UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA (UNED)

MÁSTER EN MATEMÁTICAS AVANZADAS (Especialidad Geometría y Topología)

TRABAJO FIN DE MÁSTER

Sobre Códigos Algebraico-Geométricos Basados en Curvas $C_{a,\,b}$

Autor:
Victoriano Jiménez Magdaleno

Tutor:
Milagros Izquierdo

9/10/2016

Resumen

El objeto de este trabajo es el estudio de las curvas tipo $C_{a,b}$ y sus aplicaciones en la teoría de códigos. Veremos cómo las curvas $C_{a,b}$ se pueden utilizar para construir códigos MDS (*maximum distance separable codes*) y nos centraremos en algunas curvas $C_{a,b}$ que poseen un grupo de automorfismos que puede determinarse.

The objective of this thesis is the study of $C_{a,b}$ curves and their application to coding theory. We will show how $C_{a,b}$ curves can be used to construct MDS codes (maximum distance separable codes) and we will focus on some $C_{a,b}$ curves that have automorphism groups which can be determined.

Palabras clave: Cuerpos de Funciones Algebraicas (CFA), Teorema de Riemann-Roch, Códigos Algebraico-Geométricos (Códigos AG), Ramificación, Superficie de Riemann, Fórmula del Género de Riemann-Hurwitz, Curvas $C_{a,b}$, Espacio de Módulos $\mathcal{M}_g$, Espacios de Hurwitz, Grupo de Automorfismos de Extensiones F/K, Grupo de Automorfismos de Códigos AG.

***Keywords**: Algebraic Function Fields, Riemann-Roch Theorem, Algebraic Geometry Codes (AG codes), Ramification, Riemann Surface, Riemann-Hurwitz Genus Formula, $C_{a,b}$ Curves, Moduli Space $\mathcal{M}_g$, Hurwitz Spaces, Automorphism Group of Field Extensions F/K, Automorphism Group of AG Codes.*

Agradecimientos

Quisiera dar mi más sincero agradecimiento a Milagros Izquierdo por su ayuda para la culminación de este trabajo, y sobre todo por haberme “iluminado” sobre la conexión existente entre diferentes ramas de las Matemáticas que, a primera vista, no parecen tener relación entre sí.

Quiero dar las gracias también a mi mujer Chus por su paciencia y ánimos a lo largo de estos últimos meses.

Tabla de símbolos

$\mathbb{Z}$	Anillo de los números enteros
$\mathbb{Z}[i]$	Conjunto de los enteros de Gauss
$\mathbb{Q}$	Cuerpo de los números racionales
$\mathbb{R}$	Cuerpo de los números reales
$\mathbb{C}$	Cuerpo de los números complejos
$K[X_1, \dots, X_n]$	Anillo de polinomios en n variables con coeficientes en K
$K(X_1, \dots, X_n)$	Cuerpo de funciones racionales con coeficientes en K
I	Ideal
$\|\cdot\|$	Aplicación norma
$U(A)$	Conjunto de unidades de un anillo A
$v()$	Valuación discreta
$\mathcal{O}$	Anillo de valuación discreta
DIP	Dominio de ideales principales
DFU	Dominio de factorización única
L/K	Extensión de cuerpos algebraicos
$[L:K]$	Grado de una extensión de cuerpos algebraicos
$\mathcal{M}(S)$	Conjunto de funciones meromorfas definidas sobre una superficie de Riemann S
$\overline{K}$	Cierre algebraico de un cuerpo K
$charK = p$	Característica de un cuerpo K
$Aut(L/K)$	Grupo de automorfismos del cuerpo L sobre K
$Gal(L/K)$	Grupo de Galois de L/K
$Tr_{L/K}(\alpha)$	Traza del elemento α con respecto a la extensión L/K
$\gamma()$	Aplicación camino en un espacio topológico
$\pi_1(X, a)$	Grupo fundamental del espacio topológico X en a
CFA	Cuerpo de funciones algebraicas
$\mathcal{O}^\times$	Grupo formado por la unidades del anillo de valuación $\mathcal{O}$
P	*Place* de un CFA
$\mathbb{P}_F$	Conjunto de *places* del CFA F
$degP$	Grado de un *place*
$Div(F)$	Grupo de divisores de un CFA F
D	Divisor

$suppD$	Soporte de un divisor
$degD$	Grado de un divisor
$Princ(F)$	Grupo de divisores principales de un CFA F
$\mathcal{L}(A)$	Espacio de Riemann-Roch asociado a un divisor A
$\ell(A)$	Dimension del espacio de Riemann-Roch asociado a un divisor A
g	Género
$i(A)$	Índice de especialidad de un divisor A
α_P	Adele
$\mathcal{A}_F$	Espacio de adeles de un CFA F
ω	Diferencial de Weil
Ω_F	Módulo de diferenciales de Weil
(ω)	Divisor de un diferencial de Weil
$Cl(F)$	Grupo de clases de divisores de un CFA F
ω_P	Componente local de un diferencial de Weil
res_P	Residuo con respecto a un *place* P
$Cotr_{F'/F}$	Cotraza de una extensión F'/F
$\boldsymbol{A}^n$	Espació afín n-dimensional
$\Gamma(V)$	Anillo de coordenadas de una variedad V
$K(V)$	Cuerpo de funciones racionales de una variedad V
$\boldsymbol{P}^n$	Espacio proyectivo n-dimensional
$\bar{V}$	Cierre proyectivo de una variedad V
$Div^0(V)$	Grupo de divisores de grado cero de una variedad V
$Jac(V)$	Jacobiano de una variedad V
$V(K)$	Conjunto de puntos K-racionales de una variedad V
$\mathbb{F}_q$	Cuerpo finito con q elementos
$d(a,b)$	Distancia de Hamming entre dos elementos $a, b \in \mathbb{F}_q^n$
$wt(a)$	Peso de un elemento $a \in \mathbb{F}_q^n$
$d(C)$	Distancia mínima de un código C
$[n,k,d]$	Código de longitud n, dimensión k y distancia mínima d
$\langle a,b \rangle$	Producto interior canónico de $a, b \in \mathbb{F}_q^n$

$C^{\perp}$	Código dual de C
MDS	*Maximum distance separable codes*
$C_{\mathcal{L}}(D,G)$	Código algebraico-geométrico (código AG) asociado a los divisores D, G
d^*	Distancia de diseño de um código AG
$C_{\Omega}(D,G)$	Código AG dual de $C_{\mathcal{L}}(D,G)$
$\mathcal{S}_n$	Grupo simétrico
$Aut(C)$	Grupo de automorfismos de un código C
S	Superficie de Riemann
$ord_p f$	Orden de la función meromorfa f en el punto p
$ord_P \omega$	Orden de la diferencial meromorfa ω en el punto p
$\mathcal{K}$	Clase canónica definida por las diferenciales meromorfas
$\mathcal{R}$	Divisor de ramificación de un morfismo entre superficies de Riemann
Δ	Discriminante de una curva
$C_{a,b}$	Curva de tipo a, b
$\mathcal{M}_g$	Espacio de módulos de género g
$\mathcal{H}_{\sigma}$	Espacio de Hurwitz
$\mathcal{H}_{\sigma}^{s}$	Espacio de Hurwitz simetrizado

ÍNDICE

1 INTRODUCCIÓN

El objeto de este trabajo es el estudio de las curvas tipo $C_{a,b}$ y sus aplicaciones en la teoría de códigos. Veremos cómo las curvas $C_{a,b}$ se pueden utilizar para construir códigos MDS (*maximum distance separable codes*) y nos centraremos en algunas curvas $C_{a,b}$ que poseen un grupo de automorfismos que puede determinarse.

Para ello, deberemos establecer los principios que nos permitan comprender las propiedades más características de este tipo de curvas. Nuestro estudio se basa en una doble aproximación algebraica-geométrica basada en las teorías de cuerpos de funciones algebraicas y de las superficies de Riemann.

Los cuerpos de funciones algebraicas (CFA) son un tipo de extensiones de cuerpos que surgen de forma natural en varias ramas de las matemáticas, como la geometría algebraica, la teoría de números y la teoría de las superficies de Riemann compactas; por lo que es posible el estudio de los cuerpos de funciones algebraicas desde diferentes enfoques:

En la geometría algebraica estamos interesados en las propiedades geométricas de una curva algebraica $X = \{(\alpha, \beta) \in K \times K | \, f(\alpha, \beta) = 0\}$, donde $f(X, Y)$ es un polinomio irreducible es dos variables sobre un cuerpo cerrado K. Resulta que el cuerpo $K(X)$ de funciones racionales en X (que es un cuerpo de funciones algebraicas sobre K) y el anillo de coordenadas $\Gamma(X)$ contienen toda la información relativa a la geometría de la curva.

Otra aproximación a los cuerpos de funciones viene desde el análisis complejo. El cuerpo de las funciones meromorfas definidas sobre una superficie de Riemann compacta S constituye un cuerpo de funciones algebraicas $\mathcal{M}(S)$ sobre $\mathbb{C}$, es decir el cuerpo de funciones algebraicas de la curva compleja. De nuevo aquí el cuerpo de funciones es una potente herramienta para estudiar las superficies de Riemann correspondientes.

En el presente trabajo analizaremos la estrecha relación entre ambas aproximaciones, detallando las equivalencias / isomorfismos entre las mismas (curvas algebraicas, superficies de Riemann, funciones meromorfas, funciones racionales, teorema de Riemann-Roch, anillos de coordenadas, *places*, puntos, etc.).

En la primera parte del texto, después de un capítulo 2 de preliminares donde repasamos los fundamentos de la teoría de anillos y cuerpos conmutativos y las extensiones de cuerpos, realizaremos una exposición puramente algebraica de la teoría de cuerpos de funciones algebraicas (capítulo 3). Esta línea de investigación fue iniciada por *R. Dedekind*, *L. Kronecker* y *H. M. Weber* en el siglo XIX sobre el

cuerpo $\mathbb{C}$. Posteriormente fue desarrollada por *E. Artin*, *H. Hasse*, *F. K. Schmidt* y *A. Weil* en la primera mitad del siglo XX.

La aproximación algebraica al estudio de los CFA es menos natural y sin embargo más elemental que la puramente geométrica. Para la misma tan solo se requieren conocimientos de la teoría de extensiones de cuerpos. No obstante, en la sección 3.3 presentaremos de forma somera la teoría desde un punto de vista geométrico y analizaremos su relación con el equivalente algebraico. Una ventaja adicional de la aproximación algebraica es que algunos de los principales resultados de la teoría, como el teorema de Riemann-Roch, se pueden derivar de forma más directa al hacer uso de la estructura CFA del cuerpo de funciones racionales o meromorfas. Esto facilita el camino a algunas de las aplicaciones de la teoría de funciones algebraicas, como es el caso de la teoría de códigos, que es uno de los objetivos de este trabajo.

