UNIVERSIDAD NACIONAL DE CÓRDOBA

FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

SERIE " C "

TRABAJOS DE MATEMATICA

Nº 38/10

V Encuentro Nacional de Álgebra

Notas de Cursos

9 al 14 de agosto de 2010, La Falda, Sierras de Córdoba

Antonio Behn - Lisi D'Alfonso - Fernando Fantino - Iván Pan
Pablo A. Panzone - Linda Saal - Diego Sulca - Paulo Tirao

Editores: Jorge R. Lauret – Jorge Adrover

CIUDAD UNIVERSITARIA – 5000 CÓRDOBA

REPÚBLICA ARGENTINA

La presente publicación fue financiada por el CIEM con fondos del CONICET, CCT-Cba.

Prefacio

Los Encuentros Nacionales de Álgebra vienen realizándose en las Sierras de Córdoba, periódicamente y con gran éxito, desde que en 2003 tuvo lugar el primero. El segundo Encuentro *elENA II* se realizó en 2004 y a partir de éste se hicieron en forma bianual: *elENA III* (2006) y *elENA IV* (2008).

El *Quinto Encuentro Nacional de Algebra elENA V*, se llevará a cabo durante los días 9 al 14 de agosto de 2010, en el Hotel del Lago, la Falda, Sierras de Córdoba, con la presencia de numerosos matemáticos del país y también del extranjero. Por ejemplo, esperamos contar con la grata presencia de representantes de universidades y centros de Uruguay, Chile, Paraguay, Brasil, España, Francia y los Estados Unidos.

Asimismo, se prevé la asistencia de muchos alumnos de Licenciatura, Maestría y Doctorado en Matemáticas de todo el país y también del Uruguay.

En nombre del Comité Académico y del Comité Organizador, respectivamente, nos es grato poner aquí a disposición de los asistentes a dichos cursos, y del ocasional lector, las notas de 7 de los 9 cursos dictados en dicho encuentro. Aprovechamos esta oportunidad para agradecer a todos los cursistas por preparar sus cursos y muy especialmente a aquellos que se han tomado el enorme trabajo de escribir estas notas con antelación, para que estén disponibles al momento del encuentro. Éstas representan sin duda una gran ayuda para el seguimiento y mejor aprovechamiento de los cursos por parte de los asistentes.

Nicolás Andruskiewitsch Ricardo Podestá

Córdoba, 2 de agosto de 2010.

Contenidos

Cursos para Estudiantes

Cursos Intermedios

Cursos Avanzados

Cursos para Estudiantes

ÁLGEBRA DIFERENCIAL

LISI D'ALFONSO

RESUMEN. En estas notas introducimos nociones básicas de algebra diferencial. En particular presentamos el Teorema del Elemento Primitivo Diferencial y lo aplicamos para dar una descripción alternativa de ciertos sistemas de ecuaciones diferenciales ordinarias polinomiales.

ÍNDICE

INTRODUCCIÓN

Las ecuaciones diferenciales han demostrado ser una herramienta de gran utilidad en una amplia variedad de áreas como la ingeniería, la biología o la química. Un tratamiento frecuente para la resolución numérica (o no) de sistemas de ecuaciones diferenciales consiste en transformar el sistema en otro equivalente pero de manejo más sencillo para luego encontrar las soluciones de este nuevo sistema.

Es natural pensar en modificar el sistema de ecuaciones diferenciales por medio de manipulaciones puramente algebraicas y derivaciones de las ecuaciones involucradas. El conjunto de *todas* las ecuaciones que pueden ser obtenidas de este modo (y que van a ser verificadas por todas las soluciones del sistema) forman un ideal que se llama el *ideal diferencial* asociado al sistema y el punto clave es encontrar una descripción "simple" de este ideal. Esta idea fue una de las motivaciones del desarrollo del álgebra diferencial iniciada por J.F. Ritt [10] y continuada por E.R. Kolchin [4].

En este contexto una noción importante es la de *representación resolvente* de un ideal diferencial primo en un anillo de polinomios diferenciales. Tal noción fue introducida

Financiación: UBACyT X211 (2008-2010) y ANPCyT PICT2007-816.

Agradecimientos: a Gabriela Jeronimo y a Pablo Solernó por su colaboración para escribir estas notas.

por Ritt (ver [10, 9]) como una herramienta dirigida hacia una teoría de eliminación algebraica en el marco de las ecuaciones diferenciales, aunque sus inicios (desde el punto de vista de la geometría algebraica) pueden encontrarse ya en los trabajos de Kronecker (ver [5]). A grandes rasgos, una *representación resolvente* de un ideal diferencial primo provee una parametrización de los ceros del ideal por medio de los ceros de un único polinomio diferencial irreducible. Este fenómeno es bastante general y puede ser interpretado en varios contextos, a priori diversos: la existencia del elemento primitivo de extensiones de cuerpos separables o de un vector cíclico en sistemas diferenciales lineales de primer orden, así también como el "shape lemma" en el ámbito de la geometría algebraica o analítica son ejemplos de "representaciones resolventes".

En estas notas daremos los principales resultados básicos del álgebra diferencial (Sección 1). En la Sección 2 presentamos la existencia del Elemento Primitivo siguiendo Seidenberg. Finalmente, en la Sección 3 se utiliza la construcción del elemento primitivo para deducir la existencia de una representación resolvente "a la Ritt" con las características descriptas arriba.

Las notas se complementan con ejercicios adicionales presentados con el objeto de ayudar al lector la comprensión de las distintas nociones presentadas y la resolución de los mismos es independiente de la lectura de las mismas.

1. Preliminares

El objetivo de este curso es el estudio, desde un punto de vista algebraico, de cierto tipo de sistemas de ecuaciones diferenciales ordinarias en las que las ecuaciones están dadas por polinomios en las variables incógnitas y sus derivadas (a las que consideraremos como variables independientes) y con coeficientes en un cuerpo diferencial arbitrario que contenga a $\mathbb{Q}$. A estas ecuaciones las llamaremos *ecuaciones diferenciales algebraicas* o, brevemente, DAE.

Ejemplo 1.1. Si z es una variable compleja, la ecuación en X y sus derivada dada por

$$z^2(\delta^2 X)^3 - \operatorname{sen}(z)X^2 + e^z = 0$$

es una DAE dada por un polinomio en las variables $X, \delta X, \delta^2 X$ y con coeficientes en el cuerpo de funciones meromorfas en la variable z.

Ejemplo 1.2. Por otro lado, en el mismo contexto del Ejemplo 1.1, la ecuación

$$z^2(\delta^2 X)^3 - z^2 \operatorname{sen}(X) + e^z = 0$$

no es una DAE.

Sin embargo, agregando una nueva variable $Y = \operatorname{sen}(X)$, derivando dos veces, vemos que Y satisface la ecuación $\delta X \delta^2 Y + Y(\delta X)^3 - \delta Y \delta^2 X = 0$. Tenemos entonces que las soluciones de la ecuación original son algunas de las soluciones del sistema de DAEs:

$$\begin{cases} z^2(\delta^2 X)^3 - z^2 Y + e^z & = & 0 \\ \delta X \delta^2 Y + Y(\delta X)^3 - \delta Y \delta^2 X & = & 0 \end{cases}$$

Este último ejemplo muestra que el tipo de ecuaciones que estamos considerando no es tan restrictivo como parece.

En este curso nos concentraremos en algunos resultados sobre extensiones de cuerpos diferenciales, que pueden considerarse como versiones diferenciales de resultados clásicos del álgebra conmutativa y de la teoría de extensiones de cuerpos, que nos permitirán manipular y simplificar los sitemas DAEs dados.

Aunque en este curso solo consideraremos sistemas de ecuaciones diferenciales ordinarios (es decir, con derivada respecto de una única variable), muchas de las nociones y propiedades introducidas pueden extenderse a sistemas de ecuaciones en derivadas parciales.

1.1. Definiciones básicas.

Sea R un anillo conmutativo. Una derivación sobre R es una aplicación $\delta : R \to R$ tal que para cada $a, b \in R$ se verifica

- $\delta(a+b) = \delta(a) + \delta(b)$
- $\delta(a \cdot b) = \delta(a) \cdot b + a \cdot \delta(b)$

Nos referiremos al par (R, δ) como un *anillo diferencial ordinario.*

El anillo (R, δ) es un *dominio diferencial* (respectivamente, un *cuerpo diferencial*) si es un dominio íntegro, es decir si $a \cdot b = 0$ implica que $a = 0$ ó $b = 0$ (resp. un cuerpo).

Si (K, δ) es un cuerpo diferencial y $a, b \in K, a \neq 0$, tenemos que

$$\delta(b) = \delta\left(\frac{a \cdot b}{a}\right) = a \cdot \delta\left(\frac{b}{a}\right) + \delta(a) \cdot \frac{b}{a}$$

y, por lo tanto

$$\delta\left(\frac{b}{a}\right) = \frac{a\delta(b) - \delta(a)b}{a^2}.$$

Así, si K es el cuerpo de fracciones de un dominio diferencial (R, δ), K resulta un cuerpo diferencial con la derivación usual del cociente. Más aún, como $\delta(1) = \delta(1 \cdot 1) = 1 \cdot \delta(1) + \delta(1) \cdot 1$, tenemos que $\delta(1) = 0$ y que la derivada en R coincide con la derivada en K para todos los elementos de R.

Ejemplo 1.3. Ejemplos de anillos diferenciales

1. Cualquier anillo R puede ser considerado un anillo diferencial con la derivación trivial $\delta : R \to R$ dada por $\delta(r) = 0$ para todo $r \in R$.
2. El anillo de todas las funciones $\mathcal{C}^\infty$ en una variable t sobre $\mathbb{R}$ es un anillo diferencial ordinario con $\delta = \frac{d}{dt}$ pero no es un dominio. (Ver Ejercicio 1).
3. El anillo de todas las funciones enteras en la variable compleja z, es decir, holomorfas en $\mathbb{C}$, es un dominio diferencial con $\delta = \frac{d}{dz}$. Su cuerpo de fracciones es el cuerpo diferencial de todas las funciones meromorfas. (Ver Ejercicio 1).
4. *El anillo de polinomios diferenciales.*

   Sea (K, δ) un cuerpo diferencial ordinario que contiene a los números racionales. Por ejemplo $K = \mathbb{Q}, \mathbb{R}$ ó $\mathbb{C}$ con $\delta := 0$, ó $K = \mathbb{Q}(t), \mathbb{R}(t)$ ó $\mathbb{C}(t)$ con la derivación usual $\delta(t) = 1$, etc.

   Si $X_1, \ldots, X_n$ es un conjunto arbitrario de indeterminadas diferenciales sobre K (es decir, $X_1, \ldots, X_n, \delta X_1, \ldots, \delta X_n, \ldots$ son algebraicamente independientes sobre K) por comodidad, denotamos $X_j^{(p)}$ a la p-ésima derivada sucesiva de X_j $(j = 1, \ldots, n)$ y escribimos $\dot{X}_j$ para designar a la derivada primera, o sea $\dot{X}_j = \delta(X_j)$, y $X_j^{(0)} = X_j$. Además, usaremos las notaciones $X := \{X_1, \ldots, X_n\}$, $X^{(p)} := \{X_1^{(p)}, \ldots, X_n^{(p)}\}$ y $X^{[p]} := \{X^{(i)},\ 0 \leq i \leq p\}$.

   El anillo de polinomios en infinitas variables $K[X^{(p)},\ p \in \mathbb{N}_0]$, se llama el *anillo de polinomios diferenciales* en las variables X y se lo denota por $K\{X_1, \ldots, X_n\}$ (o simplemente $K\{X\}$).

   Dado $H \in K\{X\}$, la siguiente fórmula recursiva define una derivación en $K\{X\}$ que lo hace un anillo diferencial ordinario:

$$\begin{aligned} H^{(0)} &:= H, \\ H^{(p)} &:= \delta|(H^{(p-1)})| + \sum_{i\in\mathbb{N}_0, 1\leq j\leq\alpha} \frac{\partial H^{(p-1)}}{\partial X_j^{(i)}} X_j^{(i+1)}, \quad \text{para } p \geq 1, \end{aligned}$$

donde $\delta|(H^{(p-1)})|$ es el polinomio que se obtiene de $H^{(p-1)}$ aplicando la derivación δ a todos sus coeficientes. Si δ restringido a K es cero este término es siempre cero.

Dado un polinomio diferencial $H \in K\{X\}$, diremos que H tiene orden e si alguna de las variables $X_j^{(e)}$ aparece en H y ninguna de las variables $X_j^{(s)}$ con $s > e$ aparece, es decir, e es el máximo orden de derivación al que aparece en H cualquiera de las variables.

Definición 1.4. Los elementos de un anillo diferencial (R, δ) que satisfacen $\delta(r) = 0$ se llaman *constantes*. (Ver Ejercicio 2)

1.2. Ideales diferenciales.

Un subconjunto no vacío I de un anillo conmutativo R es un *ideal* si para todo $a, b \in I$ y todo $r \in R$, $a + b \in I$ y $r \cdot a \in I$. Si (R, δ) es un anillo diferencial, $I \subset R$ es un *ideal diferencial* si es un ideal que además es cerrado por δ, es decir, para todo $a \in I$, $\delta(a) \in I$.

Si A es un subconjunto de elementos del anillo R, notamos por (A) al menor ideal de R que contiene a A. Así, un elemento $a \in (A)$ si, y solo si, existen $a_1, \dots a_n \in A$ y $b_1, \dots, b_n \in R$ tal que $a = b_1 \cdot a_1 + \cdots + b_n \cdot a_n$. Si (R, δ) es un anillo diferencial, denotamos $[A]$ al menor ideal *diferencial* que contiene al conjunto A. Es claro que los ideales (A) y $[A]$ pueden ser distintos ya que el segundo debe ser cerrado por derivaciones mientras que el primero no, como lo muestra el siguiente ejemplo.

Ejemplo 1.5. Consideremos el anillo de polinomios diferenciales en una sola variable $\mathbb{C}\{X\}$. El ideal $(\dot{X}^2 - X)$ es el conjunto de todos los múltiplos $H(X)(\dot{X}^2 - X)$ con $H(X) \in \mathbb{C}\{X\}$. Por otro lado, el polinomio $2\dot{X}X^{(2)} - \dot{X}$ pertenence al ideal $[\dot{X}^2 - X]$ pues $2\dot{X}X^{(2)} - \dot{X} = \delta(\dot{X}^2 - X)$. (Ver Ejercicio 3).

Sea R un anillo e $I \subset R$ un ideal. Consideremos la relación de equivalencia entre los elementos de R dada por $a \sim b$ si, y solo si, $a - b \in I$ y para cada $a \in R$, notemos por $\bar{a}$ a su clase de equivalencia. El conjunto de estas clases de equivalencia, al que notaremos R/I, resulta ser un anillo con las operaciones $\bar{a} + \bar{b} = \overline{a + b}$ y $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Si (R, δ) es un anillo diferencial e $I \subset R$ es un ideal diferencial, entonces R/I resulta también un anillo diferencial definiendo la derivación $\bar{\delta}(\bar{a}) = \overline{\delta(a)}$ (ver Ejercicio 5).

Diremos que $I \subset R$ es un ideal *primo* si cada vez que $a \cdot b \in I$ y $a \notin I$ entonces $b \in I$. Observar que el ideal $I \subset R$ es primo si, y solo si, el anillo R/I es un dominio íntegro. Un ideal diferencial que además es primo se llama un ideal *primo diferencial*.

2. Polinomios diferenciales y Elemento primitivo diferencial

Comenzamos esta sección considerando dos ejemplos de sistemas de ecuaciones lineales que nos sirven para ilustrar los resultados que estamos buscando.

Ejemplo 2.1. Consideremos el siguiente sistema

$$\begin{cases} \dot{X}_1 &= X_2 \\ \dot{X}_2 &= X_3 \\ \dot{X}_3 &= -4X_1 + 3X_3 \end{cases}$$

que puede escribirse de la forma $\dot{X} = M \cdot X$ con $X = \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix}$ y $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -4 & 0 & 3 \end{pmatrix}$.

Si llamamos $Y = X_1$, tenemos que $\dot{Y} = X_2$, $Y^{(2)} = X_3$ y el sistema se transforma en una única ecuación diferencial

$$Y^{(3)} - 3Y^{(2)} + 4Y = 0$$

y cuyas soluciones se obtienen encontrando las raíces del polinomio $Z^3 - 3Z^2 + 4 = 0$. Es decir, como $Z^3 - 3Z^2 + 4 = (Z-2)^2(Z+1)$, todas las soluciones de la ecuación diferencial se obtienen como combinación lineal de e^{2t}, te^{2t} y e^{-t}.

Recordando que $Y = X_1$, $\dot{Y} = X_2$ y $Y^{(2)} = X_3$, a partir de las soluciones de la ecuación se obtienen las del sistema.

Observemos que M es la matriz compañera del polinomio $Z^3 - 3Z^2 + 4$.

Ejemplo 2.2. Ahora consideramos la matriz $A = \begin{pmatrix} -4 & 2 & -2 \\ -7 & 4 & -4 \\ 3 & -1 & 3 \end{pmatrix}$ y el sistema $\dot{X} = A \cdot X$.

Si $v = (1,0,0)$ y $C = \begin{pmatrix} v \\ vA \\ vA^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 2 & -2 \\ -4 & 2 & -6 \end{pmatrix}$, podemos escribir

$$A = C^{-1} \cdot M \cdot C$$

donde M es la matriz del ejemplo anterior, y, mediante el cambio de variables

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = C \cdot X$$

obtenemos el mismo sistema que antes, al que podemos transformar en una única ecuación de la cual sabemos calcular las soluciones.

En general, mediante un cambio de base obtenido a partir de una descomposición apropiada del espacio como suma directa de subespacios cíclicos, toda matriz puede ser llevada a una matriz con bloques en la diagonal donde cada bloque es una matriz compañera de un polinomio. Así, todo sistema lineal de primer orden puede desacoplarse en ecuaciones de orden mayor pero en una sola incógnita.

En lo que sigue mostraremos algunos resultados sobre extensiones de cuerpos diferenciales. Estos resultados y en particular la versión diferencial del Teorema del Elemento Primitivo (ver [11, Theorem 1]) nos permitirán cambiar las ecuaciones que definen ciertos sistemas particulares por una única ecuación en una nueva variable junto con las parametrizaciones que nos permiten recuperar las variables originales.

2.1. Extensiones de cuerpos diferenciales.

Si (L, δ) es un cuerpo diferencial ordinario y K es un subcuerpo de L con la derivada restringida, diremos que L es una *extensión diferencial* de K. Si $u_1, \ldots, u_n$ son elementos de L, indicaremos por $K[u_1, \ldots, u_n]$ y por $K\{u_1, \ldots, u_n\}$ al menor anillo algebraico y diferencial respectivamente que contiene a K y a $u_1, \ldots, u_n$ y por $K(u_1, \ldots, u_n)$ y $K\langle u_1, \ldots, u_n \rangle$ al menor cuerpo algebraico y diferencial respectivamente que contiene a K y a $u_1, \ldots, u_n$.

Como hacemos con las variables del anillo de polinomios diferenciales, si u es un elemento de un cuerpo diferencial (K, δ), notaremos por $\dot{u} := \delta(u)$ y por $u^{(i)} := \delta^i(u)$.

Definición 2.3. Diremos que un elemento $u \in L$ es *diferencialmente algebraico* sobre un subcuerpo K si, para algún $i \in \mathbb{N}$, el conjunto $\{u, \dot{u}, \ldots, u^{(i)}\}$ es algebraicamente dependiente sobre K, es decir si existe una relación polinomial no trivial, con coeficientes en K, $H(u, \dot{u}, \ldots, u^{(i)}) = 0$ satisfecha por u y sus primeras i derivadas. Más precisamente, si Z es una indeterminada diferencial debe existir un polinomio $H(Z) \in K\{Z\}$ no nulo tal que $H(u) = 0$. Análogamente diremos que un conjunto $\{u_1, \ldots, u_n\}$ de elementos de L es diferencialmente algebraico si existe un polinomio $H(Z_1, \ldots, Z_n) \in K\{Z_1, \ldots, Z_n\}$ no nulo tal que $H(u_1, \ldots, u_n) = 0$.

Ejemplo 2.4. El elemento $t \in \mathbb{Q}(t)$ es diferencialmente algebraico sobre $\mathbb{Q}$ ya que anula al polinomio $\dot{Z} - 1 \in \mathbb{Q}\{Z\}$.

Demostramos ahora algunas propiedades básicas de las extensiones de cuerpos diferenciales.

Proposición 2.5. *Si u es un elemento diferencialmente algebraico sobre K entonces existe un $r \in \mathbb{N}$ tal que $K\langle u\rangle = K(u, \ldots, u^{(r)})$, es decir, los elementos $u^{(j)}$ con $j \geq r$ pueden escribirse como un cociente de dos elementos de $K[u, \ldots, u^{(r)}]$.*

Demostración. Como u es diferencialmente algebraico sobre K, existe un $r \geq 0$ tal que los elementos $u, \dot{u}, \ldots, u^{(r)}$ son algebraicamente dependientes sobre K pero $u, \dot{u}, \ldots, u^{(r-1)}$ son independientes. Sea $H(Z) \in K\{Z\}$ un polinomio de orden r y de grado mínimo en $Z^{(r)}$ tal que $H(u) = 0$. Sea $S_H := \frac{\partial H}{\partial Z^{(r)}}$. Como H tiene grado mínimo en $Z^{(r)}$ entre todos los polinomios que se anulan en $u, \dot{u}, \ldots, u^{(r)}$, sabemos que $S_H(u, \dot{u}, \ldots, u^{(r)}) \neq 0$. Por otro lado, si consideramos el polinomio $\dot{H} \in K[Z, \ldots, Z^{(r+1)}] \subset K\{Z\}$, $\dot{H} = S_H \cdot Z^{(r+1)} + R$ con $R \in K[Z, \ldots, Z^{(r)}]$ un polinomio que no involucra a $Z^{(r+1)}$, como $\dot{H}(u, \dot{u}, \ldots, u^{(r)}, u^{(r+1)}) = 0$, resulta que $u^{(r+1)} \in K(u, \dot{u}, \ldots, u^{(r)})$. De la misma forma, $u^{(r+j)} \in K(u, \dot{u}, \ldots, u^{(r)})$ para todo $j \geq 0$. □

De la Proposición 2.5 se deduce que el grado de trascendencia algebraico de $K\langle u\rangle$ sobre K es menor que r (ver Ejercicio 6).

Corolario 2.6. *Si u y v son elementos diferencialmente algebraicos sobre K, entonces también lo son $u + v$, $u \cdot v$ y $\frac{u}{v}$ si $v \neq 0$.*

Demostración. Ejercicio 7. □

El Teorema del Elemento Primitivo Diferencial es un paralelo del mismo teorema algebraico ([7, Th. 4.6, Ch. V]). Afirmamos que si u y v son elementos de L diferencialmente algebraicos sobre K entonces, bajo ciertas hipótesis, existe $\theta \in L$ tal que $K\langle u, v\rangle = K\langle\theta\rangle$.

La demostración en el caso algebraico se basa en el hecho de que si $G(Z_1, \ldots, Z_n)$ es un polinomio no nulo y K es un cuerpo infinito, existen $z_1, \ldots, z_n \in K$ tal que $G(z_1, \ldots, z_n) \neq 0$. En el caso diferencial este resultado no es válido sin pedir alguna condición adicional; por ejemplo, si K es un cuerpo de constantes, el polinomio $\dot{Z}$ se anula sobre todo K. De hecho, el Teorema del Elemento Primitivo Diferencial no es válido para extensiones de un cuerpo de constantes K: si X_1 y X_2 son dos variables algebraicas y se considera el cuerpo $K(X_1, X_2)$ como un cuerpo diferencial con $\dot{X}_1 = 0$ y $\dot{X}_2 = 0$, se tiene que $K\langle X_1, X_2\rangle = K(X_1, X_2)$ y, como para cualquier θ, $K\langle\theta\rangle =$

$K(\theta)$, resulta imposible que $K(X_1, X_2) = K(\theta)$ ya que tienen distintos grados de trascendencia.

Para demostrar el teorema en el caso diferencial necesitamos un resultado que nos asegure que si K es un cuerpo diferencial que contiene un elemento no constante y $G(Z_1, \ldots, Z_n)$ es un polinomio diferencial no nulo, entonces existen $z_1, \ldots, z_n \in K$ tal que $G(z_1, \ldots, z_n) \neq 0$. En la próximos sección nos concentraremos en la demostración de este resultado.

2.2. Polinomios diferenciales.

Comenzamos con el siguiente:

Lema 2.7. *Sean K un cuerpo diferencial y $\eta_1, \ldots, \eta_s$ elementos de K. Existen elementos $c_1, \ldots, c_s$ constantes no todos nulos de K tal que $c_1\eta_1 + \ldots + c_s\eta_s = 0$ si, y solo si, el determinante de la matriz $A = \begin{pmatrix} \eta_1 & \cdots & \eta_s \\ \dot{\eta}_1 & \cdots & \dot{\eta}_s \\ \vdots & \ddots & \vdots \\ \eta_1^{(s-1)} & \cdots & \eta_s^{(s-1)} \end{pmatrix}$ es cero.*

Demostración. Supongamos que $c_1, \ldots, c_s$ son constantes de K que satisfacen $c_1\eta_1 + \cdots + c_s\eta_s = 0$. Si derivamos esta igualdad $s-1$ veces obtenemos que $c_1, \ldots, c_s$ es una solución no trivial del sistema de s ecuaciones con s incógnitas

$$\begin{pmatrix} \eta_1 & \cdots & \eta_s \\ \dot{\eta}_1 & \cdots & \dot{\eta}_s \\ \vdots & \ddots & \vdots \\ \eta_1^{(s-1)} & \cdots & \eta_s^{(s-1)} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_s \end{pmatrix} = 0$$

y, por lo tanto, $\det(A) = 0$.

La otra implicación la probaremos por inducción en s. El resultado es claro para $s = 1$, supongamos entonces que es válido para todo $r < s$.

Tenemos entonces que $\det(A) = 0$ y, sin pérdida de generalidad, podemos suponer que $\det \begin{pmatrix} \eta_1 & \cdots & \eta_{s-1} \\ \dot{\eta}_1 & \cdots & \dot{\eta}_{s-1} \\ \vdots & \ddots & \vdots \\ \eta_1^{(s-2)} & \cdots & \eta_{s-1}^{(s-2)} \end{pmatrix} \neq 0$ ya que si este determinante es 0, por hipótesis inductiva, existen constantes $c_1, \ldots, c_{s-1}$ no todas nulas que satisfacen $0 = c_1\eta_1 + \cdots + c_{s-1}\eta_{s-1} = c_1\eta_1 + \cdots + 0\eta_s$, y el resultado estaría probado.

En estas condiciones, existen $\alpha_1, \ldots, \alpha_{s-1} \in K$ tal que

$$\alpha_1 \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_1^{(s-1)} \end{pmatrix} + \cdots + \alpha_{s-1} \begin{pmatrix} \eta_{s-1} \\ \vdots \\ \eta_{s-1}^{(s-1)} \end{pmatrix} + \begin{pmatrix} \eta_s \\ \vdots \\ \eta_s^{(s-1)} \end{pmatrix} = 0.$$

Tenemos entonces que $\alpha_1\eta_1 + \cdots + \alpha_{s-1}\eta_{s-1} + \eta_s = 0$ y derivando esta igualdad obtenemos $\dot{\alpha}_1\eta_1 + \ldots + \dot{\alpha}_{s-1}\eta_{s-1} + \alpha_1\dot{\eta}_1 + \cdots + \alpha_{s-1}\dot{\eta}_{s-1} + \dot{\eta}_s = 0$. Por lo tanto, $\dot{\alpha}_1\eta_1 + \cdots + \dot{\alpha}_{s-1}\eta_{s-1} = 0$ y, por hipótesis inductiva se deduce, que $\dot{\alpha}_1 = \ldots = \dot{\alpha}_{s-1} = 0$, es decir, los α_i resultan constantes. □

Lema 2.8. *Sea K un cuerpo diferencial que contiene a $\mathbb{Q}$ y un elemento no constante ξ. Si $G \in K\{Z\}$ es un polinomio diferencial no nulo de orden r, existe un elemento $\nu = c_0 + c_1\xi + \cdots + c_r\xi^r$, con $c_0, c_1, \ldots, c_n$ constantes de K, tal que $G(\nu) \neq 0$.*

Demostración. Supongamos que el resultado es falso. Entre todos los polinomios que se anulan para todos los valores $\nu = c_0 + c_1\xi + \cdots + c_r\xi^r$ con $c_0, c_1, \ldots, c_r$ constantes de K, consideremos $H(Z, \dot{Z}, \ldots, Z^{(s)})$ un polinomio de orden mínimo s y de grado mínimo en $Z^{(s)}$. Como K es infinito y G cumple esta condición, $0 < s \leq r$.

Entonces $H(\nu, \dot{\nu}, \ldots, \nu^{(s)})$ es idénticamente 0 visto como polinomio en las variables $c_0, c_1, \ldots, c_s$ y, por lo tanto, sus derivadas parciales respecto de estas variables son todas 0.

Si llamamos $\nu^{[s]} := \nu, \dot{\nu}, \ldots, \nu^{(s)}$ y $P(c_0, c_1, \ldots, c_s) := H(\nu, \dot{\nu}, \ldots, \nu^{(s)}) = H(\nu^{[s]})$ y consideramos las derivadas de P, obtenemos:

$$\begin{array}{rcll}
\frac{\partial P}{\partial c_0} & = & \frac{\partial H}{\partial Z}(\nu^{[s]}) & = 0 \\
\frac{\partial P}{\partial c_1} & = & \frac{\partial H}{\partial Z}(\nu^{[s]})\xi + \frac{\partial H}{\partial \dot{Z}}(\nu^{[s]})\dot{\xi} + \ldots + \frac{\partial H}{\partial Z^{(s)}}(\nu^{[s]})\xi^{(s)} & = 0 \\
\frac{\partial P}{\partial c_2} & = & \frac{\partial H}{\partial Z}(\nu^{[s]})\xi^2 + \frac{\partial H}{\partial \dot{Z}}(\nu^{[s]})(\dot{\xi^2}) + \ldots + \frac{\partial H}{\partial Z^{(s)}}(\nu^{[s]})(\xi^2)^{(s)} & = 0 \\
\vdots & & \vdots & \\
\frac{\partial P}{\partial c_s} & = & \frac{\partial H}{\partial Z}(\nu^{[s]})\xi^s + \frac{\partial H}{\partial \dot{Z}}(\nu^{[s]})(\dot{\xi^s}) + \ldots + \frac{\partial H}{\partial Z^{(s)}}(\nu^{[s]})(\xi^s)^{(s)} & = 0
\end{array}$$

Como $\frac{\partial H}{\partial Z^{(s)}}$ tiene grado en $Z^{(s)}$ menor que H, no se anula en todos los valores de ν posibles, por lo tanto

$$\det \begin{pmatrix} \dot{\xi} & (\dot{\xi^2}) & \ldots & (\dot{\xi^s}) \\ (\xi)^{(2)} & (\xi^2)^{(2)} & \ldots & (\xi^s)^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ (\xi)^{(s)} & (\xi^2)^{(s)} & \ldots & (\xi^s)^{(s)} \end{pmatrix} = 0$$

y, por el lema anterior, existen $a_1, \ldots, a_s$ constantes, no todos nulas, de K tales que $a_1\dot{\xi} + a_2(\dot{\xi^2}) + \ldots + a_s(\dot{\xi^s}) = 0$ y $a_1\xi + a_2\xi^2 + \ldots + a_s\xi^s = a_0$ con a_0 constante. Por lo tanto, ξ cumple una ecuación algebraica no nula sobre K. Sea $f \in K[Z]$ un polinomio de grado mínimo entre los que tienen a ξ como raíz. Si derivamos la ecuación $f(\xi) = 0$, resulta que $\frac{\partial f}{\partial Z}(\xi) \cdot \dot{\xi} = 0$ y, como $\frac{\partial f}{\partial Z}$ tiene grado menor que f, resulta que $\dot{\xi} = 0$ lo que contradice la elección de ξ □

Observación 2.9. De la misma forma que en el caso puramente algebraico, este resultado permite demostrar que si K es un cuerpo diferencial que contiene un elemento no constante y $G(Z_1, \ldots, Z_n) \in K\{Z_1, \ldots, Z_n\}$ entonces existe $\nu \in K^n$ tal que $G(\nu) \neq 0$.

2.3. Elemento primitivo diferencial.

Estamos ahora en condiciones de probar el Teorema del Elemento Primitivo.

Teorema 2.10. *([11, Theorem 1]) Sea K un cuerpo que contiene a $\mathbb{Q}$ y un elemento no constante. Si u y v son diferencialmente algebraicos sobre K, entonces existe $\lambda \in K$ tal que $K\langle u, v\rangle = K\langle u + \lambda v\rangle$.*

Demostración. Consideremos el cuerpo $K\langle u, v\rangle\langle\Lambda\rangle = K\langle u, v, \Lambda\rangle$ donde Λ es una indeterminada diferencial. Como u, v, y Λ son diferencialmente algebraicos sobre $K\langle\Lambda\rangle$, tenemos que $u + \Lambda v$ es diferencialmente algebraico sobre $K\langle\Lambda\rangle$ y por lo tanto, existe un polinomio no nulo $G(\Lambda, \ldots, \Lambda^{(t)}, Z, \dot{Z}, \ldots, Z^{(s)}) \in K\langle\Lambda\rangle\{Z\}$ tal que

$$G(\Lambda, \dot{\Lambda}, \ldots, \Lambda^{(t)}, u + \Lambda v, (u + \Lambda v)^{\cdot}, \ldots, (u + \Lambda v)^{(s)}) = 0$$

y supongamos que s es mínimo y que G tiene grado mínimo en $(u + \Lambda v)^{(s)}$.

Consideremos la derivada parcial respecto de $\Lambda^{(s)}$ de la relación anterior. Teniendo en cuenta que $\frac{\partial(u+\Lambda v)^{(i)}}{\partial\Lambda^{(s)}} = 0$ si $i < s$ y $\frac{\partial(u+\Lambda v)^{(s)}}{\partial\Lambda^{(s)}} = v$, resulta

$$\frac{\partial G}{\partial\Lambda^{(s)}}(u+\Lambda v) + \frac{\partial G}{\partial Z^{(s)}}(u+\Lambda v)\cdot v = 0.$$

Por las hipótesis de minimalidad sobre G, se tiene que $\frac{\partial G}{\partial Z^{(s)}}(u+\Lambda v) \neq 0$ y, por lo tanto

$$v = -\frac{\frac{\partial G}{\partial\Lambda^{(s)}}(u+\Lambda v)}{\frac{\partial G}{\partial Z^{(s)}}(u+\Lambda v)} \in K\langle\Lambda\rangle\langle u+\Lambda v\rangle.$$

Por la hipótesis de que el cuerpo K contiene un elemento no constante, podemos aplicar el Lema 2.8, y evaluar Λ en un elemento $\lambda \in K$ tal que $\frac{\partial G}{\partial Z^{(s)}}(u+\lambda v) \neq 0$ y así, $v \in K\langle u+\lambda v\rangle$ y, por lo tanto, $K\langle u+\lambda v\rangle = K\langle u, v\rangle$. □

Hemos probado entonces el Teorema del Elemento Primitivo Diferencial para una extensión diferencial de cuerpos que se obtiene adjuntando dos elementos diferencialmente algebraicos. Por inducción tenemos el siguiente

Corolario 2.11. *Sea K un cuerpo diferencial que contiene a $\mathbb{Q}$ y un elemento no constante. Si $u_1, \ldots, u_s$ son diferencialmente algebraicos sobre K, entonces existen $\lambda_1, \ldots, \lambda_s \in K$ tales que $K\langle u_1, \ldots, u_s\rangle = K\langle \lambda_1 u_1 + \cdots + \lambda_s u_s\rangle$.*

En la próxima sección aplicaremos estos resultados para simplificar las ecuaciones que definen ciertos sistemas DAE particulares.

Bibliografía complementaria: Demostraciones elementales de resultados sobre extensiones de cuerpos diferenciales pueden encontrarse en [8] y en [11].

