UNIVERSIDAD DE MURCIA

FACULTAD DE MATEMÁTICAS

TRABAJO FIN DE GRADO

CUERPOS FINITOS

David Gómez Saura

Curso 2014-2015

Índice general

Resumen

En el presente trabajo se realizará un estudio fundamentalmente teórico de los cuerpos finitos. El texto consta de dos capítulos, que componen el cuerpo del trabajo, un capítulo a modo de anexo, bibliografía y por último un índice terminológico para facilitar la búsqueda de las definiciones de los términos no conocidos. En el anexo se incluyen los conceptos previos de álgebra que se recomiendan al lector para el buen entendimiento del texto, así como los resultados utilizados no específicos sobre cuerpos finitos para hacer más accesible su consulta. El primer capítulo está dedicado a la caracterización de los cuerpos finitos y sus propiedades generales, mientras que el segundo capítulo se centra en el estudio de polinomios sobre cuerpos finitos.

El texto comienza en el capítulo 1 con la definición de los primeros conceptos del álgebra básica tales como *anillo conmutativo*, elemento *invertible* y *característica* de un anillo, indispensables para la introducción del término *cuerpo* y en general para el desarrollo del trabajo. Se introducirán algunos ejemplos de anillos y cuerpos, así como las primeras propiedades que serán utilizadas en resultados posteriores. Entre estas propiedades se encuentra que todo cuerpo finito tiene característica un número primo; es decir, para todo cuerpo finito existe un entero primo positivo p tal que la suma p veces de 1 es igual a 0 y, además, es el menor número positivo que cumple tal condición. Esta propiedad pese a su aparente sencillez resulta clave en la teoría de cuerpos finitos.

La segunda sección del primer capítulo estará dedicada a la introducción a la teoría de extensiones de cuerpos en general y ciertas propiedades que permitirán más tarde el desarrollo de los resultados específicos para cuerpos finitos. La sección comienza con la definición de *extensión de cuerpos* y otros conceptos relacionados, como el *grado* de la extensión o *cuerpo intermedio*. Se mostrará que toda extensión de cuerpos F/K puede ser vista como un K-espacio vectorial. Tras ello se continuará con la demostración de un teorema fundamental en la teoría, no sólo de extensiones de cuerpos finitos, sino también de extensiones generales: el teorema de multiplicidad del grado. Dicho teorema establece que el grado de una extensión finita puede obtenerse como el producto del grado de las extensiones intermedias. Se llevará a cabo la introducción de las extensiones *algebraicas* y *simples*. Una extensión de cuerpos F/K se dirá algebraica si para todo elemento $\alpha \in F$ existe un polinomio sobre K que se anule en dicho elemento. Por su parte una extensión se dirá simple si está generada por un único elemento. Se probará que en una extensión algebraica para cada elemento de la extensión existe un único polinomio mónico e irreducible que se anula en dicho elemento. Este polinomio recibirá el nombre de *polinomio mínimo*. La sección concluirá con la caracterización de extensiones finitas y la introducción de los conceptos de *clausura algebraica* y *cuerpo de escisión*.

Una vez realizada esta introducción a las extensiones de cuerpos será el momento de

profundizar en la teoría de cuerpos finitos. Resultados anteriores, como que todo cuerpo finito tiene característica un número primo y que una extensión de cuerpos puede ser vista como un espacio vectorial, permitirán obtener que para cualquier cuerpo finito su número de elementos es igual a una potencia de un número primo. Es entonces cuando se muestra uno de los teoremas de mayor importancia: el teorema de existencia y unicidad de cuerpos finitos. Este teorema establece no sólo que el número de elementos de todo cuerpo finito es igual a una potencia de un número primo, sino que para cada número primo p y cada entero positivo n existe un cuerpo finito de p^n elementos y, además, dicho cuerpo es único salvo isomorfismos. Equivalentemente, dos cuerpos cualesquiera con p^n elementos son isomorfos. Otro de los resultados de importancia será el teorema de estructura de subcuerpos de cuerpos finitos, que caracterizará los subcuerpos de un cuerpo finito con p^n elementos, como aquellos que contienen p^m elementos con m un entero positivo que divide a n. La primera sección del capítulo 1 terminará con la demostración de que el grupo de las unidades de un cuerpo finito es cíclico; es decir, generado por un elemento, que se denominará elemento *primitivo*.

En la cuarta sección del primer capítulo comenzará el estudio de las extensiones finitas de cuerpos finitos. Una vez vistas algunas propiedades sobre las extensiones algebraicas y el polinomio mínimo de un elemento en la sección 2, el objetivo central de la sección será probar uno de los resultados de mayor importancia acerca de extensiones de cuerpos finitos: que toda extensión de cuerpos finitos es una extensión *cíclica*, o, lo que es lo mismo, que es una extensión finita de Galois y que el grupo formado por los automorfismos que dejan fijos los elementos del cuerpo base de la extensión, conocido como *grupo de Galois* de la extensión, es cíclico. Para la demostración de dicho resultado será necesaria la introducción de los conceptos de extensiones *separables*, *normales* y *de Galois* y algunas de las propiedades básicas de dichas extensiones. Se definirá el concepto de *conjugados* de un elemento sobre un cuerpo y se caracterizarán los automorfismos de un cuerpo finito. Una de las conclusiones que podrá extraerse de la prueba del teorema será que el grupo de Galois de una extensión de cuerpos finitos es cíclico; pero, además, que el automorfismo generador de dicho grupo es conocido para cada extensión y recibirá el nombre de *automorfismo de Frobenius*.

Tras esto, se profundizará en las propiedades de la traza y la norma de un elemento sobre un cuerpo finito, o lo que es igual, la suma y producto respectivamente de los conjugados de un elemento. El estudio de la traza de un elemento permitirá más tarde proporcionar un método para verificar si un subconjunto dado es una base de una extensión de cuerpos finitos F/K, viendo dicha extensión como un K-espacio vectorial. Se introducirán varios tipos de bases de una extensión de cuerpos: *polinómicas*, *normales*, *duales*, *autoduales* y *primitivas normales*. Una importante propiedad que se verá es que para toda extensión de cuerpo finitos existe alguna base normal y además para toda base existe una única base dual, sin embargo, no toda extensión posee una base normal y autodual. Este resultado fue demostrado por A. Lempel y M.J. Weinberger en 1988, estableciendo además las condiciones para las cuales sí existe una base de estas características. El último resultado que aparece en la sección será un teorema de suma dificultad, el teorema de *Lenstra-Schoof*. En él se demuestra la existencia de bases primitivas normales para toda extensión de cuerpos finitos. Dicho teorema fue demostrado en 1987 con ayuda computacional y no fue hasta 2003 cuando S.D. Cohen y S. Huczynscka obtuvieron una prueba sin ayuda del ordenador. El teorema únicamente prueba la existencia de dichas bases, sin embargo el problema de determinar el número de ellas sigue siendo una incógnita.

El segundo capítulo como se ha comentado estará dedicado íntegramente al estudio de polinomios sobre cuerpo finitos. El capítulo comenzará con la introducción de los conceptos de *raíz n-ésima*, *raíz n-ésima primitiva*, *polinomio ciclotómico* y *cuerpo ciclotómico*. Se reflexionará acerca de las propiedades de las raíces n-ésimas y cuestiones relacionadas con el grado de polinomios ciclotómicos (que dependerá de la *función de Euler*), sus formas de expresión y se proporcionará un método recurrente para su cálculo. Se obtendrá que, a diferencia de los cuerpos con característica 0, los polinomios ciclotómicos sobre cuerpos finitos no son necesariamente irreducibles y el número de factores irreducibles de cada uno dependerá también de la función de Euler.

Como consecuencia del estudio de polinomios ciclotómicos se obtendrá uno de los grandes teoremas del trabajo, el teorema de *Wedderburn*. En él se establece que todo anillo de división finito es un cuerpo. Un anillo división es un anillo al que no se presupone la conmutatividad del producto y en el que todo elemento no nulo es invertible, es decir, un anillo que cumple las mismas propiedades de un cuerpo a excepción de la conmutatividad del producto. Un enunciado equivalente para el teorema será pues que el producto en todo anillo de división finito es conmutativo.

La tercera sección comenzará con la definición de orden de un polinomio y la justificación de que todo polinomio tiene orden un entero positivo. Se define el orden de un polinomio f como el menor entero e tal que f divide al polinomio $x^e - 1$. Veremos pues que para cada polinomio que no se anule en 0 existirá tal entero positivo. La sección continuará abordando técnicas para el cálculo de órdenes de polinomios en función de su factorización, para acabar dando un método para el cálculo de órdenes de polinomios irreducibles, siendo así capaces de calcular el orden de cualquier polinomio sobre cualquier cuerpo finito. Tras ello se introducirá el concepto de polinomio *primitivo*. Un polinomio se dice primitivo si es el polinomio mínimo de algún elemento primitivo; es decir, de un elemento generador del grupo de las unidades de una extensión. Se dará un resultado que caracterizará los polinomios primitivos atendiendo al orden de dicho polinomio.

La siguiente sección tratará sobre polinomios irreducibles sobre cuerpos finitos. Se introducirá la *función de Moebius* y una importante fórmula sobre la que se basan casi la totalidad de los resultados de la sección: la *fórmula de inversión de Moebius*. A partir de dicha fórmula se podrá obtener el número de polinomios mónicos irreducibles de un determinado grado sobre un cuerpo, determinar exactamente cuales son tales polinomios y una expresión para el producto de todos ellos. Se proporcionará también a partir de la fórmula de inversión de Moebius un método mucho más operativo para el cálculo de polinomios ciclotómicos que el obtenido en la segunda sección del capítulo.

Por último se presentará el algoritmo de Berlekamp, el cual permitirá la factorización de cualquier polinomio sobre cuerpos finitos. Se introducirán algunas propiedades previas para la deducción del algortimo, así como la demostración de que en efecto el algoritmo es eficaz; es decir, permite la factorización de cualquier polinomio. Finalmente se mostrará un ejemplo de aplicación del mismo.

Abstract

In the present work a fundamentally theoretical study about the finite fields will be carried out. The text has two chapters which comprise the body, a chapter acts as an annex, bibliography and lastly, an index with the terminology so as to ease the search of definitions for the unknown terms. In the annex, the previous concepts of algebra which are recommended to the reader for a better understanding of the text are included, as well as the not-specific results used in the finite fields to make the consult easier. The first chapter is devoted to the characterization of the finite fields and their general properties while the second focuses in the study of polynomials over finite fields.

The text starts in chapter 1 with the definition of the first concepts of basic algebra such as *commutative ring*, *unit* and *characteristic* of a ring, indispensable for the introduction of the term *field* and in general for the development of the work. Some examples of rings and fields will be introduced, as well as the first properties that will be essential for the latter results. Among these properties, it is to be found that every finite field has prime characteristic i.e. for any finite field there is a positive integer p such that the sum of p times of 1 is equal to 0 and moreover it is the least positive number that fulfills that condition. This property, despite its apparent ease, turns out to be the key in the theory of finite fields.

The second section of the first chapter will be devoted to the introduction to the theory of general field extensions and certain properties that will allow a later development of the specific results for finite fields. The section starts with the definition of *field extension* and other concepts in relation, like the *degree* of the extension or *intermediate field*. It will be showed that a extension of fields F/K may be regarded as a vector space over K. After that, we will continue with the proof of a fundamental theorem in field extensions theory: the theorem of multiciplity of the degree. Such theorem establishes that the degree of an extension is obtained by multiplying the degree of the intermediate extensions. The introduction of the *algebraic* and *simple* extensions will be carried out. A field extension F/K will be named algebraic if for any element $\alpha \in F$ there is a polynomial over K such that α is a root of this polynomial. Furthermore, an extension will be called simple if it is generated by a single element. It will also be proved that in an algebraic extension for each element exists a unique monic and irreducible polynomial which gets annulled in the element. This polynomial will received the name of *minimal polynomial*. The section will conclude with the characterization of the finite extensions and the introduction of the concept of *splitting field*.

Once this introduction to the extensions of fields is done, it is time to deepen into the finite fields. Previous results, such as that any finite field has prime characteristic and that an extension may be regarded as a vector space, will allow to obtain that for any finite

field its number of elements is equal to a prime power number. It is then when one of the most important theorem is showed: the existence and uniqueness of finite fields theorem. This result establishes not only that the number of elements of every finite field is equal to a prime power number, but also that for every prime power p^n there exists a finite field whose number of elements is exactly that prime power and it is unique except isomorphism. Equally, any two fields with p^n elements are isomorphic. Another of the important results will be the structure of subfields theorem, which will characterize the subfields of a finite one with p^n elements, as those that contain p^m elements with m a positive integer that divides n. The first section of chapter 1 will end with the proof that the group of non-zero elements of a finite field is *cyclic* i.e. it is generated by an element, which will be called *primitive*.

In the fourth section of the first chapter will start with the study of the finite extensions of finite fields. Once regarded some of the features about the algebraic extensions and the minimal polynomial of an element in section 2, the section's main objective will be proving one of the results of higher importance about the finite fields extensions: checking that all the extension of finite fields is a *cyclic* extension, or the same, that it is a *Galois* extension and the group formed by the automorphisms that leave the elements of the base field of the extension fixed, known as *Galois group*, is cyclic. For the proof of such result it will be needed the introduction of the extensions concepts: *separable*, *normal* and *Galois* and some of the basic properties of these extensions. It will also be defined the concept of *conjugates* of an element over a field and the automorphisms of a finite field will be characterized. One of the conclusions that may be drawn from the theorem's proof will be that Galois group of an extension of finite fields is cyclic, moreover that the generator automorphism of this group is known for each extension and will be called *Frobenius automorphism*.

After this, there will be a deepening insight in the properties of the trace and norm of an element over a finite field, in other words, the sum and product respectively of the conjugates of an element. The study of the trace of an element will later allow to provide with a method to verify if a given subset is a basis of an extension of a finite fields F/K, regarding such extension as a vector space over K. New types of bases of an extension of fields will be introduced: *polynomial*, *normal*, *dual*, *self-dual* and *primitive normal*. An important property which will be seen is that for every extension of finite fields there exists some normal basis and besides, for every basis there exists an only dual basis, nonetheless, not every extension has a normal and self-dual basis. This result was proved by A. Lempel and M.J. Weinberger in 1988, establishing the conditions for which there exists a basis of these characteristics. The last result of the section will be a theorem of high difficulty, the *Lenstra-Schoof theorem*. In this theorem, the existence of primitive normal bases for every extension of finite fields is proved. Such theorem was proved in 1987 with the help of a computer and it was not until 2003 when S.D. Cohen and S. Huczynscka obtained a proof without the help of a computer. The theorem only proves the existence of these bases, however the problem to determine the number of them still remains unkown.

The second chapter, as aforementioned, will be wholly devoted to the study of the polynomials over finite fields. The chapter will start with the introduction of the concepts *nth root of unity*, *primitive nth root* , *cyclotomic* polynomial and *cyclotomic* field. A reflection about the properties of the nth roots and questions related to the degree of the cyclotomic polynomials (which will depend on the *Euler's Function*) will be carried,

their ways of expression and a recurrent method for its calculation will be supplied. It will be obtained that, reversely the fields with zero characteristic, the cyclotomic polynomials over finite fields are not necessarily irreducible and the number of irreducible factors of each one will also depend on Euler's Function.

As a consequence of the study of cyclotomic polynomials it will be obtained one of the big theorems of work the Wedderburn's theorem, which establishes that every finite *division ring* is a field. A division ring is a ring to which it is not presupposed the commutativity of the product and in which every non-zero element is a unit i.e. a ring which fulfills the same properties of a field with the exception of the commutativity of the product. An equivalent statement for the theorem will then be that the product in every finite division ring is commutative.

The third section will start with the definition of order in a polynomial and the justification that every polynomial has a positive integer order. It is defined the order of a polynomial f as the least integer e such that f divides $x^e - 1$ polynomial. We will see then, that for every polynomial for which zero is not a root, there will exist such positive integer. The section will continue by overlooking the techniques for the calculation of polynomials' orders depending on their factorization, to end up giving a method for the calculation of irreducible polynomials' orders, being then able of calculate the order of any polynomial over any finite field. After this, the concept of *primitive polynomial* will be introduced. A polynomial is called primitive if it is the minimal polynomial of some primitive element. A result that will characterize the primitive polynomials according to the order of such polynomial will be provided.

The following section will deal with irreducible polynomials over finite fields. The *Moebius Function* will be introduced and an important formula over which the majority of the results of the section is based, called the *Moebius Inversion Formula.* Such formula will allow to obtain the number of monic irreducible polynomials of a fixed degree over a field, it will also allow to exactly determine which these polynomials are and an expression for the product of all of them. From the Moebius Inversion Formula, it will also be provided a much less complex method for the calculation of cyclotomic polynomials than the one obtained in the second section of the chapter.

Lastly, the *Berlekamp's Algorithm* will be presented, which will allow the factorization of any polynomial over finite fields. Some previous properties for the deduction of the algorithm will be introduced, as well as the proof that the algorithm is indeed efficient. Finally, an example of application of it will be shown.

Capítulo 1

Cuerpos finitos

1.1. Anillos y cuerpos

Esta primera sección estará dedicada a introducir algunos conceptos del álgebra básica que serán utilizados constantemente para el desarrollo del texto. A lo largo de toda la memoria se utilizará la siguiente notación: $\mathbb{N}$ para el conjunto formados por todos los números naturales sin incluir el 0, $\mathbb{Z}$ para el de los números enteros, $\mathbb{Q}$ para el de los números racionales, $\mathbb{R}$ para el de los números y $\mathbb{C}$ para el de los números complejos. Otra cuestión que cabe aclarar es que los resultados del apéndice que sea necesario citar serán referidos de la forma $(A.\ .\ )$, donde los últimos espacios corresponderán a la numeración de la proposición correspondiente.

Definición 1.1.1. *Un **anillo** es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones $+$ y $\cdot$ en A, generalmente llamadas suma y producto respectivamente, que verifican:*

1. *$(A, +)$ es un grupo abeliano. Al elemento neutro de $(A, +)$, que sabemos que es único, se le denominará elemento **cero** (o cero) y se denotará por 0.*

2. *El producto es asociativo.*

3. *Se verifica la propiedad distributiva, es decir, dados $a, b, c \in A$ se verifica*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad y \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

*Si el producto es conmutativo se dirá que el anillo es **conmutativo**. Si tiene elemento neutro para el producto, que llamaremos uno o identidad y se denotará como 1, se dirá que es anillo **unitario**.*

Notación: A lo largo de todo el texto consideraremos siempre, salvo que se indique lo contrario, anillos conmutativos unitarios, con $1 \neq 0$, y se utilizará simplemente el término *anillo* para nombrarlos. Por otro lado se utilizará también la notación ab para hacer referencia al producto, $a \cdot b$, de dos elementos a y b de un anillo.

Ejemplos 1.1.2. *1. El conjunto $\mathbb{N}$, con la suma y el producto usuales, no es un anillo ya que $(\mathbb{N}, +)$ no es un grupo.*

2. Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, con las operaciones suma y producto usuales, son anillos.

3. *El conjunto $\mathbb{Z}_n$ de clases de restos módulo n con las operaciones inducidas por las de $\mathbb{Z}$.*

$$[a+n\mathbb{Z}]+[b+n\mathbb{Z}]=[(a+b)+n\mathbb{Z}] \quad y \quad [a+n\mathbb{Z}][b+n\mathbb{Z}]=[ab+n\mathbb{Z}],$$

es un anillo. En adelante, si no induce a confusión, utilizaremos la notación $\overline{a}$ para denotar la clase $[a+n\mathbb{Z}]$ de restos módulo n.

4. *Si A es un anillo, el conjunto $A[x]$ de los polinomios en una indeterminada con coeficientes en A es un anillo con la suma y el producto usuales de polinomios.*

Definición 1.1.3. *Un elemento a en un anillo A se dice que es **invertible**, o bien que es una **unidad**, si existe algún elemento $b \in A$ tal que $ab = 1$; es decir, a es invertible si tiene simétrico respecto al producto y a dicho elemento, que es único, se le denotará por a^{-1}. Al conjunto de unidades de A se le denotará A^*.*

*Un elemento a en un anillo A se dice que es un **divisor de cero** si existe un elemento $b \in A$, $b \neq 0$ tal que $ab = 0$. Un anillo sin divisores de cero no nulos se dice que es un **dominio de integridad** o, simplemente, un **dominio**.*

Notación: Si A es un anillo, $a \in R$ y $n \in \mathbb{N}$ usaremos las siguientes notaciones:

$$n\,a = \overbrace{a+\cdots+a}^{n \text{ veces}} \quad \text{y} \quad a^n = \overbrace{a\cdots a}^{n \text{ veces}}$$

y si $n \in \mathbb{Z}^-$, denotaremos

$$n\,a = \overbrace{(-a)+\cdots+(-a)}^{-n \text{ veces}}$$

Por último se tendrá que

$$0 \cdot a = 0 \quad \text{y} \quad a^0 = 1.$$

Con estas notaciones, a partir de las propiedades de asociatividad y distributividad, se tiene el siguiente resultado:

Proposición 1.1.4. *Sea A un anillo, entonces $\forall\, a, b \in A$ y $\forall\, m, n \in \mathbb{N}$ se cumplen las siguientes propiedades:*

1. $(ma)(nb) = (mn)(ab) = (na)(mb)$.
2. $(m+n)a = ma + na$.
3. $m(na) = (mn)a$.
4. $a^{m+n} = a^m a^n$.
5. $(a^m)^n = a^{mn}$.

Definición 1.1.5. *Se llama **característica** de un anillo A, y se denota $car(A)$, al menor entero positivo n tal que $n\,1 = 0$, o equivalentemente, al menor entero positivo tal que $1 + \overset{n}{\cdots} + 1 = 0$. Si tal entero no existe se dice que la característica del anillo es 0.*

Definición 1.1.6. *Un anillo en el que todo elemento no nulo es invertible se denomina **cuerpo**. Diremos que un cuerpo es **finito** si tiene un número finito de elementos.*

Ejemplos 1.1.7. *Anillos y cuerpos.*

1. *Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos, todos ellos de característica 0.*
2. *$\mathbb{Z}$ no es un cuerpo, aunque sea subanillo de los cuerpos anteriores.*
3. *Los anillos de polinomios no son cuerpos, pues el ideal generado por la indeterminada es un ideal propio y no nulo (ver A.2.13).*
4. *El conjunto con cuatro elementos $K = \{0, 1, \alpha, \alpha + 1\}$ es un cuerpo con las operaciones dadas por las tablas*

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Como un elemento invertible no es un divisor de cero, todo cuerpo es un dominio.
Veremos ahora bajo que condición el anillo de enteros módulo n, $\mathbb{Z}_n$, es un cuerpo:

Proposición 1.1.8. *$\mathbb{Z}_n$ es un cuerpo si y solo si n es un número entero primo.*

Demostración. $\Rightarrow$ Veremos esta implicación demostrando el contrarrecíproco. Supongamos que n no es un entero primo, entonces existen enteros n_1, n_2 con $1 < n_1, n_2 < n$ tales que $n = n_1 \cdot n_2$. Pero entonces $\bar{n_1}, \bar{n_2} \neq 0$ y $= \bar{n_1} \cdot \bar{n_2} = \bar{n} = \bar{0}$ en $\mathbb{Z}_n$. Así, $\mathbb{Z}_n$ no es un dominio, por lo que no puede ser un cuerpo.

$\Leftarrow$ Supongamos ahora que n es primo. Tenemos que ver que todo elemento no nulo de $\mathbb{Z}_n$ es invertible. Sea $\bar{a} \neq 0$ un elemento cualquiera de $\mathbb{Z}_n$. Entonces se tiene $0 < a < n$ y por ser n primo $mcd(a, n) = 1$. Ahora como $\mathbb{Z}$ es un DIP (ver [4], teorema 1.2.11 (página 15)), aplicando el resultado A.5.10, existen $s, t \in \mathbb{Z}$ con $s \neq 0$ tales que $1 = tn + sa$. Así, $sa \equiv 1 \bmod n$, por lo que $\bar{s}\bar{a} = \bar{s}\bar{a} = \bar{1}$ y en consecuencia $\bar{a}$ es una unidad de $\mathbb{Z}_n$. □

Observación 1.1.9. *Aplicando este resultado se tiene que $\mathbb{Z}_4$ no es un cuerpo, aunque como hemos visto en el punto 4 de los ejemplos anteriores sí que existen cuerpos finitos con 4 elementos.*

Proposición 1.1.10. *Si la característica de un cuerpo F es distinta de 0 entonces es un número primo.*

Demostración. Si un cuerpo F tiene característica $n \neq 0$ y no fuese un número primo, podría factorizarse como $n = n_1 n_2$ con $n_1, n_2 < n$. Entonces $(n_1\,1)(n_2\,1) = (n_1 n_2)\,1 = 0$, ahora por ser F un cuerpo no contiene divisores de 0 luego, $n_1\,1 = 0$ o $n_2\,1 = 0$, en contradicción con que n sea el menor entero positivo que cumple dicha condición. □

Proposición 1.1.11. *Todo cuerpo finito tiene característica p, donde p es un número primo.*

Demostración. Por el resultado anterior bastará ver que si F es un cuerpo finito entonces no tiene característica cero. Sea $1 \in F$ la identidad y consideremos los elementos $\{n\,1\}_{n\in\mathbb{N}}$. Como F contiene sólo un número finito de elementos, existen enteros k y m con $1 \leq k < m$ tales que $k\,1 = m\,1$, o equivalentemente $(m-k)\,1 = 0$; de donde se obtiene el resultado. □

Definición 1.1.12. *Un subanillo de un anillo A que sea además un cuerpo se denominará* ***subcuerpo*** *de A.*

Se llama ***subcuerpo primo*** *de un cuerpo F al menor subcuerpo de F; es decir, K es el subcuerpo primo de F si es subcuerpo de F y además está contenido en todos los subcuerpos de F*

Se tiene un resultado importante acerca de la característica de un cuerpo y su subcuerpo primo.

