XXVII ESCUELA VENEZOLANA DE MATEMÁTICAS
EMALCA-VENEZUELA 2014

INTRODUCCIÓN A LOS ANILLOS FINITOS Y SUS APLICACIONES

Edgar Martínez-Moro, Alejandro Piñera-Nicolás
e Ignacio Fernández Rúa

MÉRIDA, VENEZUELA, 31 de agosto al 5 de septiembre de 2014

XXVII ESCUELA VENEZOLANA DE MATEMÁTICAS
EMALCA - VENEZUELA 2014

Introducción a los Anillos Finitos y sus Aplicaciones

E. Martínez-Moro, A. Piñera-Nicolás

Instituto de Investigación en Matemáticas y
Departamento de Matemática Aplicada
Universidad de Valladolid, España
edgar@maf.uva.es, anicolas@maf.uva.es

I.F. Rúa

Departamento de Matemáticas
Universidad de Oviedo. España
rua@uniovi.es

MÉRIDA, VENEZUELA, 31 DE AGOSTO AL 5 DE SEPTIEMBRE DE 2014

XXVII ESCUELA VENEZOLANA DE MATEMÁTICAS

La Escuela Venezolana de Matemáticas es una actividad de los postgrados en matemáticas de las instituciones siguientes: Centro de Estudios Avanzados del Instituto Venezolano de Investigaciones Científicas, Facultad de Ciencias de la Universidad Central de Venezuela, Facultad de Ciencias de la Universidad de Los Andes, Universidad Simón Bolívar, Universidad Centroccidental Lisandro Alvarado y Universidad de Oriente, y se realiza bajo el auspicio de la Asociación Matemática Venezolana. La XXVII Escuela Venezolana de Matemáticas recibió financiamiento de la Academia de Ciencias Físicas, Matemáticas y Naturales de Venezuela, el Banco Central de Venezuela, el Fondo Nacional de Ciencia, Tecnología e Innovación (FONACIT), el Instituto Venezolano de Investigaciones Científicas (Centro de Estudios Avanzados, Departamento de Matemáticas y Ediciones IVIC), la Universidad de los Andes (CEP, CDCHT, Departamento de Matemáticas de la Facultad de Ciencias, Decanato de Ciencias y Vicerrectorado Administrativo), Unión Matemática de América Latina y el Caribe (UMALCA) y Centre International de Mathematiques Pures et Appliquees (CIMPA).

2010 Mathematics Subject Classication: 11T30; 94B99; 13M05; 13M10

Instituto Venezolano de Investigaciones Científicas
Rif: G-20004206-0

Introducción a los anillos infnitos y sus aplicaciones
E. Martínez-Moro, A. Piñera-Nicolás, I.F. Rúa

Diseño y edición: Escuela Venezolana de Matemáticas
Preprensa e impresión: Gráficas Lauki C.A.
Deposito legal: If66020145102244
ISBN: 978-980-261-151-5
Caracas, Venezuela
2014

Índice general

Prefacio

En las áreas matemáticas en las que se involucra el modelado algebraico es de suma importancia disponer de modelos discretos adecuados para su implementación práctica. Usualmente para la mayoría de las aplicaciones, especialmente en el ámbito de la criptografía y de la codificación algebraica, los modelos de cálculo y computación subyacente han sido los cuerpos finitos y sus anillos de polinomios. Sin embargo numerosos estudios apuntan a que un modelo más general, el anillo finito, aporta un mejor control de la situación de modelado. El ejemplo paradigmático es la demostración por Hammos et. al.[1] de que diversos códigos binarios no lineales se pueden ver como módulos sobre el anillo finito $\mathbb{Z}_4$ de los enteros módulo 4. Desde ese momento el estudio de códigos sobre anillos (de cadena, anillos de tipo Galois, anillos de cadena y el caso más general de anillos finitos de Frobenius) ha sido una de las más fructíferas áreas de investigación en la codificación algebraica. De igual forma se pueden observar similares hitos en diferentes áreas relacionadas con la criptografía, combinatoria y la computación discreta-simbólica (*shift registers, system theory, design theory*, etc).

El principal objetivo de este texto es el entrenamiento del lector en las construcciones básicas en el ámbito de los anillos finitos. Un conocimiento mínimo de álgebra abstracta (teoría básica de grupos y anillos) y álgebra lineal será deseable para seguir el curso. En el Capítulo 1 (Preliminares) se apuntan aquellos resultados previos que el alumno debe recordar de sus encuentros anteriores con el álgebra. El desarrollo del curso en la Escuela Venezolana de Matemáticas 2014 se adaptará a la formación inicial del alumnado y será lo más autocontenido posible. La

[1] Hammons AR Jr, Kumar PV, Calderbank AR, Sloane NJA, Sole P (1994) "The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals and related codes". IEEE Trans. Inform. Theory 40:301–319

imposibilidad de cubrir todas las aplicaciones de los anillos finitos nos ha hecho centrarnos en los códigos algebraicos sobre los que los autores centran su investigación en este momento. Como complemento al curso hemos realizado unas sesiones en SAGE[2] que estarán disponibles para los participantes en la escuela y que mostrarán las principales construcciones del texto desde un punto de vista computacional. También, para aquél lector interesado en profundizar en la temática del curso, hemos recopilado en un breve anexo (sin duda sesgado en su contenido por nuestros intereses) unas pinceladas sobre las lecturas que pueden seguir en el ámbito de los códigos algebraicos.

Los autores de estas notas desean agradecer a La Escuela Venezolana de Matemáticas y todas las organizaciones que la auspician la invitación para dictar este curso y la ayuda y paciencia brindada para la elaboración de las notas y la realización del curso. Este agradecimiento se extiende de forma particular a Stella Brasesco y Carlos Uzcategui por su ayuda en todo momento.

Septiembre de 2014, Los Autores

[2]William A. Stein et al. *Sage Mathematics Software*. The Sage Development `http://www.sagemath.org`.

Capítulo 1

Preliminares

El presente capítulo es una enumeración de resultados previos que el lector debe conocer del álgebra conmutativa relativos a anillos, ideales y módulos. Todos ellos se encuentran enunciados en el libro clásico de Atiyah y MacDonald [1] en sus dos primeros capítulos. Es recomendable al menos una lectura previa rápida de los preliminares para fijar la notación y conceptos a utilizar durante todo el texto.

1.1. Anillos e ideales

Un *anillo* A es un conjunto con dos operaciones $+ : A \times A \to A$, $(a_1, a_2) \mapsto a_1 + a_2$, y $\cdot : A \times A \to A$, $(a, a_1) \mapsto a \cdot a_1$, que denominamos *suma* y *producto*, tales que

1. A es un grupo abeliano con respecto a la suma.

2. La multiplicación es asociativa y distributiva con respecto al producto.

Durante todo el texto sólo consideraremos anillos conmutativos con unidad, es decir verificando $a \cdot b = b \cdot a$, $a, b \in A$ y que contengan un elemento $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$. Salvo que explícitamente se cite otro caso entenderemos por anillo un anillo conmutativo con unidad.

Diremos que un anillo A es un *cuerpo* si para cada elemento $a \in A$ no nulo existe su inverso respecto de la multiplicación que denotaremos a^{-1}.
Una aplicación $f : A \to B$ entre los anillos A y B, diremos que es un *homomorfismo* de anillos si cumple

1. $f(a_1 + a_2) = f(a_1) + f(a_2)$, para todo par $a_1, a_2 \in A$.
2. $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$, para todo par $a_1, a_2 \in A$.
3. $f(1_A) = 1_B$.

La imagen y el núcleo de f son subanillos de B y de A respectivamente, es decir, un subconjuntos de B y de A que, con las operaciones correspondientes en A o B, son anillos. La composición de homomorfismos de anillos es un homomorfismo de anillos.
Un subconjunto $\mathfrak{a} \subseteq A$ del anillo A diremos que es un *ideal* de A si es un subgrupo del grupo abeliano $(A, +)$ y cumple que $a \cdot \lambda \in \mathfrak{a}$ para todo $a \in A$ y todo $\lambda \in \mathfrak{a}$. La intersección de ideales es un ideal. Dado un subconjunto $S \subseteq A$, denotaremos por $\langle S \rangle$ al ideal mínimo de A que contiene a S, es decir, la intersección de todos los ideales de A que contienen a S.

$$\langle S \rangle = \left\{ a \in A \mid a = \sum_{i=1}^{n} a_i \cdot s_i \text{ donde } s_i \in S, a_i \in A \text{ y } n \text{ natural} \right\}.$$

Dado $a \in A$, notaremos por $\langle a \rangle = aA$ y lo denominaremos *ideal principal* generado por a.
Como $\mathfrak{a}$ es un subgrupo de A, podemos considerar el grupo cociente $A/\mathfrak{a}$. Definimos el producto de las clases de equivalencia como la clase que contiene el producto de dos de sus representantes. Se puede comprobar que dicho producto está bien definido y que dota a $A/\mathfrak{a}$ de una estructura de anillo que es la única que podemos definir en $A/\mathfrak{a}$ de modo que el morfismo de paso al cociente $A \to A/\mathfrak{a}$ sea un homomorfismo de anillos.

Proposición 1.1.1. *Sea $\mathfrak{a} \subseteq A$ un ideal del anillo A y $\pi : A \to A/\mathfrak{a}$ el homomorfismo de paso al cociente. Se verifica la correspondencia biunívoca entre los ideales de A que contienen a $\mathfrak{a}$ y los ideales de $A/\mathfrak{a}$.*

Un ideal $\mathfrak{p} \subseteq A$ del anillo A diremos que es un *ideal primo* de A si cumple que si $a \cdot b \in \mathfrak{p}$ entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. un ideal $\mathfrak{a} \subseteq A$ es *primario* si y sólo si para todo a y b tales que $ab \in \mathfrak{a}$, si $a \notin \mathfrak{a}$ entonces existe un entero natural n tal que $b^n \in \mathfrak{a}$.
Un elemento $a \in A$ diremos que es un *divisor de cero* si existe un elemento $b \in A$ no nulo tal que $a \cdot b = 0$. Diremos que un *anillo de integridad o íntegro* el elemento nulo es el único divisor de cero. Diremos que un ideal $\mathfrak{m} \subseteq A$ es *maximal* si los únicos ideales que contienen a $\mathfrak{m}$ son $\mathfrak{m}$ y A.

Proposición 1.1.2. *Sea A un anillo.*

1. *Un ideal $\mathfrak{p} \subseteq A$ es un ideal primo de A si y sólo si $A/\mathfrak{p}$ es un anillo íntegro.*
2. *En todo anillo $A \neq 0$ existen ideales maximales.*
3. *En todo anillo $A \neq 0$ existen ideales primos minimales.*
4. *Todo ideal $\mathfrak{a} \subseteq A$ está incluido en un ideal maximal.*
5. *Un ideal $\mathfrak{m} \subseteq A$ es maximal si y sólo si $A/\mathfrak{m}$ es un cuerpo. En particular, los ideales maximales son ideales primos.*

Aquellos anillos que tienen exactamente un anillo maximal se denominan *locales.*

Proposición 1.1.3.

1. *Sea A un anillo y $\mathfrak{m} \neq \langle 1 \rangle$ un ideal de A tal que cada $x \in A - \mathfrak{m}$ es una unidad de A. Entonce A es un anillo local y $\mathfrak{m}$ su único ideal maximal.*
2. *Sea A un anillo y $\mathfrak{m}$ un ideal maximal de A tal que cada elemento de $1 + \mathfrak{m}$ es una unidad de A. Entonces A es un anillo local.*

Un elemento $x \in A$ del anillo A es *nilpotente* si existe un entero no negativo n tal que $x^n = 0$. El conjunto $\mathfrak{N}$ de todos los elementos nilpotentes de A es un ideal que se denomina *nilradical* de A.

Proposición 1.1.4. *El nilradical de A es la intersección de todos los ideales primos de A.*

El *radical de Jacobson* $\mathfrak{R}$ de un anillo A es la intersección de todos los ideales maximales de A.

Proposición 1.1.5. *Un elemento $x \in \mathfrak{R}$ pertenece al radical de Jacobson si y sólo si $1 - xy$ es una unidad en A para todo elemento $y \in A$.*

1.2. Módulos

Sea A un anillo y M un conjunto. Diremos que una operación $+ : M \times M \to M$, $(m_1, m_2) \mapsto m_1 + m_2$ y una aplicación $\cdot : A \times M \to M$, $(a, m) \mapsto a \cdot m$ definen en M una estructura de *A-módulo* cuando cumplen

1. $(M, +)$ es un grupo conmutativo.
2. $a \cdot (m + n) = a \cdot m + a \cdot n$, para todo $a \in A$ y $m, n \in M$.
3. $(a + b) \cdot m = a \cdot m + b \cdot m$, para todo $a, b \in A$ y $m \in M$.
4. $(ab) \cdot m = a \cdot (b \cdot m)$, para todo $a, b \in A$ y $m \in M$.
5. $1 \cdot m = m$, para todo $m \in M$.

Nótese que todo ideal $\mathfrak{a} \subseteq A$ es un A-módulo con la suma definida y el producto ya definido en A. Un subconjunto $N \subseteq M$ de un A-módulo M es un *submódulo* de M si con la operaciones que definen M es un A-módulo. Como N es un subgrupo de M, podemos considerar el grupo cociente M/N. Definimos el producto de una clase de equivalencia por un elemento del anillo $a \in A$ como la clase que contiene el producto de uno de sus representantes por a. Se puede comprobar que dicho producto está bien definido y que dota a M/N de una estructura de módulo.
Sea $\{M_i\}_{i \in I}$ una familia de A-módulos. Su *producto directo* se denotará por $\prod_{i \in I} M_i$, mientras que su *suma directa* $\bigoplus_{i \in I} M_i$ denotará el subconjunto de $\prod_{i \in I} M_i$ formado por aquellos elementos con un número finito de entradas no nulas. Ambos son A-módulos con la suma definida componente a componente y el producto por un elemento $a \in A$ se realiza multiplicanco cada una de sus componentes por a.
Una aplicación $f : M \to M$ entre A-módulos M_1, M_2 es un *homomorfismo de A-módulos* si cumple

1. $f(m+n) = f(m) + f(n)$, para todo $m, n \in M$.
2. $f(am) = af(m)$, para todo $a \in A$ y $m \in M$.

Los elementos de un módulo M que por un homomorfismo de A-módulos $f : M \to N$ tienen su imagen en el 0_M se les denomina *núcleo* de f y denota por $\operatorname{Ker} f$. $\operatorname{Ker} f$ es un submódulo de M y f es inyectiva si y sólo si $\operatorname{Ker} f = \{0_N\}$. Los elementos de la imagen $\operatorname{Im} f$ forman un submódulo de M. Cuando f es biyectiva diremos que f es un *isomorfismo* de A-módulos y lo denotaremos por $\cong$.

Proposición 1.2.1. *Sea $f : M \to N$ un morfismo de A-módulos. Se cumple que*

$$M/\operatorname{Ker} f \cong \operatorname{Im} f,$$

donde la aplicación viene dada por la proyección natural.

Dado un conjunto $\{M_i\}_{i\in I}$ de submódulos de M denotaremos

$$\sum_{i\in I} M_i = \left\{ m \in M \mid m = \sum_{i\in I} m_i, \text{con } m_i \in M_i \text{nulos para casi todo } i \in I \right\}$$

que es el menor submódulo de M que contiene a los submódulos de la familia $\{M_i\}_{i\in I}$. Diremos que dos submódulos M_1, M_2 de M son una *suma directa* si $M_1 \cap M_2 = \{0\}$, es decir q el homomorfismo $M_1 \oplus M_2 \to M_1 + M_2$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo.
Sea $\{m_i\}_{i\in I}$ un conjunto de elementos de un A-módulo M, denotaremos por $\langle m_i\rangle_{i\in I}$ al conjunto

$$\left\{ m \in M \mid m = \sum_{i\in I} a_i m_i,\ a_i \in A,\ \text{con } a_i = 0 \text{ salvo un número finito} \right\}.$$

$\langle m_i\rangle_{i\in I}$ es el menor submódulo de M que contiene la familia $\{m_i\}_{i\in I}$ que denominamos *sistema generador* de M si $\langle m_i\rangle_{i\in I} = M$, si el conjunto de índices I es finito diremos que el módulo M es de *tipo finito* o *finitamente generado*.

Proposición 1.2.2 (Lema de Nakayama)**.** *Sea A un anillo local con ideal maximal $\mathfrak{m}$ y M un A-módulo finitamente generado. Denotemos*

$$\mathfrak{m}M = \left\{ m \in M \mid m = \sum a_i m_i,\ \textit{con } a_i \in \mathfrak{m} \textit{ y } m_i \in M \right\}.$$

Se tiene que $\mathfrak{m}M = M$ *si y sólo si* $M = 0$. *Por lo tanto* $m_1, \ldots, m_n \in M$ *es un sistema generador de* M *si la clases correspondientes en* $M/\mathfrak{m}M$ *por la proyección natural son un sistema de generadores de* $M/\mathfrak{m}M$.

Cado un A-módulo M diremos que el conjunto $B = \{b_1, b_2, \ldots, b_n\}$ es una *base libre* de M si y sólo si

1. B es un conjunto generador de M y
2. si $a_1b_1 + a_2b_2 + \cdots + a_nb_n = 0_M$ con $a_i \in A$ para $i = 1, 2, \ldots, n$, entonces $a_i = 0_A$ para $i = 1, 2, \ldots, n$

Si M tiene una base libre con n elementos, entonces M se dice *máodulo libre de rango* n, o más generalmente libre de rango finito.

Capítulo 2

Cuerpos finitos

En este capítulo comenzaremos revisando algunas generalidades de la estructura algebraica de cuerpo, aunque rápidamente nos centraremos en el estudio de los cuerpos finitos. Seguidamente, haremos una introducción a la teoría de Galois; para terminar con el estudio del retículo de subcuerpos de un cuerpo y las funciones traza y norma. Aunque el capítulo intente ser autocontenido, los conceptos básicos de la teoría de cuerpos pueden encontrase en [4].

2.1. Cuerpos y extensiones de cuerpos

Definición 2.1.1. *Un cuerpo* $(\mathbb{F}, +, \cdot)$ *es un conjunto no vacío en el que se han definido dos operaciones binarias: la adición, denotada por* $+$*, y el producto, denotado por* $\cdot$*. Los conjuntos* $(\mathbb{F}, +)$ *y* $(\mathbb{F} \setminus \{0\}, \cdot)$ *son grupos abelianos y además, el producto es distributivo con respecto a la adición. Los elementos neutros de ambas operaciones son diferentes y se denotan, respectivamente, como 0 y 1.*

Nota. En adelante, adoptaremos la notación $\mathbb{F}^*$ para el conjunto de elementos no nulos de $\mathbb{F}$.

Definición 2.1.2. *Un cuerpo se llama primo si no contiene ningún subcuerpo propio.*

Teorema 2.1.1. *Todo cuerpo* $\mathbb{F}$ *contiene un cuerpo primo que es, o bien* $\mathbb{Q}$*, o bien* $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ *para algún primo* p*.*

Demostración. La aplicación

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathbb{F} \\ m & \longrightarrow & m1_{\mathbb{F}} \end{array}$$

es claramente un isomorfismo de anillos. Por tanto, $\mathbb{Z}/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi \leq \mathbb{F}$. Si φ es un monomorfismo, $\mathbb{Q}$, el cuerpo de fracciones de $\mathbb{Z}$ debe estar contenido en $\mathbb{F}$. En otro caso, φ no es inyectiva y $\mathrm{Ker}\,\varphi$ es un ideal no nulo de $\mathbb{Z}$. Puesto que $\mathbb{Z}/\mathrm{Ker}\,\varphi$ es un dominio de integridad, $\mathrm{Ker}\,\varphi$ es un ideal primo no nulo, y por tanto maximal, de $\mathbb{Z}$. Así pues, ha de existir un primo $p \in \mathbb{Z}$ tal que $\mathrm{Ker}\,\varphi = p\mathbb{Z}$. Así pues $\mathbb{Z}_p$ es un cuerpo y $\mathbb{Z}_p \leq \mathbb{F}$. ■

Definición 2.1.3. *Un cuerpo $\mathbb{F}$ tiene característica cero si $\mathbb{Q} \leq \mathbb{F}$, y tiene característica p si $\mathbb{Z}_p \leq \mathbb{F}$.*

Observación 2.1.1. Notemos que cualquier cuerpo de característica cero, como $\mathbb{R}$ o $\mathbb{C}$, contiene el cuerpo primo $\mathbb{Q}$, por tanto tiene un número infinito de elementos. A su vez, un cuerpo finito tiene necesariamente característica p. Sin embargo, existen cuerpos de característica p que no son finitos.

Definición 2.1.4. *Un par de cuerpos $\mathbb{K}$ y $\mathbb{F}$ con $\mathbb{F} \subseteq \mathbb{K}$ se llama extensión de cuerpos y se denota por $\mathbb{K}|\mathbb{F}$.*

Ejemplo 2.1.1. $\mathbb{C}|\mathbb{Q}$, $\mathbb{C}|\mathbb{R}$, $\mathbb{R}|\mathbb{Q}$ son extensiones de cuerpos.

Dada una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos, es fácil ver que $\mathbb{K}$ es un $\mathbb{F}$-espacio vectorial. Así pues, tiene sentido la siguiente definición.

Definición 2.1.5. *Se llama grado de la extensión $\mathbb{K}|\mathbb{F}$ a la dimensión del $\mathbb{F}$-espacio vectorial $\mathbb{K}$. Se denota por $[\mathbb{K} : \mathbb{F}]$. La extensión se dice finita si su grado es finito, e infinita en caso contrario.*

Si $\mathbb{K}|\mathbb{F}$ es una extensión de cuerpos y $S \subseteq \mathbb{K}$, el cuerpo obtenido a partir de $\mathbb{F}$ por la adjunción de S es $\mathbb{F}(S) = \bigcap\{\mathbb{L} \leq \mathbb{K} \,|\, \mathbb{F} \cup S \subseteq \mathbb{L}\}$. Es claro que $\mathbb{F}(S)|\mathbb{F}$ es la menor extensión de $\mathbb{F}$ que contiene a S. En el caso en que $S = \{a\}$, la extensión $\mathbb{F}(a)|\mathbb{F}$ se dice simple y se puede probar que $\mathbb{F}(a) = \left\{ \frac{f(a)}{g(a)} \,|\, f, g \in \mathbb{F}[x], g(a) \neq 0 \right\}$.

Definición 2.1.6. *Dada una extensión de cuerpos $\mathbb{K}|\mathbb{F}$, un elemento $a \in \mathbb{K}$ se dice algebraico sobre $\mathbb{F}$ si existe un polinomio no nulo $f(x) \in \mathbb{F}[x]$ tal que $f(a) = 0$. En caso contrario, el elemento se dice trascendente. La extensión $\mathbb{K}|\mathbb{F}$ se dice algebraica si todos los elementos de $\mathbb{K}$ son algebraicos sobre $\mathbb{F}$. En caso contrario, se dice trascendente.*

Ejemplo 2.1.2. El elemento $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, pues es la raíz del polinomio $x^2 - 2$. Por otra parte, $i \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$, ya que es la raíz de $x^2 + 1$. La extensión $\mathbb{R}|\mathbb{Q}$ no es algebraica; por ejemplo, π y e son trascendentes sobre $\mathbb{Q}$.

Teorema 2.1.2. *Sean $\mathbb{K}|\mathbb{F}$ una extensión y $a \in \mathbb{K}$ un elemento algebraico sobre $\mathbb{F}$. Entonces:*

1. *Existe un único polinomio mónico irreducible $p(x) \in \mathbb{F}[x]$ tal que $p(a) = 0$.*
2. *Si $g(x) \in \mathbb{F}[x]$, entonces $g(a) = 0$ si y sólo si $p(x)|g(x)$ en $\mathbb{F}[x]$.*
3. *$\mathbb{F}(a) = \mathbb{F}[a] = \{f(a) \mid f(x) \in \mathbb{F}[x]\}$. Además, todo elemento de $\mathbb{F}(a)$ admite una expresión única de la forma $r(a)$, con $r = 0$ o con $\mathrm{gr}(r) < \mathrm{gr}(p)$. Así pues, si $n = \mathrm{gr}(f)$, el conjunto $\{1, a, \ldots, a^{n-1}\}$ es una $\mathbb{F}$-base de $\mathbb{F}(a)$.*

Demostración. Es claro que si a es raíz del polinomio $f(x) = \sum_{i=0}^{m} f_i x^i$ con $f_m \neq 0$, entonces también lo es del polinomio mónico $f_m^{-1} f(x)$. Denotaremos por $p(x)$ un polinomio mónico de grado mínimo en $\mathbb{F}[x]$. Es evidente que $p(x)$ debe ser irreducible, pues, en otro caso existiría un divisor propio de $p(x)$, denotado por $q(x)$, con grado estrictamente menor que el de $p(x)$ tal que $q(a) = 0$.
En cuanto a la unicidad, supongamos que existe otro polinomio $s(x) \in \mathbb{F}[x]$ mónico e irreducible tal que $s(a) = 0$. Entonces, $\mathrm{gr}(p) < \mathrm{gr}(s)$. Dividiendo por $p(x)$ encontramos dos polinomios, $q(x)$ y $r(x)$ tales que $s(x) = p(x)q(x) + r(x)$ con $r = 0$ o $\mathrm{gr}(r) < \mathrm{gr}(p)$. Si $r(x)$ no es nulo, entonces tendríamos $r(a) = 0$, lo que contradice la minimalidad del grado de $p(x)$. Así pues, $q(x)|p(x)$, pero esto es imposible, ya que $p(x)$ es irreducible.
Un razonamiento análogo nos permite probar la segunda afirmación.
Por último, consideramos la aplicación

$$\begin{array}{rcl} \theta : \mathbb{F}[x] & \longrightarrow & \mathbb{F}[a] \\ f(x) & \longrightarrow & f(a) \end{array}$$

Puesto que a es algebraico sobre $\mathbb{F}$, $\operatorname{Ker}\theta = \langle p(x)\rangle$ es un ideal maximal de $\mathbb{F}[x]$. Por tanto, $\mathbb{F}[x]/\operatorname{Ker}\theta \cong \mathbb{F}[a]$ es un cuerpo contenido en $\mathbb{F}(a)$, y entonces, $\mathbb{F}[a] = \mathbb{F}(a)$. Así pues, dado un elemento $b \in \mathbb{F}(a)$ cualquiera, podemos encontrar un polinomio $g(x) \in \mathbb{F}[x]$ tal que $b = g(a)$. Si dividimos $g(x)$ entre $p(x)$ tendremos que $g(x) = c(x)p(x) + r(x)$, con $r(x) = 0$ o tal que $\operatorname{gr}(r) < \operatorname{gr}(p)$. Sustituyendo en a, tenemos que $b = g(a) = r(a)$.
Para probar la unicidad, supongamos que $b = r(a) = r_1(a)$, con $\operatorname{gr}(r) < \operatorname{gr}(p) = n$ y $\operatorname{gr}(r_1) < \operatorname{gr}(p) = n$. Entonces $(r - r_1)(a) = 0$, por lo que tiene que $p(x)|(r - r_1)(x)$. Ahora bien, puesto que $\operatorname{gr}(r - r_1) < n$, debe tenerse que $r(x) - r_1(x) = 0$.
Probaremos ahora que el conjunto $\{1, a, \ldots, a^{n-1}\}$ es una $\mathbb{F}$-base de $\mathbb{K}$. Es libre puesto que si existen escalares de $\mathbb{F}$ tales que $\lambda_0 1 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1} = 0$, entonces a es una raíz de $f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1}$. En consecuencia $p(x)|f(x)$ y $f(x) = 0$. Es un sistema generador de $\mathbb{F}(a)$ puesto que si $b \in \mathbb{F}(a)$, entonces existe un polinomio $r(x) \in \mathbb{F}[x]$ con grado estrictamente menor que n tal que $b = r(a)$. Así pues, $b = \lambda_0 1 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1}$. ■

Definición 2.1.7. *Dados un cuerpo $\mathbb{F}$ y un polinomio $f(x) \in \mathbb{F}[x]$, se llama cuerpo de descomposición de $f(x)$ sobre $\mathbb{F}$ a un cuerpo $\mathbb{K}$ extensión de $\mathbb{F}$ que cumple estas dos propiedades:*

1. *$f(x)$ tiene todas las raíces en $\mathbb{K}$, por tanto, existen $\lambda \in \mathbb{K}$ y $a_1, \ldots, a_n \in \mathbb{K}$ tales que $f(x) = \lambda(x - a_1)\cdots(x - a_n) \in \mathbb{K}[x]$.*

2. *$\mathbb{K}$ es la menor extensión de $\mathbb{F}$ con esta propiedad, esto es, $\mathbb{K} = \mathbb{F}(a_1 \ldots, a_n)$.*

La existencia y la unicidad del cuerpo de descomposición de un polinomio se establecen en el siguiente resultado, cuya demostración se puede encontrar en [4].

Teorema 2.1.3. *Para cada polinomio $f(x) \in \mathbb{F}[x]$ de grado $n \geq 1$ existe un cuerpo de descomposición sobre $\mathbb{F}$. Este cuerpo de descomposición es único salvo isomorfismo.*

2.2. Anillos de polinomios sobre cuerpos finitos

Tras introducir las nociones generales de cuerpos y extensiones de cuerpos, así como algunas de sus propiedades, en esta sección nos centraremos en los cuerpos finitos. En adelante, si no se refiere lo contrario, $\mathbb{K}$ representará un cuerpo finito de caracteristica p. Su cuerpo primo será $\mathbb{Z}_p$ y si el grado de la extensión $[\mathbb{K} : \mathbb{Z}_p] = n$, entonces $|\mathbb{K}| = p^n$.

Teorema 2.2.1. *Sea $\mathbb{K}$ un cuerpo, no necesariamente finito, y G un subgrupo del grupo multiplicativo $(\mathbb{K}^*, \cdot)$. Si G es finito, entonces G es un grupo cíclico. En particular, si $\mathbb{K}$ es finito, $(\mathbb{K}^*, \cdot)$ es un grupo cíclico.*

Demostración. Supongamos que G es finito. En ese caso, G es un producto directo de grupos cíclicos. Sean $|G| = n$ y $\exp(G) = r$ el orden y el exponente de G. En ese caso, $g^r = 1$ para todo $g \in G$, es decir, los elementos de G son raíces del polinomio $x^r - 1 \in \mathbb{Z}_p[x] \subseteq \mathbb{K}[x]$. Este polinomio tendrá, como máximo, r raíces en $\mathbb{K}$, por tanto, $n = |G| \leq r$. Como el exponente de G divide a su orden, necesariamente $n = r$. Así pues, G posee un único factor invariante y por tanto es cíclico. ■

Observación 2.2.1. Si $\mathbb{K}$ es un cuerpo finito, entonces $(\mathbb{K}^*, \cdot) \cong C_{p^n-1}$ con $|\mathbb{K}| = p^n$. Por otra parte, $(\mathbb{K}, +) \cong C_p \oplus \cdots \oplus C_p$, por tanto, el grupo aditivo $(\mathbb{K}, +)$ tiene exponente p.

Corolario 2.2.1 (Pequeño teorema de Fermat)**.** *Para todo $n \in \mathbb{Z}$ y p primo, $n^p \equiv n (mod\ p)$. Si $(n, p) = 1$, entonces $n^{p-1} \equiv 1 (mod\ p)$.*

Demostración. Sea $\mathbb{K} = \mathbb{Z}_p$, entonces $(\mathbb{K}^*, \cdot) \cong C_{p-1}$. Si $n \in \mathbb{Z}$ es relativamente primo con p, entonces su imagen por el epimorfismo canónico $\bar{\cdot} : \mathbb{Z} \to \mathbb{Z}_p$ es diferente de cero, esto es, $\overline{n} \neq 0$. En ese caso, $\overline{n}^{p-1} = \overline{1}$. Por tanto, $n^{p-1} \equiv 1 \,(\text{mod } p)$ y, en consecuencia, $n^p \equiv n (\text{mod } p)$. El resultado es trivial si n es un múltiplo de p. ■

Teorema 2.2.2 (Teorema del elemento primitivo para cuerpos finitos)**.** *Sean $\mathbb{F}$ un cuerpo finito y $\mathbb{K}|\mathbb{F}$ una extensión finita. Entonces la extensión es simple, es decir, existe un elemento $u \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(u)$.*

Demostración. Si la extensión $\mathbb{K}|\mathbb{F}$ es finita y $\mathbb{F}$ es un cuerpo finito, entonces $\mathbb{K}$ también es finito. Sea $u \in \mathbb{K}$ el generador del grupo multiplicativo $(\mathbb{K}^*, \cdot)$. Es fácil ver que $\mathbb{K} = \mathbb{Z}_p(u) = \mathbb{F}(u)$. ■

Observación 2.2.2. Nótese que si u es un generador del grupo multiplicativo $\mathbb{K}^*$, esto es, $\mathbb{K}^* = \langle u \rangle$, entonces $\mathbb{K} = \mathbb{Z}_p(u) = \mathbb{F}(u)$ para cualquier cuerpo intermedio $\mathbb{Z}_p \leq \mathbb{F} \leq \mathbb{K}$. Sin embargo, el recíproco no es cierto, pues si $\mathbb{K} = \mathbb{Z}_p(u)$, no necesariamente, $\mathbb{K}^* = \langle u \rangle$.