3. El sistema $F = 0$ y su Representación Resolvente

En esta sección consideraremos sistemas DAE del tipo:

$$\left\{\begin{array}{rcl} f_1(X, \dot{X}, \ldots, X^{(e_1)}) & = & 0 \\ & \vdots & \\ f_n(X, \dot{X}, \ldots, X^{(e_n)}) & = & 0 \end{array}\right. \tag{3.1}$$

donde, para cada $1 \leq j \leq n$, f_j es un polinomio en las variables $X := X_1, \ldots, X_n$ (que representan las incógnitas) y sus derivadas $X^{(i)} := X_1^{(i)}, \ldots, X_n^{(i)}$, $1 \leq i \leq e_j$, con coeficientes en el cuerpo diferencial K que contiene a $\mathbb{Q}(t)$. Cada entero no negativo e_j denota el máximo orden de derivación de las variables que aparece en el polinomio f_j. Decimos que el sistema tiene orden e si $e := \text{máx}\{e_j\}$ y supondremos siempre que $e \geq 1$.

Denotaremos por $F := f_1, \ldots, f_n$, $F^{(i)} := f_1^{(i)}, \ldots, f_n^{(i)}$ y $F^{[i]} := F, F^{(1)}, \ldots, F^{(i)}$ y usaremos la notación abreviada $F = 0$ para referirnos al sistema anterior.

Nuestro objetivo será conseguir una sola ecuación diferencial y parametrizaciones que nos permitan obtener las soluciones del sistema original a partir de las soluciones de esta nueva ecuación. (Comparar con los Ejemplos 2.1 y 2.2)

Vamos a suponer que el ideal diferencial $[F] \subset K\{X\}$ es un ideal primo. Sea $\mathbb{L} := \text{Frac}(K\{X\}/[F])$ el cuerpo de fracciones del dominio $K\{X\}/[F]$. Por simplicidad y para poder aplicar directamente el Teorema del Elemento Primitivo Diferencial, vamos a considerar sistemas que satisfagan que cada una de las clases de las variables en $\mathbb{L}$,

$\bar{X}_1, \ldots, \bar{X}_n$, es diferencialmente algebraica sobre $\mathbb{K}$. Con estas hipótesis, el Teorema 2.10 en este contexto nos permite dar la siguiente

Definición 3.1. Con las notaciones e hipótesis anteriores, existe un elemento $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = K\langle\gamma\rangle$. Más aún, por el Ejercicio 8, γ puede ser elegido como una combinación lineal $\gamma = \lambda_1\bar{X}_1 + \cdots + \lambda_n\bar{X}_n$ con $\lambda_i \in \mathbb{Q}[t]$ para $i = 1, \ldots, n$. Un elemento γ que satisface estas condiciones se llama un *elemento primitivo* de la extensión $K \hookrightarrow \mathbb{L}$.

Si fijamos el elemento primitivo γ, podemos escribir a todos los elementos de $\mathbb{L}$ en función de γ, más precisamente, como cociente de polinomios en γ. En la siguiente Proposición mostraremos que estos polinomios pueden tomarse de orden acotado para todos los elementos de $\mathbb{L}$.

Proposición 3.2. *Sea γ un elemento primitivo de la extensión $K \hookrightarrow \mathbb{L}$. Sea $s \in \mathbb{N}$ el máximo entero positivo tal que $\{\gamma, \ldots, \gamma^{(s-1)}\}$ es algebraicamente independiente sobre K. Sea T una nueva variable diferencial. Entonces para cada $\eta \in K\{X\}$ existen polinomios P_η y Q_η en $K[T^{[s]}]$ tales que $\bar{\eta} = \dfrac{P_\eta(\gamma^{[s]})}{Q_\eta(\gamma^{[s]})}$.*

Demostración. Notemos primero que el entero s existe ya que estamos suponiendo que $\bar{X}_1, \ldots, \bar{X}_n$ son diferencialmente algebraicas sobre K y, por lo tanto, también lo son todos los elementos de $\mathbb{L}$.

Sea $\eta \in K\{X\}$. Como $\bar{\eta} \in \mathbb{L}$ y γ es un elemento primitivo de la extensión $K \hookrightarrow \mathbb{L}$, exiten polinomios P y Q en $K\{T\}$ tales que $\bar{\eta} = \dfrac{P(\gamma)}{Q(\gamma)} \in \mathbb{L}$. Estos polinomios P y Q pueden tener orden mayor que s y nuestro objetivo es encontrar polinomios de orden menor o igual que s.

La hipótesis sobre s nos asegura la existencia de un polinomio $M \in K[T^{[s]}]$ tal que $M(\gamma^{[s]}) = 0$ en $\mathbb{L}$. Más aún, podemos suponer que M tiene grado mínimo en la variable $T^{(s)}$.

Llamemos $I_M \in K[T^{[s-1]}]$ al coeficiente principal de M en la variable $T^{(s)}$ y $S_M \in K[T^{[s]}]$ al polinomio $\dfrac{\partial M}{\partial T^{(s)}}$. La hipótesis de grado mínimo sobre M nos permite asegurar que $I_M(\gamma^{[s-1]}) \neq 0$ y $S_M(\gamma^{[s]}) \neq 0$ en $\mathbb{L}$.

Usando una versión simplificada del proceso de derivación y división descripto en [4, Ch. I, Sec.9, Proposition 1] (ver Ejercicio 9), se sigue que existen enteros no negativos a_1, b_1, a_2, b_2 y polinomios R_P y R_Q en $K[T^{[s]}]$ tales que los polinomios $I_M^{a_1}S_M^{b_1}P - R_P$ y $I_M^{a_2}S_M^{b_2}Q - R_Q$ pertenecen al ideal diferencial $[M] \subset K\{T\}$.

Como $M^{(j)}(\gamma^{[s+j]}) = 0$ para todo $j \geq 0$, tenemos las siguientes identidades en $\mathbb{L}$:

$$R_P(\gamma^{[s]}) = I_M^{a_1}(\gamma^{[s-1]})S_M^{b_1}(\gamma^{[s]})P(\gamma) \quad \text{y} \quad R_Q(\gamma^{[s]}) = I_M^{a_2}(\gamma^{[s-1]})S_M^{b_2}(\gamma^{[s]})Q(\gamma).$$

Así, podemos definir

$$P_\eta := I_M^{a_2}S_M^{b_2}R_P \in K[T^{[s]}] \quad \text{y} \quad Q_\eta := I_M^{a_1}S_M^{b_1}R_Q \in K[T^{[s]}]$$

y otenemos la identidad $\eta = \dfrac{P_\eta(\gamma^{[s]})}{Q_\eta(\gamma^{[s]})}$. □

Observación 3.3. De la Proposición 3.2 deducimos que, si γ es un elemento primitivo de la extensión de cuerpos $K \hookrightarrow \mathbb{L}$, entonces los elementos $\gamma, \dot{\gamma}, \ldots, \gamma^{(s-1)}$ forman una base de trascendencia (algebraica) de dicha extensión, es decir, un conjunto algebraicamente independiente tal que la extensión $K(\gamma, \ldots, \gamma^{(s-1)}) \hookrightarrow \mathbb{L}$ es algebraica. Como todas las bases de trascendencia tienen el mismo cardinal ([7, Theorem 1.1, Ch. VIII] o Ejercicio

6), podemos afirmar que el entero s sólo depende de la extensión y que cualquier otro elemento primitivo ω cumplirá que el conjunto $\{\omega, \dot{\omega}, \ldots, \omega^{(s-1)}\}$ es trascendente sobre K mientras que $\omega^{(s)}$ es algebraico sobre $K(\omega, \dot{\omega}, \ldots, \omega^{(s-1)})$.

3.1. Representación Resolvente.

Fijemos por ahora un elemento primitivo γ de la extensión $K \hookrightarrow \mathbb{L}$. Consideremos un polinomio mónico minimal de $\gamma^{(s)}$ en la extensión de cuerpos algebraica $K(\gamma, \ldots, \gamma^{(s-1)}) \hookrightarrow \mathbb{L}$. Multiplicando a este polinomio por un elemento no nulo de $K(\gamma, \ldots, \gamma^{(s-1)})$ y renombrando las variables $\gamma, \ldots, \gamma^{(s-1)}$ por $T, \ldots, T^{(s-1)}$ obtenemos un polinomio irreducible $M \in K[T, \ldots, T^{(s-1)}, T^{(s)}]$ tal que $M(\gamma, \ldots, \gamma^{(s)}) = 0$ en $\mathbb{L}$. En otras palabras, si $\Gamma = \lambda_1 X_1 + \ldots + \lambda_n X_n$, es decir $\bar{\Gamma} = \gamma$, $M(\Gamma, \ldots, \Gamma^{(s)}) \in [F]$. Diremos que $M \in K[T, \ldots, T^{(s)}]$ es un polinomio minimal de γ si M es irreducible y $M(\gamma, \ldots, \gamma^{(s)}) = 0$ en $\mathbb{L}$.

Observemos que si $P \in K[T, \ldots, T^{(s-1)}, T^{(s)}]$ es un polinomio tal que $P(\gamma, \ldots, \gamma^{(s)}) = 0$ en $\mathbb{L}$, entonces cualquier polinomio M, minimal de γ, divide a P en $K(T, \ldots, T^{(s-1)})[T^{(s)}]$ y, como M es primitivo, también lo divide en $K[T, \ldots, T^{(s)}]$. Por lo tanto, el ideal $\{P \in K[T^{[s]}] : P(\gamma^{[s]}) = 0\}$ está generado por cualquier polinomio minimal de γ. Así, un polinomio minimal de γ en la extensión $K \hookrightarrow \mathbb{L}$ está univocamente determinado salvo un factor escalar en $K \setminus \{0\}$.

Por otro lado, de la Proposición 3.2 tenemos que para cada variable X_i, con $i = 1, \ldots, n$, existen polinomios P_i y $Q_i \in K[T^{[s]}]$, con $Q_i(\gamma^{[s]}) \neq 0$ tales que $\bar{X}_i = \dfrac{P_i(\gamma)}{Q_i(\gamma)}$ en $\mathbb{L}$, es decir $\bar{\Gamma} = \gamma$, $Q_i(\Gamma)X_i - P_i(\Gamma) \in [F]$, para todo $i = 1, \ldots, n$.

Definición 3.4. Fijado un elemento primitivo γ y con las notaciones e hipótesis anteriores, el conjunto

$$\{M(T), Q_1(T)X_1 - P_1(T), \ldots, Q_n(T)X_n - P_n(T)\},$$

donde $M(T)$ es un polinomio minimal de γ en $K \hookrightarrow \mathbb{L}$, se llama una *representación resolvente* del ideal primo $[F]$ o del sistema $F = 0$ con respecto al elemento primitivo γ.

3.2. Ejemplo.

En esta sección presentamos un ejemplo del cálculo de la representación resolvente para un sistema DAE.

Ejemplo 3.5. Consideremos el siguiente sistema diferencial sobre $K = \mathbb{Q}(t)$:

$$\begin{cases} \dot{X}_1 - X_1^2 = 0 \\ \dot{X}_2 - X_1^2 = 0 \\ \quad\vdots \\ \dot{X}_n - X_1^2 = 0 \end{cases}.$$

con $f_i = \dot{X}_i - X_1^2$ y $\mathbb{L} = \mathrm{Frac}(K\{X\}/[F])$.

Por simplicidad, de ahora en más, usaremos la misma notación, $X = X_1, \ldots, X_n$ para representar a las variables del anillo diferencial $K\{X\}$ y sus clases en el cuerpo diferencial $\mathbb{L}$.

Observemos que $X_1, \ldots, X_n \in \mathbb{L}$ son algebraicamente independientes sobre K y que $\dot{X}_1, \ldots, \dot{X}_n$ son algebraicas sobre $K(X_1, \ldots, X_n)$, por lo tanto el grado de trascendencia algebraico de la extensión $K \hookrightarrow \mathbb{L}$ es n (ver Ejercicio 10). Más aún, $\mathbb{L} = K(X_1, \ldots, X_n)$

y así, el ideal $[F] \subset K\{X_1, \ldots, X_n\}$ es un primo diferencial. Estamos entonces en las hipótesis del Corolario 2.11.

Vamos a mostrar ahora un elemento primitivo de la extensión $K \hookrightarrow \mathbb{L}$:

Afirmación 3.1. *Si $n \geq 2$ entonces el elemento $\gamma := X_2 + tX_3 + \cdots + t^{n-2}X_n \in \mathbb{L}$ es un elemento primitivo de la extensión diferencial $K = \mathbb{Q}(t) \hookrightarrow \mathbb{L}$.*

Demostración. En esta demostración usaremos la siguiente notación: dado un vector $v = (v_1, \ldots, v_m)$ de m coordenadas y un polinomio $H := a_1 + a_2t + \cdots + a_mt^{m-1}$, escribiremos

$$\langle H, v\rangle := a_1v_1 + a_2v_2t + \cdots + a_mv_mt^{m-1}.$$

Con esta notación, tenemos que si $Q := 1 + t + \cdots + t^{n-2}$, $\gamma = \langle Q, (X_2, X_3, \ldots, X_n)\rangle$.

Para cada $l \in \mathbb{N}$, en el anillo $K\{X\}/[F]$, se verifican las siguientes igualdades:

$$\gamma^{(l)} = \left\langle Q^{(l)}, (X_{l+2}, \ldots, X_n)\right\rangle + \sum_{j=0}^{l-1} \frac{l!}{j!} Q^{(j)} X_1^{l+1-j} \tag{3.2}$$

y, en particular, como $Q^{(n-1)} = Q^{(n)} = 0$,

$$\gamma^{(n-1)} = \sum_{j=0}^{n-2} \frac{(n-1)!}{j!} Q^{(j)} X_1^{n-j} \quad \text{y} \quad \gamma^{(n)} = \sum_{j=0}^{n-1} \frac{n!}{j!} Q^{(j)} X_1^{n+1-j}$$

de donde podemos deducir que $nX_1\gamma^{(n-1)} = \gamma^{(n)}$ y entonces $X_1 = \dfrac{\gamma^{(n)}}{n\gamma^{(n-1)}}$ en $\mathbb{L}$.

Reemplazando X_1 en (3.2) para $l = n-2$, tenemos que

$$\gamma^{(n-2)} = (n-2)!X_n + \sum_{j=0}^{n-3} \frac{(n-2)!}{j!} Q^{(j)} \left(\frac{\gamma^{(n)}}{n\gamma^{(n-1)}}\right)^{n-1-j}.$$

Entonces, X_n se puede escribir en $\mathbb{L}$ como el cociente de dos polinomios que involucran solamente a γ y sus derivadas:

$$X_n = \frac{1}{(n-2)!}\left(\gamma^{(n-2)} - \sum_{j=0}^{n-3} \frac{(n-2)!}{j!} Q^{(j)} \left(\frac{\gamma^{(n)}}{n\gamma^{(n-1)}}\right)^{n-1-j}\right).$$

Aplicando sucesivamente las identidades en (3.2) para $l = n-3, \ldots, 1$, todas las variables pueden escribirse como cociente de polinomios en $\gamma, \ldots, \gamma^{(n)}$. Con esto demostramos que γ es un elemento primitivo de la extensión diferencial $K \hookrightarrow \mathbb{L}$. □

De esta última demostración tenemos que, en $K\{X\}/[F]$,

$$\gamma^{(n-1)} = \sum_{j=0}^{n-2} \frac{(n-1)!}{j!} Q^{(j)} X_1^{n-j} \quad \text{y} \quad X_1 = \frac{\gamma^{(n)}}{n\gamma^{(n-1)}}.$$

Reemplazando X_1 en la primera fórmula, obtenemos el polinomio

$$M := -n^n \left(T^{(n-1)}\right)^{n+1} + \sum_{j=0}^{n-2} \frac{(n-1)!}{j!} Q^{(j)} \left(nT^{(n-1)}\right)^j (T^{(n)})^{n-j}$$

tal que $M(\gamma^{[n]}) \in [F]$. Como sabemos que el grado de trascendencia de la extensión $K \hookrightarrow \mathbb{L}$ es n, para demostrar que M es un polinomio minimal de γ, alcanza con ver que:

Afirmación 3.2. *$M \in \mathbb{Q}[t][T^{[n]}]$ es un polinomio irreducible.*

Demostración. Supongamos que no es así, entonces M se puede factorizar como producto de dos polinomios en el anillo $\mathbb{Q}[t, T^{(n-1)}][T^{(n)}]$ ambos de grado positivo en la varible $T^{(n)}$. Lo mismo debe suceder si evaluamos $t = 0$, y así, el polinomio

$$-n^n \left(T^{(n-1)}\right)^{n+1} + \sum_{j=0}^{n-2} \frac{(n-1)!}{j!} \left(nT^{(n-1)}\right)^j (T^{(n)})^{n-j}$$

puede escribirse como producto de dos polinomios en $\mathbb{Q}[T^{(n-1)}, T^{(n)}]$.

Pero $\displaystyle\sum_{j=0}^{n-2} \frac{(n-1)!}{j!} \left(nT^{(n-1)}\right)^j (T^{(n)})^{n-j}$ y $-n^n \left(T^{(n-1)}\right)^{n+1}$ son polinomios homogéneos con grados consecutivos y sin factores comunes y, por lo tanto, su suma es irreducible (Ejercicio 11). □

Bibliografía complementaria: Otros ejemplos de representaciones resolventes pueden encontrarse en [1]. En [2] y [3] se describen procedimientos efectivos para el cálculo de estas representaciones.

Ejercicios.

1. *a*) Probar que el las funciones $\mathcal{C}^\infty$ en la variable t sobre $\mathbb{R}$, con $\delta = \frac{d}{dt}$ forman un anillo diferencial que no es un dominio.
   b) Probar que las funciones enteras en la variable compleja z con $\delta = \frac{d}{dz}$ forman un dominio diferencial.
2. *a*) Probar que si (R, δ) es un anillo diferencial, el conjunto de todos los elementos constantes forman un subanillo.
   b) Probar que si (K, δ) es un cuerpo diferencial que contiene a $\mathbb{Q}$, los elementos constantes forman subcuerpo infinito.
3. Sea (K, δ) un cuerpo diferencial y $K\{X\}$ el anillo de polinomios diferenciales en la indeterminada X con coeficientes en K.
   a) Probar que los ideales $(\dot{X}^2 - X)$ y $[\dot{X}^2 - X]$ son distintos.
   b) Probar que el ideal $(\dot{X}^2 - X)$ es primo mientras que $[\dot{X}^2 - X]$ no lo es.
4. Un anillo se dice *noetheriano* si todo ideal está generado por un número finito de elementos. Un resultado clásico del álgebra conmutativa dice que si el anillo R es noetheriano, el anillo de polinomios con coeficientes en R también lo es (ver, por ejemplo, [6, Chapter I, Proposition 2.3]). Este ejercicio muestra que este resultado no es cierto si se considera el anillo de polinomios diferenciales.

   En el anillo de polinomios diferenciales en una variable X con coeficientes en $\mathbb{Z}$, $\mathbb{Z}\{X\}$ consideremos el ideal diferencial $I = [X^2, (\dot{X})^2, \ldots, (X^{(i)})^2, \ldots]$. Probar que I no puede ser generado por un número finito de polinomios.
5. Probar que si (R, δ) es un anillo diferencial e I es un ideal diferencial de R, el conjunto de clases de equivalencias R/I resulta un anillo diferencial con la derivación $\bar{\delta}(\bar{a}) = \overline{\delta(a)}$.
6. Sea $E \hookrightarrow F$ una extensión de cuerpos y sea $\{x_1, \ldots, x_m\}$ un conjunto de elementos de F algebraicamente independientes sobre E y tal que la extensión $E(x_1, \ldots, x_m) \hookrightarrow F$ es algebraica. Probar que cualquier otro conjunto de elementos de F con la misma propiedad tiene m elementos. Un tal conjunto se llama una *base de trascendencia* de la extensión $E \hookrightarrow F$ y m es el grado de trascendencia de dicha extensión.
7. Demostrar el Corolario 2.6.

8. Sea K un cuerpo diferencial que contiene a $\mathbb{Q}$ y a un elemento tal que $\dot{\xi} = 1$. Sea $G(Z_1, \ldots, Z_n) \in K\{Z_1, \ldots, Z_n\}$ un polinomio diferencial no nulo de orden r. Probar que existen elementos $\nu_j = c_{j0} + c_{j1}\xi + \ldots + c_{jr}\xi^r$ $(j = 1, \ldots n)$, con $c_{j0}, \ldots, c_{jr} \in \mathbb{Q}$, tal que $G(\nu_1, \ldots, \nu_n) \neq 0$.
9. Sea K un cuerpo diferencial y T una indeterminada diferencial sobre K. Sea $P \in K\{T\}$ un polinomio diferencial de orden e y grado d en $T^{(e)}$. Definimos $S_P := \frac{\partial P}{\partial T^{(e)}}$ (el polinomio separante de P) e I_P el coeficiente de $(T^{(e)})^d$ en P (el polinomio inicial de P). Si $Q \in K\{T\}$ es un polinomio cualquiera, probar que existen enteros no negativos a y b y un polinomio R_Q que o bien tiene orden menor que e o bien tiene orden e pero grado menor que d tal que

$$I_P^a \cdot S_P^b \cdot Q - R_Q \in [P].$$

10. Probar que en el Ejemplo 3.5 los elementos $X_1, \ldots, X_n \in \mathbb{L}$ son algebraicamente independientes sobre K.
11. Probar que la suma de dos polinomios homogéneos de grados consecutivos y sin factores comunes es irreducible.
12. Consideremos el siguiente sistema diferencial de cuatro ecuaciones con cuatro incógnitas X_1, X_2, X_3, X_4:

$$\left\{ \begin{array}{lcl} \dot{X}_1 & = & \alpha X_1 \\ \dot{X}_2 & = & \alpha X_2 \\ \dot{X}_3 & = & \beta X_3 + X_4 X_1 \\ f(t) & = & X_2 + X_3 \end{array} \right. ,$$

donde $\alpha, \beta \in \mathbb{Q}$, $f(t) \in \mathbb{Q}(t)$ y el cuerpo diferencial base del sistema es $\mathbb{Q}(t)$ provisto de la derivación usual, $t' = 1$.

a) Probar que $\gamma = X_1 + tX_2$ es un elemento primitivo de la extensión $\mathbb{Q}(t) \hookrightarrow \mathbb{L}$.

b) Encontrar un polinomio minimal para γ.

Referencias

[1] T. Cluzeau, E. Hubert, *Resolvent representation for regular differential ideals*, AAECC **13** (2003) 395–425.

[2] T. Cluzeau, E. Hubert, *Probabilistic algorithms for computing resolvent representations of regular differential ideals*, AAECC 19 (2008) 365–392.

[3] L. D'Alfonso, G. Jeronimo, P. Solernó, *On the Complexity of the Resolvent Representation of Some Prime Differential Ideals*. J. Complexity **22** (2006) 396–430.

[4] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York (1973).

[5] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math. **92** (1882) 1–122.

[6] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser Boston, Inc., Boston, MA, 1985.

[7] S. Lang, *Algebra, Third edition*, Graduate Texts in Mathematics **211**, Springer Verlag, New York (2002).

[8] H. W. Raudenbush, *Differential fields and ideals of differential forms*, Ann. of Math. **34**, (1933) 509–517.

[9] J.F. Ritt, *Differential equations from the algebraic standpoint*, Amer. Math. Soc. Colloq. Publ., Vol. **14**, New York, (1932).

[10] J.F. Ritt, *Differential Algebra*, Amer. Math. Soc. Colloq. Publ., Vol. **33**, New York, (1950).

[11] A. Seidenberg, *Some basic theorems in differential algebra (characteristic p arbitrary)*, Trans. Amer. Math. Soc. **73**, 174–190 (1952).

Departamento de Ciencias Exactas, Ciclo Básico Común, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina.
E-mail address: lisi@dm.uba.ar

FORMAS CUADRÁTICAS

FERNANDO FANTINO

RESUMEN. En este curso veremos las nociones básicas de formas cuadráticas sobre cuerpos, mostraremos criterios de representación y diagonalización y daremos algunos resultados de clasificación. Además, se discutirán y resolverán ejercicios.

ÍNDICE

INTRODUCCIÓN

Notación. Denotaremos por $\mathbb{N} = \{1, 2, \dots\}$ al conjunto de los números naturales, por $\mathbb{F}$ a un cuerpo, por $\dot{\mathbb{F}}$ al grupo multiplicativo $\mathbb{F} - \{0\}$ del cuerpo $\mathbb{F}$, por $\dot{\mathbb{F}}^2$ al conjunto de los cuadrados de $\dot{\mathbb{F}}$ y por $\dot{\mathbb{F}}/\dot{\mathbb{F}}^2$ al grupo de clases de cuadrados de $\mathbb{F}$. Para m, $n \in \mathbb{N}$, $\mathbb{F}^{m\times n}$ denotará las matrices de tamaño $m \times n$ con coeficientes en $\mathbb{F}$. El conjunto de los vectores filas con coeficientes en $\mathbb{F}$ se escribirá $\mathbb{F}^n$.

En este curso asumiremos, salvo expresa mención de lo contrario, que el cuerpo $\mathbb{F}$ es de característica distinta de 2.

1. FORMAS CUADRÁTICAS Y ESPACIOS CUADRÁTICOS

1.1. Definiciones y generalidades.

2010 *Mathematics Subject Classification.* 11E04, 11E10, 11E81.
El autor agradece a los organizadores del V elENA y a sus auspiciantes.

Definición 1.1. Una *forma cuadrática (o $\mathbb{F}$-forma) de dimensión n* sobre un cuerpo $\mathbb{F}$ es un polinomio homogéneo de grado 2 en n indeterminadas.

Una forma cuadrática de dimensión n se escribe

$$f(X_1, \dots, X_n) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j, \qquad a_{ij} \in \mathbb{F}. \tag{1.1}$$

Tomando $b_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$ se tiene que $b_{ij} = b_{ji}$, para todo i, j, y

$$f(X_1, \dots, X_n) = \sum_{1 \leq i,j \leq n} b_{ij} X_i X_j. \tag{1.2}$$

Para $n = 1$, 2 y 3, la forma cuadrática se dice *unaria*, *binaria* y *ternaria*, respectivamente. Una forma cuadrática de dimensión n f escrita como en (1.2) da lugar a una matriz simétrica $m_f = (b_{ij})_{ij}$. Recíprocamente, una matriz simétrica $(b_{ij})_{ij}$ de tamaño $n \times n$ con coeficientes en $\mathbb{F}$, da lugar a una forma cuadrática de dimensión n mediante (1.2).

Denotemos por $\mathbf{X} = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ el vector columna de las indeterminadas $X_1, \dots, X_n$ y $\mathbf{X}^t$ su vector tranpuesto. Luego, la expresión (1.2) escrita en notación matricial es

$$f(\mathbf{X}) = \mathbf{X}^t \cdot m_f \cdot \mathbf{X}. \tag{1.3}$$

Definición 1.2. Una $\mathbb{F}$-forma f se dice *diagonal* si es de la forma $f(X_1, \dots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2$.

Definición 1.3. Sean f y g formas cuadráticas de dimensión n sobre $\mathbb{F}$. Se dice que f y g son *equivalentes* si existe una matriz inversible $A \in \mathbb{F}^{n \times n}$ tal que $g(A \cdot \mathbf{X}) = f(\mathbf{X})$, es decir si f se obtiene de g por una transformación lineal no singular de las indeterminadas $X_1, \dots, X_n$. Se escribe $f \simeq g$ o $f \simeq_A g$.

Es fácil ver que la relación $\simeq$ es de equivalencia. Más aún, $f \simeq g$ si y sólo si $m_f = A^t m_g A$. Denotaremos por (f) a la clase de equivalencia de una $\mathbb{F}$-forma f.

Ejemplo 1.4. Sean $f(X_1, X_2) = X_1^2 - X_2^2$, $g(X_1, X_2) = X_1 X_2$ y $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Luego,

$$g(X_1, X_2) = (X_1, X_2) \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix},$$
$$g(A\mathbf{X}) = (X_1, X_2) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix},$$

y $f \simeq g$.

Veremos otra manera de presentar formas cuadráticas.

Definición 1.5. Sea V un $\mathbb{F}$-espacio vectorial de dimensión finita. Una *forma bilineal* sobre V es una aplicación $B : V \times V \to \mathbb{F}$ lineal en ambos argumentos; si además B satisface $B(x, y) = B(y, x)$, para todo $x, y \in V$, B se dice simétrica.

Si B es una forma bilineal simétrica se tiene que

$$B(x + y, x + y) = B(x, x) + B(y, y) + 2B(x, y). \tag{1.4}$$

Si la característica de $\mathbb{F}$ es distinta de 2, se obtiene la *identidad polar*

$$B(x,y) = 1/2\,(B(x+y,x+y) - B(x,x) - B(y,y))\,. \tag{1.5}$$

Esta identidad dice que una forma bilineal simétrica está totalmente determinada por las valores que toma en la "diagonal" de $V \times V$.

Veremos que dada una forma bilineal B sobre un $\mathbb{F}$-espacio vectorial V y fijada una base de V, se tiene asociada de manera natural una forma cuadrática y, recíprocamente, toda forma cuadrática da lugar a una forma bilineal.

Sea B una forma bilineal simétrica sobre un espacio vectorial V. Definimos $q_B : V \to \mathbb{F}$ por $q_B(x) = B(x,x)$. Se verifican las siguientes propiedades:

(I) $q_B(ax) = a^2 q_B(x)$, para todo $a \in \mathbb{F}$, $x \in V$.
(II) $2B(x,y) = q_B(x+y) - q_B(x) - q_B(y)$, para todo $x, y \in V$.

Luego, la aplicación $(x,y) \mapsto q_B(x+y) - q_B(x) - q_B(y)$ es bilineal como aplicación de $V \times V$ en $\mathbb{F}$.

Definición 1.6. Sea V un $\mathbb{F}$-espacio vectorial de dimensión finita. Una aplicación $q : V \to \mathbb{F}$ se dice *cuadrática* sobre V si verifica

(I) $q_B(ax) = a^2 q_B(x)$, para todo $a \in \mathbb{F}$, $x \in V$, y
(II) $(x,y) \mapsto q_B(x+y) - q_B(x) - q_B(y)$ es una aplicación bilineal $V \times V$ en $\mathbb{F}$.

Se observó anteriormente que toda aplicación bilineal simétrica $B : V \times V \to \mathbb{F}$ define una aplicación cuadrática q_B tal que $q_B(x) = B(x,x)$. Recíprocamente, si la característica de $\mathbb{F}$ es distinta de 2, entonces toda aplicación cuadrática $q : V \to \mathbb{F}$ define una forma bilineal simétrica $B : V \times V \to \mathbb{F}$ por $B(x,y) = 1/2(q(x+y) - q(x) - q(y))$; es inmediato comprobar que $B(x,x) = q(x)$.

Así, si $\mathbb{F}$ es un cuerpo de característica distinta de 2, entonces toda forma bilineal B sobre un $\mathbb{F}$-espacio vectorial de dimensión finita define una única aplicación cuadrática $q : V \to \mathbb{F}$ y, recíprocamente, toda aplicación cuadrática define una única forma bilineal.

Definición 1.7. Un *espacio cuadrático* es un $\mathbb{F}$-espacio vectorial de dimensión finita munido de una aplicación cuadrática $q : V \to \mathbb{F}$.

Lo denotaremos por (V,q) o (V,B), donde B es la forma bilineal asociada a q.

Sea (V,q) un espacio cuadrático y $\{v_1, \dots, v_n\}$ una base de V. La matriz de la forma bilineal asociada B respecto de esta base es $(b_{ij}) \in \mathbb{F}^{n\times n}$, donde $b_{ij} = B(v_i, v_j)$. Si $v \in V$, con $v = \sum_{i=1}^n x_i v_i$, $x_i \in \mathbb{F}$, entonces

$$q(v) = B(v,v) = B(\sum_{i=1}^n x_i v_i, \sum_{i=j}^n x_j v_j) = \sum_{i,j=1}^n b_{ij} x_i x_j. \tag{1.6}$$

Luego, la matriz (b_{ij}) define una forma cuadrática $f_B(X_1, \dots, X_n) = \sum_{1\le i,j\le n} b_{ij} X_i X_j$. Así, especializando las indeterminadas X_i por x_i se obtiene que $f_B(x_1, \dots, x_n) = q(v)$. Es decir, fijada una base de V la aplicación cuadrática q es la especialización de una forma cuadrática f_B en las coordenadas de cada $v \in V$. Por esta razón se suele definir forma cuadrática como lo que aquí llamamos aplicación cuadrática.

Ejemplo 1.8. Sea f una $\mathbb{F}$-forma de dimensión n y sea $m_f = (b_{ij})$ la matriz (simétrica) de los coeficientes b_{ij} de f, ver (1.2). Consideremos $\mathbb{F}^n$ el $\mathbb{F}$-espacio vectorial de las n-uplas ordenadas de elementos de $\mathbb{F}$ y $B_f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ definida por $B_f(e_i, e_j) = b_{ij}$, con $e_1, \dots, e_2$ la base canónica de $\mathbb{F}^n$. B_f da lugar a la aplicación cuadrática $q_f : \mathbb{F}^n \to \mathbb{F}$

dada por $q_f(x) = B_f(x,x)$, $x \in \mathbb{F}^n$. Luego, $(\mathbb{F}^n, B_f)$ es un espacio cuadrático y se tiene la siguiente relación

$$f(x) = f(x_1, \ldots, x_n) = x^t \cdot m_f \cdot x = B_f(x,x) = q_f(x), \qquad \forall\, x \in \mathbb{F}^n. \tag{1.7}$$

Además, de (1.3) y la identidad polar se tiene que

$$B_f(x,y) = x^t \cdot m_f \cdot y, \qquad \forall\, x, y \in \mathbb{F}^n. \tag{1.8}$$

Sean (V,B) un espacio cuadrático, $v_1, \ldots, v_n$ una base de V y f_B la forma cuadrática asociada cuya matriz es $m_{f_B} = (B(v_i, v_j))$, la matriz de la forma bilineal B respecto de esa base. Si $w_1, \ldots, w_n$ es otra base de V y f'_B es la forma cuadrática definida respecto de esta base, entonces $f_B \simeq f'_B$. En efecto, si para cada j tenemos $w_j = \sum_{i=1}^n c_{ij} v_i$, entonces

$$(m_{f'_B})_{i,j} = B(w_i, w_j) = B(\sum_{k=1}^n c_{ki} v_k, \sum_{\ell=1}^n c_{\ell j} v_\ell) = \sum_{k,\ell} c_{ki} B(v_k, v_\ell) c_{\ell j} = (C^t \cdot m_{f_B} \cdot C)_{ij},$$

donde $C = (c_{ij})$. Luego, $m_{f'_B} = C^t \cdot m_{f_B} \cdot C$.

Definición 1.9. Sean (V_1, B_1), (V_2, B_2) dos espacios cuadráticos sobre $\mathbb{F}$. Se dice que son *isométricos* y se denotan $V_1 \simeq V_2$ si existe un $\mathbb{F}$-isomorfismo lineal $\varphi : V_1 \to V_2$ tal que $B_2(\varphi(v), \varphi(w)) = B_1(v,w)$, para todo $v, w \in V_1$.

Es fácil ver que la isometría es una relación de equivalencia. Denotaremos por $[(V,B)]$ a la clase de espacios cuadráticos isométricos a (V,B).

Ejemplo 1.10. El mapa $\varphi(v) = -v$, $v \in V$, es una isometría de cualquier espacio cuadrático (V,B) en sí mismo.

Ejemplo 1.11. Si f y g son $\mathbb{F}$-formas equivalentes de dimensión n, entonces los espacios cuadráticos $(\mathbb{F}^n, B_f)$ y $(\mathbb{F}^n, B_g)$ definidos en el Ejemplo 1.8 son isométricos. En efecto, tomar $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ por $\varphi(x) = A \cdot x$, donde A es la matriz inversible que da la equivalencia entre f y g.

