tag{3.9}$$

A partir de ahora asumiremos que $q = 2^v$ para algún v entero positivo. Las igualdades 3.6 y 3.7 pueden reescribirse como

$$\alpha\beta = \beta_m \tag{3.10}$$

$$\alpha\beta_{(-m)\,\%n} = \beta_\ell + \beta_{(-m)\,\%n} \tag{3.11}$$

Aplicando σ_m a 3.11 se tiene $\alpha_m\beta = \beta_{(\ell+m)\,\%n} + \beta_0$ que junto a 3.9 da $\alpha\beta_m = \alpha_m\beta$ de donde $\sigma_m(\alpha\beta^{-1}) = \alpha_m\sigma_m(\beta)^{-1} = \alpha_m\beta_m^{-1} = \alpha\beta^{-1}$ multiplicando esto con 3.10 da $\alpha^2 = \sigma_m(\alpha\beta^{-1}\beta) = \sigma_m(\alpha)$. Ahora si h es un entero positivo tal que $\sigma_{(hm)\,\%n}(\alpha) = \alpha^{2^h}$, entonces $\sigma_{((h+1)m)\,\%n}(\alpha) = \sigma_{(m+hm)\,\%n}(\alpha) = \sigma_m(\sigma_{(hm)\,\%n}(\alpha)) = \sigma_m(\alpha^{2^h}) = (\sigma_m(\alpha))^{2^h} = (\alpha^2)^{2^h} = \alpha^{2^{h+1}}$. Luego $\sigma_{(km)\,\%n}(\alpha) = \alpha^{2^k}$ para todo k entero positivo. En particular si $k = \frac{n}{\mathrm{mcd}(n,m)}$, entonces $km = \frac{nm}{\mathrm{mcd}(n,m)} = \mathrm{mcm}(n,m)$ luego $n \mid km$ y por tanto $\alpha^{2^k} = \sigma_0(\alpha) = \alpha$ lo cual dice que $\alpha \in \mathbb{F}_{2^k}$ luego si $g(x)$ es el polinomio mínimo de α sobre $\mathbb{F}_2$, entonces por 3.3.7 $\deg g(x) \mid k$, así $\deg g(x) \leq k \leq n$.

Afirmación 1. α tiene grado n sobre $\mathbb{F}_q$.

En efecto, sea $f(x)$ el polinomio mínimo de α en $\mathbb{F}_q[x]$, entonces $f(\alpha) = 0$ y como α genera una base normal, se sigue de 3.3.5 que $\deg f(x) \geq n$. Por otro lado, por 3.3.7 $\deg f(x) \mid n$, así $\deg f(x) \leq n$. Por tanto $\deg f(x) = n$.

Afirmación 2. $\deg g(x) \geq n$.

En efecto, como $g(x)$ es el polinomio mínimo de α sobre $\mathbb{F}_2$ se tiene que $g(\alpha) = 0$ y como $\mathbb{F}_2 \subseteq \mathbb{F}_q$ se sigue que $g(x) \in \mathbb{F}_2[x] \subseteq \mathbb{F}_q[x]$, luego por 3.3.7 $f(x) \mid g(x)$, así, $n = \deg f(x) \leq \deg g(x)$.