Proposición 2.2.1. *Sea $\mathbb{K}$ un cuerpo con característica p diferente de cero. Si $r \geq 1$, entonces la aplicación*

$$\begin{array}{rccc} \varphi : \mathbb{K} & \longrightarrow & \mathbb{K} \\ a & \longrightarrow & a^{p^r} \end{array}$$

es un $\mathbb{Z}_p$-homomorfismo de $\mathbb{K}$ en $\mathbb{K}$. Si $\mathbb{K}$ es finito, entonces φ es un automorfismo de cuerpos.

Demostración. La aplicación φ es claramente un homomorfismo de cuerpos. En efecto, $\varphi(a+b) = (a+b)^p = a^{p^r} + b^{p^r} = \varphi(a) + \varphi(b)$ y $\varphi(ab) = (ab)^{p^r} = a^{p^r} b^{p^r} = \varphi(a)\varphi(b)$, para todo $a, b \in \mathbb{K}$. Para ver que es $\mathbb{Z}_p$-homomorfismo, debemos probar que φ fija todos los elementos de $\mathbb{Z}_p$. Si $a \in \mathbb{Z}_p$, claramente $a^p = a$ y entonces $\varphi(a) = a$. Por último, si $\mathbb{K}$ es finito, la inyectividad de φ implica que φ es un automorfismo. En consecuencia, φ es un $\mathbb{Z}_p$-automorfismo de $\mathbb{K}$. ■

Teorema 2.2.3 (Teorema de existencia y unicidad de cuerpos finitos)**.** *Si $p > 0$ es primo y $n \geq 1$ es un número cualquiera, entonces existe un cuerpo $\mathbb{K}$ con orden $|\mathbb{K}| = p^n$. Si $\mathbb{K}_1$ y $\mathbb{K}_2$ son cuerpos y $|\mathbb{K}_1| = |\mathbb{K}_2| = p^n$, entonces $\mathbb{K}_1$ y $\mathbb{K}_2$ son $\mathbb{Z}_p$ isomorfos.*

Demostración. Sea $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ y sea Σ el cuerpo de descomposición de dicho polinomio sobre $\mathbb{Z}_p$. Sea $\mathbb{K}$ el conjunto formado por todas las raíces de $f(x)$ en Σ. Puesto que $f'(x) = -1 \neq 0$, el polinomio $f(x)$ no tiene raíces dobles, así pues el cardinal de $\mathbb{K}$ será igual al grado de $f(x)$, esto es p^n.
Veamos ahora que $\mathbb{K}$ es un cuerpo y que $\mathbb{Z}_p \subseteq \mathbb{K}$. Dados dos elementos cualesquiera $a, b \in \mathbb{K}$, ambos son raíces de $f(x)$, y por tanto, satisfacen $a^{p^n} = a$ y $b^{p^n} = b$. Así pues, $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$. De igual forma, puede verse que $(ab)^{p^n} = ab$. Así pues, $\mathbb{K}$ es un cuerpo y, por el corolario 2.2.1, $\mathbb{Z}_p \subseteq \mathbb{K}$. En consecuencia, $\Sigma = \mathbb{Z}_p(\mathbb{K}) = \mathbb{K}$ y $|\mathbb{K}| = p^n$. Recíprocamente, supongamos que $\mathbb{K}$ es un cuerpo y que $|\mathbb{K}| = p^n$. El grupo $\mathbb{K}^*$ es cíclico y tiene orden $p^n - 1$, por tanto, para todo elemento

$a \in \mathbb{K}^*$ tendremos que $a^{p^n-1} = 1$ y entonces $a^{p^n} = a$. Lo mismo sucede si $a = 0$. Así pues, los elementos de $\mathbb{K}$ son las raíces del polinomio $x^{p^n} - x$. Como $|\mathbb{K}| = p^n$ y el número de raíces del polinomio $x^{p^n} - x$ es a lo sumo p^n, $\mathbb{K}$ es el conjunto de raíces de $x^{p^n} - x$ y, por tanto, el cuerpo de descomposición de $x^{p^n} - x$ sobre $\mathbb{Z}_p$. Por último, si $\mathbb{K}_1$ y $\mathbb{K}_2$ son cuerpos con $|\mathbb{K}_1| = |\mathbb{K}_2| = p^n$, $\mathbb{K}_1$ y $\mathbb{K}_2$ son cuerpos de descomposición de $x^{p^n} - x$ sobre $\mathbb{Z}_p$ y, por el teorema 2.1.3, son $\mathbb{Z}_p$-isomorfos. ■

Nota. El cuerpo de p^n elementos de denotará en adelante como $\mathbb{F}_{p^n}$.

Corolario 2.2.2. *Si $\mathbb{K}$ es un cuerpo finito tal que $|\mathbb{K}| = p^n$ y $\mathbb{F}$ es un subcuerpo de $\mathbb{K}$, entonces $x^{p^n} - x \in \mathbb{Z}_p[x] \subseteq \mathbb{F}[x]$ se escinde en $\mathbb{K}$, esto es, $x^{p^n} - x = \prod_{a \in \mathbb{K}} (x - a)$.*

2.3. Introducción a la Teoría de Galois

En esta sección determinaremos el grupo de $\mathbb{F}$-automorfismos de una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos finitos. Este grupo se conoce como grupo de Galois de la extensión $\mathbb{K}|\mathbb{F}$.

Definición 2.3.1. *Un polinomio irreducible $f(x) \in \mathbb{F}[x]$ se dice separable sobre $\mathbb{F}$ si todas las raíces de $f(x)$ en un cuerpo de descomposición $\mathbb{K}$ sobre $\mathbb{F}$ son simples. En caso contrario, el polinomio se dice inseparable.*

Definición 2.3.2. *Sea $\mathbb{K}|\mathbb{F}$ una extensión algebraica. Un elemento $a \in \mathbb{K}$ se dice separable sobre $\mathbb{F}$ si su polinomio irreducible asociado es separable sobre $\mathbb{F}$. La extensión $\mathbb{K}|\mathbb{F}$ se dice separable si todo elemento $a \in \mathbb{K}$ es separable sobre $\mathbb{F}$.*

Teorema 2.3.1. *Sea $\mathbb{K}$ un cuerpo finito. Entonces $\mathbb{K}$ es una extensión separable de $\mathbb{Z}_p$ y, por tanto, de cualquier $\mathbb{F}$ con $\mathbb{Z}_p \subseteq \mathbb{F} \subseteq \mathbb{K}$. El grupo de $\mathbb{F}$-automorfismos de $\mathbb{K}$, $Aut_{\mathbb{F}}(\mathbb{K})$, es un grupo cíclico generado por el automorfismo de Frobenius*

$$\begin{array}{rcl} \phi : \mathbb{K} & \longrightarrow & \mathbb{K} \\ a & \longrightarrow & a^q \end{array}$$

con $q = |\mathbb{F}|$. El orden de ϕ es $n = [\mathbb{K} : \mathbb{F}]$.

Demostración. Sea $|\mathbb{K}| = q^n$. Sabemos que $\mathbb{K}$ es cuerpo de descomposición del polinomio $x^{q^n} - x \in \mathbb{Z}_p[x]$. Todas las raíces del polinomio $f(x) = x^{q^n} - x$ son simples ($f'(x) \neq 0$). Por otra parte, el polinomio irreducible asociado a cualquier $a \in \mathbb{K}$ debe dividir a $f(x)$ y, por tanto, sólo puede tener raíces simples. Es decir, a es separable sobre $\mathbb{Z}_p$ y la extensión $\mathbb{K}|\mathbb{Z}_p$ es separable. Lo mismo sucede para cualquier extensión intermedia $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{Z}_p$.
La aplicación $\phi : \mathbb{K} \to \mathbb{K}$ es claramente un automorfismo (proposición 2.2.1). Puesto que $|\mathbb{F}| = q$, $\mathbb{F}$ es cuerpo de descomposición del polinomio $x^q - x$ sobre $\mathbb{Z}_p$. Por tanto, $a^q = a$ para todo $a \in \mathbb{F}$ y ϕ fija todos los elementos de $\mathbb{F}$. Esto es, ϕ es un $\mathbb{F}$-automorfismo de $\mathbb{K}$ y tenemos que $\langle\phi\rangle \leq Aut_{\mathbb{F}}(\mathbb{K})$.
Veamos ahora que el orden de ϕ, $o(\phi)$, es el grado n de la extensión $\mathbb{K}|\mathbb{F}$. Es claro que $\phi^n(b) = b^{q^n} = b$ para todo $b \in \mathbb{K}$. Por ello, $\phi^n = 1_{\mathbb{K}}$ y $o(\phi)|n$. Por otra parte, si $o(\phi) = m \neq n$, esto implica que $\phi^m = 1_{\mathbb{K}}$. Esto es, $\phi^m(b) = b^m = b$ para todo $b \in \mathbb{K}$ y todos los elementos de $\mathbb{K}$ son raíces del polinomio $x^{q^m} - x$ con $m < n$, lo que contradice la definición de $\mathbb{K}$. Luego, $o(\phi) = n$.
Por último, probemos que $Aut_{\mathbb{F}}(\mathbb{K}) = \langle\phi\rangle$. Para ello, tomamos un elemento $\varphi \in Aut_{\mathbb{F}}(\mathbb{K})$ cualquiera. Puesto de $\mathbb{K}^* = \langle a\rangle$ para un cierto $a \in \mathbb{K}$ y $\mathbb{K} = \mathbb{Z}_p(a) = \mathbb{F}(a)$ (observación 2.2.2), el $\mathbb{F}$-automorfismo φ queda unívocamente determinado por la imagen $\varphi(a)$. Sea $p(x)$ el polinomio irreducible asociado a a. Este polinomio tiene grado n y se escinde en $\mathbb{K}$. Por tanto, $\varphi(p(a)) = p(\varphi(a)) = 0$. Es decir, $\varphi(a)$ es una raíz de $p(x)$ en $\mathbb{K}$. Puesto que $p(x)$ tiene a lo sumo n raíces en $\mathbb{K}$, existen a lo sumo n elecciones para el valor $\varphi(a)$. Así, el orden $|Aut_{\mathbb{F}}(\mathbb{K})| \leq n$. Ahora bien, $\langle\phi\rangle \leq Aut_{\mathbb{F}}(\mathbb{K})$ y $n = |\langle\phi\rangle| \leq |Aut_{\mathbb{F}}(\mathbb{K})| \leq n$. Por tanto $Aut_{\mathbb{F}}(\mathbb{K}) = \langle\phi\rangle$. ■

Corolario 2.3.1. *Sea f un polinomio irreducible de grado n en $\mathbb{F}_q[x]$. El cuerpo de descomposición de f sobre $\mathbb{F}_q$ es $\mathbb{K} = \mathbb{F}_{q^n}$.*

Demostración. Sea a una raíz de $f(x)$ en su cuerpo de descomposición, $\mathbb{K}$, sobre $\mathbb{F}$. Por el teorema anterior, las imágenes de a por las diferentes potencias de ϕ, $\phi(a) = a^q, \ldots, \phi^{n-1}(a) = a^{q^{n-1}}, \phi^n(a) = a$, constituyen todas las raíces de $f(x)$. Así pues, $\mathbb{K} = \mathbb{F}(a, a^q, \ldots, a^{q^{n-1}}) = \mathbb{F}(a)$. Puesto que el grado de la extensión es n, se tiene que $\mathbb{K} = \mathbb{F}_{q^n}$. ■

2.4. Subcuerpos, traza y norma. Bases

Dedicaremos esta sección al estudio del retículo de subcuerpos de un cuerpo finito. Introduciremos también las funciones traza y norma, definidas desde el cuerpo en alguno de sus subcuerpos. Por último, terminaremos la sección con el concepto de base normal.

Teorema 2.4.1 (Teorema del subcuerpo)**.** *Sean $\mathbb{K}$ y $\mathbb{F}$ cuerpos finitos tales que $|\mathbb{K}| = p^n$ y $|\mathbb{F}| = p^m$. Entonces $\mathbb{F}$ es un subcuerpo de $\mathbb{K}$ si y sólo si $m|n$.*

Demostración. Supongamos que $\mathbb{F} \leq \mathbb{K}$. En ese caso, $\mathbb{K}$ es una extensión finita de $\mathbb{F}$. Por tanto, cualquier $\mathbb{F}$-base de $\mathbb{K}$ tiene cardinal finito, que denotamos por k. Así pues, $p^n = p^{km}$ y $m|n$.
Recíprocamente, supongamos que $m|n$. En ese caso, $p^m - 1$ divide a $p^n - 1$ y, en consecuencia, $x^{p^m} - x$ divide al polinomio $x^{p^n} - x$ en $\mathbb{Z}_p[x]$. Por tanto, todas las raíces de $x^{p^m} - x$ lo son también de $x^{p^n} - x$, lo que implica que $\mathbb{F} \leq \mathbb{K}$. ■

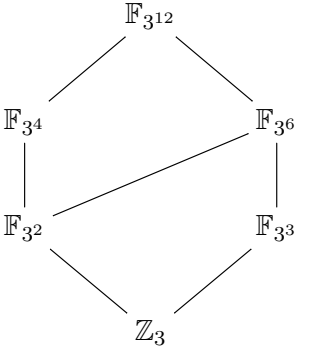

Figura 2.1: Retículo de subcuerpos de $\mathbb{F}_{3^{12}}$

Corolario 2.4.1. *1. Sean $\mathbb{K}$ un cuerpo finito tal que $|\mathbb{K}| = q = p^m$ y $n \geq 1$ un número natural. Entonces, existe una extensión simple de $\mathbb{K}$, $\mathbb{K}(a)$, con $|\mathbb{K}(a) : \mathbb{K}| = n$.*

2. Si $\mathbb{K}_1$ y $\mathbb{K}_2$ son extensiones de $\mathbb{K}$ y $[\mathbb{K}_1 : \mathbb{K}] = n = [\mathbb{K}_2 : \mathbb{K}]$, entonces $\mathbb{K}_1$ y $\mathbb{K}_2$ son $\mathbb{K}$-isomorfas.

3. *Para todo natural $n \geq 1$ existe un polinomio irreducible de grado n sobre $\mathbb{K}$.*

Demostración. Para el punto 1, basta considerar el polinomio $x^{q^n} - x$ y $\mathbb{L}$ el cuerpo de descomposición de este polinomio sobre $\mathbb{Z}_p$. Sabemos que $|\mathbb{L}| = q^n$ y, por el teorema 2.4.1, $\mathbb{K} \leq \mathbb{L}$. Como $|\mathbb{L}| = q^n = |\mathbb{K}|^n$, entonces, $[\mathbb{L} : \mathbb{K}] = n$ y, por el teorema 2.2.2, existe un elemento $a \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(a)$. Para el punto 2, si $\mathbb{K}_1$ y $\mathbb{K}_2$ son dos extensiones de $\mathbb{K}$ tales que $[\mathbb{K}_1 : \mathbb{K}] = [\mathbb{K}_2 : \mathbb{K}] = n$, entonces $|\mathbb{K}_1| = |\mathbb{K}_2| = q^n$ y, por tanto, $\mathbb{K}_1$ y $\mathbb{K}_2$ son cuerpos de descomposición del polinomio $x^{q^n} - x$ sobre $\mathbb{K}$. Por el teorema 2.1.3, $\mathbb{K}_1$ y $\mathbb{K}_2$ son $\mathbb{K}$-isomorfos. Por último, para el punto 3, tomamos $p(x) \in \mathbb{K}[x]$ el polinomio irreducible asociado al elemento a del punto 1. ■

A continuación definiremos una aplicación de un cuerpo finito $\mathbb{K}$ en un subcuerpo suyo $\mathbb{F}$ que recibe el nombre de traza. Veremos que esta aplicación es $\mathbb{F}$-lineal, pero no $\mathbb{K}$-lineal.

Definición 2.4.1. *Sean $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. Para cada elemento $a \in \mathbb{K}$, la traza de a, $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ se define como*

$$\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) = a + a^q + \cdots + a^{q^{n-1}}.$$

Si $\mathbb{F}$ es el cuerpo primo de $\mathbb{K}$, entonces $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ se llama traza absoluta de a y se denota por $\mathrm{Tr}_{\mathbb{K}}(a)$.

Notemos que, dado un elemento $a \in \mathbb{K}$, su traza es la suma de todas las imágenes de a por las diferentes potencias del automorfismo de Frobenius, ϕ. Por ello, $\phi(\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ para todo $a \in \mathbb{K}$. Y entonces, $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) \in \mathbb{F}$ para todo $a \in \mathbb{K}$.
Las principales propiedades de la función traza se encuentran resumidas en el siguiente resultado, cuya demostración puede encontrarse en [9].

Teorema 2.4.2. *Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. La función traza satisface las siguientes propiedades:*

1. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a + b) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) + \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(b)$ *para todo $a, b \in \mathbb{K}$.*
2. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(ca) = c\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ *para todo $c \in \mathbb{F}$ y $a \in \mathbb{K}$.*
3. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}$ *es una transformación lineal suprayectiva de $\mathbb{K}$ en $\mathbb{F}$.*

4. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) = na$ *para todo* $a \in \mathbb{F}$.

5. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a^q) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ *para todo* $a \in \mathbb{K}$.

Dada una cadena de extensiones de cuerpos, la función traza se puede calcular utilizando el siguiente resultado.

Teorema 2.4.3. *Sea* $\mathbb{F}$ *un cuerpo finito. Sean* $\mathbb{K}$ *una extensión finita de* $\mathbb{F}$ *y* $\mathbb{L}$ *una extensión finita de* $\mathbb{K}$. *Entonces, para todo* $a \in \mathbb{L}$,

$$\mathrm{Tr}_{\mathbb{L}|\mathbb{F}}(a) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}|\mathbb{K}}(a)).$$

Demostración. Supongamos que $\mathbb{F} = \mathbb{F}_q$ y que los grados $[\mathbb{K} : \mathbb{F}]$ y $[\mathbb{L} : \mathbb{K}]$ son m y n respectivamente. Entonces $[\mathbb{L} : \mathbb{F}] = mn$ y para todo $a \in \mathbb{F}$ tenemos que

$$\begin{aligned} \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}|\mathbb{K}}(a)) &= \sum_{i=0}^{m-1} (\mathrm{Tr}_{\mathbb{L}|\mathbb{K}}(a))^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} a^{q^{jm}} \right)^{q^i} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a^{q^{jm+i}} = \sum_{k=0}^{mn-1} a^{q^k} = \mathrm{Tr}_{\mathbb{L}|\mathbb{F}}(a). \end{aligned}$$

■

Aún podemos definir otra función de un cuerpo $\mathbb{K}$ sobre un subcuerpo suyo $\mathbb{F}$. Esta función se obtiene mediante el producto de un elemento $a \in \mathbb{K}$ por todos sus conjugados sobre el subcuerpo $\mathbb{F}$.

Definición 2.4.2. *Sea* $\mathbb{F} = \mathbb{F}_q$ *un cuerpo finito y sea* $\mathbb{K} = \mathbb{F}_{q^n}$ *una extensión suya. La norma* $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$ *de un elemento* $a \in \mathbb{K}$ *sobre* $\mathbb{F}$ *se define como*

$$\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) = a \cdot a^q \cdot \cdots \cdot a^{q^{n-1}}.$$

Notemos que la imagen de $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$, para todo $a \in \mathbb{K}$ es invariante por el automorfismo de Frobenius. Por ello, $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) \in \mathbb{F}$ para todo $a \in \mathbb{K}$. Las propiedades de la función norma se resumen a continuación. Una demostración de ellas se puede encontrar en [9].

Teorema 2.4.4. *Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. La función norma satisface las siguientes propiedades:*

1. $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(ab) = \mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)\mathrm{N}_{\mathbb{K}|\mathbb{F}}(b)$ *para todo* $a, b \in \mathbb{K}$.
2. $N_{\mathbb{K}|\mathbb{F}}$ *es una transformación lineal suprayectiva de* $\mathbb{K}$ *en* $\mathbb{F}$ *y de* $\mathbb{K}^*$ *en* $\mathbb{F}^*$.
3. $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) = a^n$ *para todo* $a \in \mathbb{F}$.
4. $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a^q) = \mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$ *para todo* $a \in \mathbb{K}$.

El comportamiento de la función norma con respecto a las extensiones intermedias de un cuerpo es similar al de la traza, como se puede apreciar en el resultado siguiente.

Teorema 2.4.5. *Sea $\mathbb{F}$ un cuerpo finito. Sean $\mathbb{K}$ una extensión finita de $\mathbb{F}$ y $\mathbb{L}$ una extensión finita de $\mathbb{K}$. Entonces, para todo $a \in \mathbb{L}$,*

$$\mathrm{N}_{\mathbb{L}|\mathbb{F}}(a) = \mathrm{N}_{\mathbb{K}|\mathbb{F}}(\mathrm{N}_{\mathbb{L}|\mathbb{K}}(a)).$$

Por último, introducimos el concepto de base normal.

Definición 2.4.3. *Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. Una $\mathbb{F}$-base de $\mathbb{K}$ de la forma $\{a, a^q \ldots, a^{q^{n-1}}\}$, que consiste en un elemento a adecuado y todos sus $\mathbb{F}$-conjugados, recibe el nombre de base normal de $\mathbb{K}$ sobre $\mathbb{F}$.*

Es posible probar, ver [9], que si $\mathbb{F}$ es un cuerpo finito y $\mathbb{K}$ es una extensión finita de $\mathbb{F}$, entonces es posible construir una base normal de $\mathbb{K}$ sobre $\mathbb{F}$. Este resultado se conoce como teorema de la base normal.
Finalmente, damos un criterio para decidir cuándo un conjunto de n elementos constituyen una $\mathbb{F}$-base de $\mathbb{K}$. Su demostración puede encontrarse también en [9].

Teorema 2.4.6. *Sea $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. El conjunto $\{a_1, \ldots, a_n\}$ es una $\mathbb{F}$-base de $\mathbb{K}$ si y sólo si*

$$\begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^q & a_2^q & \cdots & a_n^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_n^{q^{n-1}} \end{vmatrix} \neq 0$$

2.5. Estructura multiplicativa. Raíces de la unidad

Terminaremos este capítulo estudiando la estructura multiplicativa de un cuerpo finito, es decir, el conjunto de las raíces de la unidad.

Definición 2.5.1. *Sea $\mathbb{K}$ un cuerpo de característica $p \geq 0$ y sea n un número natural. Se llama n-simo cuerpo ciclotómico sobre $\mathbb{K}$, denotado por $\mathbb{K}^{(n)}$, al cuerpo de descomposición sobre $\mathbb{K}$ del polinomio $x^n - 1 \in \mathbb{K}[x]$. El conjunto de raíces de ese polinomio en $\mathbb{K}^{(n)}$ se llama conjunto de n-raíces de la unidad sobre $\mathbb{K}$ y se denota por $E^{(n)}$.*

Proposición 2.5.1.

1. *$E^{(n)}$ es un subgrupo cíclico finito del grupo multiplicativo $\mathbb{K}^{(n)}\setminus\{0\}$. Si $p \nmid n$ (en particular si $p = 0$), entonces $E^{(n)}$ es un grupo cíclico de orden n.*

2. *Si $E^{(n)} = \langle\xi\rangle$, entonces $\mathbb{K}^{(n)} = \mathbb{K}(\xi)$.*

3. *Si $n = mp^a$ con $(m, p) = 1$, entonces se tiene que $E^{(m)} = E^{(n)}$ y $\mathbb{K}^{(m)} = \mathbb{K}^{(n)}$.*

Demostración. Para probar la primera afirmación notemos que el conjunto $E^{(n)}$ está formado por todas las raíces del polinomio $x^n - 1 \in \mathbb{K}[x]$. Por tanto, su cardinal debe ser, necesariamente, menor o igual a n. Por otra parte, es fácil ver que $E^{(n)}$ es un subgrupo de $\mathbb{K}^{(n)}\setminus\{0\}$ y, por tanto, cíclico. Ahora bien, si $p \nmid n$, $f(x) = x^n - 1$ y $f'(x) = nx^{n-1}$ no tienen raíces en común, por lo que $f(x)$ tiene exactamente n raíces diferentes en $\mathbb{K}^{(n)}$ y $|E^{(n)}| = n$.
La segunda afirmación se sigue del hecho

$$\mathbb{K}^{(n)} = \mathbb{K}(E^{(n)}) = \mathbb{K}(\xi, \xi^2, \ldots) = \mathbb{K}(\xi).$$

Por último, si $n = mp^a$, $\xi \in E^{(n)}$ si y sólo si $\xi^n = 1$, es decir, si y sólo si $\xi^n - 1 = 0$, o lo que es lo mismo, si y sólo si $\xi^{mp^a} - 1 = (\xi^m - 1)^{p^a} = 0$, o equivalentemente, $\xi \in E^{(m)}$. ∎

Definición 2.5.2. *Sea $\mathbb{K}$ un cuerpo de característica $p \geq 0$. Sea $n \in \mathbb{N}$ tal que $(n, p) = 1$. Se llama n-raíz primitiva de la unidad, ξ, a cualquier*

generador de $E^{(n)}$. El polinomio que tiene como raíces todas las n-raíces primitivas de la unidad recibe el nombre de n-simo polinomio ciclotómico y se representa por $\phi_n(x)$.

Nótese que, si ξ es una n-raíz primitiva de la unidad, entonces $\xi^n = 1$ mientras que $\xi^m \neq 1$ para cualquier $m < n$. Por otra parte, es fácil ver que ξ^s es n-raíz primitiva para todo s relativamente primo con n. Así pues, el n-simo polinomio ciclotómico se puede escribir como

$$\phi_n(x) = \prod_{(s,n)=1, s<n} (x - \xi^s) \in \mathbb{K}^{(n)}[x].$$

Por tanto, si φ representa la función de Euler, el grado de $\phi_n(x)$ será $\varphi(n)$.

Ejemplo 2.5.1. Sea $\mathbb{K} = \mathbb{Q}$ y $n = 4$. En ese caso,

$$E^{(4)} = \{1, -1, i, -i\} = \langle i \rangle = \langle -i = i^3 \rangle.$$

Así pues, las 4-raíces primitivas de la unidad son $\{i, -i\}$ y el cuarto polinomio ciclotómico

$$\phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

Proposición 2.5.2.

1. *$x^n - 1 = \prod_{d|n} \phi_d(x)$.*
2. *Si $\mathbb{F}$ es el cuerpo primo de $\mathbb{K}$, entonces $\phi_n(x) \in \mathbb{F}[x]$. Si la característica de $\mathbb{F}$ es cero, entonces $\phi_n(x) \in \mathbb{Z}[x]$.*

Demostración. Para probar la primera afirmación notemos que las raíces del polinomio $x^n - 1$, en $\mathbb{K}^{(n)}$, son las n-raíces de la unidad. Supongamos que ξ es una n-raíz primitiva, es decir, $E^{(n)} = \langle \xi \rangle$, entonces si η es una raíz de $x^n - 1$, $\eta = \xi^s$ para un cierto s. Es claro que η es una d-raíz primitiva para $d = n/(n, s)$ que, claramente, es un divisor de n. Puesto que las raíces de los polinomios ciclotómicos son primitivas, dos polinomios $\phi_m(x)$ y $\phi_d(x)$ no pueden tener raíces en común a menos que $m = d$. Por tanto, η es raíz de un único $\phi_d(x)$.
La segunda afirmación se prueba por inducción sobre n. Los detalles de la misma se pueden encontrar en [4, proposición V.8.2]. ∎

Observación 2.5.1. La proposición anterior permite calcular los polinomios ciclotómicos de forma recursiva. Es fácil ver que $\phi_1(x) = x - 1$ y que $\phi_2(x) = x + 1$, pues 1 y -1 son, respectivamente, 1-raíces y 2-raíces primitivas de la unidad. Ahora bien, utilizando la proposición anterior podemos ver que

$$\phi_3(x) = \frac{x^3 - 1}{\phi_1(x)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1,$$
$$\phi_4(x) = \frac{x^4 - 1}{\phi_1(x)\phi_2(x)} = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1.$$

Y así sucesivamente.

Proposición 2.5.3. *Sea $\mathbb{K} = \mathbb{F}_q$. Entonces $\mathbb{K}$ es el $(q-1)$-simo cuerpo ciclotómico sobre cualquier subcuerpo suyo $\mathbb{F}$.*

Demostración. El grupo multiplicativo $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ está constituido por las $(q-1)$-raíces de la unidad sobre $\mathbb{F}$. Por tanto, el polinomio $x^{q-1} - 1 \in \mathbb{F}[x]$ se escinde sobre $\mathbb{K}$. Claramente, $\mathbb{K}$ es el cuerpo más pequeño con esta propiedad. ■

Proposición 2.5.4. *Sea $d \neq n$ un divisor de n. Entonces, el n-simo polinomio ciclotómico $\phi_n(x)$ divide al cociente $\frac{x^n-1}{x^d-1}$ en $\Pi[x]$, donde Π representa el cuerpo primo.*

Demostración. Si $d \mid n$, es fácil ver que $x^d - 1 \mid x^n - 1$. Es decir, $x^n - 1 = (x^d - 1)g(x)$ con $g(x) \in \Pi[x]$. Ahora bien, $\phi_n(x) \mid x^n - 1$ y $(\phi_n(x), x^d - 1) = 1$. Por tanto, $\phi_n(x) \mid g(x)$. ■

Teorema 2.5.1. *Sea $\mathbb{K} = \mathbb{F}_q$. Entonces $\phi_n(x)$ se factoriza como producto de $\frac{\phi(n)}{d}$ factores irreducibles del mismo grado d. Además, d es el menor número natural que cumple $q^d \equiv 1 (mod\ n)$. Si la característica de $\mathbb{K}$ es cero, entonces $\phi_n(x)$ es irreducible en $\mathbb{Q}[x]$ y, por tanto, en $\mathbb{Z}[x]$.*

Demostración. Supongamos que $p(x)$ es un factor irreducible de $\phi_n(x)$ en $\mathbb{K}[x]$ y que $\xi \in \mathbb{K}^{(n)}$ es una raíz suya. Es evidente que ξ es una n-raíz primitiva de la unidad y que $\mathbb{K}^{(n)} = \mathbb{K}(\xi)$. Por otra parte, el grado del polinomio $p(x)$ ha de ser el grado de la extensión $[\mathbb{K}(\xi) : \mathbb{K}] = [\mathbb{K}^{(n)} : \mathbb{K}]$. Es claro que lo mismo sucede para cualquier factor irreducible de

$\phi_n(x)$. Por tanto, $\phi_n(x)$ se descompone como producto de irreducibles del mismo grado. Ahora bien, si $\mathbb{L}$ es una extensión de $\mathbb{K}$ que contiene a la raíz ξ y su cardinal es $|\mathbb{L}| = m = q^t$, entonces $\xi^{m-1} = 1$. Puesto que ξ es una n-raíz de la unidad, su orden multiplicativo es n, por tanto, $m - 1 \mid n$ y $q^t \equiv 1 (\mathrm{mod}\ n)$. Sea d el menor natural tal que $q^d \equiv 1 (\mathrm{mod}\ n)$. Entonces, $\xi \in \mathbb{F}_{q^d}$, pero $\xi \notin \mathbb{L}$ para cualquier cuerpo $\mathbb{L}$ tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}_{q^d}$. Así pues, $\mathbb{F}_{q^d} = \mathbb{K}^{(n)}$ y, por tanto, el grado del polinomio irreducible asociado a ξ ha de ser $[\mathbb{K}^{(n)} : \mathbb{K}] = d$.
La demostración de la irreducibilidad de $\phi_n(x)$ en $\mathbb{Q}[x]$ se puede encontrar en la proposición V.8.3 de [4]. ■

Terminaremos esta sección comprobando cómo se factoriza un polinomio ciclotómico dependiendo de quién sea el cuerpo primo.

Ejemplo 2.5.2. Sea $\phi_{12}(x) = x^4 - x^2 + 1$ el 12-polinomio ciclotómico. Por el resultado anterior, este polinomio es irreducible en $\mathbb{Q}[x]$ y, por tanto, sobre $\mathbb{Z}[x]$.
Si ahora trabajamos sobre $\mathbb{F}_7[x]$, puesto que $7^2 \equiv 1 (\mathrm{mod}\ 12)$, el polinomio $\phi_{12}(x)$ se factoriza como producto de dos polinomios irreducibles de grado 2. Esto es,

$$\phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 2)(x^2 + 4).$$

Lo mismo sucede sobre $\mathbb{F}_{11}[x]$. En este caso, $11^2 \equiv 1 (\mathrm{mod}\ 12)$ y entonces

$$\phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 6x + 1)(x^2 + 5x + 1).$$

Por último, puesto que $\mathbb{F}_{13}$ es cuerpo de descomposición del polinomio $x^{12} - 1$, el polinomio $\phi_{12}(x)$ deberá escindirse sobre él y factorizarse como producto de cuatro polinomios de grado uno. Esto es,

$$\phi_{12}(x) = x^4 - x^2 + 1 = (x + 2)(x + 6)(x + 7)(x + 11).$$

Capítulo 3

Anillos de Galois

En este tercer capítulo introducimos los anillos de Galois y presentamos sus propiedades más importantes, especialmente aquellas de relevancia en aplicaciones a Teoría Algebraica de Códigos.