Proposición 1.1.13. *El subcuerpo primo de un cuerpo F es isomorfo a $\mathbb{Q}$ si la característica de F es 0 e isomorfo a $\mathbb{Z}_p$ si la característica de F es un entero primo p.*

Demostración. Ver [4], corolario 2.9.7 (página 57). □

1.2. Extensiones de cuerpos

En esta sección se abordarán resultados relacionados con las extensiones de cuerpos. Se llevará a cabo un estudio de definiciones, conceptos relacionados y propiedades de extensiones generales, que serán aplicados para obtener resultados específicos sobre cuerpos finitos.

Definición 1.2.1. *Una* ***extensión de cuerpos*** *es un par (K, F) donde F es un cuerpo y Kun subcuerpo de F. En lo sucesivo se denotará a una extensión de cuerpos de la forma F/K, aunque en algunos textos es denotada como $K \subseteq F$.*

LLamaremos ***cuerpo intermedio*** *de la extensión a todo subcuerpo de F que contenga a K.*

Todo cuerpo puede ser considerado como una extensión de un cuerpo que no tiene subcuerpos propios, su subcuerpo primo; que, como ya hemos visto, será isomorfo a $\mathbb{Q}$ si tiene característica cero o a $\mathbb{Z}_p$ si tiene característica p, que será un número primo.

Definición 1.2.2. *Sea F/K una extensión de cuerpos y S un subconjunto de F. A la intersección de todos los cuerpos intermedios de la extensión que contienen a S, que es el menor cuerpo intermedio de la extensión que contiene al conjunto S, lo denominaremos* ***cuerpo intermedio generado por S*** *y se denotará $K(S)$.*

Diremos que una extensión es ***finitamente generada*** *cuando existe un subconjunto finito $S \subseteq F$ tal que $F = K(S)$.*

Diremos que una extensión de cuerpos F/K es una extensión ***simple*** *si existe algún $\alpha \in F$ tal que $F = K(\alpha)$.*

Proposición 1.2.3. *Sea F/K una extensión de cuerpos. Entonces F es un espacio vectorial sobre K.*

Demostración. Es claro que la suma en F y el producto en F de elementos de K por elementos de F dotan a F de estructura de K- espacio vectorial. □

Definición 1.2.4. *A la dimensión de F como K-espacio vectorial se le llama* ***grado*** *de F sobre K.*

Definición 1.2.5. *Diremos que una extensión de cuerpos F/K es* ***finita*** *si F como espacio vectorial sobre Ktiene dimensión finita m, en cuyo caso llamaremos a m* ***grado*** *de la extensión y se denotará como $[F : K] = m$.*

El siguiente teorema es un teorema fundamental en la teoría de cuerpos y será muy útil en gran cantidad de resultados a lo largo de todo el texto.

Teorema 1.2.6 (Multiplicidad del grado)**.** *Sea F/K una extensión de cuerpos y L un cuerpo intermedio. Entonces F/K es finita si y solo si las extensiones F/L y L/K son ambas finitas. Y, en este caso, se verifica:*

$$[F : K] = [F : L] \cdot [L : K]$$

Demostración. $\Rightarrow$ Supongamos que F/K es finita. Como L es un subespacio vectorial de F sobre K claramente L/K es finita. Por otro lado si $\{\alpha_1, ..., \alpha_n\}$ es un conjunto generador de F como espacio vectorial sobre K , también lo será como espacio vectorial sobre L luego F/L es finita.

$\Leftarrow$ Supongamos que F/L y L/K son finitas y sean $\{\alpha_1, ..., \alpha_n\}$ y $\{\beta_1, ..., \beta_m\}$ bases de F como espacio vectorial sobre L y de L como espacio sobre K respectivamente; probaremos que $\{\alpha_j\beta_i : 1 \leq j \leq n, 1 \leq i \leq m\}$ es una base de F como espacio vectorial sobre K .

Si $\theta \in F$, por ser $\{\alpha_1, ..., \alpha_n\}$ una base de F como espacio vectorial sobre L se tiene que

$$\theta = \sum_{1 \leq j \leq n} b_j\alpha_j \text{ donde } b_j \in L \ \forall j = 1, ..., n$$

y, por ser $\{\beta_1, ..., \beta_m\}$ una base de L como espacio vectorial sobre K, para cada b_j se tendrá que

$$b_j = \sum_{1 \leq i \leq m} a_{ij}\beta_i \text{ donde } a_{ij} \in K \ \forall i = 1, ..., m$$

Sustituyendo estas expresiones en la anterior, se obtiene

$$\theta = \sum_{1 \leq j \leq n} b_j\alpha_j = \sum_{1 \leq j \leq n} \left(\sum_{1 \leq i \leq m} a_{ij}\beta_i \right) \alpha_j = \sum_{\substack{1 \leq j \leq n \\ 1 \leq i \leq m}} a_{ij}(\beta_i\alpha_j)$$

Hemos visto pues que $\{\alpha_j\beta_i : 1 \leq j \leq n, 1 \leq i \leq m\}$ es un conjunto generador; veamos ahora que es linealmente independiente. Sean $a_{ij} \in K$ tales que

$$\sum_{\substack{1 \leq j \leq n \\ 1 \leq i \leq m}} a_{ij}(\beta_i\alpha_j) = 0$$

Entonces por la independencia lineal de los α_j, se tiene que, para cada j,

$$\sum_{1 \leq i \leq m} a_{ij}\beta_i = 0$$

y de nuevo por la independencia lineal de los β_i, $a_{ij} = 0$ para todo $i = 1, ..., m$ y todo $j = 1, ..., n$. □

A continuación se introducirán una clase relevante de extensiones, las extensiones algebraicas, que tendrán gran importancia en el caso particular de cuerpos finitos.

Definición 1.2.7. *Sea una extensión de cuerpos F/K. Un elemento $\theta \in F$ se dice que θ es un elemento **algebraico** sobre K si existe un polinomio no nulo $p(x) \in K[x]$ tal que $p(\theta) = 0$.*

*Una extensión de cuerpos F/K se dice **algebraica** si todo elemento de F es algebraico sobre K.*

Proposición 1.2.8. *Sea $K(\alpha)/K$ una extensión simple con α algebraico sobre K, entonces:*

1. *Existe un polinomio mónico irreducible $f(x) \in K[x]$, único, tal que $f(\alpha) = 0$. A este polinomio se le denominará* ***polinomio mínimo de*** α ***sobre*** K.
2. *$[K(\alpha) : K] = n = \deg(f(x))$ (grado del polinomio mínimo de α sobre K).*
3. *Si $g(x) \in K[x]$ y $g(\alpha) = 0$, entonces $f(x)|g(x)$.*
4. *$\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ sobre K.*
5. *Todo elemento de $K(\alpha)$ se escribe de forma única como $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ con los $a_i \in K$.*

Demostración. Si se considera el homomorfismo de evaluación en α, $\varphi_\alpha : K[x] \longrightarrow K(\alpha)$, definido por $\varphi_\alpha(h(x)) = h(\alpha)$, se tendrá que $Im(\varphi_\alpha) = K[\alpha]$, el menor subanillo de $K(\alpha)$ que contiene a K y a α y, al ser α algebraico sobre K, $Ker(\varphi_\alpha) \neq 0$.

Como $K[x]$ es un DIP (ver A.7.13), existirá un polinomio $f(x) \in K[x]$, único si se le exige ser mónico, tal que $Ker(\varphi_\alpha) = (f(x))$. En estas condiciones, aplicando el primer teorema de isomorfía (A.4.7) se tiene $K[x]/(f(x)) \cong K[\alpha]$ que es un dominio de integridad, por lo que por el resultado A.5.9, $f(x)$ es un polinomio irreducible lo que demuestra 1. Además por la misma proposición $(f(x))$ es un ideal maximal por lo que por el isomorfismo dado, $K[\alpha]$ será un cuerpo y, por ser $K(\alpha)$ el menor cuerpo que contiene a K y α, se tiene que $K(\alpha) = K[\alpha]$ y la aplicación es suprayectiva.

Ahora si $g(x) \in K[x]$,

$$g(\alpha) = 0 \Longleftrightarrow g(x) \in Ker(\varphi_\alpha) = (f(x)) \Longleftrightarrow f(x)|g(x)$$

lo que prueba 3.

Sea $n = \deg(f(x))$. Para probar 4, si $\sum_{i=0}^{n-1} a_i\alpha^i = 0$ con los $a_i \in K$ y se considera el polinomio $g(x) = \sum_{i=0}^{n-1} a_i x^i \in K[x]$, entonces $g(\alpha) = 0$ por lo que $f(x)|g(x)$, pero como $g(x)$ tiene grado estrictamente menor que $f(x)$ debe ser $g(x) = 0$ y $a_i = 0$ para todo i, luego $\{1, \alpha, \ldots, \alpha^{n-1}\}$ son linealmente independientes sobre K.

Por otro lado, si $\beta \in K(\alpha)$, como la aplicación es suprayectiva, existe $h(x) \in K[x]$ tal que $\beta = h(\alpha)$. Dado $h(x)$ por el resultado A.7.16, existirán $q(x), r(x) \in K[x]$ tales que $h(x) = f(x)q(x) + r(x)$, con $r(x) = 0$ o $\deg(r(x)) < n$, por lo que, en cualquier caso,

$$\beta = h(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) \in < 1, \alpha, \ldots, \alpha^{n-1} > .$$

Se ha demostrado que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es también un sistema de generadores y, por tanto, una base de $K(\alpha)$ sobre K. Las propiedades 2 y 5 son, entonces, consecuencia de este hecho. □

Aplicando esta última proposición y el teorema de multiplicidad del grado se obtiene el siguiente resultado:

Corolario 1.2.9. *Sea F/K una extensión de cuerpos finita y $\alpha \in F$. Se verifica que el polinomio mínimo de α sobre K tiene grado un divisor de $[F : K]$.*

El siguiente resultado proporcionará una caracterización para las extensiones de cuerpos finitas.

Proposición 1.2.10. *Sea F/K una extensión de cuerpos. Las siguientes afirmaciones son equivalentes:*

1. *F/K es finita.*
2. *F/K algebraica y finitamente generada.*
3. *F/K está generada por un conjunto finito de elementos algebraicos.*

Demostración. Ver [1], proposiciones 2.3.16 y 2.3.17 (página 43). □

Definición 1.2.11. *Un cuerpo F se llama **algebraicamente cerrado** si no existen extensiones algebraicas propias de F. Es decir, si L/F es una extensión algebraica ello obliga a que $L = F$.*

Definición 1.2.12. *Sea K un cuerpo. Una extensión F/K se dice una clausura algebraica (de K) cuando se verifican las dos condiciones siguientes:*

1. *F es algebraicamente cerrado.*
2. *F/K es una extensión algebraica.*

Teorema 1.2.13. *Para todo cuerpo K existe una clausura algebraica de K y además es única salvo K-isomorfismos.*

Demostración. Ver [1], teorema 4.1.12 (página 62) y corolario 4.1.18 (página 64). □

Observación 1.2.14. *Como consecuencia de la existencia y unicidad de la clausura algebraica de cualquier cuerpo K, se tiene que, para cada polinomio $f(x) \in K[X]$ existe una determinada extensión de K en la que dicho polinomio tiene todas sus raíces. El cuerpo generado sobre K por dichas raíces, denominado el **cuerpo de escisión** de $f(x)$ sobre K es, además, único salvo K-isomorfismos (ver Teorema A.7.26).*

1.3. Cuerpos finitos. Existencia y unicidad

La presente sección tiene por objetivo la obtención de dos resultados clave en la teoría de cuerpos finitos: el teorema de existencia y unicidad de cuerpos de finitos y el teorema de estructura. El teorema de existencia y unicidad establece que para cada potencia de primo p^n existe un único cuerpo (salvo isomorfismos) que contiene este número de elementos. Por su parte el teorema de estructura caracterizará los subcuerpos de un cuerpo finito de p^n elementos precisamente como aquellos cuerpos de p^m elementos donde, m es un divisor de n . Para obtener estos resultados será necesario introducir ciertos conceptos y obtener algunas propiedades previas.

Proposición 1.3.1. *Sean F un cuerpo finito y K un subcuerpo de F con q elementos. Entonces $|F|=q^m$, donde $m = [F : K]$, es la dimensión de F como K-espacio vectorial.*

Demostración. Como F es finito, ha de ser, necesariamente, de dimensión finita sobre K; por lo que podemos tomar una base B= $\{\beta_1, ..., \beta_m\}$ de F sobre K. Así todo elemento $\alpha \in F$ puede expresarse de modo único de la forma:

$$\alpha = a_1\beta_1 + \cdots + a_m\beta_m \text{ con } a_i \in K \text{ para todo } i = 1, .., m$$

y α está unívocamente determinado por la m-upla $(a_1, ..., a_m)$. Como K tiene q elementos, habrá q^m m-uplas distintas de elementos de K; y, por tanto, $|F|=q^m$. □

Teorema 1.3.2. *Sea F un cuerpo finito. El cardinal de F es p^m, donde p es la característica de F y m es el grado de F sobre su subcuerpo primo.*

Demostración. Aplicando la proposición 1.1.13, tenemos que el subcuerpo primo de F es isomorfo a $\mathbb{Z}_p$; por lo que contiene p elementos y el resultado se sigue de la proposición anterior. □

Notación: En lo sucesivo denotaremos, salvo que se especifique lo contrario, como q al número de elementos de un cuerpo finito, teniendo presente que $q = p^r$ donde p será siempre un número primo y $r \in \mathbb{N}$.

Lema 1.3.3. *Si F es un cuerpo finito con q elementos y $a \in F$ es un elemento no nulo entonces $a^{q-1} = 1$, por tanto $a^q = a$ para cada a no nulo.*

Demostración. Si $a \in F$ es un elemento no nulo entonces a es invertible por ser F un cuerpo. Sabemos que existen $q-1$ unidades. Aplicando teorema de Lagrange (A.1.5) el orden multiplicativo de a divide a $q-1$ y por tanto $a^{q-1} = 1$. □

Observación 1.3.4. *Para todo $a \in F$, con $a \neq 0$, donde F es un cuerpo de orden q tendremos que a^{q-2} será inverso de a pues $a^{q-2}a = a^{q-1} = 1$.*

Observación 1.3.5. *El polinomio $x^q - x$ tiene grado q, por tanto tendrá a lo sumo q raíces en cualquier cuerpo por el teorema A.7.12. Del lema anterior se deduce que si F es un cuerpo de orden q todo elemento de F es raíz de $x^q - x$.*

De la observación anterior, se obtiene inmediatamente el siguiente lema:

Lema 1.3.6. *Si F es un cuerpo finito con q elementos se tiene la siguiente factorización del polinomio $x^q - x$ en $F[x]$:*

$$x^q - x = \prod_{a \in F} (x - a)$$

Una vez obtenidos estos resultados estamos en disposición de enunciar el siguiente teorema clave en la teoría de cuerpos finitos:

Teorema 1.3.7 (Existencia y unicidad de cuerpo finitos)**.** *Para cada número primo p y cada entero positivo $n \geq 1$ existe un cuerpo finito con p^n elementos. Además cualquier cuerpo finito con p^n elementos es isomorfo al cuerpo de escisión del polinomio $x^{p^n} - x$ sobre Z_p.*

Demostración. Veamos en primer lugar la parte de existencia. Tomemos $q = p^n$ con p primo y un entero $n \geq 1$. Consideremos el polinomio $r(x) = x^q - x$ con coeficientes en Z_p y sea F el cuerpo de escisión de $r(x)$ sobre $\mathbb{Z}_p$. Tomemos ahora el conjunto $S = \{a \in F : a^q - a = 0\}$. Observemos que el polinomio derivado de $r(x)$ es $r'(x) = qx^{q-1} - 1 = -1$ en $\mathbb{Z}_p$, por lo que $r(x)$ no tiene raíces múltiples en virtud de la proposición A.7.11 y por tanto $|S| = q$. Veamos ahora que S es un subcuerpo de F:

- Es claro que $0, 1 \in S$.
- Sean $a, b \in S$. Entonces por los resultados 1.3.3 y A.2.15:

$$(a-b)^q - (a-b) = a^q - b^q - (a-b) = a - b - (a-b) = 0$$

por lo que $a - b \in S$.

- Sean $a, b \in S$ con $b \neq 0$. Entonces:

$$(ab^{-1})^q - ab^{-1} = a^q b^{-q} - ab^{-1} = ab^{-1} - ab^{-1} = 0$$

de donde $ab^{-1} \in S$.

Luego en efecto S es un subcuerpo de F por la proposición A.2.10. Pero además, por el lema anterior, $x^q - x$ se escinde en S , por lo que $F = S$ es un cuerpo con $q = p^n$ elementos.

Veamos ahora la unicidad. Si F es un cuerpo con p^n elementos, entonces F debe tener característica p y contendrá a $\mathbb{Z}_p$ como subcuerpo. Por tanto aplicando de nuevo el lema anterior F es el cuerpo de escisión de $x^{p^n} - x$ sobre $\mathbb{Z}_p$ y por la unicidad del cuerpo de escisión salvo $\mathbb{Z}_p$-isomorfismos (teorema A.7.26) se obtiene el resultado. □

Observación 1.3.8. *Del teorema anterior obtenemos que el cuerpo de un determinado número de elementos es único salvo isomorfismo de cuerpos. Esto nos permitirá en lo sucesivo hablar 'del' cuerpo finito de orden q y se denotará F_q.*

Observación 1.3.9. *El resultado 1.1.8 junto con el teorema de existencia y unicidad de cuerpos finitos muestra que el cuerpo F_{p^m} es isomorfo a $\mathbb{Z}_{p^m}$ si y solo si $m = 1$ pues en caso contrario $\mathbb{Z}_{p^m}$ no será un cuerpo.*

El objetivo ahora será demostrar otro importante teorema en la teoría de cuerpos finitos, el teorema de estructura, para lo que será necesario un resultado previo:

Lema 1.3.10. *Sean $n, m \in \mathbb{N}$ y sea p un entero primo positivo. Entonces si m es divisor de n el polinomio $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$.*

Demostración. Si m divide a n , $n = md$ para cierto entero $d \in \mathbb{N}$. Sea α una raíz de $x^{p^m-1} - 1$, en una clausura algebraica, si vemos que α es raíz de $x^{p^n-1} - 1$ habremos terminado. Se tiene:

$$p^n - 1 = p^{md} - 1 = (p^m - 1)\left(p^{m(d-1)} + p^{m(d-2)} + \cdots + p^m + 1\right)$$

Por lo que, teniendo en cuenta que $\alpha^{p^m-1} = 1$:

$$\alpha^{p^n-1} = \alpha^{(p^m-1)\left(p^{m(d-1)}+p^{m(d-2)}+\cdots+p^m+1\right)} = 1^{\left(p^{m(d-1)}+p^{m(d-2)}+\cdots+p^m+1\right)} = 1$$

□

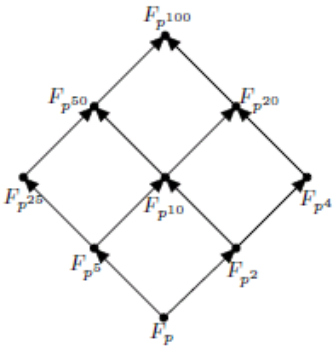
Teorema 1.3.11 (Estructura de subcuerpos)**.** *Sea F_{p^n} un cuerpo finito con p^n elementos. Se verifica que cada subcuerpo de F_{p^n} tiene p^m elementos para algún entero positivo m divisor de n. Recíprocamente para cualquier entero positivo m divisor de n existe un único subcuerpo de F_{p^n} de orden p^m.*

Demostración. Veamos en primer lugar que, en efecto, cualquier subcuerpo de F_{p^n} tiene p^m elementos con m divisor de n. Un subcuerpo K deberá tener p^m elementos distintos con $m \leq n$. Aplicando la proposición 1.3.1 se obtiene que p^n debe ser potencia de p^m, por lo que m divide a n .

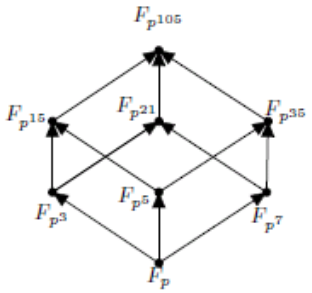
Veamos el recíproco. Supongamos que m divide a n . Aplicando el lema anterior $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$ y en consecuencia, $x^{p^m} - x$ divide a $x^{p^n} - x$, por lo que

toda raíz de $x^{p^m} - x$ será raíz de $x^{p^n} - x$. Por tanto F_{p^n} contiene al cuerpo de escisión de $x^{p^m} - x$ sobre F_p y dicho cuerpo de escisión contiene exactamente p^m elementos distintos utilizando el mismo razonamiento que en la prueba del teorema de existencia y unicidad de cuerpos finitos.
Por último, la unicidad es consecuencia de que un cuerpo contiene un único subcuerpo de escisión de un polinomio que se escinda completamente en él. □

Ejemplos 1.3.12. *Los siguientes diagramas son ejemplos de retículos de subcuerpos de determinados cuerpos finitos.*



Subcuerpos de $F_{p^{100}}$



Subcuerpos de $F_{p^{105}}$

Observación 1.3.13. *Dado el cuerpo F_q, considerando el cuerpo de escisión del polinomio $x^{q^m} - x$ sobre F_q, tendremos un cuerpo finito de q^m que contiene a F_q.*

La siguiente proposición permitirá obtener que el grupo de las unidades de un cuerpo finito es cíclico:

Proposición 1.3.14. *Sea K un cuerpo y G un subgrupo del grupo multiplicativo de todos los elementos no nulos de G. Entonces si G es finito, G es cíclico*

Demostración. Supongamos $|G| = n$. Por ser K un cuerpo G es abeliano, luego por la proposición A.1.8 obtenemos que :

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s} \text{ con cada } d_i \geq 1 \text{ y } d_i | d_{i+1} \text{ para } i = 1, ..., s-1$$

por lo que se tiene $n = d_1 \cdots d_s$. Hay que ver que $s = 1$. Utilizando notación multiplicativa, identificaremos $\mathbb{Z}_{d_i}$ con C_{d_i}, donde este último es un grupo cíclico de orden d_i.
Cada elemento de C_{d_i} satisface $g^{d_i} = 1 = g^{d_s}$, pues $d_i | d_s$. Por tanto, todo elemento $a \in C_{d_1} \times \cdots \times C_{d_s}$ cumple:

$$a^{d_s} = (a_1, ..., a_s)^{d_s} = (1, ..., 1)$$

y por el isomorfismo con G, $g^{d_s} = 1 \ \forall g \in G$.
Pero entonces todo $g \in G \subseteq K$ es solución de $x^{d_s} - 1 = 0$, y como G tiene n elementos, tenemos que $d_s \geq n$. Ahora bien, $n = d_1 \cdots d_s$, luego $n = d_s$ y $s = 1$. □

Resulta como corolario inmediato el siguiente resultado, que será clave para la demostración de resultados posteriores:

Corolario 1.3.15. *El grupo multiplicativo* $\left(F_q^*, \cdot\right)$ *de las unidades de un cuerpo* F_q *es cíclico.*

Definición 1.3.16. *Un elemento de* F_q *que genere el grupo multiplicativo* F_q^* *de las unidades de* F_q *recibirá el nombre de* ***elemento primitivo****.*

Veamos ahora dos resultados relacionados con el orden de elementos de un grupo y elementos primitivos:

Lema 1.3.17. *Sea* $g \in G$ *un elemento de orden finito* n *de un grupo* G *y sea* k *un número entero. Se verifica la siguiente fórmula:*

$$o\left(g^k\right) = \frac{n}{mcd\left(n,k\right)}$$

Demostración. Sea $s := o\left(g^k\right)$. Como $1 = \left(g^k\right)^s = g^{ks}$ se deduce que n divide a ks , por lo que podemos escribir $nn_1 = ks$. Sea $d = mcd\left(n,k\right)$. Entonces $\frac{k}{d}s = \frac{n}{d}n_1$, y como $mcd\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ se tiene que $\frac{n}{d}$ divide a s . Por otro lado $\left(g^k\right)^{\frac{n}{d}} = g^{\frac{kn}{d}} = \left(g^n\right)^{\frac{k}{d}} = 1$ de donde s divide a $\frac{n}{d}$, luego

$$s = \frac{n}{d} = \frac{n}{mcd\left(n,k\right)}.$$

□

Directamente de la aplicación de esta fórmula y el hecho de que un elemento primitivo tiene orden $q-1$ en el grupo F_q^* se obtiene el siguiente resultado:

Proposición 1.3.18. *Si* g *es un elemento primitivo de* F_q *entonces* g^t *es un elemento primitivo de* F_q *si y solo si* $mcd\left(q-1,t\right) = 1$*.*

1.4. Extensiones finitas de cuerpos finitos

A continuación se mostrará una importante propiedad de los cuerpos finitos, no compartida en general por cuerpos arbitrarios.