Por tanto $k = n$, luego $\text{mcd}(n, m) = 1$.
Ahora, como $g(x) \in \mathbb{F}_q[x]$, $g(\alpha) = 0$ y $\deg g(x) = n$ por 3.3.5 se tiene $g(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i})$, pero por 3.3.7 y la afirmación 1 se tiene que $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ son las n raíces de $f(x)$, así, $f(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i})$, luego $f(x) = g(x)$. Así, los conjugados de α sobre $\mathbb{F}_q$ son los mismos que aquellos sobre $\mathbb{F}_2$, a saber, $\alpha, \alpha^2, ..., \alpha^{2^{n-1}}$. Además, como $f(x) = g(x)$ se tiene que $g(x)$ es irreducible en $\mathbb{F}_2[x]$ y en $\mathbb{F}_q[x] = \mathbb{F}_{2^v}[x]$, luego por 3.3.8 se tiene que $\text{mcd}(v, n) = 1$. Como $\overline{m} \in \mathbb{Z}_n^\star$, sea $\overline{m_1}$ el inverso en $\mathbb{Z}_n^\star$ de $\overline{m}$, así existe $m_1 > 0$ tal que $mm_1 \equiv 1(\text{mod}n)$. Entonces como $(\alpha\beta^{-1})^{q^m} = \alpha\beta^{-1}$ elevando repetidamente a la potencia q^m se tiene $\alpha\beta^{-1} = (\alpha\beta^{-1})^{q^{mm_1}} = (\alpha\beta^{-1})^{q^{(mm_1)\,\%n}} = (\alpha\beta^{-1})^q$ (pues $\alpha\beta^{-1} \in \mathbb{F}_{q^n}$), lo cual implica que $\alpha\beta^{-1} \in \mathbb{F}_q$, así $\alpha\beta^{-1} = r \in \mathbb{F}_q^\star$ luego $\alpha = r\beta$ de donde $\text{Tr}(\alpha) = r\text{Tr}(\beta)$ y como $\text{Tr}(\alpha) = \text{Tr}(\beta) = -1$ se tiene $\alpha = \beta$. Así como D es la transpuesta de $T = D$ se tiene

$$D_{ij} = D_{ji} \text{ para todo } i, j \in \{0, 1, ..., n-1\}. \tag{3.12}$$

Sea z un cero de $x^2 - \alpha x + 1$ en una extensión $\mathbb{F}_{q^{2n}}$ de $\mathbb{F}_{q^n}$, así z^{-1} es la otra raíz y $z + z^{-1} = \alpha$. Como $z \neq 0$, $z \in \mathbb{F}_{q^{2n}}^\star$ luego $\text{ord}(z) \mid q^{2n} - 1$, así $\text{ord}(z)$ es impar, digamos $\text{ord}(z) = 2t + 1$.
Para cada entero i sea $r_i = z^i + z^{-i}$, así $r_0 = 0$ y $r_1 = \alpha$. Además $r_i = r_j$ si y sólo si los ceros z^i, z^{-i} de $x^2 - r_i x + 1$ coinciden con los ceros z^j, z^{-j} de $x^2 - r_j x + 1$ si y sólo si $i \equiv \pm j (\text{mod } 2t + 1)$. Por tanto hay exactamente t elementos diferentes no nulos entre los r_i, a saber, $r_1, r_2, ..., r_t$. Cada uno de los n conjugados de α es de la forma $\alpha^{2^j} = z^{2^j} + z^{-2^j} = r_{2^j}$ para j entero y por tanto ocurre entre los r_i. Esto implica que $n \leq t$. Mostramos que $n = t$, probando que cada r_i no nulo es un conjugado de α. Lo cual se hará por inducción sobre i.

Nótese que $r_1 = \alpha$ y $r_2 = \alpha^2$ así basta probarlo para $3 \leq i \leq t$. Veamos

$$\begin{aligned}\alpha r_{i-s} = r_1 r_{i-s} &= (z + z^{-1})(z^{i-s} + z^{s-i}) \\ &= (z^{i-s+1} + z^{-(i-s+1)}) + (z^{i-s-1} + z^{-(i-s-1)}) \\ &= r_{i-s+1} + r_{i-s-1}.\end{aligned}$$

Así $\alpha r_{i-2} = r_{i-1} + r_{i-3}$ y $\alpha r_{i-1} = r_{i-2} + r_i$. Por hipótesis de inducción r_{i-2}, r_{i-1} son conjugados de α y $r_{i-3} = 0$ o r_{i-3} es conjugado de α. supongamos que $r_{i-1} = \alpha_a$ y $r_{i-2} = \alpha_b$ ($\alpha_u = \alpha^{2^u}$) como $i \geq 3$, $i - 1 \neq 1$ luego $r_{i-1} \neq r_1$, es decir, $\alpha_a \neq \alpha_0$. Así

$$\alpha\alpha_b = \alpha_a + r_{i-3} \tag{3.13}$$

$$\alpha\alpha_a = \alpha_b + r_i \tag{3.14}$$

Por 3.13 $D_{b\,a} = 1$ luego por 3.12 $D_{a\,b} = 1$ y como $a > 0$ se tiene $\alpha\alpha_a = \alpha_b + \alpha_c$, de donde $r_i = \alpha_c$ por tanto r_i es un conjugado de α.