Un código corrector de errores es un subespacio de $\mathbb{F}_q^n$, el espacio vectorial n-dimensional sobre un cuerpo finito $\mathbb{F}_q$. Estos códigos se usan ampliamente para la transmisión de información de forma fiable. La teoría de códigos algebraico-geométricos emergió en los inicios de la década de los ochenta como resultado de la confluencia de varias ramas de las matemáticas: por un lado las respetables y ya plenamente desarrolladas teoría de números y la geometría algebraica; por el otro lado, la teoría de transmisión de la información, desarrollada durante el siglo XX, y su incipiente teoría “hija”, la teoría algebraica de los códigos de corrección de errores. La relación entre ambos dominios, a priori tan distantes entre sí, fue descubierta por *V. D. Goppa*, quien se percató de que se podían asociar códigos con determinados divisores de cuerpos de funciones algebraicas, lo que permitía construir una gran clase de códigos. Los trabajos de *V. D. Goppa*, junto a las aportaciones de *Y. Manin*, *M. Tsfasman*, *S. Vladut* y *T. Zin*k, dieron lugar al nacimiento de un nuevo dominio de las matemáticas, la teoría de los códigos algebraico-geométricos.

Las propiedades de esos códigos están estrechamente relacionadas con las propiedades de cuerpo de funciones correspondiente, y el teorema de Riemann-Roch proporciona estimaciones, de gran exactitud en algunos casos, para las principales propiedades de los códigos (dimensión, mínima distancia, etc.), que presentaremos en el capítulo 4 de este trabajo.

El diseño de nuevos códigos algebraico-geométricos ha sido un campo de gran investigación durante las últimas décadas. En este diseño un hecho de gran importancia es el número de puntos de una curva algebraica sobre un cuerpo finito. Por lo tanto es natural que las curvas algebraicas que se han empleado hasta ahora sean curvas para las que ese número de puntos pueda ser calculado. ¿Existe alguna familia de curvas que sea idónea para construir buenos códigos? Las curvas hermíticas han sido usadas con éxito por varios autores ([19], [10], [22]), en adición

a las curvas hiperelípticas y otras familias de curvas. Sin embargo, las curvas más naturales para este propósito son las curvas superelípticas. Las curvas hiperelípticas y superelípticas han sido estudiadas en detalle y sus propiedades son bien conocidas y constituyen la clase principal de curvas usadas en las teorías de codificación y criptografía. Para su estudio nos hemos fijado en los trabajos de T. Shaska y coautores [2], [4], [7], [15], [13].

Nuestro objetivo es el estudio de un tipo de curvas que pertenece a la familia de las curvas superelípticas, las que denominamos curvas $C_{a,b}$. Las curvas $C_{a,b}$ son curvas algebraicas con propiedades aritméticas muy interesantes. En este trabajo vamos a estudiar cómo estas propiedades (como la existencia de determinados divisores para estas curvas) son de utilidad para la construcción de “buenos” códigos algebraico-geométricos.

Éste será el tema central del capítulo 5, donde comenzaremos (secciones 5.1, 5.2 y 5.3) con un repaso de las teorías de superficies de Riemann, recubridores de una variedad algebraica y ramificación, para llegar a la fórmula de Riemann-Hurwitz, de gran utilidad para calcular el género de una curva. Los conceptos presentados nos servirán de base para explicar las propiedades de las curvas que introducimos a continuación en las secciones 5.4 y 5.5: curvas elípticas, hiperelípticas, superelípticas y admisibles. Pasaremos luego al objeto de nuestro estudio, las curvas $C_{a,b}$ (secciones 5.6 y 5.7), donde expondremos sus propiedades más importantes, así como su grupo de automorfismos para algunos casos en los que puede determinarse. Finalizaremos en la sección 5.8 con un ejemplo de código basado en una curva $C_{a,b}$ de género 3.

2 PRELIMINARES

2.1 FUNDAMENTOS DE LA TEORÍA DE ANILLOS Y CUERPOS CONMUTATIVOS.

En esta sección estudiaremos las propiedades generales de los anillos y cuerpos conmutativos. Estos conceptos nos servirán de base para desarrollos posteriores en el resto de capítulos.

Como ejemplos de anillos conmutativos, que van a ser recurrentes a lo largo de este trabajo, tenemos el conjunto $\mathbb{Z}$ de los números enteros, el conjunto de los enteros de Gauss $\mathbb{Z}[i]$ y el anillo de polinomios en n indeterminadas con coeficientes en un anillo o cuerpo A, y que denotamos por $A[X_1,\ldots, X_n]$. Como ejemplos de cuerpos conmutativos nos encontramos frecuentemente con los conjuntos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ de los números racionales, reales y complejos.

Como texto de referencia para esta sección nos hemos basado en [5].

Sea A un anillo. Se llama divisor de cero a un elemento $x \in A^* = A\backslash\{0_A\}$ tal que $xy = 0_A$ para algún $y \in A^*$. Está claro que los cuerpos no tienen divisores de cero, pero $\mathbb{Z}$ sin ser un cuerpo tampoco los tiene. Luego debemos introducir una clase de anillos más amplia que la de los cuerpos.

Se llama **dominio de integridad** a un anillo unitario y conmutativo sin divisores de cero. Aunque un dominio de integridad no es necesariamente un cuerpo, se le puede asociar de modo natural uno:

Cuerpo de fracciones de un dominio de integridad: sean A un dominio de integridad y $T = A \times A^*$ (producto cartesiano). En T se define una relación de equivalencia:

$$(x, y) \text{ está relacionado con } (x', y') \text{ si } xy' = yx'$$

la clase de equivalencia de (x, y) la denotaremos $[x, y]$. El conjunto cociente de T para esta relación, que denotaremos K, es un anillo con las operaciones:

$$[x, y] + [x', y'] = [xy' + yx', yy'] \quad \text{y} \quad [x, y] \cdot [x', y'] = [xx', yy']$$

Además se cumple que K es un cuerpo cuyo elemento cero es $[0,1]$ y el uno es $[1,1]$.

Este cuerpo K se denomina cuerpo de fracciones de A y sus elementos se representan por x/y en lugar de $[x,y]$.

Ejemplos:

1) El conjunto de matrices cuadradas de orden 2 (con elementos en un anillo A) es un anillo pero no es dominio de integridad, ya que

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad (x \in A)$$

2) El cuerpo de fracciones del anillo de los números enteros $\mathbb{Z}$ es el cuerpo $\mathbb{Q}$ de los números racionales. Para $A = \mathbb{Z}[i]$ obtenemos $K = \mathbb{Q}[i]$, es decir, el cuerpo de fracciones de $\mathbb{Z}[i]$, consistente en los números complejos $a + bi$, donde $a, b \in \mathbb{Q}$.

3) Un anillo de polinomios $A[X_1, \dots, X_n]$ es dominio de integridad si y solo si lo es A.

4) Cuerpos de funciones racionales: sea A dominio de integridad y K su cuerpo de fracciones; podemos suponer $A \subset K$ vía $x \mapsto x/1$. Como A es dominio, $A[X_1, \dots, X_n]$ también lo es y tiene como cuerpo de fracciones F que describiremos a continuación.

   Los elementos de F son fracciones f/g con $f, g \in A[X_1, \dots, X_n]$ y $g \neq 0$.

   En particular, $K \subset F$, pues dados $a, b \in A$, $b \neq 0$, tomando $f = a, g = b$, el elemento a/b está en F. Tenemos pues:

$$A[X_1, \dots, X_n] \subset K[X_1, \dots, X_n] \subset F$$

   y que F es también el cuerpo de fracciones de $K[X_1, \dots, X_n]$ (obsérvese que aunque K es cuerpo, $K[X_1, \dots, X_n]$ no lo es, ya que $X_1 \neq 0$ no es unidad en $K[X_1, \dots, X_n]$).

   En lo sucesivo adoptaremos el siguiente convenio:

Los cuerpos de fracciones de $A[X_1, \dots, X_n]$ y $K[X_1, \dots, X_n]$ se identifican por un isomorfismo y se denotan por

$$K(X_1, \dots, X_n)$$

que se denomina **cuerpo de funciones racionales** con coeficientes en K y en n indeterminadas.

Como ejemplo, para polinomios en una sola variable T, tenemos

$$\mathbb{Z}[T] \subset \mathbb{Q}[T] \subset \mathbb{Q}(T) \quad \text{y} \quad \mathbb{Z}[i][T] \subset \mathbb{Q}[i][T] \subset \mathbb{Q}[i](T)$$

Sea A un anillo unitario conmutativo. Se llama **ideal** a un subconjunto $I \subset A$ tal que:

1) I es un subgrupo de A para la suma (en particular, $0 \in I$).
2) Para cualesquiera $x \in I$, $a \in A$ el producto ax pertenece a I.

Anillos cociente: la importancia de la noción de ideal radica en que es la adecuada para definir relaciones de equivalencia en un anillo de tal manera que el conjunto cociente pueda ser dotado de estructura de anillo.

Sean A un anillo conmutativo e $I \subset A$ un ideal propio. Se define en A la relación de equivalencia:

$$x \text{ está relacionado con } y \text{ si } x - y \in I \quad (x, y \in A)$$

El conjunto cociente de A para esta relación se denota A/I y la clase de equivalencia de un elemento $x \in A$ es:

$$x + I = \{x + a | \, a \in I\}$$

Sea A un anillo unitario conmutativo. Un ideal $I \subset A$ se llama **finitamente generado** si es el ideal generado por un subconjunto finito $L = \{x_1, \dots, x_r\} \subset A$. Se denota por $I = (x_1, \dots, x_r)$. Si $r = 1$, es decir, si el ideal está generado por un solo elemento, entonces I de llama **ideal principal**.

Ejemplos:

1) En un cuerpo K no existen más ideales que $\{0\}$ y K. En efecto, si I es un ideal no trivial de K, si cogemos un elemento $x \in I \backslash \{0\}$, entonces existe $x^{-1} \in K$ (por ser K cuerpo). Como I es ideal $1 = x^{-1}x \in I$, consecuentemente I es el ideal impropio A.

2) En el anillo de $\mathbb{Z}$ de los números enteros todos los ideales son principales: para cada número entero k tenemos el ideal:

$$I_k = (k) = \{pk | \, p \in \mathbb{Z}\}$$

Ahora bien, k y $-k$ generan el mismo ideal, luego podemos tomar siempre $k \geq 0$. Esto proporciona una biyección entre los ideales de $\mathbb{Z}$ y los números enteros no negativos en la que a 0 le corresponde el ideal trivial y a 1 el ideal impropio $\mathbb{Z}$.

Sean A un anillo unitario conmutativo e I un ideal de A. Se dice que I es **maximal** si se verifica una (y por tanto ambas) de las dos condiciones equivalentes siguientes:

1) El anillo cociente A/I es un cuerpo.

2) I es un ideal propio y ningún otro ideal propio lo contiene estrictamente.

Sean A un anillo unitario conmutativo e I un ideal de A. Se dice que I es **primo** si se verifica una (y por tanto ambas) de las dos condiciones equivalentes siguientes:

1) El anillo cociente A/I es un dominio de integridad.