Proposición 1.4.1. *Sea* F_r/F_q *una extensión finita de cuerpos. Se tiene que* F_r/F_q *es una extensión simple y algebraica y además para cualquier elemento primitivo* $\theta \in F_r$ *se cumple que* $F_r = F_q\left(\theta\right)$*.*

Demostración. Que la extensión sea algebraica se tiene en virtud de la proposición 1.2.10. Veamos entonces que la extensión es simple comprobando que está generada por cualquier elemento primitivo:

Sea θ un elemento primitivo de F_r. Como $F_q \subseteq F_r$ y $\theta \in F_r$, se tiene que $F_q\left(\theta\right) \subseteq F_r$. Por otro lado, $F_q\left(\theta\right)$ contiene a 0, θ y todas las potencias de θ, luego $F_r \subseteq F_q\left(\theta\right)$ por ser θ un elemento primitivo de F_r. En consecuencia $F_r = F_q\left(\theta\right)$, como se quería demostrar. □

Corolario 1.4.2. *Para cualquier potencia de primo* q *y cualquier entero* $n \geq 1$ *existe un polinomio irreducible de grado* n *sobre* F_q*.*

Demostración. Basta tomar el polinomio mínimo sobre F_q de un elemento primitivo en un cuerpo de escisión, F_{q^n}, de $x^{q^n} - x$ sobre F_q. □

Aunque el tema de polinomios sobre cuerpos finitos se abordará con mayor detalle en el siguiente capítulo, a continuación se enunciarán algunos resultados necesarios para seguir profundizando en la teoría de extensiones de cuerpos.

Lema 1.4.3. *Sea $f(x) \in F_q[x]$ un polinomio irreducible de grado m. Entonces f divide al polinomio $x^{q^n} - x$ si y solo si m divide a n .*

Demostración. $\Leftarrow$ Supongamos que m divide a n. Entonces por teorema de estructura (1.3.11), F_{q^m} es un subcuerpo de F_{q^n}. Sea α una raíz de f , se tiene pues que $[F_q(\alpha) : F_q] = m$. Ahora bien aplicando de nuevo el teorema de estructura existe un único subcuerpo de q^m elementos, luego podemos escribir $F_q(\alpha) = F_{q^m}$ y como consecuencia de la observación 1.3.5 todo elemento de F_{q^m} es raíz de $x^{q^m} - x$. Pero por hipótesis m divide a n, luego aplicando lema 1.3.10, $x^{q^m} - x$ divide a $x^{q^n} - x$ y así $\alpha^{q^n} - \alpha = 0$ en F_{q^m}. Hemos obtenido entonces que toda raíz de f es raíz de $x^{q^n} - x$ y por tanto que f divide a $x^{q^n} - x$.
$\Rightarrow$ Supongamos que f divide a $x^{q^n} - x$ y sea α una raíz de f. Tenemos la torre de cuerpos:

$$F_q \subseteq F_q(\alpha) \subseteq F_{q^n}$$

El resultado se obtiene entonces de la aplicación del teorema de multiplicidad del grado pues:

$$n = [F_{q^n} : F_q] = [F_{q^n} : F_q(\alpha)]\,[F_q(\alpha) : F_q] = [F_{q^n} : F_q(\alpha)] \cdot m$$

□

El resultado siguiente permitirá la descripción de las raíces de un polinomio irreducible sobre un cuerpo finito:

Proposición 1.4.4. *Si $f(x) \in F_q[x]$ es un polinomio irreducible de grado m sobre F_q entonces $f(x)$ tiene alguna raíz $\alpha \in F_{q^m}$. Es más, todas la raíces de f son simples y son exactamente $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$.*

Demostración. Sea α una raíz de f en su cuerpo de escisión sobre F_q.
Como $[F_q(\alpha) : F_q] = m$ utilizando un razonamiento análogo al de la demostración anterior α es un elemento de $F_{q^m} = F_q(\alpha)$.
Escribamos ahora $f(x) = \sum_{i=0}^{m} a_i x^i$ donde $a_i \in F_q$ y sea β una raíz cualquiera de f . Observemos que:

$$f\left(\beta^q\right) = \sum_{i=0}^{m} a_i \left(\beta^q\right)^i = \sum_{i=0}^{m} a_i^q \left(\beta^q\right)^i = \left(\sum_{i=0}^{m} a_i \beta^i\right)^q = 0$$

Luego β^q es también una raíz de f . Análogamente se comprueba que β^{q^j} es raíz de f para $j > 0$. Veamos ahora que en efecto las raíces son simples, es decir, vamos a ver que para $1 \leq i < j < m$ se tiene que $\beta^{q^i} \neq \beta^{q^j}$. Supongamos por reducción al absurdo que $\beta^{q^i} = \beta^{q^j}$, elevando ambos miembros a q^{m-j} obtenemos que $\beta^{q^{i+m-j}} = \beta^{q^m} = \beta$. Pero entonces β es tambíen una raíz de $x^{q^{i+m-j}} - x$, por lo que aplicando lema anterior m divide a $(i + m - j)$ y así i y j son congruentes módulo m , obteniéndose una contradicción pues $1 \leq i < j < m$. □

Como consecuencia se obtiene el siguiente resultado :

Corolario 1.4.5. *Sea $f \in F_q[x]$ un polinomio irreducible de grado m. Se tiene que F_{q^m} es el cuerpo de escisión de f sobre F_q.*

Definición 1.4.6. *Sea una extensión de cuerpos F_{q^m}/F_q y sea $\alpha \in F_{q^m}$. A los elementos $\alpha, \alpha^q, ..., \alpha^{q^{m-1}}$ se les denomina **conjugados** α sobre F_q.*

A partir de la proposición 1.4.4 y la definición de conjugados de un elemento $\alpha \in F_{q^m}$ se obtiene el siguiente resultado:

Proposición 1.4.7. *Sea $\alpha \in F_{q^m}$, sea $f(x)$ el polinomio mínimo de α sobre F_q y denotemos d al grado de dicho polinomio (que como ya se ha visto anteriormente será divisor de m). Consideremos el conjunto $\alpha, \alpha^q, ..., \alpha^{q^{m-1}}$ de conjugados de α. Entonces si m=d los elementos de dicho conjunto son distintos, en otro caso cada conjugado estará repetido m/d veces.*

Proposición 1.4.8. *Sea $\alpha \in F_q^*$. Se tiene que todos los conjugados de α sobre cualquier subcuerpo de F_q tienen el mismo orden en el grupo F_q^*.*

Demostración. Recordemos que consideramos $q = p^r$ donde p es un número primo y r un entero positivo. Observando que el máximo común divisor de una potencia de p y $q - 1 = p^r - 1$ es igual a 1 el resultado es consecuencia entonces de la fórmula que proporciona el lema 1.3.17. □

Corolario 1.4.9. *Si $\alpha \in F_q^*$ es un elemento primitivo entonces los conjugados de α con respecto a cualquier subcuerpo son también elementos primitivos.*

El siguiente resultado proporciona la descripción explícita del conjunto de automorfismos de un cuerpo finito:

Teorema 1.4.10. *Los distintos F_q-automorfismos de F_{q^m} vienen dados por las funciones $\sigma_0, ..., \sigma_{m-1}$ donde $\sigma_j : F_{q^m} \longrightarrow F_{q^m}$ está definida por $\sigma_j(\alpha) = \alpha^{q^j}$ para cada $\alpha \in F_{q^m}$ con $0 \leq j \leq m - 1$.*

Demostración. Veamos en primer lugar que en efecto dichas aplicaciones son F_q-automorfismos de F_{q^m}. Para cada σ_j y cada $\alpha, \beta \in F_{q^m}$, es claro que se verifica

$$\sigma_j(\alpha\beta) = (\alpha\beta)^{q^j} = (\alpha)^{q^j}(\beta)^{q^j} = \sigma_j(\alpha)\sigma_j(\beta)$$

y además también

$$\sigma_j(\alpha + \beta) = (\alpha + \beta)^{q^j} = (\alpha)^{q^j} + (\beta)^{q^j} = \sigma_j(\alpha) + \sigma_j(\beta)$$

por la relación que proporciona el lema A.2.15, luego se tiene que σ_j es un endomorfismo de F_{q^m}. Ahora, como F_{q^m} es un cuerpo, no contiene divisores de cero luego $Ker(\sigma_j) = 0$; por lo que aplicando la proposición A.4.5 es una aplicación inyectiva. Tenemos pues, una aplicación inyectiva de un conjunto finito en sí mismo, por lo que σ_j será también suprayectiva y en consecuencia es un automorfismo de F_{q^m}. Veamos por último que, en efecto, deja fijos los elementos de F_q. Sea $a \in F_q$, entonces $\sigma_j(a) = a^{q^j} = a$ en virtud del lema 1.3.3. Ya hemos comprobado entonces que cada σ_j es un F_q-automorfismo de F_{q^m}.

En los últimos resultados se ha comprobado que si β es un elemento primitivo de F_{q^m} y se tiene $i \neq j \in \{0, ..., m-1\}$ entonces $\beta^{q^i} \neq \beta^{q^j}$, luego $\sigma_i \neq \sigma_j$ para $i \neq j$. Veamos por último que todo F_q-automorfismo de F_{q^m} es precisamente de esta forma. Sea σ un F_q-automorfismo de F_{q^m} arbitrario, $\beta \in F_{q^m}$ un elemento primitivo y sea $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 \in F_q[x]$ su polinomio mínimo sobre F_q. Entonces

$$0 = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0) = \sigma(\beta)^m + \sigma(\beta)^{m-1} + \cdots + a_0$$

por lo que $\sigma(\beta)$ es también una raíz de f en F_{q^m}. Aplicando ahora proposición 1.4.4 se tendrá $\sigma(\beta) = \beta^{q^k}$ para cierto k con $0 \leq k \leq m - 1$. En consecuencia $\sigma = \sigma_k$, pues un automorfismo de un cuerpo finito está completamente determinado por su acción sobre un elemento primitivo. □

A continuación pasaremos a la definición del llamado *grupo de Galois* de una extensión de cuerpos.

Definición 1.4.11. *Sea una extensión de cuerpos F/K. Se llama* ***grupo de Galois*** *de dicha extensión, y se denotará $Gal\,(F/K)$, al conjunto de K-automorfismos de F con la composición de aplicaciones.*

El objetivo en lo que resta de capítulo será demostrar que el grupo de Galois de un extensión de cuerpos finitos es cíclico, algo que no ocurre para extensiones de cuerpos arbitrarias, para lo que será necesaria la introducción de tres nuevas clases de extensiones de cuerpos: extensiones separables, extensiones normales y extensiones de Galois. Se demostrarán aquellos resultados relacionados con los cuerpos finitos, remitiendo el resto de resultados generales a textos de la bibliografía.

Definición 1.4.12. *Sea F/K una extensión de cuerpos algebraica, sea $f(x) \in K\,[x]$ un polinomio no constante y $\alpha \in F$ un elemento arbitrario. Diremos que:*

1. *El polinomio f es* ***separable*** *si no tiene raíces múltiples en una clausura algebraica de K.*

2. *α es un elemento* ***separable*** *sobre K si su polinomio mínimo es un polinomio separable.*

3. *La extensión F/K es* ***separable*** *si todo elemento de F es separable sobre K.*

Proposición 1.4.13. *Sea F/K una extensión finita y sea L una clausura algebraica de F (y por tanto también de K). El conjunto de los K-homomorfismos de cuerpos $f : F \longrightarrow L$ es finito y su cardinal, denotado por $[F : K]_s$ y llamado* ***grado de separabilidad*** *de F/K, es menor o igual que $[F : K]$.*

Demostración. Ver [1], proposición 7.2.4 (página 89). □

Proposición 1.4.14. *Las siguientes condiciones son equivalentes para una extensión de cuerpos finita F/K:*

1. *F/K es separable.*

2. *$[F : K]_s = [F : K]$.*

Demostración. Ver [1], proposición 7.2.7 (página 90). □

A continuación introduciremos los conceptos de transitividad y estabilidad por levantamientos de una clase de extensiones de cuerpos:

Definición 1.4.15. *Diremos que una clase de extensiones de cuerpos P es* ***transitiva*** *si dada una torre de cuerpos $K \subseteq L \subseteq F$ tales que L/K y F/L son extensiones en la clase P, entonces se tiene también que F/K está en la clase P.*

Diremos que una clase de extensiones de cuerpos P es ***estable por levantamientos*** *si dada cualquier extensión de cuerpos F/K y cuerpos intermedios L_1, L_2, tales que L_1/K es una extensión de P, entonces también L_1L_2/L_2 es una extensión de P.*

Proposición 1.4.16. *La clase de las extensiones separables es transitiva y estable por levantamientos.*

Demostración. Ver [1], proposición 7.3.2 (página 91). □

Definición 1.4.17. *Un cuerpo K se dice **perfecto** cuando todo polinomio irreducible de $K[x]$ es separable, o, equivalentemente, cuando toda extensión algebraica F/K es separable.*

Proposición 1.4.18. *Todo cuerpo finito es perfecto.*

Demostración. Consecuencia de la proposición 1.4.4 y la definición de cuerpo perfecto. □

Definición 1.4.19. *Sea F/K una extensión algebraica y sea L una clausura algebraica de F. Decimos que F/K es una **extensión normal** si todo K-homomorfismo $\sigma : F \longrightarrow L$ cumple $\sigma(F) \subseteq F$.*

Proposición 1.4.20. *Sea F/K una extensión algebraica. Las siguientes condiciones son equivalentes:*

1. *F/K es una extensión normal.*
2. *Todo polinomio irreducible $f(x) \in K[x]$ que tenga una raíz en F se escinde sobre F.*
3. *F es cuerpo de escisión sobre K de algún conjunto de polinomios no constantes de $K[x]$.*

Demostración. Ver [2], teorema 2.1, capítulo 16 (página 295). □

Proposición 1.4.21. *Sea $K \subseteq E \subseteq F$ una torre de cuerpos. Entonces si F/K es normal, F/E también es normal.*

Demostración. Ver [1], corolario 6.1.8 (página 83). □

Nota: Esta última proposición no determina la transitividad de las extensiones normales. La clase de las extensiones normales NO es transitiva.

Proposición 1.4.22. *La clase de las extensiones normales es estable por levantamientos.*

Demostración. Ver [1], proposición 6.1.9 (página 83). □

Veamos por último la definición de extensión de Galois y algunas de sus propiedades:

Definición 1.4.23. *Sea F/K una extensión algebraica. Se dice que F/K es una **extensión de Galois** si es normal y separable.*

Proposición 1.4.24. *Sea F/K una extensión de Galois y sea M un cuerpo intermedio de la misma. Entonces la extensión F/M es de Galois.*

Demostración. Ver [1], teorema 5.3.6 (página 76). □

Proposición 1.4.25. *Sea F/K una extensión finita. Las siguientes condiciones son equivalentes:*

1. *F/K es de Galois.*
2. *$[F : K] = |Gal(F/K)|$*

Demostración. Ver [2], teorema 1.6, capítulo 17 (página 316). □

Definición 1.4.26. *Una extensión de cuerpos F/K se dice que es* ***cíclica*** *cuando es finita, de Galois y su grupo $Gal\,(F/K)$ es cíclico.*

Estamos, ahora sí, en condiciones de enunciar y demostrar el resultado buscado:

Teorema 1.4.27. *Toda extensión de cuerpos finitos es una extensión cíclica.*

Demostración. Sea F_{q^m}/F_q una extensión de cuerpos finitos donde recordemos $q = p^r$ con p número primo y $r \geq 1$.

Consideremos la extensión $F_{q^m}/\mathbb{Z}_p$. Habíamos visto en la proposición 1.4.18 que todo cuerpo finito es perfecto, así que la extensión es separable y además por el teorema de existencia y unicidad de cuerpos finitos (1.3.7), F_{q^m} es isomorfo al cuerpo de escisión del polinomio $x^{q^m} - x$ sobre $\mathbb{Z}_p$, por lo que aplicando la proposición 1.4.20 es también una extensión normal y, en consecuencia, es una extensión de Galois. Observemos ahora que se tiene la torre de cuerpos

$$\mathbb{Z}_p \subseteq F_q \subseteq F_{q^m}$$

por lo que aplicando la proposición 1.4.24, la extensión F_{q^m}/F_q es de Galois.

Tenemos que ver ahora que $Gal\,(F_{q^m}/F_q)$ es cíclico; pero como

$$Gal\,(F_{q^m}/F_q) < Gal\,(F_{q^m}/\mathbb{Z}_p)\,,$$

por el lema A.1.7, los subgrupos de un grupo cíclico son cíclicos, bastará ver que $Gal\,(F_{q^m}/\mathbb{Z}_p)$ es un grupo cíclico. Consideremos el autormorfismo $\phi : F_{q^m} \longrightarrow F_{q^m}$ dado por $\phi(\alpha) = \alpha^p$. Denotando $n := [F_{q^m} : Z_p]$, se tendrá $q^m = p^n$, por lo que por el lema 1.3.3

$$\phi^n(\alpha) = \alpha^{p^n} = \alpha \text{ para todo } \alpha \in F_{q^m}$$

y en consecuencia ϕ^n es la aplicación identidad en F_{q^m}. Supongamos ahora que ϕ^k es igual a la aplicación identidad para cierto $k < n$. Entonces el polinomio $x^{p^k} - x$ tendría p^n raíces distintas (todos los elementos de F_{q^m}) lo cual no es posible. Así, el orden de ϕ es n y como por la proposición 1.4.25 se verifica la igualdad

$$|Gal\,(F_{q^m}/\mathbb{Z}_p)| = [F_{q^m} : \mathbb{Z}_p]$$

se tiene que $Gal\,(F_{q^m}/\mathbb{Z}_p) = \langle\phi\rangle$, es decir, la extensión es cíclica. □

Observación 1.4.28. *Análogamente a como se ha visto en la demostración del teorema anterior, si tenemos una extensión de cuerpos finitos arbitraria F_q^m/F_q, entonces el F_q-automorfismo $\sigma : F_{q^m} \longrightarrow F_{q^m}$ dado por $\sigma(\alpha) = \alpha^q$ genera el grupo $Gal\,(F_{q^m}/F_q)$. Dicho automorfismo recibirá el nombre de* ***automorfismo de Frobenius****. Los conjugados de un elemento $\alpha \in F_{q^m}$ serán por tanto los elementos obtenidos de la aplicación sucesiva del automorfismo de Frobenius sobre α.*

1.5. Traza y norma

A lo largo de esta sección, con el objeto de simplificar la notación, convendremos salvo que se indique lo contrario que $K := F_q$ y $F := F_{q^m}$ donde $m \geq 1$ corresponde al grado de la extensión.

Definición 1.5.1. *Para cada $\alpha \in F$ se define la **traza** de α sobre K y se denotará $Tr_{F/K}(\alpha)$ como:*

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Es decir, la traza de α sobre K es la suma de los conjugados de α.

Pasaremos ahora a estudiar algunas de las propiedades principales de la traza de un elemento.

Lema 1.5.2. *Para cualquier $\alpha \in F$ se verifica que $Tr_{F/K}(\alpha) \in K$.*

Demostración. Sea $f(x)$ el polinomio mínimo de $\alpha \in F$ sobre K y sea $d = deg(f)$. Consideremos ahora el polinomio $g(x) = f(x)^{\frac{m}{d}}$ donde recordemos $m = [F : K]$. Así las raíces de $g(x)$ serán las mismas que las de $f(x)$ pero repetidas m/d veces cada una. Entonces por definición, $Tr_{F/K}(\alpha)$ será exactamente la suma de las raíces de $g(x)$, y a su vez por las fórmulas de Cardano-Vieta (A.7.22), $Tr_{F/K}(\alpha)$ será igual al coeficiente de la variable x^{m-1} en $g(x)$, que es un polinomio de $K[x]$. En consecuencia $Tr_{F/K}(\alpha) \in K$. □

Proposición 1.5.3. *La traza de un elemento verifica las siguientes propiedades:*

1. *$Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ para cada $\alpha, \beta \in F$.*
2. *$Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ para cada $\alpha \in F, c \in K$.*
3. *La traza es una aplicación linear suprayectiva de F en K.*
4. *$Tr_{F/K}(\alpha) = m\alpha$ para todo $\alpha \in K$, donde recordemos $m = [F : K]$.*
5. *$Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$ para cada $\alpha \in F$.*

Demostración.
1. Sean $\alpha, \beta \in F$, se verfica:

$$\begin{aligned} Tr_{F/K}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{m-1}} \\ &= (\alpha+\beta) + (\alpha^q+\beta^q) + \cdots + (\alpha^{q^{m-1}} + \beta^{q^{m-1}}) \\ &= (\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}) + (\beta + \beta^q + \cdots + \beta^{q^{m-1}}) \\ &= Tr_{F/K}(\alpha) + Tr_{F/K}(\beta) \end{aligned}$$

donde la segunda igualdad es consecuencia del lema A.2.15.

2. Sea $\alpha \in F, c \in K$:

$$\begin{aligned} Tr_{F/K}(c\alpha) &= (c\alpha) + (c\alpha)^q + \cdots + (c\alpha)^{q^{m-1}} = c\alpha + c^q\alpha^q + \cdots + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + \cdots + c\alpha^{q^{m-1}} = c\left(\alpha + \cdots + \alpha^{q^{m-1}}\right) = cTr_{F/K}(\alpha) \end{aligned}$$

donde la tercera igualdad es consecuencia del lema 1.3.3.

3. En las dos propiedades anteriores se ha visto la linealidad de la traza. Además se verifica claramente que $Tr_{F/K}(0) = 0$; vamos a ver también que $Tr_{F/K}(\alpha) \neq 0$ para algún $\alpha \in F$, y por tanto que la imagen de la función $Tr_{F/K}$ es todo $K = F_q$.

El núcleo de la aplicación traza es precisamente el conjunto de raíces del polinomio $p(x) = \sum_{i=0}^{m-1} x^{q^i}$, que tiene grado q^{m-1}, y por tanto, a lo sumo q^{m-1} raíces distintas. Pero el cuerpo $F = F_{q^m}$ contiene q^m elementos, por lo que alguno de ellos no pertenece al núcleo.

4. Supongamos $\alpha \in K$. Entonces:

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} = \alpha + \alpha + \cdots + \alpha = m\alpha$$

donde en la segunda igualdad se ha aplicado el lema 1.3.3.

5. Sea $\alpha \in F$.

$$Tr_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha^{q^m} = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha = Tr_{F/K}(\alpha)$$

aplicando de nuevo lema 1.3.3. □

Proposición 1.5.4. *Para cualquier $\alpha \in K$ se tiene que $\left|\{\beta \in F : Tr_{F/K}(\beta) = \alpha\}\right| = q^{m-1}$.*

Demostración. Sabemos, por resultado anterior, que la aplicación traza $Tr_{F/K} : F \longrightarrow K$ es lineal y suprayectiva; luego teniendo en cuenta que $[F : K] = m$ y que K visto como K -espacio vectorial tiene dimensión 1, obtenemos que
$dim\left(Ker(Tr_{F/K})\right) = m - 1$. Además se tiene que

$$\left\{\beta \in F : Tr_{F/K}(\beta) = \alpha\right\} = \left\{\beta_0 + \gamma : \gamma \in Ker\left(Tr_{F/K}\right)\right\}$$

donde $\beta_0 \in F$ es un elemento fijo que cumple $Tr_{F/K}(\beta_0) = \alpha$, el cual debe existir por la suprayectividad. Por tanto,

$$\left|\{\beta \in F : Tr_{F/K}(\beta) = \alpha\}\right| = \left|Ker(Tr_{F/K})\right| = q^{m-1}.$$

□

El siguiente resultado proporciona un método para generar todas las aplicaciones lineales de F en K :

Proposición 1.5.5. *Sea $\beta \in F$ y denotemos L_β a la aplicación de F en K dada por $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)\ \forall \alpha \in F$. Se tiene que si $\gamma \in F$ es tal que $\beta \neq \gamma$ entonces $L_\beta \neq L_\gamma$. Es más, las transformaciones lineales de F en K son exactamente las aplicaciones de la forma L_β donde β varía entre los elementos del cuerpo F.*

Demostración. La linealidad de la aplicación L_β se deduce de la linealidad de la función traza y de la aplicación dada por $\alpha \longmapsto \beta\alpha$ con $\alpha \in F$. Sean $\beta, \gamma \in F$ tales que $\beta \neq \gamma$, o lo que es equivalente, $\beta - \gamma \neq 0$. Sea $\alpha \in F$ tal que $Tr_{F/K}(\alpha) \neq 0$ y denotemos $\eta := (\beta - \gamma)^{-1}\alpha$. Se tiene

$$Tr_{F/K}\left((\beta - \gamma)\eta\right) = Tr_{F/K}(\alpha) \neq 0$$

es decir

$$Tr_{F/K}\left(\beta\eta\right) - Tr_{F/K}\left(\gamma\eta\right) \neq 0$$

Por tanto $L_\beta \neq L_\gamma$. Por otro lado, sabemos que una transformación lineal está determinada completamente por su acción sobre una base. En este caso, el cuerpo $F = F_{q^m}$ tiene una base de m elementos sobre el cuerpo $K = F_q$; por lo que habrá a lo sumo q^m aplicaciones lineales de F_{q^m} en F_q. Ahora bien $\{L_\beta : \beta \in F_{q^m}\}$ es un conjunto de q^m aplicaciones lineales distintas, de donde se obtiene el resultado. □

Veamos ahora que la traza de un elemento puede ser calculada a través de los cuerpo intermedios.