Ejemplo 1.12. Sea (V,B) un espacio cuadrático, $v_1, \ldots, v_n$ una base de V y f_B la $\mathbb{F}$-forma correspondiente. Consideremos el espacio cuadrático $(\mathbb{F}^n, B_{f_B})$ como en el Ejemplo 1.8. Sea $\varphi : V \to \mathbb{F}^n$ tal que $\varphi(v_i) = e_i$, $1 \le i \le n$. Luego, φ es un isomorfismo lineal y se tiene que

$$B_{f_B}(\varphi(v_i), \varphi(v_j)) = B_{f_B}(e_i, e_j) = \text{ coef } (i,j) \text{ de } f_B = B(v_i, v_j).$$

Por lo tanto, φ es una isometría entre (V,B) y $(\mathbb{F}^n, B_{f_B})$.

Proposición 1.13. *Existe una correspondencia biyectiva entre las clases de equivalencias de formas cuadráticas de dimensión n sobre $\mathbb{F}$ y las clases de isometría de espacios cuadráticos sobre $\mathbb{F}$ de dimensión n.*

Demostración. Se deja para el lector. □

Esta proposición nos permite identificar a las clases de isometría de espacios cuadráticos con las correspondientes clases de equivalencias de $\mathbb{F}$- formas, lo que constituye una linealización del problema de estudiar las clases de equivalencias de formas cuadráticas sobre cuerpos.

En lo sucesivo nos referiremos indistintamente a las formas cuadráticas o a los espacios cuadráticos. La correspondencia de la Proposición 1.13 será considerada como $(f) \mapsto [(V_f, B_f)]$ y $[(V,B)] \mapsto (f_B)$.

1.2. Representación de escalares por una forma cuadrática. Un problema importante en la teoría de formas cuadráticas es determinar las condiciones para que una $\mathbb{F}$-forma f de dimensión n *represente* de manera no trivial al cero.

Definición 1.14. Sea f una F-forma de dimensión n y $d \in \mathbb{F}$. Se dice que f *representa a* d si existe $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$, $x \neq 0$, tal que $f(x) = d$. Diremos que f es *isótropa* si representa al cero y todo $x \in \mathbb{F}^n$, $x \neq 0$, tal que $f(x) = 0$ se llama *vector isótropo* para f. Si f es no isótropa se dice *anisótropa*.

Sea f una F-forma y (V, B) su correspondiente espacio cuadrático. Denotaremos por $D_{\mathbb{F}}(f)$ o $D_{\mathbb{F}}(V)$ al conjunto de los elementos de $\mathbb{F}$ representados por f. Notar que $D_{\mathbb{F}}(f) = \{d \in \mathbb{F} : B(v, v) = d, \text{ para algún } v \in V\}$.

Es fácil verificar que si f y g son $\mathbb{F}$-formas isométricas, entonces $D_{\mathbb{F}}(f) = D_{\mathbb{F}}(g)$. La recíproca no es cierta.

Observación 1.15. (a) Si f y g son F-formas equivalentes, entonces f es isótropa si y sólo g es isótropa.

(b) Sea (V, B) un espacio cuadrático y f su correspondiente $\mathbb{F}$-forma. En el caso que f es isótropa decimos que (V, B) es un espacio isótropo. En este caso, existe $v \in V$, $v \neq 0$, tal que $B(v, v) = 0$.

De (a) deducimos que la isotropía es un invariante de las clases de equivalencias de $\mathbb{F}$-formas. Para estudiar éste y otros invarantes nos interesará encontrar representantes de las clases de equivalencias de $\mathbb{F}$-formas que sean lo más sencillos posible. Demostraremos que toda F-forma es equivalente a una $\mathbb{F}$-forma diagonal. Previo a ello haremos algunas consideraciones.

Definición 1.16. Sean (V, B) un espacio cuadrático y $x, y \in V$. Se dice que x es *ortogonal* a y si $B(x, y) = 0$. Si U es un $\mathbb{F}$-subespacio de V, se define el *complemento ortogonal* de U como $U^{\perp} = \{y \in V \mid B(x, y) = 0, \forall\, x \in U\}$.

Es fácil verificar que $U^{\perp}$ es un subespacio de V. A $V^{\perp}$ se lo llama el *radical* de V y se lo denota por $r(V, B)$ o $r(V)$ si el contexto es claro. Diremos que (V, B) es *regular* o que B es *no degenerada* si $r(V) = 0$.

Observación 1.17. (a) La regularidad es propiedad de la clase de isometría.

(b) Si (V, B) tiene una *base ortogonal* (es decir, los vectores de la base son ortogonales tomados de a dos) que contiene un vector isótropo, entonces no es regular.

Espacios cuadráticos regulares (resp. no regulares) pueden contener subespacios no regulares (resp. regulares) como lo muestran los siguientes ejemplos.

Ejemplo 1.18. Sea $(\mathbb{F}^2, B)$, donde $B((x_1, x_2), (y_1, y_2)) = x_2 y_2$. B es una forma bilineal simétrica cuya matriz asociada en la base canónica es $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ y $f_B(X_1, X_2) = X_2^2$. El espacio cuadrático $(\mathbb{F}^2, B)$ no es regular pues $r(\mathbb{F}^2) = \{(x, 0) : x \in \mathbb{F}\}$, pero $U = \{(0, x) : x \in \mathbb{F}\}$ es un subespacio regular.

Ejemplo 1.19. Sea $(\mathbb{F}^2, B)$, donde $B((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$. Se puede ver que $(\mathbb{F}^2, B)$ es regular, pero $W = \{(x, 0) : x \in \mathbb{F}\}$ no es regular. Notar que $W^{\perp} = W$.

Teorema 1.20. *Todo espacio cuadrático (V, B) admite una base ortogonal.*

Demostración. Sea W un complemento de $r(V)$, o sea, $V = r(V) \oplus W$. El espacio cuadrático (W, B'), donde B' es la resticción de B a W, es regular. En efecto, si $x \in$

$r(W)$ e $y = u+v \in V$, con $u \in r(V)$, $v \in W$, entonces $B(x,y) = B(x,u)+B'(x,v) = 0$; esto implica que $x \in r(V) \cap W = 0$. Por esta razón basta demostrar el teorema para el caso en que V es regular.

Asumamos que V es regular. Procederemos por inducción en $\dim V$. Para $\dim V = 0, 1$ la conclusión es trivial. Supongamos que el teorema es válido para todo espacio regular de dimensión n y sea V de dimensión $n+1$. De la regularidad y la identidad polar se tiene que existe $v \in V$ tal que $B(v,v) \neq 0$. Es claro que $\mathbb{F}v \cap (\mathbb{F}v)^\perp = 0$; además, como $B(x - \frac{B(x,v)}{B(v,v)}v, v) = 0$, para todo $x \in V$, se tiene que $V = \mathbb{F}v + (\mathbb{F}v)^\perp$. Luego, $V = \mathbb{F}v \oplus (\mathbb{F}v)^\perp$. Ahora bien si $w \in (\mathbb{F}v)^\perp$ y $B(w, (\mathbb{F}v)^\perp) = 0$, entonces $w \in r(V) = 0$, lo que dice que $(\mathbb{F}v)^\perp$ es regular. Por hipótesis inductiva, existe una base ortogonal $w_1, \ldots, w_n$ de $(\mathbb{F}v)^\perp$. Por lo tanto, $v, w_1, \ldots, w_n$ es una base ortogonal de V. □

Observación 1.21. Dado un vector no isótropo v de un espacio cuadrático (V,B), se puede construir una base de V que contenga a v.

Sean f una $\mathbb{F}$-forma de dimensión n y $a_1 \in D_{\mathbb{F}}(f)$, con $a_1 \neq 0$. Para cualquier espacio cuadrático (V,B) correspondiente a (f) existe un vector v tal que $B(v,v) = a_1$. Por la Observación 1.21, existe una base ortogonal $v_1 = v, v_2, \ldots, v_n$ de V que contiene a v. Consideremos la $\mathbb{F}$-forma f_B asociada a esta base, cuya matriz asociada es $m_{f_B} = (B(v_i, v_j))_{i,j}$. Se tiene que $f \simeq f_B$. Luego, f es equivalente a una $\mathbb{F}$-forma diagonal cuya matriz asociada es

$$\begin{pmatrix} a_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & a_n \end{pmatrix} \tag{1.9}$$

lo que se denota por $f \simeq \langle a_1, \ldots, a_n \rangle$ y se llama una *representación diagonal* de f. En términos de polinomios (1.9) significa que, bajo isometría, $f(X_1, \ldots, X_n) = a_1X_1^2 + \cdots + a_nX_n^2$.

Ejemplo 1.22. Una representación diagonal de la forma $g(X_1, X_2) = X_1X_2$ dada en el Ejemplo 1.4 es $\langle 1, -1 \rangle$.

Observación 1.23. Es fácil mostrar que f es regular si y sólo si cualquier representación diagonal de f tiene todos sus términos no nulos.

Definición 1.24. Se define el *determinante* de una $\mathbb{F}$-forma f como $\det(f) = \det(m_f)$, el determinante de su matriz asociada.

Notar que si $f \simeq_A g$, entonces $\det(f) = \det(m_f) = \det(A^t m_g A) = \det(A)^2 \det(g)$, lo cual implica que $\det(f) = \det(g) \mod \dot{\mathbb{F}}^2$. Llamaremos también determinante de f a $d(f) = \det(f) \mod \dot{\mathbb{F}}^2$. Luego, d es un invariante de las clases de equivalencias de $\mathbb{F}$-formas.

Proposición 1.25. *Sea f una $\mathbb{F}$-forma. Las siguientes afirmaciones son equivalentes:*

(I) *f es regular,*
(II) *$d(f) \neq 0$,*
(III) *m_f es no singular.*

Demostración. (I) y (II) resultan equivalentes por la Observación 1.23 y porque el determinante de una forma diagonal $\langle a_1, \ldots, a_n \rangle$ es $a_1 \cdots a_n$. La equivalencia entre (II) y (III) es obvia. □

Proposición 1.26. *Si (V, B) es un espacio cuadrático regular, entonces $h : V \to V^*$, definida por $h_v(u) = B(u, v)$, $u, v \in V$, es un isomorfismo lineal.*

Demostración. Sea $\mathcal{B} = \{v_1, \dots, v_n\}$ una base de V y consideremos su base dual $\mathcal{B}^* = \{v_1^*, \dots, v_n^*\}$. La matriz de h relativa a las bases $\mathcal{B}$ y $\mathcal{B}^*$ coincide con la matriz $(B(v_i, v_j))$ que es no singular por hipótesis, lo que muestra que h es un isomorfismo lineal. □

1.3. Diagonalización de formas cuadráticas: algoritmo de Lagrange. Sea $f(X_1, \dots, X_n) = \sum_{1 \le i,j \le n} a_{ij} X_i X_j$ una forma cuadrática de dimensión n, con (a_{ij}) matriz simétrica. Se quiere encontrar una forma cuadrática $g(Y_1, \dots, Y_n) = \sum_{1 \le i \le n} b_i Y_i^2$ con $f \simeq g$. Consideremos dos casos:

(a) $a_{11} = \cdots = a_{nn} = 0$.
(b) $a_{ii} \neq 0$, para algún i, $1 \le i \le n$.

En el caso (a) se puede suponer que $a_{12} \neq 0$ y escribir

$$f(X_1, \dots, X_n) = 2X_1(a_{12}X_2 + \cdots + a_{1n}X_{1n}) + p(X_2, \dots, X_n),$$

donde $p(X_2, \dots, X_n)$ es independiente de X_1. Se define $Y_2 := a_{12}X_2 + \cdots + a_{1n}X_{1n} - X_1$ e $Y_i = X_i$ si $i \neq 2$. Luego, $f_1(Y_1, \dots, Y_n) = 2Y_1(Y_1 + Y_2) + p(Y_2, \dots, Y_n)$ es una forma cuadrática equivalente a f ya que la matriz que define el cambio de indeterminadas de $\mathbf{X}$ a $\mathbf{Y}$ tiene determinante $a_{12} \neq 0$. En consecuencia el caso (a) se reduce al caso (b).

Supongamos que existe i tal que $a_{ii} \neq 0$. Podemos suponer que $i = 1$ y escribir $f(\mathbf{X}) = a_{11}X^2 + 2a_{12}X_1X_2 + \cdots + 2a_{1n}X_1X_n + \sum_{i,j>1} a_{ij}X_iX_j$. Luego,

$$f(X_1, \dots, X_n) = a_{11}^{-1}(a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n)^2 + p(X_2, \dots, X_n).$$

Si definimos $Y_1 = a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n$ e $Y_i = X_i$, $i > 1$, entonces la forma cuadrática $f_1(Y_1, \dots, Y_n) = a_{11}^{-1}Y_1^2 + p(Y_2, \dots, Y_n)$ es equivalente a f pues el determinante de la matriz que define el cambio de indeterminadas de $\mathbf{X}$ a $\mathbf{Y}$ es $a_{11} \neq 0$.

Aplicando de manera iterada el mismo procedimiento a las formas p's se obtiene una forma diagonal equivalente a f, donde la matriz de cambio de indeterminadas es el producto de las matrices de cambio de indeterminadas utilizadas.

Ejemplo 1.27. Diagonalizar sobre $\mathbb{F}$, con $\mathbb{F}$ cuerpo de característica distinta de 2, la $\mathbb{F}$-forma $f(X_1, X_2) = X_1X_2$. Aplicaremos (a) del algoritmo de Lagrange para reducir al caso (b). Escribimos $f(X_1, X_2) = 2X_1(\frac{1}{2}X_2)$ y definimos $Z_1 = X_1$ e $Z_2 = \frac{1}{2}X_2 - X_1$; luego, $f_1(Z_1, Z_2) = 2Z_1(Z_1 + Z_2) = 2Z_1^2 + 2Z_1Z_2$. Aplicamos ahora el procedimiento descripto en el caso (b) del algoritmo a la $\mathbb{F}$ forma f_1. Se puede ver que $f_1(Z_1, Z_2) = \frac{1}{2}(2Z_1 + Z_2)^2 - \frac{1}{2}Z_2$; si definimos $Y_1 = 2Z_1 + Z_2$ e $Y_2 = Z_2$, entonces se tiene $f_2(Y_1, Y_2) = \frac{1}{2}Y_1^2 - \frac{1}{2}Y_2^2$. Los cambios de indeterminadas están dados por las matrices

$$P_1 = \begin{pmatrix} 1 & 0 \\ -1 & \frac{1}{2} \end{pmatrix} \quad \text{y} \quad P_2 = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix},$$

respectivamente. Por lo tanto, la forma $f(X_1, X_2) = X_1X_2$ es equivalente a la forma diagonal $f(Y_1, Y_2) = \frac{1}{2}Y_1^2 - \frac{1}{2}Y_2^2$ mediante la matriz

$$P = P_2 \cdot P_1 = \begin{pmatrix} 1 & \frac{1}{2} \\ -1 & \frac{1}{2} \end{pmatrix}.$$

Se recomienda al lector verificar que se cumplen $P_1^t \cdot m_{f_1} \cdot P_1 = m_f$, $P_2^t \cdot m_{f_2} \cdot P_2 = m_{f_1}$ y $P^t \cdot m_{f_2} \cdot P = m_f$.

Ejemplo 1.28. Apliquemos el algoritmo de Lagrange a la $\mathbb{R}$-forma $f(\mathbf{X}) = X_1^2 - X_2^2 + 3X_3^2 + X_1X_3$. Reescribimos:

$$f(\mathbf{X}) = X_1^2 + 2(\frac{1}{2}X_1X_3) - X_2^2 + 3X_3^2 = (X_1 + \frac{1}{2}X_3)^2 - X_2^2 + \frac{11}{4}X_3^2.$$

Si definimos $Y_1 = X_1 + \frac{1}{2}X_3$, $Y_2 = X_2$ e $Y_3 = \frac{\sqrt{11}}{2}X_3$, entonces se obtiene que $g(\mathbf{Y}) = Y_1^2 - Y_2^2 + Y_3^2$. La matriz de cambio de coordenadas es

$$P = \begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 1 & \frac{\sqrt{11}}{2} \end{pmatrix}$$

y se tiene que $g(\mathbf{Y}) = g(P \cdot \mathbf{X}) = \mathbf{X}^t \cdot (P^t \cdot m_g \cdot P) \cdot \mathbf{X}$. Además,

$$P^t \cdot m_g \cdot P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{\sqrt{11}}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 1 & \frac{\sqrt{11}}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ \frac{1}{2} & 1 & 3 \end{pmatrix} = m_f,$$

lo que muestra la relación $g(P \cdot \mathbf{X}) = f(\mathbf{X})$

2. Suma ortogonal de espacios cuadráticos

Sean (V_1, B_1) y (V_2, B_2) espacios cuadráticos de dimensión n y m, respectivamente. Se define la *suma ortogonal* $V_1 \perp V_2$ de (V_1, B_1) y (V_2, B_2) como el espacio cuadrático (V, B) donde $V = V_1 \oplus V_2$ y $B : V \times V \to \mathbb{F}$, $B((v_1, v_2), (w_1, w_2)) = B_1(v_1, w_1) + B_2(v_2, w_2)$, $v_\ell, w_\ell \in V_\ell$, $\ell = 1, 2$. Claramente, B es bilineal y $B\,|_{V_i \times V_i} = B_i$, $i = 1, 2$. Si f y g son $\mathbb{F}$-formas de dimensión n y m, respectivamente, entonces $f \perp g$ denota la $\mathbb{F}$-forma correspondiente a la clase de isometría del espacio suma ortogonal de $(\mathbb{F}^n, B_f)$ y $(\mathbb{F}^m, B_g)$. Explícitamente, si $f = f(X_1, \ldots, X_n)$ y $g = g(X_1, \ldots, X_m)$, entonces $f \perp g$ es la forma

$$(f \perp g)(X_1, \ldots, X_{n+m}) = f(X_1, \ldots, X_n) + g(X_{n+1}, \ldots, X_{n+m}).$$

Es claro que si $f \simeq f'$ y $g \simeq g'$, entonces $f \perp g \simeq f' \perp g'$. Para $k \in \mathbb{N}$, denotaremos por $f^{\perp k}$ a la suma ortogonal de f consigo misma k veces.

Ejemplo 2.1. Sean $f(X_1, X_2) = X_1^2 + 2X_2^2$ y $g(X_1, X_2) = 2X_1^2 + X_1X_2 + 3X_2^2$. Luego, la suma ortogonal de f y g es $(f \perp g)(X_1, X_2, X_3, X_4) = X_1^2 + 2X_2^2 + 2X_3^2 + X_3X_4 + 3X_4^2$.

Observación 2.2. Una $\mathbb{F}$-forma diagonal es suma ortogonal de $\mathbb{F}$-formas unarias. En efecto, $\langle a_1, \ldots, a_n \rangle = \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle$.

Proposición 2.3. *Si (V, B) es un espacio cuadrático y U es un subespacio regular de V, entonces $V = U \perp U^\perp$.*

Demostración. Claramente, $U \cap U^\perp = 0$. Sea $v_1, \ldots, v_k$ una base ortogonal de U. Por la regularidad de U se tiene que $B(v_i, v_i) \neq 0$ y se puede mostrar que para cualquier $v \in V$, $B(y_v, v_j) = 0$, $j = 1, \ldots, k$, donde $y_v = v - \sum_{i=1}^k \frac{B(v,v_i)}{B(v_i,v_i)} v_i$; luego, $B(y_v, U) = 0$. Esto permite encontrar $v_{k+1}, \ldots, v_n \in U^\perp$ tales que $v_1, \ldots, v_n$ es base de V. Es claro verificar que se cumplen las condiciones sobre la formas bilineales. □

Corolario 2.4. *Sea (V, B) un espacio cuadrático y U un subespacio regular de V. Si $V = U \perp W$, entonces $W = U^\perp$.* □

La siguiente aplicación del corolario se deja como ejercicio para el lector (ver Ejercicio 5): dos formas binarias $f = \langle a, b\rangle$ y $g = \langle c, d\rangle$ son isométricas si y sólo si representan un elemento en común y tienen el mismo determinante módulo $\dot{\mathbb{F}}^2$, o sea $d(f) = d(g)$.

Con esta afirmación se puede mostrar que $\langle 1, -1\rangle \simeq \langle a, -a\rangle$, para todo $a \in \dot{\mathbb{F}}$. En efecto, tienen el mismo determinante módulo $\dot{\mathbb{F}}^2$ y ambas $\mathbb{F}$-formas representan a $a = \frac{(a+1)^2}{4} - \frac{(a-1)^2}{4}$. Es claro que la forma cuadrática

$$\mathfrak{h} := \langle 1, -1\rangle \tag{2.1}$$

es isótropa. Más aún, representa a todo elemento de $\mathbb{F}$. El espacio cuadrático correspondiente se llama *plano hiperbólico* sobre $\mathbb{F}$ y se lo denota H o $H_{\mathbb{F}}$. Un espacio cuadrático que es suma ortogonal de planos hiperbólicos recibe el nombre de *espacio hiperbólico*. Notar que H es espacio regular.

Proposición 2.5. *Sea f una forma cuadrática regular. Entonces f es isótropa si y sólo si contiene un plano hiperbólico.*

Demostración. Como f es regular existe una representación diagonal $\langle a_1, \dots, a_n\rangle$ de f, con $a_i \neq 0$, para todo i. Si f contiene un plano hiperbólico, es decir si $f \simeq \mathfrak{h} \perp g$ para alguna $\mathbb{F}$-forma g, entonces es claro que f es isótropa. Recíprocamente, si $x = (x_1, \dots, x_n)$ es vector isótropo para f, entonces $a_1x_1^2 + \cdots + a_nx_n^2 = 0$. Asumamos que $x_\ell \neq 0$, dividiendo por x_ℓ^2 se tiene que la forma $\langle a_1, \dots, a_{\ell-1}, a_{\ell+1} \dots, a_n\rangle$ representa a $-a_\ell$. Luego, existen $b_1, \dots, b_{n-2} \in \mathbb{F}$ tal que $\langle a_1, \dots, a_{\ell-1}, a_{\ell+1} \dots, a_n\rangle \simeq \langle -a_\ell, b_1 \dots, b_{n-2}\rangle$. Por Observación 2.2, sumando $\langle a_\ell\rangle$ se tiene que $f \simeq \langle a_\ell, -a_\ell\rangle \perp \langle b_1 \dots, b_{n-2}\rangle$. □

Definición 2.6. Una forma cuadrática sobre $\mathbb{F}$ que representa a todo elemento de $\dot{\mathbb{F}}$ se llama *universal*.

Por la Proposición 2.5, toda forma regular isótropa es universal. La recíproca no es cierta: la $\mathbb{Q}$-forma $\langle 1, 2, 5, -10\rangle$ es universal y anisótropa. Más aún, si $\mathbb{F}$ es un cuerpo que satisface

(I) toda forma cuadrática de dimensión mayor o igual a 5 es isótropa, y
(II) existen formas anisótropas de dimensión 4,

entonces toda forma anisótropa de dimensión 4 es universal.

3. Teorema de Cancelación de Witt

Uno de los resultados más importantes en la teoría de formas cuadráticas sobre cuerpos es el teorema de Cancelación de Witt. Dado que en este curso nos interesa el estudio de las clases de equivalencia de formas regulares, la demostración del teorema que daremos aquí supone regularidad, pero no es necesaria. Comenzamos con el siguiente resultado.

Proposición 3.1. *Sean f, g y h $\mathbb{F}$-formas. Si $g \simeq h$, entonces $f \perp g \simeq f \perp h$.*

Demostración. Si $g \simeq_A h$ y f es de dimensión n, entonces $f \perp g \simeq_B f \perp h$, donde $B = \begin{pmatrix} I_n & 0 \\ 0 & A \end{pmatrix}$. □

Lo que el teorema de Cancelación de Witt afirma es que para formas regulares vale la recíproca. Veamos antes un lema.

Sean (V, B) un espacio cuadrático regular e $y \in V$ tal que $B(y, y) \neq 0$. Consideremos $\rho_y : V \to V$ definida por

$$\rho_y(x) = x - 2\frac{B(x, y)}{B(y, y)}y.$$

Luego, ρ_y es $\mathbb{F}$-endomorfismo de V, $\rho_y(x) = x$, para todo $x \in (\mathbb{F}y)^\perp$ y $B(\rho_y(x), \rho_y(x')) = B(x, x')$, para todo $x, x' \in V$. Ahora, si $\rho_y(x) = 0$, entonces $x \in r(V) = 0$, por la regularidad de (V, B). Esto implica que ρ_y es $\mathbb{F}$-automorfismo de V. Por lo tanto, ρ_y es isometría del espacio (V, B) que deja invariante el subespacio $(\mathbb{F}y)^\perp$ y que aplica y en $-y$. Por esta razón se dice que ρ_y es una *reflexión*.

Lema 3.2. *Sean (V, B) un espacio cuadrático regular y $x, y \in V$ tales que $B(x, x) = B(y, y) \neq 0$. Entonces existe una isometría ρ de V en sí mismo tal que $\rho(x) = y$.*

Demostración. Ya que $B(x + y, x + y) + B(x - y, x - y) = 4B(x, x) \neq 0$, se tiene que $B(x + y, x + y)$ y $B(x - y, x - y)$ no pueden ser ambos nulos. Supongamos que $B(x - y, x - y) \neq 0$, en caso contrario reemplazar y por $-y$ (el cual es una isometría por Ejemplo 1.10). La reflexión ρ_{x-y} es una isometría de V en sí mismo y

$$\rho_{x-y}(x) = x - 2\frac{B(x, x - y)}{B(x - y, x - y)}(x - y) = y$$

pues $B(x - y, x - y) = 2B(x, x - y)$. □

Teorema 3.3. (Teorema de Cancelación de Witt). *Sean f, g y h $\mathbb{F}$-formas regulares. Si $f \perp g \simeq f \perp h$, entonces $g \simeq h$.*

Demostración. Sea $f \simeq \langle a_1, \ldots, a_n \rangle$ una representación diagonal de f, con $a_i \neq 0$, para todo i. Procederemos por inducción en n. Supongamos que $n = 1$. Sea (V, B) un espacio cuadrático correspondiente a la clase de equivalencia de $\langle a_1 \rangle \perp g \simeq \langle a_1 \rangle \perp h$. Entonces existen $x, y \in V$ tales que $B(x, x) = B(y, y) = a_1$ tales que g se identifica con $(\mathbb{F}x)^\perp$ y h con $(\mathbb{F}y)^\perp$, respectivamente, por el Corolario 2.4. Por el Lema 3.2, existe una isometría ρ de V en sí mismo que aplica x en y; luego, ρ aplica $(\mathbb{F}x)^\perp$ en $(\mathbb{F}y)^\perp$, lo que implica $g \simeq h$. Verificar el paso inductivo es fácil y se deja para el lector. □

Corolario 3.4. (Teorema de Descomposición de Witt). *Toda forma cuadrática sobre $\mathbb{F}$ regular se descompone como una suma ortogonal*

$$f \simeq f_{\mathrm{a}} \perp \mathfrak{h} \perp \cdots \perp \mathfrak{h} = f_{\mathrm{a}} \perp \mathfrak{h}^{\perp r},$$

donde f_{a} es una subforma anisótropa de f que está unívocamente determinada (salvo isometría), r es entero no negativo y $\mathfrak{h}$ es la forma cuadrática asociada al plano hiperbólico H.

La subforma f_{a} se llama la *parte anisótropa* de f, o la *forma núcleo* de f , y r recibe el nombre de *índice de Witt* de f.

Demostración. Si f es anisótropa, entonces tomamos $f_{\mathrm{a}} = f$ y $r = 0$. Supongamos que f es isótropa. Por la Proposición 2.5, se puede escribir $f \simeq \mathfrak{h} \perp f_1$. Si f_1 es anisótropa, entonces el teorema queda demostrado; en caso contrario, aplicamos el procedimiento a f_1. Despues de un número finito de pasos se llega a la descomposición buscada. La unicidad (salvo isometría) de f_{a} es consecuencia del Teorema 3.3. □

4. Anillo de Witt

El objetivo de esta sección es munir al conjunto de las clases de isometría de $\mathbb{F}$-formas con una estructura de anillo. La suma será la suma ortogonal vista anteriormente y el producto estará dado por el *producto tensorial de formas cuadráticas* que describiremos a continuación.

4.1. Producto tensorial de formas cuadráticas y anillo de Witt.

Definición 4.1. Sean (V_1, B_1), (V_2, B_2) $\mathbb{F}$-espacios cuadráticos. El *producto tensorial* de los $\mathbb{F}$-espacios cuadráticos dados es (V, B), donde $V = V_1 \otimes V_2$ y $B : V \times V \to \mathbb{F}$ es la única forma bilineal simétrica que satisface $B(x_1 \otimes y_1, x_1 \otimes y_1) = B_1(x_1, y_1)B_2(x_2, y_2)$.

Así, si f y g son dos formas cuadráticas de dimensión n y m, respectivamente, donde $f = \langle a_1, \ldots, a_n\rangle$ y $g = \langle b_1, \ldots, b_m\rangle$, entonces el producto tensorial de f y g es la forma

$$f \otimes g = \langle a_1b_1, \ldots, a_1b_m, a_2b_1, \ldots, a_2b_m, , \ldots, a_nb_1, \ldots, a_nb_m\rangle.$$

Es inmediato comprobar que el producto tensorial definido es asociativo, conmutativo, distributivo respecto de la suma ortogonal de formas diagonales y tiene elemento identidad la $\mathbb{F}$-forma unaria $\langle 1\rangle$. Además, $f \otimes \mathfrak{h} = \mathfrak{h}^{\perp \dim f}$. Por otro lado, se verifica fácilmente que si $f \simeq f'$ y $g \simeq g'$, entonces $f \otimes g \simeq f' \otimes g'$. Esto permite definir el producto tensorial entre clases de isometría de $\mathbb{F}$-formas como $(f) \otimes (g) = (f \otimes g)$.

Como señalamos anteriormente nuestro interés es estudiar las clases de isometría de $\mathbb{F}$-formas, por lo que, para simplificar la notación identificaremos las clases de isometría con sus representantes, y algunas veces escribiremos $=$ en lugar de $\simeq$.

Definición 4.2. Se dice que dos $\mathbb{F}$-formas f y g son *Witt-equivalentes* y se denota por $f \sim g$, si $f_{\mathrm{a}} = g_{\mathrm{a}}$, es decir si f y g tienen la misma parte anisótropa.

Por ejemplo, la forma cuadrática cero 0 tiene la misma parte anisótropa que $\mathfrak{h}$; así, $0 \sim \mathfrak{h}$. La Witt-equivalencia $\sim$ es relacion de equivalencia sobre el conjunto de la clase de isometría de $\mathbb{F}$-formas. Al conjunto cociente lo denotamos por $W\mathbb{F}$. Las operaciones de suma ortogonal y producto tensorial se extienden naturalmente al conjunto de clases de Witt-equivalencia el cual resulta un anillo conmutativo con identidad la clase de $\langle 1\rangle$.

Definición 4.3. Llamaremos a $W\mathbb{F} = (W\mathbb{F}, \perp, \otimes)$ el *anillo de Witt* de formas cuadráticas sobre $\mathbb{F}$.

Notar que $\langle a\rangle \perp \langle -a\rangle = \langle a, -a\rangle = 0$ en $W\mathbb{F}$; luego, $\langle -a\rangle = -\langle a\rangle$. Más aún, si $f = \langle a_1, \ldots, a_n\rangle$, entonces $-f = \langle -a_1, \ldots, -a_n\rangle$. Además, puede verse que dos $\mathbb{F}$-formas f y g son isométricas si y sólo si tienen la misma dimensión y representan el mismo elemento en $W\mathbb{F}$.

Por construcción $W\mathbb{F}$ está en correspondencia biyectiva con el conjunto de formas cuadráticas regulares y anisótropas sobre $\mathbb{F}$; por esta razón se suele referir a $W\mathbb{F}$ como el anillo de formas anisótropas sobre $\mathbb{F}$. Notar que la suma ortogonal de formas anisótropas puede ser isótropas, por ejemplo $\langle a\rangle \perp \langle -a\rangle = \langle a, -a\rangle = \mathfrak{h}$. Por lo tanto, la anterior es sólo una manera de referirse a $W\mathbb{F}$.

Observación 4.4. Sea $\mathbb{F}$ un cuerpo *cuadráticamente cerrado*, es decir, que todo elemento de $\mathbb{F}$ es un cuadrado. Si $a \in \dot{\mathbb{F}}$, entonces $\langle a\rangle \simeq \langle 1\rangle$. Esto implica que $f \simeq g$ si y sólo si $\dim f = \dim g$. Si $\dim f$ es par, entonces f es hiperbólica y si $\dim f$ es impar, entonces $f = \langle 1\rangle$, por lo que $W\mathbb{F}$ es isomorfo a $\mathbb{Z}_2$.

4.2. Anillo de Witt sobre cuerpos finitos $\mathbb{F}_q$, con q impar. El siguiente resultado muestra una aplicación cuando $\mathbb{F}$ es un cuerpo finito de característica distinta de 2.

Proposición 4.5. *Sea p primo, con $p \neq 2$ y $\mathbb{F} = \mathbb{F}_q$, donde $q = p^n$. Entonces:*

(a) *$\mathbb{F}_q/\dot{\mathbb{F}}_q^2$ tiene exactamente dos elementos;*
(b) *en $\mathbb{F}_q$ todo elemento es suma de cuadrados;*
(c) *$-1 \in \dot{\mathbb{F}}_q^2$ si y sólo si $q \equiv 1 \mod 4$ y $-1 \in s\dot{\mathbb{F}}_q^2$ si y sólo si $q \equiv 3 \mod 4$;*
(d) *toda $\mathbb{F}_q$-forma ternaria es isótropa;*
(e) $W\mathbb{F}_q \simeq \begin{cases} \mathbb{Z}_2[\mathbb{F}_q/\dot{\mathbb{F}}_q^2], & \text{si } q \equiv 1 \mod 4, \\ \mathbb{Z}_4 & \text{si } q \equiv 3 \mod 4. \end{cases}$

Demostración. (a). Consideremos la sucesión de grupos

$$1 \to \dot{\mathbb{F}}_q^2 \to \dot{\mathbb{F}}_q \xrightarrow{\pi} \{\pm 1\} \to 1,$$

donde $\pi(x) = x^{\frac{q-1}{2}}$. Así, $x \in \ker \pi$ si y sólo si $x^{\frac{q-1}{2}} = 1$. Tomamos y en la clausura algebraica de $\mathbb{F}_q$ tal que $y^2 = x$; luego, $y^{q-1} = 1$. Esto implica que $y \in \mathbb{F}_q$, pues $\mathbb{F}_q$ es el cuerpo de descomposición del polinomio $X^q - X$ sobre su cuerpo primo. Por lo tanto, x es un cuadrado en $\mathbb{F}_q$ y $\ker \pi = \dot{\mathbb{F}}_q^2$.

(b). Denotemos por 1 y s los representantes de las dos clases cuadradas de $\mathbb{F}_q$. Luego $\dot{\mathbb{F}}_q = \dot{\mathbb{F}}_q^2 \cup s\dot{\mathbb{F}}_q^2$; lo que nos dice que basta demostrar que s es la suma de dos cuadrados en $\mathbb{F}_q$. Si $-1 \in \dot{\mathbb{F}}_q^2$, entonces $\langle 1, 1\rangle \simeq \langle 1, -1\rangle$, lo que implica que $\langle 1, 1\rangle$ es universal y representa en particular a s. Si $-1 \notin \dot{\mathbb{F}}_q^2$, entonces $1 + \dot{\mathbb{F}}_q^2$ no contiene al cero, y como $\operatorname{card}(1 + \dot{\mathbb{F}}_q^2) = \operatorname{card} \dot{\mathbb{F}}_q^2$ se tiene que $1 + \dot{\mathbb{F}}_q^2$ no está contenido en $\dot{\mathbb{F}}_q^2$; en consecuencia $1 + u^2 \notin \dot{\mathbb{F}}_q^2$. Por lo tanto, $1 + u^2 \notin s\dot{\mathbb{F}}_q^2$, y s resulta suma de cuadrados.