3.1. Definición y primeras propiedades

Definición 3.1.1. *Un anillo asociativo A se llama* anillo de Galois (denotado "GR" por sus siglas en inglés: *Galois Ring*) *si es finito, conmutativo, con identidad y existe $d \in \mathbb{N}$ tal que el conjunto de divisores de cero de A es igual a dA.*

Los primeros ejemplos de anillos de Galois que nos encontramos son los cuerpos finitos $\mathbb{F}_{p^r}$ y los anillos de residuos de enteros de orden potencia de primo $\mathbb{Z}_{p^n}$. En ambos casos basta con tomar $d = p$.
En la definición de anillo de Galois no es necesario imponer la conmutatividad del anillo, ya que ésta puede ser deducida del resto de las condiciones. Sin embargo este hecho no se deriva de forma inmediata, sino que requiere una aproximación al estudio de los Anillos de Galois más extensa de la que aquí recogemos. Por lo tanto, y por cuestiones de brevedad, asumiremos directamente la conmutatividad del anillo. A continuación presentamos las propiedades básicas de los anillos de Galois.

Teorema 3.1.1. *Sea A un GR en el que el conjunto de divisores de cero es pA. Entonces se verifican las siguientes propiedades:*

1. *El conjunto $A^* = A \setminus pA$ es un grupo multiplicativo abeliano (el grupo de las unidades de A).*

2. *A es un anillo local con ideal maximal pA. El anillo cociente $\overline{A} = A/pA$ es un cuerpo finito $\mathbb{F}_q$ donde $q = p^r$ (para algún $r \in \mathbb{N}$). Es decir, p es un número primo.*

3. *La característica de A es igual a p^n, $n \in \mathbb{N}$.*

4. *El conjunto de ideales de A es la cadena estrictamente decreciente:*

$$A = p^0 A \rhd p^1 A \rhd \cdots \rhd p^{n-1} A \rhd p^n A = 0. \tag{3.1}$$

5. *Para todo $t \in \{0, \ldots, n\}$ se verifica la igualdad:*

$$|p^t A| = q^{n-t}.$$

En particular: $|A| = q^n$ y $|A^*| = (q-1)q^{n-1}$. Además, para todo $b \in p^t A \setminus p^{t+1} A$, y para todo $t \in \{0, \ldots, n-1\}$, se verifica:

$$Ab = bA = p^t A.$$

Demostración.

1. Todos los elementos de A son divisores de cero o unidades: si $x \in A$ no es un divisor de cero, entonces la aplicación $R_x : A \to A$ dada por $R_x(y) = yx$ es inyectiva y, por ser A finito, biyectiva, por lo que existe $y \in A$ tal que $yx = e$ (donde e es la identidad de A) y así x es una unidad. Por lo tanto A^* es el grupo multiplicativo de las unidades de A y es, claramente, abeliano.

2. Como todos los elementos del conjunto A^* son unidades pA es el único ideal maximal de A. Por lo tanto $\overline{A} = A/pA$ es un cuerpo finito $\mathbb{F}_q$ de característica p.

3. Supongamos que la característica de A es $k = p^n l$ (con $n \in \mathbb{N}_0$, $l \in \mathbb{N}$ y $(p, l) = 1$) y que $l > 1$. Entonces los elementos $a = p^n e$ y $b = le$ son divisores de cero, por lo que $le \in pA$. De aquí $l\overline{e} = \overline{0} \in \overline{A}$ y así p divide a l, lo que es imposible. Por lo tanto $l = 1$.

4. Para todo $t \in \{0, \ldots, n\}$ el conjunto $p^t A$ es un ideal de A y los contenidos en (3.1) son estrictos, ya que si existe $t < n$ tal que $p^t A = p^{t+1} A$ entonces $p^s A = p^t A$ para todo $s \geq t$. En particular $p^{n-1} A = p^n A = 0$ y $p^{n-1} e = 0$, lo cual es una contradicción.

   Si I es un ideal no nulo de A entonces existe $t \in \{0, \ldots, n-1\}$ tal que $I \subseteq p^t A$ pero $I \not\subseteq p^{t+1} A$. Sea $a \in I \setminus p^{t+1} A$, es decir, $a = p^t b$, con $b \in A^*$. Como $bA = A$ tenemos $p^t A = p^t bA = aA \subseteq I$, i.e. $I = p^t A$.

5. Vamos a ver que el orden de $A_t = p^t A / p^{t+1} A$ es q, para lo cual definimos $\cdot : \overline{A} \times A_t \to A_t$ como $\overline{\lambda} \cdot \widetilde{a} = \widetilde{\lambda a}$ donde

$$\widetilde{a} = a + p^{t+1} A \in A_t \text{ y } \overline{\lambda} = \lambda + pA \in \overline{A}.$$

   El producto $\cdot$ está bien definido y convierte a A_t en un $\mathbb{F}_q$-espacio vectorial. Si $a \in p^t A \setminus p^{t+1} A$, entonces $a = p^t b$ con $b \in A^*$, por lo que $Ab = A$ y $Aa = A(p^t b) = p^t A$, es decir, $\overline{A} \cdot \widetilde{a} = A_t$. Así $\dim_{\overline{A}} A_t = 1$ y $|A_t| = q$.

■

Utilizaremos la siguiente notación a lo largo de todo el capítulo.

Nota. Si A es un GR y $a, b \in A$ tales que $a - b = p^t r$ con $t \in \mathbb{N}$ y $r \in A$, entonces escribimos $a \underset{p^t}{\equiv} b$.

3.2. Teoremas de existencia y unicidad

En el estudio de los anillos de Galois juega un papel muy importante su cuerpo finito cociente, ya que muchas de sus propiedades pueden ser "levantadas" mediante el uso de técnicas polinomiales. Además un anillo de Galois está determinado unívocamente (salvo isomorfismo) por el cardinal de su cuerpo finito cociente y por su característica.

Nota. Sea A un GR de característica p^n y $\overline{A} = A/pA = \mathbb{F}_{p^r}$. Dado un polinomio $f(x) = \sum_{i=0}^{r} a_i x^i \in A[x]$ denotaremos por $\overline{f}(x)$ el polinomio $\sum_{i=0}^{r} \overline{a_i} x^i \in \overline{A}[x]$.

Definición 3.2.1. *Si A es un GR, entonces un polinomio $g(x) \in A[x]$ se dice* polinomio de Galois *si es mónico y $\overline{g}(x) \in \overline{A}[x]$ es irreducible sobre $\overline{A}$.*

La existencia de polinomios de Galois de cualquier grado sobre un anillo de Galois queda garantizada por la existencia de polinomios mónicos e irreducibles de cualquier grado sobre cuerpos finitos. El siguiente teorema ilustra cómo las técnicas de construcción de cuerpos finitos pueden ser "levantadas" para construir anillos de Galois.

Teorema 3.2.1. *Sea A un GR de característica p^n y q^n elementos ($q = p^r$), $m \in \mathbb{N}$ y $g(x) \in A[x]$ un polinomio de Galois de grado m. Entonces $S = A[x]/\langle g(x)\rangle$ es un GR de característica p^n y cardinal q^{mn}.*

Demostración. Claramente la característica de S es p^n, su cardinal es $(q^n)^m$ y, como $(pS)^n = p^n S = 0$, todos los elementos del conjunto pS son divisores de cero. Veamos que todo elemento de $S^* = S \setminus pS$ es una unidad. Cualquier elemento de S se presenta de forma única como $f(x) + \langle g(x)\rangle = [f(x)]_g$ donde $f(x) \in A[x]$ es un polinomio de grado menor que m.
Si $[f(x)]_g \in S^*$ entonces $f(x) \notin pA$ y $\overline{f}(x) \neq \overline{0}$. Como el grado de $\overline{f}(x)$ es menor que el grado de $\overline{g}(x)$, se verifica que $(\overline{f}(x), \overline{g}(x)) = \overline{e}$ (donde e denota la identidad de A). Por lo tanto existen polinomios $u(x), v(x) \in A[x]$ tales que $\overline{u}(x)\overline{f}(x) + \overline{v}(x)\overline{g}(x) = \overline{e}$, es decir, $u(x)f(x) + v(x)g(x) = e + pb(x)$ para cierto $b(x) \in A[x]$. De aquí

$$[u(x)]_g[f(x)]_g = [e]_g + p[b(x)]_g$$

$$[u(x)]_g^{p^{n-1}}[f(x)]_g^{p^{n-1}} = ([e]_g + p[b(x)]_g)^{p^{n-1}} = [e]_g,$$

esto es, $[f(x)]_g$ es una unidad. ∎

Notemos que, en las condiciones del teorema anterior, S es un A-módulo libre de rango m con base $\{[e]_g, [x]_g, \ldots, [x^{m-1}]_g\}$.

Nota. Si A es un subanillo de S y ambos son GR, entonces el cuerpo finito $\overline{A} = A/pA$ es un subcuerpo de $\overline{S} = S/pS$.

Definición 3.2.2. *Si A y S son dos GR tales que $A \subseteq S$, con $[\overline{S} : \overline{A}] = m$, entonces diremos que S es una* extensión de Galois de grado m de A *(o que A es un* subanillo de Galois de S*) y denotaremos el grado de esta extensión como $[S : A]$.*

Corolario 3.2.1. *Para todo anillo de Galois A y para todo $m \in \mathbb{N}$ existe una extensión de Galois de grado m de A.*

Corolario 3.2.2 (Existencia)**.** *Para todo número primo p y para cualesquiera $r, n \in \mathbb{N}$, existe un anillo de Galois S de característica p^n y cardinal p^{rn} que es extensión de Galois de grado r de $\mathbb{Z}_{p^n}$.*

Nota. Si S es una extensión de Galois de A y $a \in S$, entonces llamamos *extensión de A por a*, y lo denotaremos $A[a]$, al subanillo de S generado por $A \cup \{a\}$. Claramente $A[a] = \{f(a) \mid f(x) \in A[x]\} \cong A[x]/\mathfrak{a}$ donde $\mathfrak{a}$ es el ideal anulador $\{f(x) \in A[x] \mid f(a) = 0\}$.

Las analogías que presentan los polinomios irreducibles sobre cuerpos finitos y los polinomios de Galois sobre anillos de Galois se muestran en los resultados que siguen.

Lema 3.2.1. *Sea S una extensión de Galois de un anillo de Galois A, $a \in S$ y $f(x) \in A[x]$ tal que $\overline{f}(\overline{a}) = \overline{0}$ y $\overline{f}'(\overline{a}) \neq \overline{0}$. Entonces existe un único $b \in S$, raíz de $f(x)$, tal que $\overline{b} = \overline{a}$.*

Demostración. Vamos a construir una serie de elementos $b_0, \ldots, b_{n-1} \in S$ de tal forma que $\overline{b_t} = \overline{a}$ y $f(b_t) \underset{p^{t+1}}{\equiv} 0$ para todo $t \in \{0, \ldots, n-1\}$. La construcción es inductiva:
$b_0 = a$ y, si el elemento b_{t-1} ya está construido,

$$b_t = b_{t-1} - f'(b_{t-1})^{-1} f(b_{t-1}).$$

Vamos a probar por inducción que la secuencia está bien definida y que satisface las condiciones enunciadas. El caso $t = 0$ es claro.
Construida la secuencia hasta el paso $t-1$, como $\overline{b_{t-1}} = \overline{a}$, se verifica que $\overline{f}'(\overline{b_{t-1}}) = \overline{f}'(\overline{a}) \neq \overline{0}$ y, por tanto, $f'(b_{t-1})$ es una unidad. Además, como $f(b_{t-1}) \underset{p^t}{\equiv} 0$, tenemos $\overline{b_t} = \overline{b_{t-1}} = \overline{a}$ y, si consideramos el desarrollo de Taylor del polinomio $f(x)$ en el punto b_{t-1}, obtenemos

$$f(x) = f(b_{t-1}) + f'(b_{t-1})(x - b_{t-1}) + R_2(x - b_{t-1})$$

donde $R_2(x - b_{t-1})$ es una expresión en $(x - b_{t-1})^2$. De esta forma

$$f(b_t) = R_2(b_t - b_{t-1}) = R_2(-f'(b_{t-1})^{-1} f(b_{t-1}))$$

y, como $f(b_{t-1}) \underset{p^t}{\equiv} 0$, tenemos que $f(b_t) \underset{p^{2t}}{\equiv} 0$, es decir, $f(b_t) \underset{p^{t+1}}{\equiv} 0$. Por lo tanto el elemento $b = b_{n-1}$ está en las condiciones de teorema.
Veamos que la raíz b es única. Supongamos que c es otra raíz de $f(x)$ tal que $\overline{c} = \overline{a}$. Si $c \neq b$ entonces $c = b + p^t d$ para ciertos $d \in S^*$ y $t \in \{1, \ldots, n-1\}$. Por lo tanto, si consideramos el desarrollo de Taylor de $f(x)$ centrado en el punto b, tenemos

$$f(c) = f(b) + f'(b)(c-b) + R_2(c-b) = f(b) + p^t d f'(b) + p^{t+1} h$$

para cierto $h \in S$. Como $f(c) = f(b) = 0$ deducimos que $p^t d f'(b) \in p^{t+1}S$, lo cual es imposible ya que $\overline{f}'(\overline{b}) \neq \overline{0}$ implica que $df'(b) \notin pS$. ■

Lema 3.2.2. *Sea S una extensión de Galois de grado m de un anillo de Galois A y $a \in S$ tal que $\overline{A}[\overline{a}] = \overline{S}$. Entonces*

$$S = A[a] = \{f(a) \mid f(x) \in A[x],\ \mathrm{gr}(f(x)) < m\}.$$

Demostración. Para demostrar el resultado basta probar que el conjunto $H = \{f(a) \mid f(x) \in A[x],\ \mathrm{gr}(f(x)) < m\}$ tiene cardinal igual a $|S|$ o, equivalentemente, que si $f(x) \in A[x]$ es un polinomio no nulo de grado menor que m, entonces $f(a) \neq 0$.
Si $f(x)$ es no nulo, entonces existe $t \in \{0, \ldots, n-1\}$ tal que $f(x) = p^t h(x)$ donde $h(x) \in A[x]$ tiene grado menor que m y $\overline{h}(x) \neq \overline{0}$. Si $f(a) = 0$ entonces $0 = p^t h(a)$ y, por tanto, $h(a) \in pS$. De aquí se sigue que $\overline{a}$ es una raíz del polinomio no nulo $\overline{h}(x)$. Pero el grado de este polinomio es menor que m, que es el grado del polinomio mínimo de $\overline{a}$ con respecto a $\overline{A}$ (ya que por hipótesis $\overline{A}[\overline{a}] = \overline{S}$), lo cual es una contradicción. ■

Teorema 3.2.2. *Sea S una extensión de Galois de grado m de A, un GR de característica p^n y cardinal p^{rn}. Sea $g(x) \in A[x]$ un polinomio de Galois de grado k. Entonces:*

1. *$g(x)$ tiene una raíz en S si y sólo si $k \mid m$.*
2. *Si $k \mid m$, entonces $g(x)$ posee exactamente k raíces $a_1, \ldots, a_k \in S$, distintas módulo pS, y $g(x) = (x - a_1) \ldots (x - a_k)$.*
3. *Para todo elemento $a \in S$ la igualdad $S = A[a]$ es cierta si y sólo si a es una raíz de un polinomio de Galois de grado m sobre A.*

Demostración.

1. Si $a \in S$ es raíz de $g(x)$, entonces $\overline{a} \in \overline{S}$ es una raíz de $\overline{g}(x)$, polinomio mónico e irreducible, por lo que k divide a $[\overline{S} : \overline{A}] = m$.

   Recíprocamente, si $k \mid m$, entonces $\overline{g}(x) \in \overline{A}[x]$ posee una raíz $\overline{a} \in \overline{S}$ y, además, $\overline{g}'(\overline{a}) \neq \overline{0}$ al ser un polinomio irreducible sobre un cuerpo finito. De acuerdo al Lema 3.2.1 el polinomio $g(x)$ posee una raíz $a \in S$.

2. Como $k \mid m$ el polinomio $\overline{g}(x)$ posee exactamente k raíces distintas $b_1, \ldots, b_k \in \overline{S}$. Además $\overline{g}'(b_i) \neq \overline{0}$ para todo $i \in \{1, \ldots, k\}$, por lo que de acuerdo al Lema 3.2.1, existen elementos únicos $a_1, \ldots, a_k \in S$ tales que $g(a_i) = 0$ y $\overline{a_i} = b_i$, es decir, elementos distintos módulo pS. De aquí se sigue que para cualesquiera $i, j \in \{1, \ldots, k\}$ con $i \neq j$, el elemento $a_i - a_j$ es una unidad. Como $g(a_1) = 0$ podemos descomponer $g(x)$ en la forma $(x-a_1)g_1(x)$ con $g_1(x) \in A[x]$ mónico. Para todo $i \in \{2, \ldots, k\}$ tenemos $0 = g(a_i) = (a_i - a_1)g_1(a_i)$, por lo que $g_1(a_i) = 0$. Análogamente $g_1(x) = (x - a_2)g_2(x)$ con $g_2(x) \in A[x]$ mónico y $g_2(a_i) = 0$ para todo $i \in \{3, \ldots, k\}$.

   Repitiendo este argumento obtenemos, finalmente, que

   $$g(x) = (x - a_1) \ldots (x - a_k).$$

3. Si a es una raíz de un polinomio de Galois $g(x) \in A[x]$ de grado m entonces $\overline{a} \in \overline{S}$ es una raíz de $\overline{g}(x) \in \overline{A}[x]$ y, como $[\overline{S} : \overline{A}] = m$, tenemos que $\overline{A}[\overline{a}] = \overline{S}$. Por el Lema 3.2.2 deducimos $S = A[a]$.

   Recíprocamente, si $S = A[a]$, entonces $\overline{S} = \overline{A}[\overline{a}]$ y, por el Lema 3.2.2, $S = \{f(a) \mid f(x) \in A[x],\ \mathrm{gr}(f(x)) < m\}$. Por lo tanto $a^m = f(a)$ donde $f(x) \in A[x]$ es un polinomio de grado menor que m, es decir, a es una raíz del polinomio $g(x) = x^m - f(x)$ de grado m. Como $\overline{S} = \overline{A}[\overline{a}]$ y $[\overline{S} : \overline{A}] = m$, tenemos que $g(x) \in A[x]$ es un polinomio de Galois de grado m.

■

Los siguientes corolarios se obtienen de forma inmediata.

Corolario 3.2.3. *Si S es una extensión de Galois de grado m de un anillo de Galois A entonces $S \cong A[x]/\langle g(x)\rangle$ donde $g(x) \in A[x]$ es un polinomio de Galois cualquiera de grado m. Además, S es un A-módulo libre de rango m con base $\{e, x, \ldots, x^{m-1}\}$. En particular, si S es un GR de característica p^n y cardinal p^{sn}, entonces $S \cong \mathbb{Z}_{p^n}[x]/\langle g(x)\rangle$ donde $g(x) \in \mathbb{Z}_{p^n}$ es un polinomio de Galois cualquiera de grado s.*

Demostración. Todo polinomio de Galois $g(x) \in A[x]$ de grado m posee una raíz $a \in S$ y $S = A[a]$. Por la Nota 3.2, $S = A[a] \cong A[x]/\langle g(x)\rangle$. El resto del corolario se obtiene sin más que aplicar el resultado al subanillo

$$S_0 = \{0, e, 2e, \ldots, (p^n - 1)e\} \cong \mathbb{Z}_{p^n},$$

generado por la identidad $e \in S$. ■

Corolario 3.2.4 (Unicidad)**.** *Dos anillos de Galois son isomorfos si y sólo si tienen la misma característica y el mismo cardinal. Al único GR, salvo isomorfismo, de característica p^n y cardinal p^{rn} lo denotaremos $GR(p^{rn}, p^n)$.*

Con la notación introducida $\mathbb{F}_{p^r} = GR(p^r, p)$, $\mathbb{Z}_{p^n} = GR(p^n, p^n)$ y, si $R = GR(q^n, p^n)$ $(q = p^r)$, entonces $\overline{R}$ es isomorfo a $\mathbb{F}_q$. En todo lo que resta de capítulo supondremos siempre que $q = p^r$, con $r \in \mathbb{N}$.

Nota. Si $A = GR(q^n, p^n)$, entonces para todo $t \in \{1, \ldots, n\}$ se tiene $A/p^tA = GR(q^t, p^t)$.

3.3. Conjunto Coordenado de Teichmüller

Otra herramienta fundamental en el estudio de los anillos de Galois es la utilización de conjuntos coordenados, que son el objeto de estudio de esta sección.

Definición 3.3.1. *Si A es un GR, entonces un* conjunto coordenado *es un subconjunto $\Gamma \subseteq A$ tal que sus elementos forman un sistema completo de representantes módulo pA, esto es, $\overline{\Gamma} = \{\overline{a} \mid a \in \Gamma\} = \overline{A}$ y $|\Gamma| = |\overline{A}|$.*

Ejemplo 3.3.1. Si $A = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, entonces $\Gamma = \{0, 1, \ldots, p-1\}$ es un conjunto coordenado de A.

Fijado un conjunto coordenado, un anillo de Galois puede descomponerse fácilmente de forma p-ádica.

Proposición 3.3.1. *Si A es un GR y $\Gamma \subseteq A$ es un conjunto coordenado, entonces para todo $a \in A$ existen elementos únicos $a_0, \ldots, a_{n-1} \in \Gamma$ tales que $a = \sum_{i=0}^{n-1} p^i a_i$.*

Demostración. Consideramos la secuencia $a_0, \ldots, a_{n-1}$ definida de la siguiente manera: $a_0 \in \Gamma$ es el único elemento de Γ tal que $\overline{a} = \overline{a_0}$ y, construidos $a_0, \ldots, a_{t-1}$, escogemos el único elemento $a_t \in \Gamma$ tal que $\overline{a_t} = \overline{s}$, donde $a = a_0 + pa_1 + \cdots + p^{t-1}a_{t-1} + p^t s$. La secuencia está bien definida y verifica la propiedad enunciada.
PoA otro lado hay un total de $|\Gamma|^n = |\overline{A}|^n$ posibles secuencias de longitud n, que es el número de elementos de A, por lo que cada elemento tiene asociada una única secuencia de elementos en las condiciones anteriores. ■

En un anillo de Galois se pueden considerar diferentes conjuntos coordenados pero, entre todos los posibles, hay uno que tiene especial interés.

Definición 3.3.2. *Un conjunto coordenado de un anillo de Galois A se dice* conjunto coordenado de Teichmüller (TCS) *si es cerrado para el producto.*

Proposición 3.3.2. *Si $A = GR(q^n, p^n)$, entonces*

$$\Gamma(A) = \{a \in A \mid a^q = a\}$$

es el único TCS de A.

Demostración. Por un lado $\Gamma(A)$ es cerrado para el producto y, por otro lado, los elementos de $\Gamma(A)$ son las raíces del polinomio $f(x) = x^q - x \in A[x]$. Como $\overline{f}(x) = x^q - x \in \overline{A}[x]$ tiene como raíces (todas ellas simples) los q elementos del cuerpo $\overline{A}$, por el Lema 3.2.1, podemos "levantar" todas estas raíces a raíces de $f(x)$ y, además, de forma única. Así $f(x)$ se escinde en A como $f(x) = \prod_{a \in \Gamma(A)}(x - a)$ y el cardinal de $\Gamma(A)$ es igual al cardinal de $\overline{A}$ y, por el Lema 3.2.1, todas las raíces son distintas módulo pA. Por lo tanto $\Gamma(A)$ es un TCS.
Además, es único, ya que si $\Gamma \subseteq A$ es un TCS, entonces el epimorfismo canónico $\pi : A \to \overline{A}$ induce un isomorfismo multiplicativo $\Gamma \to \overline{A}$, al ser

Γ cerrado para el producto. De esta forma todo elemento $a \in \Gamma$ satisface la ecuación $a^q = a$, es decir, $a \in \Gamma(A)$. Por lo tanto $\Gamma = \Gamma(A)$. ■

Nota. Si $A^{=}GR(q^n, p^n)$ entonces el epimorfismo canónico $A \to \overline{A}$ induce un isomorfismo multiplicativo $\Gamma(A) \to \overline{A}$.

Dado un anillo de Galois A con conjunto coordenado de Teichmüller $\Gamma(A)$ podemos considerar, para cada elemento $a \in A$, la descomposición p-ádica asociada a $\Gamma(A)$:

$$a = \gamma_0(a) + p\gamma_1(a) + \cdots + p^{n-1}\gamma_{n-1}(a) \tag{3.2}$$

donde $\gamma_i(a) \in \Gamma(A)$ para todo $i \in \{0, \ldots, n-1\}$.

Definición 3.3.3. *Si A es un GR y $\Gamma(A)$ su TCS, entonces las aplicaciones $\gamma_i : A \to \Gamma(A)$ inducidas por la descomposición p-ádica asociada a $\Gamma(A)$ se llaman* funciones coordenadas de A.

Proposición 3.3.3. *Si $A = GR(q^n, p^n)$, $\Gamma(A)$ es su TCS y $\gamma_0 : A \to \Gamma(A)$ es la primera función coordenada, entonces $\gamma_0(x) = x^{q^{n-1}}$.*

Demostración. Vamos a probar, por inducción en t, que se verifica la congruencia $\gamma_0(x) \underset{p^{t+1}}{\equiv} x^{q^t}$. El caso $t = 0$ es claro, puesto que $\overline{\gamma_0(x)} = \overline{x}$. Si se verifica la congruencia para $t-1$ entonces $\gamma_0(x) = x^{q^{t-1}} + p^t y_x$ con $y_x \in A$. Elevamos ambos miembros de la igualdad a q y obtenemos

$$\gamma_0(x)^q = x^{q^t} + \binom{q}{1}(x^{q^t-1})^{q-1}p^t y_x + \cdots + (p^t y_x)^q = x^{q^t} + p^{t+1}z_t$$

para cierto $z_t \in A$. Basta notar que $\gamma_0(x) \in \Gamma(A)$ y que, por tanto, $\gamma_0(x)^q = \gamma_0(x)$ para concluir $\gamma_0(x) \underset{p^{t+1}}{\equiv} x^{q^t}$. ■

Ejemplo 3.3.2. Si $A = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, con $n = 1$ ó $p = 2$, entonces el TCS de A es el conjunto $\Gamma(A) = \{0, 1, \ldots, p-1\}$. Si $n > 1$ y $p \neq 2$, entonces $\Gamma(A) \neq \{0, 1, \ldots, p-1\}$, ya que $(-1)^p = -1$ y, por tanto, $-1 \in \Gamma(A)$. En este caso $\Gamma(A) = \{0, 1, 2^{p^{n-1}}, \ldots, (p-1)^{p^{n-1}}\}$.

Nota. Si $A = GR(q^n, p^n)$, entonces el conjunto coordenado de Teichmüller $\Gamma(A)$ no es, en general, un conjunto cerrado para la suma: basta notar que $\Gamma(\mathbb{Z}_{p^n})$, con $p \neq 2$, no es cerrado para la suma.

Vamos a introducir una nueva función suma en el conjunto coordenado de Teichmüller, con el objeto de que éste sea cerrado para la suma.

Definición 3.3.4. *Si $\Gamma(A)$ es el TCS de un anillo de Galois A, entonces definimos la suma $\oplus : \Gamma(A) \times \Gamma(A) \to \Gamma(A)$ como $a \oplus b = \gamma_0(a+b)$ para todo $a, b \in \Gamma(A)$.*

Proposición 3.3.4. *Si $A = GR(q^n, p^n)$ y $\Gamma(A) \subseteq A$ es su TCS, entonces $(\Gamma(A), \oplus, \cdot)$ es un cuerpo finito de q elementos y el epimorfismo canónico $\pi : \Gamma(A) \to \overline{A}$ es un isomorfismo de cuerpos.*

Demostración. La aplicación π es un isomorfismo multiplicativo que, dados $a, b \in \Gamma(A)$, verifica

$$\pi(a \oplus b) = \pi(\gamma_0(a+b)) = \pi\gamma_0(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b).$$

Por lo tanto π es un isomorfismo y $(\Gamma(A), \oplus, \cdot)$ es un cuerpo finito de q elementos. ∎

El conjunto coordenado de Teichmüller nos permite describir los subanillos de Galois y el grupo de automorfismos de los anillos de Galois. También nos permite estudiar la estructura del grupo multiplicativo de las unidades.

3.4. Subanillos de Galois. Automorfismos

Estudiamos a continuación el retículo de subanillos de Galois de un anillo de Galois.

Teorema 3.4.1. *Si $S = GR(p^{sn}, p^n)$ y $A = GR(p^{rn}, p^n) \subseteq S$ es un subanillo de Galois, entonces r divide a s. Recíprocamente, para cada divisor r de s, existe exactamente un subanillo de Galois de S de la forma $GR(p^{rn}, p^n)$.*

Demostración. Si A es un subanillo de Galois de S entonces $\overline{A} = A/pA = \mathbb{F}_{p^r}$ puede considerarse subcuerpo de $\overline{S} = S/pS = GF(p^s)$, por lo que r divide a s.
Recíprocamente, si r divide a s, entonces el subanillo S_0 generado por la identidad de S es $\mathbb{Z}_{p^n} = GR(p^n, p^n)$ y S es una extensión de Galois

grado s de S_0. Sea $g(x) \in S_0[x]$ un polinomio de Galois de grado r. Como $r \mid s$, de acuerdo al Teorema 3.2.2, $g(x)$ tiene una raíz $a \in S$ y el subanillo $A = S_0[a]$, es isomorfo a $\mathbb{Z}_{p^n}[x]/\langle g(x)\rangle$. Por el Corolario 3.2.3, $A = GR(p^{rn}, p^n)$. Veamos que éste es el único subanillo de Galois de S de cardinal p^{rn}. Es claro que $\Gamma(A) = \{a \in A \mid a^{p^r} = a\} \subseteq \{a \in S \mid a^{p^r} = a\} \subseteq \Gamma(S)$, puesto que r divide a s. Así $\Gamma(A) \subseteq \{a \in \Gamma(S) \mid a^{p^r} = a\}$ y, como $p^r = |\Gamma(A)| \leq |\{a \in \Gamma(S) \mid a^{p^r} = a\}| = p^r$, tenemos que $\Gamma(A) = \{a \in \Gamma(S) \mid a^{p^r} = a\}$. Para otro subanillo de Galois T de S con $T = GR(p^{rn}, p^n)$ se tiene que $\Gamma(T) = \{a \in \Gamma(S) \mid a^{p^r} = a\} = \Gamma(A)$, es decir, el TCS de A y T es el mismo y así

$$\begin{aligned} A &= \{a_0 + pa_1 + \cdots + p^{n-1}a_{n-1} \mid a_i \in \Gamma(A) = \Gamma(T), \forall i \in \{0, \ldots, n-1\}\} \\ &= T. \end{aligned}$$

■

Notemos que, si S es una extensión de Galois de grado m de A, entonces el cuerpo $(\Gamma(S), \oplus, \cdot)$ es una extensión de Galois de grado m del cuerpo $(\Gamma(A), \oplus, \cdot)$.

Nota. Si $S = GR(p^{sn}, p^n)$, con $s, n > 1$, entonces existen subanillos de S que no son, necesariamente, de Galois. Por ejemplo, si $S_0 = GR(p^n, p^n)$ denota el subanillo generado por la identidad, entonces

$$A = \Gamma(S_0) + p\Gamma(S_0) + \cdots + p^{n-2}\Gamma(S_0) + p^{n-1}\Gamma(S)$$

es un subanillo propio de S, ya que $A = S_0 + p^{n-1}\Gamma(S)$, que no es de Galois, puesto que $|A| = p^{n-1}p^s$.

Con ayuda del conjunto coordenado de Teichmüller también podemos estudiar cuál es el grupo de automorfismos de un anillo de Galois A que denotamos como $Aut(A)$.

Teorema 3.4.2. *Si $A = GR(q^n, p^n)$, entonces:*

1. *Todo $\tau \in \mathrm{Aut}(A)$ estabiliza el TCS de A, es decir, $\tau(\Gamma(A)) = \Gamma(A)$. Además, la restricción $\tau|_{\Gamma(S)} = \widehat{\tau}$ es un automorfismo del cuerpo $(\Gamma(A), +, \oplus)$.*

2. *Para todo* $\tau \in \mathrm{Aut}(A)$ *existe* $v \in \{0, \ldots, s-1\}$ *tal que*

$$\tau(a) = \gamma_0(a)^{p^v} + p\gamma_1(a)^{p^v} + \cdots + p^{n-1}\gamma_{n-1}(a)^{p^v}$$

con $a \in A$.