2) I es un ideal propio y para cualesquiera $x, y \in A$, si $xy \in I$, entonces $x \in I$ o $y \in I$.

Ejemplos:

1) Todo ideal maximal es primo, pues todo cuerpo es dominio de integridad.

2) El ideal generado por 6 en el anillo $\mathbb{Z}$ no es primo, pues contiene a $6 = 2 \cdot 3$, pero no contiene ni a 2 ni a 3.

3) La razón del término ideal primo está en que los ideales primos del anillo de los números enteros son precisamente los generados por los números primos.

Se cumple que si I es un ideal primo de un anillo unitario conmutativo A tal que el anillo cociente A/I es finito, entonces I es un ideal maximal.

Si $y \in A^*$ genera un ideal primo, diremos que y es **primo.** Todo elemento primo es irreducible.

Se dice que A es un **dominio euclidiano** (DE) si existe una aplicación, que llamaremos norma

$$\|\cdot\|: A \longrightarrow \mathbb{N}$$

siendo $\mathbb{N}$ el conjunto de los números naturales, tal que:

1) $\|x\| = 0$ si y solo si $x = 0$

2) $\|xy\| = \|x\| \cdot \|y\|$

3) Si $x, y \in A^*$, existe $r \in A$, tal que $y|(x - r)$ y $\|r\| < \|y\|$

Ejemplos:

1) Sea $A = \mathbb{Z}[i]$. En este subanillo de $\mathbb{C}$ definimos $\|\cdot\|$ elevando al cuadrado en módulo de cada elemento de A considerado como número complejo: $\|x\| = a^2 + b^2$, para $x = a + bi \in A$. Se comprueba fácilmente que $\mathbb{Z}[i]$ es un dominio euclidiano.

2) Dado el anillo de polinomios en una variable $A[T]$, definimos la aplicación $\|\cdot\|: A[T] \longrightarrow \mathbb{N}$ tal que $\|f\| = 2^{degf}$, donde $degf$ es el grado del polinomio $f \in A[T]$. Se comprueba que $A[T]$ es un dominio euclidiano sí y solo sí A es un cuerpo.

Sea A un dominio euclidiano. Se cumple: $U(A) = \{x \in A |\ \|x\| = 1\ \}$, donde $U(A)$ es el conjunto formado por las unidades del anillo A.

Ejemplo: vamos a calcular las unidades de $\mathbb{Z}[i]$, determinando los elementos $x = a + bi$ tales que $a^2 + b^2 = 1$. Resultando: $U(\mathbb{Z}[i]) = \{+1, -1, +i, -i\}$

Introducimos ahora el concepto de valuación discreta, al que recurriremos con frecuencia a lo largo del texto.

Una **valuación discreta** de un cuerpo K es una aplicación $v: K \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:

1) $v(x) = \infty \Leftrightarrow x = 0$

2) $v(xy) = v(x) + v(y)\ para\ todo\ x, y\ \in K$

3) $v(x + y) \geq min\{v(x), v(y)\}\ para\ todo\ x, y\ \in K$

El subconjunto de K: $\mathcal{O} = \{0\} \cup \{r \in K |\ v(r) \geq 0\}$ es un anillo, al que llamamos **anillo de valuación discreta** de v.

Se cumple que los anillos de valuación discreta son dominios euclidianos, pues la valuación produce la norma.

Ejemplo: supongamos que $p \in \mathbb{Z}$ es un elemento primo. La aplicación: $v_p: \mathbb{Q}^* \longrightarrow \mathbb{Z}$ tal que $v_p\left({}^{a}/_{b}\right) = ord_p(a) - ord_p(b)$ para todos los enteros a, b no nulos, donde $ord_p(a)$ es el exponente de mayor potencia de p que divide a a. Se comprueba fácilmente que v_p es una valuación discreta.

Tenemos los siguientes resultados sobre lo que denominaremos domino de ideales principales:

En un dominio euclidiano todos los ideales son principales.

Se denomina **dominio de ideales principales** (DIP) a un dominio de integridad en el que todos sus ideales son principales.

Ejemplo:

1) Según la proposición anterior un DE es un DIP. $\mathbb{Z}$ y $\mathbb{Z}[i]$ son DIP.

2) $A[T]$ es un DIP siempre y cuando A sea un cuerpo. En particular, esto significa que $A[X_1, \dots, X_n]$ nunca es DIP para $n \geq 2$, pues

$$A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n]$$

y $A[X_1, \dots, X_{n-1}]$ nunca es cuerpo (ya que X_1 no es unidad).

Supongamos que A es un dominio de ideales principales. Entonces se cumple que todo elemento irreducible $a \in A^*$ genera un ideal maximal.

Hay otra propiedad importante que cumplen los DIP:

Sea A un dominio de ideales principales. Para cada elemento $x \in A^*$ que no es unidad se verifica:

1) Existen elementos irreducibles $a_1, \dots, a_r \in A$ dos a dos primos entre sí y enteros $\alpha_1, \dots, \alpha_r > 0$ tales que $x = {a_1}^{\alpha_1} \dots {a_r}^{\alpha_r}$. Estos elementos a_i se denominan **factores irreducibles** de x.

2) Los elementos $a_1, \dots, a_r$ son únicos (salvo productos por unidades de A), así como los enteros $\alpha_1, \dots, \alpha_r$.

Un **dominio de factorización única** (DFU) es un dominio de integridad en el que se cumple:

1) (P) todo elemento irreducible es primo.

2) (F) todo elemento no nulo que no sea unidad es producto de elementos irreducibles.

Ejemplos:

1) Los anillos $\mathbb{Z}$ y $\mathbb{Z}[i]$ son DIP, luego son DFU. Para $\mathbb{Z}$ reencontramos el **teorema fundamental de la aritmética**: todo número entero positivo n se escribe de modo único como producto de números primos positivos $p_1, \dots, p_r$ en la forma: $n = {p_1}^{\alpha_1} \dots {p_r}^{\alpha_r}$

2) Se cumple que si A es un dominio de factorización única entonces $A[X_1, \dots, X_n]$ también lo es; luego el anillo $\mathbb{Z}[T]$ es un DFU pero no es un DIP (por no ser $\mathbb{Z}$ un cuerpo). Así, en general $DFU \not\Rightarrow DIP$.

2.2 EXTENSIONES DE CUERPOS

A continuación vamos a recordar algunos conceptos de la teoría de extensiones cuerpos algebraicos, a los que recurriremos frecuentemente a lo largo de este trabajo.

Como texto de referencia para esta sección nos hemos basado en [20].

Sea L un cuerpo que contiene a K como subcuerpo. Se denomina a L/K **extensión de cuerpos**. Si consideramos a L como espacio vectorial sobre K, su dimensión se llama grado de L/K y se denota como $[L:K]$.

Se dice que L/K es una **extensión finita** si $[L:K] = n < \infty$. Entonces existe una base $\{\alpha_1, \dots, \alpha_n\}$ de L/K; i.e., todo $\gamma \in L$ tiene una representación única

$$\gamma = \sum_{i=1}^{n} c_i \alpha_i$$

con $c_i \in K$. Si L/K y M/L son extensiones finitas, entonces M/K es también finita con grado $[M:K] = [M:L] \cdot [L:K]$.

Ejemplos

1) Dado un cuerpo K, habíamos definido anteriormente el cuerpo de funciones racionales con coeficientes en K y en 1 indeterminada $K(X)$. Este cuerpo es una extensión algebraica de K, $K(X)/K$.

2) Dada una superficie de Riemann S (*ver sección 5.1*), el conjunto de todas las funciones meromorfas definidas en S es un cuerpo que se denomina $\mathcal{M}(S)$, que es una extensión algebraica del cuerpo de los números complejos $\mathbb{C}$, si identificamos cada número complejo con la correspondiente función constante definida en $\mathcal{M}(S)$.

Un elemento $\alpha \in L$ es **algebraico** sobre K si existe un polinomio no nulo $f(X) \in K[X]$ (anillo de polinomios sobre K) tal que $f(\alpha) = 0$. De entre todos estos polinomios hay uno único, que es mónico (su coeficiente principal es 1) y de grado mínimo; dicho polinomio se denomina **polinomio mínimo** de α sobre K.

La extensión de cuerpos L/K se denomina **extensión algebraica** si todos los elementos $\alpha \in L$ son algebraicos sobre K, en cualquier otro caso se dice que L/K es una **extensión transcendental**.

Sean $\gamma_1, \dots, \gamma_r \in L$. El subcuerpo más pequeño de L que contiene a K y a todos los elementos $\gamma_1, \dots, \gamma_r$ se denota por $K(\gamma_1, \dots, \gamma_r)$. La extensión $K(\gamma_1, \dots, \gamma_r)/K$ es finita si y solo si todos los γ_i son algebraicos sobre K.

En particular, $\alpha \in L$ es algebraico sobre K si y solo si $[K(\alpha):K] < \infty$. Sea $p(X) \in K[X]$ el polinomio mínimo de α sobre K y $r = deg\, p(X)$. Entonces $[K(\alpha):K] = r$, y los elementos $1, \alpha, \alpha^2, \dots, \alpha^{r-1}$ constituyen una base de $K(\alpha)/K$.

Ejemplos:

1) $\mathbb{C} = \mathbb{R}(i)$, el cuerpo de los números complejos es una extensión del cuerpo de los números reales. El número imaginario $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$ pues es la raíz del polinomio $X^2 + 1 \in \mathbb{R}[X]$. Como i es algebraico, la extensión $\mathbb{C}/\mathbb{R}$ es finita y $[\mathbb{R}(i):\mathbb{R}] = 2$ (pues el polinomio mínimo es de grado 2). El conjunto $\{1, i\}$ constituye una base de $\mathbb{C}/\mathbb{R}$.

2) A su vez, el cuerpo $\mathbb{R}$ de los números reales es una extensión del cuerpo $\mathbb{Q}$ de los números racionales, luego $\mathbb{R}/\mathbb{Q}$ es una extensión de cuerpos.

   En $\mathbb{R}/\mathbb{Q}$, el elemento $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, pues es la raíz del polinomio $X^4 - 10X + 1 \in \mathbb{Q}[X]$.

   En $\mathbb{R}/\mathbb{Q}$, el número transcendente $e \in \mathbb{R}$ no es algebraico sobre $\mathbb{Q}$, porque no existe polinomio con coeficientes racionales que tenga a e como raíz. En $\mathbb{C}/\mathbb{R}$ e es algebraico, pues es la raíz del polinomio $X - e \in \mathbb{R}[X]$.

   Luego la extensión $\mathbb{R}/\mathbb{Q}$ es transcendental e infinita, se cumple que $[\mathbb{R}:\mathbb{Q}]$ es igual a la cardinalidad del continuo.

3) Se comprueba de forma sencilla que $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es una extensión algebraica.