Proposición 1.5.6 (Transitividad de la función traza)**.** *Consideremos la torre de cuerpos finitos $K \subseteq F \subseteq E$. Entonces para cualquier elemento $\alpha \in E$ se verifica:*

$$Tr_{E/K}(\alpha) = Tr_{F/K}\left(Tr_{E/F}(\alpha)\right)$$

Demostración. Denotemos $n = [E : F]$ y $m = [F : K]$ y sea $\alpha \in E$ fijo. Entonces se tiene:

$$\begin{aligned} Tr_{F/K}\left(Tr_{E/F}(\alpha)\right) &= \sum_{i=0}^{m-1} \left(Tr_{E/F}(\alpha)\right)^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}}\right)^{q^i} \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = Tr_{E/K}(\alpha) \end{aligned}$$

□

De forma análoga a como se ha introducido la traza se puede definir un nuevo concepto, la norma de un elemento.

Definición 1.5.7. *Sea una extensión de cuerpos F/K. Se define la **norma** de un elemento $\alpha \in F$ sobre K, y se denotará $Norm_{F/K}(\alpha)$, como:*

$$Norm_{F/K}(\alpha) = \alpha\alpha^q \cdots \alpha^{q^{m-1}} = \textstyle\prod_{i=0}^{m-1} \alpha^{q^i} = \alpha^{(q^m-1)/(q-1)}$$

Es decir, la norma de un elemento α sobre K es igual al producto de todos sus conjugados.

Proposición 1.5.8. *Para cada $\alpha \in F$ se verifica que $Norm_{F/K}(\alpha) \in K$.*

Demostración. Sea $f(x)$ el polinomio mínimo de $\alpha \in F$ sobre K y sea $d = deg(f)$. Consideremos ahora el polinomio $g(x) = f(x)^{\frac{m}{d}}$ donde recordemos $m = [F : K]$. Así las raíces de $g(x)$ serán las mismas que las de $f(x)$ pero repetidas m/d veces cada una. Entonces por definición $Norm_{F/K}(\alpha)$ será exactamente el producto de las raíces de $g(x)$ y a su vez por las fórmulas de Cardano-Vieta, $Norm_{F/K}(\alpha)$ será el coeficiente independiente (salvo signo) en $g(x)$, que es un polinomio de $K[x]$. En consecuencia $Norm_{F/K}(\alpha) \in K$. □

La norma cumple propiedades similares a las de la traza, como se muestra en el siguiente resultado:

Proposición 1.5.9. *Se cumplen las siguientes propiedades:*

1. *$Norm_{F/K}(\alpha\beta) = Norm_{F/K}(\alpha)Norm_{F/K}(\beta)$ para cada $\alpha, \beta \in F$.*
2. *Es una función suprayectiva de F en K y de F^* en K^*.*

3. $Norm_{F/K}(\alpha) = \alpha^m$ *para cada* $\alpha \in K$.

4. $Norm_{F/K}(\alpha^q) = Norm_{F/K}(\alpha)$ *para cada* $\alpha \in F$.

Demostración.
1. Consideremos $\alpha, \beta \in F$. Entonces:

$$\begin{aligned} Norm_{F/K}(\alpha\beta) &= (\alpha\beta)(\alpha\beta)^q ... (\alpha\beta)^{q^{m-1}} = \alpha\alpha^q ... \alpha^{q^{m-1}} \beta\beta^q ... \beta^{q^{m-1}} \\ &= Norm_{F/K}(\alpha) Norm_{F/K}(\beta) \end{aligned}$$

2. Por ser F y K cuerpos (y por tanto, no contienen divisores de 0), se tiene que $Norm_{F/K}(\alpha) = 0$ si y solo si $\alpha = 0$. Será suficiente probar entonces que la norma es una aplicación suprayectiva de F^* en K^* . De la propiedad 1, se obtiene que $Norm_{F/K}$ es un homomorfismo entre ambos grupos. Ahora, por definición de $Norm_{F/K}$, se tiene que $Ker\left(Norm_{F/K}\right)$ es exactamente el conjunto de raíces del polinomio $x^{(q^m-1)/(q-1)} \in K[x]$, por lo que denotando d al orden del núcleo, se satisface la desigualdad $d \leq (q^m - 1)/(q - 1)$. Aplicando el primer teorema de isomorfía para grupos (A.4.6), se tiene que la imagen de la aplicación $Norm_{F/K}$ tiene orden $(q^m - 1)/d$ y por la anterior desigualdad, $(q^m - 1)/d \geq q - 1$. Pero el orden de K^* es precisamente $q - 1$, luego hemos comprobado la suprayectividad de $Norm_{F/K}$.

3. Sea $\alpha \in K$. Entonces directamente de la aplicación del resultado 1.3.3 se obtiene:

$$Norm_{F/K}(\alpha) = \alpha\alpha^q \cdots \alpha^{q^{m-1}} = \alpha\alpha \cdots \alpha = \alpha^m$$

4. Por la propiedad 1 se tiene que

$$Norm_{F/K}(\alpha^q) = (Norm_{F/K}(\alpha))^q = Norm_{F/K}(\alpha)$$

ya que $Norm_{F/K}(\alpha) \in K$ y por el lema 1.3.3, $a^q = a$ para cualquier $a \in K$. □

La norma al igual que la traza también es transitiva.

Proposición 1.5.10 (Transitividad de la norma)**.** *Consideremos la torre de cuerpos finitos* $K \subseteq F \subseteq E$ *y* $\alpha \in E$. *Se verifica que*

$$Norm_{F/K}(\alpha) = Norm_{F/K}(\alpha)\left(Norm_{E/F}(\alpha)\right)$$

Demostración. Tomando $n = [E : F]$, $m = [F : K]$ y $\alpha \in E$ se tiene:

$$\begin{aligned} Norm_{F/K}\left(Norm_{E/F}(\alpha)\right) &= Norm_{F/K}\left(\alpha^{(q^{mn}-1)/(q^m-1)}\right) \\ &= \left(\alpha^{(q^{mn}-1)/(q^m-1)}\right)^{(q^m-1)/(q-1)} \\ &= \alpha^{(q^{mn}-1)/(q-1)} \\ &= Norm_{E/K}(\alpha) \end{aligned}$$

□

Otra forma de introducir la traza y la norma de un elemento, que aparece en algunos textos es la siguiente:

Sea una extensión de cuerpos finita F/K y un elemento $\alpha \in F$. Consideremos la homotecia h_α, dada por $h_\alpha(x) = \alpha x$ para $x \in F$, que es una aplicación K-lineal de F

en sí mismo. Consideremos la matriz $A_\alpha = (a_{ij})$ de la aplicación respecto de una base cualquiera. Entonces se define la traza de $\alpha \in F$ como la suma de la traza de la matriz A_α y la norma de α como el determinante de dicha matriz:

$$\begin{aligned} Tr_{F/K}(\alpha) &= Tr(A_\alpha) = \textstyle\sum_i a_{ii} \\ Norm_{F/K}(\alpha) &= |A_\alpha| \end{aligned}$$

Veamos que estas definiciones y las dadas anteriormente en el texto son equivalentes:

Sea $\alpha \in F$ una raíz de un polinomio irreducible sobre K, $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$.

Consideremos la torre de cuerpos $K \subseteq K(\alpha) \subseteq F$, entonces por la proposición 1.2.8, una base de la extensión $K(\alpha)/K$ será $B = \left\{1, \alpha, ..., \alpha^{d-1}\right\}$. Ahora bien, tomando $r = \frac{m}{d}$ y $B' = \{\beta_1, ..., \beta_r\}$ una base de $F/K(\alpha)$, por la demostración del teorema de multiplicidad del grado (1.2.6), se tendrá que el conjunto

$$\left\{\beta_1, \beta_1\alpha, ..., \beta_1\alpha^{d-1}, \beta_2, \beta_2\alpha, ..., \beta_2\alpha^{d-1}, ..., \beta_r, \beta_r\alpha, ..., \beta_r\alpha^{d-1}\right\}$$

es una base de F/K.

Teniendo en cuenta que α es una raíz de f, se tienen las relaciones para cada i=1,..,r:

$$\begin{aligned} \alpha \cdot \beta_i &= \alpha\beta_i = \beta_i\alpha \\ \alpha \cdot \beta_i\alpha &= \alpha\beta_i\alpha = \beta_i\alpha^2 \\ &\vdots \\ \alpha \cdot \beta_i\alpha^{d-1} &= \beta_i\alpha^d = -a_0\beta_i - a_1\beta_i\alpha - \cdots - a_{d-1}\beta_i\alpha^{d-1} \end{aligned}$$

Por lo que la matriz $M_B(h_\alpha)$ de la aplicación h_α respecto de la base B vendrá dada por:

$$M_B(h_\alpha) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 & & & & & \\ 1 & 0 & \cdots & 0 & -a_1 & & & & & \\ 0 & 1 & 0\cdots & 0 & -a_2 & & & & & \\ \vdots & & \ddots & & \vdots & & & & & \\ 0 & \cdots & 0 & 1 & -a_{d-1} & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 0 & \cdots & \cdots & 0 & -a_0 \\ & & & & & & 1 & 0 & \cdots & 0 & -a_1 \\ & & & & & & 0 & 1 & 0\cdots & 0 & -a_2 \\ & & & & & & \vdots & & \ddots & & \vdots \\ & & & & & & 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

Tenemos entonces que

$$Tr(M_B(h_\alpha)) = r(-a_{d-1}) = \tfrac{m}{d}(-a_{d-1}) \text{ y } Norm_{F/K}(\alpha) = r(-1)^d a_0 = \tfrac{m}{d}(-1)^d a_0$$

ahora aplicando las fórmulas de Cardano-Vieta(A.7.22):

$$-a_{d-1} = (-1)^2 s_1(\alpha_1, ..., \alpha_d) = s_1\left(\alpha, ..., \alpha^{q^{d-1}}\right) = \alpha + \alpha^q + \cdots + \alpha^{q^{d-1}}$$

$$a_0(-1)^d = s_{d-1}(\alpha_1, ..., \alpha_d) = s_{d-1}\left(\alpha, ..., \alpha^{q^{d-1}}\right) = \alpha\alpha^q \cdots \alpha^{q^{d-1}}$$

donde se ha aplicado la proposición 1.4.4, que establece que las raíces de f son precisamente $\alpha, ..., \alpha^{q^{d-1}}$. Teniendo en cuenta que es un resultado conocido del álgebra lineal que la traza y el determinante de la matriz de una aplicación no dependen de la base elegida, y aplicando la proposición 1.4.7, se comprueba que efectivamente ambas definiciones para la traza y norma son equivalentes.

1.6. Bases

Al principio del capítulo se vio que todo cuerpo finito puede ser considerado como un espacio vectorial sobre cada subcuerpo y por tanto existe una base sobre dichos subcuerpos. En esta sección nos ocuparemos de la definición de diferentes tipos bases, proporcionar métodos de comprobación para ver que un determinado conjunto es una base, así como enunciar algunos resultados de existencia de este tipo bases. Análogamente a la sección anterior denotaremos como F al cuerpo finito F_{q^m} y K al cuerpo finito F_q en algunos resultados para simplificar la notación.

La primera cuestión que se abordará será cómo identificar bases de cuerpos finitos; es decir, dado un conjunto $\{\alpha_1, ..., \alpha_m\} \subseteq F$, establecer un criterio para determinar si dicho conjunto es, o no, una base de F sobre K, criterio que nos proporcionará el concepto de *discriminante*.

Definición 1.6.1. *Sea F/K una extensión de cuerpos y sea $\{\alpha_1, ..., \alpha_m\}$ un conjunto de m elementos de F visto como espacio espacio vectorial sobre K. Se define el* ***discriminante*** *de $\alpha_1, ..., \alpha_m$ y se denotará $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ como el determinante*

$$\Delta_{F/K}(\alpha_1, ..., \alpha_m) = \begin{vmatrix} Tr_{F/K}(\alpha_1\alpha_1) & . & . & . & Tr_{F/K}(\alpha_1\alpha_m) \\ . & & . & & . \\ . & & & . & . \\ . & & & . & . \\ Tr_{F/K}(\alpha_m\alpha_1) & . & . & . & Tr_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

Proposición 1.6.2. *Sea F/K una extensión de cuerpos y $\alpha_1, ..., \alpha_m \in F$, donde m es la dimensión de F sobre K. El conjunto $\{\alpha_1, ..., \alpha_m\}$ es una base de F sobre K si y solo si $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ es no nulo.*

Demostración. $\Rightarrow$ Supongamos que $\{\alpha_1, ..., \alpha_m\}$ es una base. Vamos a ver que el discriminante es distinto de 0 comprobando que las m columnas de la matriz en la definición de discriminante son linealmente independientes. Denotemos como $C_1, ..., C_m$ las columnas de la matriz correspondiente al discriminante $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ y supongamos que existen $a_1, ..., a_m \in K$ tales que $a_1C_1 + \cdots + a_mC_m = 0$; es decir, para cada $1 \leq j \leq m$ se tendrá que

$$a_1 Tr_{F/K}(\alpha_1\alpha_j) + \cdots + a_m Tr_{F/K}(\alpha_m\alpha_j) = 0$$

Tomemos ahora $\beta := a_1\alpha_1 + \cdots + a_m\alpha_m$. Entonces, por la relación anterior, y teniendo en cuenta la linealidad de la traza, se tiene que $Tr_{F/K}(\alpha\beta) = 0$ para todo $\alpha \in F$; pero esto solo puede ocurrir si $\beta = 0$; es decir, $a_1 = \cdots = a_m = 0$ pues por hipótesis $\{\alpha_1, ..., \alpha_m\}$ es una base de F sobre K.

$\Leftarrow$ Supongamos ahora que $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ y que $a_1\alpha_1 + ... + a_m\alpha_m = 0$ para ciertos $a_1, ..., a_m \in K$. Pero entonces se verificará también

$$\beta := a_1\alpha_1\alpha_j + \cdots + a_m\alpha_m\alpha_j = 0 \text{ donde } 1 \leq j \leq m$$

Tomando la traza de β y aplicando las propiedades de la función traza vistas en la proposición 1.5.3 se obtiene

$$a_1 Tr_{F/K}(\alpha_1\alpha_j) + \cdots + a_m Tr_{F/K}(\alpha_m\alpha_j) = 0 \text{ con } 1 \leq j \leq m$$

Ahora bien, hemos supuesto que $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ y por tanto las columnas de la matriz son linealmente independientes por lo que

$$a_1 C_1 + \cdots + a_m C_m = 0 \Rightarrow a_1 = \cdots = a_m = 0$$

Obtenemos así que $\alpha_1, ..., \alpha_m$ son m elementos linealmente independientes y por tanto una base de F sobre K . □

A continuación, se proporcionará un nuevo método para verificar que un subconjunto de un cuerpo es una base, a priori, menos costoso que el anterior:

Corolario 1.6.3. *Sea una extensión de cuerpos F/K y consideremos elementos $\alpha_1, ..., \alpha_m \in F$. El conjunto $\{\alpha_1, ..., \alpha_m\}$ es una base de F sobre K si y solo si el determinante*

$$\begin{vmatrix} \alpha_1 & . & . & . & \alpha_m \\ \alpha_1^q & . & & & \alpha_m^q \\ . & & . & & . \\ . & & & . & . \\ \alpha_1^{q^{m-1}} & . & . & . & \alpha_m^{q^{m-1}} \end{vmatrix}$$

es no nulo.

Demostración. Denotemos como A a la matriz

$$\begin{pmatrix} \alpha_1 & . & . & . & \alpha_m \\ \alpha_1^q & . & & & \alpha_m^q \\ . & & . & & . \\ . & & & . & . \\ \alpha_1^{q^{m-1}} & . & . & . & \alpha_m^{q^{m-1}} \end{pmatrix}$$

Sea A^T su matriz traspuesta y consideremos la matriz $B := A^T A$. Utilizando la definición de traza se tiene que

$$B = \begin{pmatrix} Tr_{F/K}(\alpha_1\alpha_1) & . & . & . & Tr_{F/K}(\alpha_1\alpha_m) \\ . & & . & & . \\ . & & & . & . \\ . & & & . & . \\ Tr_{F/K}(\alpha_m\alpha_1) & . & . & . & Tr_{F/K}(\alpha_m\alpha_m) \end{pmatrix}$$

Tomando determinantes obtenemos $\Delta_{F/K}(\alpha_1, ..., \alpha_m) = |B| = |A|^2$. El resultado es consecuencia entonces de la proposición anterior. □

Pasaremos, ahora sí, a la definición de varios tipos de bases:

Definición 1.6.4. *Sea $\theta \in F_{q^m}$ una raíz de un polinomio irreducible de grado m sobre F_q. Entonces a una base $\left\{1, \theta, ..., \theta^{m-1}\right\}$ de F_{q^m} sobre F_q se le denomina* ***base polinómica.***

Nota: Que en efecto el conjunto $\left\{1, \theta, ..., \theta^{m-1}\right\}$ forma una base de F_{q^m} sobre F_q es consecuencia en la proposición 1.2.8, ya que en las condiciones anteriores θ es un elemento primitivo de la extensión.

Definición 1.6.5. *Supongamos que $\theta \in F_{q^m}$ es tal que el conjunto*

$$\left\{\theta^{q^i} : 0 \leq i \leq m-1\right\}$$

*es una base de F_{q^m} sobre F_q. Entonces a una base de esta forma se le denomina **base normal** de F_{q^m} sobre F_q.*

En el siguiente teorema se mostrará que para cada extensión de cuerpos finitos existe una base normal. A lo largo de la prueba se utilizarán conceptos y resultados introducidos en la sección *Operadores lineales* del apéndice.

Teorema 1.6.6 (Existencia de bases normales)**.** *Para cualquier entero $m \geq 2$ existe una base normal de F_{q^m} sobre F_q.*

Demostración. Comencemos viendo que $x^m - 1$ es precisamente el polinomio mínimo del automorfismo de Frobenius, que denotaremos σ. Es claro que el automorfismo de Frobenius es anulado por $x^m - 1$ pues

$$\left(\sigma^m - I\right)(a) = a^{q^m} - a = 0 \text{ para cada } a \in F_{q^m}$$

Consideremos ahora un polinomio $p(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ de grado menor que m y consideremos el operador:

$$p(\sigma) = a_{m-1}\sigma^{m-1} + \cdots + a_1\sigma + a_0$$

Sabemos por el teorema 1.4.10 que el autormorfismo de Frobenius y sus potencias forman una colección de m automorfismos distintos (incluyendo identidad). Aplicando entonces el lema de Artin A.4.9, existe algún $\alpha \in F$ tal que $(p(\alpha)) \neq 0$. Pero entonces $p(x)$ no puede ser el polinomio mínimo del automorfismo de Frobenius; por lo que efectivamente el polinomio mínimo es $x^m - 1$.
Por el resultado A.6.3 el polinomio característico tiene grado m , $x^m - 1$ es también el polinomio característico de σ, pues en general el polinomio mínimo divide al polinomio característico aplicando la proposición A.6.4. Pero de esto, aplicando el resultado A.6.6, se obtiene que el automorfismo de Frobenius tiene un vector cíclico, el cual denotaremos α. Se sigue entonces de la definición que un vector cíclico de σ genera una base normal, esto es, para $\alpha \in F_{q^m}$ entonces $\left\{\alpha, \sigma(\alpha) = \alpha^q, ..., \sigma^{m-1}(\alpha) = \alpha^{q^{m-1}}\right\}$ forma una base de F_q^m sobre F_q. □

A continuación, se enunciará un resultado de caracterización de bases normales cuya demostración remitiremos a uno de los textos de la bibliografía:

Teorema 1.6.7. *Sea una extensión de cuerpos F_{q^m}/F_q. El conjunto $\left\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\right\}$ es una base normal de F_{q^m} sobre F_q si y solo si los polinomios $x^m - 1$ y $\alpha x^{m-1} + \alpha^q x^{m-2} + ... + \alpha^{q^{m-1}}$ son relativamente primos, es decir, si el máximo común divisor (en F_{q^m}) de ambos es 1.*

Demostración. Ver [8], teorema 2.39 (página 58). □

Definición 1.6.8. *Sea F/K una extensión de cuerpos. Dos bases de F sobre K, $\{\alpha_1, ..., \alpha_m\}$ y $\{\beta_1, ..., \beta_m\}$, se dicen* ***duales****, si verifican*

$$Tr_{F/K}(\alpha_i\beta_j) = \begin{cases} 0 & si\ i \neq j, \\ 1 & si\ i = j. \end{cases}$$

Una base se dice ***autodual*** *si es dual a sí misma.*

Proposición 1.6.9. *Cada base de un cuerpo finito F_{q^m} tiene una única base dual.*

Demostración. Ver [9], teorema 1.5.7 (página 22). □

Hemos visto hasta ahora que todo cuerpo finito posee una base normal y que toda base tiene una única base dual, sin embargo el próximo resultado pone de manifiesto que no para toda extensión de cuerpos finitos existe una base normal y autodual.

Teorema 1.6.10. *El cuerpo F_{q^m} tiene una base sobre F_q normal y autodual si y solo si q es par y m no es múltiplo de 4 o tanto q como m son número impares.*

Demostración. Ver [7], páginas 193-198. □

A continuación introduciremos un último tipo de bases, las *primitivas normales.*

Definición 1.6.11. *Sea una extensión de cuerpos F_{q^m}/F_q. Diremos que una base es* ***primitiva normal*** *si es de la forma $\left\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\right\}$ donde α es un elemento primitivo de F_{q^m}.*

El problema de probar la existencia de bases primitivas normales es harto complicado. En 1987 Lenstra y Schoof, matemáticos holandeses, consiguieron demostrar el resultado para el caso general con ayuda de la computadora. Hasta el momento solo se había conseguido demostrar la existencia de dichas bases para extensiones del tipo F_{p^m}/F_p. Finalmente en 2003, Cohen y Huczynska obtuvieron una demostración sin necesidad de cálculos computacionales no recogida aquí por su extensión y complejidad.

Teorema 1.6.12 (Lenstra-Schoof)**.** *Para todo $q = p^r$ con $r \geq 1$ y todo entero $m \geq 2$ existe una base primitiva normal de F_{q^m} sobre F_q.*

Demostración. Ver [3], páginas 41-56. □

Capítulo 2

Polinomios sobre cuerpos finitos

Algunas propiedades de los polinomios han sido ya introducidas en el capítulo anterior para la demostración de ciertos resultados de estructura de cuerpos, por lo que el presente capítulo tendrá por objetivo la introducción de nuevos conceptos, así como profundizar en la teoría de polinomios sobre cuerpos finitos. La primera sección estará dedicada a polinomios y cuerpos ciclotómicos. El estudio de sus propiedades permitirá en la siguiente sección la obtención del teorema de *Wedderburn*. En la tercera sección del capítulo se introducirá los conceptos de *orden* de un polinomio y polinomio *primitivo* y se mostrarán resultados relacionados con estos nuevos términos. La cuarta sección estará dedicada al estudio de polinomios irreducibles. Se desarrollarán técnicas para determinar el número de dichos polinomios en un cuerpo finito y sus formas de expresión, entre otras propiedades. Por último, se presentará el *algoritmo de Berlekamp*, que proporcionará un método efectivo para la factorización de polinomios sobre cuerpos finitos.

2.1. Polinomios y cuerpos ciclotómicos

En esta sección se procederá a la introducción y estudio de ciertas propiedades de las raíces n-ésimas de la unidad, los polinomios ciclotómicos y sus respectivos cuerpos de escisión. Algunos de los resultados de esta parte se enunciarán para cuerpos arbitrarios de característica p (donde queda incluido el caso $p = 0$) para acabar con resultados específicos acerca de cuerpos finitos.

Definición 2.1.1. *Sea K un cuerpo y n un entero positivo. Un elemento $a \in K$ se dice que es una* ***raíz n-ésima de la unidad*** *si $a^n = 1$, o, equivalentemente, si es raíz del polinomio $x^n - 1$.*
LLamaremos n-ésimo ***cuerpo ciclotómico****, donde $n \in \mathbb{N}$, al cuerpo de escisión de $x^n - 1$ sobre K y se le denotará por $K^{(n)}$.*
Al conjunto de raíces n-ésimas de la unidad en $K^{(n)}$ se le denotará por $E^{(n)}$.

Observación 2.1.2. *El conjunto $E^{(n)}$ es un subgrupo del grupo multiplicativo $K^{(n)^*}$ y además es finito de orden menor o igual que n pues el polinomio $x^n - 1$ tiene a lo sumo n raíces distintas.*

Proposición 2.1.3. *Sea n un entero positivo y K un cuerpo de característica p. Se verifica:*

1. *$E^{(n)}$ tiene orden n si y solo si p no divide a n.*
2. *Si p divide a n, y $n = mp^r$ donde m y r son enteros positivos con m no divisible entre p, e,ntonces $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ y las raíces de $x^n - 1$ en $K^{(n)}$ son los elementos de $E^{(m)}$, cada uno con multiplicidad p^r.*

Demostración. 1. $\Rightarrow$ Si $car(K) = 0$ el resultado es claro. Supongamos entonces $car(K) = p \neq 0$. Expresemos n de la forma $n = p^r m$ donde $r \geq 0$ y p no divide a m . Tenemos entonces la igualdad $x^n - 1 = (x^m - 1)^{p^r}$, con lo que el número de raíces en $K^{(n)}$ de $x^n - 1$ es menor igual que m . Ahora como se dan las relaciones $m \leq n$ y $|E^{(n)}| = n$, se tiene que $m = n$ y así p no divide a n , pues hemos supuesto que p no divide a m.