(c). Es clara. (d). Las formas binarias sobre $\mathbb{F}_q$ son $\langle 1, 1\rangle$, $\langle s, s\rangle$ y $\langle 1, s\rangle$. Las dos primeras son universales por (b), mientras que la tercera lo es puesto que $\dot{\mathbb{F}}_q = \dot{\mathbb{F}}_q^2 \cup s\dot{\mathbb{F}}_q^2$. Sea $\langle a, b, c\rangle$ una $\mathbb{F}_q$-forma ternaria; $\langle b, c\rangle$ representa a $-a$. Luego, $\langle b, c\rangle \simeq \langle -a, x\rangle$; esto implica que $\langle a, b, c\rangle \simeq \langle -a, a, x\rangle$ y por lo tanto $\langle a, b, c\rangle$ es isótropa.

(e). Si $q \equiv 1 \mod 4$, entonces las formas anisótropas sobre $\mathbb{F}$ son 0, $\langle 1\rangle$, $\langle s\rangle$, $\langle 1, s\rangle$, por (c) y (d). Luego identificando el grupo de unidades de $W\mathbb{F}_q$, esto es $\langle 1\rangle$, $\langle s\rangle$ con $\mathbb{F}_q/\dot{\mathbb{F}}_q^2$, concluimos lo afirmado.

Por otro lado, si $q \equiv 3 \mod 4$, entonces las formas anisótropas sobre $\mathbb{F}$ son 0, $\langle 1\rangle$, $\langle -1\rangle$, $\langle 1, 1\rangle$. Como $\langle -1\rangle$ es la parte anisótropa de $\langle 1, 1, 1\rangle$, las clases de $W\mathbb{F}_q$ pueden representarse por 0, $\langle 1\rangle$, $\langle 1, 1\rangle$ y $\langle 1, 1, 1\rangle$ de donde resulta que $W\mathbb{F}_q$ es isomorfo a $\mathbb{Z}_4$. □

4.3. Cuerpo euclidiano. Signatura de una forma cuadrática.

Definición 4.6. Un cuerpo se dice *euclidiano* si tiene exactamente dos clases módulo cuadrados y satisface que la forma $\langle 1\rangle^{\perp n} = \langle 1, \ldots, 1\rangle$ es anisótropa para todo $n \in N$.

Observación 4.7. El cuerpo de números reales $\mathbb{R}$ es euclidiano.

Sea $\mathbb{F}$ un cuerpo euclidiano. Como $\dot{\mathbb{F}}/\dot{\mathbb{F}}^2 = \{\pm 1\}$, toda forma cuadrática (regular) f sobre $\mathbb{F}$ tiene una diagonalización $f \simeq \langle a_1, \ldots, a_n\rangle$, donde $a_1 = \cdots = a_r = 1$ y $a_{r+1} = \cdots = a_n = -1$. Si $r = 0$ o $r = n$, entonces f es anisótropa, en caso contrario, f es isótropa. Definamos $s := n - r$. Veamos que r y s no dependen de la diagonalización empleada. Consideremos dos diagonalizaciones de f y escribamos $f \simeq \langle 1\rangle^{\perp r_1} \perp \langle -1\rangle^{\perp s_1} \simeq \langle 1\rangle^{\perp r_2} \perp \langle -1\rangle^{\perp s_2}$. Si $s_1 \geq s_2$, entonces $\langle 1\rangle^{\perp r_1} \perp \langle -1\rangle^{\perp (s_1 - s_2)} \simeq$

$\langle 1\rangle^{\perp r_2}$, por el Teorema de Cancelación de Witt; si $s_1 - s_2 > 0$, entonces la forma $\langle 1\rangle^{\perp r_1} \perp \langle -1\rangle^{\perp(s_1-s_2)}$ es isótropa, por lo que $\langle 1\rangle^{\perp r_2}$ también, lo cual no es posible en $\mathbb{F}$ (recordar que la forma 0 es anisótropa). Luego, $s_1 = s_2$ y, por el Teorema de Cancelación de Witt, $\langle 1\rangle^{\perp r_1} \simeq \langle -1\rangle^{\perp r_2}$. Con el mismo argumento se concluye que $r_1 = r_2$.

Esto nos permite dar la siguiente definición.

Definición 4.8. Sea f una forma cuadrática sobre un cuerpo euclidiano $\mathbb{F}$. Se define la *signatura* de f como $\operatorname{sgn} f := (r, s)$.

Lo hecho en el párrafo anterior prueba el siguiente resultado.

Teorema 4.9. (Ley de Inercia de Sylvester). *Sobre un cuerpo euclidiano dos formas cuadráticas f y g son isométricas y si sólo si tienen las misma dimensión y la misma signatura.* □

El *rango* de una forma cuadrática f es el rango de su matriz asociada m_f y se denota $\operatorname{rg} f$. Se ve inmediatamente que si $\mathbb{F}$ euclidiano, entonces $\operatorname{rg} f = r + s$.

La signatura sgn puede extenderse al anillo WF. Definimos la *signatura* en $W\mathbb{F}$ como la aplicación $\operatorname{Sgn} : W\mathbb{F} \to Z$ dada por $\operatorname{Sgn}(q) \in \mathbb{Z}$. Esta definición es consistente pues $\operatorname{Sgn} \mathfrak{h} = 0$. Es fácil verificar que Sgn es un homomorfismo de anillos; más aún, si $\operatorname{Sgn}(q) = 0$, entonces q es hiperbólica. Luego, $\operatorname{Sgn} : W\mathbb{F} \to \mathbb{Z}$ es un isomorfismo de anillos.

5. Formas de Pfister

5.1. Ideal fundamental de $W\mathbb{F}$. Consideremos el anillo de Witt $W\mathbb{F}$ de formas cuadráticas anisótropas sobre un cuerpo $\mathbb{F}$. Denotaremos por $I\mathbb{F}$ al subconjunto de $W\mathbb{F}$ formado por todas las formas de dimensión par sobre $\mathbb{F}$. Es claro que $I\mathbb{F}$ es un ideal de $W\mathbb{F}$; se lo llama *ideal fundamental* de $W\mathbb{F}$.

Proposición 5.1. *El ideal $I\mathbb{F}$ es maximal en $W\mathbb{F}$ y está generado aditivamente por formas binarias del tipo $\langle 1, a\rangle$, $a \in \dot{\mathbb{F}}$. Además, $I\mathbb{F}$ es el único ideal primo de $W\mathbb{F}$ que contiene a $\langle 1, 1\rangle$.*

Demostración. Como $W\mathbb{F}/I\mathbb{F} \simeq \mathbb{Z}_2$, $I\mathbb{F}$ es ideal maximal. Por otro lado, toda forma $\langle a, b\rangle$ en $W\mathbb{F}$ puede escribirse como $\langle a, b\rangle = \langle 1, a\rangle + \langle -1, b\rangle = \langle 1, a\rangle - \langle 1, -b\rangle$; en consecuencia $I\mathbb{F}$ está generado aditivamente por formas $\langle 1, a\rangle$, $a \in \dot{\mathbb{F}}$.

Veamos la última afirmación. Sea P un ideal primo de $W\mathbb{F}$ tal que $\langle 1, 1\rangle \in P$. Luego, $\langle 1\rangle^{\perp 2} = 0$ en $W\mathbb{F}/P$, por lo que $W\mathbb{F}/P$ es un dominio de integridad de característica 2. Como $(\langle a\rangle + \langle 1\rangle) - (\langle a\rangle - \langle 1\rangle) = 0$ en $W\mathbb{F}$, se tiene que $\langle a\rangle = \langle 1\rangle$ o $\langle a\rangle = -\langle 1\rangle$. Esto implica que si $q = \langle a_1, \ldots, a_n\rangle \in I\mathbb{F}$, entonces $q = 0$ en $W\mathbb{F}/P$. Por lo tanto, $I\mathbb{F} \subseteq P$, y por la maximalidad $I\mathbb{F} = P$. □

Sea P un ideal primo de $W\mathbb{F}$. Definiremos la *característica de P* en $W\mathbb{F}$ como la característica del dominio de integridad $W\mathbb{F}/P$ y la denotamos por $\operatorname{car} P$. Por ejemplo, como vimos, la característica de $I\mathbb{F}$ en $W\mathbb{F}$ es 2.

Proposición 5.2. *Si P es un ideal primo de $W\mathbb{F}$ y $\operatorname{car} P = p$, con p primo, entonces $W\mathbb{F}/P \simeq \mathbb{Z}_p$.*

Demostración. Como $W\mathbb{F}$ está generado aditivamente por formas $\langle a\rangle$, $a \in \mathbb{F}$, y en $W\mathbb{F}/P$ es $\langle a\rangle = \langle 1\rangle$ o $\langle a\rangle = \langle -1\rangle$, se tiene que la imagen de $W\mathbb{F}$ en $W\mathbb{F}/P$ está generada aditivamente por $\langle 1\rangle$. Luego, $W\mathbb{F}/P$ es isomorfo a $\mathbb{Z}_p$ pues $\operatorname{car} P = p$. □

5.2. Formas de Pfister sobre $\mathbb{F}$. Como $I\mathbb{F}$ está generado aditivamente por las formas $\langle 1, a\rangle$, $a \in \dot{\mathbb{F}}$, se tiene que para $n \geq 1$, $(I\mathbb{F})^n = I^n\mathbb{F}$ está generado aditivamente por las formas $\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \langle 1, a_n\rangle$, $a \in \dot{\mathbb{F}}$. Denotaremos a estas formas por $\langle\langle a_1, \ldots, a_n\rangle\rangle$ y las llamaremos *n-formas de Pfister sobre* $\mathbb{F}$. Es inmediato observar que

1. toda n-forma de Pfister es de dimensión 2^n;
2. toda n-forma de Pfister representa a 1;
3. $\langle\langle 1, a_2, \ldots, a_n\rangle\rangle \simeq \langle\langle a_2, \ldots, a_n\rangle\rangle^{\perp 2}$;
4. $\langle\langle -1, a_2, \ldots, a_n\rangle\rangle \simeq \mathfrak{h}^{\perp 2^{n-1}}$.

Convenimos en considerar como 0-forma de Pfister la forma unidimensional $\langle 1\rangle$. Antes de probar algunas propiedades importantes de las formas de Pfister veamos algunos resultados.

Lema 5.3. (a) *Si $b \in D_{\mathbb{F}}(\langle\langle a_1\rangle\rangle)$, entonces $\langle\langle a_1, a_2\rangle\rangle \simeq \langle\langle a_1, a_2 b\rangle\rangle$.*
(b) *Si $c \in D_{\mathbb{F}}(\langle a_1, a_2\rangle)$, entonces $\langle\langle a_1, a_2\rangle\rangle \simeq \langle\langle c, a_1 a_2\rangle\rangle$.*

Demostración. (a). Puesto que $b \in D_{\mathbb{F}}(\langle\langle a_1\rangle\rangle)$, $\langle 1, a_1\rangle$, resulta que $\langle b, a_1 b\rangle$ son isométricas pues tienen el mismo determinante y representan un elemento en común. Luego,

$$\begin{aligned}\langle\langle a_1, a_2\rangle\rangle &\simeq \langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \simeq \langle 1, a_1\rangle \perp \big(\langle a_2\rangle \otimes \langle 1, a_1\rangle\big) \simeq \\ &\simeq \langle 1, a_1\rangle \perp \big(\langle a_2\rangle \otimes \langle b, a_1 b\rangle\big) \simeq \langle 1, a_1, a_2 b, a_1 a_2 b\rangle \simeq \langle\langle a_1, a_2 b\rangle\rangle.\end{aligned}$$

(b). Se tiene que $\langle\langle a_1, a_2\rangle\rangle \simeq \langle 1\rangle \perp \langle a_1, a_2\rangle \perp \langle a_1 a_2\rangle$. Luego,

$$\langle\langle a_1, a_2\rangle\rangle \simeq \langle 1, c, c a_1 a_2, a_1 a_2\rangle \simeq \langle\langle c, a_1 a_2\rangle\rangle,$$

pues $\langle a_1, a_2\rangle \simeq \langle c, c a_1 a_2\rangle$. □

Dada una n-forma de Pfister f existe una única (salvo isometría) forma f' tal que $f \simeq \langle 1\rangle \perp f'$. A f' se la llama la *subforma pura* de f.

Teorema 5.4. (Teorema de la subforma pura). *Sean $f \simeq \langle\langle a_1, \ldots, a_n\rangle\rangle$ una n-forma de Pfister y $b \in \dot{\mathbb{F}}$. Entonces $b \in D_{\mathbb{F}}(f')$ si y sólo si existen $b_2, \ldots, b_n \in \dot{\mathbb{F}}$ tales que $f \simeq \langle\langle b, b_2, \ldots, b_n\rangle\rangle$.*

Demostración. Si existen $b_2, \ldots, b_n \in \dot{\mathbb{F}}$ tales que $f \simeq \langle\langle b, b_2, \ldots, b_n\rangle\rangle$, entonces

$$\langle 1\rangle \perp f' \simeq f \simeq \langle 1, b\rangle \otimes \langle 1, b_2\rangle \otimes \cdots \otimes \langle 1, b_n\rangle \simeq \langle 1, b, b_2, \ldots\rangle \simeq \langle 1\rangle \perp \langle b, b_2, \ldots\rangle,$$

y, por el Teorema de Cancelación de Witt, resulta que $b \in D_{\mathbb{F}}(f')$.

Probaremos la recíproca por inducción en n. Si $n = 1$, entonces $f \simeq \langle\langle a_1\rangle\rangle$ y $f' \simeq \langle a_1\rangle$; luego, $b \in D_{\mathbb{F}}(\langle a_1\rangle)$ implica que $\langle a_1\rangle \simeq \langle b\rangle$, y entonces $f \simeq \langle\langle b\rangle\rangle$. Veamos el paso inductivo. Definimos $g \simeq \langle\langle a_1, \ldots, a_{n-1}\rangle\rangle$. Se tiene que $f \simeq g \otimes \langle 1, a_n\rangle \simeq g \perp \langle a_n\rangle \otimes g$; luego, $f' \simeq g' \perp \langle a_n\rangle \otimes g$. Como $b \in D_{\mathbb{F}}(f')$, se tiene que $b = u' + a_n v$, donde $u' \in D_{\mathbb{F}}(g') \cup \{0\}$ y $v \in D_{\mathbb{F}}(g) \cup \{0\}$. Puesto que $v \in D_{\mathbb{F}}(g) \cup \{0\}$, podemos escribir $v = t^2 + v'$, con $v' \in D_{\mathbb{F}}(g') \cup \{0\}$. Por hipótesis inductiva,

$$g \simeq \begin{cases} \langle\langle u', c_2, \ldots, c_{n-1}\rangle\rangle, & \text{si } u' \neq 0, \\ \langle\langle v', d_2, \ldots, d_{n-1}\rangle\rangle, & \text{si } v' \neq 0. \end{cases}$$

Si $v = 0$, entonces $u' = b \in \dot{\mathbb{F}}$ y $f \simeq g \otimes \langle\langle a_n\rangle\rangle \simeq \langle\langle b, c_2, \ldots, c_{n-1}, a_n\rangle\rangle$, con lo que el teorema quedaría demostrado. Supongamos que $v \neq 0$; vamos a probar que

$$f \simeq \langle\langle a_1, \ldots, a_{n-1}, v a_n\rangle\rangle. \tag{5.1}$$

Podemos asumir que $v' \neq 0$, pues en caso contrario $v = t^2$ y (5.1) es obvio. Luego,

$$f \simeq g \otimes \langle\langle a_n \rangle\rangle \simeq \langle\langle v', d_2, \dots, d_{n-1}, a_n \rangle\rangle \simeq \langle\langle d_2, \dots, d_{n-1} \rangle\rangle \otimes \langle\langle v', a_n \rangle\rangle \overset{\text{Lema 5.3 (a)}}{\simeq}$$
$$\simeq \langle\langle d_2, \dots, d_{n-1} \rangle\rangle \otimes \langle\langle v', a_n v \rangle\rangle \simeq \langle\langle v', d_2, \dots, d_{n-1}, a_n v \rangle\rangle \simeq \langle\langle a_1, \dots, a_{n-1}, a_n v \rangle\rangle.$$

Ahora, si $u' = 0$, entonces $b = a_n v$, y (5.1) nos terminaría la prueba. Por otro lado, si $u' \neq 0$, entonces

$$f \simeq \langle\langle u', c_2, \dots, c_{n-1}, a_n v \rangle\rangle \simeq \langle\langle u', a_n v \rangle\rangle \otimes \langle\langle c_2, \dots, c_{n-1} \rangle\rangle \simeq$$
$$\simeq \langle\langle u' + a_n v, u' a_n v \rangle\rangle \otimes \langle\langle c_2, \dots, c_{n-1} \rangle\rangle \simeq \langle\langle b, c_2, \dots, c_{n-1}, u' a_n v \rangle\rangle,$$

lo que finaliza la demostración. □

5.3. Grupo de isotropía de una forma cuadrática. Dada una forma cuadrática f sobre $\mathbb{F}$, es fácil ver que $G_{\mathbb{F}}(f) := \{a \in \dot{\mathbb{F}} : \langle a \rangle \otimes f \simeq f\}$ es un subgrupo de $\dot{\mathbb{F}}$.

Definición 5.5. Llamaremos a $G_{\mathbb{F}}(f)$ el *grupo de isotropía* de f.

Teorema 5.6. *Sea f una n-forma de Pfister sobre $\mathbb{F}$.*

(a) *Si f es isótropa, entonces es hiperbólica.*

(b) *$D_{\mathbb{F}}(f)$ es subgrupo del grupo multiplicativo $\dot{\mathbb{F}}$.*

Demostración. (a). Si f isótropa, entonces contiene un plano hiperbólico y se puede escribir como $\langle 1 \rangle \perp f' \simeq f \simeq \langle 1, -1 \rangle \perp g$. Cancelando $-1 \in D_{\mathbb{F}}(f')$ y aplicando el teorema anterior se tiene que $f \simeq \langle\langle -1, \cdots \simeq \mathfrak{h}^{\perp 2^{n-1}} \rangle\rangle$.

(b). Es inmediato que $G_{\mathbb{F}}(f) \subseteq D_{\mathbb{F}}(f)$. Si $a \in D_{\mathbb{F}}(f)$, entonces $\langle -1, a \rangle \otimes f \simeq f \perp \langle -a \rangle \otimes f \simeq f \perp \langle -a, \dots \rangle$, y en consecuencia $\langle -1, a \rangle \otimes f$ es isótropa y, por lo tanto, hiperbólica. Así, $f = \langle a \rangle \cdot f$ en $W\mathbb{F}$; luego, por dimensión, se tiene que $f \simeq \langle a \rangle \otimes f$ y $a \in G_{\mathbb{F}}(f)$. Por lo tanto, $G_{\mathbb{F}}(f) = D_{\mathbb{F}}(f)$ y, en particular, $D_{\mathbb{F}}(f)$ es subgrupo de $\dot{\mathbb{F}}$. □

Observamos que $\langle 1 \rangle^{\perp 2^n}$ es una n-forma de Pfister sobre $\mathbb{F}$ y que $a \in D_{\mathbb{F}}(\langle 1 \rangle^{\perp 2^n})$ si y sólo si a es suma de 2^n cuadrados en $\dot{\mathbb{F}}$. Por el Teorema 5.6, las sumas de 2^n cuadrados forman un grupo multiplicativo en $\dot{\mathbb{F}}$. Este resultado está vinculado a un problema de gran interés en la teoría de números: *si en un cuerpo $\mathbb{F}$ la suma de m cuadrados multiplicada por la suma de m cuadrados es siempre una suma de m cuadrados, entonces m es potencia de 2 y recíprocamente*. Los casos $m = 1, 2, 4, 8$, son resultados conocidos desde hace tiempo, en particular, el caso $m = 4$ se conoce como la identidad de Euler-Lagrange y el caso $m = 8$ se conoce como la identidad de Cayley. A. Hurwitz demostró que si el producto de la suma de m cuadrados por la suma de m cuadrados es siempre una suma de m cuadrados donde además estos últimos dependen linealmente de los primeros, entonces $m = 1, 2, 4$ u 8. En 1965, A. Pfister probó que si no se pide la condición de linealidad mencionada, entonces para todo n y sobre cualquier cuerpo las sumas de 2^n cuadrados forman un grupo.

6. Formas cuadráticas reales

En esta sección damos brevemente la clasificación de las formas cuadráticas sobre el cuerpo de los números reales $\mathbb{R}$. Mencionaremos dos maneras de clasificar formas cuadráticas f sobre $\mathbb{R}$: una según la signatura de f y otra según los menores principales de la matriz asociada m_f.

Primero recordamos que una matriz simétrica $A \in \mathbb{R}^{n \times n}$ se dice:

(a) *definida positiva* si y sólo si $x^t \cdot A \cdot x > 0$, para todo $x \in \mathbb{R}^{n \times 1} - \{0\}$ si y sólo si todos los autovalores de A son estrictamente positivos;

(b) *definida negativa* si y sólo si $x^t \cdot A \cdot x < 0$, para todo $x \in \mathbb{R}^{n\times 1} - \{0\}$ si y sólo si todos los autovalores de A son estrictamente negativos;
(c) *semidefinida positiva* si y sólo si $x^t \cdot A \cdot x \geq 0$, para todo $x \in \mathbb{R}^{n\times 1} - \{0\}$, y existe $x \in \mathbb{R}^{n\times 1} - \{0\}$ tal que $x^t \cdot A \cdot x = 0$ si y sólo si A tiene autovalores positivos, no tiene autovalores negativos y el 0 es autovalor de A;
(d) *semidefinida negativa* si y sólo si $x^t \cdot A \cdot x \leq 0$, para todo $x \in \mathbb{R}^{n\times 1} - \{0\}$, y existe $x \in \mathbb{R}^{n\times 1} - \{0\}$ tal que $x^t \cdot A \cdot x = 0$ si y sólo si A tiene autovalores negativos, no tiene autovalores positivos y el 0 es autovalor de A;
(e) *indefinida* si y sólo si existen $x, y \in \mathbb{R}^{n\times 1} - \{0\}$ tales que $x^t \cdot A \cdot x > 0$ e $y^t \cdot A \cdot y < 0$ si y sólo si A tiene al menos un autovalor positivo y al menos uno negativo.

Definición 6.1. Sea f una forma cuadrática sobre $\mathbb{R}$ y m_f su matriz asociada (ver (1.3)). Se dice que f es *definida positiva* (resp. *negativa*), *semidefinida positiva* (resp. *negativa*), *indefinida* si m_f es definida positiva (resp. negativa), semidefinida positiva (resp. negativa), indefinida, respectivamente.

Recordamos que f se dice nula cuando $x^t \cdot m_f \cdot x = 0$, para todo $x \in \mathbb{R}^{n\times 1}$.

En la Observación 4.7, se mencionó que $\mathbb{R}$ es un cuerpo euclidiano. Luego, si f es una forma cuadrática de dimensión n sobre $\mathbb{R}$, entonces f tiene una diagonalización $f \simeq \langle a_1, \ldots, a_n\rangle$, donde $a_1, \ldots, a_r$ son todos positivos, $a_{r+1}, \ldots, a_{r+s}$ son todos negativos y $a_{r+s+1} = \cdots = a_n = 0$. El rango y la signatura de f son $\operatorname{rg} f = r + s$ y $\operatorname{sgn} f = (r, s)$, respectivamente. Así, podemos dar la clasificación de las formas cuadráticas sobre $\mathbb{R}$ mediante su signatura de la siguiente manera.

Teorema 6.2. *Sea f una forma cuadrática de dimensión n sobre $\mathbb{R}$. Entonces f es:*
(a) *definida positiva si y sólo si* $\operatorname{sgn} f = (n, 0)$;
(b) *definida negativa si y sólo si* $\operatorname{sgn} f = (0, n)$;
(c) *semidefinida positiva si y sólo si* $\operatorname{sgn} f = (r, 0)$, *con* $0 < r < n$;
(d) *semidefinida negativa si y sólo si* $\operatorname{sgn} f = (0, s)$, *con* $0 < s < n$;
(e) *indefinida si y sólo si* $\operatorname{sgn} f = (r, s)$ *con* $0 < r, s$;
(f) *nula si y sólo si* $\operatorname{sgn} f = (0, 0)$. □

Si bien se puede obtener siempre una diagonalización de f, resulta útil clasificar las formas cuadráticas sobre $\mathbb{R}$ de acuerdo a los menores principales de m_f. Para una matriz $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$ y k, con $1 \leq k \leq n$, definimos $A_k = \begin{pmatrix} a_{11} & \ldots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \ldots & a_{kk} \end{pmatrix}$, y denotamos por $\Delta_k = \det A_k$ al k-ésimo menor principal de A.

Proposición 6.3. (Criterio de Sylvester o de los menores principales). *Sea f una forma cuadrática de dimensión n sobre $\mathbb{R}$. Entonces f es*
(i) *definida positiva si y sólo si* $\Delta_k > 0$, *para todo* k, $1 \leq k \leq n$;
(ii) *definida negativa si y sólo si* $(-1)^k \Delta_k > 0$, *para todo* k, $1 \leq k \leq n$;
(iii) *semidefinida positiva si* $\Delta_k > 0$, *para todo* k, $1 \leq k \leq n-1$ *y* $\Delta_n = 0$;
(iv) *semidefinida negativa si* $(-1)^k \Delta_k > 0$, *para todo* k, $1 \leq k \leq n-1$ *y* $\Delta_n = 0$;
(v) *indefinida si o bien* $\Delta_k \neq 0$, $1 \leq k \leq n$, *y no se cumple* (i) *ni* (ii), *o bien* $\Delta_k \neq 0$, $1 \leq k \leq n-1$, $\Delta_n = 0$ *y no se cumple* (iii) *ni* (iv). □

Ejercicios

1. Sean $f(X_1, X_2, X_3) = X_1^2 + X_3^2 - 2X_1X_2 - 2X_1X_3 + 10X_2X_3$ y $g(X_1, X_2, X_3) = X_1^2 - X_2^2 + 8X_2X_3$. Mostrar que $f \simeq g$.

2. Sean (V, B) un espacio cuadrático regular y U un subespacio de V. Probar que
   a) $\dim V = \dim U + \dim U^{\perp}$.
   b) $(U^{\perp})^{\perp} = U$.
3. Sea (V, B) un espacio cuadrático regular. Demostrar que un subespacio U de V es regular si y sólo si existe un subespacio W de V tal que $V = U \perp W$.
4. Sea (V, B) un espacio cuadrático de dimensón 2. Probar que son equivalentes
   a) V es regular e isótropo (es decir, plano hiperbólico).
   b) V es regular con $d(V) = -1$.
5. Dos formas binarias $f = \langle a, b\rangle$ y $g = \langle c, d\rangle$ son isométricas si y sólo si representan un elemento en común y tienen el mismo determinante módulo $\dot{\mathbb{F}}^2$, o sea $d(f) = d(g) \mod \dot{\mathbb{F}}^2$.
6. Sean (V, B) un espacio cuadrático regular y U un subespacio no nulo de V *totalmente isótropo*, o sea $B(u, u) = 0$, para todo $u \in U$. Demostrar que existe un subespacio W de V, con $\dim W = 2 \dim U$ tal que U esta contenido en W.
7. Para un cuerpo $\mathbb{F}$ demostrar que son equivalentes:
   a) toda $\mathbb{F}$-forma de dimensión 4 y determinante -1 es isótropa;
   b) toda $\mathbb{F}$-forma de dimensión par y determinante -1 es isótropa;
   c) toda $\mathbb{F}$-forma de dimensión 3 representa a su determinante;
   d) toda $\mathbb{F}$-forma de dimensión impar representa a su determinante.
8. Mostrar que para cada $n \in \mathbb{N}$ la forma $f(X_1, \dots, X_{2n}) = X_1X_2 + X_3X_4 + \cdots + X_{2n-1}X_{2n}$ es hiperbólica y que es equivalente a la forma diagonal $g(Y_1, \dots, Y_{2n}) = Y_1^2 - Y_2^2 + Y_3^2 - Y_4^2 + \cdots + Y_{2n-1}^2 - Y_{2n}^2$.
9. Si $f \simeq g$ sobre $\mathbb{F}$, entonces $f \perp (-g)$ es equivalente a una forma hiperbólica.
10. Sean a, $b \in \mathbb{F}$ tales que $c = a^2 + b^2 \neq 0$. Probar que el espacio $\langle 1, 1, -c, -c\rangle$ es hiperbólico.
11. Probar que $I^2\mathbb{F}$ está formado por las formas f de dimensión par $2k$ tales que $d(f) = (-1)^{\frac{2k(2k-1)}{2}}$.
    (Ayuda: definir $d_{\pm} : W\mathbb{F} \to \dot{\mathbb{F}}/\dot{\mathbb{F}}^2$ como $d_{\pm}(f) = d(f)(-1)^{\frac{2k(2k-1)}{2}}$. Mostrar que está bien definida y que la restricción a $I\mathbb{F}$ es un epimorfismo de grupos cuyo núcleo es $I^2\mathbb{F}$.)
12. Demostrar que $W\mathbb{F}$ es noetheriano si y sólo si $\mathbb{F}$ tiene un número finito de clases módulo cuadrados.
13. Demostrar que en $W\mathbb{F}$ se tiene $\langle a\rangle \perp \langle b\rangle = \langle a + b\rangle \otimes (\langle 1\rangle + \langle ab\rangle)$, $a, b, a + b \in \dot{\mathbb{F}}$.
14. Sea f una forma cuadrática sobre un cuerpo $\mathbb{F}$. Demostrar que
    a) $G_{\mathbb{F}}(f)$ es un subgrupo de $\dot{\mathbb{F}}$ tal que $\dot{\mathbb{F}}^2 \subseteq G_{\mathbb{F}}(f)$.
    b) si f es hiperbólica, entonces $G_{\mathbb{F}}(f) = \dot{\mathbb{F}}$.
    c) si f es de dimensión impar, entonces $G_{\mathbb{F}}(f) = \dot{\mathbb{F}}^2$.
    d) Si $a \in D_{\mathbb{F}}(f)$, entonces $aG_{\mathbb{F}}(f) \subseteq D_{\mathbb{F}}(f)$.
    e) $-1 \in G_{\mathbb{F}}(f)$ si y sólo si $f \perp f$ es hiperbólica.
15. Probar que dos formas ternarias isótropas que tienen el mismo determinante son isométricas.
16. Sean $f = \langle a_1, \dots, a_n\rangle$ y $g = \langle b_1, \dots, b_n\rangle$ dos formas diagonales de dimensión n. Se dice que f es *equivalente-simple* a g si existen i, j, $1 \leq i, j \leq n$, tales que $\langle a_i, a_j\rangle \simeq \langle b_i, b_j\rangle$ y $a_k = b_k$ para todo $k \neq i, j$. Se dice que f es *equivalente en cadena* a g si existe una sucesión de formas $f_0, \dots, f_m$, tales que $f_0 = f$, $f_m = g$ y f_{i-1} es equivalente-simple a f_i para todo i, $1 \leq i \leq m$. Probar
    a) La «equivalencia en cadena» es una relación de equivalencia en el conjunto de formas diagonales de la misma dimensión.

b) Dos formas diagonales de la misma dimensión son equivalentes si y sólo si son equivalentes en cadena.

17. Probar que si $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$, entonces $(\langle a_1\rangle - 1)\cdots(\langle a_n\rangle - 1) = (\langle b_1\rangle - 1)\cdots(\langle b_n\rangle - 1)$ en $W\mathbb{F}$.
18. Probar que $I\mathbb{F}$ es el único ideal maximal de $W\mathbb{F}$ que contiene al 2.
19. Probar que $W\mathbb{F}$ es finito si y sólo si -1 es una suma de cuadrados en $\mathbb{F}$ y $\dot{\mathbb{F}}/\dot{\mathbb{F}}^2$ es finito.
20. Toda forma cuadrática de dimensión $n \geq 3$ sobre un cuerpo finito de característica distinta de 2 es isótropa.
21. Sean $\mathbb{F}$ cuerpo, con $|\mathbb{F}| > 5$, y $f = \langle a_1, \ldots, a_n\rangle$. Si f es isótropa, entonces existen $x_1, \ldots, x_n \in \dot{\mathbb{F}}$ tales que $f(x_1, \ldots, x_n) = 0$.
22. Diagonalizar las siguientes formas sobre $\mathbb{R}$ y calcular sus rangos y signaturas.
    a) $f(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2 + X_1X_2 + X_1X_3 + X_2X_3$.
    b) $f(X_1, X_2, X_3) = X_2^2 + 2X_3^2 + 4X_1X_2 + 2X_1X_3$.
    c) $f(X_1, X_2, X_3) = X_1^2 + 2X_2^2 + 2X_1X_2 + 3X_3^2$.
    d) $f(X_1, \ldots, X_n) = \sum_{i=1}^{n-1} X_iX_{i+1}$.
23. Clasificar las formas del Ejercicio 22 según el criterio de Sylvester y según sus signaturas.

Referencias

[1] T. Y. Lam, *The algebraic theory of quadratic forms*, Benjamin, New York (1973).
[2] O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften **No. 117**, Springer-Verlag (1973).
[3] F. M. Piscoya H., *Estructuras algebraicas VI (Formas cuadráticas)*, Serie de Matemática, Monografía **No. 23**, Secretaría Gral. de la Organización de Estados Americanos, Washington (1981).
[4] A. R. Rajwade, *Squares*, London Math. Soc. Lecture Note Ser. **No. 171**, Cambridge Univ. Press (1993).

Facultad de Matemática, Astronomía y Física &
Facultad de Ciencias Exactas, Físicas y Naturales
Universidad Nacional de Córdoba.
CIEM – CONICET.
Medina Allende s/n, Ciudad Universitaria
5000 Córdoba, Argentina
E-mail address: fantino@famaf.unc.edu.ar

EL GRUPO DE HEISENBERG

LINDA SAAL

Índice

1. El grupo de Heisenberg

Denotaremos por $\mathfrak{gl}(n,R)$ el espacio vectorial de las matrices $n \times n$. Si $A, B \in \mathfrak{gl}(n,R)$, definimos el corchete de Lie por

$$[A,B] = AB - BA.$$

Este corchete da una estructura de álgebra de Lie a $\mathfrak{gl}(n,R)$.

En efecto, un álgebra de Lie es un espacio vectorial (real ó complejo) munido de un producto $[,]$ que satisface las siguientes propiedades:

i) $[A,B] = -[B,A]$, (antisimetría)

ii) $[A,[B,C]] + [C,[A,B]] + [B,[C,A]] = 0$ (identidad de Jacobi).

Sea $Gl(n,R) = \{A \in \mathfrak{gl}(n,R) : A \text{ es invertible}\}$. Entonces la aplicación exponencial

$$\exp : \mathfrak{gl}(n,R) \to Gl(n,R),$$

está definida por $\exp(A) = \sum_{n=0}^{\infty} \frac{A^n}{n!}$.

No es ni inyectiva ni suryectiva, pero sí es un difeo local pues $\frac{d\exp(tX)}{dt}(0) = X$ (*probarlo*).

Definición 1.1. El álgebra de Heisenberg $\mathfrak{h}_n$ es la subálgebra de Lie de $\mathfrak{gl}(n,R)$, consistente de las matrices de la forma

$$\begin{pmatrix} 0 & x_1 & . & . & . & x_n & t \\ 0 & . & . & . & . & 0 & y_1 \\ . & & & & & & y_2 \\ . & & & & & & . \\ . & & & & & & . \\ 0 & & & & & & y_n \\ 0 & & & & & & 0 \end{pmatrix}$$

y que denotamos por (x, y, t). Observamos que

$$\left[(x, y, t), \left(x^{'}, y^{'}, t^{'}\right)\right] = \left(0, 0, x.y^{'} - x^{'}.y\right),$$

donde $x.y^{'}$ es el producto escalar canónico en R^n.