Consideremos las extensiones de cuerpos L_1/K y L_2/K. Un homomorfismo $\sigma: L_1 \longrightarrow L_2$ se denomina embebemiento de L_1 sobre L_2 si $\sigma(a) = a$ para todo $a \in K$. Se observa que σ es inyectivo y genera un isomorfismo de L_1 en el subcuerpo $\sigma(L_1) \subseteq L_2$. Un embebemiento sobreyectivo (luego biyectivo) de L_1 en L_2 sobre K es un K-isomorfismo.

Dado un cuerpo K y un polinomio no constante $f(X) \in K[X]$, entonces existe una extensión de cuerpos algebraica $L = K(\alpha)$ con $f(\alpha) = 0$. Si $f(X)$ es irreducible, esta extensión de cuerpos es única hasta K-isomorfismos. Esto significa que si $L' = K'(\alpha)$ es otra extensión de cuerpos con $f(\alpha') = 0$ entonces existe un K-isomorfismo $\sigma: L \longrightarrow L'$ con $\sigma(\alpha) = \alpha'$. Decimos que $L = K(\alpha)$ se ha obtenido añadiendo una raíz de $f(X)$ a K.

Si $f_1(X), \ldots, f_r(X) \in K[X]$ son polinomios mónicos de grado $d \geq 1$, existe una extensión de cuerpos $Z \supseteq K$ tal que todos los $f_i(X)$ se descomponen en factores lineales $f_i(X) = \prod_{j=1}^{d_i}(X - \alpha_{ij})$ con $\alpha_{ij} \in Z$, y $Z = K(\{\alpha_{ij} | \ 1 \leq i \leq r \ y \ 1 \leq j \leq d_i\})$. El cuerpo Z es único hasta K-isomorfismos y se denomina el **cuerpo descomposición** de $f_1, \ldots, f_r$ sobre K.

Se dice que un cuerpo M es **algebraicamente cerrado** si todo polinomio $f(X) \in M[X]$ de grado ≥ 1 tiene una raíz en M.

Para todo cuerpo K existe una extensión algebraica $\overline{K}/K$ con un cuerpo algebraicamente cerrado $\overline{K}$. El cuerpo $\overline{K}$ es único hasta K-isomorfismos; se denomina el **cierre algebraico** de K.

Ejemplo: $\mathbb{C}$ es el cierre algebraico de $\mathbb{R}$ ya que todas las raíces de polinomios con coeficientes en $\mathbb{R}$ están en $\mathbb{C}$.

Sea K un cuerpo y $1 \in K$ el elemento neutro con respecto a la multiplicación. Para cada entero $m > 0$, sea $\overline{m} = 1 + 1 + \ldots + 1 \in K$ (m sumandos). Si $\overline{m} \neq 0$ (el elemento cero de K) para todo $m > 0$, decimos que K tiene **característica** cero. En caso contrario, existe un número primo único $p \in \mathbb{N}$ tal que $\bar{p} = 0$, se dice entonces que K tiene característica p. En adelante utilizaremos la abreviatura $charK$. Es conveniente identificar un entero $m \in \mathbb{Z}$ con el elemento $\overline{m} \in K$; i.e., simplemente escribimos $m = \overline{m} \in K$.

Si $charK = 0$, entonces K contiene al cuerpo $\mathbb{Q}$ de los números racionales (hasta isomorfismos). En el caso en que $charK = p > 0$, K contiene al cuerpo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

En un cuerpo de característica $p > 0$ se cumple que $(a + b)^q = a^q + b^q$ para todo $a, b \in K \ y \ q = p^j, j \geq 0$.

Sea $f(X) \in K[X]$ un polinomio mónico de grado $d \geq 1$. Sobre alguna extensión de cuerpos $L \supseteq K$, $f(X)$ se descompone en factores lineales $f(X) = \prod_{i=1}^{d}(X - \alpha_i)$. Se

dice que el polinomio $f(X)$ es **separable** si $\alpha_i \neq \alpha_j$ para todo $i \neq j$; en caso contrario, f es polinomio **inseparable**.

Si $charK = 0$, todos los polinomios irreducibles son separables. En el caso en que $charK = p > 0$, un polinomio irreducible $f(X) = \sum a_i X^i \in K[X]$ es separable si y solo si $a_i \neq 0$ para algún $i \not\equiv 0 mod p$.

La derivada de $f(X) = \sum a_i X^i \in K[X]$ se define de la manera usual como $f'(X) = \sum i a_i X^{i-1}$. Un polinomio irreducible $f(X) \in K[X]$ es separable si y solo si $f'(X) \neq 0$.

Sea L/K una extensión de grupos algebraicos. Un **elemento** $\alpha \in L$ se denomina **separable** sobre K si su polinomio mínimo $f(X) \in K[X]$ es un polinomio separable. L/K es una **extensión separable** si todo $\alpha \in L$ es separable sobre K. Si $charK = 0$, entonces todas las extensiones algebraicas L/K son separables.

Un elemento $x \in F$ se denomina **elemento separante** de F/K si $F/K(x)$ es una extensión algebraica separable.

Dada un torre $M \supseteq L \supseteq K$ de extensiones de cuerpos algebraicas, la extensión M/K es separable si y solo si lo son M/L y L/K.

Consideremos ahora una extensión algebraica L/K donde $charK = p > 0$. Un elemento $\gamma \in L$ se llama **puramente inseparable** sobre K si $\gamma^{p^r} \in K$ para algún $r \geq 0$. En este caso el polinomio mínimo de γ sobre K tiene la forma $f(X) = X^{p^e} - c$ con $c \in K$ (y $e \leq r$). La **extensión** L/K es **puramente inseparable** si todos los elementos $\gamma \in L$ son puramente inseparables sobre K.

Dada una extensión algebraica arbitraria L/K, se cumple que existe un único cuerpo intermedio $S, K \subseteq S \subseteq L$, tal que S/K es separable y L/S puramente inseparable.

Un cuerpo K se denomina **perfecto** si todas las extensiones algebraicas L/K son separables. Cuerpos de característica cero son perfectos siempre. Un cuerpo K de característica $p > 0$ es perfecto si y solo si todo $\alpha \in K$ puede escribirse como $\alpha = \beta^p$, para algún $\beta \in K$. Todos los cuerpos finitos son perfectos.

Una **extensión algebraica** L/K es **simple** si $L = K(\alpha)$ para algún $\alpha \in L$. El elemento α se denomina **elemento primitivo** de L/K. Toda extensión de cuerpos algebraica finita y separable es simple.

Ejemplo: vimos anteriormente que $\mathbb{C} = \mathbb{R}(i)$. Luego $\mathbb{C}/\mathbb{R}$ es una extensión simple.

Supongamos que $L = K(\alpha_1, \dots, \alpha_r)$ es una extensión finita y separable y $K_0 \subseteq K$ es un subconjunto finito de K. Entonces existe un elemento primitivo α de la forma $\alpha = \sum_{i=1}^{r} c_i\, \alpha_i$ con $c_i \in K_0$.

Para una extensión de cuerpos L/K llamamos al **grupo de automorfismos** de L sobre K como $Aut(L/K)$. Es decir, un elemento $\sigma \in Aut(L/K)$ es un K-isomorfismo de L en L. Si $[L{:}K] < \infty$, el orden de $Aut(L/K)$ es siempre $\leq [L{:}K]$. Se dice que la extensión L/K es de ***Galois*** si el orden de $Aut(L/K)$ es $[L{:}K]$. En este caso llamamos a $Gal(L/K) \coloneqq Aut(L/K)$ el **grupo de *Galois*** de L/K.

Las siguientes condiciones son equivalentes para una extensión de cuerpos L/K de grado finito:

1) L/K es *Galois*

2) L es el cuerpo descomposición de los polinomios separables $f_1(X), \dots, f_r(X) \in K[X]$ sobre K.

3) L/K es separable y todo polinomio irreducible $p(X) \in K[X]$ que tiene una raíz en L se descompone en factores lineales en $L[X]$.

Sea L/K una extensión de cuerpos. Un **elemento** $x \in L$ que no es algebraico sobre K se denomina **transcendental** sobre K. Un subconjunto finito $\{x_1, \dots, x_n\} \subseteq L$ es **algebraicamente independiente** sobre K si no existe un polinomio no nulo $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ con $f(x_1, \dots, x_n) = 0$. Un subconjunto arbitrario $S \subseteq L$ es algebraicamente independiente sobre K si todo subconjunto finito de S es algebraicamente independiente sobre K.

Ejemplos:

1) Como ya vimos con anterioridad, en $\mathbb{R}/\mathbb{Q}$ el elemento e es transcendental.

2) El caso especial de $\mathbb{C}/\mathbb{Q}$ es de gran importancia, ya que los elementos algebraicos y transcendentales de esta extensión de cuerpos se usan para describir los números complejos que son algebraicos y transcendentales respectivamente.

3) Todas las extensiones transcendentales son de grado infinito, luego todas las extensiones finitas son algebraicas; sin embargo hay extensiones infinitas que

son algebraicas. De hecho el cuerpo de todos los números algebraicos es una extensión infinita del cuerpo $\mathbb{Q}$ de los números racionales.

Un **base de transcendencia** de L/K es un subconjunto de L algebraicamente independiente que es maximal. Cualquier par de bases de transcendencia de L/K tienen la misma cardinalidad, que se denomina **grado de transcendencia** de L/K.

Se dice que una extensión L/K es **puramente transcendental** si y solo si existe una base de transcendencia S de L/K tal que $L = K(S)$.

Ejemplos:

1) Consideremos la extensión $\mathbb{Q}(x, \sqrt{x})/\mathbb{Q}(x)$, donde x es transcendental sobre $\mathbb{Q}$. El conjunto $\{x\}$ es algebraicamente independiente puesto que x es transcendental. Obviamente la extensión $\mathbb{Q}(x, \sqrt{x})/\mathbb{Q}(x)$ es algebraica, luego $\{x\}$ es una base de transcendencia. Pero $\{x\}$ no genera toda la extensión porque no hay expresión polinómica para $\sqrt{x}$ en x. Es fácil ver que $\{\sqrt{x}\}$ es una base de transcendencia que genera $\mathbb{Q}(x, \sqrt{x})$, luego esta extensión es puramente transcendental.

2) $\mathbb{R}/\mathbb{Q}$ es una extensión transcendental, como ya hemos visto anteriormente, aunque no es puramente transcendental.

3) $K(X)/K$ es puramente transcendental.

4) Una extensión simple es finita si está generada por un elemento algebraico y puramente transcendental si está generada por un elemento transcendental. Luego $\mathbb{R}/\mathbb{Q}$ no es simple, al no ser ni finita ni puramente transcendental.

5) Una extensión es algebraica si y solo si su grado de transcendencia es cero. El conjunto vacío sirve aquí como base de transcendencia.

6) El cuerpo de las funciones racionales en n indeterminadas $K(X_1, \dots, X_n)$ es una extensión puramente transcendental con grado de transcendencia n sobre K. Podemos tomar, por ejemplo, $\{X_1, \dots, X_n\}$ como base de transcendencia.