$\Leftarrow$ Si $p = car(K)$ no divide a n entonces el polinomio es separable por A.7.11 pues la única raíz de su polinomio derivado es 0, que no es raíz de $x^n - 1$. Por tanto, el número de raíces de $x^n - 1$ en $K^{(n)}$ es n , es decir, $E^{(n)} = n$.

2. La segunda afirmación es directa a partir de la igualdad $x^n - 1 = x^{mp^r} - 1 = (x^m - 1)^{p^r}$ y el razonamiento llevado a cabo en 1. □

Observación 2.1.4. *El apartado anterior junto con la proposición 1.3.14, muestran que si $car(K)$ no divide a n , entonces $E^{(n)}$ es un grupo cíclico de orden n.*

Definición 2.1.5. *Sea K un cuerpo de característica p y n un entero positivo no divisible por p. Se llama raíz n-ésima **primitiva** de la unidad sobre K a todo elemento de $E^{(n)}$ que sea generador de dicho grupo.*

Proposición 2.1.6. *Si ξ es una raíz n-ésima primitiva de la unidad entonces ξ^r lo es también si y solo si $mcd(r, n) = 1$.*

Demostración. $\Rightarrow$ Si ξ^r es una raíz n-ésima primitiva, existe un $a \in \mathbb{Z}$ tal que $\xi = \xi^{ra}$, de donde $\xi^{ra-1} = 1$ y existe un $t \in \mathbb{Z}$ tal que $tn = ra - 1$, por lo que aplicando la proposición A.5.10 se tiene que $mcd(r, n) = 1$.
$\Leftarrow$ Aplicando la misma proposición existen $a, b \in Z$ tales que $ar + bn = 1$. Entonces para cada raíz n-ésima de la unidad η se tiene $\eta = \xi^s$ para algún s y en consecuencia

$$\eta = \xi^s = \xi^{asr} = (\xi^r)^{as}$$

Se tiene así que ξ^r es un generador del grupo de las raíces n-ésimas primitivas de la unidad, es decir, una raíz n-ésima primitiva. □

Definición 2.1.7. *Sea n un entero positivo y K un cuerpo cuya característica no divide a n. Se llama n-ésimo **polinomio ciclotómico** sobre K al polinomio*

$$\Phi_n = (x - \xi_1) \cdots (x - \xi_r)$$

donde $\xi_1, ..., \xi_r$ son raíces n-ésimas primitivas de la unidad sobre K.

Definición 2.1.8. *Se denomina **función ϕ de Euler** a la aplicación $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ que a cada entero positivo n asocia el número de enteros positivos r tales que $1 \leq r < n$ y $mcd(n, r) = 1$.*

Proposición 2.1.9. *Sea n un entero positivo y K un cuerpo cuya característica no divide a n. Se verifcan las siguientes propiedades:*

1. *$deg(\Phi_n) = \phi(n)$.*
2. *$x^n - 1 = \prod_{d|n} \Phi_d(x)$.*
3. *$\Phi_n(x) \in P[x]$, donde P es el subcuerpo primo de K. Además en el caso en que la característica de K sea 0, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Demostración. 1. Es consecuencia de la definición de función de Euler y la proposición 2.1.6.
2. Si $d|n$ y $d \neq n$, entonces $E^{(d)}$ está contenido estrictamente en $E^{(n)}$ y además $\eta \in E^{(d)}$ es una raíz d-ésima primitiva si y solo si su orden es d, de donde

$$\Phi_d(x) = \prod_{\eta \in E^{(n)}, |\eta| = d} (x - \eta)$$

y se tiene pues

$$x^n - 1 = \prod_{\eta \in E^{(n)}} (x - \eta) = \prod_{d|n} \left(\prod_{\eta \in E^{(n)}, |\eta| = d} (x - \eta) \right) = \prod_{d|n} \Phi_d(x)$$

3. Procederemos por inducción en n. Por la definición, es claro que Φ_n es mónico para cualquier n. Para $n = 1$ se tiene $\Phi_1(x) = x - 1$ y el resultado es claro. Supongamos el resultado cierto para $1 \leq d < n$ y veámoslo para n. Por la segunda afirmación se tiene que

$$\Phi_n(x) = (x^n - 1)/f(x) \text{ donde } f(x) = \prod_{d|n, d<n} \Phi_d(x)$$

Por hipótesis de inducción $f(x)$ es un polinomio con coeficientes en el subcuerpo primo P de K (o $\mathbb{Z}$ en el caso en que la característica de K sea 0). Empleando entonces el algoritmo de la división con $x^n - 1$ y $f(x)$, se obtiene que los coeficientes de Φ_n pertenecen al subcuerpo primo de K o a $\mathbb{Z}$ respectivamente. □

Ejemplo 2.1.10. *El anterior resultado proporciona un método para el cálculo de polinomios ciclotómicos de forma recurrente:*
1. Es fácil ver que $\Phi_1(x) = x - 1$ *y* $\Phi_2(x) = x + 1$. *Entonces:*

$$\Phi_4(x) = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1$$

2. Se tiene la igualdad $x^3 - 1 = (x - 1)(x^2 + x + 1)$, *luego* $\Phi_3(x) = x^2 + x + 1$.

3. Hemos visto que $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$ *y* $\Phi_3(x) = x^2 + x + 1$ *y además se da la igualdad*

$$x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

Luego $\Phi_6(x) = x^2 - x + 1$.

Proposición 2.1.11. *La extensión de cuerpos* $K^{(n)}/K$ *es una extensión simple.*

Demostración. Si existe una raíz n-ésima primitiva de la unidad sobre K , digamos ξ, es claro que $K^{(n)} = K(\xi)$. En otro caso aplicando la segunda afirmación de 2.1.3 y escribiendo $n = mp^r$ donde p no divide a m se tendrá que $K^{(n)} = K^{(m)}$ y $K^{(m)} = K(\eta)$ donde η es una raíz m-ésima primitiva. □

Proposición 2.1.12. *Si* $K = \mathbb{Q}$, *entonces el n-ésimo polinomio ciclotómico* $\Phi_n(x)$ *es irreducible sobre* $\mathbb{Q}$ *y además* $\left[\mathbb{Q}^{(n)} : \mathbb{Q}\right] = \phi(n)$.

Demostración. Ver [1] teorema 9.2.2 y corolario 9.2.4 (página 109). □

Terminaremos la sección con dos importantes resultados específicos de cuerpos finitos y un lema que será utilizado para la demostración del teorema de Wedderburn en la siguiente sección:

Proposición 2.1.13. *Sea F_q un cuerpo finito, n un entero positivo tal que $mcd(q,n) = 1$, $\Phi_n(x)$ el n-ésimo polinomio ciclotómico sobre F_q y d el menor entero positivo que verifica la condición $q^d \equiv 1 \ mod\ n$. Se tiene que:*

1. *$\Phi_n(x)$ se factoriza en $F_q[x]$ como producto de $\frac{\phi(n)}{d}$ factores irreducibles de grado d.*
2. *El n-ésimo cuerpo ciclotómico sobre F_q es el cuerpo de escisión sobre F_q de cualquiera de dichos factores irreducibles y la extensión $F_q^{(n)}/F_q$ tiene grado d.*

Demostración. Sea $f(x)$ un factor irreducible arbitrario de $\Phi_n(x)$ y sea ξ una raíz n-ésima primitiva de la unidad sobre F_q que sea raíz de $f(x)$. Entonces:

$$\xi \in F_{q^t} \Longleftrightarrow \xi^{q^t} = \xi \Longleftrightarrow \xi^{q^t-1} = 1 \Longleftrightarrow q^t \equiv 1 \ mod\ n$$

de donde se obtiene que $\xi \in F_{q^d}$ y no pertenece a ningún subcuerpo propio de F_{q^d} por ser d el menor entero positivo que verifica tal condición; es decir, el grado del polinomio mínimo de ξ sobre F_q es igual al grado de $f(x)$ y por tanto $deg(f(x)) = d$. Ahora como $deg(\Phi_n(x)) = \phi(n)$, se tiene que el número de factores irreducibles de $\Phi_n(x)$ es $\frac{\phi(n)}{d}$.
Para concluir basta observar que el n-ésimo cuerpo ciclotómico es $F_q(\xi)$ donde ξ raíz n-ésima primitiva de la unidad. □

Ejemplo 2.1.14. *Consideremos el cuerpo $K = \mathbb{Z}_{11}$:*

1. *Sea el polinomio ciclotómico $\Phi_6(x) = x^2 - x + 1 \in \mathbb{Z}_{11}[x]$. Se tiene que $mcd(11,6) = 1$ y el menor entero positivo d, tal que $11^d \equiv 1 \ mod\ 6$, es $d = 2$. Aplicando entonces la proposición anterior se tiene que $\Phi_6(x)$ se factoriza como producto de $\phi(6)/2 = 1$ polinomio irreducible de grado 2. En consecuencia $\Phi_6(x)$ es irreducible en $\mathbb{Z}_{11}[x]$.*
2. *Consideremos ahora el polinomio $\Phi_{12}(x) = x^4 - x^2 + 1 \in \mathbb{Z}_{11}[x]$. Se verifica que $mcd(11,12) = 1$ y el menor entero positivo d, tal que $11^d \equiv 1 \ mod\ 12$, es $d = 2$. Aplicando la proposición anterior se tiene que $\Phi_{12}(x)$ se factoriza como producto de $\phi(12)/2 = 2$ polinomios irreducibles de grado 2. Es más:*

   $$\Phi_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1) \ en\ \mathbb{Z}_{11}[x].$$

   Además aplicando ahora la segunda afirmación del resultado anterior el cuerpo ciclotómico $K^{(12)} = \mathbb{Z}_{11}^{(12)}$ será F_{121}.

Proposición 2.1.15. *El cuerpo F_q es el $(q-1)$-ésimo cuerpo ciclotómico sobre cualquiera de sus subcuerpos.*

Demostración. El polinomio $x^{q-1} - 1$ se escinde en F_q pues sus raíces son exactamente todos los elementos no nulos de F_q. Pero entonces dicho polinomio no se escinde en ningún subcuerpo propio de F_q, de donde se obtiene el resultado. □

Lema 2.1.16. *Si d es un divisor de n con $1 \leq d < n$, se tiene que el polinomio ciclotómico $\Phi_n(x)$ divide a $(x^n-1)/\left(x^d-1\right)$ siempre que $\Phi_n(x)$ esté definido; es decir, siempre que la característica del cuerpo base no divida a n.*

Demostración. Por la segunda afirmación de la proposición 2.1.9, sabemos que $\Phi_n(x)$ divide a

$$x^n - 1 = \left(x^d - 1\right) \cdot \frac{x^n - 1}{x^d - 1}.$$

Pero como d es un divisor propio de n , $\Phi_n(x)$ y $x^d - 1$ no tienen raíces comunes por lo que el máximo común divisor de ambos es 1, de donde se obtiene que $\Phi_n(x)$ debe dividir a $(x^n-1)/\left(x^d-1\right)$. □

2.2. El teorema de Wedderburn

Es un resultado conocido que todo dominio finito es un cuerpo (A.2.11), en esta sección iremos más allá y como aplicación del estudio realizado de los polinomios ciclotómicos se demostrará que todo anillo de división finito es un cuerpo finito. Comenzaremos con la definición del concepto de *anillo de división*, para pasar directamente al enunciado del teorema. A lo largo de la prueba se utilizarán términos y resultados de la teoría de grupos, para lo cual se recomienda ver la sección dedicada a grupos del apéndice.

Definición 2.2.1. *Un **anillo de división** es un anillo no necesariamente conmutativo en el que todo elemento no nulo es invertible.*

Un anillo de división es, por tanto, un anillo que verifica las mismas propiedades que un cuerpo, a excepción de la conmutatividad del producto, razón por la cual se conozca también con el nombre de **cuerpo no conmutativo**.

Teorema 2.2.2 (Teorema de Wedderburn)**.** *Todo anillo de división finito es un cuerpo.*

Demostración. Sea D un anillo de división finito y sea $Z(D) = \{z \in D : zd = dz \ \forall d \in D\}$ el centro de D . Por ser D un anillo de división todos los elementos no nulos son invertibles, luego por la definición de centro de D se tiene que $Z(D)$ es un cuerpo, por tanto $Z(D) = F_q$ para cierta potencia de primo q . Ahora bien D es un espacio vectorial sobre $Z(D)$ de dimensión n, por lo que D tiene q^n elementos. Si vemos que $n = 1$, se tendrá que $D = Z(D)$ y obtendremos el resultado el resultado.
Supongamos por reducción al absurdo que $n > 1$. Consideremos un elemento $a \in D$ y definamos el conjunto $N_a = \{b \in D : ab = ba\}$. Es claro que N_a es un anillo de división que contiene a $Z(D)$, por lo que N_a tiene q^r elementos, donde $1 \leq r \leq n$. Veamos que r divide a n . Como N_a^* es un subgrupo de D^*, aplicando teorema de Lagrange (A.1.5) se tiene que $q^r - 1$ divide a $q^n - 1$. Escribamos $n = rm + t$, con $0 \leq t < r$. Entonces:

$$q^n - 1 = q^{rm}q^t - 1 = q^t\left(q^{rm} - 1\right) + \left(q^t - 1\right).$$

Como $q^r - 1$ divide a $q^n - 1$ y también a $q^{rm} - 1$, $q^r - 1$ debe dividir a $q^t - 1$. Ahora bien se tiene que $q^t - 1 < q^r - 1$, por lo que $t = 0$ y así r divide a n.

Consideremos ahora la ecuación de clases para el grupo D^* (ver A.1.12). Se tiene que el centro de D^* es Z^*, que tiene orden $q-1$. Además para $a \in D^*$ el normalizador de a en D^* es exactamente N_a^*. Por tanto, una clase de conjugación en D^* que contenga más de un elemento tendrá $(q^n - 1)/(q^r - 1)$ elementos, donde r es un divisor de n con $1 \leq r < n$. Así la ecuación de clases queda

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1}$$

donde $r_1, ..., r_k$ son divisores de n no necesariamente distintos y tales que $1 \leq r_i < n$ para $1 \leq i \leq k$.
Tomemos el n-ésimo polinomio ciclotómico Φ_n sobre el cuerpo de los números racionales. Como la característica de $\mathbb{Q}$ es 0, aplicando la tercera afirmación afirmación de la proposición 2.1.9 $\Phi_n(x) \in \mathbb{Z}[x]$, por lo que $\Phi_n(q)$ es un número entero. De nuevo por la proposición 2.1.9, ahora por la segunda afirmación, $\Phi_n(q)$ divide a $q^n - 1$. Además por el lema 2.1.16, se tiene $\Phi_n(q)$ divide a $(q^n - 1)/(q^{r_i} - 1)$ para $1 \leq i \leq k$, por lo que de la ecuación de clases concluimos que $\Phi_n(q)$ divide a $q - 1$.
Por otro lado, de la definición de polinomio ciclotómico se tiene que

$$\Phi_n(x) = \prod_{s=1, mcd(s,n)=1}^{n} (x - \xi^s)$$

donde ξ es un número complejo que es raíz n -ésima primitiva de la unidad sobre el cuerpo de los número racionales. Tomando módulos de números complejos:

$$|\Phi_n(q)| = \prod_{s=1, mcd(s,n)=1}^{n} |q - \xi^s| > \prod_{s=1, mcd(s,n)=1}^{n} (q-1) \geq q - 1$$

pues hemos supuesto $n > 1$ y se tiene $q \geq 2$. Pero esta desigualdad es incompatible con el hecho de que $\Phi_n(q)$ divida a $q - 1$ obteniéndose una contradicción. Así $n = 1$, lo que prueba el resultado. □

2.3. Orden de un polinomio y polinomios primitivos

Definición 2.3.1. *Sea $f \in F_q[x]$ un polinomio no nulo. Si $f(0) \neq 0$ entonces al menor entero positivo $e \in \mathbb{N}$ tal que $f(x)$ divide a $x^e - 1$ se denomina **orden de f** y se denota indistintamente por $ord(f)$ u $ord(f(x))$.*
*Por otro lado si $f(0) = 0$, entonces f es de la forma $f(x) = x^h g(x)$, donde $h > 0$ y $g \in F_q[x]$ cumpliendo $g(0) \neq 0$ son únicos. En este caso se tiene por definición que el **orden** de f es igual al orden de g.*

A continuación veremos que para todo polinomio no nulo sobre un cuerpo finito que no se anule en el 0, existe un número entero positivo e tal que dicho polinomio divide a $x^e - 1$ y en consecuencia, el concepto de orden es aplicable a cualquier polinomio.

Lema 2.3.2. *Sea $f \in F_q[x]$ un polinomio de grado $m \geq 1$ con $f(0) \neq 0$. Entonces existe un entero positivo e con, $e \leq q^m - 1$, tal que $f(x)$ divide a $x^e - 1$.*

Demostración. Veamos en primer lugar que el anillo cociente $F_q[x]/(f)$ contiene $q^m - 1$ clases no nulas. Sea $g \in F_q[x]$, realizando la división euclídea se tiene

$$\bar{g}(x) = \bar{q}(x) \cdot \bar{f}(x) + \bar{r}(x) = \bar{r}(x)$$

donde $r(x) = 0$ o $deg(r(x)) < deg(f(x)) = m$. Es decir, podemos identificar la clase del polinomio g con la del resto r . Se tiene entonces que

$$r(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \text{ con } a_i \in F_q \text{ para cada } i = 0, ..., m-1.$$

Habrá por tanto q^m combinaciones posibles para el polinomio $r(x)$. Eliminando aquella en que todos los coeficientes son 0 obtenemos $q^m - 1$ clases no nulas.
Una vez visto esto, se tiene que las q^m clases $x^j + (f)$ con $j = 0, 1, ..., q^{m-1}$ son todas no nulas; por lo que existen enteros r y s con $0 \leq r < s \leq q^m - 1$ tales que $x^s \equiv x^r \, mod \, f(x)$. Ahora, como $f(0) \neq 0$, se tiene que x y $f(x)$ son relativamente primos, de donde $x^{s-r} \equiv 1 \, mod \, f(x)$. Pero entonces $f(x)$ divide a $x^{s-r} - 1$ y se cumple $0 < s - r \leq q^{m-1}$, como se quería demostrar. □

El siguiente resultado caracteriza el orden de un polinomio irreducible sobre un cuerpo finito:

Proposición 2.3.3. *Sea $f \in F_q[x]$ un polinomio irreducible sobre F_q de grado m tal que $f(0) \neq 0$. Entonces $ord(f)$ es igual al orden de cualquiera de sus raíces en el grupo multiplicativo $F^*_{q^m}$.*

Demostración. Sabemos por el corolario 1.4.5 que F_{q^m} es el cuerpo de escisión de f sobre F_q. Además por 1.4.8 todas las raíces de f tienen el mismo orden en el grupo $F^*_{q^m}$. Sea $\alpha \in F^*_{q^m}$ una raíz cualquiera. Aplicando la tercera afirmación de 1.2.8 tendremos que $\alpha^e = 1$ si y solo si $f(x)$ divide a $x^e - 1$. El resultado se sigue ahora directamente de las definiciones de $ord(f)$ y orden de α en $F^*_{q^m}$. □

Corolario 2.3.4. *Si $f \in F_q[x]$ es un polinomio irreducible sobre F_q de grado m entonces $ord(f)$ divide a $q^m - 1$.*

Demostración. Si $f(x) = cx$ con $c \in F^*_q$ entonces $ord(f) = 1$ y el resultado es inmediato. En otro caso el resultado se sigue del resultado anterior y del hecho de que $F^*_{q^m}$ es un grupo de orden $q^m - 1$ y el orden de todo elemento debe dividir al orden del grupo por el teorema de Lagrange (A.1.5). □

A continuación se mostrará un resultado que permitirá calcular el número de polinomios mónicos irreducibles de un determinado grado y orden en un cuerpo finito, aunque antes conviene definir un nuevo concepto:

Definición 2.3.5. *Sean n un entero positivo y b un entero tales que $mcd(n, b) = 1$. LLamaremos **orden multiplicativo** de b módulo n al menor entero positivo k tal que $b^k \equiv 1 \, mod \, n$.*

Proposición 2.3.6. *El número de polinomios mónicos irreducibles en $F_q[x]$ de grado m y orden e es:*

- *$\phi(e)/m$ si $e \geq 2$ y m es el orden multiplicativo de q módulo e, donde ϕ es la función de Euler.*
- ***2*** *si $m = e = 1$.*
- ***0*** *en otro caso.*

Demostración. Sea $f \in F_q[x]$ un polinomio irreducible con $f(0) \neq 0$. Por la proposición 2.3.3 se tiene que $ord(f) = e$ si y solo si todas las raíces de f son raíces e-ésimas primitivas de la unidad. Equivalentemente, $ord(f) = e$ si y solo si f divide al polinomio ciclotómico Φ_e. Ahora bien, aplicando la proposición 2.1.13 cualquier factor irreducible de Φ_e tiene el mismo grado m , donde m es el menor entero positivo tal que $q^m \equiv 1 \, mod \, e$ y el número de dichos factores viene dado por $\phi(e)/m$.