3. *La aplicación* $\varphi : \mathrm{Aut}(A) \to \mathrm{Aut}(\Gamma(A))$, *dada por* $\varphi(\tau) = \widehat{\tau}$, *es un isomorfismo de grupos y* $\mathrm{Aut}(A)$ *es un grupo cíclico de orden* r.

Demostración.

1. Si $a \in \Gamma(A)$, entonces $a^{p^r} = a$ y, por tanto, $\tau(a)^{p^r} = \tau(a)$, con lo que τ estabiliza $\Gamma(A)$. Además $\widehat{\tau}$ es un isomorfismo multiplicativo y, si $a, b \in \Gamma(A)$, entonces: $\widehat{\tau}(a \oplus b) = \tau(\gamma_0(a+b)) = \tau((a+b)^{q^{n-1}}) = \tau(a+b)^{q^{n-1}} = (\tau(a) + \tau(b))^{q^{n-1}} = \gamma_0(\widehat{\tau}(a) + \widehat{\tau}(b)) = \widehat{\tau}(a) \oplus \widehat{\tau}(b)$.

2. Como $\widehat{\tau} \in \mathrm{Aut}((\Gamma(A), +, \oplus))$ y $|\Gamma(A)| = p^r$, existe $v \in \{0, \ldots, r-1\}$ tal que para todo $a \in \Gamma(A)$: $\widehat{\tau}(a) = a^{p^v}$. Para todo $a \in A$: $\tau(a) = \tau(\gamma_0(a) + p\gamma_1(a) + \cdots + p^{n-1}\gamma_{n-1}(a)) = \widehat{\tau}(\gamma_0(a)) + p\widehat{\tau}(\gamma_1(a)) + \cdots + p^{n-1}\widehat{\tau}(\gamma_{n-1}(a)) = \gamma_0(a)^{p^v} + p\gamma_1(a)^{p^v} + \cdots + p^{n-1}\gamma_{n-1}(a)^{p^v}$.

3. Claramente φ es un homomorfismo y, además, es inyectivo, ya que de acuerdo al apartado 2, si $\widehat{\tau} = \widehat{\sigma}$, entonces $\tau = \sigma$. Veamos que es suprayectivo: A es una extensión de grado r del subanillo generado por la identidad $A_0 = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, por lo que $A = A_0[a]$ donde $a \in A$ es una raíz de un polinomio de Galois de grado r, $g(x) \in A_0[x]$. Por el Teorema 3.2.2, $g(x)$ posee r raíces distintas $a_1 = a, a_2, \ldots, a_r \in A$ y $A = A_0[a_i]$ para todo $i \in \{1, \ldots, r\}$. Para cada $i \in \{1, \ldots, r\}$ la aplicación $\sigma_i(a) = a_i$ y $\sigma_i(b) = b$ para todo $b \in A_0$ es un automorfismo de A, y todos ellos son distintos. Por lo tanto el orden del grupo $\mathrm{Aut}(A)$ es, al menos, r y la aplicación φ es suprayectiva.

■

Corolario 3.4.1. *Si* $A = GR(q^n, p^n)$ *y* $S = GR(q^{mn}, p^n)$ *es una extensión de Galois de grado* m *suya, entonces el grupo* $\mathrm{Aut}(S|A)$, *de los automorfismos de* S *que dejan fijos los elementos del subanillo* A, *es isomorfo al grupo* $Aut(\Gamma(S)|\Gamma(A))$. *Por tanto* $Aut(\Gamma(S)|\Gamma(A))$ *es un grupo cíclico de orden* m *generado por el automorfismo*

$$\tau(a) = \gamma_0(a)^q + p\gamma_1(a)^q + \cdots + p^{n-1}\gamma_{n-1}(a)^q$$

para todo $a \in S$.

Demostración. Puesto que A es igual al conjunto $\Gamma(A) + p\Gamma(A) + \cdots + p^{n-1}\Gamma(A)$, si $\sigma \in \mathrm{Aut}(S|A)$ entonces $\widehat{\sigma} \in \mathrm{Aut}(\Gamma(S)|\Gamma(A))$ y, la aplicación φ del Teorema 3.4.2 induce un isomorfismo $\varphi : \mathrm{Aut}(S|A) \to \mathrm{Aut}(\Gamma(S)|\Gamma(A))$. Así $\mathrm{Aut}(S|A)$ es cíclico de orden m generado por el automorfismo τ tal que $\widehat{\tau}$ es el automorfismo de Frobenius $\widehat{\tau}(a) = a^q$, para todo $a \in \Gamma(S)$. ■

Para terminar esta sección introducimos el concepto de traza de una extensión de Galois, que generaliza la traza de una extensión de cuerpos. La función traza de un anillo de Galois nos va a permitir, en secciones posteriores, representar ciertas secuencias recurrentes lineales y describir cierto tipo de códigos lineales sobre anillos de Galois.

Definición 3.4.1. *Sea* $S = GR(q^{mn}, p^n)$ *una extensión de Galois de grado* m *de* $A = GR(q^n, p^n)$. *La función* traza *de la extension* $S|A$ *es la aplicación:*

$$\mathrm{Tr}_A^S(a) = \sum_{\sigma \in \mathrm{Aut}(S|A)} \sigma(a).$$

Proposición 3.4.1. *Si* $S = GR(q^{mn}, p^n)$ *es una extensión de Galois de grado* m *de* $A = GR(q^n, p^n)$ *y* $\mathrm{Tr} = \mathrm{Tr}_A^S$ *es la función traza de la extensión* $S|A$, *entonces* $\mathrm{Tr} : S \to A$ *es un epimorfismo de* A*-módulos.*

Demostración. La aplicación Tr es un homomorfismo de A-módulos y por el Corolario 3.4.1, si $a \in \Gamma(S)$, entonces $\mathrm{Tr}(a) = a + a^q + \cdots + a^{q^{m-1}}$. Por tanto, $\gamma_0(\mathrm{Tr}(a)) = \gamma_0(a + a^q + \cdots + a^{q^{m-1}}) = \gamma_0(a) \oplus \gamma_0(a)^q \oplus \cdots \oplus \gamma_0(a)^{q^{m-1}} = a \oplus a^q \oplus \cdots \oplus a^{q^{m-1}} = \mathrm{Tr}_{\Gamma(A)}^{\Gamma(S)}(a)$, donde $\mathrm{Tr}_{\Gamma(A)}^{\Gamma(S)}$ es la traza de la extensión de cuerpos $\Gamma(S)|\Gamma(A)$. Como $\mathrm{Tr}_{\Gamma(A)}^{\Gamma(S)}$ es suprayectiva, existe $a \in \Gamma(S)$ tal que $e = \mathrm{Tr}_{\Gamma(A)}^{\Gamma(S)}(a) = \gamma_0(\mathrm{Tr}(a))$, es decir, $\mathrm{Tr}(a)$ es una unidad. Por lo tanto $A = A\mathrm{Tr}(a) = \mathrm{Tr}(Aa) \subseteq \mathrm{Tr}(Sa) = \mathrm{Tr}(S) \subseteq A$. ■

Capítulo 4

Anillos finitos locales

En este capítulo nos ocuparemos de la estructura de los anillos locales. Como veremos en el teorema de estructura, estos anillos son los bloques fundamentales con los que se construyen los anillos conmutativos finitos. Terminaremos el capítulo estudiando someramente los anillos de cadena, clase que incluye como ejemplo paradigmático a los anillos de Galois, estudiados en el capítulo anterior. La referencia básica de este capítulo es el clásico libro de McDonald sobre anillos finitos con identidad [6]. Para ser congruentes con dicho texto y distinguirla del caso de anillo de Galois denotaremos la proyección sobre el cuerpo residual como μ en lugar de $\bar{\cdot}$.

4.1. Estructura de los anillos finitos

Como vimos en los preliminares un anillo conmutativo A es *local* si tiene un único ideal maximal que denotaremos por $\mathfrak{m}$. Las siguientes propiedades son equivalentes a la definición que acabamos de enunciar (siempre que $1 \neq 0$)

1. Si la suma de cualquier par elementos en A que no sean unidades no es tampoco una unidad.

2. Si $a \in A$, entonces a o bien $1 - a$ es una unidad.

3. Si una suma finita es una unidad, entonces también lo será alguno de sus sumandos.

La demostración de estas propiedades puede encontrarse en [1] así como una introducción a los anillos locales.

Ejemplo 4.1.1. Si $\mathbb{F}$ es un cuerpo y n es un entero positivo entonces el anillo cociente $A = \mathbb{F}[x]/\langle x^n \rangle$ es local y su ideal maximal $\mathfrak{m}$ son aquellas clases representadas por polinomios con término constante nulo. Simplemente comprobando la Definición 3.1.1 se tiene que A no es un anillo de Galois.

El *teorema chino de los restos* es una técnica recurrente dentro del álgebra, proporcionamos a continuación la versión que utilizaremos durante este curso. Consideremos A un anillo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A. Diremos que los ideales $\mathfrak{a}_i$ y $\mathfrak{a}_j$ con $i \neq j$ son *coprimos* si se cumple que $\mathfrak{a}_i + \mathfrak{a}_j = A$. Dado el siguiente homomorfismo de anillos

$$\phi : A \to A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_n \tag{4.1}$$

donde $\phi(a) = (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$. Las siguientes propiedades se pueden verificar fácilmente:

1. Si para cada par $i \neq j$ se tiene que $\mathfrak{a}_i$, $\mathfrak{a}_j$ son ideales coprimos entonces
$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \cdots \cdot \mathfrak{a}_n.$$
2. Si $\mathfrak{a}_i$, $\mathfrak{a}_j$ son ideales coprimos entonces también lo son sus potencias $\mathfrak{a}_i^m$, $\mathfrak{a}_j^m$ para $m = 1, 2, \ldots$.
3. El homomorfismo de anillos ϕ en (4.1) es inyectivo si y sólo si $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \{0\}$.
4. El homomorfismo de anillos ϕ en (4.1) es sobreyectivo si y sólo si $\mathfrak{a}_i$, $\mathfrak{a}_j$ son coprimos si $i \neq j$.

La demostración de las propiedades anteriores se dejan como ejercicio al lector.

Definición 4.1.1. *Un elemento $e \in A$ de un anillo A diremos que es un idempotente si $e^2 = e$. Diremos que dos idempotentes e_1 y e_2 son ortogonales si $e_1 \cdot e_2 = 0$ y que e es un idempotente central si $e \cdot a = a \cdot e$ para todo elemento a del anillo A.*

Los siguientes resultados se presentan sin demostración pues son unos fáciles ejercicios para el lector.

Lema 4.1.1. *Un dominio de integridad finito es un cuerpo.*

Proposición 4.1.1. *Si A es un anillo, las siguientes proposiciones son equivalentes:*

1. *A se puede expresar como una suma directa de anillos A_i con $i = 1, 2, \ldots, n$.*
2. *Existen idempotentes e_i con $i = 1, 2, \ldots, n$ centrales en el anillo A tales que*
$$1 = \sum_{i=1}^{n} e_i \quad \textit{and} \quad A_i \simeq e_i A. \tag{4.2}$$
3. *A es suma directa de ideales $\mathfrak{a}_i \simeq A_i$ para $i = 1, 2, \ldots, n$.*

Con los resultados y notación anterior alcanzamos la siguiente caracterización de los anillos conmutativos finitos.

Teorema 4.1.1 (Estructura de los anillos conmutativos finitos)**.** *Sea A un anillo conmutativo finito. A descompone de manera única (salvo reordenamiento de los sumandos) como una suma directa de anillos locales.*

Demostración. Consideremos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos de A, claramente $A/\mathfrak{p}_i$ es un cuerpo teniendo en cuenta el Lema 4.1.1, de donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ son ideales maximales de A. Tenemos que $\mathrm{Rad}(A) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$ y como $\mathfrak{p}_i$, $\mathfrak{p}_j$ son coprimos si $i \neq j$ tenemos que $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \cdots \mathfrak{p}_n$ y existe un m entero mínimo tal que $\mathrm{Rad}(A)^m = \mathfrak{p}_1^m \cdot \mathfrak{p}_2^m \cdot \cdots \mathfrak{p}_n^m = \{0\}$ pues es un ideal nilpotente. Definimos el homomorfismo de anillos

$$\phi_m : A \to A/\mathfrak{p}_1^m \oplus \cdots \oplus A/\mathfrak{p}_n^m \tag{4.3}$$

donde $\phi_m(a) = (a + \mathfrak{p}_1^m, \ldots, a + \mathfrak{p}_n^m)$. Como $\bigcap_{i=1}^n \mathfrak{p}_i^m = \{0\}$ tenemos que ϕ_m es inyectivo. Además $\mathfrak{p}_i$, $\mathfrak{p}_i^m$ con $i \neq j$ son coprimos, por lo que ϕ_m también es sobreyectivo.
Para cada elección de $1 \leq i \leq n$ los ideales de $A/\mathfrak{p}_i^m$ están en correspondencia natural con los ideales de A que contienen a $\mathfrak{p}_i^m$ y, como $\mathfrak{p}_i$ es el

único ideal maximal con $A \supset \mathfrak{p}_i \supset \mathfrak{p}_i^m$, entonces $A/\mathfrak{p}_i$ es un anillo local con ideal maximal $\mathfrak{m}_i = \mathfrak{p}_i/\mathfrak{p}_i^m$.
Supongamos ahora que tenemos dos descomposiciones de A diferentes que cumplan el enunciado del teorema. Correspondiendo a cada una tendremos las siguientes expresiones de la unidad como suma de idempotentes ortogonales

$$1 = \sum_{i=1}^{n} e_i = \sum_{j=1}^{n'} f_j.$$

Teniendo en cuenta que los sumandos Ae_i y Af_j son locales ningún e_i puede ser suma de dos idempotentes. Por lo tanto de $e_i = \sum_{j=1}^{n'} e_i f_j$ se sigue que $e_i = e_i f_{j(i)}$ y de manera similar $f_j = f_j e_{i(j)}$. Es decir, tenemos la siguiente igualdad

$$e_i = e_i f_{j(i)} = e_i f_{j(i)} e_{i(j(i))}.$$

Como los e_i son ortogonales entonces $i = i(j(i))$ y existe una biyección entre $\{e_i\}_{i=1}^{n}$ y $\{f_j\}_{j=1}^{n'}$. De aquí se sigue que $e_i = e_i f_{j(i)}$ y de manera similar $f_{j(i)} = f_{j(i)} e_i$ y por lo tanto $e_i = f_{j(i)}$. ■

La demostración del siguiente resultado también se deja como un ejercicio sencillo para el lector.

Proposición 4.1.2. *Sea $A = A_1 \oplus A_2 \oplus \cdots \oplus A_n$ la descomposición en anillos locales de un anillo finito conmutativo, entonces*

1. *$U(A) = U(A_1) \times U(A_2) \times \cdots \times U(A_n)$ y*
2. *el anillo de polinomios $A[x]$ factoriza*

$$A[x] = \bigoplus_{i=1}^{n} A_i[x].$$

4.2. El anillo de polinomios $A[x]$

Durante esta sección el anillo A será siempre un anillo conmutativo finito local con ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$. Denotaremos por μ la proyección natural

$$\mu : A[x] \to \mathbb{K}[x]$$

de donde el morfismo natural de A en $\mathbb{K}$ es simplemente la restricción de μ a los polinomios constantes.

Teorema 4.2.1. *Sean A y B dos anillos tales que $A \subset B$. Entonces si $b \in B$ existe un polinomio mónico $f \in A[x]$ tal que $f(b) = 0$.*

Demostración. Consideremos el conjunto

$$T = \left\{ \sum_{\text{fta}} a_i b^i \mid a_i \in A \right\}.$$

Claramente $A \subset T \subset B$, escojamos para cada elemento de T el representante con menor grado como polinomio en b. Sea R el conjunto de estos representantes y m el mayor grado de los polinomios en b representados en R. Como b^{m+1} está en T se tiene que $b^{m+1} = p(b)$ donde $p(b)$ está en B. Esto es, b satisface la relación dada por el polinomio mónico $x^{m+1} - p(x)$. ■

Definición 4.2.1. *Sean $f, g \in A[x]$ dos polinomios sobre el anillo A.*

1. *Diremos que f es nilpotente si existe un entero n con $f^n = 0$.*
2. *f es una unidad si existe $g \in A[x]$ tal que $fg = 1$.*
3. *f es regular si f no es un divisor de 0.*
4. *f es primo si el ideal $\langle f \rangle$ es un ideal primo propio.*
5. *f es ireducible si no es una unidad y si $f = gh$ implica que, bien g es una unidad o bien h lo es.*
6. *f es primario si el ideal $\langle f \rangle$ es un ideal primario.*
7. *f y g están asociados si $\langle f \rangle = \langle g \rangle$.*
8. *f y g son coprimos so $\langle f \rangle + \langle g \rangle = A[x]$.*

El siguiente teorema es una consecuencia directa de las propiedades que se transmiten mediante el homomorfismo μ y su demostración se deja como ejercicio al lector.

Teorema 4.2.2. *Consideremos el polinomio*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x].$$

1. *Los siguientes enunciados son equivalentes:*
   a) *f es una unidad,*
   b) *$\mu(f)$ es una unidad,*
   c) *a_0 es una unidad y $a_1, \ldots, a_n$ son nilpotentes.*
2. *Los siguientes enunciados son equivalentes:*
   a) *f es un polinomio nilpotente,*
   b) *$\mu(f) = 0$,*
   c) *$a_1, \ldots, a_n$ son nilpotentes,*
   d) *f es un divisor de 0,*
   e) *existe un elemento no nulo $a \in A$ con $af = 0$.*
3. *Los siguientes enunciados son equivalentes:*
   a) *f es un polinomio regular,*
   b) *$\langle a_1, \ldots, a_n \rangle = A$,*
   c) *existe un índice i, $0 \leq i \leq n$ tal que a_i es una unidad,*
   d) *$\mu(f) \neq 0$.*

Definición 4.2.2. *Sea $\mathfrak{a}$ un ideal del anillo A, denotaremos por $\mathfrak{a}[x]$ al conjunto de polinomios de $A[x]$ dados por*

$$\mathfrak{a}[x] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x] \mid a_i \in \mathfrak{a},\ i = 1, \ldots, n\}.$$

El siguiente teorema nos muestra una caracterización del radical del anillo de polinomios $A[x]$.

Teorema 4.2.3. *Sea $\mathfrak{m}$ el ideal maximal del anillo A. Entonces se tiene que*

1. *Nilradical de $A[x]$.*

$$\mathfrak{m}[x] = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } A[x]\}.$$

2. *Radical de Jacobson de* $A[x]$.

$$\mathfrak{m}[x] = \{f \mid gf + 1 \text{ es una unidad para todo } g \in A[x]\}.$$

Llamaremos a $\mathfrak{m}[x]$ *el radical de* $A[x]$ *y lo denotaremos por* $\mathrm{Rad}(A[x])$.

Demostración. Para demostrar la primera parte simplemente hay que tener en cuenta que

$$\bigcap\{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } A[x]\} = \{f \in A[x] \mid f \text{ es nilpotente}\}.$$

Utilizando la caracterización de nilpotencia en el Teorema 4.2.2 se sigue el resultado.
Para demostrar la segunda parte, como la suma de un elemento nilpotente y una unidad es una unidad tenemos la siguiente contención

$$\mathfrak{m}[x] \subseteq \{f \mid gf + 1 \text{ es una unidad para todo } g \in A[x]\} = J.$$

Por otra parte, si $f \in J$ con $f = a_0 + a_1x + \cdots + a_nx^n$, entonces $xf + 1$ es una unidad y por el Teorema 4.2.2 $a_1, \ldots, a_n$ son nilpotentes y por lo tanto están en $\mathfrak{m}$. ■

Definición 4.2.3. *Sean* f, g *dos polinomios en el anillo* $A[x]$. *Diremos que* f *es un divisor de* g *si* $\langle g\rangle \subset \langle f\rangle$. *Diremos que es un divisor propio si la contención es extricta.*

En el caso de que g sea un polinomio regular se puede comprobar de forma fácil que f es un divisor propio de g si y sólo si $\mu(f)$ lo es de $\mu(g)$.

Teorema 4.2.4 (Lema de Hensel)**.** *Sea* $f \in A[x]$ *un polinomio y*

$$\mu(f) = \prod_{i=1}^{n} \bar{g}_i$$

donde los polinomios $\bar{g}_i$ *con* $i = 1, 2, \ldots, n$ *son coprimos dos a dos en* $\mathbb{K}[x]$. *Entonces existen* $g_i \in A[x]$, $i = 1, 2, \ldots, n$ *tales que:*

1. g_i, $i = 1, 2, \ldots, n$ *son coprimos dos a dos,*

2. $\mu(g_i) = \bar{g}_i$ *para* $i = 1, 2, \ldots, n$ *y*

3. $f = \prod_{i=1}^{n} g_i$.

Demostración. Procederemos por inucción a partir del caso $n = 2$. Consideremos

$$f = h_1 h_2 + v$$

donde $\mu(h_i) = \bar{g}_i$ para $i = 1, 2$ y $v \in \mathfrak{m}[x]$. Como $\bar{g}_1$ y $\bar{g}_2$ son coprimos si y sólo si lo son h_1 y h_2 entonces existen $\lambda_1, \lambda_2 \in A[x]$ tales que $1 = \lambda_1 h_1 + \lambda_2 h_2$. Tomemos ahora los siguientes polinomios

$$h_{11} = h_1 + \lambda_2 v, \qquad h_{21} = h_2 + \lambda_1 v$$

se tiene que

$$h_{11} h_{21} = f + \lambda_1 \lambda_2 v^2.$$

Por lo tanto $f \equiv h_{11} h_{21} \mod (v^2)$ y además $\mu(h_{i1}) = \mu(h_i)$ para $i = 1, 2$. Además h_{11}, h_{21} son coprimos luego podemos repetir el argumento. Tenemos por lo tanto que para cada positivo s podemos construir dos polinomios h_{1s}, h_{2s} tales que

$$f \equiv h_{1s} h_{2s} \mod (v^s), \qquad \mu(h_{is)} = \mu(h_i) \text{ para } i = 1, 2.$$

Como $v \in \mathfrak{m}[x]$ es nilpotente podemos tomar un s' adecuado de forma que $f = h_{1s'} h_{2s'}$ con lo que se concluye el caso $n = 2$.
El resultado se sigue ahora del hecho que si h_1 es coprimo con h_i para $i = 2, 3, \ldots, n$, entonces h_1 y $\prod_{i=2}^{n} h_i$ también son coprimos. ∎

Lema 4.2.1. *Si f es un polinomio regular en el anillo $A[x]$ existen polinomios mónicos $f_i \in A[x]$, $i = 1, 2, \ldots$ tales que*

$$\mathrm{gr}(f_i) = \mathrm{gr}(\mu(f)), \quad f_i \equiv f_{i+1} \mod \mathfrak{m}^j$$

y existen $g_i \in \mathfrak{m}[x]$ y una unidad $b_i \in A$ tales que

$$b_i f \equiv f_i + g_i f_i \mod \mathfrak{m}^j$$

Demostración. Consideremos

$$f = a_0 + a_1 x + \cdots + a_n x^n \text{ con } a_n \neq 0 \text{ y } \mathrm{gr}(\mu(f)) = t \leq n.$$

Entonces a_t es una unidad, tomemos

$$f_1 = a_t^{-1} f \text{ y } g_1 = 0$$

y procedamos por inducción.
Supongamos que $f_1, f_2, \ldots, f_j$ satisfacen el enunciado del lema, por lo tanto $b_j f \equiv f_j + g_j f_j + h$ con $h \in \mathfrak{m}^j[x]$. El polinomio f_j es mónico y podemos tomar $q, r \in A[x]$ tales que $h = qf_j + r$ con $\mathrm{gr}(r) < \mathrm{gr}(f_j) = \mathrm{gr}(\mu(f))$ o $r = 0$. Definamos ahora

$$f_{j+1} = f_j + r \text{ y } g_{j+1} = g_j + q.$$

Si $r = 0$ es claro que $g_{j+1} \in \mathfrak{m}[x]$ y que $r \in \mathfrak{m}^j[x]$. Veamos que también es cierto en el resto de los casos. Supongamos que

$$f_j = b_0 + b_1 x + \cdots + b_{t-1}x^{t-1} + x^t \quad \text{y} \quad q = c_0 + c_1 x + \cdots + c_s x^s.$$

El coeficiente correspondiente a x^{t+s} en el producto qf_j es c_s, el correspondiente a x^{t+s-1} es $c_s b_{t-1} + c_{s-1}$ etc. Como $h \equiv 0$ y $\mathrm{gr}(r) < \mathrm{gr}(f_j) = t$ es fácil ver que c_s, $c_{s-1}, \ldots$ pertenecen a $\mathfrak{m}^j$ y por lo tanto $q \in \mathfrak{m}^j[x]$, de donde $r = h - qf_j \in \mathfrak{m}^j[x]$ y se tiene:

$$\begin{aligned} b_j f = f_j + g_i f_j + h &= (f_j + r) + (g_j + q)(f_j + r) - rg_j - rq \\ &\equiv f_{j+1} + g_{j+1} f_{j+1} \quad \text{mód } \mathfrak{m}^{j+1}. \end{aligned}$$

■

Utilizando el lema anterior podemos demostrar que cada polinomio regular posee un representante mónico único.

Teorema 4.2.5. *Si f es un polinomio regular de $A[x]$ entonces existe un unico polinomio mónico $f^\star$ tal que $\mu(f) = \mu(f^\star)$ y tal que si $a \in A$ entonces $f(a) = 0$ si y sólo si $f^\star(a) = 0$. Además existe una unidad $v \in A$ tal que $vf = f^\star$.*

Demostración. Supongamos que el índice de nilpotencia de $\mathfrak{m}$ es β. Por el Lema 4.2.1 tenemos

$$b_\beta f = f_\beta + g_\beta f_\beta = (1 + g_\beta) f$$

con f_β polinomio mónico, b_β y $1 + g_\beta$ unidades puesto que $g_\beta \in \mathfrak{m}[x]$. Por lo tanto con la elección $f^\star = f_\beta$ tenemos el resultado. ■

Denotaremos por J el conjunto de todos los polinomios en $A[x]$ tales que $\mu(f)$ tiene raíces distintas en la clausura algebraica de $\mathbb{K}$. El siguiente teorema caracteriza los polinomios regulares irreducibles de $A[x]$.

Teorema 4.2.6 (Polinomios regulares irreducibles)**.** *Sea $f \in A[x]$ un polinomio regular. Entonces*

1. *Si $\mu(f)$ es irreducible en $\mathbb{K}[x]$ entonces f también lo es.*
2. *Si f es un polinomio irreducible entonces $\mu(f) = \delta g^n$ con $\delta \in \mathbb{K}$ y g un polinomio mónico irreducible de $\mathbb{K}[x]$.*
3. *Si f pertenece al conjunto J entonces f es irreducible si y sólo si lo es $\mu(f)$.*

Demostración. Supongamos que $\mu(f)$ es irreducible, entonces si $f = gh$ o bien $\mu(g)$ o $\mu(h)$ es una unidad en $\mathbb{K}[x]$ ya que $\mu(f)$ es primo (irreducible). Considerando el Teorema 4.2.2 tenemos entonces que o bien g o bien h es una unidad y entonces f es irreducible.
Por otro lado, si $f \in A[x]$ es irreducible, supongamos que

$$\mu(f) = \delta g_1^{e_1} g_2^{e_2} \dots g_t^{e_t}$$

con δ una unidad y $g_i \in \mathbb{K}[x]$ polinomios mónicos irreducibles para $i = 1, 2, \dots, t$ coprimos entre sí. Por lo tanto, excepto en el caso $t = 1$, por el lema de Hensel (Teorema 4.2.4) f factoriza de forma no trivial. Esto es, si f es irreducible entonces $\mu(f) = \delta g^n$. ■

Nótese que un polinomio primo del anillo $A[x]$ es irreducible, sin embargo un polinomio irreducible del mismo anillo no tiene por qué ser primo. Esta es una característica que distingue a los cuerpos finitos tratados en el Capítulo 2 de los anillos locales finitos (por ejemplo los anillos de Galois en el Capítulo 3).

Lema 4.2.2. *Consideremos f un polinomio en $A[x]$ regular irreducible que esté contenido en el conjunto J. Entonces f es primo si y sólo si $\mathfrak{m} \subseteq \langle f \rangle$ donde $\mathfrak{m}$ es el ideal maximal del anillo A.*

Demostración. Si f es primo $A[x]/\langle f \rangle$ es un cuerpo finito. Sea $a \in \mathfrak{m}$, la clase de equivalencia $a + \langle f \rangle$ es nilpotente en el cuerpo, esto es $a \in \langle f \rangle$.

Por otra parte, en el caso de que $\mathfrak{m} \subseteq \langle f \rangle$, tenemos que $\mathfrak{m}[x] \subseteq \langle f \rangle$. Supongamos que la clase de equivalencia $g + \langle f \rangle$ es nilpotente en el cociente $A[x]/\langle f \rangle$, entonces el polinomio f debe dividir a g^n para algún índice n y por lo tanto $\mu(f)$ debe dividir a $\mu(g)^n$. Como f pertenece a J se sigue que $\mu(f)$ debe dividir a $\mu(g)$,

$$\mu(f) = \bar{h}\mu(g).$$

Tomemos $h \in A[x]$ tal que $\mu(h) = \bar{h}$. $hf = g + j$ con $j \in \mathfrak{m}[x]$, de donde $g \in \langle f \rangle$ y el cociente $A[x]/\langle f \rangle$ es un cuerpo. ■

Teorema 4.2.7 (Caracterización de los cuerpos finitos)**.** *Sea A un anillo conmutativo finito y local. Los siguientes enunciados son equivalentes:*

1. *A es un cuerpo finito.*
2. *Cada polinomio de $A[x]$ irreducible y regular es también primo.*
3. *Existe al menos un polinomio irreducible y regular en el conjunto J que es primo.*

Demostración. Es claro que las implicaciones descendentes $1. \Rightarrow 2. \Rightarrow 3.$ se cumplen. Mostraremos ahora $3. \Rightarrow 1.$ Supongamos que A no sea un cuerpo y tomemos un polinomio $f \in J$ irreducible y regular. Tomemos un elemento no nulo del ideal maximal $0 \neq a \in \mathfrak{m}$. El ideal $\langle f \rangle$ no puede contener al elemento a pues f es regular y por la comparación de sus grados. Por lo tanto $\mathfrak{m} \not\subset \langle f \rangle$ y f no es primo aplicando el Lema 4.2.2. ■

4.2.1. Factorización en $A[x]$

En esta sección mostraremos la factorización de un elemento regular del anillo $A[x]$. Recuérdese que A denota un anillo conmutativo finito y local con ideal maximal $\mathfrak{m}$. También hay que recordar que en general, para un anillo local A, el anillo de polinomios $A[x]$ no es un anillo de factorización única, por ejemplo en $\mathbb{Z}_{p^2}[x]$ tenemos que $x^2 = x \cdot x = (x - p) \cdot (x + p)$.

Teorema 4.2.8 (Factorización)**.** *Consideremos un polinomio regular en el anillo $A[x]$.*

1. $$f = \delta \prod_{i=1}^{n} g_i,$$

   donde δ es una unidad y g_i con $i = 1, 2, \ldots, n$ son polinomios regulares primarios coprimos entre sí.

2. *Si*
   $$f = \delta \prod_{i=1}^{n} g_i = \delta' \prod_{j=1}^{n'} h_j,$$

   donde δ, δ' son unidades y g_i con $i = 1, 2, \ldots, n$, h_j con $j = 1, 2, \ldots, n'$, son polinomios regulares primarios coprimos entre sí dentro de cada serie. Entonces $n = n'$ y tras un posible reordenamiento $\langle g_i \rangle = \langle h_i \rangle$ para $i = 1, 2, \ldots, n$.

Demostración. Al ser f regular en $A[x]$ es no nulo y por lo tanto

$$\mu(f) = \bar{\delta} \prod_{i=1}^{n} \bar{\pi}_i^{n_i}$$

con $\bar{\delta}$ un elemento no nulo de $\mathbb{K}$ y $\bar{\pi}_i \in \mathbb{K}[x]$ $i = 1, 2, \ldots, n$ polinomios irreducibles y coprimos entre sí. Utilizando el lema de Hensel (Teorema 4.2.4) tenemos que

$$f = \delta \prod_{i=1}^{n} \pi_i$$

con $\mu(\delta) = \bar{\delta}$ y $\mu(\pi_i) = \bar{\pi}_i$ para $i = 1, 2, \ldots, n$. Es fácil comprobar que dichos polinomios π_i son regulares primarios y coprimos entre sí. La segunda propiedad se sigue de la igualdad

$$\langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle = \langle h_1 \rangle \langle h_2 \rangle \cdots \langle h_{n'} \rangle$$

y de que cada uno de los ideales principales en la ecuación anterior son primarios y coprimos. ■

Definición 4.2.4. *Diremos que un polinomio irreducible $\pi \in A[x]$ es básico irreducible si $\mu(\pi)$ es irreducible en $\mathbb{K}[x]$.*

De toda la discusión anterior se sigue fácilmente el siguiente resultado.