7) $\mathbb{Q}(\pi, \sqrt{2})$ tiene grado de transcendencia 1 sobre $\mathbb{Q}$ porque $\sqrt{2}$ es algebraica mientras que π es transcendental.

8) El grado de transcendencia de $\mathbb{C}$ o $\mathbb{R}$ sobre $\mathbb{Q}$ es la cardinalidad del continuo.

9) El grado de transcendencia de $\mathbb{Q}(\pi, e)$ sobre $\mathbb{Q}$ es 1 o 2. La respuesta precisa es desconocida porque no se sabe si π y e son algebraicamente independientes.

Si L/K tiene grado de transcendencia finito n y $\{x_1, \dots, x_n\}$ es una base de transcendencia de L/K, entonces el cuerpo $K(x_1, \dots, x_n) \subseteq L$ es K-isomorfo a $K(X_1, \dots, X_n)$, el cuerpo cociente del anillo de polinomios $K[X_1, \dots, X_n]$ en n variables sobre K. La extensión $L/K(x_1, \dots, x_n)$ es algebraica.

Sea L/K una extensión de cuerpos de grado $[L: K] = n < \infty$. Cada elemento $\alpha \in L$ induce una aplicación K-lineal $\mu_\alpha: L \longrightarrow L$ definido por $\mu_\alpha(z) \coloneqq \alpha \cdot z$ para $z \in L$. Definimos la **traza** de α con respecto a la extensión L/K por:

$$Tr_{L/K}(\alpha) \coloneqq Trace(\mu_\alpha)$$

esto significa que si $\{\alpha_1, \dots, \alpha_n\}$ es una base de L/K y

$$\alpha \cdot \alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \text{ con } a_{ij} \in K,$$

entonces

$$Tr_{L/K}(\alpha) = \sum_{i=1}^{n} a_{ii}$$

2.3 EL GRUPO FUNDAMENTAL

Pasamos ahora a la Topología Algebraica para recordar la definición del grupo fundamental de un espacio topológico, la cual es necesaria para el desarrollo de la teoría de espacios recubridores y ramificación, que abordaremos en la sección 5.2. Como texto de referencia nos hemos apoyado en [23].

Un camino γ en un espacio topológico X es una aplicación continua $\gamma: [0,1] \longrightarrow X$. Si se escribe $\gamma(0) = a$ y $\gamma(1) = b$, se dice que el camino γ tiene su origen en a y su extremo en b.

Dados dos caminos $\gamma_0, \gamma_1: [0,1] \longrightarrow X$ con el mismo origen, $\gamma_0(0) = \gamma_1(0) = a$ y el mismo extremo $\gamma_0(1) = \gamma_1(1) = b$, diremos que son homótopos si existe una aplicación continua

$$h: \begin{cases} [0,1] \times [0,1] \longrightarrow X \\ (s,t) \longmapsto h(s,t) \end{cases}$$

tal que $\gamma_s(t) = h(s,t)$ es una familia de caminos parametrizada por $s \in [0,1]$ en la que todas las curvas γ_s tienen su origen en a: $\gamma_s(0) = a$ y su extremo en b $\gamma_s(1) = b$, y de tal forma que el camino correspondiente al valor del parámetro $s = 0$ coincide con el camino γ_0 del enunciado, mientras que el camino correspondiente a $s = 1$ coincide con γ_1.

La relación de homotopía entre los caminos γ_0 y γ_1 la denotaremos como $\gamma_0 \sim \gamma_1$, y la aplicación continua h se llamará homotopía de γ_0 con γ_1. La clase de equivalencia de todas los caminos homótopos a γ_0 lo denominaremos $[\gamma_0]$.

Fijado un punto $a \in X$ denotaremos con Γ_a a los caminos en X que tienen su origen y extremo en a, esto es, Γ_a son lazos con base en a.

Dados los caminos γ, γ' en Γ_a, se llama producto de γ por γ' y se denota por $\gamma' \cdot \gamma$, al camino definido por

$$(\gamma' \cdot \gamma)(t) = \begin{cases} \gamma(2t), & si\ 0 \leq t \leq 1/2 \\ \gamma'(2t-1) & si\ 1/2 \leq t \leq 1 \end{cases}$$

Análogamente, dado el camino γ en Γ_a, definimos γ^{-1} como $\gamma^{-1}(t) = \gamma(1-t), t \in [0,1]$

Sabemos que [23]:

El producto de lazo en a es compatible con la relación de homotopía, esto es, si $\gamma_0 \sim \gamma_1$ y $\gamma'_0 \sim \gamma'_1$ entonces $\gamma'_0 \cdot \gamma_0 \sim \gamma'_1 \cdot \gamma_1$.

Dado $\gamma \in \Gamma_a$ entonces $\gamma^{-1} \cdot \gamma \sim a$, el camino constante de valor a.

El producto de clases de homotopía de caminos es asociativo.

Dado un espacio topológico X en el que hemos fijado un punto a, el conjunto de clases de homotopía de lazos con base en a es un grupo algebraico que denotaremos por $\pi_1(X, a)$ y llamaremos **grupo fundamental** de X en a.

Si X es conexo por caminos, dados dos puntos cualesquiera a y $b \in X$ se cumple que $\pi_1(X, a) \simeq \pi_1(X, b)$.

Diremos que una variedad topológica conexa X es simplemente conexa si su grupo fundamental $\pi_1(X, a)$ se reduce al elemento neutro del mismo, es decir, todo lazo con base a es homótopo al lazo constante a.

Ejemplo: el plano complejo $\mathbb{C}$ es simplemente conexo. Sea $\gamma: [0,1] \longrightarrow \mathbb{C}$ un camino con origen y extremo el origen de coordenadas $\gamma(0) = \gamma(1) = 0$. La homotopía

$$h: \begin{cases} [0,1] \times [0,1] \longrightarrow \mathbb{C} \\ h(s,t) = s \cdot \gamma(t) \end{cases}$$

cumple $h(0,t) = 0,\ h(1,t) = \gamma(t)$, con lo que el lazo en el origen $\gamma(t)$ es homótopo al lazo constante 0.

El mismo argumento prueba que el disco unidad $D = \{z \in \mathbb{C} |\ |z| < 1\}$ es simplemente conexo.

Sea $f: X \longrightarrow Y$ una aplicación continua entre variedades topológicas. Sea $a \in X$ y $b = f(a) \in Y$. Entonces f induce una aplicación entre los grupos fundamentales $f_*: \pi_1(X, a) \longrightarrow \pi_1(Y, b)$ como sigue: dado un lazo γ con base a, entonces $f_*(\gamma) = f \circ \gamma$ es un lazo en b. Esta aplicación está bien definida, pues si $\gamma,\ \gamma'$ son lazos con base a homótopos por medio de la homotopía $h: [0,1] \times [0,1] \longrightarrow X$, entonces $f \circ h$ es una homotopía entre $f \circ \gamma$ y $f \circ \gamma'$.

3 CUERPOS DE FUNCIONES ALGEBRAICAS (CFA)

3.1 FUNDAMENTOS DE LOS CUERPOS DE FUNCIONES ALGEBRAICAS (CFA)

Comenzamos el capítulo dedicado a los CFA con una sección introductoria de los conceptos básicos y resultados de la teoría: valuaciones, *places*, divisores, género de un CFA, adeles, diferenciales de Weil y los teoremas de Riemann y de Riemann-Roch, estos últimos de gran transcendencia para la determinación de algunas propiedades de los códigos AG.

En la sección 3.3 veremos ejemplos de CFA y conceptos que posteriormente aplicaremos para el caso de curvas algebraicas en el capítulo 5 de este trabajo.

Como texto de referencia para esta sección nos hemos basado en [20].

Un **cuerpo de funciones algebraicas** F/K de una variable sobre un cuerpo K es una extensión de cuerpos $F \supseteq K$ tal que F es una extensión finita algebraica de $K(x)$ para algún elemento $x \in F$ que es transcendental sobre K.

El conjunto $\overline{K} \coloneqq \{z \in F \mid z\ es\ algebraico\ sobre\ K\}$ es un subcuerpo de F y se denomina el **cuerpo de constantes** de F/K. Se cumple que $K \subseteq \overline{K} \subsetneq F$. Decimos que K es algebraicamente cerrado en F si $\overline{K} = K$.

El ejemplo más simple de CFA es el **cuerpo de funciones racionales**. Se denomina racional a F/K si $F = K(x)$ para algún $x \in F$ que es transcendental sobre K.

Un **anillo de valuación** del CFA F/K es un anillo $\mathcal{O} \subseteq F$ con las siguientes propiedades:

1) $K \subsetneq \mathcal{O} \subsetneq$ F, y
2) para cada $z \in F$ tenemos que $z \in \mathcal{O}\ o\ z^{-1} \in \mathcal{O}$

Veremos en lo que sigue que los anillos de valuación son las anillos de valuación discreta de la página 16. Más adelante veremos también que *places* y puntos se corresponden.

Proposición: sea $\mathcal{O}$ un anillo de valuación del CFA F/K. Se cumple lo siguiente:

1) $\mathcal{O}$ es un anillo local; i.e., $\mathcal{O}$ tiene un único ideal maximal $P = \mathcal{O}\backslash\mathcal{O}^{\times}$, donde $\mathcal{O}^{\times} = \{z \in \mathcal{O} | \, existe\ un\ elemento\ w \in \mathcal{O}\ con\ zw = 1\}$ es el grupo formado por las unidades de $\mathcal{O}$.

2) Dado $0 \neq x \in F$. Entonces $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.

3) Para el cuerpo de constantes $\overline{K}$ de F/K se cumple que $\overline{K} \in \mathcal{O}\ y\ \overline{K} \cap P = \{0\}$.

Teorema [20]: sea $\mathcal{O}$ un anillo de valuación del CFA F/K y sea P su ideal maximal y único. Se cumple lo siguiente:

1) P es un ideal principal

2) Si $P = t\mathcal{O}$ entonces cada $0 \neq z \in F$ tiene una única representación de la forma $z = t^n u$ para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^{\times}$.

3) $\mathcal{O}$ es un dominio de ideales principales (DIP). Más precisamente, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal, entonces $I = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.

Ya hemos visto que los anillos que poseen las propiedades anteriores se denominan **anillos de valuación discreta**.

Un ***place*** P del CFA F/K es el ideal maximal de algún anillo de valuación $\mathcal{O}$ de F/K. Cada elemento $t \in P$ tal que $P = t\mathcal{O}$ se denomina **elemento primo** de P.

Denominamos al conjunto de *places* de F/K por

$$\mathbb{P}_F \coloneqq \{P | \, P\ es\ un\ place\ de\ F/K\}.$$

Si $\mathcal{O}$ es un anillo de valuación de F/K y P es su ideal maximal, entonces $\mathcal{O}$ está determinado únicamente por P, ya que $\mathcal{O} = \{z \in F | \, z^{-1} \notin P\}$. En consecuencia, $\mathcal{O}_P \coloneqq \mathcal{O}$ se denomina el anillo de valuación del *place* P.