En el caso en que $m = e = 1$ de la fórmula anterior tenemos $\phi(1)/1 = 1$, pero además habrá que considerar el polinomio $f(x) = x$. □

A continuación estudiaremos como determinar el orden de una potencia de un polinomio irreducible, así como el orden del producto de polinomios relativamente primos. Para ello veamos dos resultados previos:

Lema 2.3.7. *Sea c un número entero positivo. Un polinomio $f \in F_q[x]$ tal que $f(0) \neq 0$, divide a $x^c - 1$ si y solo si $ord(f)$ divide a c.*

Demostración. $\Leftarrow$ Si $e := ord(f)$ entonces $f(x)$ divide a $x^e - 1$, ahora aplicando la hipótesis de que e divide a c se tiene que $x^e - 1$ divide a $x^c - 1$, con lo que $f(x)$ divide a $x^c - 1$.
$\Rightarrow$ Si $f(x)$ divide a $x^c - 1$, de la definición de orden de f se tiene que $c \geq e$, luego podemos escribir $c = me + r$ con $m \in \mathbb{N}$ y $0 \leq r < e$. Se tiene pues que

$$x^c - 1 = (x^{me} - 1)\, x^r + (x^r - 1)$$

Pero entonces $f(x)$ debe dividir a $x^r - 1$ y de nuevo por la definición de $ord(f)$ esto solo es posible si $r = 0$. Luego efectivamente e divide a c . □

Lema 2.3.8. *Sean e_1 y e_2 enteros positivos y sea $d = mcd(e_1, e_2)$. Entonces $x^d - 1$ es el máximo común divisor de $x_1^e - 1$ y $x_2^e - 1$ en $F_q[x]$.*

Demostración. Supongamos que $f(x)$ es el máximo común divisor (mónico) de $x_1^e - 1$ y $x_2^e - 1$. Como d es divisor de e_1 y e_2, $x^d - 1$ divide a $x_1^e - 1$ y $x_2^e - 1$. Entonces por la definición de máximo común divisor $x^d - 1$ divide a $f(x)$. Ahora bien, $f(x)$ es divisor común de $x_1^e - 1$ y $x_2^e - 1$, por lo que aplicando el lema anterior se tiene que $ord(f)$ divide a e_1 y e_2. Pero como $d = mcd(e_1, e_2)$, $ord(f)$ divide a d y de nuevo por el lema anterior $f(x)$ divide a $x^d - 1$. En consecuencia $f(x) = x^d - 1$. □

Observación 2.3.9. *Sea un polinomio $f(x)$ tal que $f(0) = 0$. Por la definición de orden, se tiene que $ord(f) = ord(g)$ donde g es un polinomios y h un número entero tales que $f(x) = x^h g(x)$ y $g(0) \neq 0$ siendo además los únicos que cumplen tales condiciones. Por tanto en los siguientes resultados no será necesario considerar polinomios que se anulan en el 0.*

Proposición 2.3.10. *Sea $g \in F_q[x]$ un polinomio irreducible sobre F_q con $g(0) \neq 0$, $e := ord(g)$ y consideremos el polinomio $f(x) = g^b(x)$, donde b es un entero positivo. Sea t el entero más pequeño tal que $p^t \geq b$, donde p es la característica de F_q. Entonces se cumple que $ord(f) = ep^t$.*

Demostración. Tomemos $c := ord(f)$. Como $f(x)$ divide a $x^c - 1$, se tiene que $g(x)$ divide a $x^c - 1$, de donde aplicando el lema 2.3.7, e divide a c .Por otro lado $g(x)$ divide a $x^e - 1$, luego $f(x)$ divide a $(x^e - 1)^b$ (pues $f = g^b$), por lo que $f(x)$ divide a $(x^e - 1)^{p^t} = x^{ep^t} - 1$. Aplicando de nuevo el lema 2.3.7 obtenemos que c divide a ep^t. Se tiene pues que c es de la forma $c = ep^u$ con $0 \leq u \leq t$. Ahora por 2.3.4, se tiene que la característica p no divide a $e = ord(g)$, por lo que aplicando la proposición 2.1.3 el polinomio $x^e - 1$ tendrá solo raíces simples. En consecuencia, todas la raíces de $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ tienen multiplicidad p^u. Pero $g^b(x)$ divide a $x^{ep^u} - 1$, de donde $p^u \geq b$ comparando multiplicidad de raíces y por la elección de t , $u = t$ y $c = ep^t$. □

Proposición 2.3.11. *Sean $g_1, ..., g_k$ polinomios no nulos relativamente primos dos a dos sobre F_q y sea el polinomio $f = g_1 \cdots g_k$. Entonces $ord(f) = mcm\,(ord(g_1), ..., ord(g_k))$.*

Demostración. Como se ha comentado ya anteriormente, podemos suponer que $g_i(0) \neq 0$ para cada $i = 1, ..., k$. Sea $e = ord(f)$, $e_i = ord(g_i)$ para cada $i = 1, ..., k$ y denotemos $c := mcm(e_1, ..., e_k)$. Entonces cada $g_i(x)$ divide a $x^{e_i} - 1$ y así $g_i(x)$ divide a $x^c - 1$. Ahora como los polinomios $g_i(x)$ son relativamente primos $f(x)$ divide a $x^c - 1$ y por 2.3.7 e divide a c . Por otro lado $f(x)$ divide a $x^e - 1$, por lo que cada $g_i(x)$ divide también a $x^e - 1$. De nuevo aplicando el lema 2.3.7 obtenemos que cada e_i divide a e y por tanto c divide a e . Concluimos pues que $e = c$. □

Proposición 2.3.12. *Sea $f_1, ..., f_n$ un conjunto de polinomios no nulos sobre un cuerpo finito F_q. Entonces el orden del mínimo común múltiplo de $f_1, ..., f_n$ es igual al mínimo común múltiplo de los órdenes de cada f_i. Es decir:*

$$ord\,(mcm\,(f_1, ..., f_n)) = mcm\,(ord\,(f_1)\,, ..., ord\,(f_n)).$$

Demostración. Consideremos la factorización canónica de cada polinomio f_i:

$$f_i = g_1^{b_{i_1}} \cdots g_k^{b_{i_k}}$$

con g_i polinomios irreducibles para cada $i = 1, .., n$ y $b_{i_j} \geq 0$ para cada $j = 1, .., k$ admitiendo el caso en que $b_{i_j} = 0$. Definamos ahora el polinomio

$$f := mcm\,(f_1, ..., f_n) = g_1^{max\{b_{i_1}\}} \cdots g_k^{max\{b_{i_k}\}} \text{ con } i = 1, .., n.$$

y denotemos $c_i := ord(g_i)$. Aplicando los resultados 2.3.10 y 2.3.11, considerando p la característica de F_q y teniendo en cuenta que p no divide a los c_j y los g_i son relativamente primos entre sí, se tiene:

$$ord(f) = mcm\left(p^{t_1}c_1, ..., p^{t_k}c_k\right) = p^t mcm(c_1, ..., c_k)$$

donde t_i es el menor entero tal que $p^{t_i} \geq max\{b_{i_j}\}$ con $j = 1, .., k$ y $t = max\{t_i\}$ con $i = 1, ..., n$. Por otro lado

$$ord(f_i) = mcm\left(ord(g_1^{b_{i_1}}), ..., ord(g_k^{b_{i_k}})\right) = mcm\,(p^{r_{i1}}c_1, ..., p^{r_{ik}}c_k) = p^{h_i} mcm(c_1, ..., c_k)$$

donde r_{ij} es el menor entero tal que $p^{r_{ij}} \geq b_{i_j}$ y $h_i = max\,\{r_{ij}\}$. Por tanto

$$mcm\,(ord(f_1), ..., ord(f_n)) = p^{max\{h_i\}} mcm(c_1, ..., c_k) = p^t mcm(c_1, ..., c_k) = ord(f)$$

□

Una vez vistos estos resultados se obtiene de forma directa la siguiente proposición:

Proposición 2.3.13. *Sea F_q un cuerpo finito de característica p, y sea $f \in F_q[x]$ un polinomio de grado positivo con $f(0) \neq 0$. Sea la factorización canónica de f,*
$f = af_1^{b_1} ... f_k^{b_k}$, donde $a \in F_q$, $b_1, ..., b_k \in \mathbb{N}$ y $f_1, ..., f_n$ son polinomios mónicos irreducibles distintos de $F_q[x]$. Entonces $ord(f) = ep^t$, donde e es el el mínimo común múltiplo de $ord(f_1), ..., ord(f_k)$ y t es el menor entero tal que $p^t \geq max\{b_1, ..., b_k\}$.

De los resultados obtenidos hasta el momento se desprende que el orden de cualquier polinomio se puede obtener a partir de conocer los órdenes de los polinomios irreducibles que aparecen en su factorización canónica. Ahora bien, hasta el momento no se ha proporcionado ningún método para el cálculo del orden de polinomios irreducibles más allá del resultado obtenido en la proposición 2.3.3 y para lo cual, necesitamos conocer alguna raíz del polinomio, lo que no siempre será fácil de obtener. A continuación se proporcionará un método para dicho cálculo:
Sea $f \in F_q[x]$ un polinomio irreducible de grado m tal que $f(0) \neq 0$. Tomemos $e := ord(f)$. De la definición de orden de un polinomio se obtiene que e es el menor entero positivo tal que $f(x)$ divide a $x^e - 1$, por tanto e será también el menor entero positivo tal que $x^e \equiv 1 \ mod\ f(x)$. Además por el corolario 2.3.4, e divide a $q^m - 1$. Obviando el caso trivial en que f es un polinomio constante, se verifica $q^m > 2$. Consideremos la factorización de $q^m - 1$:

$$q^m - 1 = p_1^{r_1} \cdots p_s^{r_s} \text{ donde } p_1, ..., p_s \text{ son primos distintos y } r_i \geq 1 \ \forall i = 1, ..., s.$$

Para $1 \leq j \leq s$ calculamos los residuos de $x^{(q^m-1)/p_j} \ mod\ f(x)$:

- Si $x^{(q^m-1)/p_j} \not\equiv 1 \ mod\ f(x)$ entonces e es múltiplo de $p_j^{r_j}$.
- Si $x^{(q^m-1)/p_j} \equiv 1 \ mod\ f(x)$ entonces e no es múltiplo de $p_j^{r_j}$. Habrá entonces que ver si e es múltiplo de $p_j^{r_j-1}, ..., p_j$, calculando los residuos respectivamente de

$$x^{(q^m-1)/p_j^2}, ..., x^{(q^m-1)/p_j^{r_j}} \ mod\ f(x).$$

Procediendo de esta forma para cada factor primo de $q^m - 1$, $e = ord(f)$ será el menor entero positivo que satisfaga las condiciones obtenidas para cada primo p_i.

A continuación veremos un ejemplo en el que se aplicarán los resultados obtenidos hasta el momento en esta sección para el cálculo del orden de un polinomio:

Ejemplo 2.3.14. *Calculemos el orden del polinomio* $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. *Se tiene que la factorización canónica de* $f(x)$ *sobre* $\mathbb{Z}_2$ *es:*

$$f(x) = x^{10} + x^9 + x^3 + x^2 + 1 = \left(x^2 + x + 1\right)^3 \left(x^4 + x + 1\right)$$

Calculemos los órdenes respectivos de $\left(x^2 + x + 1\right)^3$ *y* $\left(x^4 + x + 1\right)$ *por separado:*

- $\left(x^2 + x + 1\right)^3$*: Como el orden de* $x^2 + x + 1$ *debe dividir a* $2^2 - 1 = 3$ *por el corolario 2.3.4, las únicas posibles opciones son 1 y 3. Ahora bien, es claro que* $x^2 + x + 1$ *no divide a* $x - 1$*, por lo que* $ord(x^2 + x + 1) = 3$*. Entonces aplicando la proposición 2.3.10 se tiene que* $ord(x^2 + x + 1)^3 = 3 \cdot 2^2 = 12$.
- $\left(x^4 + x + 1\right)$*: Sabemos que* $ord(x^4 + x + 1)$ *divide a* $2^4 - 1 = 15$ *y por tanto los únicos valores posibles son 1,3,5 o 15. Aplicaremos entonces el método anteriormente explicado. Aplicando el algoritmo de la división se obtiene que* $x^5 \not\equiv 1 \ mod\ (x^4+x+1)$ *por lo que* $ord(x^4 + x + 1)$ *es múltiplo de 3, e igualmente* $x^3 \not\equiv 1 \ mod\ (x^4 + x + 1)$ *por lo que también es múltiplo de 5, con lo que* $ord(x^4 + x + 1) = 15$.

Aplicando entonces la proposición 2.3.11 se tiene que $ord(f) = mcm(12, 15) = 60$*. Un hecho destacable es que* $ord(f)$ *no divide a* $2^{10} - 1$*, lo que muestra que el corolario 2.3.4 no es cierto en general para polinomios no irreducibles.*

Una vez visto este ejemplo, pasaremos ya a la definición y estudio de polinomios primitivos:

Definición 2.3.15. *Diremos que un polinomio $f \in F_q[x]$ de grado $m \geq 1$ es un **polinomio primitivo** sobre F_q si f es el polinomio mínimo sobre F_q de un elemento primitivo de F_{q^m}. Por tanto un polinomio primitivo sobre F_q de grado m será un polinomio mónico, irreducible, que tiene una raíz $\alpha \in F_{q^m}$ que genera el grupo de las unidades $F_{q^m}^*$.*

A continuación se dará una caracterización para este tipo de polinomios:

Proposición 2.3.16. *Un polinomio $f \in F_q[x]$ de grado m es un polinomio primitivo sobre F_q si y solo si f es mónico, $f(0) \neq 0$ y $ord(f) = q^m - 1$.*

Demostración. $\Rightarrow$ Si f es primitivo sobre F_q, entonces f es mónico. Además por ser irreducible se tiene que $f(0) \neq 0$ y $ord(f) = q^m - 1$ aplicando el resultado 2.3.3 y el hecho de que f tiene como raíz algún elemento primitivo de F_{q^m}.
$\Leftarrow$ Si $ord(f) = q^m - 1$ entonces $m \geq 1$. Vamos a ver ahora que f es irreducible sobre F_q. Supongamos por reducción al absurdo que no lo es, entonces f es potencia de un polinomio irreducible o puede expresarse como producto de dos polinomios relativamente primos de grado estrictamente menor que m (no necesariamente irreducibles).

En el primer caso se tiene que $f = g^b$ donde $g \in F_q[x]$ es un polinomio irreducible sobre F_q, $g(0) \neq 0$ y $b \geq 2$. Aplicando la proposición 2.3.10 y denotando la característica de F_q como p , se tiene que $ord(f) = q^m - 1$ es divisible entre p , ahora bien como $q = p^r$ para cierto entero positivo r , esto no es posible, por lo que obtenemos una contradicción.

En el segundo caso tendremos que $f = g_1 \cdot g_2$, donde g_1, g_2 son polinomios mónicos de $F_q[x]$, relativamente primos y de grados respectivos $0 < m_1, m_2 < m$. Si tomamos $e_1 = ord(g_1)$ y $e_2 = ord(g_2)$, obtenemos por la proposición 2.3.11 que se satisface la desigualdad $ord(f) \leq e_1 e_2$, pues $ord(f) = mcm(e_1, e_2)$. Además por el lema 2.3.2 $e_i \leq q^{m_i} - 1$ para $i = 1, 2$, luego:

$$ord(f) \leq (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1+m_2} - 1 = q^m - 1$$

obteniendo de nuevo una contradicción. Por tanto f es irreducible sobre F_q y aplicando 2.3.3 todas sus raíces tendrán orden $q^m - 1$ en el grupo $F_{q^m}^*$, es decir, es un polinomio primitivo. □

Observación 2.3.17. *La condición $f(0) \neq 0$ es solo necesaria para la exclusión del polinomio no primitivo $f(x) = x$ sobre el cuerpo $F_q[x]$.*

Ejemplo 2.3.18. *Consideremos el polinomio $f(x) = x^4+x^3+x^2+2x+2 \in \mathbb{Z}_3[x]$. Como f no tiene raíces en $\mathbb{Z}_3$ ni puede expresarse como producto de polinomios irreducibles de grado 2 de $Z_3[x]$, f es irreducible. Aplicaremos entonces el método provisto anteriormente para calcular su orden. Se tiene que $e := ord(f)$ divide a $3^4 - 1 = 80$, además la factorización en producto de primos es $80 = 2^4 \cdot 5$. Veamos entonces:*

- *Se tiene que el resto de la división (en $\mathbb{Z}_3[x]$) del polinomio x^{40} entre $f(x) = x^4 + x^3 + x^2 + 2x + 2$ es 2, por tanto, $x^{40} \not\equiv 1 \ mod\ f(x)$, luego e es múltiplo de $2^4 = 16$.*
- *De igual forma se obtiene que el resto de la división en $\mathbb{Z}_3[x]$ de x^{16} entre $f(x)$ es $2x^3 + 1$ y por tanto $x^{16} \not\equiv 1 \ mod\ f(x)$, luego e es también múltiplo de 5.*

En consecuencia $e = 80$. Tenemos entonces que f es un polinomio mónico, que no se anula en 0 y tal que $ord(f) = q^m - 1 = 3^4 - 1 = 80$, por lo que aplicando la proposición anterior es un polinomio primitivo.

2.4. Polinomios irreducibles

El objetivo central de la sección será obtener el número de polinomios mónicos irreducibles de un determinado grado sobre un cuerpo finito y encontrar una expresión para el producto de todos ellos. Para ello será necesario dar unos resultados previos e introducir la *fórmula de Moebius*. Aparecerán de nuevo los polinomios ciclotómicos y se utilizarán los resultados obtenidos en la sección para proporcionar un método de cálculo de dichos polinomios mucho más efectivo que el método recurrente dado anteriormente.

Proposición 2.4.1. *Para cada cuerpo finito F_q y cada entero positivo n, el producto de todos los polinomios mónicos e irreducibles sobre F_q cuyos grados dividen a n es igual al polinomio $g(x) = x^{q^n} - x$.*

Demostración. En virtud del resultado 1.4.3 del capítulo anterior, los polinomios mónicos irreducibles que aparecen en la factorización de $g(x) = x^{q^n} - x$ en $F_q[x]$ son precisamente aquellos cuyos grados dividen a n . Ahora bien, como el polinomio derivado de g es $g'(x) = -1$, g no tiene raíces múltiples en su cuerpo de escisión sobre F_q (ver proposición A.7.11). Así cada polinomio mónico irreducible sobre F_q cuyo grado divida a n aparecerá exactamente una vez en la factorización de g en $F_q[x]$. □

Notación: En lo sucesivo utilizaremos los símbolos $\sum_{d|n}$ y $\prod_{d|n}$ para denotar la suma y el producto respectivamente, extendidos a todos los divisores d de n con $d, n \in \mathbb{N}$.

Corolario 2.4.2. *Denotando como $N_q(d)$ al número de polinomios mónicos irreducibles de $F_q[x]$ de grado d, se tiene que para cada entero positivo n se verifica la igualdad:*

$$q^n = \sum_{d|n} d \cdot N_q(d).$$

Demostración. Sea un entero positivo n fijo pero arbitrario. Consideremos el polinomio $g(x) = x^{q^n} - x$. Aplicando el resultado anterior, g es producto de todos los polinomios mónicos irreducibles de $F_q[x]$ cuyos grados dividen a n. Pero entonces se sigue inmediatamente que $deg(g) = q^n$ cumple

$$q^n = \sum_{d|n} d \cdot N_q(d).$$

□

Definición 2.4.3. *La **función de Moebius** $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ es la función definida por*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ es producto de } k \text{ primos distintos}, \\ 0 & \text{si algún primo en la factorización de } n \text{ tiene exponente mayor que 1.} \end{cases}$$

Lema 2.4.4. *Para cada entero positivo n la función de Moebius satisface:*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & si\ n = 1, \\ 0 & si\ n > 1. \end{cases}$$

Demostración. Ver [8], lema 3.23 (página 83). □

A continuación consideraremos una importante igualdad dentro de la teoría elemental de números que será utilizada posteriormente en varios resultados de lo que resta de sección: la *fórmula de inversión de Moebius.*

Teorema 2.4.5 (Fórmula de inversión de Moebius)**.** *Distingamos los casos:*

1. ***Caso aditivo:*** *Sean dos funciones $h, H : \mathbb{N} \longrightarrow G$ donde G es un grupo abeliano aditivo. Entonces:*

$$H(n) = \sum_{d|n} h(d) \quad para\ todo\ n \in \mathbb{N}$$

si y solo si

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \quad para\ todo\ n \in \mathbb{N}$$

2. ***Caso multiplicativo:*** *Sean dos funciones $h, H : \mathbb{N} \longrightarrow G$ donde G es un grupo abeliano multiplicativo. Entonces:*

$$H(n) = \prod_{d|n} h(d) \quad para\ todo\ n \in \mathbb{N}$$

si y solo si

$$h(n) = \prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} \quad para\ todo\ n \in \mathbb{N}$$

Demostración. Ver [8], teorema 3.24 (página 83) y [1], proposición 9.1.18 (página 106). □

Proposición 2.4.6. *El número de polinomios mónicos irreducibles de grado n en $F_q[x]$, que denotaremos por $N_q(n)$, viene dado por:*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Demostración. Aplicaremos el caso aditivo de la fórmula de inversión de Moebius para el grupo $G = \mathbb{Z}$. Consideremos las funciones $h(n) = nN_q(n)$ y $H(n) = q^n$ donde $n \in \mathbb{N}$. Por el corolario 2.4.2 se tiene la igualdad

$$q^n = \sum_{d|n} d \cdot N_q(d)$$

es decir, se tiene que $H(n) = \sum_{d|n} h(d)$ por lo que aplicando la fórmula de inversión de Moebius se tendrá que

$$nN_q(n) = \sum_{d|n} \mu(\frac{n}{d}) q^d = \sum_{d|n} \mu(d) q^{\frac{n}{d}}$$

de donde se obtiene la igualdad deseada. □

Observación 2.4.7. *A partir de este teorema podemos llegar a la misma conclusión que en el corolario 1.4.2; es decir, que para cada potencia de primo q y cada $n \in \mathbb{N}$, existe algún polinomio irreducible en $F_q[x]$ de grado n, pues a partir de la fórmula que proporciona este resultado y teniendo en cuenta que $\mu(1) = 1$ y $\mu(n) \geq -1$ para todo $n \in \mathbb{N}$, se obtiene :*

$$N_q(n) \geq \frac{1}{n}\left(q^n - q^{n-1} - \cdots - q\right) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right) > 0$$

A continuación estudiaremos otra aplicación de la fórmula de inversión de Moebius: proporcionar una fórmula explícita para la expresión de polinomios ciclotómicos.

Proposición 2.4.8. *Sea K un cuerpo de característica p y sea $n \in \mathbb{N}$ no divisible por p. Entonces el n-ésimo polinomio ciclotómico $\Phi_n(x)$ sobre K puede escribirse de la forma*

$$\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(\frac{n}{d})} = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)}.$$

Demostración. Aplicaremos el caso multiplicativo de la fórmula de inversión de Moebius tomando G igual al grupo de las funciones racionales sobre K, es decir, las funciones de la forma $\frac{f}{g}$ con $f, g \in K[x]$. Consideremos las funciones $h(n) = \Phi_n(x)$ y $H(n) = x^n - 1$. Por la segunda afirmación de la proposición 2.1.9 del capítulo anterior se verifica que

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

es decir, que $H(n) = \prod_{d|n} h(d)$. Aplicando la fórmula de inversión de Moebius

$$\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(\frac{n}{d})} = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)}$$

□

Ejemplo 2.4.9. *En el ejemplo 2.1.10 obtuvimos que $\Phi_6(x) = x^2 - x + 1$,veamos ahora que aplicando este nuevo método se obtiene el mismo resultado sin necesidad de obtener los polinomios ciclotómicos anteriores. Sea K un cuerpo cuya característica no divida a 6. Aplicando el resultado anterior se tiene que*

$$\Phi_6(x) = \prod_{d|6} \left(x^{6/d} - 1\right)^{\mu(d)} = (x^6-1)^{\mu(1)}(x^3-1)^{\mu(2)}(x^2-1)^{\mu(3)}(x-1)^{\mu(6)} =$$
$$= \frac{(x^6-1)(x-1)}{(x^3-1)(x^2-1)} = x^2 - x + 1$$

tal y como se obtuvo anteriormente.

En la proposición 2.4.6 se proporcionó una fórmula para determinar el número de polinomios mónicos irreducibles en $F_q[x]$ de un determinado grado. El objetivo ahora será dar una fórmula para determinar el polinomio resultante de hacer el producto de todos ellos, polinomio al que denotaremos $I(q,n;x)$, donde n hará referencia al grado de los polinomios.

Proposición 2.4.10. *Se verifica que el producto de todos los polinomios mónicos irreducibles de grado n en $F_q[x]$, denotado como $I(q,n;x)$, viene dado por la fórmula*

$$I(q,n;x)=\prod_{d|n}\left(x^{q^d}-x\right)^{\mu(\frac{n}{d})}=\prod_{d|n}\left(x^{q^{n/d}}-x\right)^{\mu(d)}$$

Demostración. Por la proposición 2.4.1 se tiene que $x^{q^n}-x=\prod_{d|n}I(q,d;x)$. Aplicando ahora el caso multiplicativo de la fórmula de inversión de Moebius considerando el grupo de las funciones racionales sobre F_q y tomando las funciones $h(n)=I(q,n;x)$ y $H(n)=x^{q^n}-x$ para todo $n\in\mathbb{N}$ se obtiene la fórmula del enunciado. □

Enunciaremos por último un resultado que permitirá expresar $I(q,n;x)$ como producto de polinomios ciclotómicos y así conocer cuáles son exactamente los polinomios mónicos irreducibles de $F_q[x]$.

Proposición 2.4.11. *Para $n>1$ se verifica la igualdad*

$$I(q,n;x)=\prod_{m}\Phi_m(x)$$

donde el producto está extendido a aquellos divisores m de q^n-1 para los que n es el orden multiplicativo de q módulo m, es decir, aquellos divisores m para los que n es el menor entero tal que $q^n\equiv 1\ mod\ m$ y donde $\Phi_m(x)$ es el m-ésimo polinomio ciclotómico sobre F_q.

Demostración. Sea $n>1$ y consideremos el conjunto S de los elementos de F_{q^n} de grado n sobre F_q. Se tiene pues que para cada $\alpha\in S$ su polinomio mínimo sobre F_q tendrá grado n y será así una raíz de $I(q,n;x)$. Recíprocamente si γ es raíz de $I(q,n;x)$ entonces será raíz de algún polinomio mónico irreducible con grado n de $F_q[x]$, por lo que $\gamma\in S$. Así se tiene la igualdad:

$$I(q,n;x)=\prod_{\alpha\in S}(x-\alpha)\qquad(1)$$

Si $\alpha\in S$ entonces $\alpha\in F_{q^n}^*$ y el orden de α en $F_{q^n}^*$ será divisor de q^n-1. Observemos que $\gamma\in F_{q^n}^*$ es un elemento de un subcuerpo propio de F_{q^n}, que podemos denotar F_{q^d}, si y solo si $\gamma^{q^d}=\gamma$, o lo que es igual si y solo si el orden de γ divide a q^d-1. Así se obtiene que el orden, denotado por m , de un elemento $\alpha\in S$ debe verificar que n sea el menor entero positivo cumpliendo que $q^n\equiv 1\ mod\ m$, es decir, que n sea el orden multiplicativo de q módulo m . Consideremos m un divisor positivo de q^n-1 en estas condiciones y denotemos como S_m el conjunto de elementos de S de orden m en $F_{q^n}^*$, S será entonces unión disjunta de los subconjuntos S_m y la igualdad (1) puede escribirse como

$$I(q,n;x)=\prod_{m}\prod_{\alpha\in S_m}(x-\alpha)$$

Ahora bien S_m contiene exactamente todos los elementos de $F_{q^n}^*$ de orden m , o lo que es igual, es el conjunto de raíces m-ésimas primitivas de la unidad sobre F_q. Entonces directamente de la definición de polinomio ciclotómico se tiene que

$$\prod_{\alpha \in S_m} (x - \alpha) = \Phi_m(x)$$

y así

$$I(q, n; x) = \prod_m \Phi_m(x)$$

□

Ejemplo 2.4.12. *Determinar todos los polinomios mónicos irreducibles en* $\mathbb{Z}_2[x]$ *de grado 4.*

Aplicando la proposición 2.4.10 se tiene la igualdad

$$I(q, n; x) = \frac{(x^{16} - x)}{(x^4 - x)} = x^{12} + x^9 + x^6 + x^3 + 1$$

por lo que habrá tres polinomios mónicos irreducibles. Unos sencillos cálculos permiten obtener que los únicos divisores m *de* $q^n - 1 = 2^4 - 1 = 15$ *tales que* $2^4 \equiv \ mod\, m$ *son 5 y 15 por lo que* $I(q, n; x) = \Phi_5(x)\Phi_{15}(x)$.