Proposición 4.2.1. *Un polinomio $f \in A[x]$ es primario, regular no unidad si y sólo si es de la forma*

$$f = \delta\pi^n + \beta$$

donde δ es una unidad, π es un polinomio básico irreducible, n es un entero positivo y β pertenece al ideal $\mathfrak{m}[x]$.

4.2.2. Raíces de un polinomio

Como en las secciones anteriores A denota un anillo conmutativo finito y local con ideal maximal $\mathfrak{m}$ y $\mathbb{K} = A/\mathfrak{m}$ es su cuerpo de residuos. Sea β el índice de nilpotencia del ideal maximal $\mathfrak{m}$ y consideremos la siguente cadena de homomorfismos de anillos

$$A = A/\mathfrak{m}^\beta \xrightarrow{\sigma_\beta} A/\mathfrak{m}^{\beta-1} \xrightarrow{\sigma_{\beta-1}} \cdots \xrightarrow{\sigma_1} \mathbb{K} = A/\mathfrak{m} \xrightarrow{\sigma_0} 0. \tag{4.4}$$

Además para cáda índice $i = 0, 1, \ldots, \beta$ consideraremos el homomorfismo de anillos dado por

$$\mu_i : R/\mathfrak{m}^i \longrightarrow \mathbb{K}.$$

El nucleo de cada uno de los homomorfismos σ_β es $\mathfrak{m}^{i-1}/\mathfrak{m}^i$. Nótese que $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ está dotado de una estructura de $\mathbb{K}$-espacio vectorial con la multiplicación $\star$ por escalares dada como sigue: $\bar{\alpha} \star m = \alpha m$ donde $m \in \mathfrak{m}^{i-1}/\mathfrak{m}^i$ y $\mu_i(\alpha) = \bar{\alpha}$.
La construcción que realizaremos pretende, a partir de las soluciones en $A/\mathfrak{m}^{i-1}[x]$, "levantarlas" a soluciones en el anillo $A/\mathfrak{m}^i[x]$. Para ello sea t la dimensión como $\mathbb{K}$-espacio vectorial de $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ y consideremos una base del mismo $\mathcal{B} = \{v_1, v_2, \ldots, v_t\}$.
Dado $\bar{s}_i$ un cero en $A/\mathfrak{m}^{i-1}$ del polinomio $\sigma_i(f)$ supongamos que $\sigma_i(s_i) = \bar{s}_i$. Tomemos $s = s_i + \eta$ con $\eta \in \mathfrak{m}^{i-1}/\mathfrak{m}^i$. Tenemos que conseguir un η adecuado tal que $f(s) = 0$ en $A/\mathfrak{m}^i$.
Primero observamos que $(\mathfrak{m}^{i-1}/\mathfrak{m}^i)^2 = 0$, por lo tanto

$$\begin{aligned} f(s) = f(s_i + \eta) &= f(s) + \eta f'(s_i) + \eta^2 \cdot (\text{otros términos en } A/\mathfrak{m}^i) \\ &= f(s_i) + \eta f'(s_i) \end{aligned}$$

donde f es la derivada formal de f'. La condición $f(s) = 0$ implica que

$$f(s_i) = -\eta f'(s_i) = -\mu_i(f'(s_i))\eta,$$

pues $\eta \in \mathfrak{m}^{i-1}/\mathfrak{m}^i$. También $f(s_i) \in \mathfrak{m}^{i-1}/\mathfrak{m}^i$ pues $\sigma_i(f(\bar{s}_i)) = 0$. Calculemos todo ahora relativo a la base $\mathcal{B}$.

$$f(s_i) = \sum_{i=1}^{t} b_i v_i, \quad -\eta = \sum_{i=1}^{t} a_i v_i, \qquad a_i, b_i \in \mathbb{K}.$$

$$\begin{aligned} 0 &= \sum_{i=1}^{t} b_i v_i + \mu_i(f'(s_i)) \left(\sum_{i=1}^{t} a_i v_i \right) \\ &= \sum_{i=1}^{t} \left(b_i + \mu_i(f'(s_i)) a_i \right) v_i. \end{aligned}$$

Nótese que queremos calcular los coeficientes a_i y que para cada $i = 1, 2, \ldots, t$ tenemos

$$b_i + \mu_i(f'(s_i))a_i = 0.$$

Hay tres posibles casos:

1. Si $f'(s_i)$ es una unidad entonces $\mu_i(f'(s_i)) \neq 0$ y por lo tanto los a_i están determinados de forma única y existe una única solución.

2. Si $f'(s_i) \in \mathfrak{m}/\mathfrak{m}^i$ y existe al menos un $b_j \neq 0$. En este caso no hay solución.

3. Si $f'(s_i) \in \mathfrak{m}/\mathfrak{m}^i$ y $b_i = 0$ para todo $i = 1, 2, \ldots, t$. En este caso $f(s_i) = 0$ para todo s_i tal que $\sigma_i(s_i) = \bar{s}_i$. Esto es esisten $|\mathbb{K}|^t$ soluciones (cualquier elección para los a_i es posible).

Con este procedimiento logramos todos los ceros de f pues el primer paso en la cadena de homomorfismos en (4.4) se reduce a encontrar las soluciones en $\mathbb{K}$.

4.3. Estructura de los anillos locales

Teorema 4.3.1 (Estructura de los anillos locales)**.** *Sea A un anillo conmutativo local con característica p^n, ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$. Sea $r = [\mathbb{K} : \mathbb{F}_p]$ y $\{m_1, m_2, \ldots, m_t\} \subset \mathfrak{m}$ un sistema de generadores minimal de $\mathfrak{m}$. Entonces existe un subanillo C de A tal que*

1. *$C \simeq GR(p^{nr}, p^n)$ es único y es la mayor extensión de Galois de $\mathbb{Z}_{p^n}$ en A.*
2. *A es una imagen mediante un homomorfismo de anillos del anillo de polinomios $C[x_1, x_2, \ldots, x_t]$.*

El anillo de Galois C se denomina anillo de coeficientes de A.

Demostración. Sea $\bar{a}$ un generador del grupo de unidades del cuerpo $\mathbb{K}$ y consideremos el polinomio irreducible $\bar{f} = \mathrm{Irr}(\bar{a}, \mathbb{F}_p) \in \mathbb{F}_p[x]$. Tomemos un polinomio $f \in \mathbb{Z}_{p^n}[x]$ preimagen de $\bar{f}$ con $\mu(f) = \bar{f}$, $a \in A$ con $\mu(a) = \bar{a}$ y $f(a) = 0$ (Ver analogías entre polinomios irreducibles y polinomios de Galois en el Capítulo 3). Claramente

$$C = \mathbb{Z}_{p^n}[a] \simeq \mathbb{Z}_{p^n}[x]/\langle f \rangle$$

es el único anillo de Galois con dichas propiedades y, además, la mayor extensión de $\mathbb{Z}_{p^n}$ contenida en A.
Es claro que $C[m_1, m_2, \ldots, m_t] \subseteq A$. Tomemos ahora un $c \in A$, existe un $b \in C$ tal que

$$c \equiv b \mod \mathfrak{m}$$

pues C se proyecta sobreyectivamente mediante μ también en $\mathbb{K}$. Construiremos una sucesión

$$\{c_j\}_{j=1}^{\beta-1} \subset C[m_1, m_2, \ldots, m_t]$$

con β el índice de nilpotencia del ideal $\mathfrak{m}$ tal que

$$c \equiv c_j \mod \mathfrak{m}^{j+1} \qquad \text{y } c_j \in C[m_1, \ldots, m_t].$$

Tomemos $c_0 = b$ y supongamos que hemos calculado hasta c_j con $j \geq 1$.

$$c_j = c - \sum d_i w_i, \qquad d_i \in A$$

con w_i un producto de potencias de los elementos en $\{m_1, m_2, \ldots, m_t\}$. Existe un $b_i \in C$ con $b_i \equiv d_i \mod \mathfrak{m}$. Esto es

$$c - c_j \equiv \sum b_i w_i \mod \mathfrak{m}^{j+2}.$$

Si tomamos $c_{j+1} = c_j + \sum b_i w_i$, como $\mathfrak{m}^\beta = 0$ entonces $c = c_{\beta-1}$ y $c \in C[m_1, m_2, \ldots, m_t]$. ∎

Por lo tanto un anillo local A es de la forma

$$C[x_1, x_2, \ldots, x_t]/\mathfrak{q}$$

donde C es un anillo de Galois y $\mathfrak{q}$ es un ideal primario con $\mathfrak{q} \cap C = \{0\}$. Además el radical de $\mathfrak{q}$ es $\langle p, x_1, x_2, \ldots, x_t \rangle$ y finalmente como C es una imagen mediante un homomorfismo de $\mathbb{Z}_{p^n}$ podemos concluir que cualquier anillo local es una imagen, mediante un homomorfismo de anillos de $\mathbb{Z}_{p^n}[x_1, x_2, \ldots, x_t, x_{t+1}]$.

Teorema 4.3.2. *Sea A un anillo local conmutativo con característica p^n. Si el conjunto $\{a_1, a_2, \ldots, a_s\}$ son generadores del grupo de unidades de A entonces el anillo A es una imagen mediante un homomorfismo de anillos del anillo de polinomios $\mathbb{Z}_{p^n}[x_1, x_2, \ldots, x_s]$.*

Demostración. Claramente $\mathbb{Z}_{p^n}[a_1, a_2, \ldots, a_s]$ es un subanillo de A que contiene todas las unidades de A. Si m es un elemento del ideal maximal $\mathfrak{m}$ entonces $c = m - b$ es una unidad para cada unidad b. Por lo tanto $\mathfrak{m} \subset \mathbb{Z}_{p^n}[a_1, a_2, \ldots, a_s]$ con lo que concluimos la prueba. ∎

4.4. Anillos de cadena

Definición 4.4.1. *Un anillo de cadena es un un anillo local conmutativo con todos su ideales propios principales.*

Consideremos la situación del Teorema 4.3.1 para un anillo A principal local con característica p^n ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$ y anillo de coeficientes el anillo de Galois $C = GR(p^{rn}, p^n)$.
Si tomamos un elemento $\theta \in \mathfrak{m} \setminus \mathfrak{m}^2$ entonces $\langle \theta \rangle = \mathfrak{m}$ y cada ideal de A es de la forma $\langle \theta^i \rangle$ para $i = 1, 2, \ldots, \beta - 1$ donde β es el índice de nilpotencia de $\mathfrak{m}$. Es siguiente resultado se sigue de forma inmediata.

Lema 4.4.1. *Sea A un anillo de cadena, cualquier elemento de A es de la forma $u\theta^i$ con i único y la unidad u está unívocamente determinada módulo el ideal $\langle\theta^{\beta-i}\rangle$.*

Corolario 4.4.1. *Si $1 \leq i < j \leq \beta$ y $\theta^i c \in \langle\theta^j\rangle$ entonces $c \in \langle\theta^{j-i}\rangle$. En particular, si $\langle\theta^i\rangle \neq 0$ entonces $c \in \langle\theta^{\beta-i}\rangle$.*

Lema 4.4.2. *Sea A un anillo de cadena y sea $V \subseteq A$ un conjunto de representantes de las clases de equivalencia de $A/\langle\theta\rangle$. Entonces:*

1. *Para cada $a \in A$ existen elementos únicos $a_0, \ldots, a_{\beta-1} \in V$ tales que*
$$a = \sum_{i=0}^{\beta-1} a_i \cdot \theta^i.$$
2. *$|V| = |A/\mathfrak{m}|$.*
3. *$|\langle\theta^j\rangle| = |A/\mathfrak{m}|^{\beta-j}$ con $0 \leq j \leq \beta - 1$.*

Demostración.

1. Construyamos $a_0, \ldots, a_{\beta-1} \in V$ de forma inductiva. Consideremos a_0 el único elemento con $\mu(a_0) = \mu(a)$. supongamos que hemos construido hasta a_j, tomemos entonces
$$a - \sum_{i=0}^{j} a_i \cdot \theta^i = v_{j+1}\theta^{j+1}$$
para algún elemento $v_{j+1} \in A$. Tomaremos como a_{j+1} al elemento de V tal que $\mu(a_{j+1}) = \mu(v_{j+1})$. Es claro que
$$a \equiv \sum_{i=0}^{j+1} a_i \cdot \theta^i \mod \theta^{j+2}.$$
Para demostrar la unicidad consideremos
$$a = \sum_{i=0}^{\beta-1} a_i \cdot \theta^i = \sum_{i=0}^{\beta-1} b_i \cdot \theta^i$$

con $a_i, b_i \in V$ para $i = 0, 1, \ldots, \beta - 1$. Es decir,

$$\sum_{i=0}^{\beta-1}(a_i - b_i) \cdot \theta^i = 0$$

y aplicando repetidamente el Corolario 4.4.1 tenemos que $\mu(a_i) = \mu(b_i)$ para $i = 0, 1, \ldots, \beta-1$, lo que implica $a_i = b_i$ pues pertenecen a V.

2. Es una consecuencia directa del hecho que V es un conjunto maximal de A con la propiedad $\mu(a_1) \neq \mu(a_2)$ para todo par $a_1, a_2 \in A$ tal que $a_1 \neq a_2$.

3. Simplemente notar que hay $|V|$ posibilidades para cada coeficiente a_i y $a \in \langle \theta^j \rangle$ si y sólo si $a_0 = \cdots = a_{j-1} = 0$.

■

Lema 4.4.3. *Con la notación anterior existen enteros positivos s y t tales que:*

1. $A = C \oplus C\theta \oplus \cdots \oplus C\theta^{s-1}$ *como C-módulos.*

2. $\theta^s = p(a_{s-1}\theta^{s-1} + \cdots + a_1\theta + a_0)$ *donde $a_i \in C$ para $i = 1, 2, \ldots, s-1$ y a_0 es una unidad.*

3. *Como C-módulos*

$$C\theta^i \simeq C, \quad 1 \leq i \leq t-1$$
$$C\theta^i \simeq Cp, \quad t \leq i \leq s-1.$$

4.
$$\beta = (n-1)s + t, \qquad 1 \leq t \leq s.$$

Además si $n = 1$ se tiene que $s = t = \beta$.

Demostración. El elemento p se encuentra en el ideal $\mathfrak{m}$, por lo tanto esiste un entero s tal que $p = v\theta^s$ con v una unidad. Por lo tanto $v^{-1}p = \theta^s$ y entonces $\theta^{s(n-1)} \neq 0$ y $\theta^{sn} = 0$. Por lo tanto existe un entero no negativo t con $1 \leq t \leq s$ tal que

$$\beta = s(n-1) + t.$$

En el caso $n = 1$ en el anillo A el elemento $p = 0$ y tomamos $t = s = \beta$. Considerando el razonamiento en la demostración del Teorema 4.3.1 se sigue que

$$\begin{aligned} A &= C[\theta] \\ &= C + C\theta + C\theta^2 + \cdots + C\theta^{\beta-1} \\ &= (C + C\theta + C\theta^2 + \cdots + C\theta^{s-1}) + Ap \\ &= C + C\theta + C\theta^2 + \cdots + C\theta^{s-1} \end{aligned}$$

por el lema de Nakayama (Proposición 1.2.2). Además $u = v^{-1} = a_{s-1}\theta^{s-1} + \cdots + a_1\theta + a_0$ con a_0 una unidad lo que prueba 2.
Para probar 1 y 2 definamos el morfismo

$$\begin{array}{rccc} \phi_j : & C & \longrightarrow & C\theta^j \\ & x & \mapsto & x\theta^j \end{array}$$

El elemento $p^{n-1}\theta^j$ es nulo si y sólo si $j \geq t$. Por lo tanto para los valores $j < t$ el núcleo del homomorfismo es $\{0\}$ y se tiene $C \simeq C\theta^j$. En el resto de los casos $t \leq j < s-1$ el núcleo del morfismo es Cp^{n-1} de donde $Cp \simeq C\theta^j$.
Finalmente para demostrar que es una suma directa probaremos que

$$|A| = \prod_{i=0}^{s-1} |C\theta^i|.$$

Como $C = GR(p^{rn}, p^n)$, tenemos que su cardinal es p^{nr} y tenemos que el cardinal de $C\theta^i$ también es p^{nr} cuando $0 \leq i < t$. Además el cardinal de Cp es $p^{(n-1)r}$ por lo que el cardinal de $C\theta^i$ es $p^{(n-1)r}$ cuando $t \leq i < s$. Observemos ahora que $A\theta^i/A\theta^{i+1}$ es un $\mathbb{K}$-espacio vectorial de dimensión 1 para $0 \leq i < \beta$ de donde

$$|A| = (p^r)^\beta = p^{nrt}p^{(n-1)r(s-t)}.$$

■

Definición 4.4.2. *Para el anillo de Galois C en el teorema anterior el polinomio*

$$g(x) = x^s + p(a_{s-1}x^{s-1} + \cdots + a_1x + a_0) \in C[x]$$

donde a_0 es una unidad se denomina polinomio de Eisenstein sobre C. El anillo $C[x]/\langle g(x)\rangle$ se denomina extensión de Eisenstein de C.

De los resultados anteriores se sigue de forma directa la siguiente caracterización de los anillos de cadena.

Teorema 4.4.1 (Caracterización de los anillos de cadena)**.** *Sea A un anillo de cadena con característica p^n ideal maximal $\mathfrak{m}$ con nilpotencia β y $r = [A/\mathfrak{m} : \mathbb{F}_p]$. Existen enteros no negativos t y s tales que $\beta = (n-1)s + t$, $1 \leq t \leq s$ y*

$$A \simeq GR(p^{rn}, p^n)[x]/\langle g(x), p^{n-1}x^t\rangle$$

y $g(x)$ es un polinomio de Eisenstein de grado s sobre $GR(p^{rn}, p^n)$. El resultado recíproco también es cierto, cualquier anillo cociente de ese tipo es un anillo de cadena.

Nótese que el polinomio de Eisenstein es de la forma $g(x) = x^s + pf(x)$ por lo que la estructura de A depende de dicho polinomio f que a su vez depende de la elección de θ el generador del ideal maximal $\mathfrak{m}$, en otras palabras, f no es canónico.
En la demostración del Lema 4.4.3 sabemos que $p = v\theta^s$ donde v es una unidad de A. El polinomio $x^s - \mu(v)$ tiene un cero simple $\bar{\rho}$ en $\mathbb{K}$ si $(s, p) = 1$. Se puede probar que en dichas condiciones $x^s - v$ tiene un cero en A. Por lo tanto $p = (\rho\theta)^s$. Además ρ es una unidad pues lo es v y se tiene que $\langle\theta\rangle = \langle\rho\theta\rangle$ y si tomamos $\theta_1 = \rho\theta$ como el generador del ideal maximal $\mathfrak{m}$ el polinomio de Eisenstein es $g(x) = x^s + p$.
Con la discusión anterior hemos probado que

Corolario 4.4.2. *En las condiciones del teorema anterior, si $(p, s) = 1$ se tiene que*

$$A \simeq GR(p^{rn}, p^n)[x]/\langle x^s + p, p^{n-1}x^t\rangle$$

En este caso el anillo A se denomina *anillo de cadena puro.*

4.4.1. Factorización de polinomios en anillos de cadena

Diremos que un polinomio $f \in A[x]$ con A un anillo de cadena es *libre de cuadrados* si $g^2|f$ implica que g es una unidad.

Proposición 4.4.1. *Si $g \in A[x]$ con A un anillo de cadena y $\mu(g)$ es libre de cuadrados entonces g factoriza de forma única como un producto de polinomios mónicos básicos irreducibles coprimos entre sí.*

Demostración. Por el Teorema 4.2.8 sabemos que g factoriza como un producto de $g_1, \ldots, g_k$ polinomios mónicos y primos dos a dos que generan un ideal primario. Como $\mu(g)$ es libre de cuadrados también lo son los polinomios $\mu(g_i)$. Entonces teniendo en cuenta la Proposición 4.2.1 $g_i = h_i + v_i$ con h_i básico irreducible y $v_i \in \langle\theta\rangle[x]$, por lo que $\mu(g_i)$ es irreducible y por lo tanto lo es g_i. ■

Lema 4.4.4. *Sean $f, g \in A[x]$ con A un anillo de cadena. Los polinomios f, g son coprimos entre sí si y sólo si $\mu(f), \mu(g)$ son coprimos.*

Demostración. Sea I el ideal generado por f, g en $A[x]$ y I' el ideal generado por $\mu(f), \mu(g)$. Es fácil probar que $\mu(I) = I'$ y como $h \in A[x]$ es una unidad si y sólo si lo es $\mu(h)$ entonces I contiene una unidad si y sólo si la contiene I'. ■

El lema anterior se puede probar también de forma constructiva, es decir, dados f, g en $A[x]$ construir $u, v \in \mathbb{K}[x]$ tales que $u\mu(f) + v\mu(g) = 1$ y con una técnica similar al levantamiento de Hensel construir u_1, v_1 con $u_1 f + v_1 g = 1$. El lector interesado en esta construción puede consultar el texto [2].

Capítulo 5

Códigos correctores de errores

En este capítulo mostraremos una de las aplicaciones más conocidas de los anillos finitos: los códigos correctores de errores. La extensión de este manual no nos permite abarcar con suficiente intensidad la teoría de la codificación algebraica y por lo tanto los contenidos son claramente sesgados. Hemos eliminado conscientemente cualquier alusión a la descodificación de los mismos a pesar de ser un punto clave en su diseño y concepción salvo una breve alusión a la descodificación por síndrome. En nuestra descarga podemos aludir que ya existe un volumen de la presente colección que trata dicho problema y los códigos correctores sobre cuerpos y su descodificación con mayor extensión [12]. Gran parte de la introducción que se presenta a los códigos lineales sobre cuerpos finitos está extraída de dicho manual. Para el lector más interesado recomendamos [2] por su relación con la temática de este volumen, también el texto ya clásico pero siempre importante manual de McWilliams Sloane [5] o [3].

5.1. La información y los errores

5.1.1. La información digital

La información digital se caracteriza por presentarse en un formato discreto, esto es, como una secuencia finita $m = x_1 x_2 \cdots \in \mathcal{A}^*$ de símbolos de un alfabeto finito $\mathcal{A}$. Un texto escrito (este libro) es un buen ejemplo

de información digital. Por conveniencia, el alfabeto $\mathcal{A}$ suele identificarse con algún sistema numérico y muy a menudo con $\{0, 1\}$, conjunto que interpretaremos como el cuerpo finito $\mathbb{F}_2$. De manera análoga, si $\mathcal{A}$ contiene q elementos y q es la potencia de un número primo, entonces $\mathcal{A}$ se identifica con el cuerpo finito con q elementos $\mathbb{F}_q$. Esta identificación permite aplicar a los problemas de codificación todos los recursos del álgebra y la geometría sobre cuerpos finitos.
Una vez se tiene la información en el formato digital adecuado (binario o no) es apta para su manipulación o transmisión, siguiendo un esquema del tipo

Figura 5.1: Esquema de una transmisión de información.

En un sentido amplio, el canal puede ser espacial o temporal: envío por línea telefónica, óptica, almacenamiento en un disco, etc. Al recibir el mensaje, el receptor no puede estar seguro de que alguna parte del mismo haya sido corrompida durante la transmisión. Sí puede, sin embargo, conocer la frecuencia con se producen los errores y, por tanto, determinar cuantos errores (en media) cabe esperar que hayan ocurrido.
En lugar de enviar la información directamente, la transformamos (*codificamos*) añadiéndole cierta redundancia con arreglo a unas reglas sistemáticas. Es esta información codificada la que realmente se transmite por el canal (Figura 2). En base a la redundancia añadida el receptor puede detectar, y eventualmente corregir, los errores producidos y devolverla a su formato original. Este proceso recibe el nombre de *descodificación.*

5.1.2. Códigos correctores

Como hemos señalado, la información se presenta originalmente como una secuencia $m = x_1x_2 \cdots \in \mathcal{A}^*$. Fijamos dos enteros $k < n$ y troceamos m en bloques de longitud $k : m = (x_1 \cdots x_k)(x_{k+1} \cdots x_{2k}) \cdots$. Cada uno de estos bloques se codifica (y posteriormente se enviará y descodificará) independientemente de los demás, como su imagen mediante una aplicación inyectiva $c : \mathcal{A}^k \longrightarrow \mathcal{A}^n$. La codificación del mensaje completo

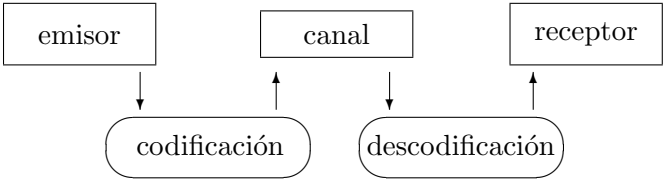

Figura 5.2: Esquema de una transmisión de información codificada.

se obtiene concatenando la codificación de los bloques que lo integran:

$$c(m) = c(x_1, \ldots, x_k)c(x_{k+1}, \ldots, x_{2k}) \cdots$$

El conjunto $\mathcal{C} = \mathrm{Im}(c)$ es, por definición, el *código* utilizado.

Definición 5.1.1. *Un* código corrector de errores *es un subconjunto $\mathcal{C} \subseteq \mathcal{A}^n$, siendo $\mathcal{A}$ un alfabeto finito y n un entero positivo. Los elementos de $\mathcal{C}$ son llamados* palabras *y n es su* longitud.

Cada palabra de $\mathcal{C}$ contiene k símbolos de información y $n-k$ símbolos redundantes: el número k/n se llama *tasa de transmisión* de $\mathcal{C}$.
Supongamos que se ha enviado una palabra $\mathbf{c} \in \mathcal{C}$ y recibido un vector $\mathbf{x} \in \mathcal{A}^n$. Si p es la probabilidad de que un símbolo resulte alterado en la transmisión, podemos esperar una media de np símbolos erróneos en $\mathbf{x}$. La capacidad de corrección de errores de $\mathcal{C}$ debe superar al menos esa cota. Cuando $\mathbf{x} \notin \mathcal{C}$, ciertamente ha habido errores; de hecho, aún en el caso de que $\mathbf{x} \in \mathcal{C}$, nunca podremos estar realmente seguros de que no hayan existido errores. Ahora bien, si el código se ha diseñado correctamente, sus palabras serán muy 'diferentes' unas de otras, de manera que resulte 'suficientemente improbable' que $\mathbf{x} \in \mathcal{C}$ a causa de los errores aleatorios sufridos en el canal.
La forma adecuada de medir la diferencia entre dos palabras (o dos vectores de $\mathcal{A}^n$) es la distancia de Hamming.

Definición 5.1.2. *Dados $\mathbf{x}, \mathbf{y} \in \mathcal{A}^n$, llamamos* distancia de Hamming *entre $\mathbf{x}$ e $\mathbf{y}$ al número de coordenadas distintas que poseen,*

$$d(\mathbf{x}, \mathbf{y}) = |\{i \mid 1 \leq i \leq n,\, x_i \neq y_i\}|.$$

Obsérvese que la función d es realmente una distancia en $\mathcal{A}^n$. El hecho de que d *no* sea invariante por cambios de base, hace que la teoría de códigos no sea una parte trivial del álgebra lineal. La capacidad de corrección de errores de $\mathcal{C}$ viene determinada por su *distancia mínima*, definida como

$$d = d(\mathcal{C}) = \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{y}\}.$$

En efecto, recibido el vector $\mathbf{x} \in \mathcal{A}^n$, se descodifica $\mathbf{x}$ por la palabra $\mathbf{c} \in \mathcal{C}$ 'más parecida' a $\mathbf{x}$, es decir, que minimiza $d(\mathbf{x}, \mathbf{c})$. Como las bolas (para la métrica de Hamming) de radio $(d-1)/2$ centradas en las palabras del código son disjuntas, si el número de errores en $\mathbf{x}$ no supera $\lfloor (d-1)/2 \rfloor$, entonces la palabra corregida coincide con la realmente enviada. Así, nuestra estrategia permite detectar $d-1$ errores y corregir $\lfloor (d-1)/2 \rfloor$ errores.

El objetivo principal (o mejor, uno de los objetivos principales) de la teoría de códigos correctores de errores es encontrar *buenos* códigos, es decir, códigos que maximicen solidariamente los parámetros k/n y d/n. Sin embargo estas demandas son mutuamente contradictorias: al aumentar uno de los parámetros, el otro tiende siempre a disminuir. En la práctica habremos de conformarnos con un cierto equilibrio entre ellos.

Otro requerimiento importante para un buen código es que posea algún método de descodificación computacionalmente efectivo. El sistema al que nos hemos referido anteriormente –evaluar la distancia de $\mathbf{x}$ a todas las palabras de $\mathcal{C}$ y quedarnos con la más cercana– es inviable en la práctica (excepto para códigos de pequeño tamaño). Relativamente pocos códigos permiten estos métodos efectivos. En el lenguaje de la Teoría de la Complejidad Computacional, el problema de descodificar un código es NP-Completo. Retomaremos el tema de los buenos códigos un poco más adelante.

5.1.3. Algunos ejemplos

Ejemplo 5.1.1 (El código ASCII)**.** En su versión habitual (no extendida), ASCII permite codificar $128 = 2^7$ símbolos (letras, números, signos y controles no imprimibles) de uso general para computadoras. A cada uno de ellos se le asigna un número de orden y se le codifica mediante la escritura binaria (con 7 bits) de ese número. Para aumentar la fiabilidad de esta codificación, a cada 7-upla $x_1, \ldots, x_7 \in \mathbb{F}_2^7$ se le añade un bit

control x_8, calculado de manera que $x_1 + \cdots + x_7 + x_8 \equiv 0 \pmod 2$. Este sistema permite detectar, aunque no corregir, cualquier número impar de errores.

Ejemplo 5.1.2 (Códigos de Hamming)**.** Los códigos de Hamming constituyen una familia doblemente infinita de códigos (para cada potencia q de un número primo existe una familia infinita de ellos). Vamos a describir con cierto detalle al más pequeño.
Deseamos codificar una 4-upla $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4$. Vamos a hacerlo añadiendo a estos cuatro bits otros tres redundantes, $c(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3,\ x_4, x_5, x_6, x_7)$. Para ello consideremos tres circunferencias cortándose en posición general, tal y como se ve en el dibujo. Estas tres circunferencias determinan 7 regiones (más la exterior no acotada). Numerémoslas.

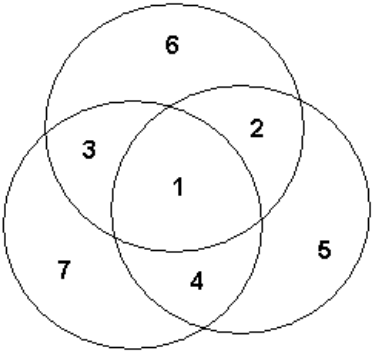

Figura 5.3: Tres circunferencias.

Colocamos cada bit x_i en la región i de la figura, $(i = 1, \ldots, 7)$. Los x_5, x_6, x_7, se calculan de manera que cada círculo contenga un número par de 1. Por ejemplo, (1010) se codifica como (1010100). El conjunto $\mathcal{C} = \{c(x_1, x_2, x_3, x_4) \ \mid (x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4\}$ se llama *código de Hamming binario de redundancia 3* y habitualmente se denota $\mathcal{H}_2(3)$.
Es un ejercicio instructivo y fácil comprobar que dos palabras cualesquiera de $\mathcal{H}_2(3)$ se diferencian en al menos tres coordenadas (es decir, que $\mathcal{H}_2(3)$ tiene distancia mínima $d = 3$) y diseñar un algoritmo de corrección de errores. Se observará que en este código (a diferencia de lo que ocurre en general) la descodificación de cualquier vector recibido

es siempre posible; será correcta cuando el vector recibido contenga un error como máximo e incorrecta en otro caso.
Ilustremos con un ejemplo como aumenta la fiabilidad de la transmisión mediante el empleo de $\mathcal{H}_2(3)$. Si, durante la transmisión, la probabilidad de error por bit es de 0,1 (suposición únicamente académica y –afortunadamente– muy poco realista), entonces un sencillo cálculo muestra que

- la probabilidad de transmisión sin error en 4 bits de información es 0,6561 sin codificar y 0,8503 codificando;
- la probabilidad de transmisión incorrecta no detectada en 4 bits de información es 0,3439 sin codificar y 0,0257 codificando.

Claro está que esta ganancia se consigue al precio de enviar un volumen de datos 7/4 veces mayor.