A un *place* $P \in \mathbb{P}_F$ asociamos una aplicación $v_P \colon F \to \mathbb{Z} \cup \{\infty\}$ de la siguiente forma: elegimos un elemento primo t de P. Entonces cada $0 \neq z \in F$ tiene una única representación $z = t^n u$ con $u \in \mathcal{O}^{\times}$ y $n \in \mathbb{Z}$. Definimos $v_P(z) \coloneqq n\ y\ v_P(0) \coloneqq \infty$.

Teorema [20]: sea F/K un CFA:

1) Para un *place* $P \in \mathbb{P}_F$, la aplicación v_P definida anteriormente es una valuación discreta de F/K *(véase valuación discreta en sección 2.1)*. Además se cumple:

   - $\mathcal{O}_P = \{z \in F | \, v_P(z) \geq 0\}$
   - $\mathcal{O}_P^{\times} = \{z \in F | \, v_P(z) = 0\}$
   - $P = \{z \in F | \, v_P(z) > 0\}$

2) Un elemento $x \in F$ es elemento primo de P si y solo si $v_P(x) = 1$

3) Al contrario, supongamos que v es una valuación discreta de F/K, entonces el conjunto $P = \{z \in F | v(z) > 0\}$ es un *place* de F/K y $\mathcal{O}_P = \{z \in F | \, v_P(z) \geq 0\}$ es el anillo de valuación correspondiente.

4) Cada anillo de valuación $\mathcal{O}$ de F/K es un subanillo maximal y propio de F.

Sea $P \in \mathbb{P}_F$, definimos:

1) $F_P \coloneqq \mathcal{O}_P/P$ el cuerpo formado por la clase de equivalencia de $\mathcal{O}_P$ módulo P (es un cuerpo dado que P es un ideal maximal). La aplicación $x \to x(P)$ desde F a $F_P \cup \{\infty\}$ (donde $x(P) = \infty \; si \; x \in F \backslash \mathcal{O}_P$) se denomina **aplicación de clases de equivalencia con respecto a P**.

2) $degP \coloneqq [F_P : K]$ es el **grado** de P. Un *place* de grado uno se denomina también ***place* racional** de F/K.

3) El grado de un *place* es siempre finito, más preciso, se cumple que:

$$degP \leq [F : K(x)] < \infty$$

Sea $z \in F$ y $P \in \mathbb{P}_F$. Decimos que P es un **cero** de z si $v_P(z) > 0$; P es un **polo** de z si $v_P(z) < 0$. Si $v_P(z) = m > 0$, P es un **cero** de z de **orden** m; si $v_P(z) = -m < 0$, P es un **polo** de z de **orden** m.

Definimos el **grupo de divisores** de F/K como el grupo abeliano libre generado por los *places* de F/K; lo denominamos $Div(F)$. Los elementos de $Div(F)$ se llaman **divisores** de F/K. En otras palabras, un divisor es una suma formal: $D = \sum_{P \in \mathbb{P}_F} n_P P$ con $n_P \in \mathbb{Z}$ donde, salvo un número finito, todos los $n_P = 0$.

Se define el **soporte** del divisor D como: $suppD \coloneqq \{P \in \mathbb{P}_F | \, n_P \neq 0\}$.

Se cumple: $D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P$

Para $Q \in \mathbb{P}_F$ y $D = \sum n_P P \in Div(F)$ definimos $v_Q(D) \coloneqq n_Q$, luego $D = \sum_{P \in suppD} v_P(D) \cdot P$.

Definimos un ordenamiento parcial en $Div(F)$ por $D_1 \leq D_2 : \Leftrightarrow \; v_P(D_1) \leq v_P(D_2)$ para todo $P \in \mathbb{P}_F$. Un divisor $D \geq 0$ se denomina positivo.

El **grado de un divisor** se define como: $degD \coloneqq \sum_{P \in \mathbb{P}_F} v_P(D) \cdot degP$

Sea $0 \neq x \in F$ y denotamos por $Z \; (resp. N)$ el conjunto de ceros (resp. polos) de x en $\mathbb{P}_F$. Definimos:

1) $(x)_0 \coloneqq \sum_{P \in Z} v_P(x) \cdot P$, el **divisor cero** de x.
2) $(x)_\infty \coloneqq \sum_{P \in N} (-v_P(x)) \cdot P$, el **divisor polo** de x.
3) $(x) \coloneqq (x)_0 - (x)_\infty$, el **divisor principal** de x.

Se observa que $(x)_0 \geq 0 \; y \; (x)_\infty \geq 0$ y $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) \cdot P$. Los elementos $0 \neq x \in F$ que son constantes se caracterizan por: $x \in K \Leftrightarrow (x) = 0$.

El conjunto de divisores $Princ(F) \coloneqq \{(x) | \, 0 \neq x \in F\}$ se denomina **grupo de divisores principales** de F/K. Es un subgrupo de $Div(F)$. El grupo cociente: $Cl(F) \coloneqq Div(F)/Princ(F)$ se denomina **grupo de clases de divisores** de F/K. Para un divisor $D \in Div(F)$, el elemento correspondiente en el grupo cociente $Cl(F)$ se denota por $[D]$, la clase de divisores de D. Dos divisores $D, \; D' \in Div(F)$ son **equivalentes** (escribiéndose $D \sim D'$) si $[D] = [D']: i.e., D = D' + (x) \; para \; algún \; x \in F \backslash \{0\}$. Se verifica que se trata de una relación de equivalencia.

Para un divisor $A \in Div(F)$ definimos el **espacio de *Riemann-Roch*** asociado a A por:

$$\mathcal{L}(A) \coloneqq \{x \in F | (x) \geq -A\} \cup \{0\}.$$

Sea $A \in Div(F)$, se cumple por los teoremas anteriores:

1) $x \in \mathcal{L}(A)$ si y solo si $\nu_P(x) \geq -\nu_P(A)$ para todo $P \in \mathbb{P}_F$.

2) $\mathcal{L}(A) \neq 0$ si y solo si existe un divisor $A \sim A'$ con $A' \geq 0$.

3) $\mathcal{L}(A)$ es un espacio vectorial sobre K.

4) Si A' es un divisor equivalente a A, entonces $\mathcal{L}(A) \simeq \mathcal{L}(A')$.

Tenemos los siguientes resultados (ver [20]):

Lema:

1) $\mathcal{L}(0) = K$

2) $Si\ A < 0\ entonces\ \mathcal{L}(A) = \{0\}$

Proposición: para cada divisor $A \in Div(F)$ se cumple que el espacio $\mathcal{L}(A)$ es un espacio vectorial finito sobre K.

Para $A \in Div(F)$ el entero $\ell(A) := dim\ \mathcal{L}(A)$ se denomina la **dimensión del divisor** A.

Teorema [20]: todos los divisores principales tienen grado cero. Más preciso: sea $x \in F \backslash K$ y $(x)_0$ resp. $(x)_\infty$ denotan el divisor cero resp. polo de x. Entonces:

$$deg(x)_0 = deg(x)_\infty = [F : K(x)].$$

Esto significa que un elemento $0 \neq x \in F$ tiene tantos ceros como polos, contando los mismos apropiadamente.

Corolario: se cumple:

1) Sean A y A' divisores tales que $A \sim A'$. Entonces $\ell(A) = \ell(A')$ y $degA = degA'$.

2) $Si\ degA < 0\ entonces\ \ell(A) = 0$

3) Para un divisor de grado cero, las siguientes sentencias son equivalentes:

   a) A es principal

b) $\ell(A) = 1$

Proposición: existe una constante $\gamma \in \mathbb{Z}$ tal que para todos los divisores $A \in Div(F)$ se cumple que: $degA - \ell(A) \leq \gamma$

Lo importante aquí es el hecho de que γ es independiente del divisor A; depende solo del CFA F/K.

Se define el **género** de F/K como:

$$g \coloneqq max\{degA - \ell(A) + 1 |\ A \in Div(F)\}$$

Esta definición tiene sentido por la proposición anterior. El género es el invariante más importante de un CFA**.**

Corolario: el género de F/K es un entero no negativo.

Demostración: en la definición de g, tomamos $A = 0$. $Entonces\ \deg(0) - \ell(0) + 1 = 0$, luego $g \geq 0$.

Teorema de Riemann [20]: sea F/K un CFA de género g. Se cumple que:

1) Para todos los divisores $A \in Div(F)$,

$$\ell(A) \geq degA + 1 - g.$$

2) Existe un entero c, que depende solo de F/K, tal que:

$$\ell(A) = degA + 1 - g,\ siempre\ que\ degA \geq c.$$

Para un divisor $A \in Div(F)$, el entero:

$$i(A) \coloneqq \ell(A) - degA + g - 1$$

Se denomina **índice de especialidad** de A.

Los códigos algebraico-geométricos, que veremos en el siguiente capítulo, se basan en espacios de diferenciales en CFA; a continuación explicamos estos conceptos

Un **adele** de F/K es una aplicación:

$$\alpha: \begin{cases} \mathbb{P}_F \longrightarrow F \\ P \longrightarrow \alpha_P \end{cases}$$

Tal que $\alpha_P \in \mathcal{O}_P$ para casi todo $P \in \mathbb{P}_F$. El adele se considera como un elemento del producto directo $\prod_{P\in\mathbb{P}_F} F$ y usamos la notación $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$ o, incluso de forma más simple, $\alpha = (\alpha_P)$. El conjunto:

$$\mathcal{A}_F \coloneqq \{\alpha |\ \alpha\ es\ un\ adele\ de\ F/K\}$$

se denomina el **espacio de adeles** de F/K.

El adele principal de un elemento $x \in F$ es el adele en la que todos sus componentes son igual a x (esta definición tiene sentido pues x tiene solo un número finito de polos). Esto proporciona un embebemiento $F \hookrightarrow \mathcal{A}_F$. De esta forma las valuaciones ν_P de F/K se extienden de forma natural a $\mathcal{A}_F$ definiendo $\nu_P(\alpha) \coloneqq \nu_P(\alpha_P)$ (donde α_P es la P-componente del adele α). Por definición se cumple que $\nu_P(\alpha) \geq 0$ para casi todo $P \in \mathbb{P}_F$.

Para $A \in Div(F)$ definimos:

$$\mathcal{A}_F(A) \coloneqq \{\alpha \in \mathcal{A}_F |\ \nu_P(\alpha) \geq -\nu_P(A)\ para\ todo\ P \in \mathbb{P}_F\}$$

que es un K-subespacio de $\mathcal{A}_F$.

Teorema [20]: para cada divisor $A \in Div(F)$ el índice de especialidad es

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

Corolario:

$$g = \dim(\mathcal{A}_F/\mathcal{A}_F(0) + F))$$

demostración: $i(0) = \ell(0) - \deg(0) + g - 1 = 1 - 0 + g - 1 = g$

El teorema anterior puede expresarse de otra forma: para todo $A \in Div(F)$ se cumple que:

$$\ell(A) = degA + 1 - g + \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

que es un versión preliminar del teorema de Riemann-Roch que veremos más adelante.