Una computación sencilla muestra que

$$\exp \begin{pmatrix} 0 & x_1 & . & . & . & x_n & t \\ 0 & . & . & . & . & 0 & y_1 \\ . & & & & & & . \\ . & & & & & & . \\ . & & & & & & . \\ 0 & & & & & 0 & y_n \\ 0 & . & . & . & . & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & x_1 & . & . & . & x_n & t + \frac{1}{2}x.y \\ 0 & 1. & . & . & . & 0 & y_1 \\ . & & & & & & . \\ . & & & & & & . \\ . & & & & & & . \\ 0 & & & & & & y_n \\ 0 & & & & & & 1 \end{pmatrix}$$

y que toda matriz del tipo

$$\begin{pmatrix} 1 & x_1 & . & . & . & x_n & a \\ 0 & 1. & . & . & . & 0 & y_1 \\ . & & & & & & y \\ . & & & & & & . \\ . & & & & & & . \\ 0 & & & & & & y_n \\ 0 & & & & & & 1 \end{pmatrix} \tag{1.1}$$

es la exponencial de un elemento en $\mathfrak{h}_n$.

Definición 1.2. El grupo de Heisenberg H_n es el subgrupo de $Gl(n, R)$ consistente de las matrices (1.1).

Como $\exp : \mathfrak{h}_n \to H_n$ es un difeomorfismo, H_n admite un sistema de coordenadas globales.

Además,

$$\exp(x, y, t) . \exp\left(x^{'}, y^{'}, t^{'}\right) = \exp\left(x + x^{'}, y + y^{'}, t + t^{'} + \frac{1}{2}\left(x.y^{'} - x^{'}.y\right)\right),$$

y por lo tanto es un grupo de Lie.

Si en $R^{2n+1} = R^n \times R^n \times R$ definimos el producto

$$(x, y, t) . \left(x^{'}, y^{'}, t^{'}\right) = \left(x + x^{'}, y + y^{'}, t + t^{'} + \frac{1}{2}\left(x.y^{'} - x^{'}.y\right)\right),$$

obtenemos un grupo isomorfo al grupo de Heisenberg, donde el isomorfismo viene dado por la exp.

El centro de H_n es $Z = \{(0, 0, t) : t \in \mathbb{R}\}$ y $H_n/Z \simeq \mathbb{R}^{2n}$ (ejercicio).

Proposición 1.3. *El grupo de Heisenberg es unimodular y la medida de Haar es la medida de Lebesgue en* $\mathbb{R}^{2n+1}$.

Demostración. En efecto, como la medida de Lebesgue en $\mathbb{R}^{2n+1}$ es invariante por traslaciones, tenemos que

$$\begin{aligned}\int_{H_n} f\left((x,y,t)\left(x^{'},y^{'},t^{'}\right)\right)dx\,dy\,dt &= \int_{H_n} f\left((x,y,t)\right)dxdydt = \\ &= \int_{H_n} f\left(\left(x^{'},y^{'},t^{'}\right)(x,y,t)\right)dx\,dy\,dt.\end{aligned}$$

y la proposición sigue. □

Podemos definir al grupo de Heisenberg de un modo intrínseco.

Definición 1.4. Una forma bilineal Ψ sobre un espacio vectorial V se dice *no degenerada* si $\Psi(u,v)=0$ para todo $v\in V$ implica $u=0$. Una forma simpléctica es una forma bilineal, antisimétrica, no degenerada, sobre V.

Teorema 1.5. *Si* $\Psi: V\times V\to\mathbb{R}$ *es una forma simpléctica, entonces* $\dim V$ *es par y existe una base* $\{e_{1,...}e_n, f_1,...,f_n,\}$ *de* V *tal que* $\Psi(e_j,e_k)=\Psi(f_j,f_k)=0$, $\Psi(e_j,f_k)=\delta_{j,k}$.

Demostración. Sea $w\in V$. Entonces $\lambda_w: v\to\Psi(v,w)$ es un funcional lineal y $\lambda_w=0\Rightarrow w=0$, pues Ψ es no degenerada.

Por lo tanto $\lambda: V\to V'$ es inyectiva Sea $e_1\neq 0$ y sea f_1 tal que $\Psi(e_1,f_1)=1$. Luego por antisimetría $\Psi(e_1,e_1)=\Psi(f_1,f_1)=0$. En particular, e_1 y f_1 son linealmente independientes. Si $\dim V\geq 3$, existe e_2 tal que $\Psi(e_2,e_1)=\Psi(e_2,f_1)=0$ .En efecto, si v es linealmente independiente con e_1 y con f_1, tomar $e_2=v-\Psi(e_1,v)f_1-\Psi(v,f_1)e_1$. Sea f_2 tal que $\Psi(e_2,f_2)=1$. Iterando este proceso, probamos el teorema. □

La matriz de Ψ en esta base, es de la forma $[\Psi]=\left(\begin{smallmatrix}0 & -I\\ I & 0\end{smallmatrix}\right)$, donde I denota la matriz identidad $n\times n$. Por lo tanto si $(x_1,...x_n,y_1,...y_n)$ son las coordenadas de v con respecto a dicha base y, $(x_1',...x_n',y_1',...y_n')$ las de v', entonces $\Psi(v,v')=x.y'-x'.y$.

Dada una forma simpléctica Ψ sobre V, podemos definir un álgebra de Lie en $V\oplus\mathbb{R}$ por

$$[(v,t),(v',t')]=(0,\Psi(v,v')).$$

Por la antisimetría de Ψ, el corchete $[,]$ es antisimétrico y la igualdad de Jacobi se satisface automáticamente pues $[,[,]]=0$.

Más aún, por el teorema anterior, $V\oplus\mathbb{R}$ es isomorfa al álgebra de Heisenberg. Análogamente, si en $V\oplus\mathbb{R}$ definimos el producto por

$$(v,t)(v',t')=\left(v+v',t+t'+\frac{1}{2}\Psi(v,v')\right),$$

obtenemos un grupo de Lie isomorfo a $H_{n.}$

En particular se puede mirar el grupo de Heisenberg como $\mathbb{C}^n\times\mathbb{R}$ con el producto dado por

$$(z,t).(w,t')=\left(z+w,t+t'-\frac{1}{2}\mathrm{Im}\left(z\overline{w}\right)\right).$$

2. Campos vectoriales invariantes a izquierda

En $\mathbb{R}^n$, los operadores diferenciales que conmutan con traslaciones, son los operadores diferenciales a coeficientes constantes, y constituyen un álgebra generada por $\left\{\frac{\partial}{\partial x_j}, j=1,...,n.\right\}$. En el grupo de Heisenberg, un conjunto de generadores del álgebra de operadores diferenciales que conmutan con las traslaciones del grupo, están dados por

$$\begin{aligned} X_j f(x,y,t) &= \frac{d}{ds}_{/s=0} f((x,y,t)(se_j,0,0)) = \frac{d}{ds}_{/s=0} f\left(se_j+x,y,t-\frac{1}{2}sy_j\right) \\ &= \frac{\partial f}{\partial x_j} - \frac{1}{2}y_j\frac{\partial f}{\partial t}, \end{aligned}$$

$$\begin{aligned} Y_j f(x,y,t) &= \frac{d}{ds}_{/s=0} f((x,y,t)(0,se_j,0)) = \frac{d}{ds}_{/s=0} f\left(x,y+se_j,t+\frac{1}{2}sx_j\right) \\ &= \frac{\partial f}{\partial y_j} + \frac{1}{2}x_j\frac{\partial f}{\partial t}, \end{aligned}$$

$$Tf(x,y,t) = \frac{d}{ds}_{/s=0} f((0,0,s)(x,y,t)) = \frac{d}{ds}_{/s=0} f((x,y,t+s)) = \frac{\partial f}{\partial t}.$$

(Aquí e_j denota el vector en $\mathbb{R}^n$ que tiene un 1 en la coordenada j-ésima y todas las otras coordenadas nulas.)

Identificamos una base del álgebra de Lie $\{(e_j,0,0),(0,e_j,0),(0,0,1),j=1,...,n.\}$, con la correspondiente base de campos invariantes a izquierda $\{X_j,Y_j,T.\}$. Entonces $[X_j,Y_j]=T$ y todos los otros corchetes son nulos.

3. El grupo $Aut(\mathfrak{h}_n)$ de automorfismos de $\mathfrak{h}_n$

Pongamos $\mathfrak{h}_n = V\oplus\mathbb{R}$ y sea $[(v,t),(v',t')] = (0,\Psi(v,v'))$

Definición 3.1. Un automorfismo de $\mathfrak{h}_n$ es una transformación lineal $g:\mathfrak{h}_n\to\mathfrak{h}_n$ tal que

$$g[X,Y] = [g(X),g(Y)] \tag{3.1}$$

para todo $X,Y\in\mathfrak{h}_n$.

Es inmediato ver que basta comprobar (3.1) para vectores de la forma $X=(v,0)$, $Y=(v',0)$, y, por abuso de notación, que

$$g[v,v'] = [gv,gv'].$$

Observemos, además, que un automorfismo preserva el centro (ejercicio). Describamos primero $Aut_V(\mathfrak{h}_n) = \{g\in Aut(\mathfrak{h}_n) \text{ tal que } g:V\to V\}$. Si g actúa en el centro por 1, entonces (3.1) es equivalente a

$$[v,v'] = \Psi(gv,gv').$$

Esto es, $Jv.v' = Jgv.gv'$, o sea $g^tJg = J$. Precisamente, el grupo simpléctico es $Sp(n,\mathbb{R}) = \{g\in Gl(2n,\mathbb{R}) : g^tJg = J\}$.

Además, para s positivo, es fácil ver que $\delta_s(v,t) = \left(s^{\frac{1}{2}}v, st\right)$ define un automorfismo.

Luego si g actúa por s en el centro de $\mathfrak{h}_n$, podemos escribir $g = \delta_s g'$, siendo entonces g' un automorfismo que actúa en el centro por la identidad, o sea $g' \in Sp(n,\mathbb{R})$.

También θ definido por $\theta(x,y,t) = (x,-y,-t)$ si $v = (x,y)$, define un automorfismo, y por lo tanto si g actúa por $-s$ en el centro, entonces $g = \theta\delta_s g'$, con $g' \in Sp(n,\mathbb{R})$.

Dejamos como ejercicio probar que $Aut(\mathfrak{h}_n) \simeq Aut_V(\mathfrak{h}_n) \times \mathbb{R}^{2n}$ (producto semidirecto), donde $\mathbb{R}^{2n}$ está inmerso como un subgrupo normal, abeliano de $Aut(\mathfrak{h}_n)$.

4. Elementos de la teoría de representaciones

Sea G un grupo topológico. Sea H un espacio de Hilbert y denotemos por $U(H)$ el álgebra de los operadores unitarios sobre H. Una representación unitaria de G sobre H, es un homomorfismo $\pi : G \to U(H)$, tal que la aplicación $G \times H \to H, (g,v) \to \pi(g)v$, es continua.

La denotamos por $(\pi, H.)$ Se puede probar que esta condición es equivalente a la continuidad de $\pi : G \to U(H)$, donde la topología en $U(H)$ es la fuerte.

Dadas dos representaciones unitarias (π_1, H_1), (π_2, H_2), un *operador de entrelazamiento* entre ambas, es un operador continuo $A : H_1 \to H_2$ tal que $\pi_2(g) \circ A = A \circ \pi_1(g)$.

Una representación (π, H) se dice *irreducible* si los únicos subespacios de H invariantes por la acción de π son el nulo y el total. En otras palabras, H no contiene subspacios propios, no nulos, invariantes por π.

Lema 4.1. *Lema de Schur. Sea (π, H) una representación irreducible de G, y sea A un operador de entrelazamiento de la representación. Entonces $A = \mu I$.*

Demostración. La demostración requiere del teorema espectral para operadores autoadjuntos y, por lo tanto, solo daremos una idea.

Observemos, en primer lugar que, si A es de entrelazamiento, también lo es su operador adjunto A^*pues $\pi(g)$ es unitario, y luego lo es AA^*. Por lo tanto podemos suponer que A es autoadjunto. En este caso, vale que

$$\sigma(A) = \{\lambda \in C : A - \lambda I \text{ es no invertible } \} \subset \mathbb{R}.$$

El teorema espectral para operadores autoadjuntos afirma que existe una familia de proyecciones $\{P_\lambda\}$ sobre H tal que si $\lambda \leq \mu$, Im $P_\lambda \subset \text{ImP}_\mu$, y tal que

$$\left\| A - \sum \lambda_i \left(P_{\lambda_i} - P_{\lambda_{i-1}}\right) \right\|_{B(H)} \to 0 \; si\, (\lambda_i - \lambda_{i-1}) \to 0. \tag{4.1}$$

Ponemos

$$A = \int_{\sigma(A)} \lambda dP_\lambda$$

Además el teorema espectral asegura que las proyecciones P_λ conmutan con todo operador que conmute con A. En nuestro caso esto dice que P_λ es también de entrelazamiento. Luego el núcleo y la imagen de P_λ son subespacios invariantes. Como la representación es irreducible, esto dice que $P_\lambda = 0$, ó $P_\lambda = I$. Por la monotonía de la familia $\{P_\lambda\}$ y la (4.1, tenemos que $A = \lambda_0 I$. □

Finalmente si A es arbitrario, escribimos $A = \frac{(A+A^*)}{2} + \frac{(A-A^*)}{2i}$.

Ejercicio. Sea $A : L^2([0,1]) \to L^2([0,1])$ definido por $(Af) = xf(x)$. Hallar $\sigma(A)$ y la familia $\{P_\lambda\}$ dada por el teorema espectral.

Corolario 4.2. *Corolario. Las representaciones unitarias, irreducibles de un grupo conmutativo G, son de dimensión 1 y por lo tanto están en correspondencia con los homomorfismos continuos de G en S^1.*

Demostración. En efecto, sea(π, H) una representación unitaria, irreducible. Entonces $\pi(g)$ conmuta con $\pi(h)$ para todo $h \in G$. Luego $\pi(g) = \chi(g) I$. Luego todo subespacio de H es invariante por π, y como π es irreducible, $\dim H = 1$. Como π es continuo y unitario, $\chi : G \to S^1$ es continuo. □

Ejemplo 4.3. Determinemos los caracteres del grupo $\mathbb{R}$: un tal χ satisface que

$$\chi(x+y) = \chi(x)\chi(y), \tag{4.2}$$

y que $\chi(0) = 1$. Luego, por continuidad, $\chi(x)$ es positivo para x en un intervalo $(0,\delta)$. Sea $c = \int_0^\delta \chi(x)\,dx$. Entonces $c\chi(y) = \int_0^\delta \chi(x)\chi(y)\,dx = \int_0^\delta \chi(x+y)\,dx = \int_y^{y+\delta} \chi(t)\,dt$. Esto dice que χ es una función derivable y derivando (4.2) en $y = 0$, obtenemos que $\chi'(x) = \chi(x)\chi'(0)$ Luego $\chi(x) = e^{\chi'(0)x}$ y como $|\chi(x)| = 1, \chi'(0) \in i\mathbb{R}$.

El análisis armónico en $\mathbb{R}$ está asociado, al estudio de la transformada de Fourier. Por lo anterior, los homomorfismos del grupo $\mathbb{R}$ están dados por $\chi_\lambda(x) = e^{i\lambda x}$, y son precisamente los homomorfismos del álgebra $L^1(\mathbb{R})$, (vía integración). La transformada de Fourier está definida sobre $L^1(\mathbb{R})$ por

$$\widehat{f}(\lambda) = \int f(x)\, e^{-i\lambda x} dx = \int f(x)\, \chi_\lambda(-x)\, dx.$$

El teorema de Plancherel asegura que la transformada de Fourier se extiende a una isometría de $L^2(\mathbb{R})$, es decir $\|f\|^2 = \left\|\widehat{f}\right\|^2$, para $f \in L^2(\mathbb{R})$. Además si f y $\widehat{f} \in L^1(\mathbb{R})$, vale la fórmula de inversión

$$f(x) = \int \widehat{f}(\lambda)\, e^{i\lambda x} d\lambda, ppx \in \mathbb{R}.$$

El análisis armónico en un grupo de Lie G, consiste, en principio, en determinar las representaciones unitarias, ireducibles de G. Si (π, H) es una tal representación, y $f \in L^1(G)$, se define la transformada de Fourier de f por

$$\widehat{f}(\pi) = \int f(x)\, \pi(x)\, dx,$$

donde dx denota la medida de Haar de G. Aquí, la transformada de Fourier de f toma valores en el espacio de operadores continuos sobre H, que denotamos por $B(H)$. Además, en cada caso, se pretende probar una versión análoga al teorema de Plancherel y una correspondiente formula de inversión. Esto es lo que desarrollaremos para el caso $G = H_n$.

5. Representaciones irreducibles de H_n

Denotemos por Z el centro de H_n.Entonces $Z = \{(0,0,t), t \in \mathbb{R}\}$

Observemos que si (π, H) es una representacion, unitaria e irreducible, entonces por el lema de Schur, $\pi(0,0,t) = e^{i\lambda t}$ para algún λ real. Si $\lambda = 0$, entonces π induce una representacion irreducible sobre $H_n/Z \simeq \mathbb{R}^{2n}$. Luego $\pi(x,y,t) = e^{i(\xi.x+\eta.y)}$.

Supongamos $\lambda \neq 0$, y sea (π, H) una representación unitaria tal que $\pi(0,0,t) = e^{i\lambda t}$.

Supongamos que $\dim H$ es finita. Para $v \in H$, podemos definir una representación de $\mathfrak{h}_n$, llamada *la diferencial de* π por

$$d\pi(X)v = \frac{d}{ds}_{/s=0} \pi(sX)v.$$

Como $\pi(sX)$ es un operador unitario, $d\pi(X)$ es antisimétrico. En efecto, derivando en $s = 0$ la identidad $\langle \pi(sX)v, \pi(sX)w\rangle = \langle v, w\rangle$, obtenemos $\langle d\pi(X)v, w\rangle + \langle v, d\pi(X)w\rangle = 0$.

(Ejercicio. Probar que si $B : H \times H \to \mathbb{R}$ es una aplicación bilineal , entonces $dB_{(a,b)}(u,v) = B(a,v) + B(u,b)$.)

Como H es de dimensión finita, y $d\pi(X)$ es lineal, $d\pi(X)$ es un operador continuo. Además

Proposición 5.1. *Si $X, Y \in \mathfrak{h}_n$, entonces*

$$d\pi[X,Y] = d\pi(X)d\pi(Y) - d\pi(Y)d\pi(X), \tag{5.1}$$

En particular $d\pi(X_j)d\pi(Y_j) - d\pi(Y_j)d\pi X_j) = d\pi(T) = i\lambda I$.

Demostración. Sea $A \in Gl(2n+1)$, y sea $I_A : Gl(2n+1) \to Gl(2n+1)$ definida por $I_A(B) = ABA^{-1}$.Como I_A es lineal, su derivada en cualquier punto es ella misma . Sea $\phi : H_n \to U(H)$ un homomorfismo. Entonces, si $A \in H_n, X \in \mathfrak{h}_n$

$$\phi(I_A(\exp tX) = I_{\phi(A)}(\phi(\exp tX)).$$

. Derivando en $t = 0$, obtenemos

$$d\phi_{Id}\left(AXA^{-1}\right) = \phi(A)\, d\phi(X)\, \phi(A)^{-1}.$$

Ahora poniendo $A = \exp tY$, y derivando de nuevo en $t = 0$, obtenemos

$$d\phi(YX - XY) = d\phi(Y)\, d\phi(X) - d\phi(X)\, d\phi(Y).$$

En efecto, la última igualdad resulta de observar que $t \to (\exp tY)X(\exp -tY)$ es bilineal y por lo tanto su derivada en $t = 0$ es $YX - XY$. □

Proposición 5.2. *No existen operadores acotados, antisimétricos P, Q, satisfaciendo $PQ - QP = i\lambda I$, con $\lambda \neq 0$.*

Demostración. Por inducción se ve que $PQ - QP = i\lambda I$ implica $PQ^n - Q^nP = ni\lambda Q^{n-1}$.Luego tendríamos $n|\lambda|\,\|Q^{n-1}\| \leq 2\|P\|\,\|Q^n\| \leq 2\|P\|\,\|Q\|\,\|Q^{n-1}\|$, o sea $2\|P\|\,\|Q\| \geq n|\lambda|$, para todo n, lo cual es un absurdo. □

Por lo tanto si (π, H) es una representación unitaria tal que $\pi(0,0,t) = e^{i\lambda t}I$, necesariamente $\dim H = \infty$. Por otra parte como

$(x,y,t) = (x,0,0)(0,y,0)\left(0,0,t - \frac{1}{2}x.y\right)$, uno está tentado de definir una representación $\pi(x,y,t) = e^{i\lambda\left(t-\frac{1}{2}x.y\right)}\sigma(x)\tau(y)$, donde $\sigma(x)$ y $\tau(y)$ son representaciones unitarias de $\mathbb{R}^n$ sobre cierto espacio de Hilbert H.

Lema 5.3. *Lema. Si* $\sigma(x)\tau(y) = e^{i\lambda x.y}\tau(y)\sigma(x)$, *entonces*

$$\pi(x,y,t) = e^{i\lambda\left(t-\frac{1}{2}x.y\right)}\sigma(x)\tau(y)$$

define una representación (unívocamente determinada) de H_n, *tal que* $\pi_\lambda(x,0,0) = \sigma(x)$, $\pi_\lambda(0,y,0) = \tau(y)$, $\pi_\lambda(0,0,t) = e^{i\lambda t}$.

Demostración. Queda como ejercicio. □

Nada más natural que tomar $H = L^2(\mathbb{R}^n)$. Sean

$$\sigma(x)\varphi(u) = \varphi(x+u), \text{ y}$$

$$\tau(y)\varphi(u) = e^{iy.u}\varphi(u).$$

Entonces σ y τ satisfacen las hipótesis del lema con $\lambda = 1$ y se tiene que

$$\begin{aligned}\pi_1(x,y,t)\varphi(u) &= e^{i\left(t-\frac{1}{2}x.y\right)}\sigma(x)(\tau(y)\varphi)(u) = e^{i\left(t-\frac{1}{2}x.y\right)}(\tau(y)\varphi)(x+u)\\ &= e^{i\left(t-\frac{1}{2}x.y\right)}e^{i(x+u).y}\varphi(x+u).\end{aligned}$$

Esto es,

$$\pi_1(x,y,t)\varphi(u) = e^{i\left(t+\frac{1}{2}x.y+u.y\right)}\varphi(x+u).$$

Para $\lambda \neq 0$, la aplicación $(x,y,t) \to (x,\lambda y,\lambda t)$ es un automorfismo y por lo tanto

$$\pi_\lambda(x,y,t) = \pi_1(x,\lambda y,\lambda t)$$

define una representación de H_n, llamada representación de Schrödinger.

Sea $\varphi \in S(R^n)$. Entonces

$$\begin{aligned}d\pi_\lambda(X_j)\varphi(u) &= \frac{d}{ds}_{/s=0}(\pi_\lambda(sX_j)\varphi)(u) = \frac{d}{ds}_{/s=0}\varphi(se_j+u) = \frac{\partial\varphi}{\partial u_j}(u),\\ d\pi_\lambda(Y_j)f(u) &= \frac{d}{ds}_{/s=0}(\pi_\lambda(sY_j)\varphi)(u) = \frac{d}{ds}_{/s=0}e^{i\lambda s u_j}\varphi(u) = i\lambda u_j\varphi(u),\\ d\pi_\lambda(T)\varphi(u) &= i\lambda\varphi(u).\end{aligned}$$

6. Funciones de Hermite

Para comenzar, supongamos $n = 1, \lambda = 1$. Pongamos

$$Z = \frac{1}{2}(X - iY), \quad \overline{Z} = \frac{1}{2}(X + iY).$$

Entonces $d\pi_\lambda(Z) = \frac{1}{2}\left(\frac{d}{du} + u\right)$ y $d\pi_\lambda\left(\overline{Z}\right) = \frac{1}{2}\left(\frac{d}{du} - u\right)$.

Sea $D = \frac{1}{2}\left(\frac{d}{du} + u\right)$ y sea $\overline{D} = \frac{1}{2}\left(\frac{d}{du} - u\right)$. Sea $\varphi_0(u) = e^{-\frac{u^2}{2}}$, entonces $D\varphi_0 = 0$.

Teorema 6.1. *Las funciones* $\varphi_n = \overline{D}^n\varphi_0$ *forman una base ortonormal de* $L^2(R)$, *tal que*

$$\overline{D}\varphi_n = \varphi_{n+1},\ D\varphi_n = -\frac{n}{2}\varphi_{n-1}. \tag{6.1}$$

Además $D\overline{D}\varphi_n = -\frac{n+1}{2}\varphi_n$ *y* $\overline{D}D\varphi_n = -\frac{n}{2}\varphi_n$.

Demostración. La primera de (6.1) sigue de la definición de φ_n. Para la segunda observamos que $\left[D,\overline{D}\right]=-\frac{1}{2}I$. Entonces usando inducción tenemos

$$D\varphi_n=D\overline{D}\varphi_{n-1}=\overline{D}D\varphi_{n-1}+\left[D,\overline{D}\right]\varphi_{n-1}=-\frac{n-1}{2}\overline{D}\varphi_{n-2}-\frac{1}{2}\varphi_{n-1}=-\frac{n}{2}\varphi_{n-1}$$

Es evidente por el decaimiento exponencial de φ_0, y por la definición de $\overline{D}$, que $\varphi_n\in L^2$.

Probemos la ortogonalidad: tenemos $\langle\varphi_0,\varphi_n\rangle=\left\langle\varphi_0,\overline{D}\varphi_{n-1}\right\rangle=-\langle D\varphi_0,\varphi_{n-1}\rangle=0$, $\forall n\neq 0$. Entonces, por inducción,

$$\langle\varphi_m,\varphi_n\rangle=\left\langle\varphi_m,\overline{D}\varphi_{n-1}\right\rangle=-\langle D\varphi_m,\varphi_{n-1}\rangle=\frac{m}{2}\langle\varphi_{m-1},\varphi_{n-1}\rangle=0$$

si $m\neq n$.

Probemos la completitud: Si $f\in L^2$, tenemos que

$$\widehat{\left(fe^{-x^2}\right)}(\xi)=\int f(x)\,e^{-x^2}e^{-i\xi x}dx=\sum_{n=0}^{\infty}\frac{(-i\xi x)^n}{n!}\int f(x)\,e^{-x^2}x^n dx.$$

Luego si $\int f(x)\,e^{-x^2}x^n dx=0$ para todo n, entonces $\widehat{\left(fe^{-x^2}\right)}=0$ y por lo tanto $f=0$. Como $\varphi_n(u)=p_n(u)\,e^{-u^2}$, donde p_n es un polinomio de grado n, queda probada la completitud de la $\{\varphi_n\}$. □

Las matrices de $d\pi(Z)$ y $d\pi\left(\overline{Z}\right)$ están dadas por

$$d\pi(Z)=\begin{pmatrix}0&-\sqrt{\frac{1}{2}}&&&&&\\&0&-1&&&&\\&&0&&&&\\&&&0&-\sqrt{\frac{n}{2}}&&\\&&&&0&\ldots&\\&&&&&\ldots&\end{pmatrix}$$

y

$$d\pi\left(\overline{Z}\right)=\begin{pmatrix}0&&&&&\\\sqrt{\frac{1}{2}}&0&&&&\\&1&0&&&\\&&\ldots&0&&\\&&&\sqrt{\frac{n}{2}}&0&\ldots\\&&&&\ldots.&\ldots\end{pmatrix}$$

Ejercicio. Probar que $\widehat{\varphi_n}=(-i)^n\varphi_n$, siguiendo las siguientes observaciones

i) $\widehat{\varphi_0}=\varphi_0$.

ii) Como $\widehat{\frac{d}{du}\phi}(\xi)=i\xi\widehat{\phi}(\xi)$, y $\widehat{(u\phi)}(\xi)=i\left(\frac{d}{d\xi}\widehat{\phi}\right)(\xi)$, tenemos que

$=\widehat{\overline{D}\varphi_0}(\xi)=\widehat{\frac{d}{du}\varphi_0}(\xi)-\widehat{(u\varphi_0)}(\xi)=i\xi\widehat{\varphi_0}(\xi)-i\left(\frac{d}{d\xi}\widehat{\varphi_0}\right)(\xi)=(-i)\,\overline{D}\varphi_0=(-i)\,\varphi_1.$

Si $\lambda\neq 1$, no es difícil ver que podemos imitar el proceso anterior considerando como base de $L^2(R^n)$ las funciones de Hermite convenientemente dilatadas.

Si $n\neq 1$, $d\pi_\lambda(Z_j)=\frac{1}{2}\left(\frac{\partial}{\partial u_j}+\lambda u_j\right)$ y $d\pi_\lambda\left(\overline{Z}_j\right)=\frac{1}{2}\left(\frac{\partial}{\partial u_j}-\lambda u_j\right)$ y la correspondiente base viene dada por las funciones de Hermite $\varphi_\alpha^\lambda(u)=\varphi_{\alpha_1}^\lambda(u_1)\ldots\varphi_{\alpha_n}^\lambda(u_n)$ si $\alpha=(\alpha_1,\ldots\alpha_n)$, donde $\varphi_{\alpha_j}^\lambda(u_j)=|\lambda|^{\frac{1}{4}}\varphi_{\alpha_j}\left(|\lambda|^{\frac{1}{2}}u_j\right)$

7. La transformada de Fourier en $L^1(H_n)$.

Para $f \in L^1(H_n)$, definimos la transformada de Fourier de f por

$$\pi_\lambda(f) = \int_{H_n} f(x,y,t)\,\pi_\lambda(x,y,t)\,dx\,dy\,dt,$$

esto es, para $\varphi, \psi \in L^2(\mathbb{R}^n)$, $\langle \pi_\lambda(f)\varphi, \psi\rangle = \int_{H_n} f(x,y,t)\,\langle \pi_\lambda(x,y,t)\varphi, \psi\rangle\,dx\,dy\,dt$.
Se tiene que $\pi_\lambda(f)$ es un operador acotado en $L^2(\mathbb{R}^n)$ y $\|\pi_\lambda(f)\|_{op} \leq \|f\|_{L1(\mathbb{R}^n)}$.
Veamos que $\pi_\lambda(f)$ es un operador integral del tipo

$$[\pi_\lambda(f)\varphi](u) = \int K_f(u,v)\,\varphi(v)\,dv,$$

con $K_f \in L^2(\mathbb{R}^n \times \mathbb{R}^n)$.
En efecto,

$$\begin{aligned}
[\pi_\lambda(f)\varphi](u) &= \int_{H_n} f(x,y,t)\,e^{i\lambda\left(t+\frac{1}{2}x.y+u.y\right)}\varphi(x+u)\,dx\,dy\,dt \\
&= \int_{\mathbb{R}^n\times\mathbb{R}^n} f\left(x,y,\widehat{-\lambda}\right)e^{i\lambda\left(\left(\frac{1}{2}x.+u\right).y\right)}\varphi(x+u)\,dx\,dy \\
&= \int_{\mathbb{R}^n} f\left(x,-\lambda\widehat{\left(\frac{1}{2}x.+u\right)},\widehat{-\lambda}\right)\varphi(x+u)\,dx \\
&= \int_{\mathbb{R}^n} f\left(u-v,\frac{-\lambda}{2}\widehat{(v+u)},\widehat{-\lambda}\right)\varphi(v)\,dv,
\end{aligned}$$

donde hicimos el cambio de variable $v = x + u$.

Por lo tanto,

$$K_{f,\lambda}(u,v) = f\left(u-v,\frac{-\lambda}{2}\widehat{(v+u)},\widehat{-\lambda}\right).$$

Queda como ejercicio probar que si $K \in L^2(\mathbb{R}^n \times \mathbb{R}^n)$, el operador

$$T\varphi(u) = \int_{\mathbb{R}^n} K(u,v)\,\varphi(v)\,dv$$

es acotado en $L^2(\mathbb{R}^n)$ y que $\|T\|_{op} \leq \|K\|_{L^2(\mathbb{R}^n\times\mathbb{R}^n)}$. (Usar la desigualdad de Schwartz en $L^2(\mathbb{R}^n)$.)

Finalmente, comentamos que un operador T así definido, es un operador de Hilbert Schmidt, es decir, dada cualquier base ortonormal $\{\varphi_j\}$de $L^2(\mathbb{R}^n)$, $\sum \|T\varphi_j\|^2$ es finita.
En efecto,

$$\langle T\varphi_i, \varphi_j\rangle = \int_{\mathbb{R}^n\times\mathbb{R}^n} K(u,v)\,\varphi_i(v)\,\overline{\varphi_j(u)}dv = \langle K, \varphi_j \otimes \overline{\varphi_i}\rangle$$

siendo $\varphi_j \otimes \overline{\varphi_i}$ una base ortonormal de $L^2(\mathbb{R}^n \times \mathbb{R}^n)$.

Luego, si $f \in L^1(\mathbb{H}_n) \cap L^1(\mathbb{H}_n)$, por la fórmula de Plancherel para funciones en $L^2(\mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R})$, obtenemos que

$$\begin{aligned}\|f\|^2 &= \left\|\widehat{f}\right\|^2 = \int_{\mathbb{R}^n\times\mathbb{R}^n\times\mathbb{R}} \left|\widehat{f}\,(\xi,\eta,\lambda)\right|^2 d\xi\, d\eta\, d\lambda \\ &= \frac{1}{2^n}\int_{\mathbb{R}^n\times\mathbb{R}^n\times\mathbb{R}} \left|\widehat{f}\left(u-v, \frac{-\lambda}{2}(v+u), -\lambda\right)\right|^2 |\lambda|^n\, du\, dv\, d\lambda \\ &= \frac{1}{2^n}\int_{\mathbb{R}} \|K_f\|^2 |\lambda|^n\, d\lambda.\end{aligned}$$

Así, hemos obtenido la fórmula de Plancherel para funciones en $L^1(\mathbb{H}_n) \cap L^1(\mathbb{H}_n)$

$$\|f\|^2 = \frac{1}{2^n}\int_{\mathbb{R}} \|\pi_\lambda(f)\|_{HS}^2 |\lambda|^n\, d\lambda.$$

Referencias

[1] F. Ricci, *Notas sobre Análisis armónico abstracto.*
[2] S. Thangavelu. *Harmonic analysis on the Heisenberg group*, Progress in Math., vol. **159**.

CIEM – CONICET, Facultad de Matemática, Astronomía y Física, (Universidad Nacional de Córdoba), Ciudad Universitaria, 5000 Córdoba, Argentina
E-mail address: saal@famaf.unc.edu.ar

Cursos Intermedios

TEORÍA DE CÓDIGOS Y CURVAS ALGEBRAICAS

ANTONIO BEHN

RESUMEN. Haremos una introducción a la teoría de códigos lineales para la detección y correción de errores. Mencionaremos algunas aplicaciones y mostraremos ejemplos clásicos, como códigos de Hamming, Reed-Solomon, BCH. Estudiaremos los códigos de Goppa clásicos y luego de introducir las curvas algebraicas sobre cuerpos finitos, veremos códigos de Goppa geométricos. También mostraremos cotas y cotas asintóticas para los parámetros de los códigos.

ÍNDICE

Prerrequisitos

El curso está dirigido a alumnos de magister, doctorado o que estén finalizando una licenciatura. Se requiere conocimiento de álgebra lineal, cuerpos finitos y anillos de polinomios. No supondremos conocimientos específicos de la teoría de códigos.

1. ¿Qué es un código?

Hay varias razones por las cuáles se podría querer codificar un mensaje.

- **Compresión de datos:** Para hacer más eficiente su transmisión o almacenamiento.
- **Criptografía:** Para ocultar su contenido a terceras personas.
- **Detección y corrección de errores:** Para aumentar la confiabilidad de su transmisión o almacenamiento.

Es solamente este último tipo de códigos el que estudiaremos en este curso.

Queremos transmitir un mensaje y sabemos que el medio por el cual se transmitirá no es completamente confiable de manera que necesitamos agregar cierta redundancia al mensaje de manera de poder detectar y ojalá corregir eventuales errores en la transmisión. Notemos que esta transmisión puede ser espacial (fotos de una sonda espacial, conversaciones de telefonía celular, transmisión de archivos por internet, etc) o temporal (Almacenamiento de datos en un disco duro, CD de música, código de barras de un producto, etc).