5.2. Códigos lineales sobre cuerpos finitos

En todo lo que sigue supondremos que el alfabeto usado $\mathcal{A}$ tiene por cardinal, q, la potencia de un número primo e identificaremos $\mathcal{A}$ con $\mathbb{F}_q$ el cuerpo finito con q elementos.
Hemos citado ya que entre los requisitos de un buen código $\mathcal{C}$ está el de poseer algoritmos eficaces de codificación y descodificación. Por lo general, esta condición pasa por que $\mathcal{C}$ posea alguna estructura algebraica. Por ejemplo, el código de Hamming ¿posee alguna estructura algebraica? No hay más que transcribir la condición de que cada uno de los tres círculos contenga un número par de 1 en términos de ecuaciones,

$$\begin{cases} x_1 + x_2 + x_3 + x_6 \equiv 0 \pmod 2 \\ x_1 + x_2 + x_4 + x_5 \equiv 0 \pmod 2 \\ x_1 + x_3 + x_4 + x_7 \equiv 0 \pmod 2. \end{cases}$$

y $\mathcal{H}_2(3)$ es un subespacio vectorial de $\mathbb{F}_2^7$. También la aplicación de codificación es lineal:

$$c(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

En general, si la aplicación de codificación $c : \mathbb{F}_q^k \to \mathbb{F}_q^n$ es lineal, decimos asimismo que el código $\mathrm{Im}(c)$ es lineal.

Definición 5.2.1. *Un* código lineal q-ario de longitud n *es un subespacio vectorial* $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Para abreviar, de un código lineal de longitud n, dimensión k y distancia mínima d, diremos que es de tipo $[n, k, d]$. Los códigos utilizados en la práctica (excepto algunos de pequeño tamaño) son siempre lineales. A continuación veremos como los procesos de codificación y descodificación, y el cálculo de la distancia mínima, son mucho más simples para los códigos lineales que para aquellos que no lo son.

5.2.1. Matriz generatriz

Todo subespacio de $\mathbb{F}_q^n$ de dimensión k puede ser interpretado como imagen de una (no única) aplicación lineal inyectiva $c : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$.

Definición 5.2.2. *Llamaremos* matriz generatriz *de* $\mathcal{C}$ *a la matriz de una aplicación lineal biyectiva* $c : \mathbb{F}_q^k \longrightarrow \mathcal{C} \subset \mathbb{F}_q^n$*, es decir, a una matriz* $k \times n$ *cuyas filas son una base de* $\mathcal{C}$.

Como una base de $\mathcal{C}$ no es única, tampoco lo es una matriz generatriz. Cualquiera de ellas, G, proporciona no solamente un código sino una codificación. En efecto, como $\mathcal{C} = \{\mathbf{a}G \mid \mathbf{a} \in \mathbb{F}_q^k\}$, (escribimos los vectores en forma de filas) un mensaje $\mathbf{a} \in \mathbb{F}_q^k$ se codifica por $\mathbf{a}G \in \mathbb{F}_q^n$. Así la codificación es para los códigos lineales de máxima simplicidad y sólo requiere el almacenamiento en memoria de la matriz G (es decir, de nk elementos de $\mathbb{F}_q$, y no de nq^k como sería el caso de un código en bloque no lineal con el mismo cardinal).
Cuando se codifica una palabra $\mathbf{a} \in \mathbb{F}_q^k$ mediante un código lineal, es a veces interesante que la palabra codificada contenga como subpalabra a $\mathbf{a}$ (podemos suponer que al comienzo de la palabra codificada), es decir sea de la forma $(\mathbf{a}, \mathbf{z})$, $\mathbf{z} \in \mathbb{F}_q^{n-k}$. Así los k primeros símbolos de la palabra contienen la información y los siguientes son de control. Este tipo de codificación es llamado *sistemático*. Evidentemente la codificación es sistemática si y sólo si la matriz G es de la forma $G = (I_k, C)$, donde I_k denota la matriz identidad $k \times k$. Esta forma de G es conocida como *forma estándar*, y el código es llamado *sistemático* si posee alguna matriz generatriz en forma estándar.

Ejemplo 5.2.1. Una matriz generatriz estándar del código de Hamming $\mathcal{H}_2(3)$ es

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Definición 5.2.3. *Diremos que dos códigos $\mathcal{C}_1, \mathcal{C}_2$, de la misma longitud, n, sobre $\mathbb{F}_q$, son* equivalentes *si existe una permutación σ del conjunto $\{1, \cdots, n\}$ tal que $\mathcal{C}_2 = \{\sigma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1\}$.*

Nota. Una permutación σ, actúa realmente sobre los índices $\{1, \cdots, n\}$ y no sobre los elementos de $\mathbb{F}_q^n$. Cuando por abuso de notación escribimos $\sigma(\mathbf{x})$, deberíamos escribir $(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$. Denotaremos por $\mathcal{S}_n$ el *grupo simétrico* de orden n, es decir, el grupo de todas las $n!$ permutaciones del conjunto $\{1, \cdots, n\}$.

Códigos equivalentes tienen los mismos parmetros k y d. Recíprocamente, dado el código $\mathcal{C}$, para cada permutación σ de $\{1, \cdots, n\}$, el conjunto

$$\sigma(\mathcal{C}) = \{\sigma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}\}$$

es un código equivalente a $\mathcal{C}$. Eventualmente puede suceder que $\sigma(\mathcal{C}) = \mathcal{C}$. De hecho podemos considerar el conjunto

$$\mathrm{Aut}(\mathcal{C}) = \{\sigma \in \mathcal{S}_n \mid \sigma(\mathcal{C}) = \mathcal{C}\}.$$

$\mathrm{Aut}(\mathcal{C})$ es un subgrupo de $\mathcal{S}_n$, llamado *grupo de automorfismos* de $\mathcal{C}$.

Proposición 5.2.1. *Todo código es equivalente a uno sistemático.*

5.2.2. Matriz de control

Un subespacio vectorial de $\mathbb{F}_q^n$ puede describirse no sólo mediante un sistema de generadores (lo que da lugar al concepto de matriz generatriz), sino también mediante unas ecuaciones implícitas. Esta forma de caracterización origina la siguiente definición.

Definición 5.2.4. *Diremos que una matriz H es una* matriz de control *del código $\mathcal{C}$ si para todo vector $\mathbf{x} \in \mathbb{F}_q^n$ se verifica que $\mathbf{x} \in \mathcal{C}$ si y sólo si $H\mathbf{x}^t = \mathbf{0}$.*

Si $\mathcal{C}$ es de tipo $[n,k]$, entonces H es de tamaño $(n-k)\times n$ y rango $n-k$.

Ejemplo 5.2.2. Una matriz del control del código de Hamming es

$$H=\begin{pmatrix}1&1&0&1&1&0&0\\1&1&1&0&0&1&0\\1&0&1&1&0&0&1\end{pmatrix}.$$

A veces se toma como código de Hamming uno equivalente a éste, disponiendo las columnas de H en orden creciente como representación binaria de los enteros 1,2,...,7. Como veremos más adelante, esta disposición es aprovechada en la descodificación.

Proposición 5.2.2. *Si G y H son matrices generatriz y de control de $\mathcal{C}$, entonces $GH^t=0$.*

Si G es una matriz generatriz de $\mathcal{C}$ dada en forma estándar, $G=(I_k,C)$, entonces es fácil ver que la matriz $H=(-C^t,I_{n-k})$ tiene tamaño $(n-k)\times n$, rango $n-k$ y verifica $GH^t=0$, luego es una matriz de control para $\mathcal{C}$. Diremos que una matriz de control está en forma estándar si es de la forma (B,I_{n-k}).
La distancia mínima de un código puede ser obtenida a partir de su matriz de control. Para poder probar este resultado nos es preciso un nuevo concepto.

Definición 5.2.5. *Sea $\mathbf{x}=(x_1,\cdots,x_n)\in\mathbb{F}_q^n$. Llamaremos* soporte *de $\mathbf{x}$ al conjunto* $\mathrm{sop}(\mathbf{x})=\{i\mid 1\le i\le n, x_i\neq 0\}$. *Llamaremos* peso de Hamming *de $\mathbf{x}$ a $w(\mathbf{x})=|\mathrm{sop}(\mathbf{x})|=d(\mathbf{x},\mathbf{0})$ siendo $\mathbf{0}$ el vector $\mathbf{0}=(0,0,\cdots,0)$.*

La aplicación w, así definida, es una norma en $\mathbb{F}_q^n$ y que d es la distancia asociada a esta norma. Análogamente a la distancia mínima de un código, podemos definir su *peso mínimo* como

$$w(\mathcal{C})=\min\{w(\mathbf{c})\mid \mathbf{c}\in\mathcal{C},\mathbf{c}\neq\mathbf{0}\}. \tag{5.1}$$

Lema 5.2.1. *En un código lineal, la distancia mínima es igual al peso mínimo.*

Demostración. $d(\mathbf{x},\mathbf{y})=w(\mathbf{x}-\mathbf{y})$. ■

Proposición 5.2.3. *Sea $\mathcal{C}$ un código lineal de matriz de control H y distancia mínima d. Entonces $d > r$ si y sólo si cualesquiera r columnas de H son linealmente independientes. Por tanto, la distancia mínima de $\mathcal{C}$ coincide con el menor cardinal de un conjunto de columnas linealmente dependientes en H.*

Demostración. Cualesquiera r columnas de H son independientes si y sólo si para ningún vector de peso $\leq r$ sucede que $H\mathbf{x}^t = \mathbf{0}$. ■

Ejemplo 5.2.3. Consideremos el código de Hamming y sea H su matriz de control. Las columnas de H son todos los elementos de $\mathbb{F}_2^3$, excepto $(0,0,0)$. En particular todas son distintas, luego (siendo $\mathbb{F}_2$ el cuerpo base) linealmente independientes dos a dos. Por tanto $d \geq 3$. Como $1110000 \in \mathcal{C}$, concluimos que $d = 3$. Puede comprobarse que $\mathcal{H}_2(3)$ es el código binario de distancia 3 y dimensión 4 con la mayor longitud posible.

Corolario 5.2.1 (Cota de Singleton)**.** *La distancia mínima de un código lineal $[n,k]$ verifica $d \leq n - k + 1$.*

Los códigos lineales para los que se alcanza la igualdad en la cota anterior, $d = n - k + 1$, son llamados de *máxima distancia de separación* (o MDS) y juegan un papel preponderante tanto a nivel teórico como práctico.

5.2.3. Dualidad

La matriz de control, H, de un código lineal $\mathcal{C}$, puede ser interpretada como matriz generatriz de otro código sobre $\mathbb{F}_q$, llamado *dual* de $\mathcal{C}$ y denotado $\mathcal{C}^\perp$. Obviamente, si $\mathcal{C}$ tiene dimensión k, entonces $\mathcal{C}^\perp$ tiene dimensión $n - k$. Además, si G es una matriz generatriz de $\mathcal{C}$, como la igualdad $GH^t = 0$ implica $HG^t = 0$, se deduce que G es una matriz de control para $\mathcal{C}^\perp$.

Proposición 5.2.4. *Si $\mathcal{C}$ es un código lineal, entonces su dual $\mathcal{C}^\perp$ es el ortogonal de $\mathcal{C}$ con respecto a la forma bilineal*

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{F}_q. \tag{5.2}$$

Demostración. Sean G y H matrices generatriz y de control de $\mathcal{C}$. El resultado es consecuencia de la igualdad $GH^t = 0$, ya que rango(G) + rango$(H) = n$. ■

Como la forma bilineal $\langle \cdot, \cdot \rangle$ es simétrica y no degenerada, se verifica que $(\mathcal{C}^\perp)^\perp = \mathcal{C}$, es decir, el dual del dual de un código es el propio código. Obsérvese que puede darse la situación $\mathcal{C} \cap \mathcal{C}^\perp \neq \{\mathbf{0}\}$. El caso extremo se presenta cuando $\mathcal{C} = \mathcal{C}^\perp$.

Definición 5.2.6. *Diremos que un código lineal es* autodual *cuando coincide con su código dual.*

A diferencia de lo que ocurre con la dimensión, no es posible, en general, determinar la distancia mínima de $\mathcal{C}^\perp$ únicamente en términos de la distancia mínima de $\mathcal{C}$.

5.2.4. Descodificación por síndrome

En esta sección vamos a exponer un método general de descodificación para códigos lineales. Sean $\mathcal{C}$ un código lineal $[n, k, d]$ sobre $\mathbb{F}_q$ y H una matriz de control. Como sabemos $\mathcal{C}$ corrige $t = \lfloor \frac{d-1}{2} \rfloor$ errores. Supongamos enviada una palabra $\mathbf{c} \in \mathcal{C}$ y recibido un vector $\mathbf{y} \in \mathbb{F}_q^n$. El error cometido durante la transmisión ha sido $\mathbf{e} = \mathbf{y} - \mathbf{c}$. La estrategia que seguiremos para descodificar $\mathbf{y}$ es simple (en esencia la misma que en 5.1.2): calculamos la distancia de $\mathbf{y}$ a todas las palabras de $\mathcal{C}$ y la descodificamos por la más próxima (si existe). Si durante la transmisión se han cometido a lo más t errores (es decir, si $w(\mathbf{e}) \leq t$), entonces $d(\mathbf{c}, \mathbf{y}) = w(\mathbf{e}) \leq t$ y $\mathbf{c}$ es la única palabra del código con tal propiedad; la descodificación es por tanto correcta. Si $t < w(\mathbf{e}) < d$, podemos detectar que se han producido errores (puesto que $\mathbf{y} \notin \mathcal{C}$), pero no corregirlos en general. Si $w(\mathbf{e}) \geq d$ la descodificación fallará eventualmente.
Llevar a cabo este proceso es mucho más simple y computacionalmente económico para los códigos lineales, debido a su estructura algebraica.

Definición 5.2.7. *Llamaremos* síndrome *de* $\mathbf{y}$ *al vector*

$$s(\mathbf{y}) = H\mathbf{y}^t \in \mathbb{F}_q^{n-k}. \tag{5.3}$$

Notemos que $\mathbf{y} \in \mathcal{C}$ si y sólo si $s(\mathbf{y}) = \mathbf{0}$. Por tanto, al ser el síndrome una aplicación lineal, $s(\mathbf{y}) = s(\mathbf{c}+\mathbf{e}) = s(\mathbf{c}) + s(\mathbf{e}) = s(\mathbf{e})$. Así, recibido $\mathbf{y}$, conocemos inmediatamente el síndrome del error cometido.

Proposición 5.2.5. *El síndrome del vector recibido* $\mathbf{y}$ *es una combinación lineal de las columnas de* H *correspondientes a las posiciones de error.*

Para ver en que modo puede ayudarnos el síndrome a detectar y corregir errores examinemos un caso simple. Supongamos que $\mathcal{C}$ corrige al menos un error y que durante la transmisión ha ocurrido un único error (es decir, que $w(\mathbf{e}) = 1$, pongamos $\mathbf{e} = (0, \cdots, 0, e_i, 0, \cdots, 0)$). Por ser $d \geq 3$, cualesquiera dos columnas de H son linealmente independientes, es decir ninguna columna de H es múltiplo de ninguna otra. Así el síndrome del vector recibido $\mathbf{y}$ ser múltiplo de una y sólo una columna de H. Según la proposición anterior, la posición de esa columna es precisamente la posición en que se ha cometido el error, es decir, si $\mathbf{h}_i$ es la i-sima columna de H, $s(\mathbf{y}) = e_i\mathbf{h}_i$, de donde pueden deducirse inmediatamente $\mathbf{e}$ y el mensaje enviado $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

Ejemplo 5.2.4. Utilizando el código de Hamming binario $\mathcal{H}_2(3)$ de matriz de control

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

se envía el mensaje $\mathbf{c} = 0010110$. Durante la transmisión ocurre un error, de manera que se recibe $\mathbf{y} = 0011110$. El síndrome del vector recibido es

$$H(0011110)^t = (100)^t.$$

Como 100 es la representación binaria de 4, el error ha ocurrido en la cuarta posición, luego $\mathbf{y}$ se descodifica por 0010110, que era el mensaje enviado.

Consideremos en $\mathbb{F}_q^n$ la relación de equivalencia: $\mathbf{u} \sim \mathbf{v}$ si y sólo si $\mathbf{u}-\mathbf{v} \in \mathcal{C}$. El espacio vectorial cociente obtenido, módulo tal relación, se denota por $\mathbb{F}_q^n/\mathcal{C}$. Los elementos de $\mathbb{F}_q^n/\mathcal{C}$ son clases de equivalencia $\mathbf{u}+\mathcal{C} = \{\mathbf{u}+\mathbf{x} \mid \mathbf{x} \in \mathcal{C}\}$. Como cada clase posee $|\mathcal{C}| = q^k$ elementos (o *representantes*),

el cardinal de $\mathbb{F}_q^n/\mathcal{C}$ es q^{n-k} y su dimensión es $n-k$. Nótese que $\mathbf{u}-\mathbf{v} \in \mathcal{C}$ si y sólo si $s(\mathbf{u}) = s(\mathbf{v})$, luego recibido $\mathbf{y}$, al calcular $s(\mathbf{y})$ conocemos la clase a la que pertenece el error.

Definición 5.2.8. *Si en una clase existe un único elemento de peso mínimo, éste recibe el nombre de* líder *de la clase.*

Algunos autores exigen, además, que el peso de tal elemento sea $\leq t$ (siendo t la capacidad de corrección del código) para darle el nombre de líder. En cualquier caso, en general no toda clase tendrá líder ya que el elemento de peso mínimo no será, en general, único. Sin embargo, si una clase contiene un elemento de peso $\leq t$, éste es el líder de la clase.

Proposición 5.2.6. *Cada clase de $\mathbb{F}_q^n/\mathcal{C}$ posee a lo más un elemento de peso $\leq t$.*

Demostración. Si existen $\mathbf{u}, \mathbf{v}$ en la misma clase, ambos de peso $\leq t$, entonces $\mathbf{u} - \mathbf{v} \in \mathcal{C}$ y $w(\mathbf{u} - \mathbf{v}) \leq w(\mathbf{u}) + w(\mathbf{v}) \leq 2t < d(\mathcal{C})$, lo cual implica que $\mathbf{u} = \mathbf{v}$. ■

Algoritmo del líder

Recibido un vector $\mathbf{y}$, como todos los vectores $\mathbf{y} - \mathbf{x}$, $\mathbf{x} \in \mathcal{C}$, están en la misma clase de $\mathbb{F}_q^n/\mathcal{C}$, que es la de $\mathbf{y}$, el mínimo de $d(\mathbf{y}, \mathbf{x}) = w(\mathbf{y} - \mathbf{x})$ se obtiene cuando $\mathbf{y} - \mathbf{x}$ es el líder de la clase. Por tanto la descodificación es posible si y sólo si la clase del vector recibido posee líder, y el error es asumido como el líder de la clase. La proposición 5.2.6 garantiza que si el número de errores no supera la capacidad correctora del código, entonces la descodificación es correcta.
Para llevar a cabo este proceso, construimos una tabla con dos columnas y tantas filas como clases hay en $\mathbb{F}_q^n/\mathcal{C}$ (es decir, q^{n-k} filas). En la primera columna escribimos el síndrome de un elemento cualquiera de cada una de las clases; en la segunda el líder de la clase correspondiente (si existe). Esta tabla se construye de una vez por todas y sirve para la descodificación de cualquier vector. Ahora, recibido $\mathbf{y}$, hacemos

Algoritmo 1. Recibido un vector $\mathbf{y}$,
1. calcular $s(\mathbf{y})$ y buscarlo en la columna de síndromes
2. si la clase correspondiente no posee líder, la descodificación falla. Fin.
3. Si la clase posee líder, $\mathbf{e}$, se decide que $\mathbf{e}$ es el error cometido. La palabra descodificada es $\mathbf{y} - \mathbf{e}$. Fin.

5.2.5. Códigos cíclicos

Los códigos cíclicos constituyen la familia más ampliamente utilizada de códigos correctores de errores. Para su estudio alteraremos ligeramente las notaciones que venimos utilizando, y escribiremos las coordenadas de los vectores desde 0 a $n-1$. Así pondremos $\mathbf{x} = (x_0, \cdots, x_{n-1})$ en lugar de $(x_1, \cdots, x_n)$. Enseguida podrá apreciarse la utilidad de este cambio de notación.

Noción de código cíclico

Definición 5.2.9. *Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$, es* cíclico *si para cada $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ se verifica que $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$.*

En otros términos, se exige a $\mathcal{C}$ ser invariante por permutaciones cíclicas. Sean $\mathbb{F}_q[x]_{(n-1)}$ el espacio vectorial de los polinomios sobre $\mathbb{F}_q$ con grado menor que n y A el anillo cociente $A = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. En virtud de los isomorfismos de espacios vectoriales

$$\mathbb{F}_q^n \cong \mathbb{F}_q[x]_{(n-1)} \cong A \tag{5.4}$$

podemos identificar cada vector $(a_0, \cdots, a_{n-1})$ con el polinomio $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ y con la clase, en A, $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$. Consecuentemente, un código sobre $\mathbb{F}_q$ puede considerarse como un subconjunto de A. En lo que sigue utilizaremos libremente estas identificaciones. Por otra parte, impondremos la restricción adicional $\mathrm{mcd}(q, n) = 1$. Esto garantiza que el polinomio $x^n - 1$ tiene todos sus factores irreducibles distintos y sus raíces forman un grupo cíclico de orden n. La propiedad fundamental de los códigos cíclicos es la siguiente.

Teorema 5.2.1. *Sea $\mathcal{C}$ un código lineal no nulo de longitud n sobre el cuerpo finito $\mathbb{F}_q$. $\mathcal{C}$ es cíclico si y sólo si, considerado inmerso en A, es un ideal.*

Demostración. Supongamos que $\mathcal{C}$ es cíclico. Puesto que $\mathcal{C}$ es ya un subgrupo abeliano de A, basta probar que si $a(x) \in \mathcal{C}$ entonces $Xc(x) \in \mathcal{C}$. Ahora bien

$$x(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) \equiv c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1}$$

y el hecho de que este último polinomio pertenezca al código no es sino la definición de código cíclico interpretada en lenguaje polinómico. El recíproco se demuestra de manera idéntica. ■

Es conocido que todo ideal del anillo A es principal, es decir, consiste en el conjunto de múltiplos de un polinomio $g(x)$ divisor de $x^n - 1$.

Corolario 5.2.2. *Dado un código cíclico no nulo $\mathcal{C}$ de longitud n, existe un único polinomio mónico $g(x) \in \mathbb{F}_q[x]$ divisor de $x^n - 1$, tal que $\mathcal{C} = \langle g(x) \rangle$. En consecuencia, los elementos de $\mathcal{C}$ pueden identificarse con los polinomios de grado menor que n múltiplos de $g(x)$.*

Matrices generatriz y de control

Proposición 5.2.7. *Sea $\mathcal{C}$ un código cíclico de longitud n sobre $\mathbb{F}_q$ con polinomio generador $g(x)$ de grado $n - k$. El conjunto*

$$\{g(x), xg(x), \cdots, x^{k-1}g(x)\} \tag{5.5}$$

es una base de $\mathcal{C}$. En particular, $\mathcal{C}$ tiene dimensión k.

Demostración. Basta probar la primera afirmación. Tomemos $f(x)g(x) \in \mathcal{C}$. Podemos suponer $\deg f(x) < k$ (en caso contrario puede encontrarse en A un polinomio $f'(x)$ con $\deg f'(x) < k$ y $f(x)g(x) = f'(x)g(x)$). Sea pues $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$. La escritura

$$f(x)g(x) = a_0g(x) + a_1xg(x) + \cdots + a_{k-1}x^{k-1}g(x) \tag{5.6}$$

es la combinación lineal buscada, luego $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ es un sistema de generadores. Veamos que es un conjunto libre. Una relación de dependencia lineal

$$b_0g(x) + b_1xg(x) + \cdots + b_{k-1}x^{k-1}g(x) = 0 \tag{5.7}$$

puede escribirse también $b(x)g(x) = 0$, siendo $b(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1}$. Como $\deg(b(x)g(x)) < n$ y $g(x) \neq 0$, se verifica (en A) que $b(x) = 0$, luego $b_i = 0$ para $i = 0, 1, \cdots, k-1$. ■

Corolario 5.2.3. *Un codigo cíclico de longitud n y polinomio generador* $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ *tiene matriz generatriz*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & & & & \\ & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & & & & \\ & & \ddots & \ddots & & \ddots & \ddots & & & \\ & & & & \ddots & \ddots & & \ddots & \ddots & \\ & & & & & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} \end{pmatrix}.$$

La codificación con un código cíclico $\mathcal{C}$ de parámetros $[n, k]$, puede hacerse del modo usual –a partir de cualquiera de las matrices generatrices descritas anteriormente– o utilizando la notación polinómica. Con esta notación el mensaje sin codificar puede identificarse con un polinomio $a(x)$ de grado menor que k y su codificación es simplemente

$$g(x)a(x) \in \mathcal{C} \tag{5.8}$$

siendo $g(x)$ el polinomio (de grado $n-k$) generador de $\mathcal{C}$. Si se desea que la codificación sea sistemática, entonces realizamos la división euclídea

$$x^{n-k}a(x) = g(x)q(x) + r(x) \tag{5.9}$$

con $\deg r(x) < \deg g(x) = n - k$. El mensaje $a(x)$ se codifica por

$$x^{n-k}a(x) - r(x) \in \mathcal{C}. \tag{5.10}$$

Nótese que la codificación es sistemática en las últimas k posiciones. Vamos ya con la matriz de control.

Definición 5.2.10. *Si* $\mathcal{C}$ *es un código cíclico de longitud n, con polinomio generador* $g(x)$ *de grado* $n-k$*, llamaremos* polinomio de control *de* $\mathcal{C}$ *a*

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1x + \cdots + h_kx^k. \tag{5.11}$$

Proposición 5.2.8. *Con las notaciones de la definición anterior, la matriz (de tamaño $(n-k)\times n$)*

$$H = \begin{pmatrix} & & & & & h_k & h_{k-1} & \dots & h_1 & h_0 \\ & & & & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & \\ & & & . & . & . & . & . & & \\ & & & & & & & & & \\ & & . & . & . & . & & & & \\ h_k & h_{k-1} & \dots & h_1 & h_0 & & & & & \end{pmatrix}$$

es una matriz de control de $\mathcal{C}$.

Demostración. Basta con probar la identidad $GH^t = 0$. Para todo $1 \leq i \leq k, 1 \leq j \leq n-k$, el elemento (i,j) de la matriz producto GH^t, es el coeficiente de $x^{n-i-j+1}$ en el polinomio $g(x)h(x) = x^n - 1$. ■

Teniendo en cuenta la definición 5.2.10, resulta evidente que $h(x)$ es un generador de $\mathcal{C}^\perp$. Esto demuestra que el dual de un código cíclico es también cíclico.

Ceros de un código cíclico

Sea $x^n - 1 = f_1(x)f_2(x)\cdots f_m(x)$ la descomposición de $x^n - 1$ en factores irreducibles y sea α_i una raíz de $f_i(x)$. Para el código cíclico $\mathcal{C}_i$ engendrado por $f_i(x)$, se verifica $\mathcal{C}_i = \langle f_i(x)\rangle = \{c(x) \in A \mid c(\alpha_i) = 0\}$. En general, para el código cíclico $\mathcal{C}$ engendrado por $g(x) = f_{i_1} f_{i_2} \cdots f_{i_r}$, se tendrá

$$\mathcal{C} = \langle g(x)\rangle = \{c(x) \mid c(\alpha_{i_1}) = c(\alpha_{i_2}) = \cdots = c(\alpha_{i_r}) = 0\}, \qquad (5.12)$$

lo que muestra que los códigos cíclicos pueden definirse, alternativamente, como conjuntos de polinomios con ciertas raíces n-ésimas de 1 como ceros. Esto permite invertir el proceso: en lugar de partir del polinomio generador $g(X)$ y tomar los ceros adecuados (uno en cada factor irreducible de $g(X)$), podemos tomar, a priori, un conjunto de elementos $\{\alpha_1, \cdots, \alpha_r\}$ en una extensión finita $\mathbb{F}_{q^t}$ de $\mathbb{F}_q$ y definir

$$\mathcal{C} = \{c(x) \in A \mid c(\alpha_1) = \cdots = c(\alpha_r) = 0\}. \qquad (5.13)$$

Tal código es automáticamente cíclico, pues si $f_i(x)$ es el polinomio irreducible de α_i, se verifica que $\mathcal{C} = \langle g(x) \rangle = \text{mcm}(f_1, \cdots, f_r)$. Si n_i es el orden de α_i en $\mathbb{F}_{q^t}^*$ y $n = \text{mcm}\{n_1, \cdots, n_r\}$, es claro que $g(x)|x^n - 1$ y por tanto $\mathcal{C}$ es un código cíclico de longitud n.
Con esta caracterización de los códigos cíclicos puede comprobarse fácilmente si una palabra recibida está o no en el código. Para ello consideramos la matriz

$$H' = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \cdots & \alpha_r^{n-1} \end{pmatrix}. \tag{5.14}$$

Si, para un polinomio $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$, convenimos en considerar –forzando las notaciones– que

$$H'f(X) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_r)) \tag{5.15}$$

entonces $f(x) \in \mathcal{C}$ si y sólo si $H'f(x) = 0$, lo que autoriza a considerar a H' como un tipo de matriz de control del código. Nótese, sin embargo, que H' no tiene ni coeficientes en $\mathbb{F}_q$ ni dimensiones $(n-k) \times n$, por lo que no es una matriz de control en sentido estricto.
A continuación veremos como los códigos de Hamming pueden obtenerse de esta forma.

Ejemplo 5.2.5. Si $\text{mcd}(q-1, r) = 1$, entonces el código de Hamming q-ario $\mathcal{H}_q(r)$ es equivalente a un código cíclico. En particular, todo código de Hamming binario es equivalente a un código cíclico. En efecto, $\mathcal{H}_2(r)$ tiene longitud $n = 2^r - 1$ y dimensión $k = 2^r - r - 1$. Sea α un elemento primitivo de $\mathbb{F}_{2^r}$ (una raíz primitiva n-ésima de la unidad). Puesto que los elementos de $\mathbb{F}_{2^r}$ son las potencias de α, una matriz de control de $\mathcal{H}_2(r)$ es la matriz

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \end{pmatrix}$$

(identificando cada α^i con el vector columna de sus coordenadas en la base $1, \alpha, \cdots, \alpha^{r-1}$). Por tanto $\mathcal{H}_2(r)$ puede identificarse con el conjunto de los polinomios que tienen a α por raíz o, dicho de otra forma, con el código cíclico generado por el polinomio $\text{Irr}(\alpha, \mathbb{F}_2)$.

5.2.6. Códigos BCH y RS

Los códigos BCH (denominados así en honor de sus descubridores, Bose, Chaudhuri y Hocquenghem) constituyen la más importante familia de códigos cíclicos. Se ha visto en la sección anterior, que los códigos cíclicos pueden determinarse prescribiendo un conjunto de elementos como ceros de su polinomio generador. En concreto, si tomamos como ceros los elementos $\alpha_1, \cdots, \alpha_r$, entonces la matriz

$$H' = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \cdots \\ 1 & \alpha_r & \cdots & \alpha_r^{n-1} \end{pmatrix} \tag{5.16}$$

se comporta como una matriz de control del código obtenido, $\mathcal{C}$. En particular, la distancia mínima de $\mathcal{C}$ es $\geq d$ si cualesquiera $d-1$ columnas de H' son linealmente independientes. No es fácil, en general, determinar este número para una elección arbitraria de los α_i. Una excepción la constituye el caso en que los α_i son potencias consecutivas de una raíz primitiva n-ésima de la unidad, $\alpha_i = \alpha^i$, $i = 1, \cdots, r < n$, pues entonces todo menor de la correspondiente matriz H' se reduce a un determinante de tipo Vandermonde y $d(\mathcal{C}) \geq r + 1$.

Construcción y parámetros

Fijemos un cuerpo $\mathbb{F}_q$ y números naturales n, b y δ, $2 \leq \delta \leq n$. Sean m el orden multiplicativo de q módulo n (es decir, el menor número natural tal que $q^m \equiv 1 \pmod{n}$) y $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad.

Definición 5.2.11. *Llamaremos* código BCH *de longitud n y* distancia mínima prevista *δ, al código cíclico de longitud n cuyo polinomio generador tiene por raíces $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$.*

Si se toma $b = 1$, el código se denominar BCH *en sentido estricto*. Si la longitud n es de la forma $n = q^m - 1$, entonces se hablar de códigos BCH *primitivos* (en este caso el exponente m coincide con el orden multiplicativo de q módulo n y α es un elemento primitivo de $\mathbb{F}_{q^m}$); si, además, $m = 1$, (es decir, $n = q - 1$ y por tanto $\alpha \in \mathbb{F}_q$) el código se denomina *Reed-Solomon*. Los códigos Reed-Solomon son importantes por derecho propio y volveremos sobre ellos más adelante.