Vamos a introducir ahora el concepto de diferencial de Weil, que constituye una herramienta muy útil para el estudio de los CFA.

Un **diferencial de Weil** de F/K es una aplicación K-lineal $\omega: \mathcal{A}_F \longrightarrow K$ que vale cero en $\mathcal{A}_F(A) + F$ para algún divisor $A \in Div(F)$. Llamamos

$$\Omega_F \coloneqq \{\omega |\ \omega\ es\ un\ diferencial\ de\ Weil\ de\ F/K\}$$

el módulo de diferenciales de Weil de F/K. Para $A \in Div(F)$ sea:

$$\Omega_F(A) \coloneqq \{\omega \in \Omega_F |\ \omega\ vale\ cero\ en\ \mathcal{A}_F(A) + F\}$$

que es un subespacio de Ω_F.

Lema [20]: para $A \in Div(F)$ se cumple que:

$$dim\Omega_F(A) = i(A)$$

Para $x \in F\ y\ \omega \in \Omega_F$ definimos $x\omega: \mathcal{A}_F \longrightarrow K$ por: $(x\omega)(\alpha) \coloneqq \omega(x\alpha)$

se comprueba fácilmente que $x\omega$ es un diferencial de Weil de F/K. De hecho, si ω vale cero en $\mathcal{A}_F(A) + F$ entonces $x\omega$ vale a su vez cero en $\mathcal{A}_F(A + (x)) + F$.

Proposición: Ω_F es un espacio vectorial unidimensional sobre F.

Vamos ahora a asociar un divisor a cada diferencial de Weil $\omega \neq 0$. Con esa finalidad, consideremos (para un ω fijo) el conjunto de divisores:

$$M(\omega) \coloneqq \{A \in Div(F) |\ \omega\ vale\ cero\ en\ \mathcal{A}_F(A) + F\}$$

Lema [20]: sea $0 \neq \omega \in \Omega_F$. Entonces existe un único divisor $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.

Las definiciones que vienen a continuación tienen sentido por el lema precedente y, a semejanza de lo que ocurre para *places* se tiene:

Definición:

1) El **divisor** (ω) **de un diferencial de Weil** $\omega \neq 0$ es el divisor de F/K determinado únicamente que satisface:

   a) ω vale cero en $\mathcal{A}_F\big((\omega)\big) + F$, y

   b) si ω vale cero en $\mathcal{A}_F(A) + F$ entonces $A \leq (\omega)$.

2) Para $0 \neq \omega \in \Omega_F$ y $P \in \mathbb{P}_F$ se define $\nu_P(\omega) \coloneqq \nu_P((\omega))$.

3) Se dice que un *place* P es un cero (resp. un polo) de ω si $\nu_P(\omega) > 0$ (resp. $\nu_P(\omega) < 0$). El diferencia de Weil ω se denomina **regular en P** si $\nu_P(\omega) \geq 0$, y **regular** (u holomorfo) si es regular en todos los *places* $P \in \mathbb{P}_F$.

4) Un divisor W se denomina **divisor canónico** de F/K si $W = (\omega)$ para algún $\omega \in \Omega_F$.

Nota: se sigue inmediatamente de las definiciones anteriores:

1) $\Omega_F(A) \coloneqq \{\omega \in \Omega_F | \ \omega = 0 \ o \ A \leq (\omega)\}$

2) $\Omega_F(0) \coloneqq \{\omega \in \Omega_F | \ \omega = es \ regular\}$

3) $dim\Omega_F(0) = g$

Proposición:

1) Para $0 \neq x \in F$ y $0 \neq \omega \in \Omega_F$ se cumple que: $(x\omega) = (x) + (\omega)$

2) Todo par de divisores canónicos de F/K son equivalentes.

Se concluye de esta proposición que los divisores canónicos de F/K forman una clase completa $[W]$ dentro del grupo de clases de divisores $Cl(F)$: esta clase de divisores se denomina la **clase canónica** de F/K.

Teorema de dualidad [20]: sea A un divisor arbitrario y $W = (\omega)$ un divisor canónico de F/K. Entonces la aplicación:

$$\mu: \begin{cases} \mathcal{L}(W - A) \longrightarrow \Omega_F(A) \\ x \qquad\quad \longrightarrow x\omega \end{cases}$$

es un isomorfismo de espacios K-vectoriales. En particular:

$$i(A) = \ell(W - A)$$

Teniendo en cuenta los resultados expuestos hasta ahora esta sección, los cuales se han extraído del excelente texto de Stichtenoth [20], obtenemos el teorema de Riemann-Roch, que con diferencia es el teorema más importante en la teoría de CFA. La demostración del mismo se puede encontrar en libro de Stichtenoth.

Teorema de Riemann-Roch [20]: sea W un divisor canónico de F/K. Entonces para cada divisor $A \in Div(F)$ se cumple:

$$\ell(A) = degA + 1 - g + \ell(W - A)$$

Corolario: para un divisor canónico W tenemos:

$$degW = 2g - 2 \;\; y \;\; \ell(W) = g$$

Teorema [20]: si A es un divisor de F/K de grado $degA \geq 2g - 1$ entonces:

$$\ell(A) = degA + 1 - g$$

Vamos a ver ahora algunas conclusiones extraídas del teorema de Riemann-Roch

Caracterización del cuerpo de funciones racionales*:* las siguientes condiciones son equivalentes,

1) F/K es racional; i.e. $F = K(x)$ para algún elemento x que es transcendental sobre el cuerpo K.

2) F/K tiene género nulo y existe un divisor $A \in Div(F)$ con $degA = 1$.

Proposición: sea $P \in \mathbb{P}_F$. Entonces para cada $n \geq 2g$ existe un elemento $x \in F$ con divisor polo $(x)_\infty = nP$.

Componentes locales de diferenciales Weil: sea $P \in \mathbb{P}_F$;

1) Para $x \in F$ sea $\iota_P(x) \in \mathcal{A}_F$ el adele cuyo componente P es x y todos los demás componentes son nulos.

2) Para un diferencial Weil $\omega \in \Omega_F$ se define su componente local $\omega_P: F \longrightarrow K$ por:

$$\omega_P(x) \coloneqq \omega(\iota_P(x))$$

Proposición: sea $\omega \in \Omega_F$ y $\alpha = (\alpha_P) \in \mathcal{A}_F$. Entonces $\omega_P(\alpha_P) \neq 0$ para al menos un conjunto finito de *places* P y:

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P) \quad \text{, en particular} \quad \sum_{P \in \mathbb{P}_F} \omega_P(1) = 0$$

Proposición:

1) Sea $\omega \neq 0$ un diferencial Weil de F/K y $P \in \mathbb{P}_F$, se cumple:

$$v_P(\omega) = max\{r \in \mathbb{Z} |\ \omega_P(x) = 0\ para\ todo\ x \in F\ con\ \ v_P(x) \geq -r\}$$

2) Si $\omega, \omega' \in \Omega_F$ y $\omega_P = \omega_{P'}$ para algún $P \in \mathbb{P}_F$, entonces $\omega = \ \omega'$

Vamos a particularizar ahora para cuerpo de funciones racionales $F = K(x)$. Teniendo en cuenta que P_∞ es el divisor polo de x y P_a el divisor cero de $x - a$ (para $a \in K$), los siguientes resultados serán importantes posteriormente:

1) El divisor $-2P_\infty$ es canónico.

2) Existe un diferencial Weil único $\eta \in \Omega_{K(x)}$ con $(\eta) = -2P_\infty$ y $\eta_{P_\infty}(x^{-1}) = -1$

3.2 DIFERENCIALES DE CUERPOS DE FUNCIONES ALGEBRAICAS. TEOREMA DEL RESIDUO.

Hemos visto que los diferenciales de Weil constituyen una herramienta muy útil para el estudio de los CFA. Vamos a hacer ahora un repaso de la teoría de diferenciales y de su relación con los diferenciales de Weil, para terminar con la noción de la completitud P-adic y, a partir de misma, definir el concepto de residuo de un diferencial y describir el teorema del residuo, que se utilizará posteriormente para mostrar la forma más comúnmente usada para representar los códigos AG, utilizando componentes locales de diferenciales de Weil. Para ello nos seguiremos basando en el mismo texto de referencia [20].

Consideramos un CFA F/K de una variable donde K es el cuerpo de constantes de F y asumimos que K es perfecto.

Sea M un espacio vectorial sobre F, se dice que una aplicación $\delta: F \longrightarrow M$ es una derivación de F/K si δ es K-linear y la regla del producto:

$$\delta(u \cdot v) = u \cdot \delta(v) + v \cdot \delta(u)$$

se cumple para todo $u, v \in F$.

Algunas consecuencias de esta definición se describen en los siguientes lemas [20]:

Lema: sea $\delta: F \longrightarrow M$ una derivación de F/K en M. Se cumple entonces:

1) $\delta(a) = 0$ para cada $a \in K$.
2) $\delta(z^n) = nz^{n-1} \cdot \delta(z)$ para $z \in F$ y $n \geq 0$.
3) Si $charK = p > 0$, entonces $\delta(z^p) = 0$ para cada $z \in F$.
4) $\delta(x/y) = (y \cdot \delta(x) - x \cdot \delta(y))/y^2$, para $x, y \in F$ e $y \neq 0$.

Lema: supongamos que x es un elemento separante de F/K y que $\delta_1, \delta_2: F \longrightarrow M$ son derivaciones de F/K con $\delta_1(x) = \delta_2(x)$. Entonces $\delta_1 = \delta_2$.

Proposición:

1) Supongamos que E/F es una extensión separable y finita de F y que $\delta_0: F \longrightarrow N$ es una derivación de F/K en un cuerpo $N \supseteq E$. Entonces δ_0 se puede extender a una derivación $\delta: E \longrightarrow N$. Esta extensión está determinada únicamente por δ_0.

2) Si $x \in F$ es un elemento separante de F/K y $N \supseteq F$ es un cuerpo, entonces existe una única derivación $\delta: F \longrightarrow N$ de F/K con la propiedad $\delta(x) = 1$.

Sea x un elemento separante del CFA F/K. La única derivación $\delta_x: F \longrightarrow F$ de F/K con la propiedad $\delta_x(x) = 1$ se denomina **derivación con respecto a x**.

Sea $Der_F \coloneqq \{\eta: F \longrightarrow F \mid \eta\ es\ una\ derivación\ de\ F/K\}$. Para $\eta_1, \eta_2 \in Der_F$ y $z, u \in F$ definimos:

$$(\eta_1 + \eta_2)(z) \coloneqq \eta_1(z) + \eta_2(z) \quad \text{y} \quad (u \cdot \eta_1)(z) \coloneqq u \cdot \eta_1(z)$$

es obvio que $\eta_1 + \eta_2$ y $u \cdot \eta_1$ son derivaciones de F/K, en consecuencia Der_F es un F-módulo y se denomina el **módulo de derivaciones de F/K**.