Ahora por la proposición 2.1.13 del capítulo anterior sabemos que $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ *es irreducible, mientras que* $\Phi_{15}(x)$ *puede expresarse como producto de dos polinomios irreducibles en* $\mathbb{Z}_2[x]$ *de grado 4. Aplicando el método proporcionado en 2.4.8 para el cálculo de polinomios ciclotómicos se tiene que*

$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 \text{ en } \mathbb{Z}_2[x]$$

Ahora observemos que $\Phi_5(x + 1) = x^4 + x^3 + 1$ *es irreducible y distinto de* $\Phi_5(x)$, *por lo que será uno de los que aparezcan en la factorización de* $\Phi_{15}(x)$. *Realizando la división*

$$\frac{x^8 + x^7 + x^5 + x^4 + x^3 + x + 1}{x^4 + x^3 + 1} = x^4 + x - 1 = x^4 + x + 1$$

obtenemos el otro polinomio. Por tanto los polinomios mónicos irreducibles de grado 4 en $\mathbb{Z}_2[x]$ *serán:*

$$x^4 + x^3 + x^2 + x + 1, \quad x^4 + x^3 + 1 \quad y \quad x^4 + x + 1.$$

2.5. Factorización de polinomios. Algoritmo de Berlekamp

En la presente sección se proporcionará un método para la expresión de un polinomio, que podremos suponer mónico, $f(x) \in F_q[x]$ de grado positivo en la forma:

$$f(x) = f_1(x)^{r_1} \cdots f_k(x)^{r_k}$$

donde $f_i(x)$ son polinomios mónicos irreducibles distintos de $F_q[x]$ y $r_i \geq 1$ para cada $i = 1, ..., k$. Para ello se hará uso del *algoritmo de Berlekamp.*

En primer lugar veremos que podemos limitarnos al caso en que el polinomio $f(x)$ no tenga factores múltiples, es decir, el caso en que todos los r_i sean igual a 1 en la factorización. Denotando $d(x) := mcd(f(x), f'(x))$ distingamos los siguientes casos:

1. Si $d(x) = 1$, entonces directamente $f(x)$ no tiene factores múltiples.
2. Si $d(x) = f(x)$, entonces $f'(x) = 0$ y por tanto $f(x) = g(x)^{p^r}$ para cierto polinomio $g(x)$ y donde p es la característica de F_q. A continuación se repite el razonamiento sustituyendo $f(x)$ por $g(x)$.
3. Si $d(x) \neq 1$, entonces $d(x)$ es un factor no trivial de $f(x)$ y así el polinomio $f(x)/d(x)$ no tiene factores múltiples, en cuyo caso la factorización de $f(x)$ se reduce a la de los polinomios $d(x)$ y $f(x)/d(x)$.

Así en lo sucesivo se supondrá que $f(x)$ es un polinomio sin factores múltiples.

Proposición 2.5.1. *Si $f(x) \in F_q[x]$ es un polinomio mónico y $h(x) \in F_q[x]$ es tal que $h(x)^q \equiv h(x)\ mod\ f(x)$, entonces*

$$f(x) = \prod_{c \in F_q} mcd\,(f(x), h(x) - c)$$

Demostración. Tomando $c, c' \in F_q$ con $c \neq c'$, se tiene

$$\frac{1}{c' - c}\,(h(x) - c) - \frac{1}{c' - c}\,(h(x) - c') = 1$$

por lo que $mcd\,(h(x) - c, h(x) - c') = 1$, aplicando A.5.10.

Por tanto, $mcd\,(f(x), h(x) - c')$ y $mcd\,(f(x), h(x) - c)$ son relativamente primos cuando $c \neq c'$ y se tiene que

$$\left(\prod_{c \in F_q} mcd\,(f(x), h(x) - c)\right) \mid\ f(x)$$

Por otro lado, aplicando el lema 1.3.6, el polinomio $x^q - x \in F_q[x]$ factoriza en este anillo en la forma

$$x^q - x = \prod_{c \in F_q} (x - c)$$

de donde por la hipótesis $h(x)^q \equiv h(x)\ mod\ f(x)$, se tiene que

$$f(x)\ |\,(h(x)^q - h(x)) = \prod_{c \in F_q} (h(x) - c)$$

Así,

$$f(x)\ |\ \prod_{c \in F_q} mcd\,(f(x), h(x) - c)$$

y como ambos polinomios son mónicos

$$f(x) = \prod_{c \in F_q} mcd\,(f(x), h(x) - c)$$

□

En general, la descomposición obtenida en la proposición anterior no conduce a la factorización completa de $f(x)$, pues alguno de los polinomios $mcd\,(f(x), h(x) - c)$ puede no ser irreducible en $F_q[x]$. Es más, si $f(x)|\,(h(x) - c)$ para algún $c \in F_q$, entonces la descomposición es trivial.

Definición 2.5.2. *Un polinomio $h(x) \in F_q[x]$ tal que $h(x)^q \equiv h(x)\ mod\ f(x)$, donde $f(x) \in F_q[x]$ es un polinomio mónico, se dice* ***f(x)-reductor*** *si da lugar a una descomposición de f(x) no trivial.*

El algoritmo de Berlekamp hace uso del teorema chino de los restos (A.7.19) para construir polinomios $f(x)$-reductores. Es claro que si $h(x)^q \equiv h(x)\ mod\ f(x)$ y $0 < deg(h(x)) < deg(f(x))$, entonces $h(x)$ es un polinomio $f(x)$-reductor.

Consideremos ahora $f(x) = f_1(x) \cdots f_k(x)$ una factorización en irreducibles de $f(x)$ en $F_q[x]$. Sea $(c_1, ..., c_k)$ una k-upla de elementos de F_q. Aplicando el teorema chino de los restos existe un polinomio $h(x)$, único módulo $f(x)$, tal que

$$h(x) \equiv c_i \ \ mod \ \ f_i(x) \text{ para } 1 \leq i \leq k \quad \text{y} \quad deg(h(x)) < deg(f(x)) \tag{1}$$

y por tanto

$$h(x)^q \equiv c_i^q = c_i \equiv h(x)\ mod\ f_i(x)$$

de donde

$$h(x)^q \equiv h(x)\ mod\ f(x).$$

Recíprocamente, si $h(x)$ cumple que $h(x)^q \equiv h(x)\ mod\ f(x)$ y $deg(h(x)) < deg(f(x))$, a partir de la condición

$$h(x)^q - h(x) = \prod_{c \in F_q} (h(x) - c)$$

se obtiene que para cada $f_i(x)$ existe un $c_i \in F_q$ tal que $f_i(x) | (h(x) - c_i)$ y en consecuencia

$$h(x) \equiv c_i\ mod\ f_i(x)$$

de donde se concluye que $h(x)$ es el único polinomio obtenido por el procedimiento anterior para la k-upla $(c_1, ..., c_k)$.
Este razonamiento permite deducir que existen exactamente q^k soluciones de (1) y eliminando aquellos polinomios con grado 0, se tendrá que hay $q^k - q$ polinomios $f(x)$-reductores $h(x)$, con $0 < deg(h(x)) < deg(f(x))$. A continuación se detallará un método para determinarlos.

Sea $n := deg(f(x))$. Se tiene que $h(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F_q[x]$ cumple que

$$h(x)^q \equiv h(x)\ mod\ f(x)$$

si y solo si

$$h(x)^q = a_0 + a_1 x^q + \cdots + a_{n-1} x^{(n-1)q} \equiv a_0 + a_1 + \cdots + a_{n-1} x^{n-1}\ mod\ f(x)$$

donde para el cálculo de $h(x)^q$ se han aplicado los resultados A.2.15 y 1.3.3.
Ahora tomando para $0 \leq i \leq n-1$

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j\ mod\ f(x),$$

donde los b_{ij} son coeficientes en F_q adecuados, y sustituyendo en la condición previa, se tiene:

$$\sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1} b_{ij} x^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i b_{ij} \right) x^j = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

o lo que es equivalente en notación matricial

$$(a_0, a_1, ..., a_{n-1}) = (a_0, a_1, ..., a_{n-1})B \quad \text{donde } B = (b_{ij}).$$

En consecuencia, encontrar polinomios $f(x)$-reductores es equivalente a encontrar soluciones del sistema

$$(a_0, ..., a_{n-1})(B - I_n) = 0 \qquad (2)$$

Ya sabemos que este sistema tiene q^k soluciones, por tanto la dimensión del espacio núcleo de la matriz $B - I_n$ es k , y así el rango de $B - I_n$ es $n - k$. Existirán entonces polinomios no constantes $h_2(x), ..., h_k(x)$ con $0 < deg(f_i(x)) < n$ tales que los vectores determinados por sus coeficientes junto con el vector (1,0,...,0), que siempre es solución y corresponde al polinomio $h(x) = 1$, formarán una base del espacio vectorial núcleo. Los polinomios $h_i(x)$ con $i = 2, ..., k$ son $f(x)$-reductores. Además todos los polinomios $f(x)$-reductores serán precisamente aquellos que estén en el subespacio generado por los vectores de coeficientes de $h_1(x), ..., h_k(x)$ menos el generado por $(1, 0, ..., 0)$.

A continuación se procederá a describir el **algoritmo de Berlekamp:**

1. Dado $f(x)$ con $n := deg(f)$, se toman

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \ mod \ f(x)$$

   donde $0 \leq i < n$. Se calcula el rango de la matriz $(B - In)$, que se denotará como r , de donde se obtiene el número de factores irreducibles de $f(x)$, que será igual a $k = n - r$.

2. Si $k = 1$ entonces $f(x)$ es irreducible. Si $k > 1$, se resuelve el sistema (2), tomamos el polinomio $h_2(x)$ asociado a un vector solución y se calcula $mcd\,(f(x), h_2(x) - c)$ para cada $c \in F_q$, utilizando por ejemplo el algoritmo de Euclides (ver [8], página 22). El resultado será una factorización no trivial de $f(x)$, aunque no necesariamente con factores irreducibles.

3. Si la factorización obtenida consta de k factores el proceso acaba. En caso contrario se calcula el $mcd\,(g(x), h_3(x) - c)$ para cada $c \in F_q$ y cada factor $g(x)$ obtenido con $h_2(x)$.

Procediendo sucesivamente de esta forma se obtiene la factorización buscada.

A continuación comprobaremos la efectividad del algoritmo. Para ello tendremos que ver que dos factores irreducibles distintos de $f(x)$ se obtienen de la aplicación del algoritmo con distintos polinomios $h_i(x)$, donde recordemos se está considerando $f(x)$ sin factores múltiples.

Sean $f_1(x)$ y $f_2(x)$ dos factores irreducibles distintos de $f(x)$ y consideremos

$$h_j(x) \equiv c_{j1} \ mod \ f_1(x) \text{ y } h_j(x) \equiv c_{j2} \ mod \ f_2(x)$$

para $1 \leq j \leq k$. Entonces $c_{j1} = c_{j2}$ obliga a que para cualquier solución de

$$h(x)^q \equiv h(x) \ mod \ f(x)$$

con $deg(h(x)) < deg(f(x))$ (que será una combinación lineal de $h_1(x), ..., h_k(x)$) existe $c \in F_q$ tal que

$$h(x) \equiv c \ mod \ f_1(x) \qquad \text{y} \qquad h(x) \equiv c \ mod \ f_2(x)$$

Ahora bien, por el teorema chino de los restos sabemos que existe alguna solución $h(x)$ tal que

$$h(x) \equiv 0 \ mod \ f_1(x) \qquad \text{y} \qquad h(x) \equiv 1 \ mod \ f_2(x)$$

y así $c_{j1} \neq c_{j2}$ para cierto $j \in \{1, ..., k\}$. Por tanto $h(x) - c_{j1}$ será divisible por $f_1(x)$ pero no por $f_2(x)$.

Ejemplo 2.5.3. *Factorizar el polinomio* $f(x) = x^8 + x^6 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.

1. El polinomio derivado de $f(x)$ es

$$f'(x) = 8x^7 + 6x^5 + 4x^3 + 3x^2 + 1 = x^2 + 1$$

ahora como $mcd\,(f(x), f'(x)) = 1$, $f(x)$ no tiene factores múltiples.

2. Se calculan las potencias $x^{i2} \ mod \ f(x)$ para $i = 0, ..., 7$ obteniendo:

$$\begin{array}{ll} x^0 \equiv 1 \ mod \ f(x) & x^8 \equiv 1 + x^3 + x^4 + x^6 \ mod \\ x^2 \equiv x^2 \ mod \ f(x) & x^{10} \equiv 1 + x^2 + x^3 + x^4 + x^5 \ mod \ f(x) \\ x^4 \equiv x^4 \ mod \ f(x) & x^{12} \equiv x^2 + x^4 + x^5 + x^6 + x^7 \ mod \\ x^6 \equiv x^6 \ mod \ f(x) & x^{14} \equiv 1 + x + x^3 + x^4 + x^5 \ mod \ f(x) \end{array}$$

3. Se obtienen las matrices B y $(B - I_8)$:

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$B - I_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Estudiando el rango se obtiene que $rg(B - I_8) = 6$, por lo que $f(x)$ tiene dos factores irreducibles.

4. Resolviendo el sistema

$$(a_0, ..., a_7)(B - I_8) = (0, ..., 0)$$

se obtienen los vectores solución $(1,0,0,0,0,0,0,0)$ y $(0,1,1,0,0,1,1,1)$, y por tanto los polinomios $h_1(x) = 1$ y $h_2(x) = x^7 + x^6 + x^5 + x^2 + x$.

5. Mediante el algoritmo de Euclides calculamos $mcd(f(x), h(x) - c)$ con $c \in \mathbb{Z}_2$, obteniendo:

$$mcd(f(x), h_2(x)) = x^6 + x^5 + x^4 + x + 1 \quad \text{y} \quad mcd(f(x), h_2(x) - 1) = x^2 + x + 1$$

por lo que que $f(x) = \left(x^6 + x^5 + x^4 + x + 1\right)\left(x^2 + x + 1\right)$.

Apéndice A

Anexo

Esta sección estará dedicada a definir algunos conceptos necesarios para la correcta comprensión del texto y mostrar los resultados que, pese a no ser específicos de cuerpos finitos, son utilizados a lo largo del trabajo. Las pruebas de dichos resultados se remitirán a obras de la bibliografía.

A.1. Grupos

Definición A.1.1. *Un **grupo** es un par $(G, \cdot)$ formado por un conjunto no vacío G y una operación $\cdot$ en G que cumple:*

1. *Es asociativa: para cualesquiera $x, y, z \in G$, se tiene $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.*
2. *Tiene elemento neutro que llamaremos uno o identidad: existe $1 \in G$ tal que para cada $x \in G$ se tiene $x \cdot 1 = x = 1 \cdot x$.*
3. *Todo elemento $x \in G$ tiene simétrico: existe $y \in G$ tal que $x \cdot y = 1 = y \cdot x$.*

*Además diremos que un grupo es **abeliano** si la operación es conmutativa, es decir, si $a \cdot b = b \cdot a \ \forall a, b \in G$.*

En lo sucesivo se utilizará simplemente el término *grupo* para referirnos a un grupo abeliano.

Observación A.1.2. *A la hora de denotar un grupo G pueden utilizarse dos tipos de notaciones:*

- ***Notación aditiva:** Se considera el grupo G con la operación $+$,se escribe como 0 el elemento neutro, $-a$ el inverso y $na = a + \overset{n}{\cdots} + a$ con $n \in \mathbb{N}$ la potencia de cada $a \in G$. Se dice en este caso que G es un grupo **aditivo.***
- ***Notación multiplicativa:** Se considera el grupo G con la operación $\cdot$,se escribe como 1 el elemento neutro, a^{-1} el inverso y $a^n = a \overset{n}{\cdots} a$ con $n \in \mathbb{N}$ la potencia de cada $a \in G$. Se dice en este caso que G es un grupo **multiplicativo.***

Definición A.1.3. *Sea $(G, \cdot)$ un grupo. Un **subgrupo** de G es un subconjunto H de G cerrado para el producto, es decir $\forall a, b \in H \ ab \in H$, y tal que $(H, \cdot)$ es un grupo. Denotaremos que H es un subgrupo de G escribiendo $H < G$.*

Definición A.1.4. *Se llama **orden** de un grupo finito G a su cardinal, que se denotará por $|G|$.*
*Se llama **orden** de un elemento $a \in G$ donde G es un grupo, al menor entero positivo n tal que $a^n = 1$, (si dicho entero existe) y se denotará como $o(a) = n$.*

Todo grupo G tiene exactamente un elemento de orden 1, además si G es finito todo elemento de G tiene orden. A continuación se enunciará el teorema de Lagrange, fundamental para la caracterización de los órdenes de los subgrupos de un grupo:

Teorema A.1.5 (Teorema de Lagrange)**.** *Si G es un grupo finito, el orden de cualquier subgrupo de G divide al orden de G. En particular, el orden de cualquier elemento de un grupo finito divide al orden del grupo.*

Demostración. Ver [2], teorema 3.9, capítulo 4 (página 77). □

Definición A.1.6. *Un grupo G se dice **cíclico** si existe algún elemento $g \in G$ tal que todo $h \in G$ puede escribirse como $h = g^n$ para algún entero positivo n, en cuyo caso diremos que g es un generador del grupo G y se escribirá $G = \langle g \rangle$.*

Directamente de la definición se obtiene que un grupo finito G de orden n es cíclico si y solo si existe un elemento $g \in G$ de orden n , es decir:

$$G = \langle g \rangle = \left\{ g^1, ..., g^n = 1 \right\}$$

Lema A.1.7. *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Ver [2], teorema 4.3, capítulo 4 (página 82). □

Teorema A.1.8 (Primer teorema de estructura de grupos)**.** *Sea A un grupo abeliano finito no trivial. Existe una colección, unívocamente determinada por A, de enteros $d_1, ..., d_s$ mayores que 1 cumpliendo las siguientes condiciones:*

1. *$d_i | d_{i+1}$ para cada $i = 1, ..., s-1$.*
2. *$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$.*

Demostración. Ver [2], teorema 3.1, capítulo 8 (página 137). □

A continuación se introducirán tres nuevos términos relacionados con el concepto de grupo: *centro*, *normalizador* y *clase de conjugación de un elemento*, para terminar con un último resultado conocido como la *ecuación de clases.*

Definición A.1.9. *Sea G un grupo y sean elementos $a, x \in G$. El **conjugado** de a por x es elemento $a^x = x^{-1}ax$. Un elemento $b \in G$ es un conjugado de a si es de la forma $b = a^x$ para cierto $x \in G$.*

La relación ser conjugados es una relación de equivalencia en un grupo G . Las clases de equivalencia para dicha relación se llaman **clases de conjugación** de G , de modo que G es la unión disjunta de sus clases de conjugación. La clase de conjugación de un elemento a se denota por a^G, es decir, $a^G = \{a^x : x \in G\}$.

Definición A.1.10. *Sea S un subconjunto no vacío de un grupo g. Se llama* ***normalizador*** *de S en G al conjunto*

$$N(S) = \left\{a \in G : aSa^{-1} = S\right\}.$$

Definición A.1.11. *Dado un grupo G, se define su* ***centro*** *como el subconjunto*

$$Z(G) = \{a \in G : ag = ga \ \forall g \in G\}$$

Proposición A.1.12 (Ecuación de clases)**.** *Sea G un grupo finito y Ω un conjunto de representantes de las clases de conjugación con más de un elemento de G. Entonces se verifica la fórmula*

$$|G| = |Z(G)| + \sum_{b \in \Omega} \left|b^G\right|$$

Demostración. Ver [4], proposición 5.9.5 (página 140). □

A.2. Anillos, dominios y cuerpos

Definición A.2.1. *Un* ***anillo*** *es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones $+$ y $\cdot$ en A, generalmente llamadas suma y producto respectivamente, que verifican:*

1. *$(A, +)$ es un grupo abeliano. Al elemento neutro de $(A, +)$, que sabemos que es único, se le denominará elemento* ***cero*** *(o cero) y se denotará por 0.*
2. *El producto es asociativo.*
3. *Se verifica la propiedad distributiva, es decir, dados $a, b, c \in A$ se verifica*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad y \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Si el producto es conmutativo se dirá que el anillo es ***conmutativo****. Si tiene elemento neutro para el producto, que llamaremos uno o identidad y se denotará como 1, se dirá que es anillo* ***unitario****.*

Definición A.2.2. *Si $(A, +, \cdot)$ es un anillo, un subconjunto $B \subseteq A$ se dice que es un* ***subanillo*** *de A si B es cerrado para la suma y el producto, $1 \in B$ y $(B, +, \cdot)$ es un anillo.*

La siguiente proposición proporciona una caracterización para identificar si un subconjunto de un anillo es en efecto un subanillo:

Proposición A.2.3. *Sea A un anillo y $B \subseteq A$ un subconjunto. Son equivalentes:*

1. *B es un subanillo de A.*
2. *$1 \in B$ y si $a, b \in B$ entonces $a + b \in B$, $ab \in B$ y $-a, -b \in B$.*
3. *$1 \in B$ y si $a, b \in B$ entonces $a - b \in B$ y $ab \in B$.*

Demostración. Ver [4], proposición 2.3.2 (página 40). □

Definición A.2.4. *Un subconjunto I de un anillo A se dice que es un **ideal** de A si verifica:*

1. $a + b \in I \quad \forall a, b \in I$.
2. $ra \in I \quad \forall a \in I \ , \forall r \in A$.
3. $I \neq \emptyset$.

Definición A.2.5. *Si A es un anillo cualquiera y $b \in A$ el conjunto*

$$(b) = \{ba : a \in A\}$$

*es un ideal de A llamado **ideal principal generado por b**.*

Definición A.2.6. *Sean A un anillo e I un ideal propio de A, es decir, $I \neq A$.*
*Se dice que I es **maximal** si no está contenido en ningún ideal propio de A (excepto en sí mismo).*
*Se dice que I es **primo** si $\forall a, b \in A$ la relación $ab \in I$ implica $a \in I$ o $b \in I$.*

Proposición A.2.7. *Todo ideal maximal es también un ideal primo.*

Demostración. Ver [4], proposición 2.8.6 (página 53). □

Definición A.2.8. *Un elemento $a \in A$, donde A es un anillo, se dice **divisor de cero** si existe algún $b \in A$ no nulo tal que $ab = 0$.*

Definición A.2.9. *Un anillo en el que el único elemento divisor de cero es el propio cero recibe el nombre de **dominio**.*

Proposición A.2.10. *Sea K un cuerpo y $B \subseteq K$ un subconjunto. Son equivalentes:*

1. *B es un subcuerpo de K.*
2. *$0, 1 \in B$ y si $a, b \in B$ entonces $a - b \in B$ y $ab^{-1} \in B$.*

Demostración. Consecuencia de la proposición A.2.3 y la definición de subcuerpo. □

Proposición A.2.11. *Todo cuerpo es un dominio y todo dominio finito es un cuerpo.*

Demostración. Ver [8], teorema 1.31 y observación previa (página 12). □

Proposición A.2.12. *Se verifican las siguiente propiedades para un anillo A y un ideal I de A:*

1. *I es un ideal maximal $\iff$ A/I es un cuerpo.*

2. I es un ideal primo $\iff$ A/I es un dominio.

Demostración. Ver [4], proposición 2.8.6 (página 53). □

Proposición A.2.13. *Las siguientes condiciones son equivalentes para un anillo A:*

1. A es un cuerpo.

2. Los únicos ideales de A son 0 y el propio A.

Demostración. Ver [10], proposición 2.39, capítulo 0. □

Proposición A.2.14. *Si $f : K \longrightarrow A$ es un homomorfismo de anillos, siendo K un cuerpo y A un anillo entonces f es inyectivo. En particular, todo homomorfismo de cuerpos es inyectivo.*

Demostración. Ver [10], corolario 2.40, capítulo 0. □

Lema A.2.15. *Sea A un anillo con característica prima p. Entonces se verifican las siguientes relaciones:*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad y \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

para todo $n \in \mathbb{N}$ y $a, b \in A$.

Demostración. Ver [8], teorema 1.46 (página 16). □

A.3. Congruencias y anillos cociente

Definición A.3.1. *Sean $a, b \in \mathbb{Z}$ y consideremos $n \in \mathbb{N}$. Se dice que a es **congruente** con b módulo n, y se denotará $a \equiv b \ mod\ n$, si n divide a la diferencia $a - b$, es decir, si existe $k \in \mathbb{Z}$ tal que $a = b + kn$.*

Es fácil ver que la relación ser congruentes módulo n es una relación de equivalencia en $\mathbb{Z}$. Las clases de equivalencia para esta relación serán los conjuntos:

$$\begin{aligned}
&\overline{0} = \{..., -2n, -n, 0, n, 2n, ...\} \\
&\overline{1} = \{..., -2n+1, -n+1, 1, n+1, 2n+1, ...\} \\
&. \\
&. \\
&. \\
&\overline{n-1} = \{..., -n-1, -1, n-1, 2n-1, 3n-1, ...\}
\end{aligned}$$

Definiendo la siguiente operación:

$$\overline{a} + \overline{b} = \overline{a+b} \qquad (1)$$

obtenemos que el conjunto $\left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$ junto con esta operación tiene estructura de grupo abeliano, cuyo elemento neutro es $\overline{0}$.

Además la operación $\cdot$ dada por

$$\overline{a} \cdot \overline{b} = \overline{ab} \qquad (2)$$

cuyo elemento neutro es $\overline{1}$, dota al conjunto de estructura de anillo conmutativo.