Proposición 5.2.9. *Un código BCH de distancia prevista δ, posee distancia mínima $d \geq \delta$.*

Demostración. Cualquier menor $(\delta - 1) \times (\delta - 1)$ de la matriz

$$H' = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \cdots \\ 1 & \alpha_r & \cdots & \alpha_r^{n-1} \end{pmatrix}$$

se reduce a un determinante de tipo Vandermonde, luego cualesquiera $\delta - 1$ de sus columnas son linealmente independientes. ■

Dado que, en general, no es factible conocer la auténtica distancia de un código BCH, en la práctica se utiliza δ como un sustituto de la misma. Claro está que la distancia mínima real puede ser mayor que la prevista (como veremos a continuación en los ejemplos).
Un polinomio generador del código puede obtenerse del modo siguiente: para $i = b, \cdots, b + \delta - 2$, sea $m_i(x)$ el polinomio irreducible de α^i sobre $\mathbb{F}_q$. Entonces

$$g(x) = \text{ mcm}\{m_b(x), \cdots, m_{b+\delta-2}(x)\} \tag{5.17}$$

es el polinomio generador buscado. La dimensión del código es, como en todos los códigos cíclicos, $n - \deg g(x)$.

Ejemplo 5.2.6. Por simplicidad trabajaremos con códigos BCH binarios, primitivos y en sentido estricto. Así, sean $m \in \mathbb{Z}$, $n = 2^m - 1$ y $\alpha \in \mathbb{F}_{2^m}$ una raíz primitiva n-ésima de la unidad (es decir, un elemento primitivo de $\mathbb{F}_{2^m}$). El caso más simple de código BCH se da para $\delta = 2$, obteniéndose

$$\mathcal{C}_2 = \{c(x) \in A = \mathbb{F}_2[x]/\langle x^n - 1\rangle \mid c(\alpha) = 0\}.$$

Como $c(x) \in \mathbb{F}_2[x]$, si $c(\beta) = 0$, entonces $c(\beta^2) = 0$. Por tanto

$$\mathcal{C}_2 = \mathcal{C}_3 = \{c(x) \in A \mid c(\alpha) = c(\alpha^2) = 0\}.$$

Como ya sabemos, $\mathcal{C}_2 = \mathcal{C}_3$ es un código de Hamming, de distancia mínima 3.

El siguiente caso a considerar es $\delta = 4$. El código que se obtiene es

$$\begin{aligned} \mathcal{C}_4 &= \{c(x) \in A \mid c(\alpha) = c(\alpha^2) = c(\alpha^3) = 0\} \\ &= \{c(x) \in A \mid c(\alpha) = c(\alpha^3) = 0\}. \end{aligned}$$

Como en el caso anterior, los polinomios de $\mathcal{C}_4$ verifican automáticamente la condición $c(\alpha^4) = 0$, luego $\mathcal{C}_4 = \mathcal{C}_5$ y este código tiene distancia mínima ≥ 5. Una matriz de control es

$$H' = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \end{pmatrix}$$

Si $m_1(x) = \mathrm{Irr}(\alpha, \mathbb{F}_2)$ y $m_3(x) = \mathrm{Irr}(\alpha^3, \mathbb{F}_2)$, el polinomio generador de $\mathcal{C}_4$ es

$$g(x) = \mathrm{mcm}\{m_1(x), m_3(x)\}.$$

Para poder realizar un cálculo concreto fijemos $m = 4$ (luego $n = 15$). En este caso, los polinomios $m_1(x), m_3(x)$ son

$$\begin{aligned} m_1(x) &= 1 + x + x^4 \\ m_3(x) &= 1 + x + x^2 + x^3 + x^4 \end{aligned}$$

por lo que

$$g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) = 1 + x^4 + x^6 + x^7 + x^8$$

y la dimensión de $\mathcal{C}_4$ es $n - \deg g(x) = 7$. Las matrices generatriz y de control del código pueden obtenerse por el procedimiento habitual, a partir de $g(x)$, o directamente a partir de H'. Tomando la base $\{1, \alpha, \alpha^2, \alpha^3\}$ de $\mathbb{F}_{2^4}$ sobre $\mathbb{F}_2$, las coordenadas de cada elemento de $\mathbb{F}_{2^4}$ son

$$\begin{array}{cccc} 1 = 1000 & \alpha^4 = 1100 & \alpha^8 = 1010 & \alpha^{12} = 1111 \\ \alpha = 0100 & \alpha^5 = 0110 & \alpha^9 = 0101 & \alpha^{13} = 1011 \\ \alpha^2 = 0010 & \alpha^6 = 0011 & \alpha^{10} = 1110 & \alpha^{14} = 1001 \\ \alpha^3 = 0001 & \alpha^7 = 1101 & \alpha^{11} = 0111 & \end{array}$$

(recuérdese que $\mathrm{Irr}(\alpha, \mathbb{F}_2) = 1 + x + x^4$, luego $1 + \alpha = \alpha^4$). Con esto, H' es

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}$$

una matriz de control, en sentido estricto, queda

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Códigos de Reed-Solomon

Repitamos la definición, ya citada, de código de Reed-Solomon:

Definición 5.2.12. *Un código* Reed-Solomon *sobre* $\mathbb{F}_q$ *es un código BCH primitivo de longitud* $n = q - 1$.

Como caso particular de los BCH que son estos códigos, siguen los mismos procesos de codificación y descodificación que aquellos. Su característica distintiva más notable es que la raíz n-ésima, α, es un elemento de $\mathbb{F}_q$ y, por tanto, todas las manipulaciones con el código implican sólo operaciones en el propio cuerpo $\mathbb{F}_q$. Como contrapartida a esta simplicidad de manejo, queda limitada a $q - 1$ la longitud de un código Reed-Solomon sobre $\mathbb{F}_q$.
Una primera justificación del interés de estos códigos es el siguiente resultado.

Proposición 5.2.10. *Los códigos Reed-Solomon son MDS.*

Demostración. Como en todo código BCH, fijada la distancia prevista δ y la raíz n-ésima α, su distancia mínima y dimensión, d y k, verifican $d \geq \delta$ y $k = n - \deg g(x)$, siendo $g(x) = \text{mcm}\{\text{Irr}(\alpha^i, \mathbb{F}_q) \mid i = 1, \cdots, \delta - 1\}$. Ahora bien, dado que $\alpha^i \in \mathbb{F}_q$ para todo i, se tendrá $\deg g(x) = \delta - 1$ luego, teniendo en cuenta la cota de Singleton, $k = n - \delta - 1$, de donde $d = n - k + 1$. ∎

Los códigos de Reed-Solomon son habitualmente utilizados en la detección de errores (aleatorios y a ráfagas) sobre canales binarios. Dado que,

como se ha dicho, su longitud es muy pequeña, para 'alargarla' se utiliza a menudo la estrategia de descenso de cuerpo, que describimos a continuación.
Dado un cuerpo finito $\mathbb{F}_{q^r}$, extensión de $\mathbb{F}_q$, fijemos una base $\{1, \alpha, \cdots, \alpha^{r-1}\}$ de $\mathbb{F}_{q^r}$ sobre $\mathbb{F}_q$. Como sabemos, cada elemento de $\mathbb{F}_{q^r}$ puede identificarse con el vector de $\mathbb{F}_q^r$ de sus coordenadas en la base anterior. Aplicando este procedimiento a cada componente de un vector de $\mathbb{F}_{q^r}^n$, obtenemos un vector de $\mathbb{F}_q^{rn}$

$$\begin{array}{c}\text{vector original sobre } \mathbb{F}_{q^r} \\ \overbrace{*\cdots*}^{*}\overbrace{*\cdots*}^{*}\cdots\cdots\overbrace{*\cdots*}^{*} \\ \text{vector obtenido sobre } \mathbb{F}_q\end{array} \tag{5.18}$$

En particular, si $\mathcal{C}$ es un código de longitud n sobre $\mathbb{F}_{q^r}$, a partir de él podemos conseguir un código sobre $\mathbb{F}_q$ de longitud rn; se dice que este cuerpo se obtiene del original *por descenso de cuerpo.*
Esta construcción se realiza habitualmente con códigos Reed-Solomon definidos sobre $\mathbb{F}_{2^r}$. Si el código inicial tiene longitud n, entonces el código binario obtenido por descenso de cuerpo sobre $\mathbb{F}_2$ tiene longitud rn y gran capacidad de detección de errores a ráfagas.

Proposición 5.2.11. *Sea $\mathcal{C}$ un código de Reed-Solomon sobre $\mathbb{F}_{2^r}$ con distancia $d = 2t + 1$. Entonces, el código binario obtenido por descenso de cuerpo sobre $\mathbb{F}_2$ corrige todos los errores a ráfagas de longitud $l \leq (t-1)r + 1$.*

Demostración. Recibida una palabra binaria, podemos transformarla en un vector de $\mathbb{F}_{2^r}$ siguiendo el proceso contrario al descrito anteriormente (es decir, ascendiendo de cuerpo). Si los errores forman un ráfaga de longitud $l \leq (t-1)r+1$, teniendo en cuenta que cada r símbolos binarios se colapsan en uno solo de $\mathbb{F}_{2^r}$, la palabra transformada contiene a lo más t coordenadas erróneas. Pero t es precisamente la capacidad de corrección del código. ■

5.3. Códigos sobre anillos

Durante toda esta sección A sera un anillo de cadena con ideal maximal $\mathfrak{m}$. Consideraremos siempre fijado un generador del ideal maximal θ.

Recordemos de la Sección 4.4 que los ideales de A son $\langle\theta^i\rangle$ con $i = 1, 2, \ldots, \beta$ donde β es el índice de nilpotencia. Los divisores de cero corresponden al ideal $\langle\theta\rangle$ y los elementos en $A \setminus \langle\theta\rangle$ son las unidades. Para todo elemento no nulo $a \in A$ existe un único exponente tal que $a = u\theta^i$ con u una unidad única módulo $\theta^{\beta-1}$. Claramente para cada par de índices $1 \leq i < j \leq \beta$ si $c\theta^i \in \langle\theta^j\rangle$ entonces $c \in \langle\theta^{j-i}\rangle$.

5.3.1. Álgebra lineal sobre anillos de cadena

El el caso de álgebra lineal sobre anillos el rango de McCoy juega el mismo papel que el rango en el caso de cuerpos. Para un anillo de cadena se puede definir como sigue.

Definición 5.3.1. *El rango de McCoy de una matriz $\mathcal{M}$ con entradas en un anillo de cadena A es el mayor entero positivo t tal que existe un menor de la matriz que es una unidad. En caso de que no exista ningun menor que sea una unidad el rango de McCoy es 0. Notaremos el rango de McCoy de la matriz $\mathcal{M}$ por* $\mathrm{rg}_{Mc}(\mathcal{M})$.

Teorema 5.3.1. *Consideremos $\mathbf{v}_1, \ldots, \mathbf{v}_m \in A^n \setminus \theta A^n$. El conjunto $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ es linealmente dependiente si y sólo si $\{\overline{\mathbf{v}_1}, \ldots, \overline{\mathbf{v}_m}\}$ son linealmente dependientes en $\mathbb{K} = A/\mathfrak{m}$.*

Demostración. Supongamos que son linealmente dependientes en A^n, existen $\alpha_i \in A$ no todos nulos con $\sum_{i=1}^m \alpha_i \mathbf{v}_i = \mathbf{0}$. Consideremos el mayor j tal que $\theta^j | \alpha_i$ para todo $i = 1, 2, \ldots, m$. Podemos reescribir cada coeficiente como $\alpha_i = \theta^j \alpha_i'$. Claramente θ divide a $\sum_{i=1}^m \alpha_i' \mathbf{v}_i$ pues $\theta^j \sum_{i=1}^m \alpha_i' \mathbf{v}_i = \mathbf{0}$. De aqui obtenemos que $\sum_{i=1}^m \overline{\alpha_i'}\overline{\mathbf{v}_i}$ y no todos los coeficientes $\overline{\alpha_i'}$ son nulos por la maximalidad de j.
En el otro sentido, supongamos que $\{\overline{\mathbf{v}_1}, \ldots, \overline{\mathbf{v}_m}\}$ son linealmente dependientes, existen coeficientes $\beta_i \in \mathbb{K}$ no todos nulos con $\sum_{i=1}^m \beta_i \overline{\mathbf{v}_i} = 0$. Tomemos un elemento γ_i del anillo A tal que $\overline{\gamma_i} = \beta_i$. Entonces $\theta | \sum_{i=1}^m \gamma_i \mathbf{v}_i$ y existe δ con

$$\sum_{i=1}^m \delta\gamma_i \mathbf{v}_i = \delta \sum_{i=1}^m \gamma_i \mathbf{v}_i = 0,$$

con al menos una de los γ_i una unidad, esto es al menos uno de los $\delta\gamma_i$ no nulo. ∎

Corolario 5.3.1. *Dada una matriz $\mathcal{M}$ con entradas en el anillo A las siguientes proposiciones son equivalentes.*

1. $\mathrm{rg}_{Mc}(\mathcal{M}) = t$.

2. *El rango de $\overline{\mathcal{M}}$ es t.*

3. *$\mathcal{M}$ tiene t filas linealmente independientes y $t+1$ filas son siempre linealmente dependientes.*

4. *$\mathcal{M}$ tiene t columnas linealmente independientes y $t+1$ columnas son siempre linealmente dependientes.*

La regla de Cramer para sistemas sobre un anillo de cadena A se cumple (véase por ejemplo [7]). Como corolario tenemos que

$$|\{\mathbf{x} \in A^n \mid \mathcal{M} \cdot \mathbf{x}^T = 0\}| = |A|^{n-m}.$$

5.3.2. Códigos lineales sobre A

Un código lineal $\mathcal{C}$ sobre A de longitud n es un A-submódulo de A^n. Para un entero positivo k denotaremos por Id_k la matriz identidad de tamaño $k \times k$. En toda esta sección cuando mencionemos código se referirá a código lineal.

Definición 5.3.2. *Sea $\mathcal{C}$ un código lineal sobre A. Una matriz G se denomina matriz generatriz de $\mathcal{C}$ si las filas de G generan linealmente a $\mathcal{C}$ y ninguna de ellas se puede poner como una combinación lineal de las demás.*

Diremos que la matriz generatriz G del código $\mathcal{C}$ está expresada en *forma estándar* si después de una permutación de las coordenadas adecuada

tiene la siguiente forma

$$G = \begin{pmatrix} \mathrm{Id}_{k_0} & C_{0,1} & C_{0,2} & C_{0,3} & \dots & C_{0,\beta-1} & C_{0,\beta} \\ 0 & \theta\mathrm{Id}_{k_1} & \theta C_{1,2} & \theta C_{1,3} & \dots & \theta C_{1,\beta-1} & \theta C_{1,\beta} \\ 0 & 0 & \theta^2\mathrm{Id}_{k_2} & \theta^2 C_{2,3} & \dots & \theta^2 C_{2,\beta-1} & \theta^2 C_{2,\beta} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \theta^{\beta-1} Id_{k_{\beta-1}} & \theta^{\beta-1} C_{\beta-1,\beta} \end{pmatrix}$$
$$= \begin{pmatrix} C_0 \\ \theta C_1 \\ \theta^2 C_2 \\ \vdots \\ \theta^{\beta-1} C_{\beta-1} \end{pmatrix}.$$

Asociaremos a G la matriz C dada por

$$C = \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ \vdots \\ C_{\beta-1} \end{pmatrix},$$

cuyas submatrices son únicas módulo $\theta^{\beta-1}$ y sus proyecciones sobre $\mathbb{K}$ son únicas.

Proposición 5.3.1. *Cualquier código $\mathcal{C}$ sobre un anillo de cadena A tiene una matriz generatriz en forma estándar.*

La demostración deja como ejercicio al lector, como indicación se toma un conjunto arbitrario de generadores de $\mathcal{C}$ y se aplican permutaciones de columnas y pasos de eliminación gaussiana siendo cuidadoso con la restricción de no dividir por no unidades.

Definición 5.3.3. *Dado un código $\mathcal{C}$ sobre un anillo de cadena A y un elemento $a \in A$ definimos $(\mathcal{C} : a)$ como es siguiente conjunto (cociente de submodulos)*

$$(\mathcal{C} : a) = \{b \in A \mid a \cdot b \in \mathcal{C}\}. \tag{5.19}$$

Definición 5.3.4. *Dado un código $\mathcal{C}$ sobre un anillo de cadena A con θ un generador de $\mathfrak{m}$ ideal maximal de A con índice de nilpotencia β lo*

asociamos la siguiente torre de códigos

$$\mathcal{C} = (\mathcal{C} : \theta^0) \subseteq \cdots \subseteq (\mathcal{C} : \theta^i) \subseteq \cdots \subseteq (\mathcal{C} : \theta^{\beta-1}) \tag{5.20}$$

y sobre $\mathbb{K} = A/\mathfrak{m}$

$$\overline{\mathcal{C}} = \overline{(\mathcal{C} : \theta^0)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : \theta^i)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : \theta^{\beta-1})} \tag{5.21}$$

Lema 5.3.1.

1. *Consideremos un código* $\mathcal{C}$ *con matriz generatriz* G *en forma estándar y matriz asociada* C*. Para cada valor de* $i = 1, 2, \ldots, \beta-1$ *el código* $\overline{(\mathcal{C} : \theta^i)}$ *tiene matriz generatriz*

$$\begin{pmatrix} \overline{C_0} \\ \overline{C_1} \\ \overline{C_2} \\ \vdots \\ \overline{C_i} \end{pmatrix},$$

   y su dimensión es $\sum_{j=0}^{i} k_j$*.*

2. *Si la cadena* $\mathcal{E}_0 \subseteq \mathcal{E}_1 \subseteq \cdots \subseteq \mathcal{E}_{\beta-1}$ *está formada por códigos de longitud* n *sobre* $\mathbb{K}$ *entonces existe un código* $\mathcal{C}$ *sobre* A *con*

$$\overline{(\mathcal{C} : \theta^i)} = \mathcal{E}_i, \qquad i = 0, 1, \ldots, \beta - 1.$$

Demostración.

1. Es claro que $\overline{(\mathcal{C} : \theta^i)}$ contiene al código generado por dicha matriz. Tomemos ahora $\overline{\mathbf{c}} \in \overline{(\mathcal{C} : \theta^i)}$ una palabra suya y la palabra $\mathbf{c} \in (\mathcal{C} : \theta^i)$ que se proyecta sobre ella. Para cualquier i se tiene que $\theta^i \mathbf{c} \in \mathcal{C}$ por lo tanto exixten vectores $\mathbf{v}_i \in A^{k_i}$ con $i = 0, 1, \ldots, \beta-1$ tales que

$$\begin{aligned} \theta^i \mathbf{c} =& (\mathbf{v}_0, \mathbf{v}_0 C_{0,1} + \theta \mathbf{v}_1, \ldots, \mathbf{v}_0 C_{0,\beta-1} + \theta \mathbf{v}_1 C_{1,\beta-1} \\ &+ \cdots + \theta^{\beta-1} \mathbf{v}_{\beta-1}, \mathbf{v}_0 C_{0,\beta} + \cdots + \theta^{\beta-1} \mathbf{v}_{\beta-1} C_{\beta-1,\beta}) \end{aligned}$$

   Como $\theta^i \mathbf{c}$ es divisible por θ^i existe $\mathbf{w}_0 \in A^{k_0}$ tal que $\theta^i \mathbf{w}_0 = \mathbf{v}_0$. Podemos reescribir la segunda componente del vector como

$\theta^i \mathbf{w}_0 C_{0,1} + \theta \mathbf{v}_1$ y por lo tanto existe $\mathbf{w}_1 \in A^{k_1}$ tal que $\theta^{i-1}\mathbf{w}_1 = \mathbf{v}_1$. De esta forma podemos continuar hasta establecer que existen

$$\mathbf{w}_j \in A^{k_j} \text{ tal que } \theta^{i-j}\mathbf{w}_j = \mathbf{v}_j, \qquad j = 1, 2, \ldots, i.$$

Por lo tanto se tiene que

$$\theta^i \mathbf{c} = \sum_{j=0}^{i} \theta^i \mathbf{w}_j A_j + \sum_{j=i+1}^{\beta-1} \theta^j \mathbf{v}_j A_j$$

de donde se sigue que

$$g \equiv \sum_{j=0}^{i} \mathbf{w}_j A_j + \sum_{j=i+1}^{\beta-1} \theta^{j-i} \mathbf{v}_j A_j \mod \theta^{\beta-1}.$$

Por lo tanto $\overline{g} = \sum_{j=0}^{i} \overline{\mathbf{w}_j}\,\overline{A_j}$ y está generado por la matriz dada en el enunciado. Claramente por el resultado en el Teorema 5.3.1 las filas de la matriz son linealmente independientes sobre $\mathbb{K}$ y se sigue el resultado de la dimensión.

2. Sea $l_i = \dim(\mathcal{E}_i)$. Podemos suponer (eventualmente realizando alguna permutación de columnas), que cada uno de ellos se puede poner de forma sistemática con una matriz generatriz expresada como

$$\begin{pmatrix} E_0 \\ E_1 \\ \vdots \\ E_i \end{pmatrix},$$

si elegimos ahora matrices C_i con entradas en A tales que $\overline{C_i} = E_i$ el código $\mathcal{C}$ dado por su matriz generatriz cumple las condiciones deseadas

$$\begin{pmatrix} C_0 \\ \theta C_1 \\ \vdots \\ \theta^{\beta-1} C_{\beta-1} \end{pmatrix}.$$

■

Teorema 5.3.2. *Sea $\mathcal{C}$ un código de longitud n sobre un anillo de cadena A. Entonces:*

1. *Los parámetros k_i para $i = 0, 1, \ldots, k_{\beta-1}$ son independientes de la matriz generatriz en forma estándar G elegida.*
2. *Cualquier palabra $\mathbf{c} \in \mathcal{C}$ se puede escribir de forma única como*

$$\mathbf{c} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{\beta-1}) \cdot G, \quad \mathbf{v}_i \in (A/\theta^{\beta-i}A)^{k_i} \simeq (\theta^i R)^{k_i}.$$

3.
$$|\mathcal{C}| = |\mathbb{K}|^{\sum_{i=0}^{\beta-1} k_i(\beta-i)}.$$

Demostración.

1. La unicidad de los parámetros k_i para $i = 0, 1, \ldots, k_{\beta-1}$ se sigue directamente del lema anterior pues $k_0 = \dim(\overline{\mathcal{C}})$ y $k_i = \dim(\overline{(\mathcal{C} : \theta^i)}) - \dim(\overline{(\mathcal{C} : \theta^{i-1})})$ con $i = 1, 2, \ldots, \beta - 1$.

2. Tomemos $k = \sum_{i=0}^{\beta-1} k_i$ y consideremos la aplicación de codificación

$$\begin{array}{rccc} \mathrm{cod}_G : & A^k & \longrightarrow & A^n \\ & \mathbf{v} & \mapsto & \mathbf{v} \cdot G. \end{array}$$

   Claramente $\mathrm{Im}\,(\mathrm{cod}_G) = \mathcal{C}$. Tomemos ahora $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{\beta-1})$.

$$\begin{aligned} \mathrm{cod}_G(\mathbf{v}) =& (\mathbf{v}_0, \mathbf{v}_0 C_{0,1} + \theta \mathbf{v}_1, \ldots, \mathbf{v}_0 C_{0,\beta-1} + \theta \mathbf{v}_1 C_{1,\beta-1} \\ & + \cdots + \theta^{\beta-1} \mathbf{v}_{\beta-1}, \mathbf{v}_0 C_{0,\beta} + \cdots + \theta^{\beta-1} \mathbf{v}_{\beta-1} C_{\beta-1,\beta}). \end{aligned}$$

   $\mathrm{cod}_G(\mathbf{v})) = \mathbf{0}$ implica $\mathbf{v}_0 = \mathbf{0}$. Esto a su vez implica $\theta \mathbf{v}_1 = \mathbf{0}$, es decir $\mathbf{v}_1 \in \theta^{\beta-1}A$ y continuando el razonamiento $\mathbf{v}_i \in \theta^{\beta-i}A$ para $i = 0, 1, \ldots, \beta - 1$. De donde

$$\ker\,(\mathrm{cod}_G) = \prod_{i=0}^{\beta-1} \theta^{\beta-i} A^{k_i}$$

   y

$$\mathcal{C} \cong A^k \Big/ \prod_{i=0}^{\beta-1} \theta^{\beta-i} A^{k_i} \cong \prod_{i=0}^{\beta-1} \left(A/\theta^{\beta-i} A \right)^{k_i} \cong \prod_{i=0}^{\beta-1} \left(\theta^i A \right)^{k_i}. \quad (5.22)$$

3. Se sigue directamente por conteo en la Ecuación (5.22).

■

Nótese que la Ecuación (5.22) nos proporciona un método de descomposición única de cualquier submódulo de A^n.

Dualidad

A partir de este momento y con las notaciones del apartado anterior definimos

$$k_0(\mathcal{C}) = \dim(\overline{\mathcal{C}})$$
$$k_i(\mathcal{C}) = \dim(\overline{(\mathcal{C} : \theta^i)}) - \dim(\overline{(\mathcal{C} : \theta^{i-1})}), \quad 1 \leq i \leq \beta - 1.$$

Teorema 5.3.3. *Consideremos $\mathcal{C}$ un código sobre un anillo de cadena A con matriz generatriz G en forma estándar.*

1. *Si definimos*

$$H_{i,j} = -\sum_{k=i+1}^{j-1} H_{i,k} C^T_{\beta-j,\beta-k} - C^T_{\beta-j,\beta-i}, \quad 0 \leq i < j \leq \beta$$

entonces la matriz

$$H = \begin{pmatrix} H_{0,\beta} & H_{0,\beta-1} & \dots & H_{0,1} & \mathrm{Id}_{n-k(\mathcal{C})} \\ \theta H_{1,\beta} & \theta H_{1,\beta-1} & \dots & \theta \mathrm{Id}_{n-k_{\beta-1}(\mathcal{C})} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \theta^{\beta-1} H_{\beta-1,\beta} & \theta^{\beta-1}\mathrm{Id}_{n-k_1(\mathcal{C})} & \dots & 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} H_0 \\ \theta H_1 \\ \vdots \\ \theta^{\beta-1} H_{\beta-1} \end{pmatrix},$$

es una matriz de paridad de $\mathcal{C}$ (o una matriz generatriz de $\mathcal{C}^\perp$).

2. $\overline{(\mathcal{C}^\perp : \theta^i)} = \left(\overline{(\mathcal{C} : \theta^{\beta-1-i})}\right)^\perp$, $k_0(\mathcal{C}^\perp) = n - k_0(\mathcal{C})$ *y* $k_i(\mathcal{C}^\perp) = k_{\beta-1}(\mathcal{C})$ *para* $1 \leq i \leq \beta - 1$.

3. $|\mathcal{C}|^{\perp} = |A^n|/|\mathcal{C}|$ *y* $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

Demostración.

1. La demostración es directa y se deja como ejercicio basándose en comprobar que $H \cdot G^T = \mathbf{0}$.

2. Consideremos un elemento $\mathbf{b} \in \overline{(\mathcal{C}^{\perp} : \theta^i)}$ y otro $\mathbf{e} \in \overline{(\mathcal{C} : \theta^i)}$. Por lo tanto $\theta^i \mathbf{b} \in \mathcal{C}^{\perp}$ y $\theta^{\beta-i-1}\mathbf{e} \in \mathcal{C}$, y se sigue que

$$\theta^{\beta-1}\mathbf{b}\mathbf{e}^T = 0,$$

esto es, $\mathbf{b}$ y $\mathbf{e}$ son ortogonales.

Razonemos ahora sobre la dimensión. Si consideramos D el A-módulo generado por la matriz H que por el apartado anterior sabemos que es $\mathcal{C}^{\perp}$. Sabemos que la suma de las dimensiones de dos espacios ortogonales no pueden superar la dimensión del espacio ambiente. Tenemos ahora:

$$\begin{aligned} n &\geq \dim\left(\overline{(\mathcal{C} : \theta^{\beta-i-1})}\right) + \dim\left(\overline{(\mathcal{C}^{\perp} : \theta^i)}\right) \\ &= \dim\left(\overline{(\mathcal{C} : \theta^{\beta-i-1})}\right) + \dim\left(\overline{(D : \theta^i)}\right) \\ &= k_0(\mathcal{C}) + \cdots + k_{\beta-i-1}(\mathcal{C}) + k_0(D) + \cdots + k_i(D) \\ &= k_0(\mathcal{C}) + \cdots + k_{\beta-i-1}(\mathcal{C}) + n - k(\mathcal{C}) + k_{\beta-i}(\mathcal{C}) \cdots + k_{\beta-1}(\mathcal{C}) \\ &= n. \end{aligned}$$

3. Se sigue inmediatamente del apartado anterior.

■

Asociaremos a la matriz de paridad H la siguiente matriz:

$$C(\perp) = \begin{pmatrix} H_0 \\ H_1 \\ H_2 \\ \vdots \\ H_{\beta-1} \end{pmatrix}.$$

Corolario 5.3.2. *Sea $\mathcal{C}$ un código con matriz generatriz G y matriz de paridad H y matrices asociadas C y $C(\perp)$ respectivamente. Entonces $\overline{\mathcal{C}}$ tiene matriz generatriz $\overline{A_0}$ y matriz de paridad $\overline{C(\perp)}$.*

Demostración. Se sigue directamente de la igualdad

$$(\overline{\mathcal{C}})^{\perp} = \left(\overline{(\mathcal{C}^{\perp} : \theta^{0})}\right)^{\perp} = \overline{(\mathcal{C}^{\perp} : \theta^{\beta-1})}.$$

■

Nota. Nótese que las matrices C y $C(\perp)$ no son únicas para un código dado $\mathcal{C}$.

Códigos libres

La siguiente proposición es inmediata de los resultados y conocimientos previos.

Proposición 5.3.2. *Consideremos $\mathcal{C}$ un código sobre un anillo de cadena A. Los siguientes enunciados son equivalentes.*

1. *$\mathcal{C}$ es un código libre (como submódulo).*
2. *Si la matriz G es una matriz generatriz de $\mathcal{C}$ en forma estándar entonces $G = (\mathrm{Id}\,, C)$ para alguna matriz C (es decir, es sistemática).*
3. *$k(\mathcal{C}) = k_0(\mathcal{C})$.*
4. *$\overline{\mathcal{C}} = \overline{(\mathcal{C} : \theta)} = \cdots = \overline{(\mathcal{C} : \theta^{\beta-1})}$.*
5. *$\mathcal{C}^{\perp}$ es un código libre.*

5.3.3. Distancia de Hamming

Por motivos que expondremos más adelante en la Sección 5.4 la distancia de Hamming no es la más adecuada sobre un anillo de cadena siendo la elección adecuada la métrica de Lee. Aún así realizaremos un breve estudio de ella. Como en el caso de cuerpos llamaremos soporte de un elemento $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in A^n$ a

$$\mathrm{sop}(\mathbf{x}) = \{i \mid x_i \neq 0\}.$$

El soporte de un conjunto en A^n será la unión de todos los soportes de sus elementos y la distancia de Hamming de un código $\mathcal{C}$ será entonces

$$\mathrm{d}(\mathcal{C}) = \mín\{|\mathrm{sop}(\mathbf{c})| \mid \mathbf{c} \in \mathcal{C},\, \mathbf{c} \neq \mathbf{0}\}.$$

Lema 5.3.2. *Sea $\alpha = \theta^{\beta-1}$. La aplicación*

$$\begin{array}{rccc} \xi: & \alpha A^n & \longrightarrow & \mathbb{K} \\ & \alpha \cdot \mathbf{x} & \mapsto & \overline{\mathbf{x}} \end{array} \tag{5.23}$$

es un isomorfismo que preserva la distancia de Hamming.

La demostración del lema es obvia y se deja como ejercicio al lector.

Definición 5.3.5. *Llamaremos soporte minimal de un conjunto $S \subseteq A^n$ a aquellos elementos de S no nulos con soporte mínimo respecto a la inclusión. Lo denotaremos por* $\mathrm{Msop}(S)$.

Es claro que $\mathrm{d}(\mathcal{C}) = \mín\{|R| \mid R \in \mathrm{Msop}(\mathcal{C})\}$.

Teorema 5.3.4. *Sea $\mathcal{C}$ un código sobre el anillo de cadena A.*

1. $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}(\mathcal{C} \cap \theta^i\mathcal{C})$ *y* $\mathrm{d}(\mathcal{C}) = \mathrm{d}(\mathcal{C} \cap \theta^i\mathcal{C})$ *para* $0 \leq i \leq \beta - 1$.
2. $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}\left(\overline{(\mathcal{C} : \alpha)}\right)$ *y* $\mathrm{d}(\mathcal{C}) = \mathrm{d}\left(\overline{(\mathcal{C} : \alpha)}\right)$.
3. *Si* $\overline{\mathcal{C}} \neq \{\mathbf{0}\}$ *entonces* $\mathrm{d}(\mathcal{C}) \leq \mathrm{d}(\overline{\mathcal{C}})$.

Demostración.