Quizás la forma más sencilla de agregar redundancia a un mensaje sea repetirlo dos o más veces de manera que el receptor pueda comparar las versiones recibidas. Como veremos, ésta no es en general una forma eficiente pues el esfuerzo requerido es demasiado grande. Otra forma básica de código, es agregar lo que se conoce como código verificador. Por ejemplo el número de RUT utilizado en Chile tiene un código verificador después del guión que permite detectar un buen número de errores que se podrían producir al dictar o tipear el número. Lo mismo sucede con el CUIT (clave única de identificación tributaria) en Argentina Otro ejemplo del mismo tipo es el de los códigos utilizados para clasificar los libros (ISBN). Estos dígitos verificadores permiten detectar pero no corregir errores pues si el dígito verificador no corresponde, no hay manera de saber donde se produjo el error.

En general buscamos una regla que a cada mensaje (sucesión de letras o símbolos en el abecedario fuente) le asigna un código (sucesión de letras en el alfabeto codificado) de

manera única. Consideraremos el caso especial donde los códigos son todos del mismo largo (llamados códigos de bloque) y el alfabeto codificado es un cuerpo finito. En el caso donde este cuerpo tiene dos elementos, es decir las palabras del código consisten en sucesiones de ceros y unos diremos que se trata de un código binario.

1.1. Ejemplos.

Ejemplo 1.1 (ISBN (international standard book number))**.** Los libros tienen un código que los identifica que consiste de diez dígitos (recientemente ha sido alargado a 13) que satisfacen

$$\sum_{i=1}^{10} ia_i \equiv 0 \quad \text{mód } 11$$

donde el último dígito es una X si le correspondería ser 10.

Ejercicio 1.1. Verifique el ISBN 0-201-39825-7. Los guiones sirven para facilitar la lectura pero no participan en la codificación.

Ejercicio 1.2. Este código permite detectar cualquier error en un dígito y cualquier error de transposición de dos dígitos.

Ejemplo 1.2 (Códigos de repetición)**.** Supongamos ahora que queremos enviar un mensaje simple (sí/no) donde 1 significa "sí" y 0 significa "no". Si lo que hacemos es enviar un sólo bit, cualquier error en el canal de transmisión pasaría inadvertido y el mensaje recibido sería erróneo. Una estrategia simple de codificación es enviar 11111 cuando queremos decir "sí" y 00000 cuando queremos decir "no". El receptor determina cuál es el dígito que más se repite en el mensaje que ha recibido y decide que ese debe haber sido el mensaje enviado. Hemos tenido que enviar un mensaje 5 veces más largo, pero la probabilidad de que el mensaje recibido sea erróneo es mucho menor.

2. Conceptos básicos

Para poder comparar distintos códigos introduciremos algunos parámetros importantes. En primer lugar está el largo del código que se define como el número de dígitos en cada palabra del código (recordemos que consideraremos códigos cuyas palabras sean todas del mismo largo). En el caso del código de repetición del ejemplo 1.2 el largo es 5.

En segundo lugar, nos interesa conocer el número total de palabras que contiene el código. En el ejemplo 1.2 tenemos 2 palabras (00000 y 11111).

En tercer lugar queremos caracterizar la distancia entre las palabras del código para lo que definiremos:

Definición 2.1 (Peso de Hamming y distancia de Hamming)**.** *La distancia de Hamming entre dos palabras $d(a, b)$ de un código es el número de dígitos en que las palabras difieren. El peso de Hamming de una palabra $w(a)$ es el número de coordenadas distintas de 0 de la palabra (pensada ésta como vector fila). Podemos observar que $d(a, b) = w(a - b)$.*

La distancia mínima del código, definida como el mínimo de todas las distancias entre palabras distintas del código, es el tercer parámetro que buscamos. En el caso del ejemplo 1.2, esta distancia mínima es 5. Ya veremos como la distancia mínima determina cuántos errores nos permitirá detectar/corregir el código.

Ejercicio 2.1. La distancia de Hamming define una métrica en el espacio de las n-tuplas sobre el cuerpo $\mathbb{F}_q$, es decir:

$$\begin{aligned} d(x,x) &= 0 \\ d(x,y) &= d(y,x) \\ d(x,y) &\leq d(x,z)+d(z,y) \end{aligned}$$

¿Se puede interpretar el peso de Hamming como una norma cuya métrica asociada es la distancia de Hamming?

Ejercicio 2.2. ¿Cuál es la distancia mínima del código ISBN?

Teorema 2.2. *Un código con distancia mínima d nos permite detectar s errores si $d \geq s+1$ y nos permite corregir t errores si $d \geq 2t+1$. Debemos notar que no podemos lograr ambas cosas simultáneamente.*

Demostración. 1. Supongamos que $d \geq s+1$ y que el número de errores en la transmisión de una palabra c es menor o igual a s. Entonces es imposible que la palabra recibida esté en el código y sea diferente de la enviada pues la distancia mínima entre palabras del código es d. Por lo tanto, los errores son detectados.

2. Supongamos ahora que $d \geq 2t+1$ y que el número de errores en la transmisión de una palabra c es menor o igual a t recibiéndose una palabra c'. Entonces la única palabra del código a distancia menor o igual a t de c' es la palabra enviada c pues si $d(c',c'') \leq t$ entonces $d(c,c'') \leq d(c,c')+d(c',c'') \leq 2t$ lo que contradeciría que la distancia mínima entre dos palabras del código es mayor o igual a $2t+1$. □

Vemos entonces que los mejores códigos tendrán una distancia mínima lo más grande posible. Además es natural querer que el largo del código sea lo menor posible y que el número de palabras sea lo más grande posible. Lamentablemente esta condiciones se contraponen y como veremos a continuación, d, M y n no son independientes.

Definición 2.3. *Hablaremos de un (n,M,d)-código para referirnos a un código de dimensión n con M palabras y distancia mínima d.*

Ejercicio 2.3. El código $C = \{0000, 1100, 0011, 1111\}$ es un $(4,4,2)$-código.

3. Códigos lineales

Diremos que un código C es un código lineal, si el conjunto de las palabras del código forma un subespacio vectorial de $\mathbb{F}_q^n$. Hablaremos de un $[n,k]$ código si tenemos un código de largo n y dimensión k. Si además conocemos su distancia mínima, hablaremos de un $[n,k,d]$ código. De ahora en adelante todos los códigos de los que hablaremos serán lineales. Notemos que los vectores son vectores fila.

Teorema 3.1. *La distancia mínima de un código lineal C es igual al mínimo peso de los vectores no nulos de C. Notemos que esto nos permite simplificar significativamente el cálculo de la distancia mínima.*

Demostración. Ejercicio. □

3.1. Matriz generadora y matriz de control. Dada una base $\{v_1, v_2, \ldots, v_k\}$ de un código C podemos definir una matriz generadora G para el código cuyas filas serán los vectores $v_1, v_2, \ldots, v_k$. G no está únicamente determinada por C sino que depende de la elección de una base. Recíprocamente, dada una matriz de $k \times n$ cuyas filas son linealmente independientes, existe un $[n, k]$ código para el que esta matriz es una matriz generadora.

Dada una matriz generadora G, podemos definir una forma de codificar mensajes. Los mensajes son vectores arbitrarios en $\mathbb{F}_q^k$ y la matriz generadora define una inyección $\mathbb{F}_q^k \to \mathbb{F}_q^n$ que lleva un mensaje u en la palabra del código uG. La imagen de esta función es precisamente C.

Nota: Si $G = (I\ B)$ donde I es la matriz identidad de $k \times k$, diremos que G es una matriz generadora sistemática (o estándar). La ventaja de usar una matriz generadora sistemática, es que permite identificar fácilmente el mensaje original si conocemos la palabra codificada.

Observación 3.2. *Si A y B son matrices equivalentes por filas (¿qué quiere decir esto?), entonces ambas definen el mismo código. ¿Por qué?*

Ejercicio 3.1. Describa un algoritmo para obtener una matriz generadora para un código si se conoce un conjunto generador para éste. ¿Cuándo se puede obtener una matriz generadora sistemática?

Definición 3.3. *El producto interno $u \cdot v$ de vectores $u = (u_1, u_2, \ldots u_n)$ y $v = (v_1, v_2, \ldots v_n)$ en $\mathbb{F}_q^n$ se define como $u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n$.*

Definición 3.4. *Diremos que dos vectores u y v son ortogonales si $u \cdot v = 0$.*

Notemos que, a diferencia de lo que pasa en espacios vectoriales reales, es posible que $u \cdot u = 0$ sin que u sea el vector 0.

Definición 3.5. *Dado un subespacio $V \subseteq \mathbb{F}_q^n$, el complemento ortogonal de V es el conjunto de los vectores ortogonales a todos los elementos de V y se denota por $V^\perp$.*

$$V^\perp = \{u \in \mathbb{F}_q^n | u \cdot v = 0 \forall v \in V\}$$

Debemos notar que el complemento ortogonal no es un complemento de V como subespacio de $\mathbb{F}_q^n$ en el sentido usual pues ni siquiera se tiene $V \cap V^\perp = \{0\}$.

Definición 3.6. *Dado un código C podemos definir su código dual $C^\perp$ como el complemento ortogonal de C.*

OBS: En el caso especial que $C = C^\perp$ diremos que C es un código auto-dual. Además, si $C \subseteq C^\perp$ diremos que C es auto-ortogonal.

Dado un $[n,k]$ código C, el dual $C^\perp$ es un $[n,n-k]$ código (demuéstrelo) que tiene una matriz generadora H con la propiedad que $v \in C$ si y sólo si $vH^T = 0$ o equivalentemente $Hv^T = 0$ de manera que C corresponde al espacio nulo de la matriz H. Podemos entonces usar la matriz H para verificar si una palabra recibida está en el código C y es por esto que a la matriz H la llamaremos matriz de control del código C.

Ejercicio 3.2. Describa un algoritmo para obtener una matriz generadora para $C^\perp$. Esto es lo mismo que encontrar un algoritmo para obtener una matriz de control para el código C.

Teorema 3.7. *Sea C un código lineal de largo n sobre $\mathbb{F}_q$. Entonces,*

I) $|C| = q^{\dim(C)}$.
II) $C^\perp$ *es un código lineal y* $\dim(C) + \dim(C^\perp) = n$.
III) $(C^\perp)^\perp = C$.

Demostración. ejercicio □

Corolario 3.8. *La dimensión de un código auto-ortogonal de largo n debe ser $\leq n/2$ y la dimensión de un código auto-dual debe ser $n/2$.*

Lema 3.9. *Sea C un $[n,k]$-código lineal sobre $\mathbb{F}_q$ con matriz generadora G. Entonces v es ortogonal a C si y sólo si es ortogonal a todas las filas de G, es decir $v \in C^\perp \Leftrightarrow vG^T = \mathbf{0}$.*
En particular, si H es una matriz de $(n-k) \times n$, entonces es matriz de control para C si y sólo si sus filas son linealmente independientes y $HG^T = \mathbf{0}$.

Lema 3.10. *Un resultado equivalente al lema anterior es el siguiente:*
Sea C un $[n,k]$-código lineal sobre $\mathbb{F}_q$ con matriz de control H. Entonces v pertenece a C si y sólo si es ortogonal a todas las filas de H, es decir $v \in C \Leftrightarrow vH^T = \mathbf{0}$.
En particular, si G es una matriz de $k \times n$, entonces es matriz generadora para C si y sólo si sus filas son linealmente independientes y $GH^T = \mathbf{0}$.

Teorema 3.11. *Sea C un código lineal y sea H una matriz de control para C. Entonces*

I) *C tiene distancia mínima $\geq d$ si y sólo si cualquiera $d-1$ columnas de H son linealmente independientes*
II) *C tiene distancia mínima $\leq d$ si y sólo si H tiene d columnas linealmente dependientes.*

Ejercicio 3.3. Considere el código cuya matriz de control es

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

Encuentre una matriz generadora para el código y determine sus parámetros.

3.2. Decodificación y síndromes. Con la matriz generadora ya sabemos como codificar un mensaje, ahora nos interesa conocer métodos para decodificar, es decir recuperar el mensaje original a partir de la palabra recibida. Con la matriz de control podemos determinar si esta palabra está en el código. Si no lo está, debemos elegir la palabra del código más cercana (distancia de Hamming) pues siempre supondremos que el número de erores es mínimo. La principal dificultad radica en diseñar algoritmos para determinar esta palabra más cercana.

Consideremos el conjunto de las clases laterales de C en $\mathbb{F}_q^n$. La clase que corresponde a un vector $v \in \mathbb{F}_q^n$ es el conjunto $\{v + x | x \in C\}$. Recordemos un resultado de álgebra lineal:

Teorema 3.12. *Si C es un $[n, k]$-código sobre $\mathbb{F}_q$ entonces cada vector de $\mathbb{F}_q^n$ pertenece a una clase lateral de C. Cada clase contiene exactamente q^k vectores. Hay q^{n-k} clases disjuntas.*

En cada clase elegiremos un "líder" de peso minimal. (si hay más de un vector con el mismo peso minimal, elegiremos cualquiera de ellos). Para decodificar una palabra recibida, debemos determinar en cual de las clases laterales se encuentra, para luego restarle el líder de su clase, obteniéndose así una palabra del código a distancia mínima de la palabra recibida. Para implementar este algoritmo es necesario almacenar q^n palabras ordenadas según la clase a la que corresponden, distinguiendo al líder en cada clase. Veamos un ejemplo:

Ejemplo 3.1. Sea C es $[4, 2]$ código binario de matriz generadora

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

Entonces $C = \{(0000, 1011, 0101, 1110\}$ y las clases laterales de C son

$$\begin{aligned} 0000 + C &= \{(0000, 1011, 0101, 1110\} \\ 1000 + C &= \{(1000, 0011, 1101, 0110\} \\ 0100 + C &= \{(0100, 1111, 0001, 1010\} \\ 0010 + C &= \{(0010, 1001, 0111, 1100\} \end{aligned}$$

Podemos observar que este código tiene distancia mínima 2 y que, usando el algoritmo descrito, permite corregir un error si este es cometido en una de las primeras 3 posiciones (no en la cuarta).

El método descrito para decodificar es un método completamente general pero sólo es realizable para códigos de tamaños relativamente pequeños pues de lo contrario la tabla que se debe almacenar es demasiado grande y la tarea de encontrar la palabra recibida en la tabla se hace difícil.

Otro método general para decodificar códigos lineales es el que usa lo que se conoce como síndrome. La idea es aprovechar la matriz de control H que para cada clase lateral del código produce un único vector en $\mathbb{F}_q^n/\mathbb{F}_q^k = \mathbb{F}_q^{n-k}$. Más concretamente, si $v \in \mathbb{F}_q^n$,

entonces $vH^T \in \mathbb{F}_q^{n-k}$ sólo depende de la clase a la que pertenece v y le llamaremos el síndrome de v. Ahora el algoritmo de decodificación funciona como sigue. Hacemos una tabla que contiene los síndromes de cada clase y el líder correspondiente ($2q^{n-k}$ vectores en lugar de q^n). Dada una palabra recibida, calculamos su síndrome y lo encontramos en la lista. La palabra corregida será entonces $v - e$ donde e es el líder correspondiente (e es el error que se corregirá).

Ejercicio 3.4. Hacer una tabla de síndromes y líderes para el código binario cuya matriz generadora es

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

¿Cuáles son los parámetros de este código?

3.3. Equivalencia de códigos lineales.

Definición 3.13. *Dos (n, M)-códigos sobre $\mathbb{F}_q$ son equivalentes si se puede obtener uno a partir del otro con una combinación de operaciones de los siguientes tipos:*

I) *una permutación de las n coordenadas de las palabras (la misma permutación para todas las palabras).*

II) *multiplicación de los símbolos que aparecen en un posición fija por un escalar no nulo.*

Teorema 3.14. *Todo código lineal es equivalente a uno cuyo matriz generadora se puede elegir sistemática.*

Demostración. Ejercicio. □

4. Cotas básicas para los parámetros de un código

Como uno de los objetivos principales de los códigos es transmitir la mayor cantidad de información posible, minimizando los costos de transmisión (largo del código) y maximizando la posibilidad de corregir errores (distancia mínima), resulta importante conocer las limitaciones que tenemos en cuanto a la relación entre estos parámetros. Las siguientes son algunas de las cotas que se pueden establecer. (En la sección 6 veremos otras cotas.)

Lema 4.1. *Cota de Singleton Podemos establecer la siguiente cota para el número de palabras M de un código de largo n y distancia mínima d:*

$$M \leq q^{n-d+1}$$

Demostración. Consideremos las palabras obtenidas al borrar las primeras $d-1$ coordenadas de cada palabra del código. Como la distancia entre dos palabras del código es al menos d, las palabras obtenidas son todas distintas y es claro que no hay más que q^{n-d+1} de ellas pues tienen largo $n - d + 1$. □

Definición 4.2. *Diremos que un código es MDS (maximum distance separable) si alcanza la cota de Singleton.*

Podemos obtener otra cota para la relación entre los parámetros de un código si conocemos su longitud y su distancia mínima en el caso que esta última sea impar. Para ello usaremos un argumento geométrico. Supongamos que tenemos un $(n, M, 2r+1)$-código sobre $\mathbb{F}_q$. Consideremos las esferas de radio r centradas en las palabras del código (¿qué es una esfera?). Es fácil ver que estas M esferas no se intersectan (¿por qué?) y podemos contar el número de palabras que contiene cada una como sigue:

$$\sum_{i=0}^{r} \binom{n}{i}(q-1)^i = 1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

donde el i-ésimo término de la suma corresponde al número de palabras a distancia i del centro de la esfera. De esta manera, como el número total de palabras posibles es q^n, tenemos lo que se conoce como cota de Hamming:

Lema 4.3 (Cota de Hamming)**.** *Si C es un $(n, M, d)_q$-código, entonces*

$$M \sum_{i=0}^{r} \binom{n}{i}(q-1)^i \leq q^n.$$

Diremos que un código es un *código perfecto* si esta última desigualdad es una igualdad, es decir que el conjunto de las M esferas cubre completamente el espacio $\mathbb{F}_q^n$.

5. Algunas clases de códigos especiales

5.1. Códigos de Hamming. Estudiaremos ahora una clase especial de códigos perfectos llamados códigos de Hamming binarios.

Empezaremos con una relación entre la distancia mínima de un código y su matriz de control. Recordemos que un código lineal C tiene distancia mínima d si y sólo si existe una palabra $v \in C$ con exactamente d coordenadas no nulas y ninguna palabra (no nula) de C tiene menos coordenadas no nulas. Como $Hv^T = 0$ esto quiere decir que H tiene d columnas que son linealmente dependientes. Por otro lado si H tuviese un conjunto menor de columnas l.d. entonces la relación de dependencia lineal nos daría una palabra de peso menor a d en el código.

En resumen, la distancia mínima d es el menor número para el que existen d columnas de H que son linealmente dependientes.

En particular, si buscamos códigos con distancia mínima 3 (el mínimo necesario para corregir un error), la matriz de control correspondiente tendrá columnas que satisfacen que cualquiera dos de ellas son l.i. y que hay 3 de ellas que son l.d. Si nos restringimos a códigos binarios, esto quiere decir que las columnas de H son todas distintas y que existen 3 cuya suma es 0.

Definición 5.1 (Código de Hamming)**.** *Un código de Hamming H_r de largo $n = 2^r - 1$, se define por su matriz de control cuyas columnas consisten en todos los vectores*

binarios no nulos de largo r. Esto nos da un $[n, k, d]$-código lineal sobre $\mathbb{F}_2$ con $n = 2^r - 1$, $k = 2^r - r - 1$ y $d = 3$.

Observemos que el código de Hamming H_r definido de esta manera es perfecto pues

$$q^k \sum_{i=0}^{1} \binom{n}{i} (q-1)^i = 2^{2^r - r - 1}(1 + (2^r - 1)) = 2^{2^r - 1} = 2^n$$

Ejemplo 5.1. Una matriz de control para el $[7, 4, 3]$-código H_3 es:

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

donde podemos reconocer las columnas de H como las expresiones binarias de los números de 1 a 7.

Una matriz generadora para este código es

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

La decodificación para este código es particularmente fácil. Observemos que los líderes de las clases son todos los vectores de peso menor o igual a 1 (el vector 0 corresponde a la clase del código) y el síndrome correspondiente se puede interpretar como un número binario que nos indica la columna en la que ocurrió el error de transmisión sin necesidad de almacenar una tabla especial.

A modo de ejemplo, consideremos el mensaje 0110. Después de codificar tenemos 0110011. Si la palabra recibida es 0100011, la multiplicamos por H^T obteniendo (011) que corresponde al número 3. Corregimos la tercera posición recuperando 0110011 y decodificamos 0110 pues la matriz generadora es sistemática.

5.2. Códigos de Reed-Solomon. Una clase de códigos que alcanzan la cota de Singleton es la que describiremos a continuación. Consideremos el cuerpo $\mathbb{F}_q$ y numeremos sus elementos no nulos de manera que $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$. Definimos además el conjunto de los polinomios de grado menor o igual a r con coeficientes en $\mathbb{F}_q$:

$$L_r = \{f \in \mathbb{F}_q[x] | \deg(f) \leq r\}$$

Entonces para cada $k \in \mathbb{Z}$ con $1 \leq k \leq q-1$, se define el código de Reed-Solomon:

$$RS(k, q) := \{(f(\alpha_1), \ldots, f(a_{q-1})) | f \in L_{k-1}\}.$$

Notemos que $RS(k, q) \subseteq \mathbb{F}_q^{q-1}$ de manera que es un código sobre $\mathbb{F}_q$. Además, la función $\epsilon : L_{k-1} \in \mathbb{F}_q^{q-1}$ dada por $\epsilon(f) = (f(\alpha_1), \ldots, f(a_{q-1}))$ es una transformación lineal cuya imagen es $RS(k, q)$ de manera que se trata de un código lineal.

¿Cuáles son sus parámetros? Su largo es claramente $n = q - 1$ y su dimensión es a lo sumo $\dim L_{k-1} = k$. Veamos ahora que el núcleo de ϵ es trivial. Si $\epsilon(f) = 0$,

entonces f tiene al menos $q-1$ raíces, pero f tiene grado menor a $k \leq q-1$ de manera que $f = 0$. Esto demuestra que la dimensión de C es exactamente k. Para calcular la distancia mínima, supongamos que $f \neq 0$ y que $\epsilon(f)$ tiene peso $d = d_{\min}$. Entonces f tiene al menos $n-d$ ceros de manera que su grado debe ser también al menos $n-d$. Como $f \in L_{k-1}$ esto implica que $n-d \leq k-1$, o equivalentemente, que $d \geq n-k+1$. Pero ya sabemos por la cota de Singleton (lema 4.1) que $d \leq n-k+1$ de manera que $d = n-k+1$ y C es un código MDS.

5.3. Códigos cíclicos. Una clase especial de códigos usados con frecuencia es la de los códigos cíclicos que definimos a continuación:

Definición 5.2. *Un subconjunto $S \subseteq \mathbb{F}_q^n$ es cíclico si $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in S$ cada vez que $(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in S$. Un código lineal C se dice código cíclico si C es un conjunto cíclico.*

Ejercicio 5.1. Verificar que el dual de un código cíclico es también un código cíclico.

Ejemplo 5.2. Los siguientes son ejemplos de códigos cíclicos:

1. tres códigos triviales $\{\mathbf{0}\}$, $\{\lambda \cdot \mathbf{1} | \lambda \in \mathbb{F}_q\}$ y $\mathbb{F}_q^n$;
2. el [3,2,2]-código binario $\{000, 110, 101, 011\}$;
3. el código símplice

$$\begin{aligned} S(3,2) &= \{0000000, 1011100, 0101110, 0010111, \\ &\quad 1110010, 0111001, 1001011, 1100101\} \end{aligned}$$

Para facilitar el trabajo con códigos cíclicos, consideremos la siguiente correspondencia:

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1), \quad (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

Como π es un isomorfismo de espacios vectoriales sobre $\mathbb{F}_q$, de ahora en adelante identificaremos $\mathbb{F}_q^n$ con $\mathbb{F}_q[x]/(x^n-1)$ sin necesariamente mencionar π de forma explícita.

Ejemplo 5.3. Si $C = \{000, 110, 101, 011\}$, entonces $\pi(C) = \{0, 1+x, 1+x^2, x+x^2\} \subseteq \mathbb{F}_2[x]/(x^3-1)$. Notemos que $\pi(C)$ es un ideal en $F_2[x]/(x^3-1)$ y que de hecho es el ideal generado por $x+1$.

Teorema 5.3. *El anillo $F_q[x]/(x^n-1)$ es un anillo de ideales principales.*

Demostración. Ejercicio. □

Teorema 5.4. *Un subconjunto C de $\mathbb{F}_q^n$ es un código cíclico si y sólo si $\pi(C)$ es un ideal de $\mathbb{F}_q[x]/(x^n-1)$.*

Teorema 5.5. *Sea I un idea en $\mathbb{F}_q[x]/(x^n-1)$ y sea $g(x)$ un polinomio mónico de grado minimal en I. Entonces $g(x)$ es un generador de I y divide a x^n-1 en $\mathbb{F}_q[x]$.*

5.4. Códigos BCH.

Definición 5.6. *Sea α un elemento primitivo de $\mathbb{F}_{q^m}$ y denotemos por $M^{(i)}(x)$ al polinomio minimal de α^i respecto a $\mathbb{F}_q$. Un código BCH (primitivo) sobre $\mathbb{F}_q$ de largo $n = q^m - 1$ con distancia de diseño δ es un código cíclico generado por $g(x) = mcm(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x))$ para algún entero a. Frecuentemente nos restringiremos al caso $a = 1$.*

Ejercicio 5.2. Sea α un elemento primitivo de $\mathbb{F}_{2^m}$ y sea $g(x) \in \mathbb{F}_2[x]$ el polinomio minimal de α. Demuestre que el código cíclico de largo 2^m-1 cuyo polinomio generador es $g(x)$ es de hecho el $[2^m - 1, 2^m - 1 - m, 3]$-código de Hamming binario.

Note que este código BCH tiene distacia de diseño $\delta = 2$ y que basta probar que es un código con dimensión $2^m - 1 - m$ y distancia mínima 3 para concluir que se trata de un código de Hamming (revisar la definición).

Ejemplo 5.4. Otro caso especial se da si consideramos códigos BCH con $m = 1$ de manera que $n = q - 1$. Como antes, sea α un elemento primitivo de $\mathbb{F}_q$. Sea C el $[n, k]$-código cíclico q-ario generado por

$$g(x) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{n-k})$$

Mostraremos que C es equivalente a $RS(k, q)$ definido en 5.2. Para ello consideremos un polinomio $p(x)$ de grado menor a k. Podemos escribir $p(x) = v_0 + v_1 x + \ldots v_{k-1}x^{k-1}$. Definimos a continuación el polinomio $q(x) = f_0 + f_1 x + \ldots f_{n-1}x^{n-1}$. donde

$$f_h = p(\alpha^h) = \sum_{j=0}^{k-1} v_j \alpha^{jh}.$$

Notemos que si $1 \neq \beta \in \mathbb{F}_q^\times$

$$\sum_{h=0}^{n-1} \beta^h = \frac{\beta^n - 1}{\beta - 1} = 0$$

Calculemos $q(\alpha^i)$ para $1 \leq i \leq n$:

$$\begin{aligned} q(\alpha^i) &= \sum_{h=0}^{n-1} f_h \alpha^{ih} = \sum_{h=0}^{n-1} \sum_{j=0}^{n-1} v_j \alpha^{jh} \alpha^{ih} \\ &= \sum_{j=0}^{n-1} v_j \sum_{h=0}^{n-1} (\alpha^{i+j})^h = v_{n-i} \sum_{h=0}^{n-1} (\alpha^n)^h \\ &= -v_{n-i} \end{aligned}$$

En particular $q(\alpha^i) = 0 \quad \forall\ 1 \leq i \leq n - k$ de manera que q pertenece al código cíclico generado por g.

En resumen, si elegimos $\alpha_i = \alpha^i$, entonces

$$\epsilon(p) = (f_0, f_1, \ldots, f_{n-1}) \in RS(k, q) \Leftrightarrow q \in \langle g \rangle$$

Teorema 5.7. *La distancia mínima de un código BCH con distancia de diseño δ es $d \geq \delta$.*

Demostración. Sea α un elemento primitivo de $\mathbb{F}_{q^m}$ y sea C un código BCH generado por

$$g(x) = mcm\left(M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+\delta-2)}(x)\right).$$

Es claro que los elementos $\alpha^a, \alpha^{a+1}, \ldots \alpha^{a+\delta-2}$, son raíces de $g(x)$. Supongamos que $d \leq \delta - 1$ y que existe una palabra $c \in C$ que se puede escribir como:

$$c(x) = c_{i_1}x^{i_1} + c_{i_2}x^{i_2} + \cdots + c_{i_d}x^{i_d}$$

Sabemos que $c(\alpha^i) = 0$ para $i = a, a+a, \ldots, a+\delta-1$ de manera que:

$$\begin{pmatrix} (\alpha^a)^{i_1} & (\alpha^a)^{i_2} & \cdots & (\alpha^a)^{i_d} \\ (\alpha^{a+1})^{i_1} & (\alpha^{a+1})^{i_2} & \cdots & (\alpha^{a+1})^{i_d} \\ \vdots & \vdots & \cdots & \vdots \\ (\alpha^{a+\delta-2})^{i_1} & (\alpha^{a+\delta-2})^{i_2} & \cdots & (\alpha^{a+\delta-2})^{i_d} \end{pmatrix} \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \cdot \\ \cdot \\ c_{i_d} \end{pmatrix} = \mathbf{0}$$

Como $d \leq \delta - 1$ podemos borrar las últimas filas si fuera necesario para obtener:

$$\begin{pmatrix} (\alpha^a)^{i_1} & (\alpha^a)^{i_2} & \cdots & (\alpha^a)^{i_d} \\ (\alpha^{a+1})^{i_1} & (\alpha^{a+1})^{i_2} & \cdots & (\alpha^{a+1})^{i_d} \\ \vdots & \vdots & \cdots & \vdots \\ (\alpha^{a+d-1})^{i_1} & (\alpha^{a+d-1})^{i_2} & \cdots & (\alpha^{a+d-1})^{i_d} \end{pmatrix} \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \cdot \\ \cdot \\ c_{i_d} \end{pmatrix} = \mathbf{0}$$

Podemos calcular ahora el determinante de la matriz de la izquierda:

$$\begin{aligned} \det &= (\alpha^a)^{i_1}(\alpha^a)^{i_2}\ldots(\alpha^a)^{i_d} \det \begin{pmatrix} (1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_d} \\ (\alpha^2)^{i_1} & (\alpha^2)^{i_2} & \cdots & (\alpha^2)^{i_d} \\ \vdots & \vdots & \cdots & \vdots \\ (\alpha^{d-1})^{i_1} & (\alpha^{d-1})^{i_2} & \cdots & (\alpha^{d-1})^{i_d} \end{pmatrix} \\ &= \prod_{j=1}^{d}(\alpha^a)^{i_j} \prod_{k>l}(\alpha^{i_k} - \alpha^{i_l}) \neq 0. \end{aligned}$$

Concluimos que $(c_{i_1}, c_{i_2}, \ldots, c_{i_d}) = \mathbf{0}$ por lo que el peso mínimo de C es al menos δ $\square$

Ejemplo 5.5. Consideremos α un elemento primitivo de $\mathbb{F}_{16}$ con $\alpha^4 + \alpha + 1 = 0$ y tomemos $\delta = 5$. Construiremos el código BCH binario correspondiente. Para encontrar el polinomio generador del código debemos calcular $M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x)$ pero como se trata de un código binario, sabemos que $M^{(4)}(x) = M^{(2)}(x) = M^{(1)}(x)$. Además $M^{(1)}(x) = x^4 + x + 1$. Falta calcular $M^{(3)}(x)$.

Sea $\beta = \alpha^3$. Para encontrar el polinomio minimal de β podemos calcular sus potencias y buscar una relación de dependencia lineal.

$$\begin{aligned}
\beta^0 &= 1 \\
\beta^1 &= \beta = \alpha^3 \\
\beta^2 &= \alpha^6 = \alpha^2(\alpha+1) = \alpha^3 + \alpha^2 \\
\beta^3 &= \alpha(\alpha^2+1) = \alpha^3 + \alpha \\
\beta^4 &= (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1
\end{aligned}$$

Por inspección podemos ver que $M^{(3)}(x) = x^4 + x^3 + x^2 + x + 1$. Por lo tanto

$$\begin{aligned}
g(x) &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\
&= x^8 + x^7 + x^6 + x^4 + 1.
\end{aligned}$$

Este polinomio genera un $[15, 7, 5]$-código cíclico binario.

Ejemplo 5.6. Consideremos α un elemento primitivo de $\mathbb{F}_{64}$ con $\alpha^6 + \alpha + 1 = 0$ y tomemos $\delta = 7$. Construiremos el código BCH binario correspondiente. Para encontrar el polinomio generador del código debemos calcular $M^{(1)}(x), M^{(2)}(x), \ldots, M^{(6)}(x)$ pero como se trata de un código binario, sabemos que $M^{(4)}(x) = M^{(2)}(x) = M^{(1)}(x)$ y $M^{(6)}(x) = M^{(3)}(x)$. Además $M^{(1)}(x) = x^6 + x + 1$. Falta calcular $M^{(3)}(x)$ y $M^{(5)}(x)$.

Sea $\beta = \alpha^3$. Para encontrar el polinomio minimal de β podemos calcular sus potencias y buscar una relación de dependencia lineal.

$$\begin{aligned}
\beta^0 &= 1 \\
\beta^1 &= \beta = \alpha^3 \\
\beta^2 &= \alpha^6 = \alpha + 1 \\
\beta^3 &= \alpha^3(\alpha+1) = \alpha^4 + \alpha^3 \\
\beta^4 &= (\alpha+1)^2 = \alpha^2 + 1 \\
\beta^5 &= \alpha^3(\alpha^2+1) = \alpha^5 + \alpha^3 \\
\beta^6 &= (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1
\end{aligned}$$

Por inspección podemos ver que $M^{(3)}(x) = x^6 + x^4 + x^2 + x + 1$ De similar forma, poniendo $\gamma = \alpha^5$ podemos encontrar $M^{(5)}(x) = x^6 + x^5 + x^2 + x + 1$. Por lo tanto

$$\begin{aligned}
g(x) &= (x^6 + x + 1)(x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^2 + x + 1) \\
&= x^{18} + x^{17} + x^{16} + x^{15} + x^9 + x^7 + x^6 + x^3 + x^2 + x + 1.
\end{aligned}$$

Este polinomio genera un $[63, 45, d]$-código cíclico binario con $d \geq 7$. Es ilustrativo y se deja como ejercicio para el lector calcular lo que nos dirían las cotas conocidas para los parámetros de este código. Cabe también mencionar que existe un $[63, 45, 8]$-código binario.

5.5. Decodificación de códigos BCH. En esta sección discutiremos la decodificación de códigos BCH binarios con $a = 1$. Para fijar la notación, sea C un código BCH con $n = 2^m - 1$, $\delta = 2t + 1$ (¿Por qué no es necesario considerar δ par?), α un elemento primitivo de $\mathbb{F}_{2^m}$ y $g(x) = mcm(\big(M^{(1)}(x), M^{(2)}(x), \ldots, M^{(2t)}(x)\big)$. Usaremos la matriz

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

Notemos que esta no es la matriz de control estándar pues sus coeficiente no están en $\mathbb{F}_2$ y sus dimensiones no son $n - k \times n$.

Observando que $c \in C \Leftrightarrow cH^T = \mathbf{0}$ (ejercicio), podemos definir el síndrome de una palabra $w \in \mathbb{F}_2^n$ como $S_H(w) = wH^T$. Supongamos que la palabra recibida es $w(x) = w_0 + w_1 x + \cdots + w_{n-1}x^{n-1}$ y que el error en la transmisión está dado por $e(x)$ con $\mathrm{w}(e(x)) \leq t$. Así $c(x) = w(x) - e(x)$ es la palabra enviada.

Síndrome: El síndrome de $w(x)$ es

$$(s_0, s_1 \ldots, s_{\delta-2}) = (w_0, w_1, \ldots, w_{n-1})H^T.$$

Es claro que $s_i = w(\alpha^{i+1}) = e(\alpha^{i+1}) \forall i = 0, 1, \ldots, \delta - 2$, pues los α^{i+1} son raíces de $g(x)$.