Definición A.3.2. *Al anillo formado por las clases de equivalencia* $\left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$ *junto con las operaciones (1) y (2) anteriormente definidas se le llama anillo de enteros módulo n y se denota como* $\mathbb{Z}_n$.

Más detalles en [8] (páginas 4 y 5) y [2], ejemplo 3.1, capítulo 2 (página 38).

Notación: Las clases de equivalencia $\left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$ pueden denotarse también como $\{[0], [1], ..., [n-1]\}$.

Definición A.3.3. *Sea un anillo A y sea I un ideal de A. Se dice que dos elementos* $a, b \in A$ *son* ***congruentes*** *módulo I y se denota* $a \equiv b \ mod\ I$, *si la diferencia de ambos pertenece al ideal I, es decir:*

$$a \equiv b \ mod\ I \Longleftrightarrow a - b \in I$$

De igual forma que antes la relación ser congruente módulo I es una relación de equivalencia en A y por tanto, las clases de equivalencia por esta relación definen una partición de A. La clase de equivalencia de un elemento $a \in A$ será

$$[a] = \overline{a} = a + I = \{a + x : x \in I\}$$

tomando $0 + I = I$. Se tiene entonces que

$$a + I = b + I \Longleftrightarrow a \equiv b \ mod\ I.$$

El conjunto de las clases de equivalencia se denota por $A/I = \{a + I : a \in A\}$.

Definición A.3.4. *Sea A un anillo e I un ideal de A. Las operaciones suma y producto en* A/I *dadas por*

$$(a + I) + (b + I) = (a + b) + I \qquad (a + I) \cdot (b + I) = (ab) + I$$

están bien definidas y dotan a A/I *de estructura de anillo con neutro* $0 + I$ *y unidad* $1 + I$. *Este anillo recibe el nombre de* ***anillo cociente*** *de A módulo I.*

Nota: Más detalles en [4] (páginas 43 y 44) y [8] (páginas 13 y 14).

A.4. Homomorfismos.

Definición A.4.1. *Sean A y B dos grupos. Diremos que una aplicación* $f : A \longrightarrow B$ *es un* ***homomorfismo de grupos*** *si se verifica:*

1. $f(ab) = f(a)f(b) \quad \forall a, b \in A.$
2. $f(1) = 1.$

Definición A.4.2. *Sean A y B dos anillos. Diremos que una aplicación* $f : A \longrightarrow B$ *es un* ***homomorfismo de anillos*** *si se verifica:*

1. $f(a + b) = f(a) + f(b)\ \forall a, b \in A.$
2. $f(ab) = f(a)f(b)\ \forall a, b \in A.$

3. $f(1) = 1$.

Definición A.4.3. *Un homomorfismo de un anillo (resp. un grupo) en sí mismo recibirá el nombre de* ***endomorfismo.***
Un homomorfismo de anillos (resp. de grupos) que sea biyectivo se le denominará ***isomorfismo de anillos*** *(resp.* ***isomorfismo de grupos****).*
Sean A y B anillos (resp. grupos) y supongamos que existe un isomorfismo de anillos (resp. de grupos) entre A y B, diremos entonces que A y B son ***isomorfos*** *y se denotará $A \cong B$.*
A un isomorfismo de un anillo (resp. un grupo) en sí mismo se le denominará ***automorfismo****.*

Definición A.4.4. *Sea $f : A \longrightarrow B$ una aplicación. Se define el* ***núcleo*** *de f y se denotará $Kerf$ como el conjunto:*

$$Kerf = \{a \in A : f(a) = 0\}$$

Se llama ***imagen*** *de f y se denotará Imf al conjunto:*

$$Imf = \{b \in B : b = f(a) \text{ para cierto } a \in A\}$$

Proposición A.4.5. *Un homomorfismo de anillos $f : A \longrightarrow B$ es inyectivo si y solo si $Kerf = 0$.*

Demostración. Ver [4], proposición 2.6.7 (página 49). □

Teorema A.4.6 (Primer teorema de isomorfia para grupos)**.** *Sea $f : G \longrightarrow H$ un homomorfismo de grupos. Existe un único isomorfismo de grupos $\overline{f} : G/Kerf \longrightarrow Imf$ tal que $i \circ \overline{f} \circ p = f$ donde i es la inclusión $i : Imf \hookrightarrow H$ y p es la proyección canónica $p : G \longrightarrow G/Kerf$.*

Demostración. Ver [2], teorema 2.1 y corolario 2.2, capítulo 5 (páginas 95 y 96). □

Teorema A.4.7 (Primer teorema de isomorfia para anillos)**.** *Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Existe un único isomorfismo de anillos $\overline{f} : A/Kerf \longrightarrow Imf$ tal que $i \circ \overline{f} \circ p = f$ donde i es la inclusión $i : Imf \hookrightarrow B$ y p es la proyección $p : A \longrightarrow A/Kerf$ dada por $p(a) = a + Kerf$.*

Demostración. Ver [4], teorema 2.7.4 (página 50). □

Lema A.4.8. *Sea G un grupo finito de orden m y sea n un entero tal que $mcd(n, m) = 1$. Entonces la aplicación $f : G \longrightarrow G$ dada por $f(a) = a^n$ es un automorfismo.*

Demostración. Ver [9], lema A.4.2 (página 141). □

Lema A.4.9 (de Artin)**.** *Sea $\varphi_1, ..., \varphi_m$ un conjunto de homomorfismos no nulos distintos de un grupo G en el grupo multiplicativo de las unidades F^* de un cuerpo F y sean $a_1, ..., a_n \in F$ no todos nulos. Entonces existe $g \in G$ tal que:*

$$a_1\varphi_1(g) + \cdots + a_m\varphi_m(g) \neq 0$$

Demostración. Ver [8], lema 2.33 (página 55). □

A.5. Divisibilidad y factorización.

Definición A.5.1. *Sea A un anillo y sean $a, b \in A$. Se dice que a **divide a** b (en A), y se denotará $a|b$, si existe algún $c \in A$ tal que $b = ac$.*

Definición A.5.2. *Dos elementos $a, b \in A$, donde A es un anillo, se dicen **asociados** si $a|b$ y $b|a$.*

Definición A.5.3. *Sea un anillo A y sea $a \in A$. Diremos que a es un elemento **irreducible** (en A) si $a \neq 0$, a no es una unidad y si $a = bc$ con $b, c \in A$ se verifica que $b \in A^*$ o $c \in A^*$. Diremos que a es **primo** (en A) si $a \neq 0$, a no es una unidad y la relación $a|bc$ implica $a|b$ o $a|c$.*

Observación A.5.4. *Se tiene siempre que todo elemento primo es un un elemento irreducible, sin embargo, el recíproco no es cierto, en general, para anillos arbitrarios.*

Definición A.5.5. *Sea A un anillo, S un subconjunto de A y consideremos un elemento $d \in A$. Diremos que d es un **máximo común divisor** de S si verifica las siguientes condiciones:*

1. *d divide a cada elemento de S.*
2. *Si existe otro elemento $x \in A$ que divida a cada elemento de S entonces x divide a d.*

Si d es máximo común divisor de S, se denotará como $d = mcd(S)$, entendiendo que tal elemento es único salvo asociados.

Definición A.5.6. *Sea a un anillo, S un subconjunto de A y un elemento $d \in A$. Se dice que m es un **mínimo común múltiplo** de S si verifica las siguientes condiciones:*

1. *m es es múltiplo de cada elemento de S.*
2. *Si existe otro elemento $x \in A$ tal que x es múltiplo de todo elemento de S entonces x es múltiplo de m.*

Si m es máximo común divisor de S, se denotará como $m = mcm(S)$, entendiendo que dicho elemento es único salvo asociados.

A continuación se definirán y estudiarán algunas de las propiedades básicas de tres tipos de dominios: dominios euclídeos, dominios de ideales principales y dominios de factorización única.

Definición A.5.7. *Sea D un dominio. Una **función euclídea** en D es una aplicación $\delta : D\backslash\{0\} \longrightarrow \mathbb{Z}^+$ que cumple las siguientes propiedades:*

1. *Si $a, b \in D\backslash\{0\}$ son tales que $a|b$ entonces $\delta(a) \leq \delta(b)$.*
2. *Dados $a, b \in D$ con $b \neq 0$ existen $q, r \in D$ tales que $a = bq + r$ y se cumple que $r = 0$ o bien $\delta(r) < \delta(b)$.*

*Un **dominio euclídeo (DE)** es un dominio que admite una función euclídea.*

Definición A.5.8. *Un dominio D se dice que es un **dominio de ideales principales (DIP)** si para todo ideal I de D existe $a \in D$ tal que $I = (a)$, es decir, si todos los ideales de D son ideales principales.*

Proposición A.5.9. *Si D es un DIP y $a \in D \backslash D^*$ es un elemento no nulo, las siguientes condiciones son equivalentes:*

1. *a es irreducible.*
2. *(a) es un ideal maximal.*
3. *$A/(a)$ es un cuerpo.*
4. *a es primo.*
5. *(a) es un ideal primo.*
6. *$A/(a)$ es un dominio.*

Demostración. Ver [4], proposición 3.2.3 (página 70). □

Proposición A.5.10. *Sea D un DIP y sean $d \in D$ y $a_1, ..., a_n \in D$. Entonces d es máximo común divisor de $a_1, ..., a_n$ si y solo si $d|a_i$ para cada $i = 1, ..., n$ y existen $r_1, ..., r_n \in D$ tales que*

$$a_1 r_1 + \cdots + r_n a_n = d$$

Demostración. Consecuencia de que el ideal generado por los a_i será:

$$(a_1, ..., a_n) = \{c_1 a_1 + \cdots c_n a_n : c_1, \cdots, c_n \in D\}$$

y por ser D un DIP existe $b \in D$ tal que $(a_1, ..., a_n) = (b)$. El resultado se obtiene entonces de la condición:

$$a \text{ divide a } b \Longleftrightarrow (b) \subseteq (a)$$

□

Pasemos ahora a definir el concepto de dominio de factorización única, para lo cual, habrá que definir en primer lugar qué es una factorización de un elemento:

Definición A.5.11. *Sea D un dominio. Una **factorización** en producto de irreducibles de un elemento $a \in D$ es una expresión del tipo:*

$$a = up_1 \cdots p_n$$

donde $n \in \mathbb{N}$ (admitiendo el caso n=0), $u \in D^*$ y $p_1, ..., p_n$ son irreducibles de D.
*Diremos que D es un **dominio de factorización** si todo elemento no nulo de D admite una factorización en producto de irreducibles.*
Dos factorizaciones de un elemento $a \in D$ en producto de irreducibles

$$a = up_1 \cdots p_n = vq_1 \cdots q_m$$

*se dicen **equivalentes** si $n = m$ y existe una permutación σ de $\mathbb{N}_n$ (es decir, una biyección de $\{1, ..., n\}$ en sí mismo) tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, ..., n$.*
*Diremos que D es un **dominio de factorización única (DFU)** si es un dominio de factorización en el que para todo $a \in D$, todas las factorizaciones de a son equivalentes.*

Terminaremos la sección enunciando un resultado que relaciona los tres tipos de dominios definidos anteriormente

Proposición A.5.12. *Todo dominio euclídeo es un dominio de ideales principales y a su vez, todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Ver [4], proposición 3.3.3 (página 72) y proposición 3.4.6 (página 78). □

A.6. Operadores lineales

En esta sección se darán algunas definiciones y resultados básicos acerca de operadores lineales, que serán utilizados más tarde en el Capítulo 1 para demostrar la existencia de bases normales.

Definición A.6.1. *Se llama **operador lineal** a una aplicación lineal entre espacios vectoriales.*

Definición A.6.2. *Sea V un espacio vectorial y sea $T : V \longrightarrow V$ un operador lineal.*
*Se dice que un polinomio $p(x) = a_n x^n + \cdots + a_0$ **anula** a T si $p(T) = 0$, en el sentido de que si $a_n T + \cdots + a_0$ es la aplicación nula sobre V.*
*Se llama **polinomio mínimo** de T al polinomio mónico de menor grado que anula a T.*
*Se llama **polinomio característico** de T al polinomio resultante de realizar el determinante de $xI - A$ siendo A la matriz asociada al operador T respecto de una determinada base.*

Proposición A.6.3. *Sea V un espacio vectorial y $T : V \longrightarrow V$ un endomorfismo. Entonces el grado del polinomio característico de V es siempre igual a la dimensión de V.*

Demostración. Consecuencia de [5], lema 11.26. (página 184). □

Proposición A.6.4. *El polinomio mínimo de un operador lineal divide al polinomio característico.*

Demostración. Ver [5], corolario 11.28. (página 186). □

Definición A.6.5. *Un vector $v \in V$ se dice **cíclico** de T si el conjunto $\{T^k(v) : K \geq 0\}$ es un conjunto generador de V.*

Proposición A.6.6. *Un operador lineal T tiene un vector cíclico si y solo si el polinomio característico de T es igual al polinomio mínimo.*

Demostración. Consecuencia de [5], lema 11.26. (página 184). □

A.7. Polinomios

Definición A.7.1. *Sea A un anillo. LLamaremos* ***anillo de polinomios*** *en la variable x con coeficientes en A y se denotará $A[x]$ al conjunto:*

$$A[x] = \{a_n x^n + \cdots + a_1 x + a_0 : a_i \in A, n \in \mathbb{N}\}$$

Cada elemento de $A[x]$ recibe el nombre de ***polinomio*** *con coeficientes en A, o también polinomio sobre A.*

Observación A.7.2. *Si A es un anillo, entonces la suma y el producto usual de polinomios dotan a $A[x]$ de estructura de anillo.*

Nota: Más detalles en [2], capítulo 3, sección 3.1 (páginas 159 y 160).

Definición A.7.3. *Consideremos un polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$.*
Se llamará ***grado*** *de $p(x)$, y se denotará $deg(p(x))$, al mayor exponente de la indeterminada x con coeficiente no nulo y dicho coeficiente recibirá el nombre de* ***coeficiente principal****. LLamaremos* ***coeficiente independiente*** *de p al coeficiente a_0.*

Definición A.7.4. *Un polinomio se dice que es* ***mónico*** *si su coeficiente principal es 1.*

Definición A.7.5. *Un polinomio $p(x) \in A[x]$ se dice que es* ***irreducible*** *si no puede expresarse como producto de dos o más polinomios de $A[x]$ de grado estrictamente menor.*

Definición A.7.6. *Diremos que $\alpha \in A$ es una* ***raíz*** *del polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ si $p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$*

Definición A.7.7. *Sean los polinomios $p_1, ..., p_n \in A[x]$, donde A es un anillo. Entonces si $mcd(p_1, ..., p_n) = 1$, se dice que dichos polinomios son* ***relativamente primos****.*

Proposición A.7.8. *Sea A un anillo. Un elemento $\alpha \in A$ es raíz del polinomio $p(x) \in A[x]$ si y solo si el polinomio $x - \alpha$ divide a $p(x)$ en $A[x]$.*

Demostración. Ver [8], teorema 1.64 (página 27). □

Definición A.7.9. *Sea α raíz de $p(x) \in A[x]$. Se define la* ***multiplicidad*** *de α como raíz de $p(x)$ como el mayor entero m tal que $(x - \alpha)^m$ divide a $p(x)$.*
Si la multiplicidad de α es 1 diremos que α es una raíz ***simple****.*
Si la multiplicidad de α es mayor que 1 diremos que es una raíz ***múltiple****.*

Definición A.7.10. *Consideremos un polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$. Se llama* ***polinomio derivado*** *de $p(x)$ y se denota $p'(x)$ al polinomio*

$$p'(x) = n a_1 x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1$$

Proposición A.7.11. *Una raíz α de un polinomio $p(x)$ es una raíz múltiple si y solo si $p'(\alpha) = 0$.*

Demostración. Ver [4], proposición 4.3.7 (página 94). □

Teorema A.7.12. *Un polinomio de grado n sobre un cuerpo cualquiera tiene a lo sumo n raíces contando multiplicidades.*

Demostración. Consecuencia de aplicación sucesiva de la proposición A.7.8. □

Proposición A.7.13. *Sea K un anillo con* $0 \neq 1$. *Las siguientes afirmaciones son equivalentes:*

1. *K es un cuerpo.*
2. *El anillo de polinomios* $K[x]$ *es un DIP.*

Demostración. Ver [10], teorema 2.19, capítulo 2 (página 9). □

Proposición A.7.14. *Sea F un cuerpo. Se tiene que* $F[x]/(p(x))$ *es un cuerpo si y solo si* $p(x)$ *es irreducible en* $F[x]$.

Demostración. Ver [8], teorema 1.61 y observación previa (página 25). □

Proposición A.7.15. *Si K es un cuerpo, entonces el anillo de polinomio* $K[x]$ *es un dominio euclídeo. De hecho, la aplicación* $gr : K[x]\backslash\{0\} \longrightarrow \mathbb{Z}^+$ *que asocia a cada polinomio f su grado es una función euclídea.*

Demostración. Ver [4], proposición 3.3.7 (página 74). □

Como consecuencia se tiene el siguiente resultado

Proposición A.7.16. *Sea K un cuerpo y sea* $g \in K[x]$ *un polinomio no nulo. Entonces para cada* $f \in K[x]$, *existen polinomios* $q, r \in K[x]$ *tales que*

$$f = qg + r \text{ donde } deg(r) < deg(g).$$

Proposición A.7.17. *Sea un cuerpo K y consideremos los polinomios* $f_1, ..., f_n \in K[x]$ *no todos nulos. Entonces existe un único polinomio mónico* $d \in K[x]$ *tal que d es máximo común divisor de* $f_1, ..., f_n$. *Además dicho polinomio d puede expresarse de la forma:*

$$d = b_1 f_1 + \cdots + b_n f_n \text{ con } b_1, ..., b_n \in K[x]$$

Demostración. Ver [8], teorema 1.55 (página 21). □

A continuación enunciaremos un importante teorema sobre el que se apoyan diversos resultados a lo largo del texto: *la Propiedad Universal del Anillo de Polinomios*. Existe una versión análoga a dicho teorema para anillos de polinomios en n indeterminadas, sin embargo, solo se necesitará la versión para anillos de polinomios en una indeterminada.

Teorema A.7.18. *(Propiedad Universal del Anillo de Polinomios) Sean A y B dos anillos,* $\varphi : A \longrightarrow B$ *un homomorfismo,* $b \in B$ *y denotemos como* $u : A \hookrightarrow A[x]$ *la inclusión de A en* $A[x]$. *Entonces existe un único homomorfismo de anillos* $f : A[x] \longrightarrow B$ *que cumple* $f \circ u = \varphi$, *o equivalentemente que la restricción de f a A (vía u) cumple* $f|_A = \varphi$ *y además* $f(x) = b$.

Demostración. Ver [4], proposición 4.2.1 (página 90). □

A continuación se enunciará el teorema chino de los restos, teorema que pese a ser válido en un contexto más general se utilizará únicamente para el caso del anillo de polinomios sobre un cuerpo:

Teorema A.7.19 (Teorema Chino de los Restos)**.** *Sea F un cuerpo, $f_1, ..., f_k \in F[x]$ polinomios relativamente primos dos a dos y consideremos polinomios arbitrarios $g_1, ..., g_h \in F[x]$. Entonces las el sistema de congruencias:*

$$h \equiv g_i \ mod \ f_i \qquad con \ i = 1, ..., k$$

tiene solución única módulo $f = f_1 \cdots f_k$.

Demostración. Ver [6], teorema 2.25 (página 131). □

Se definirá a continuación el anillo de polinomios en n indeterminadas:

Definición A.7.20. *Sea A un anillo y $\{x_1, ..., x_n\}$ conjunto de n indeterminadas que llamamos variables. Se llamará **polinomio** en las variables x_i y coeficientes en A a toda combinación de la forma*

$f(x_1, ..., x_n) = \sum_{i \in \mathbb{N}^n} a_i x_1^{i_1} \cdots x_n^{i_n}$ *donde* $a_i \in A \ \forall i = (i_1, ..., i_n) \in \mathbb{N}^n$ *y* $a_i = 0$ *para c. t. i*

El conjunto de los polinomios en $x_1, ..., x_n$ con coeficientes en A será denotado por $A[x_1, ..., x_n]$.

Si A es un anillo, entonces también es posible dotar a $A[x_1, ..., x_n]$ de estructura de anillo, al igual que ocurre para anillos de polinomios en una indeterminada. Este anillo recibirá el nombre de **anillo de polinomios** en las variables $x_1, ..., x_n$ y coeficientes en A. (Ver [10], proposición 1.1 y observación previa, capítulo 1).

El objetivo a continuación será presentar las fórmulas de Cardano-Vieta que relacionan las raíces de un polinomio con los coeficientes de dicho polinomio. Para ello se necesitará la definición previa de los polinomios simétricos elementales:

Definición A.7.21. *Sea K un cuerpo. Un polinomio $p \in K[x_1, ..., x_n]$ se dice que es **simétrico** si para toda permutación $\sigma \in S_n$, la aplicación φ_σ de $K[x_1, ..., x_n]$ en sí mismo que es la identidad sobre K y actúa en las variables x_i como $\varphi_\sigma(x_i) = x_{\sigma(i)}$ verifica que $\varphi_\sigma(f) = f$. Se llaman **polinomios simétricos elementales** en n indeterminadas a los polinomios:*

$$s_r^n(x_1, ..., x_n) = \sum_{1 \le i_1 \le ... \le i_r \le n} x_{i_1} \cdots x_{i_r} \ con \ 0 \le r \le n$$

Proposición A.7.22 (Fórmulas de Cardano-Vieta)**.** *Sea D un DFU. Sea $f = \sum_{i=0}^n a_i x^i \in D[x]$ un polinomio mónico,es decir, $a_n = 1$. Supongamos que f se factoriza en $D[x]$ como $f = (x - \alpha_1)...(x - \ \alpha_n \ )$. Entonces si $s_1, ..., s_n$ denotan los polinomios simétricos elementales en n indeterminadas sobre D, se tiene:*

$$a_{n-r} = (-1)^r s_r(\alpha_1, ..., \alpha_n) \ para \ cada \ r = 1, ..., n.$$

Demostración. Ver [1], proposición 1.5.13 (página 26). □

La sección terminará con la definición de cuerpo de escisión de un conjunto de polinomios y el teorema de existencia y unicidad de dichos cuerpos de escisión.

Definición A.7.23. *Sea K un cuerpo y sea un polinomio $f \in K[x]$ con $deg(f) = r \geq 1$. Se dice que f se* ***escinde o factoriza completamente*** *sobre K si se verifica*

$$f = c(x - a_1) \cdots (x - a_r)$$

donde $c \in K$ y cada $x - a_i \in K[x]$.

Definición A.7.24. *Sea una extensión F/K y sea P un conjunto de polinomios no constantes sobre $K[x]$ (que puede estar formado por un solo polinomio). Diremos que F es el* ***cuerpo de escisión*** *(también llamado en algunos textos* ***cuerpo de descomposición****) del conjunto P sobre K si se verifican las siguientes condiciones:*

1. *Todo polinomio de P se escinde sobre F .*
2. *Si denotamos como S al conjunto de todos los elementos de F que son raíces de alguno de los polinomios de P, entonces $K(S) = F$.*

Antes de enunciar el teorema de existencia y unicidad introduzcamos los conceptos de *K-homomorfismo* y *K-isomorfismo*:

Definición A.7.25. *Dadas dos extensiones L/K y F/K del cuerpo K, llamaremos* ***K-homomorfismo*** *a un homomorfismo $\varphi : L \longrightarrow F$ que verifica $\varphi(a) = a \ \forall a \in K$. Un isomorfismo que cumple esta última propiedad recibe el nombre de* ***K-isomorfismo****.*

Teorema A.7.26 (Existencia y unicidad de cuerpos de escisión)**.** *Sea K un cuerpo y sea P un conjunto de polinomios no constantes de $K[x]$. Existe un cuerpo de escisión de P sobre K y además es único salvo K-isomorfismos.*

Demostración. Ver [1], proposición 4.1.5 y corolario 4.1.7 (páginas 60 y 61). □

Bibliografía

[1] J. Asensio Mayor, J.R. Caruncho Castro, J. Martínez Hernández, *Ecuaciones Algebraicas*, DM, Murcia, 2002.

[2] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul, *Basic abstract algebra*, Cambridge University Press, Cambridge, 1986.

[3] S.D Cohen, S. Huczynska, *The primitive normal basis theorem - without a computer*, Journal of the Mathematical Society, **67**, 2003.

[4] A. Del Río Mateos, J.J Simón Pinero, A. Del Valle Robles, *Álgebra Básica*, DM, Murcia, 2006.

[5] B. Hartley, T.O Hawkes, *Rings, Modules and Linea Algebra*, Chapman and Hall, London, 1970.

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

[7] A. Lempel, M.J. Weinberger, *Self-complementary normal bases for finite fields*, SIAM Journal on Discrete Mathematics, **1**, 1988.

[8] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambrigde University Press, Cambridge, 1986.

[9] G.L. Mullen, C.Mummert, *Finite Fields and Aplications*, American Mathematical Society, Providence, Rhode Island, 2007.

[10] M. Saorín Castaño, *Apuntes asignatura Ecuaciones Algebraicas*, Universidad de Murcia, curso 2013/2014.

Índice terminológico