1. Consideremos el código $\mathcal{D} = \mathcal{C} \cap \theta^{\beta-1}A^n$. Tomemos una palabra $\mathbf{c} \in \mathcal{C}$ tal que $\mathrm{sop}(\mathbf{c}) \in \mathrm{Msop}(\mathcal{C})$. Tenemos por lo tanto la siguiente cadena de inclusiones

   $$\mathrm{sop}(\mathbf{c}) \supseteq \mathrm{sop}(\theta\mathbf{c}) \supseteq \mathrm{sop}(\theta^2\mathbf{c}) \supseteq \cdots \supseteq \mathrm{sop}(\theta^{\beta-1}\mathbf{c}).$$

   Consideremos el índice j máximal tal que $\theta^j\mathbf{c} \neq 0$, entonces $\mathrm{sop}(\mathbf{c}) = \mathrm{sop}(\theta^j\mathbf{c})$ por la minimalidad de $\mathrm{sop}(\mathbf{c})$. Además $\theta^{j+1}\mathbf{c} = 0$ implica que $\theta^j\mathbf{c} \in \mathcal{D}$, como $\mathcal{D} \subset \mathcal{C}$ se sigue que $\mathrm{Msop}(\mathcal{C}) \subseteq \mathrm{Msop}(\mathcal{D})$.

   Sea ahora $\mathbf{c} \in \mathcal{D}$ con soporte minimal en $\mathrm{Msop}(\mathcal{D})$. Supongamos que no tenga soporte minimal en $\mathcal{C}$, es decir, existe $\mathbf{e} \in \mathcal{C}$ con

$\mathrm{sop}(\mathbf{c}) \supset \mathrm{sop}(\mathbf{e})$. Como $\mathrm{Msop}(\mathcal{C}) \subseteq \mathrm{Msop}(\mathcal{D})$ existe un elemento $\mathbf{e}' \in \mathcal{D}$ con $\mathrm{sop}(\mathbf{e}') = \mathrm{sop}(\mathbf{e}) \subset \mathrm{sop}(\mathbf{c})$ lo que es una contradicción.

Para $0 \leq j \leq \beta - 2$ simplemente aplicamos el resultado anterior al código $\mathcal{C} \cup \theta^j A^n$ considerando $\mathrm{Msop}(\mathcal{C}) = \mathrm{Msop}(\mathcal{C} \cap \theta^{\beta-1} A^n) = \mathrm{Msop}(\mathcal{C} \cap \theta^j A^n \cap \theta^{\beta-1} A^n) = \mathrm{Msop}(\mathcal{C} \cap \theta^j A^n)$.

2. Consideremos el isomorfismo ξ definido en el Lema 5.3.2. Se puede verificar fácilmente que $\mathcal{C} \cap \alpha A^n = \alpha(\mathcal{C} : \alpha)$ y por lo tanto $\xi(\mathcal{C} \cap \alpha A^n) = \overline{(\mathcal{C} : \alpha)}$ de donde se sigue el resultado.

3. Usándo el epígrafe anterior además de $\overline{\mathcal{C}} \neq \{\mathbf{0}\}$ y $\overline{(\mathcal{C}^j : \theta)} \subseteq \overline{(\mathcal{C}^{j+1} : \theta)}$ se tiene

$$\mathrm{d}(\mathcal{C}) = \mathrm{d}\left(\overline{(\mathcal{C} : \alpha)}\right) = \mathrm{d}\left(\overline{(\mathcal{C} : \theta^{\beta-1})}\right) \leq \mathrm{d}\left(\overline{(\mathcal{C} : \theta^{\beta-2})}\right) \leq \ldots$$

$$\cdots \leq \mathrm{d}\left(\overline{(\mathcal{C} : \theta^0)}\right) = \mathrm{d}\left(\overline{\mathcal{C}}\right).$$

■

5.3.4. Códigos cíclicos sobre anillos de cadena

Recordemos que un código es cíclico si es invariante bajo una permutación cíclica de sus coordenadas. Durante toda la sección asumiremos que la longitud del código n es coprima con la característica del anillo a utilizar de donde podemos deducir que el polinomio $x^n - 1$ tiene una descomposición única en el anillo $A[x]$. Utilizaremos para simplificar la notación A_n para denotar $A[x]/\langle x^n - 1\rangle$ y $\mathbb{K}_n$ para denotar a $\mathbb{K}[x]/\langle x^n - 1\rangle$. Claramente A_n y A^n son isomorfos como grupos abelianos con la suma ordinaria en ambos casos y es claro que un código de longitud n sobre A es cíclico si y sólo si se puede ver como un ideal en A_n. También es fácil de ver que si $\mathcal{C}$ es un código cíclico en A^n entonces $\overline{\mathcal{C}}$ es un código cíclico en $\mathbb{K}^n$, es más, los códigos

$$(\mathcal{C} : \theta^i), \qquad i = 0, 1, \ldots, \beta - 1$$

son también cíclicos.

Definición 5.3.6 (Conjunto de generadores en forma estándar)**.** *Diremos que el conjunto*

$$S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$$

es un conjunto de generadores en forma estándar para el código cíclico $\mathcal{C} = \langle S \rangle$ *si* $0 \leq s < \beta$ *y además*

1. $0 \leq a_0 < a_1 < \ldots < a_s < \beta$*;*
2. $g_{a_i} \in A[x]$ *es mónico para todo* $i = 0, 1, \ldots, s$*;*
3. $\deg(g_{a_i}) > \deg(g_{a_{i+1}})$ *para todo* $i = 0, 1, \ldots, s-1$*;*
4. $g_{a_s} | g_{a_{s-1}} | \ldots | g_{a_0} | x^n - 1$.

Lema 5.3.3. *Si* $\mathcal{C}$ *es un código cíclico no nulo entonces también lo es* $\overline{(\mathcal{C} : \theta^{\beta-1})}$.

Demostración. Consideremos $\mathbf{c} \in \mathcal{C}$ con $\mathbf{c} \neq \mathbf{0}$. Podemos escribir $\mathbf{c} = \theta^i \mathbf{u}$ con i maximal. Como $\mathcal{C}$ es un ideal entonces $\theta^{\beta-1}\mathbf{u} \in \mathcal{C}$, esto es $\mathbf{u} \in (\mathcal{C} : \theta^{\beta-1})$ y por lo tanto $\mathbf{0} \neq \overline{\mathbf{u}} \in \overline{(\mathcal{C} : \theta^{\beta-1})}$. ■

Lema 5.3.4. *Sea* $S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$ *un sistema de generadores del código cíclico* $\mathcal{C}$ *en forma estándar. Si* $i < a_0$ *entonces* $\overline{(\mathcal{C} : \theta^i)} = \{\mathbf{0}\}$*, en el resto de los casos* $\overline{(\mathcal{C} : \theta^i)} = \langle \overline{g_{a_j}} \rangle$ *donde* j *es maximal con la propiedad* $a_j \leq i$.

Demostración. Consideremos un elemento $\mathbf{c} \in \overline{(\mathcal{C} : \theta^i)}$. Entonces existe un $\mathbf{g} \in (\mathcal{C} : \theta^i)$ con $\overline{\mathbf{g}} = \mathbf{c}$. Como $\theta^i \mathbf{g} \in \langle S \rangle$ tenemos que se puede escribir de la forma

$$\theta^i \mathbf{g} = \sum_{k=0}^{s} h_{a_k} \theta^{a_k} g_{a_k}.$$

Esto es, si $i < a_0$ se tiene que

$$\mathbf{g} \equiv \sum_{k=0}^{s} h_{a_k} \theta^{a_k - i} g_{a_k} \mod \theta^{\beta-i},$$

de donde claramente $\mathbf{e} = \overline{\mathbf{g}} = \mathbf{0}$.

En el resto de los casos consideremos el índice j maximal tal que $a_j \leq i$. Como se tiene que $g_{a_s}|g_{a_{s-1}}|\dots|g_{a_0}$, existe un $h \in A[x]$ con

$$\theta^i \mathbf{g} = h g_{a_j} + \sum_{k=j+1}^{s} h_{a_k} \theta^{a_k} g_{a_k}.$$

Como g_{a_j} es mónico y la parte izquierda de la ecuación y el sumatorio son divisibles por θ^i, también lo debe ser h, esto es $h = \theta^i t$. Por lo tanto $\mathbf{e} = \overline{\mathbf{g}} = \overline{t}\overline{g_{a_j}}$ y tenemos $\overline{(\mathcal{C} : \theta^i)} \subseteq \langle \overline{g_{a_j}} \rangle$. La contención restante es inmediata. ∎

Como vimos en el capítulo anterior, para cada divisor $f|x^n - 1 \in \mathbb{K}[x]$ existe un polinomio único en $g \in A[x]$ con $\overline{g} = f$ y $g|x^n - 1$ pues $x^n - 1$ es libre de cuadrados. A dicho g le llamaremos (polinomio) *levantamiento de Hensel* de f.

Teorema 5.3.5. *Un código cíclico no nulo tiene un único conjunto generador en forma estándar.*

Demostración. Utilizando el Lema 5.3.3 tenemos que $\overline{(\mathcal{C} : \theta^{\beta-1})} \neq \{\mathbf{0}\}$ y podemos considerar el entero s maximal con la propiedad de que las inclusiones

$$\{\mathbf{0}\} \subset \overline{(\mathcal{C} : \theta^{a_0})} \subset \overline{(\mathcal{C} : \theta^{a_1})} \subset \cdots \subset \overline{(\mathcal{C} : \theta^{a_s})}$$

sean extrictas.
Como $\mathcal{C}$ es cíclico también lo son (sobre $\mathbb{K}$) cada uno de los códigos en la cadena considerada. Tomemos $f_{a_j} \in A[x]$ un polinomio mónico con $\theta^{a_j} f_{a_j} \in \mathcal{C}$ tal que $\overline{f_{a_j}}$ sea el único generador mónico de $\overline{(\mathcal{C} : \theta^{a_j})}$, y tomemos como g_{a_j} el levantamiento de Hensel de $\overline{f_{a_j}}$. Claramente $S = \{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \dots, \theta^{a_s} g_{a_s}\}$ es un conjunto de generadores en forma estándar de un código cíclico $\mathcal{D} = \langle S \rangle$.
Ahora hemos de comprobar que $\mathcal{C} = \mathcal{D}$. Como $\overline{f_{a_j}} = \overline{g_{a_j}}$ existen $h_{a_j} \in A[x]$ con la propiedad

$$\theta h_{a_j} = f_{a_j} - g_{a_j}.$$

Consideremos los polinomios $v_{a_j} = x^n - 1/g_{a_j}$, entonces en $A[x]/\langle x^n - 1 \rangle$ se tiene la identidad

$$\theta^{a_j} f_{a_j} v_{a_j} = \theta^{a_j}(g_{a_j} + \theta h_{a_j}) v_{a_j} = \theta^{a_j+1} h_{a_j} v_{a_j}.$$

Por lo tanto $\theta^{a_j+1}h_{a_j}v_{a_j} \in \mathcal{C}$ y además claramente $\overline{v_{a_j}}$ y $\overline{f_{a_j}}$ son coprimos. Aplicando el Lema 4.4.4 también lo son v_{a_j} y f_{a_j}, es decir, existen u, v tales que $v_{a_j}v + f_{a_j}u = 1$. Es decir

$$\theta^{a_j+1}h_{a_j} = \theta^{a_j+1}h_{a_j}v_{a_j}v + \theta^{a_j+1}h_{a_j}f_{a_j}u$$

de donde $\theta^{a_j+1}h_{a_j} \in \mathcal{C}$ pues $\theta^{a_j+1}h_{a_j}v_{a_j}, \theta^{a_j}f_{a_j} \in \mathcal{C}$. El elemento

$$\theta^{a_j}g_{a_j} = \theta^{a_j}f_{a_j} - \theta^{a_j+1}h_{a_j}$$

pertenece a $\mathcal{C}$ y hemos probado $\mathcal{D} \subseteq \mathcal{C}$.
Tomemos ahora f_{a_j} con $\overline{(\mathcal{C} : \theta^i)} = \langle \overline{f_{a_j}} \rangle = \langle \overline{g_{a_j}} \rangle$ para $a_j \leq i < a_{j+1}$. Por el Lema 5.3.4 se tiene $\overline{(\mathcal{D} : \theta^i)} = \langle \overline{g_{a_j}} \rangle$ para $a_j \leq i < a_{j+1}$ de donde

$$\overline{(\mathcal{D} : \theta^i)} = \overline{(\mathcal{C} : \theta^i)}, \quad i = 0, 1, \ldots, \beta - 1,$$

y se sigue $\mathcal{C} = \mathcal{D}$ pues implica $k_i(\mathcal{C}) = k_i(\mathcal{D})$.
Para demostrar la unicidad consideremos que tenemos otro conjunto generador para $\mathcal{C}$ dado por $\{\theta^{b_0}h_{b_0}, \theta^{b_1}h_{b_1}, \ldots, \theta^{b_t}h_{b_t}\}$ tal que está en forma estándar. Considerando el Lema 5.3.4 y como $\overline{h_{b_{j+1}}}$ es un divisor extricto de $\overline{h_{b_j}}$ tenemos que las inclusiones

$$\{\mathbf{0}\} \subset \overline{(\mathcal{C} : \theta^{b_0})} \subset \overline{(\mathcal{C} : \theta^{b_1})} \subset \cdots \subset \overline{(\mathcal{C} : \theta^{b_t})}$$

sean extrictas y t es maximal. Por lo tanto $t = s$ y $b_j = a_j$ para $j = 0, 1, \ldots, s$. Además $\overline{(\mathcal{C} : \theta^{b_j})} = \langle \overline{h_{b_j}} \rangle = \langle \overline{g_{b_j}} \rangle$, y $\overline{g_{b_j}} = \overline{h_{b_j}}$ pues son divisores mónicos de $x^n - 1$ y por lo tanto sus levantamientos de Hensel cumplen $g_{b_j} = h_{b_j}$. ■

El siguiente teorema nos muestra cómo obtener la matriz generatriz de un código cíclico sabiendo su sistema de generadores en forma estándar.

Teorema 5.3.6. *Sea $S = \{\theta^{a_0}g_{a_0}, \theta^{a_1}g_{a_1}, \ldots, \theta^{a_s}g_{a_s}\}$ un sistema de generadores en forma estándar del código cíclico $\mathcal{C}$.*

1. *Consideremos*

$$T = \bigcup_{i=0}^{s} \left\{ \theta^{a_i}g_{a_i}x^{d_{i-1}-d_i-1}, \ldots, \theta^{a_i}g_{a_i}x,\ \theta^{a_i}g_{a_i} \right\}$$

con $d_i = \deg(g_{a_i})$ para $i = 1, \ldots, s$ y $d_{-1} = n$, $d_{s+1} = 0$. El conjunto T define una matriz generatriz del código $\mathcal{C}$.

2. *Cualquier palabra del código* $\mathbf{c} \in \mathcal{C}$ *puede ser escrita de forma única como*

$$\mathbf{c} = \sum_{j=0}^{s} h_j g_{a_j} \theta^{a_j}$$

con $h_j \in (A/A\theta^{\beta-a_j})[x] \cong A\theta^{a_j}[x]$ *y* $\deg(h_j) < d_{j-1} - d_j$.

3. $k_i(\mathcal{C}) = d_{j-1} - d_j$ *si* $i = a_j$ *para algún* j *y* $k_i(\mathcal{C}) = 0$ *en el resto de los casos. Además*

$$|\mathcal{C}| = |\mathbb{K}|^{\sum_{j=0}^{s}(\beta-a_j)(d_{j-1}-d_j)}.$$

La demostración se deja como ejercicio para el lector así como la de las siguientes dos proposiciones.

Proposición 5.3.3. *El dual de un código cíclico es también cíclico.*

Definición 5.3.7. *Sea* $f \in A[x]$ *un polinomio no nulo. Llamaremos polinomio recíproco de* f *a*

$$f^\star = x^{\deg(f)} f\left(\frac{1}{x}\right).$$

Si el termino constante f_0 *de* f *es una unidad definimos*

$$f^\sharp = \frac{f^\star}{f_0}.$$

Proposición 5.3.4. *Sea* $\{\theta^{a_0} g_{a_0}, \theta^{a_1} g_{a_1}, \ldots, \theta^{a_s} g_{a_s}\}$ *un sistema de generadores en forma estándar del código cíclico* $\mathcal{C}$. *Definamos* $a_{s+1} = \beta$ *y* $g_{a_{-1}} = x^n - 1$. *Para* $j = 0, 1, \ldots, s+1$ *definamos* $b_j = \beta - a_{s+1-j}$ *y*

$$h_{b_j} = \left(\frac{x^n - 1}{g_{a_{s-j}}}\right)^\sharp.$$

Entonces $\{\theta^{b_0} h_{b_0}, \theta^{b_1} h_{b_1}, \ldots, \theta^{b_{s+1}} h_{b_{s+1}}\}$ *un sistema de generadores en forma estándar del código cíclico* $\mathcal{C}^\perp$.

Definición 5.3.8. *Sea* $f \in \mathbb{K}[x]$ *un polinomio mónico con* $f | x^n - 1$. *El código cíclico* $\mathcal{C} = \langle g \rangle$ *donde* g *el el levantamiento de Hensel de* f *se llama levantamiento de Hensel del código (cíclico)* $\langle f \rangle$.

Nótese que si $\mathcal{C}$ es el levantamiento de Hensel de $\mathcal{E}$ entonces $\overline{\mathcal{C}} = \mathcal{E}$ pero no es el único código cíclico cuya proyección es $\mathcal{E}$. El siguiente resultado es inmediato.

Proposición 5.3.5. *Sea $\mathcal{C}$ un código sobre el anillo A. Los siguientes enunciados son equivalentes:*

1. *$\mathcal{C}$ es el levantamiento de Hensel de un código cíclico.*
2. *$\mathcal{C}$ es cíclico y libre.*
3. *Existe un $g \in A[x]$ con $g|x^n - 1$ y $\mathcal{C} = \langle g \rangle$.*
4. *Existe un $g \in A[x]$ mónico tal que $\{g\}$ es un sistema de generadores en forma estándar del código $\mathcal{C}$.*
5. *$\mathcal{C}^{\perp}$ es el levantamiento de Hensel de un código cíclico.*

Definición mediante raíces de la unidad

Análogamente al caso de códigos cíclicos sobre cuerpos finitos podemos definir los códigos cíclicos haciendo uso de las raíces enésimas de la unidad en una extensión de anillos adecuada cuando A es un anillo de Galois (la construcción también es posible en el caso general de un anillo de cadena, véasen las referencias en el Apéndice). Si tomamos $A = GR(p^{al}, p^a)$ y m un entero positivo tal que $l|m$ y $n|p^m - 1$, el anillo $GR(p^{am}, p^a)$ es una extensión de A en la que $x^n - 1$ tiene n raíces. Podemos levantar una raíz primitiva de la unidad en el cuerpo finito $\mathbb{F}_{p^m}$ a una raíz ξ de $x^n - 1$ en el anillo $GR(p^{am}, p^a)$ que también será primitiva. Para cada elección de $i = 0, 1, \ldots, n-1$ denotaremos por $m_i(x)$ al polinomio mínimo de $\overline{\xi^i}$ en $\mathbb{F}_{p^l}[x]$. Si denotamos por U un conjunto de representantes de las clases de conjugación de $\overline{\xi}$ es bien conocido que

$$x^n - 1 = \prod_U m_i(x).$$

Denotaremos por $M_i(x) \in A[x]$ al levantamiento de Hensel de $m_i(x)$ para cada $i = 1, 2, \ldots, n-1$. Claramente los polinomios $M_i(x)$ son básicos irreducibles, además tienen las siguientes propiedades.

Lema 5.3.5. *Con la notación del párrafo anterior se tiene*

1. *Para cada* $i = 1, 2, \ldots, n-1$

$$\{j \in \{1, \ldots, n-1\} \mid M_i(\xi^j) = 0\} = \{j \in \{1, \ldots, n-1\} \mid m_i(\overline{\xi^j}) = 0\}.$$

2. *Para cada* $i = 1, 2, \ldots, n-1$ $M_i(x)$ *es el polinomio mínimo de* ξ^i.

3. U *un conjunto de representantes de las clases de conjugación de* ξ *en el anillo* $GR(p^{am}, p^a)$.

4. *Sean* $f \in A[x]$ *y* $\{i_1, \ldots, i_v\} \subseteq U$. *Si* $f(\xi^{i_j}) = 0$ *para* $j = 1, \ldots, v$ *entonces*

$$\left(\prod_{j=1}^{v} M_{i_j}(x) \right) | f.$$

5. *Sea* $f \in A[x]$ *con* $f | x^n - 1$ *y* $L \subseteq U$. *Entonces* $f = \prod_{i \in L} M_i(x)$ *si y sólo si* $L = \{i \in U | f(\xi^i) = 0\}$.

6. *Para* $k = 1, \ldots, a-1$,

$$M_i(x) \mod p^k \in (A/p^k A)[x] \cong GR(p^{kl}, p^k)[x]$$

es el polinomio mínimo de ξ^i *módulo* p^k.

La demostración del lema anterior se deja como ejercicio al lector. La formulación en el lema nos permite para un conjunto de raíces $\{\xi^{i_1}, \ldots, \xi^{i_k}\}$ definir el código cíclico

$$\mathcal{C} = \{\mathbf{c} \in A_n \mid \mathbf{c}(\xi^{i_j}) = 0,\ j = 1, \ldots, k\}.$$

Por lo tanto, de forma análoga al caso de cigos cíclicos sobre cuerpos finitos y forzando la definición podemos considerar la matriz de paridad para $\mathcal{C}$ la matriz de tipo Vandermonde

$$H = \begin{pmatrix} 1 & \xi^{i_1} & \xi^{2i_1} & \ldots & \xi^{(n-1)i_1} \\ 1 & \xi^{i_2} & \xi^{2i_2} & \ldots & \xi^{(n-1)i_2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi^{i_k} & \xi^{2i_k} & \ldots & \xi^{(n-1)i_k} \end{pmatrix}.$$

Combinando los resultados del Lema 5.3.5 y la noción de conjunto generador estándar de un código cíclico obtenemos el siguiente resultado.

Teorema 5.3.7. *Sea U un conjunto de representantes de las clases de conjugación de las raíces de $x^n - 1$ en A y $\mathcal{C}$ un submódulo de A^n. El submódulo $\mathcal{C}$ es un código cíclico si y sólo si existen enteros no negativos $0 \leq a_0 < \ldots < a_s < a_{s+1} = a$ y una partición $\{L_{a_j} \mid j = 0, \ldots, s+1\}$ del conjunto U tal que*

$$\mathcal{C} = \{\mathbf{c} \in A_n \mid p^{a-a_j}\mathbf{c}(\xi^{i_j}) = 0,\, i_j \in L_{a_j},\, j = 0, \ldots, s+1\}.$$

5.4. Los códigos Kerdock y Preparata

Finalizaremos el texto con un pequeño apunte sobre la $\mathbb{Z}_4$ linealidad de los códigos binario clásicos de Kerdock, uno de los hitos fundamentales para el desarrollo de la codificación algebraica sobre anillos. El vehículo mediante el cuál a partir de códigos $\mathbb{Z}_4$-lineales se obtienen códigos binarios es la *aplicación de Gray* dada por

$$\begin{array}{rccc} \mathfrak{G}: & \mathbb{Z}_4 & \longrightarrow & \mathbb{F}_2^2 \\ & 0 & & \mathfrak{G}(0) = 00 \\ & 1 & & \mathfrak{G}(1) = 01 \\ & 2 & & \mathfrak{G}(2) = 11 \\ & 3 & & \mathfrak{G}(3) = 10 \end{array} \tag{5.24}$$

La aplicación de Gray no es lineal y define una métrica (métrica de Lee) sobre $\mathbb{Z}_4$ dada por el peso $w_L(x) = w_H(\mathfrak{G}(x))$ para cada $x \in \mathbb{Z}_4$, donde w_H denota el peso de Hamming. La métrica de Lee se extiende de manera natural a $\mathbb{Z}_4^n$ coordenada a coordenada.
Consideremos $h(x)$ un polinomio básico irreducible de grado r en $\mathbb{Z}_4[x]$. Sea $f(x)$ el polinomio recíproco de

$$\frac{x^n - 1}{(x-1)h(x)}.$$

Definimos $K(r+1)$ el código cíclico de longitud $2^r - 1$ sobre $\mathbb{Z}_4$ generado por $f(x)$. Notaremos por $\hat{K}(r+1)$ al código que se obtiene al añadir un dígito de paridad $K(r+1)$. El *código de Kerdock* se define como su imagen mediante la aplicación de Gray, es decir $\mathcal{K}(r+1) = \mathfrak{G}(\hat{K}(r+1))$. Es un código de longitud 2^{r+1} con 4^{r+1} palabras. Se puede demostrar que mediante un simple reordenamiento de las coordenadas de las palabras

se obtiene la definición original del código de Kerdock que se puede encontrar por ejemplo en [5].
Para $r \geq 3$ e impar, si tomamos $P(r+1) = \hat{K}(r+1)^{\perp}$ como códigos sobre $\mathbb{Z}_4$ y consideramos su imagen mediante la aplicación de Gray $\mathcal{P}(r+1) = \mathfrak{G}(P(r+1))$ obtenemos los códigos de tipo Preparata.
Un estudio más exhaustivo de los códigos de Kerdock y Preparata a nivel elemental se puede encontrar en el texto [3].

Apéndice: Lecturas avanzadas: códigos sobre anillos

Esbozaremos en este anexo unas breves y sesgadas notas para el lector interesado en proseguir por su cuenta el estudio de algunos aspectos de los códigos sobre anillos finitos.

§ La construcción mostrada en el texto de códigos cíclicos ha sido generalizada al caso abeliano (y polinomial en general) tanto para el caso de raíces simples como con multiplicidad de ellas sobre anillos de cadena. Resultados en esta dirección se pueden encontrar en [26, 27, 23].

§ Como hemos comentado durante el texto, el trabajo [19], que mostró que algunos códigos óptimos no lineales podían ser vistos como la imagen mediante la aplicación de Gray de códigos $\mathbb{Z}_4$ lineales, supuso una nueva línea de investigación en la codificación algebraica. Recientemente varios tipos de códigos han sido propuestos para corregir errores en un ambiente de computación cuántica. La mayoría de este tipo de códigos se basan en la relación de los códigos cuánticos con ciertos códigos aditivos sobre $\mathbb{F}_4$ [15]. Construcciones polinomiales de este tipo de códigos se pueden encontrar en [22, 24]. También es bien conocido que los códigos cuánticos no aditivos tienen mayor dimensión comparados con su contraparte cuántica aditiva de igual distancia mínima [28]. Se han propuesto varias familias de códigos cuánticos no aditivos basados en los códigos bina-

rios de Goethals y Preparata [18]. Estos códigos binarios son ejemplos clásicos de códigos $\mathbb{Z}_4$ lineales, propiedad que ha sido generalizada a linealidad en anillos de Galois en [21].
En resumen, parece que es lógico preguntarse sobre la estructura de los códigos (tanto clásicos como aditivos) sobre anillos finitos. La clase de anillos más amplia que nos permite tener una dualidad coherente con la transformada de McWilliams, y por lo tanto aquella en la que la teoría de códigos algebraica se refleja al completo, es la de los anillos de Frobenius (véase [29]) por lo tanto es donde es deseable trabajar.

§ Por otra parte es fácil de comprobar que el estudio de códigos lineales sobre anillos finitos con la condición de Frobenius se reduce (mediante una aplicación directa del teorema chino de los restos) al estudio de los anillos finitos con la condición de Frobenius locales. Estos anillos pueden ser fácilmente caracterizados como aquellos que tienen un socle simple. Varios ejemplos denominados clases R_k and S_k y las aplicaciones de Gray relacionadas con ellas han sido propuestos en los trabajos de Dougherty et al. (véase por ejemplo [16, 17, 20]). También recientemente se ha realizado una primera clasificación de los anillos finitos con la condición de Frobenius locales con 16 elementos y sus posibles aplicaciones de Gray asociadas [25].

Bibliografía general

[1] M. Atiyah, I.G. Macdonald *Introducción al Algebra Conmutativa* Reverté, Barcelona (1973).

[2] G. Bini and F. Flamini *Finite Commutative Rings and Their Applications*. Kluwer Academic Publishers (2002).

[3] W. Cary Huffman, Vera Pless *Fundamentals of error-correcting codes.*. Cambridge University Press (2003).

[4] Thomas W. Hungerford *Algebra*. Springer-Verlag New York Inc. (1974).

[5] F.J. MacWilliams, N.J.A. Sloane *The theory of error-correcting codes*. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co. (1977).

[6] Bernard R. McDonald *Finite Rings With Identity*. Marcel Dekker Incorporated (1974).

[7] Bernard R. McDonald *Linear algebra over commutative rings*. Monographs and Textbooks in Pure and Applied Mathematics, 87. Marcel Dekker, Inc., New York, (1984).

[8] Gary L. Mullen, Daniel Panario *Handbook of Finite Fields*. Series: Discrete Mathematics and Its Applications, Chapman and Hall/CRC (2013).

[9] R. Lidl, H. Niederreiter *Introduction to Finite Fields and their applications.* Cambridge University Press (1986).

[10] G.H. Norton, A. Sălăgean *On the structure of linear and cyclic codes over a finite chain ring.* Applicable Algebra in Engineering, Communication and Computing 10 (6), 489-506 (2000)

[11] G.H. Norton, A. Sălăgean *On the Hamming distance of linear codes over a finite chain ring.* IEEE Transactions on Information Theory, 46 (3), 1060-1067 (2000)

[12] Edgar Martínez-Moro, Carlos Munuera-Gómez y Diego Ruano-Benito *Bases de Gröbner: aplicaciones a la codificación algebraica.* Escuela Venezolana de Matemáticas (2007).

[13] Alexandr A. Nechaev Finite rings with applications. In *Handbook of algebra. Vol. 5*, volume 5 of *Handb. Algebr.*, pages 213–320. Elsevier/North-Holland, Amsterdam (2008).

[14] Zhe-Xian Wan Finite Fields And Galois Rings. World Scientific Publishing Company (2011)

Otras referencias

[15] A. R. Calderbank, E. Rains, P. W. Shor, and N. J. A. Sloane. *Quantum error correction via codes over GF(4)*, IEEE Transactions on Information Theory. 44(4), 1369-1387. (1998)

[16] Dougherty, Steven T.; Karadeniz, Suat; Yildiz, Bahattin. *Cyclic codes over R_k*. Des. Codes Cryptogr. 63 (2012), no. 1, 113–126.

[17] Dougherty, Steven; Yildiz, Bahattin; Karadeniz, Suat. *Self-dual codes over R_k and binary self-dual codes*. Eur. J. Pure Appl. Math. 6 (2013), no. 1, 89–106.

[18] M. Grassl, M. Rötteler. *Non-Additive Quantum Codes from Goethals and Preparata Codes* CoRR abs/ 0801.2144: (2008)

[19] A. R. Hammons Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole. *The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes*, IEEE Trans. Information Theory, 40 (1994), pp. 301-319, Also DIMACS Technical Report 93-52, August 1993.

[20] Karadeniz, Suat; Dougherty, Steven T.; Yildiz, Bahattin. *Constructing formally self-dual codes over R_k*. Discrete Appl. Math. 167 (2014), 188–196.

[21] Kuzmin, Markov, Nechaev, Neljubin. *A generalization of the binary Preparata code*. International Workshop on Coding and Cryptography no.3, Versailles. (2006).

[22] Martínez-Moro, E.; Piñera-Nicolás, A.; Rúa, I. F. *Additive semisimple multivariable codes over* $\mathbb{F}_4$. Des. Codes Cryptogr. 69 (2013), no. 2, 161–180.

[23] Martínez-Moro, E.; Nicolás, A. P.; Rua, I. F. *On trace codes and Galois invariance over finite commutative chain rings*. Finite Fields Appl. 22 (2013), 114–121.

[24] Martínez-Moro, E.; Nicolás, A. P.; Rúa, I. F. *On additive modular bivariate codes over* $\mathbb{F}_4$. Finite Fields Appl. 28 (2014), 199–213.

[25] Martínez-Moro, E.; Szabo, S. *On codes over non chain local Frobenius rings with 16 elements*. Accepted in Communications in Mathematics. AMS. To appear.

[26] Martínez-Moro, E.; Rúa, I. F. *Multivariable codes over finite chain rings: serial codes*. SIAM J. Discrete Math. 20 (2006), no. 4, 947–959.

[27] Martínez-Moro, E.; Rúa, I. F. *On repeated-root multivariable codes over a finite chain ring*. Des. Codes Cryptogr. 45 (2007), no. 2, 219–227.

[28] E. M. Rains, R. H. Hardin, P. Shor and N. J. A. Sloane. *A nonadditive quantum code*, Phys. Rev. Lett., Vol. 79, pp. 953–954 (1997).

[29] Wood, Jay A. *Duality for modules over finite rings and applications to coding theory*. Amer. J. Math. 121 (1999), no. 3, 555–575.

La Asociación Matemática Venezolana fue fundada en 1990 como una organización civil sin fines de lucro cuya finalidad es trabajar por el desarrollo de las matemáticas en Venezuela.

Asociación Matemática Venezolana
Apartado 47.898, Caracas 1041-A, Venezuela
`http://www.ciens.ucv.ve/ciens/amv/`

Gobierno **Bolivariano** de Venezuela

Ministerio del Poder Popular para **Ciencia, Tecnología e Innovación**

juventud BICENTENARIA