Ahora probamos que $2n + 1$ es primo, para lo cual basta probar que para cada entero i, $2n + 1 \nmid i$ implica $\text{mcd}(2n + 1, i) = 1$.

Sea entonces i un entero tal que $2n + 1 \nmid i$ así $i \not\equiv 0 (\text{mod}\, 2n + 1)$, es decir, $r_i \neq 0$ luego r_i es un conjugado de α, digamos, $r_i = \alpha^{2^j}$ así $r_i = (r_1)^{2^j} = (z + z^{-1})^{2^j} = z^{2^j} + z^{-2^j} = r_{2^j}$ de donde $i \equiv \pm 2^j (\text{mod}\, 2n + 1)$ y como $\text{mcd}(\pm 2^j, 2n + 1) = 1$ se tiene $\text{mcd}(i, 2n + 1) = 1$. Por tanto $2n + 1$ es primo. Nótese que también se ha probado lo siguiente: Para todo entero i, si $2n + 1 \nmid i$, entonces $i \equiv \pm 2^j (\text{mod}\, 2n + 1)$, es decir, $i \equiv (-1)^u 2^j (\text{mod}\, 2n + 1)$ para algún $u \in \{0, 1\}$ y j entero. ($\bigstar$)

Ahora bien, como $\overline{2}, \overline{-1} \in \mathbb{Z}^\star_{2n+1}$ definimos $W = \{\overline{-1}^u\ \overline{2}^j \mid u \in \{0, 1\} \text{ y } j \text{ entero }\} \subseteq \mathbb{Z}^\star_{2n+1}$. Por otra parte, si $\overline{x} \in \mathbb{Z}^\star_{2n+1}$, entonces $2n+1 \nmid x$, así, por ($\bigstar$) $x \equiv (-1)^u 2^j (\text{mod}\ 2n+1)$ para algún $u \in \{0, 1\}$ y j entero, es decir, $\overline{x} = \overline{-1}^u\ \overline{2}^j \in W$. Por tanto $\mathbb{Z}^\star_{2n+1} \subseteq W$ y en consecuencia $\mathbb{Z}^\star_{2n+1}$ es generado por $\overline{2}$ y $\overline{-1}$. $\square$

Bibliografía

[1] George E. Andrews, Number Theory, Dover, 1971.

[2] D. W. Ash, I. F. Blake, and S. A. Vanstone, Low complexity normal bases, Discrete Appl. Math. 25 (1989) 191 - 210.

[3] S. D. Cohen and S. Huczynska, The primitive normal basis theorem, without a computer, J. London Math. Soc., 2nd Ser. 67 (2003) 41-56.

[4] S. Gao and H. W. Lenstra, Jr., Optimal normal bases, Des. Codes Cryptogr. 2 (1992) 315 - 323.

[5] S. Gao, Normal Bases over Finite Fields, PhD thesis, University of Waterloo, Canada, 1993.

[6] R. Lidl and H. Niederreiter, Finite Fields, volume 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, second edition, 1997.

[7] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, revised edition, 1994.

[8] J.L. Massey and J.K. Omura, Computational method and apparatus for Finite Field arithmetic, U.S. patent # 4,587,627, May 1986.

[9] G. L. Mullen and C. Mummert, Finite Fields and Applications, volume 41 of Student Mathematical Library, American Mathematical Society, Providence, RI, 2007.

[10] R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, Optimal normal bases in $GF(p^n)$, Discrete Appl. Math. 22 (1988/89) 149 -161.

[11] Joseph J. Rotman, Advanced Modern Algebra, Prentice Hall, 2002.

[12] A. Wassermann, (1990). Konstruktion von Normalbasen. Bayreuther Mathematische Schriften, 31, 155-164.