Supongamos entonces que los errores ocurren en las posiciones $i_0, i_1, \ldots, i_{l-1}$ con $l \leq t$, es decir

$$e(x) = x^{i_0} + x^{i_1} + \cdots + x^{i_{l-1}}$$

Obtenemos el siguiente sistema de ecuaciones:

$$\begin{array}{rcccc} e(\alpha) = & \alpha^{i_0} + \alpha^{i_1} + \cdots + \alpha^{i_{l-1}} & = & s_0 & = & w(\alpha), \\ e(\alpha^2) = & (\alpha^{i_0})^2 + (\alpha^{i_1})^2 + \cdots + (\alpha^{i_{l-1}})^2 & = & s_1 & = & w(\alpha^2), \\ \vdots & \vdots & \vdots & & \vdots & \\ e(\alpha^{2t}) = & (\alpha^{i_0})^{2t} + (\alpha^{i_1})^{2t} + \cdots + (\alpha^{i_{l-1}})^{2t} & = & s_{\delta-2} & = & w(\alpha^{2t}), \end{array}$$

y cualquier método para resolver este sistema constituye un algoritmo de decodificación para el código BCH.

Polinomio localizador de errores: Para el polinomio $e(x) = x^{i_0} + x^{i_1} + \cdots + x^{i_{l-1}}$, definimos el *polinomio localizador de errores*

$$\sigma(z) := \prod_{j=0}^{l-1} (1 - \alpha^{i_j} z).$$

Es claro que para conocer las posiciones i_j de los errores basta con encontrar las raíces de $\sigma(z)$ para lo que necesitamos conocer $\sigma(z)$.

Teorema 5.8. *Supongamos que el síndrome* $s(z) = \sum_{j=0}^{\delta-2} s_j z^j \neq 0$. *Entonces existe un polinomio* $r(z) \in F_{2^m}[x]$ *de grado* $\leq t-1$ *tal que* $mcd(r(z), \sigma(z)) = 1$ *y*

$$r(z) \equiv s(z)\sigma(z) \quad \text{mód } (z^{2t}). \tag{1}$$

Además, si $u(z)$ *y* $v(z)$ *son polinomios relativamente primos en* $F_{2^m}[x]$ *que satisfagan* $grado(u(z)) \leq t-1$, $grado(v(z)) \leq t$ *y*

$$u(z) \equiv s(z)v(z) \quad \text{mód } (z^{2t}),$$

tenemos que existe $\beta \in F_{2^m}$ *tal que*

$$\sigma(z) = \beta v(z), \qquad r(z) = \beta u(z).$$

Demostración. (Existencia.) Sea

$$r(z) = \sigma(z) \sum_{j=0}^{l-1} \frac{\alpha^{i_j}}{(1-\alpha^{i_j} z)}.$$

Es claro que $r(z)$ tiene grado $l-1 \leq t-1$ y que es relativamente primo con $\sigma(z)$ pues $r(1/\alpha^{i_j}) \neq 0$ para $j = 0, 1, \ldots, l-1$.

$$\begin{aligned} s(z) &= \sum_{j=0}^{\delta-2} \sum_{k=0}^{l-1} (\alpha^{i_k})^{j+1} z^j \\ &= \sum_{k=0}^{l-1} \alpha^{i_k} \frac{1-(\alpha^{i_k} z)^{2t}}{1-\alpha^{i_k} z} \\ &\equiv r(z) \quad \text{mód } (z^{2t}). \end{aligned}$$

□

A la luz de este teorema, basta con resolver la ecuación (1) para obtener $\sigma(z)$.

A resolver la congruencia: Por el algoritmo de división, podemos definir $r_1, r_2, \ldots, r_s$ y $q_0, q_1, \ldots, q_s$ partiendo de $r_{-1}(z) = z^{2t}$ y $r_0(z) = s(z)$ de manera que se satisfagan las relaciones:

$$\begin{aligned} r_{h-1}(z) &= q_h(z) r_h(z) + r_{h+1}(z), \\ \text{grado}(r_{h+1}(z)) &< \text{grado}(r_h(z)), \qquad \text{para } h = 0, 1, \ldots, s-1 \\ r_{s-1}(z) &= q_s(z) r_s(z) \end{aligned}$$

Definimos recursivamente los polinomios $x(z)$, $y(z)$, partiendo de $x_{-1}(z) = 1$, $y_{-1}(z) = 0$, $x_0(z) = 0$, $y_0(z) = 1$ y

$$\begin{aligned} x_{h+1}(z) &= x_{h-1}(z) - q_h(z) x_h(z) \qquad \text{para } h = 0, 1, 2, \ldots, s, \\ y_{h+1}(z) &= y_{h-1}(z) - q_h(z) y_h(z) \qquad \text{para } h = 0, 1, 2, \ldots, s. \end{aligned}$$

Las siguientes propiedades se demuestran por inducción:

$$\begin{aligned} r_h(z) &= x_h(z)z^{2t} + y_h(z)s(z) && \text{para } h = -1, 0, \ldots, s, \\ \text{grado}(y_h(z)) &= 2t - \text{grado}(r_{h-1}(z)) && \text{para } h = 0, 1, \ldots, s, \\ x_{h-1}y_h - y_{h-1}x_h &= (-1)^h && \text{para } h = 0, 1, \ldots, s. \end{aligned}$$

La última identidad demuestra en particular que x_h, y_h son relativamente primos. Supongamos ahora que b es el menor índice tal que $\text{grado}(r_b(z)) < t$ y definamos

$$\begin{aligned} r(z) &= y_b(0)^{-1} r_b(z) \\ \sigma(z) &= y_b(0)^{-1} y_b(z) \end{aligned}$$

Ejemplo 5.7. Retomemos el ejemplo 5.5 y supongamos que recibimos la palabra 1101100111001l0, es decir $w(x) = 1 + x + x^3 + x^4 + x^7 + x^8 + x^9 + x^{12} + x^{13}$. Para calcular el síndrome debemos evaluar w en $\alpha, \alpha^2, \alpha^3, \alpha^4$. Antes de proceder a los cálculos, podemos establecer las siguientes identidades en $\mathbb{F}_{16}$:

$$\alpha + 1 = \alpha^4,\ \alpha^2 + 1 = \alpha^8,\ \alpha^3 + 1 = \alpha^{14},\ \alpha^5 + 1 = \alpha^{10}$$

$$\alpha^6 + 1 = \alpha^{13},\ \alpha^7 + 1 = \alpha^9,\ \alpha^{11} + 1 = \alpha^{12}$$

Procedemos a calcular, detalles solamente en el primer cálculo:

$$\begin{aligned} s_0 &= w(\alpha) = 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^7 + \alpha^8 + \alpha^9 + \alpha^{12} + \alpha^{13} \\ &= 1 + \alpha + \alpha^3(1 + \alpha) + \alpha^7(1 + \alpha) + \alpha^9 + \alpha^{12}(1 + \alpha) \\ &= \alpha^4 + \alpha^7 + \alpha^1 1 + \alpha^9 + \alpha = \alpha^4(1 + \alpha^3) + \alpha^9(1 + \alpha^2) + \alpha \\ &= \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^5 = \alpha^{11} \\ s_1 &= w(\alpha^2) = \alpha^7 \\ s_2 &= w(\alpha^3) = \alpha^4 \\ s_3 &= w(\alpha^4) = \alpha^{14} \\ s(z) &= \alpha^{11}\alpha^7 z + \alpha^4 z^2 + \alpha^{14} z^3. \end{aligned}$$

Debemos resolver ahora la ecuación de congruencia

$$r(z) \equiv s(z)\sigma(z) \mod (z^4)$$

con $\text{grado}(r(z)) \leq 1$ y $\text{grado}(\sigma(z)) \leq 2$. Usando el algoritmo de división, tenemos

$$\begin{aligned} z^4 &= s(z)(\alpha z + \alpha^6) + (\alpha z^2 + \alpha z + \alpha^2) \\ s(z) &= (\alpha z^2 + \alpha z + \alpha^2)(\alpha^{13} z + \alpha^8) + \alpha^{14} \end{aligned}$$

Debemos ahora calcular los polinomios p

$$\begin{aligned} p_1(z) &= -q_1(z) = \alpha z + \alpha^6 \\ p_2(z) &= 1 - q_2(z)p_1(z) = 1 + (\alpha z + \alpha^6)(\alpha^{13} z + \alpha^8) \\ &= \alpha^{14} z^2 + \alpha^{14} z + \alpha^3 \end{aligned}$$

Solamente falta dividir por α^3 para obtener que $\sigma(z) = 1 + \alpha^{11} z + \alpha^{11} z^2$.

Probando tenemos que α^6 y α^{13} son raíces de $\sigma(z)$ por lo que se factoriza

$$\sigma(z) = (1 + \alpha^9 z)(1 + \alpha^2 z)$$

La palabra decodificada es entonces

$$c(x) = w(x) + x^9 + x^2 = 1 + x + x^2 + x^3 + x^4 + x^7 + x^8 + x^{12} + x^{13}$$

6. Cotas para los parámetros de un código

En la sección 4 ya vimos la cota de Singleton y la cota de Hamming, ahora agregaremos algunas más a nuestro repertorio. Pero antes de eso, la siguiente definición nos ayudará a enunciar más claramente las cotas.

Definición 6.1. *Sea q una potencia de primo y sean n, d enteros positivos con $d \leq n$. Entonces definimos $A_q(n, d)$ como el mayor valor de M para el que existe un código sobre $\mathbb{F}_q$ de largo n con M palabras y distancia mínima d. Por la cota de Singleton tenemos $A_q(n, d) \leq q^{n-d+1}$ pero esta cota no parece ser optimal para códigos largos.*

La demostración del siguiente resultado usa la desigualdad de Cauchy-Schwarz que enunciaremos a modo de referencia.

Lema 6.2 (Desigualdad de Cauchy-Schwarz)**.** *Si $\mathbf{a} = (a_1, a_2, \ldots, a_r)$ y $\mathbf{b} = (b_1, b_2, \ldots, b_r)$ son vectores con coeficientes reales, entonces*

$$\left(\sum_{k=1}^{r} a_k b_k\right)^2 \leq \left(\sum_{k=1}^{r} a_k^2\right)\left(\sum_{k=1}^{r} b_k^2\right).$$

En particular, si $\mathbf{b} = (1, 1, \ldots, 1)$ tenemos

$$\left(\sum_{k=1}^{r} a_k\right)^2 \leq r\left(\sum_{k=1}^{r} a_k^2\right) \tag{2}$$

Teorema 6.3 (Cota de Plotkin)**.** *Sea $\theta = 1 - \frac{1}{q}$. Entonces*

$$A_q(n, d) \leq \frac{d}{d - \theta n} \qquad \text{si } d > \theta n$$

Notemos que esta cota solamente se puede usar si d es relativamente grande respecto a n.

Demostración. Sea C un código de largo n con M palabras y distancia mínima d sobre $\mathbb{F}_q$. Sea $S = \sum_{\mathbf{x}\in C} \sum_{\mathbf{y}\in C} d(\mathbf{x}, \mathbf{y})$. Como d es la distancia mínima entre palabras y tenemos $M(M-1)$ pares ordenados de palabras diferentes en C, obtenemos inmediatamente que $S \geq M(M-1)d$.

A continuación obtendremos una cota superior para S. Formemos una matriz de $M \times n$ donde las filas son las palabras de C. Sea $m_{i,\alpha}$ el número de veces que el elemento

α de $\mathbb{F}_q$ aparece en la columna i-ésima. (Nótese que $\sum_{i=1}^{n} m_{i,\alpha} = M$.) Podemos ahora calcular nuevamente S como

$$\begin{aligned} S &= \sum_{i=1}^{n} \sum_{x \in C} \sum_{y \in C} d(x_i, y_i) \\ &= \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} m_{i,\alpha}(M - m_{i,\alpha}) \\ &= nM^2 - \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} m_{i,\alpha}^2 \\ &\leq nM^2 - \sum_{i=1}^{n} q^{-1} \left(\sum_{\alpha \in \mathbb{F}_q} m_{i,\alpha} \right)^2 = nM^2 - nq^{-1}M^2 = n\theta M^2 \end{aligned}$$

En resumen tenemos

$$M(M-1)d \leq S \leq n\theta M^2$$

Reordenando $M(d - \theta n) \leq d$, de manera que si $d - \theta n > 0$ obtenemos

$$M \leq \frac{d}{d - \theta n}$$

□

Cuando $d \leq n\theta$ podemos usar el teorema después de recortar el código de manera apropiada.

Corolario 6.4. *Si $n \geq \frac{d}{\theta}$, definimos $n' = \lfloor \frac{d-1}{\theta} \rfloor$ y $k = n - n'$. Entonces*

$$A_q(n, d) \leq q^k \frac{d}{d - \theta n'} \leq q^k d$$

Demostración. Sea C un código de largo n con M palabras y distancia mínima d sobre $\mathbb{F}_q$. Por el principio de las casillas, al menos M/q de estas palabras deben tener el mismo símbolo en la última posición. Consideremos el código C' que se forma al considerar esta selección de palabras de C borrándoles el último dígito. Claramente C' es un código de largo $n-1$ con al menos M/q palabras y su distancia mínima es al menos d.

Repitiendo este proceso k veces, obtenemos un código C_k con $M' \geq \frac{M}{q^k}$ palabra, largo $n' = n - k$ y distancia mínima $d' \geq d$. Como $d' \geq d > \theta n'$, podemos usar la cota de Plotkin para este nuevo código:

$$M' \leq \frac{d'}{d' - \theta n'} = \frac{d}{d - \frac{d}{d'}\theta n'} \leq \frac{d}{d - \theta n'}$$

□

La siguiente es una cota inferior para $A_q(n, d)$.

Teorema 6.5 (Cota de Gilbert-Varshamov)**.** *Si*

$$V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

es el número de puntos en una bola de radio r, entonces

$$A_q(n,d) \geq \frac{q^n}{V_q(n,d-1)}$$

OBS: Con esta notación, la cota de Hamming dice que

$$A_q(n,d) \leq \frac{q^n}{V_q(n, \lfloor \frac{d-1}{2} \rfloor)}$$

Demostración. Sea C un código de largo n sobre $\mathbb{F}_q$ con distancia mínima d y $M = A_q(n,d)$ palabras. Sea $\mathbf{y} \in \mathbb{F}_q^n$ arbitrario. Si $\mathbf{y}$ no pertenece a $B_{d-1}(\mathbf{x})$ para ningún $\mathbf{x} \in C$, entonces $d(\mathbf{x},\mathbf{y}) \geq d$ para todo $\mathbf{x} \in C$. Por lo tanto $C \cup \{\mathbf{y}\}$ es un código de largo n con distancia mínima d y $M+1$ palabras lo que contradice la maximalidad de M. Concluimos entonces que $\mathbf{y}$ pertenece a $B_{d-1}(\mathbf{x})$ para algún $\mathbf{x} \in C$. Como $\mathbf{y}$ era arbitrario, esto quiere decir que la unión de todas las bolas de radio $d-1$ centradas en palabras de C debe ser todo $\mathbb{F}_q^n$ y tenemos

$$q^n \leq M V_q(n, d-1)$$

□

6.1. Cotas asintóticas. Para entender los parámetros de códigos para valores grandes de n tiene sentido normalizar k y d dividiendo por n. En ese sentido definimos la tasa de información de un código C como $R := k/n$ y la distancia mínima relativa como $\delta := d/n$. Recordemos que si C no es lineal, $k = \log_q M$ donde M es el número de palabras de l código.

Como R y δ están entre 0 y 1, un buen código tendrá ambos valores lo más cercanos a 1 que se pueda.

El problema se transforma entonces en determinar dado δ, cuál es el mayor valor de R que se puede lograr.

Definición 6.6. *Dado q una potencia de primo y $\delta \in \mathbb{R}$ con $0 \leq \delta \leq 1$ se define*

$$\alpha_q(\delta) := \limsup_{n\to\infty} \frac{1}{n} \log_q A_q(n, \lfloor \delta n \rfloor)$$

Después de pensarlo un poco, se pueder ver que $\alpha_q(\delta)$ es el mayor valor de R tal que existe una sucesión de códigos cada vez más largo sobre $\mathbb{F}_q$ cuya distancia mínima converge a δ y cuya tasa de información converge a R. Tenemos las siguientes cotas asintóticas.

Teorema 6.7 (Cota asintótica de Plotkin)**.** *Con* $\theta = 1 - \frac{1}{q}$*, tenemos*

$$\alpha_q(\delta) \leq 1 - \frac{\delta}{\theta}, \quad si\ 0 \leq \delta \leq \theta$$
$$\alpha_q(\delta) = 0, \quad si\ \theta < \delta \leq 1$$

Demostración. Si $\theta < \delta \leq 1$, podemos usar la cota de Plotkin (6.3) para ver que

$$\begin{aligned}
\alpha_q(\delta) &= \limsup_{n\to\infty} \frac{1}{n} \log_q A_q(n, \lfloor \delta n \rfloor) \\
&\leq \limsup_{n\to\infty} \frac{1}{n} \log_q \left(\frac{\lfloor \delta n \rfloor}{\lfloor \delta n \rfloor - \theta n} \right) \\
&= \limsup_{n\to\infty} \frac{1}{n} \log_q \left(\frac{\delta n}{\delta n - \theta n} \right) \\
&= \limsup_{n\to\infty} \frac{1}{n} \log_q \left(\frac{\delta}{\delta - \theta} \right) \\
&= 0
\end{aligned}$$

Si $0 \leq \delta \leq \theta$ podemos usar el corolario 6.4 para ver que

$$\begin{aligned}
\alpha_q(\delta) &= \limsup_{n\to\infty} \frac{1}{n} \log_q A_q(n, \lfloor \delta n \rfloor) \\
&\leq \limsup_{n\to\infty} \frac{1}{n} \log_q \left(q^{n - \lfloor \frac{\lfloor \delta n \rfloor - 1}{\theta} \rfloor} \lfloor \delta n \rfloor \right) \\
&= \limsup_{n\to\infty} \frac{1}{n} \left(n - \lfloor \frac{\lfloor \delta n \rfloor - 1}{\theta} \rfloor + \log_q \left(\lfloor \delta n \rfloor \right) \right) \\
&= 1 - \frac{\delta}{\theta}
\end{aligned}$$

□

Definición 6.8. *Como ya es usual, tomamos* $\theta = 1 - \frac{1}{q}$*, y definimos la* función de entropía de Hilbert *en el intervalo* $0 \leq x \leq \theta$ *como*

$$H_q(x) := \begin{cases} 0, & si\ x = 0 \\ x \log_q(q-1) - x \log_q x - (1-x) \log_q (1-x), & si\ 0 < x \leq \theta \end{cases}$$

Lema 6.9. *Si* $0 \leq \lambda \leq 1 - \frac{1}{q}$*, tenemos*

$$\lim_{n\to\infty} \frac{1}{n} \log_q V_q(n, \lfloor \lambda n \rfloor) = H_q(\lambda)$$

donde $H_q(x)$ *es la función de entropía de Hilbert definida en el intervalo* $[0, 1 - \frac{1}{q}]$ *por*

$$H_q(x) := \begin{cases} 0, & si\ x = 0 \\ x \log_q(q-1) - x \log_q x - (1-x) \log_q (1-x), & si\ 0 < x \leq 1 - \frac{1}{q} \end{cases}$$

Demostración. Sea $t = \lfloor \lambda n \rfloor$. Debemos estimar el valor de

$$\log_q V_q(n,t) = \log_q \left(\sum_{k=0}^{t} \binom{n}{k} (q-1)^k \right)$$

En primer lugar demostraremos que los términos en la suma son crecientes. Para ello calculemos el cuociente de dos consecutivos de ellos:

$$\frac{\binom{n}{k}(q-1)^k}{\binom{n}{k-1}(q-1)^{k-1}} = \frac{(n-k+1)(q-1)}{k} \geq \frac{(n-n(1-\frac{1}{q})+1)(q-1)}{n(1-\frac{1}{q})} = 1 + \frac{q}{n}$$

Podemos entonces acotar la suma por ambos lados de la siguiente manera:

$$\binom{n}{t}(q-1)^t \leq \sum_{k=0}^{t} \binom{n}{k}(q-1)^k \leq t\binom{n}{t}(q-1)^t \tag{3}$$

Ahora estimemos el término de la izquierda

$$\log_q \left(\binom{n}{t}(q-1)^t \right) = \sum_{k=1}^{t} \big(\log_q(n-k+1) - \log_q(k) \big) + t \log_q(q-1)$$

De cálculo sabemos (o podemos deducir) que

$$b\ln b - (a-1)\ln(a-1) - (b+1-a) \leq \sum_{k=a}^{b} \ln k \leq (b+1)\ln(b+1) - a\ln a - (b+1-a)$$

en particular, (dividiendo por $\ln(q)$ para tener $\log_q$),

$$\begin{aligned} & n\log_q n - (n-t)\log_q(n-t) - \frac{t}{\ln q} \\ \leq & \sum_{k=n-t+1}^{n} \log_q(n-k+1) \\ \leq & (n+1)\log_q(n+1) - (n-t+1)\log_q(n-t+1) - \frac{t}{\ln q} \end{aligned}$$

$$\begin{aligned} t\log_q t - \frac{t-1}{\ln q} & \leq \sum_{k=2}^{t} \log_q(k) \\ & \leq (t+1)\log_q(t+1) - 2\log_q 2 - \frac{t-1}{\ln q} \end{aligned}$$

Reemplazando en la sumatoria tenemos

$$\begin{aligned} & n\log_q(\frac{n}{n-t}) + t\log_q(\frac{n-t}{t+1}) - \log_q(t+1) - \frac{1}{\ln q} + 2\log_q 2 \\ \leq & \sum_{k=1}^{t} \big(\log_q(n-k+1) - \log_q(k)\big) \\ \leq & (n+1)\log_q(\frac{n+1}{n-t+1}) + t\log_q(\frac{n-t+1}{t}) - \frac{1}{\ln q} \end{aligned}$$

Poniendo $t = n\lambda$ y dividiendo por n:

$$\begin{aligned} & \log_q(\frac{1}{1-\lambda}) + \lambda\log_q(\frac{1-\lambda}{\lambda+\frac{1}{n}}) - \frac{\log_q(n\lambda+1)}{n} - \frac{1}{n\ln q} + \frac{2\log_q 2}{n} \\ \leq & \frac{1}{n}\sum_{k=1}^{t} \big(\log_q(n-k+1) - \log_q(k)\big) \\ \leq & (1+\frac{1}{n})\log_q(\frac{1+\frac{1}{n}}{1-\lambda+\frac{1}{n}}) + \lambda\log_q(\frac{1-\lambda+\frac{1}{n}}{\lambda}) - \frac{1}{n\ln q} \end{aligned}$$

Haciendo tender n a infinito,

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{t} \big(\log_q(n+k-1) - \log_q(k)\big) &= \log_q(\frac{1}{1-\lambda}) + \lambda\log_q(\frac{1-\lambda}{\lambda}) \\ &= -\lambda\log_q\lambda - (1-\lambda)\log_q(1-\lambda) \end{aligned}$$

De lo que concluimos:

$$\lim_{n\to\infty} \frac{1}{n}\log_q\left(\binom{n}{t}(q-1)^t\right) = \lambda\log_q(q-1) - \lambda\log_q\lambda - (1-\lambda)\log_q(1-\lambda)$$

Ahora para el lado derecho de (3)

$$\lim_{n\to\infty} \frac{1}{n}\log_q\left(t\binom{n}{t}(q-1)^t\right) = \lambda\log_q(q-1) - \lambda\log_q\lambda - (1-\lambda)\log_q(1-\lambda)$$

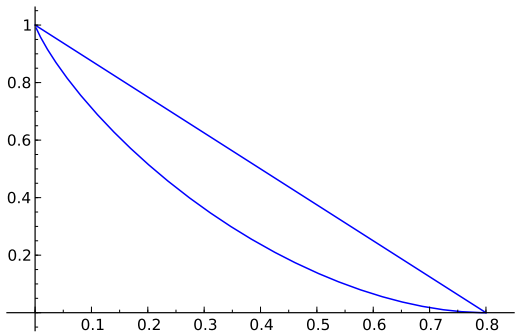
Esto termina la demostración. □

Teorema 6.10 (Cota asintótica de Gilbert-Varshamov)**.** *Para cualquier δ con $0 \leq \delta \leq \theta$, tenemos*

$$\alpha_q(\delta) \geq 1 - H_q(\delta)$$

Demostración. Ejercicio para el lector. □

A modo de ilustración incluimos una gráfica con las cotas asintóticas de Plotkin y de Gilbert-Varshamov para $q = 5$.



7. Códigos de Goppa

7.1. Códigos de Goppa clásicos. Volvamos sobre los síndromes definidos para códigos BCH reescribiendo la congruencia (1) de la página 66 como una ecuación explícita. Después de reordenar:

$$s(z) = \frac{r(z)}{\sigma(z)} - \frac{x(z)z^{2t}}{\sigma(z)} \tag{4}$$

Goppa (1980) propone reemplazar z^{2t} por un polinomio arbitrario $g(z)$, definiendo el código como el conjunto de aquellas palabras en $\mathbb{F}^n$ cuyo síndrome $s(z)$ sea congruente a 0 módulo $g(z)$. Para comenzar a entender esto, recordemos la definición de $s(z)$ en términos de la palabra recibida $w(x)$:

$$\begin{aligned}
s(z) &= \sum_{i=0}^{2t-1} s_{i+1} z^i = \sum_{i=0}^{2t-1}\sum_{j=0}^{n-1} w_j \alpha^{(i+1)j} z^i \\
&= \sum_{j=0}^{n-1} w_j \alpha^j \sum_{i=0}^{2t-1} (\alpha^j z)^i \\
&= \sum_{j=0}^{n-1} w_j \alpha^j \frac{1-(\alpha^j z)^{2t}}{1-\alpha^j z} \\
&= \sum_{j=0}^{n-1} \frac{w_j \alpha^j}{1-\alpha^j z} - \sum_{j=0}^{n-1} \frac{w_j \alpha^{(2t+1)j} z^{2t}}{1-\alpha^j z} \\
&\equiv \sum_{j=0}^{n-1} \frac{w_j \alpha^j}{1-\alpha^j z} \quad \text{mód } z^{2t}
\end{aligned}$$

Esta última congruencia debemos entenderla como una igualdad en el anillo cuociente $\mathbb{F}[z]/(z^{2t})$. Escribiendo $\gamma = \alpha^{-1}$ tenemos

$$-s(z) \equiv \sum_{j=0}^{n-1} \frac{w_j}{z-\gamma^j} \quad \text{mód } z^{2t}$$

Hasta acá solamente hemos reinterpretado los códigos BCH. Ahora redefiniremos $s(z)$ para introducir los códigos de Goppa clásicos.

Definición 7.1. *Consideremos $\mathbb{F} \subseteq \mathbb{E}$ cuerpos finitos y $P = \{\beta_1, \ldots, \beta_n\}$ elementos de $\mathbb{E}$ tales que $g(\beta_i) \neq 0$ para $i = 1, \ldots, n$. Definimos el código de Goppa $GC(P, g)$ como el conjunto de las palabras $w \in \mathbb{F}^n$ tales que*

$$s(z) = \sum_{i=1}^{n} \frac{w_j}{z - \beta_j} \equiv 0 \mod g(z)$$

Si $\mathbb{E} = \mathbb{F}$ hablaremos de código de Goppa completo y en caso contrario de código de Goppa de subcuerpo.

Observemos que los códigos RS son códigos de Goppa completos y los BCH son códigos de Goppa de subcuerpo para $g(z) = z^{2t}$.

Ejercicio 7.1. Explique esta observación en detalle.

Definición 7.2 (Congruencia para funciones racionales)**.** *En términos puramente polinomiales, si $s(z) = \dfrac{n(z)}{u(z)}$ con $mcd(n(z), u(z)) = 1$, diremos que $s(z) \equiv 0 \mod g(z)$ si $g(z)$ divide a $n(z)$. Además diremos que $s(z) \equiv t(z) \mod g(z)$ si $s(z) - t(z) \equiv 0 \mod g(z)$.*

Otra manera de desarrollar los códigos de Goppa sería encontrar polinomios $h_j(z)$ tales que $h_j(z)(z - \beta_j) \equiv 1 \mod g(z)$ con $h_j(z)$ de grado menor al grado de $g(z)$ y reemplazar estos por los $(z - \beta_j)^{-1}$ en la definición de $s(z)$. Los podemos encontrar explícitamente como:

$$h_j(z) = \frac{g(z) - g(\beta_j)}{(\beta_j - z)g(\beta_j)}$$

Definimos entonces el síndrome polinomial

$$s_p(z) = \sum_{j=1}^{n} w_j h_j(z)$$

Observación 7.3.

$$s(z) \equiv 0 \mod g(z) \Leftrightarrow s_p(z) = 0$$

Ejemplo 7.1 (Dos códigos de Goppa completos)**.** Usaremos el cuerpo $\mathbb{F} = \mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ con $\alpha^4 + \alpha + 1 = 0$, ($\mathbb{E} = \mathbb{F}$) y los polinomios $g(z) = z^3 + z + 1$ y $g^2(z) = z^6 + z^2 + 1$. Como $g(z)$ no tiene raíces en $\mathbb{F}_{16}$ (demostrarlo), podemos elegir P como el conjunto de todos los elementos del cuerpo. Si $\alpha \in \mathbb{F}_{16}$ es un elemento primitivo, las palabras en $GC(P, g)$ son los $(w_0, \ldots w_{14}, w_\infty)$ que satisfacen

$$s(z) = \sum_{j=0}^{14} \frac{w_j}{z - \alpha^j} + \frac{w_\infty}{z} \equiv 0 \mod z^3 + z + 1$$

Para $g(z)$ estas son 3 ecuaciones y para $g^2(z)$ son 5. Calcularemos primero los valores de $g(\alpha^j)$:

$$\begin{array}{lllll} g(1)=1 & g(\alpha)=\alpha^7 & g(\alpha^2)=\alpha^{14} & g(\alpha^3)=\alpha^4 & g(\alpha^4)=\alpha^{13} \\ g(\alpha^5)=\alpha^5 & g(\alpha^6)=\alpha^8 & g(\alpha^7)=\alpha^5 & g(\alpha^8)=\alpha^{11} & g(\alpha^9)=\alpha^2 \\ g(\alpha^{10})=\alpha^{10} & g(\alpha^{11})=\alpha^{10} & g(\alpha^{12})=\alpha & g(\alpha^{13})=\alpha^5 & g(\alpha^{14})=\alpha^{10} \end{array}$$

Podemos calcular los h_j correspondientes, obteniendo

$$\begin{aligned} h_0(z) &= \frac{g(z)-g(1)}{(1-z)g(1)} = \frac{z^3+z+1-1}{1-z} = z^2+z \\ h_1(z) &= \frac{z^3+z+1+\alpha^7}{(z+\alpha)\alpha^7} = \alpha^8 z^2+\alpha^9 z+\alpha \\ &\vdots \\ h_\infty(z) &= z^2+1 \end{aligned}$$

La matriz de control para el código es:

$$\begin{pmatrix} 1 & \alpha^8 & \alpha & \alpha^{11} & \alpha^2 & \alpha^{10} & \alpha^7 & \alpha^{10} & \alpha^4 & \alpha^{13} & \alpha^5 & \alpha^5 & \alpha^{14} & \alpha^{10} & \alpha^5 & 1 \\ 1 & \alpha^9 & \alpha^3 & \alpha^{14} & \alpha^6 & 1 & \alpha^{13} & \alpha^2 & \alpha^{12} & \alpha^7 & 1 & \alpha & \alpha^{11} & \alpha^8 & \alpha^4 & 0 \\ 0 & \alpha & \alpha^2 & \alpha^9 & \alpha^4 & 1 & \alpha^3 & \alpha^{13} & \alpha^8 & \alpha^{12} & 1 & \alpha^{14} & \alpha^6 & \alpha^7 & \alpha^{11} & 1 \end{pmatrix}$$

¿Cuál es la distancia mínima del código?
La forma estándar de esta matriz de control es

$$\begin{pmatrix} \alpha^8 & \alpha^6 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha^2 & \alpha^{11} & \alpha^8 & \alpha^8 & \alpha & \alpha & \alpha & \alpha^6 & 1 & 0 & 0 \\ 1 & 1 & \alpha^{11} & \alpha & \alpha^{11} & \alpha & \alpha^7 & \alpha & \alpha^9 & \alpha^{11} & \alpha^3 & \alpha^{14} & \alpha^6 & 0 & 1 & 0 \\ \alpha^{12} & 1 & \alpha & \alpha^7 & \alpha^{10} & \alpha^2 & \alpha^3 & \alpha^4 & \alpha & 1 & \alpha^{13} & \alpha^7 & \alpha^8 & 0 & 0 & 1 \end{pmatrix}$$

para $g^2(z)$, la matriz de control es

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^7 & \alpha^4 & \alpha^5 & \alpha^{14} & \alpha^5 & \alpha^8 & \alpha^{11} & \alpha^{10} & \alpha^{10} & \alpha^{13} & \alpha^5 & \alpha^{10} & 1 \\ 1 & \alpha^2 & \alpha^4 & \alpha^{10} & \alpha^8 & \alpha^{10} & \alpha^5 & \alpha^{12} & \alpha & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^{10} & \alpha^3 & \alpha^9 & 0 \\ 1 & \alpha^3 & \alpha^6 & \alpha^{13} & \alpha^{12} & 1 & \alpha^{11} & \alpha^4 & \alpha^9 & \alpha^{14} & 1 & \alpha^2 & \alpha^7 & \alpha & \alpha^8 & 0 \\ 1 & \alpha^4 & \alpha^8 & \alpha & \alpha & \alpha^5 & \alpha^2 & \alpha^{11} & \alpha^2 & \alpha^8 & \alpha^{10} & \alpha^{13} & \alpha^4 & \alpha^{14} & \alpha^7 & 0 \\ 0 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^8 & 1 & \alpha^6 & \alpha^{11} & \alpha & \alpha^9 & 1 & \alpha^{13} & \alpha^{12} & \alpha^{14} & \alpha^7 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha^6 & \alpha^{12} & \alpha^5 & \alpha^{12} & \alpha^3 & \alpha^9 & \alpha^3 & \alpha^{10} & \alpha^9 & \alpha^9 & \alpha^{12} & \alpha^6 & 0 \end{pmatrix}$$

y en forma estándar obtenemos:

$$\begin{pmatrix} \alpha^5 & \alpha^{13} & \alpha^5 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha & \alpha^{14} & \alpha^2 & 1 & 0 & 0 & 0 & 0 & 0 \\ \alpha^6 & \alpha^8 & \alpha^8 & \alpha^6 & \alpha^2 & \alpha^9 & \alpha^5 & \alpha^7 & \alpha & \alpha^6 & 0 & 1 & 0 & 0 & 0 & 0 \\ \alpha^7 & \alpha & \alpha^{10} & \alpha & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^{13} & \alpha^{14} & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ \alpha^{12} & \alpha^2 & \alpha^3 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^{10} & \alpha^5 & \alpha^{13} & 0 & 0 & 0 & 1 & 0 & 0 \\ \alpha^{12} & \alpha^4 & \alpha & \alpha^8 & \alpha^3 & \alpha^{12} & \alpha^{10} & \alpha^{11} & \alpha^{14} & \alpha & 0 & 0 & 0 & 0 & 1 & 0 \\ \alpha^7 & \alpha^2 & \alpha^4 & \alpha^{12} & 1 & \alpha^{11} & \alpha^4 & \alpha^{12} & \alpha^4 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Como ejemplo verificaremos que la siguiente es una palabra del código GC_2:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^{12} & \alpha^{12} & \alpha^7 \end{pmatrix}$$

Para ello debemos calcular su síndrome:

$$\begin{aligned} & \frac{1}{z-1}+\frac{\alpha^5}{z-\alpha^{10}}+\frac{\alpha^6}{z-\alpha^{11}}+\frac{\alpha^7}{z-\alpha^{12}}+\frac{\alpha^{12}}{z-\alpha^{13}}+\frac{\alpha^{12}}{z-\alpha^{14}}+\frac{\alpha^7}{z} \\ = & \frac{\alpha^7 z^6+\alpha^7 z^2+\alpha^7}{\alpha^4 z^6+\alpha^2 z^5+\alpha z^4+\alpha^{12} z^3+\alpha^9 z^2+z} \\ \equiv & \ 0 \mod z^6+z^2+1 \end{aligned}$$

8. Curvas algebraicas sobre cuerpos finitos

Sería necesario un curso mucho más extenso y un libro completo para empezar a hacerle justicia al título de esta sección, pero intentaremos mostrar los conceptos básicos para poder usarlos en la construcción de códigos. En particular nos restringiremos a curvas proyectiva planas y no singulares.

Definición 8.1. *Dado un cuerpo k y un polinomio $f(x,y) \in k[x,y]$ se define la curva afín $C_f(K)$ como el conjunto de soluciones de la ecuación $f(x,y)=0$ en K^2. Notemos que acá K denota una extensión del cuerpo k donde está definido el polinomio f.*

Definición 8.2. *Dado un cuerpo k se define el* plano proyectivo

$$\mathbb{P}^2(k) := \left(k^3 \setminus (0,0,0)\right) / \sim$$

donde $(X_0,Y_0,Z_0) \sim (X_1,Y_1,Z_1)$ si y sólo si existe $\alpha \in k^\times$, con $X_1=\alpha X_0$, $Y_1=\alpha Y_0$ y $Z_1=\alpha Z_0$.

Denotaremos por $(X_0:Y_0:Z_0)$ a la clase de (X_0,Y_0,Z_0).

Definición 8.3. *Dado un polinomio $f(x,y) \in k[x,y]$ de grado d se define su homogenización $F(X,Y,Z) \in k[X,Y,Z]$ como*

$$F(X,Y,Z) = Z^d f(X/Z, Y/Z)$$

Notemos que $f(x,y)=F(x,y,1)$.

Definición 8.4. *Definimos la clausura proyectiva de una curva C_f como*

$$\widehat{C_f} := \{(X,Y,Z) \in \mathbb{P}^2 | F(X,Y,Z)=0\}$$

donde F es la homogenización de f

A los puntos cuya tercera coordenada es cero, los llamaremos puntos en el infinito *de la curva. A los demás los llamaremos* puntos afines.

Ejemplo 8.1. Consideremos el polinomio $f(x,y)=y-x^2 \in \mathbb{R}[x,y]$.

$$C_f = \{(t,t^2) | t \in \mathbb{R}\}$$

$$\widehat{C_f} := \{(t:t^2:1) | t \in \mathbb{R}\} \cup \{(0:1:0)\}$$

Ejercicio 8.1. Sea $f(x,y)=x^3+x^2y-3xy^2-3y^3+2x^2-x+5$. Encuentre todos los puntos en infinito de $\widehat{C_f}(\mathbb{C})$.

Definición 8.5. *Denotaremos por $\bar{k}$ a la clausura algebraica de un cuerpo k.*

Teorema 8.6 (Teorema de Bezout)**.** *Si f y g son polinomios de grado d y e respectivamente que no tienen factor común no constante, entonces C_f y C_g se intersectan en a lo más $d \cdot e$ puntos. Más aún, sus clausuras proyectivas en $\mathbb{P}^2(\bar{k})$ se intersectan en exactamente $d \cdot e$ puntos si los contamos con multiplicidad.*

Ejercicio 8.2. Encuentre los puntos de $C(\mathbb{F}_5)$ donde C es la clausura proyectiva de la curva definida por $y^2 = x^3 + 1$

Singularidades. Para definir lo que es un punto singular, necesitamos extender el concepto de derivadas a cuerpos finitos. La definición usando límites deja de tener sentido si la característica del cuerpo es finita, por lo que definimos formalmente las derivadas parciales de f de manera que satisfagan las reglas conocidas de derivación de polinomios.

Ejemplo 8.2. Si $f(x, y) = x^2 + y^3 + xy \in k[x, y]$, entonces $f_x(x, y) = 2x + y$, y $f_y(x, y) = 3y^2 + x$. En particular, si $k = \mathbb{F}_2$, tenemos $f_x(x, y) = y$.

Definición 8.7. *Un punto $(x_0, y_0) \in \bar{k}^2$ es un* punto singular *de la curva C_f si $f(x_0, y_0) = 0$ y $f_x(x_0, y_0) = f_y(x_0, y_0) = 0$. Diremos que la curva C_f es* no-singular *si no tiene puntos singulares.*

De manera similar se define punto singular y curva no-singular en el caso proyectivo.

Género. Un resultado clásico de topología dice que toda curva no singular sobre $\mathbb{C}$ se puede incrustar topológicamente como una superficie en $\mathbb{R}^3$. Por ejemplo una curva elíptica tiene una ecuación de la forma $y^2 = f(x)$ donde $f(x)$ es un polinomio cúbico que no tiene raíces repetidas y se puede ver como un toro (rosquilla) en $\mathbb{R}^3$. En general resulta que si $f(x, y)$ es un polinomio de grado d tal que la curva $\widehat{C_f}$ es no-singular, entonces el género topológico de C_f está dado por la fórmula de Plücker

$$g = \frac{(d-1)(d-2)}{2}$$

En lo que sigue usaremos esta fórmula como definición para el género de una curva proyectiva no-singular sobre un cuerpo arbitrario.

Ejercicio 8.3. Para cada uno de los siguientes polinomios, verifique que la curva proyectiva plana correspondiente es no-singular y encuentre su género.

1. $f(x, y) = y^2 - p(x)$, donde $p(x) \in k[x]$ es de grado 3 sin raíces repetidas, y la característica de k no es 2.
2. $f(x, y) = y^2 + y - p(x)$, donde $p(x) \in k[x]$ es de grado 3 sin raíces repetidas, y la característica de k es 2.
3. $f(x, y) = x^{q+1} + y^{q+1} - 1 \in \mathbb{F}_{q^2}[x, y]$ donde q es una potencia de primo.

Puntos racionales de una curva. El título de esta seción está motivado por la idea de encontrar puntos de coordenadas en $\mathbb{Q}$ que satisfacen una cierta ecuación polinómica. Estas ecuaciones diofánticas son muy estudiadas. En el contexto de estas notas, nos interesa encontrar puntos de una curva definida sobre un cuerpo finito que tengan

coordenadas en el mismo cuerpo de definición del polinomio o en una extensión finita de este cuerpo.

Definición 8.8. *Sea k un cuerpo y sea $F(X,Y,Z) \in k[X,Y,Z]$ un polinomio homogéneo. Dada una extensión $K \supseteq k$, definimos unn punto K-racional en C como un punto en $(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(K)$ que satisface $F(X_0, Y_0, Z_0) = 0$. Denotaremos por $C(K)$ el conjunto de todos los puntos K-racionales de la curva.*

Notemos que si $k = \mathbb{F}_q$ y $K = F_{q^n}$, tenemos el automorfismo de Frobenius σ_q en K que envía a cada elemento a su q-ésima potencia. Consideremos ahora un polinomio $f(x,y) \in k[x,y]$ y la curva afín C asociada. Si $(x_0, y_0) \in C(K)$, entonces la imagen bajo la acción de σ_q también está en la curva.

Definición 8.9. *Si $(x_0, y_0) \in C(\mathbb{F}_{q^n})$, diremos que el conjunto*

$$P = \{\sigma_n^k(x_0, y_0) | k = 0, 1, \ldots n-1\}$$

es un punto de grado n de la curva C sobre $\mathbb{F}_q$.

Ejemplo 8.3. Para ilustrar, sea $k = \mathbb{F}_5$ y consideremos la curva elíptica definida por $y^2 = x^3 + 2$. La curva es no-singular $C(\mathbb{F}_5)$ posee 5 puntos afines y su clausura proyectiva tiene además 1 punto en infinito. Los puntos de la curva proyectiva $(zy^2 = x^3 + 2z^3)$ son:

$$\{(2:0:1), (3:2:1), (3:3:1), (4:1:1), (4:4:1), P_\infty = (0:1:0)\}$$

Consideremos la extensión $\mathbb{F}_{25} = \mathbb{F}_5[\alpha]$ donde α es raiz del polinomio irreducible $x^2 + 4x + 2 \in \mathbb{F}_5[x]$. Los nuevos puntos de la curva que encontramos son puntos de grado 2 sobre $\mathbb{F}_5$.

$$\begin{aligned}
P_1 &= \{(0 : \alpha + 2 : 1), (0 : 4\alpha + 3 : 1)\} \\
P_2 &= \{(0 : 2\alpha + 4 : 1), (0 : 3\alpha + 1 : 1)\} \\
P_3 &= \{(\alpha + 1 : 0 : 1), (4\alpha + 2 : 0 : 1)\} \\
P_4 &= \{(\alpha + 2 : 2\alpha + 2 : 1), (4\alpha + 3 : 3\alpha + 4 : 1)\} \\
P_5 &= \{(\alpha + 2 : 3\alpha + 3 : 1), (4\alpha + 3 : 2\alpha + 1 : 1)\} \\
P_6 &= \{(\alpha + 3 : 2 : 1), (4\alpha + 4 : 2 : 1)\} \\
P_7 &= \{(\alpha + 3 : 3 : 1), (4\alpha + 4 : 3 : 1))\} \\
P_8 &= \{(2\alpha : 2\alpha + 2 : 1), (3\alpha + 2 : 3\alpha + 4 : 1)\} \\
P_9 &= \{(2\alpha : 3\alpha + 3 : 1), (3\alpha + 2 : 2\alpha + 1 : 1)\} \\
P_{10} &= \{(2\alpha + 1 : 2\alpha + 4 : 1), (3\alpha + 3 : 3\alpha + 1 : 1)\} \\
P_{11} &= \{(2\alpha + 1 : 3\alpha + 1 : 1), (3\alpha + 3 : 2\alpha + 4 : 1)\} \\
P_{12} &= \{(2\alpha + 2 : 1 : 1), (3\alpha + 4 : 1 : 1)\} \\
P_{13} &= \{(2\alpha + 2 : 4 : 1), (3\alpha + 4 : 4 : 1)\} \\
P_{14} &= \{(2\alpha + 3 : 2\alpha + 2 : 1), (3\alpha : 3\alpha + 4 : 1)\} \\
P_{15} &= \{(2\alpha + 3 : 3\alpha + 3 : 1), (3\alpha : 2\alpha + 1 : 1)\}
\end{aligned}$$

Definición 8.10. *Sea C una curva definida sobre $\mathbb{F}_q$. Un* divisor *D de en C sobre $\mathbb{F}_q$ es un elemento del grupo abeliano libre en el conjunto de puntos de C (de distintos grados) sobre $\mathbb{F}_q$. Así cada divisor es de la forma $D = \sum n_Q Q$ (número finito de sumandos) donde los n_Q son enteros y cada Q es un punto de C. Si $n_Q \geq 0$ para todo Q, diremos que D es un divisor* efectivo *y anotaremos $D \geq 0$.*

Definimos además el grado *de un divisor* $\deg(Q) = \sum n_Q \deg Q$ *y el* soporte *de D como el conjunto* $\mathrm{supp}(D)$ *de puntos Q tales que $n_Q \neq 0$.*

Un caso particular de la definición precedente lo tenemos si consideramos la intersección de dos curvas C y C' de grados d y e respectivamente. Podemos escribir su intersección como un *divisor de intersección* $C \cap C' = P_1 + \ldots P_l$ (con multiplicidades). Este divisor es claramente efectivo y tiene grado *de*.

8.1. Cuerpo de funciones racionales.

Definición 8.11 (Cuerpo de funciones racionales)**.** *Consideremos una curva proyectiva no-singular C definida por el polinomio homogéneo $F(X,Y,Z)$ sobre el cuerpo $\mathbb{F}_q$. El* cuerpo de funciones racionales en C *se define como*

$$\mathbb{F}_q(C) := \left(\left\{ \frac{g(X,Y,Z)}{h(Z,Y,Z)} \middle| \begin{array}{l} g,h \in \mathbb{F}_q[X,Y,Z] \text{son pol. hom.} \\ \text{del mismo grado y } g,h \notin \langle F \rangle \end{array} \right\} \cup \{0\} \right) / \sim$$

donde $g/h \sim g'/h'$ si y sólo si $gh' - g'h \in \langle F \rangle$.

Ejercicio 8.4. Demuestre que efectivamente $\mathbb{F}_q(C)$ es un cuerpo y que contiene $\mathbb{F}_q$ como subcuerpo.

Definición 8.12 (Divisor de una función racional)**.** *Dada una función racional $f = \frac{g}{h}$ definida en una curva C, definimos su divisor:*

$$div(f) := \sum P - \sum Q$$

donde $\sum P$ es el divisor de intersección $C \cap C_g$ y $\sum Q$ es el divisor de intersección $C \cap C_h$. Podemos entonces pensar $div(f)$ como ceros - polos de f en la curva C.

Esta definición requiere una demostración de que no depende del representante de la función f que se elija. La demostración es engorrosa y no la incluiremos en estas notas.

Definición 8.13 (Espacio de funciones racionales asociado a un divisor)**.** *Dado un divisor D en una curva C, le asociamos un espacio de funciones racionales:*

$$L(D) := \{f \in \mathbb{F}_q(C) | div(f) + D \geq 0\} \cup \{0\}$$

Vale la pena hacer notar que $L(D)$ es un espacio vectorial (fácil) de dimensión finita (más difícil). En muchos casos, su dimensión se puede calcular usando el teorema de Riemann-Roch que enunciamos a continuación.

Teorema 8.14 (Riemann-Roch)**.** *Sea C una curva proyectiva no-singular de género g definida sobre el cuerpo $\mathbb{F}_q$ y sea D un divisor en C. Entonces dim $L(D) \geq \deg D + 1 - g$. Más aún, si* $\deg D > 2g - 2$*, entonces*

$$\dim L(D) = \deg D + 1 - g$$

La demostración de este teorema está por lejos fuera del alcance de estas notas y se puede encontrar en algún libro de geometría algebraica.

9. Códigos sobre curvas algebraicas

Volveremos a usar la definición de códigos RS dada en la sección 5.2 para motivar la generalización de estos a curvas algebraicas. El espacio L_{k-1} de polinomios de grado menor a k tiene dimensión k y definimos:

$$RS(k,q) := \{(f(\alpha_1), \ldots, f(a_{q-1}))|f \in L_{k-1}\}.$$

Veremos ahora como interpretar esto con los valores de funciones en puntos de una curva proyectiva. Para ello recordemos la definición del plano proyectivo (ver 8.2)

$$\mathbb{P}^2(k) := (k^3 \setminus (0,0,0))/\sim$$

De forma análoga podemos definir la recta proyectiva

$$\mathbb{P}^1(k) := (k^2 \setminus (0,0))/\sim$$

Podemos pensar $\mathbb{P}^1(k)$ como la curva en $\mathbb{P}^2(k)$ definida por la ecuación $Z = 0$. Resulta ser una curva de género 0.

Ejercicio 9.1. Si denotamos $P_\infty = (1:0)$, y definimos el divisor $D = (k-1)P_\infty$, podemos demostrar que $L(D) = L_{k-1}$. En esta igualdad hemos identificado cada polinomio $f(x)$ de grado d con su homogenización $Y^d f(X/Y)$.

Si definimos los puntos $P_i = (\alpha_i : 1)$, tenemos la siguiente definición alternativa de un código de Reed-Solomon:

$$RS(k,q) := \{(f(P_1), \ldots, f(P_{q-1}))|f \in L((k-1)P_\infty)\}.$$

La idea de Goppa fue de generalizar esta construcción, reemplazando la recta proyectiva por una curva. Sea X una curva proyectiva plana no singular y sea D un divisor en X. Sea $\mathcal{P} = \{P_1, \ldots, P_n\} \subset X(\mathbb{F}_q)$ un conjunto de n puntos $\mathbb{F}_q$-racionales en X y supongamos que $\mathcal{P} \cap \text{supp}(D) =$ de manera que los puntos P_i no sean polos de funciones $f \in L(D)$.

Definición 9.1. *Sean X, $\mathcal{P}$ y D como arriba. Definimos el código geométrico-algebraico asociado:*

$$C(X, \mathcal{P}, D) := \{(f(P_1), \ldots, f(P_n))|f \in L(D)\} \subseteq \mathbb{F}_q^n$$

es decir, es la imagen de la función de evaluación

$$\begin{aligned} \epsilon : L(D) &\to \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

Podemos observar que el código que hemos obtenido es un código lineal (imagen por una transformación lineal de un espacio vectorial). El largo del código es n y su dimensión es $\dim(L(D)) - \dim(\ker(\epsilon))$.

Veamos que *epsilon* es inyectiva y que por lo tanto la dimensión del código es $\dim(L(D))$. Si $\epsilon(f) = 0$ esto quiere decir $f(P_i) = 0$ para $i = 1, \ldots n$ de manera que el

coeficiente de cada P_i en el divisor de f es al menos 1. Como los P_i no están en D, esto quiere decir que $\operatorname{div}(f)+D-P_1-\ldots P_n \geq 0$. En particular $f \in L(D-P_1-\cdots-P_n)$. Si añadimos la hipótesis que el grado de D sea menor a n, tenemos $L(D-P_1-\cdots-P_n) = \{0\}$ y $f=0$.

Teorema 9.2. *Sea X una curva proyectiva plana, no-singular de género g definida sobre $\mathbb{F}_q$. Sea $\mathcal{P} \subset X(\mathbb{F}_q)$ un conjunto de n puntos $\mathbb{F}_q$-racionales de X y sea D un divisor en X cuyo soporte no intersecta $\mathcal{P}$ y que satisface $2g-2 < \deg D < n$. Entonces el código $C = C(X, \mathcal{P}, D)$ es un código lineal de largo n, dimensión $k := \deg D + 1 - g$ y distancia mínima $d \geq n - \deg D$.*

Demostración. El valor de k se desprende directamente del teorema de Riemann-Roch. Para encontrar la cota inferior para la distancia mínima procederemos de manera similar a como demostramos la inyectividad de ϵ. Supongamos que $\epsilon(f) = (f(P_1, \ldots, P_n)$ es una palabra de peso d. En particular exactamente d de sus coordenadas son diferentes de 0. Sin pérdida de generalidad podemos suponer que son las primeras d coordenadas, de manera que

$$f(P_{d+1}) = f(P_{d+2}) = \cdots = f(P_n) = 0$$

Como antes, esto quiere decir que

$$\operatorname{div}(f) + D - P_{d+1} - P_{d+2} - \cdots - P_n \geq 0$$

Esto demuestra que el divisor $D - P_{d+1} - P_{d+2} - \cdots - P_n$ tiene grado no negativo, por lo que $\deg D - (n-d) \geq 0$. □

9.1. Parámetros asintóticos de códigos algebraico-geométricos. Consideremos el código $C = C(X, \mathcal{P}, D)$, donde X es una curva de género g definida sobre $\mathbb{F}_q$, $\mathcal{P}$ es un conjunto de n puntos $\mathbb{F}_q$-racionales de X y D es un divisor en X cuyo soporte no intersecta $\mathcal{P}$ y que satisface $2g-2 < \deg D < n$. Por el teorema 9.2 sabemos que C es un código lineal de largo n, de dimensión $k = \deg D + 1 - g$ y distancia mínima $d \geq n - \deg D$.

Podemos calcular entonces la tasa de transmisión de C y estimar su distancia mínima relativa:

$$\begin{aligned} R &= \frac{k}{n} = \frac{\deg D + 1 - g}{n} \\ \delta &= \frac{d}{n} \geq \frac{n - \deg D}{n} \end{aligned}$$

Como queremos R y δ lo más grandes posible, trataremos de maximizar su suma.

$$R + \delta \geq \frac{\deg D + 1 - g}{n} + \frac{n - \deg D}{n} = \frac{n + 1 - g}{n} = 1 + \frac{1}{n} - \frac{g}{n}$$

Considerando códigos cada vez más largos, lograremos buenos parámetros en la medida que podamos tener $\frac{g}{n}$ lo más pequeño posible. Buscamos entonces curvas de género pequeño con muchos puntos $\mathbb{F}_q$-racionales.

Definición 9.3. *Sea q una potencia de primo y g un entero no negativo. Definimos*

$$N_q(g) := \text{máx}\{\#X(\mathbb{F}_q) | X \text{ es una curva de género } g \text{ sobre } \mathbb{F}_q\}$$

y

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}$$

Ejercicio 9.2. Para entender la relevancia de conocer $A(q)$, considere una sucesión de curvas X_i sobre $\mathbb{F}_q$ que tengan género g_i y que satisfagan

$$\lim_{i\to\infty} \frac{N_i}{g_i} = A(q)$$

Usando estas curvas, defina códigos que tengan tasas de transmisión R_i y distancias mínimas relativas δ_i que satisfagan

$$R_i + \delta_i \geq 1 + \frac{1}{N_i - 1} - \frac{g_i}{N_i - 1}$$

Considere $R = \lim R_i$ y $\delta = \lim \delta_i$ y deduzca una cota inferior para $\alpha_q(\delta)$

9.2. Cotas para el número de puntos de una curva. Para curvas planas, como las que hemos considerado, el número de puntos está claramente acotado superiormente por el número de puntos del plano proyectivo, es decir

$$X(\mathbb{F}_q) \leq q^2 + q + 1$$

Si nos liberamos de esta restricción, considerando curva proyectivas arbitrarias, tenemos un resultado fundamental en el área que determina una cota para el número de puntos de la curva.

Teorema 9.4 (Hasse-Weil)**.** *Sea X una curva proyectiva no-singular de género g sobre $\mathbb{F}_q$ y $N = \#X(\mathbb{F}_q)$. Entonces*

$$|N - (q+1)| \leq 2g\sqrt{q}$$

Una curva que alcanza esta cota se llama maximal. Lamentablemente no siempre existen curvas que alcancen la cota y de hecho se puede demostrar que no existen cuando $g > (q - \sqrt{q})/2$.

Volviendo a la pregunta sobre el valor de $A(q)$, tenemos la siguiente cota superior.

Teorema 9.5 (Drinfeld-Vladut[16])**.** *Para toda potencia de primo q, tenemos*

$$A(q) \leq \sqrt{q} - 1$$

Por otro lado, el siguiente resultado de Tsfasman-Vladut-Zink para $m = 1, 2$ y de Ihara en general, nos permite calcular $A(q)$ cuando q es un cuadrado perfecto.

Teorema 9.6 ([13, 6])**.** *Sea q una potencia par de un primo. Entonces existe una sucesión de curvas X_i definidas sobre $\mathbb{F}_q$ de género g_i y con N_i puntos racionales, tales que*

$$\lim_{i\to\infty} \frac{N_i}{g_i} = \sqrt{q} - 1.$$

Teorema 9.7 (Cota de Tsfasman, Vladut y Zink [13]). *Sea q un cuadrado perfecto. Entonces*

$$\alpha_q(\delta) \geq -\delta + 1 - \frac{1}{\sqrt{q} - 1}$$

Apéndice A. Cuerpos Finitos

Este apéndice pretende revisar algunos conceptos básicos sobre cuerpos finitos. Un buen libro para aprender sobre cuerpos finitos y su relación con códigos es "Coding theory: a First Course" ([8]) Recordemos que un cuerpo es una estructura algebraica que consta de un conjunto y dos operaciones binarias (suma y producto) que satisfacen ciertos axiomas (asociatividad y conmutatividad de la suma y del producto, existencia de 0 y de opuesto aditivo para cada elemento del cuerpo, existencia de 1 y de inverso multiplicativo para cada elemento distinto de cero en el cuerpo, distributividad). Los primeros ejemplos de cuerpo que uno suele conocer son los números racionales, los reales y los complejos.

Todos estos tienen una propiedad adicional que no es consecuencia de los axiomas y es que la suma de un número arbitrario de unos nunca es cero (Salvo que sumemos cero unos). Se dice que estos cuerpos tienen característica 0. Si por el contrario existe una suma de unos que resulte 0 diremos que el cuerpo tiene característica positiva. El menor número positivo de unos que sumados da cero se llama la característica del cuerpo.

A.1. Ejemplos básicos. La siguiente clase de ejemplos se basa en la aritmética modular (de reloj). Si consideramos los enteros módulo n, estos forman un cuerpo cada vez que n es un número primo. Para cada p primo, el conjunto $\mathbb{Z}/p\mathbb{Z}$ que frecuentemente se escribe simplemente como $\mathbb{Z}_p$ forma un cuerpo que contiene exactamente p elementos. Las operaciones en estos cuerpos se definen de forma relativamente sencilla pues se derivan de las respectivas operaciones para números enteros aplicadas a las clases de equivalencia módulo p. Consideremos los casos más pequeños como ejemplos para clarificar esto.

Ejemplo A.1 (p=2)**.** $\mathbb{Z}_2$ tiene dos elementos, la clase de los enteros pares (clase del 0) y la de los enteros impares (clase del 1) a las que por simplicidad denotaremos por $\bar{0}$ y $\bar{1}$ o simplemente por 0 y 1 cuando es claro el contexto. Observemos que la suma de números pares es par, la suma de un impar más un par es impar y que la suma de dos impares es par. Resumimos esto diciendo que $\bar{0}+\bar{0}=\bar{0}$, $\bar{1}+\bar{0}=\bar{1}$, $\bar{0}+\bar{1}=\bar{1}$, $\bar{1}+\bar{1}=\bar{0}$. De manera análoga, obtenemos para el producto $\bar{0}\cdot\bar{0}=\bar{0}$, $\bar{1}\cdot\bar{0}=\bar{0}$, $\bar{0}\cdot\bar{1}=\bar{0}$, $\bar{1}\cdot\bar{1}=\bar{1}$.

El conjunto $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$ con estas operacioes, forma un cuerpo. Dejamos como ejercicio verificar de forma directa que satisface todos los axiomas.

Ejemplo A.2 (p=3)**.** El segundo cuerpo finito es $\mathbb{Z}_3=\{\bar{0},\bar{1},\bar{2}\}$ con operaciones definidas en las siguientes tablas:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Ejemplo A.3 ($\mathbb{Z}_4$)**.** Si proseguimos de forma análoga con la esperanza de obtener un cuerpo con cuatro elementos, nos topamos con problemas. $\mathbb{Z}_4$ dotado con las operaciones de suma y producto de clases no es un cuerpo. Por ejemplo la clase $\bar{2}$ no tiene inverso multiplicativo.

Si bien el ejemplo anterior no dio resultado, sí existe un cuerpo con 4 elementos y en general se demuestra en un curso de álgebra que existe un cuerpo con q elementos si y sólo si $q = p^n$ para algún primo p y algún entero positivo n. El caso particular $q = 4$ lo podemos mostrar indicando sus tablas de suma y producto.

Ejemplo A.4 ($\mathbb{F}_4$)**.** El cuerpo finito es $\mathbb{F}_4 = \{0, 1, i, i+1\}$ con operaciones definidas en las siguientes tablas:

$+$	0	1	i	$i+1$
0	0	1	i	$i+1$
1	1	0	$i+1$	i
i	i	$i+1$	0	1
$i+1$	$i+1$	i	1	0

$\cdot$	0	1	i	$i+1$
0	0	0	0	0
1	0	1	i	$i+1$
i	0	i	$i+1$	1
$i+1$	0	$i+1$	1	i

Ejercicio A.1. $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo si y sólo si p es primo.

Ejercicio A.2. Si la característica de un cuerpo no es 0, entonces es p para algún primo p.

Ejercicio A.3. Si $\mathbb{F}_p$ es un cuerpo y $f(x) \in \mathbb{F}_p[x]$ es un polinomio irreducible de grado d, entonces $\mathbb{F}_p[x]/(f(x))$ es un cuerpo con p^d elementos.

Ejercicio A.4. Existe un único cuerpo con q elementos si y sólo si $q = p^n$ para algún primo p y algún entero positivo n. Este cuerpo se denota por $\mathbb{F}_q$. NOTA: Este ejercicio requiere teoría de Galois.

Ejercicio A.5. Encontrar un polinomio irreducible $r(x)$ de grado 2 sobre $\mathbb{F}_p$ ($p = 2, 3, 5$) y usarlo para escribir las tablas de multiplicación de

$$\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(r(x))$$

Ejercicio A.6. Verificar explícitamente en los cuerpos del ejercicio anterior que el grupo multiplicativo es cíclico. Este es un hecho general sobre todos los cuerpos finitos, que se demuestra en un curso de teoría de Galois.

Ejercicio A.7. Si $\mathbb{F}$ es un cuerpo, entonces $\mathbb{F}[x]$ es un dominio de ideales principales. Ayuda: Usar algoritmo de Euclides.

Ejercicio A.8. Si $\mathbb{F}$ es un cuerpo, entonces $\mathbb{F}[x]/(x^n - 1)$ es un dominio de ideales principales y cada ideal es generado por un divisor de $(x^n - 1)$.

A.2. Operatoria en $\mathbb{F}_q$. Si $q = p^n$ con p un número primo, queremos representar los elementos de $\mathbb{F}_q$ de manera que podamos operar con ellos. Quizás la forma más natural de hacerlo es encontrando un polinomio irreducible $f(x) \in \mathbb{F}_p[x]$ de grado n. Una vez que conocemos f, tenemos

$$\mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_q$$

y podemos considerar $\alpha \in \mathbb{F}_q$, la imágen de $x + (f(x))$ de manera que

$$\mathbb{F}_q = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} | a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p\}$$

La adición resulta fácil de realizar con esta notación, en cambio para multiplicar hay que trabajar más duro, pues debemos reducir las potencias de α mayores que $n-1$ usando la identidad $f(\alpha) = 0$.

Otra forma de representar los elementos de $\mathbb{F}_q$ es aprovechando que sabemos que $\mathbb{F}_q^\times$ es un grupo cíclico. Si elegimos α como un elemento primitivo de $\mathbb{F}_q$, entonces todos los elementos del cuerpo, salvo 0, se pueden escribir como potencias de α. Usando el exponente para representar a cada elemento(∞ para 0), la multiplicación ahora resulta trivial. Ahora en cambio la suma requiere más trabajo. Podemos observar que basta con saber sumar 1 pues $\alpha^n + \alpha^m = \alpha^m(\alpha^{n-m} + 1)$. Para ello podemos construir una tabla de logaritmos discretos $z(k)$ conocidos como logaritmos de Zech que cumplen que $\alpha^k + 1 = \alpha^{z(k)}$.

A.3. Polinomios en $\mathbb{F}_q[x]$.

Definición A.1. *Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F_q[x]$ definimos su derivada como $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F_q[x]$. No es difícil verificar que con esta definición, la derivada satisface una regla del producto como la conocida de cálculo.*

Teorema A.2. *Un polinomio $f(x) \in \mathbb{F}_q[x]$ tiene a $b \in \mathbb{F}_q$ como raiz múltiple si y sólo si b es raiz tanto de $f(x)$ como de $f'(x)$.*

Lema A.3. *Sea $f(x) \in F_q[x]$ un polinomio irreducible de grado m. Entonces $f(x)$ divide a $g(x) = x^{q^n} - x$ si y sólo si m divide a n.*

Demostración. Si $f(x)$ divide a $g(x)$, sea α una raiz de f su cuerpo de descomposición. Como f divide a g, tenemos que $\alpha^{q^n} - \alpha = 0$, de manera que $\alpha \in \mathbb{F}_{q^n}$. Se sigue que $\mathbb{F}_q[\alpha]$ es un subcuerpo de $\mathbb{F}_{q^n}$. Como $|\,\mathbb{F}_q[\alpha] : \mathbb{F}_q\,| = m$ y $|\,\mathbb{F}_{q^n} : \mathbb{F}_q\,| = n$ se tiene $m|n$.

Si $m|n$, entonces $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ de manera que $\alpha^{q^n} - \alpha = 0$ y porlo tanto el polinomio minimal de α ($f(x)$) divide a $g(x)$. □

Teorema A.4. *Para cada cuerpo finito $\mathbb{F}_q$ y para cada $n \in \mathbb{N}$, el productos de todos los polinomios mónicos irreducibles cuyo grado divide a n es igual a $x^{q^n} - x$*

Demostración. De acuerdo al lema A.3, los polinomios mónicos irreducibles sobre $\mathbb{F}_q$ que aparecen en la factorización canónica de $g(x) = x^{q^n} - x$ en $\mathbb{F}_q[x]$ son precisamente los que tienen grado divisor de n. Como $g'(x) = -1$, el teorema A.2 implica que $g(x)$ no tiene raíces múltiples en su cuerpo de descomposición de manera que cada

polinomio mónico irreducible sobre $\mathbb{F}_q$ aparece exactamente una vez en la factorización de canónica de $g(x)$ en $\mathbb{F}_q[x]$. □

Corolario A.5. *Si $N_q(d)$ es el número de polinomios mónicos irreducibles en $F_q[x]$ de grado d, entonces:*

$$q^n = \sum_{d|n} dN_q(d) \qquad \text{para todo } n \in \mathbb{N}.$$

Como nos interesa conocer los valores de $N_q(d)$, estudiaremos una herramienta de teoría de números, la fórmula de inversión de Moebius.

Definición A.6. *La función de Moebius está definida en $\mathbb{N}$ como:*

$$\mu(n) = \begin{cases} 1 & si\ n = 1 \\ (-1)^k & si\ n\ es\ el\ producto\ de\ k\ primos\ diferentes \\ 0 & si\ n\ es\ divisible\ por\ el\ cuadrado\ de\ un\ primo \end{cases}$$

Lema A.7. *Para cada $n \in \mathbb{N}$, la función de Moebius satisface:*

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

Teorema A.8 (Fórmula de Inversión de Moebius)**.** *Sean h y H dos funciones de $\mathbb{N}$ a $\mathbb{Z}$. Entonces:*

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

si y sólo si

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

Corolario A.9.

$$nN_q(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}} \qquad \text{para todo } n \in \mathbb{N}$$

Ejemplo A.5. El número de polinomios mónicos irreducibles de grado 20 en $\mathbb{F}_q[x]$ está dado por:

$$\begin{aligned} N_q(20) &= \frac{1}{20}(\mu(1)q^{20} + \mu(2)q^{10}) + \mu(4)q^5 + \mu(5)q^4 + \mu(10)q^2 + \mu(20)q) \\ &= \frac{1}{20}(q^{20} - q^{10} - q^4 + q^2). \end{aligned}$$

Referencias

[1] Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, and Alfred Wassermann and. *Error-Correcting Linear Codes: Classification by Isometry and Applications (Algorithms and Computation in Mathematics)*. 2006.

[2] V. D. Goppa. *Geometry and Codes (Mathematics and its Applications)*. 1988.

[3] Richard W. Hamming. *Coding and Information Theory*. 1986.
[4] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. 2003.
[5] John F. Humphreys and M. Y. Prest. *Numbers, Groups and Codes*. Cambridge University Press, 2 edition.
[6] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.
[7] Torleiv Klove. *Codes for Error Detection (Series on Coding Theory and Cryptology) (Series on Coding Theory and Cryptology)*. 2007.
[8] San Ling and Chaoping Xing. *Coding theory: a first course*. Cambridge University Press, 2004.
[9] Robert H. Morelos-Zaragoza. *The Art of Error Correcting Coding*. 2006.
[10] Oliver Pretzel. *Error-Correcting Codes and Finite Fields (Oxford Applied Mathematics and Computing Science Series)*. 1992.
[11] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojjiro Sakata, and Carlo Traverso. *Gröbner Bases, Coding, and Cryptography*. Springer, 1 edition.
[12] Sarah A. Spence. *Introduction to Algebraic Coding Theory*. se puede descargar libremente en http://www.math.niu.edu/ ∼beachy/courses/523/coding_theory.pdf.
[13] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.
[14] J. v. Lint and G. v. d. Geer. *Introduction to Coding Theory and Algebraic Geometry (Oberwolfach Seminars)*. 1989.
[15] J. H. van Lint. *Introduction to Coding Theory (Graduate Texts in Mathematics)*. 1998.
[16] S. G. Vlăduţ and V. G. Drinfeld. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.
[17] Judy L. Walker. *Codes and Curves*. se puede descargar libremente en http://www.math.unl.edu/ jwalker7/papers/rev.pdf.