Lema [20]: sea x un elemento separante de F/K. Se cumple lo siguiente:

1) Para cada derivación $\eta \in Der_F$ tenemos $\eta = \eta(x) \cdot \delta_x$. En particular, Der_F es un F-módulo unidimensional.

2) (Regla de la cadena): si y es otro elemento separante de F/K, entonces: $\delta_y = \delta_y(x) \cdot \delta_x$

3) Para $t \in F$ se cumple: $\delta_x(t) \neq 0 \Leftrightarrow t$ es un elemento separante.

En el conjunto $Z \coloneqq \{(u, x) \in F \times F \mid x\ es\ separante\}$ definimos la relación $\sim$ como: $(u, x) \sim (v, y) \Leftrightarrow v = u \cdot \delta_y(x)$, usando la regla de la cadena, se verifica que $\sim$ es una relación de equivalencia en Z.

A continuación queremos llegar de nuevo a las diferenciales de Weil, pero vamos a empezar sentando las bases que nos permitan su contextualización dentro de la teoría más general de los diferenciales de CFA.

Denotamos la clase de equivalencia de $(u, x) \in F$ con relación a la relación anterior de equivalencia como udx y lo llamamos **diferencial de $\boldsymbol{F/K}$**. La clase de equivalencia de $(1, x)$ la denotamos simplemente por dx. Se observa que:

$$udx = vdy \Leftrightarrow v = u \cdot \delta_y(x)$$

sea $$\Delta_F \coloneqq \{udx |\, u \in F, y\ x \in F\ es\ separante\}$$

el conjunto de todos los diferenciales de F/K. Definimos la suma de dos diferenciales udx, $vdy \in \Delta_F$ de la siguiente manera: elegimos un elemento separante z; entonces:

$$udx + vdy \coloneqq \big(u \cdot \delta_z(x) + v \cdot \delta_z(y)\big)dz$$

por la regla de la cadena esta definición es independiente de la elección de z. De la misma manera, definimos:

$$w \cdot (udx) \coloneqq (wu)dx \in \Delta_F$$

para $w \in F$ y $udx \in \Delta_F$. Se comprueba fácilmente de esta manera que Δ_F es un F-módulo.

Para un elemento no separante $t \in F$ definimos $dt \coloneqq 0$ (el elemento nulo de Δ_F); de esta forma obtenemos una aplicación:

$$d\colon \begin{cases} F \longrightarrow \Delta_F \\ t \longrightarrow dt \end{cases}$$

el par (Δ_F, d) se define con el nombre de **módulo diferencial de $\boldsymbol{F/K}$**.

Proposición:

1) Sea $z \in F$ un elemento separante. Entonces $dz \neq 0$ y todo diferencial $w \in \Delta_F$ se escribe de manera única de la forma $w = udz$, con $u \in F$. Luego Δ_F es un F-módulo unidimensional.

2) La aplicación $d\colon F \longrightarrow \Delta_F$ definida anteriormente es una derivación de F/K; i.e.:

$$d(ax) = adx,\ \ d(x+y) = dx + dy,\ \ y\ \ d(xy) = xdy + ydx$$

para todo $x, y \in F\ \ y\ \ a \in K$

3) Para $t \in F$ tenemos $dt \neq 0 \Leftrightarrow t$ es elemento separante

4) Supongamos que $\delta: F \longrightarrow M$ es una derivación de F/K en un F-módulo M. Entonces existe una aplicación F-linear única $\mu: \Delta_F \longrightarrow M$ tal que $\delta = \mu \circ d$.

Un **diferencial** de la forma específica $w = dx$ (con $x \in F$) se dice que es **exacto**. Los diferenciales exactos forman un K-subespacio de Δ_F.

Como Δ_F es un F-módulo unidimensional, podemos definir el cociente ${}^{w_1}/_{w_2} \in F$ para $w_1, w_2 \in \Delta_F$ y $w_2 \neq 0$ haciendo: $u = \frac{w_1}{w_2} :\Leftrightarrow w_1 = uw_2$

En particular, si $z \in F$ un elemento separante e $y \in F$, el cociente ${}^{dy}/_{dz}$ está definido y se cumple: $\delta_z(y) = {}^{dy}/_{dz}$

Usando esta notación, algunas de las fórmulas previas pueden rescribirse de una forma más sugestiva, por ejemplo:

$$udx = vdy \Leftrightarrow v = u \cdot {}^{dx}/_{dy} \Leftrightarrow u = v \cdot {}^{dy}/_{dx} \quad \text{y} \quad {}^{dy}/_{dx} = {}^{dy}/_{dz} \cdot {}^{dz}/_{dx}$$

si x y z son elementos separantes.

La completitud P-Adic: el cuerpo de números reales $\mathbb{R}$ es la completitud del cuerpo de los números racionales $\mathbb{Q}$ con relación al valor absoluto ordinario. Esto significa que el cuerpo $\mathbb{Q}$ es denso en $\mathbb{R}$ y que toda secuencia de *Cauchy* en $\mathbb{R}$ es convergente. Seguidamente vamos a desarrollar un concepto similar, denominado la completitud de un CFA F/K con relación a un *place* $P \in \mathbb{P}_F$. Esto nos proporcionará una herramienta útil para calcular la derivación ${}^{dz}/_{dt}$ (donde t es un elemento primo de P) y también nos permitirá definir el residuo de un diferencial en el *place* P. En esta exposición seguimos basándonos en el texto de Stichtenoth [20].

Decimos que una secuencia $(x_n)_{n\geq 0}$ en T es convergente si existe un elemento $x \in T$ (denominado el límite de la secuencia) que satisface: para cada $c \in \mathbb{R}$ existe un índice $n_0 \in \mathbb{N}$ tal que $v(x - x_n) \geq c$ cuando $n \geq n_0$.

Una secuencia $(x_n)_{n\geq 0}$ se llama secuencia de *Cauchy* si tiene la siguiente propiedad: para cada $c \in \mathbb{R}$ existe un índice $n_0 \in \mathbb{N}$ tal que $v(x_n - x_m) \geq c$ cuando $n, m \geq n_0$.

Si una secuencia $(x_n)_{n\geq 0}$ es convergente entonces su límite $x \in T$ es único; luego podemos escribir $x = \lim_{n\to\infty} x_n$.

Toda secuencia convergente es una secuencia de *Cauchy*.

En general no es cierto que todas las secuencias de *Cauchy* sean convergentes.

Se dice que un cuerpo valuado T es **completo** si toda secuencia de *Cauchy* en T es convergente.

Supongamos que (T, v) es un cuerpo valuado. Una **completitud** de T es un cuerpo valuado $(\hat{T}, \hat{v})$ con las siguientes propiedades:

1) $T \subseteq \hat{T}$ y v es la restricción de $\hat{v}$ a T.

2) $\hat{T}$ es completo con respecto a la valuación $\hat{v}$.

3) T es denso en $\hat{T}$; i.e., para cada $z \in \hat{T}$ existe una secuencia $(x_n)_{n\geq 0}$ en T con $\lim_{n\to\infty} x_n = z$.

Proposición: para cada cuerpo valuado (T, v) existe una completitud $(\hat{T}, \hat{v})$ única (hasta isomorfismos).

Sea $(z_n)_{n\geq 0}$ una secuencia en (T, v) y $s_m \coloneqq \sum_{i=0}^{m} z_i$. Decimos que la serie infinita $\sum_{i=0}^{m} z_i$ es convergente si la secuencia de sus sumas parciales $(s_m)_{m\geq 0}$ es convergente:

$$\sum_{i=0}^{m} z_i \coloneqq \lim_{n\to\infty} s_m$$

Sea $(z_n)_{n\geq 0}$ una secuencia de un cuerpo valuado completo (T, v). Entonces la serie infinita $\sum_{i=0}^{m} z_i$ es convergente si y solo si la secuencia $(z_n)_{n\geq 0}$ converge a cero.

Sea P un *place* de F/K. La completitud de F con relación a la valuación v_P se denomina la completitud P-adic de F. Llamamos a esta completitud $\hat{F}_P$ y v_P a su valuación.

Teorema [20]: sea $P \in \mathbb{P}_F$ un *place* de grado uno y $t \in F$ un elemento primo de P. Se cumple entonces que todo elemento $z \in \hat{F}_P$ tiene una representación única de la forma

$$z = \sum_{i=n}^{\infty} a_i t^i \text{ con } n \in \mathbb{Z} \text{ y } a_i \in K$$

Esta representación se denomina la **expansión en serie de potencias *P*-adic** de z con respecto de t.

Por otro lado, si $(c_i)_{i \geq n}$ es una secuencia en K, entonces la serie $\sum_{i=n}^{\infty} c_i t^i$ converge en $\hat{F}_P$ y se cumple:

$$v_P\left(\sum_{i=n}^{\infty} c_i t^i\right) = min\{i |\, c_i \neq 0\}$$

Continuamos considerando ahora un *place* P de F/K de grado uno y un elemento primo t de P. Sabemos que t es un elemento separante de F/K y por lo tanto podemos hablar de derivación $\delta_t: F \longrightarrow F$ con respecto de t.

Sea P un *place* de F/K de grado uno y $t \in F$ un elemento primo de P. Si $z \in F$ tiene la expansión P-adic $z = \sum_{i=n}^{\infty} a_i t^i$ con coeficientes $a_i \in K$, entonces:

$$dz/_{dt} = \sum_{i=n}^{\infty} i a_i t^{i-1}$$

Supongamos que P un *place* de F/K de grado uno y $t \in F$ un elemento primo de P. Si $z \in F$ tiene la expansión P-adic $z = \sum_{i=n}^{\infty} a_i t^i$ con $n \in \mathbb{Z}$ y $a_i \in K$, definimos su **residuo** con respecto a P y t por:

$$res_{P,t}(z) \coloneqq a_{-1}$$

Se cumple que $res_{P,t}: F \longrightarrow K$ es una aplicación K-lineal y $res_{P,t}(z) = 0$ si $v_P(z) \geq 0$.

Proposición: sean $s, t \in F$ elementos primos de P (donde P es un *place* de grado uno), entonces:

$$res_{P,s}(z) = res_{P,t}(z \cdot \frac{ds}{dt}) \text{ para todo } z \in F.$$

Sea $w \in \Delta_F$ un diferencial y $P \in \mathbb{P}_F$ un *place* de grado uno. Escogemos un elemento primo de P $t \in F$ y escribimos $w = udt$ con $u \in F$. Definimos el residuo de w en P como:

$$res_P(w) := res_{P,t}(u)$$

esta definición es independiente de la elección del elemento primo t.

Si F'/F es una extensión separable y finita de CFA definimos la **cotraza** $\omega' := Cotr_{F'/F}(\omega)$ de un diferencial Weil $\omega \in \Omega_F$; es un diferencial Weil de F' y, si F' y F tienen el mismo cuerpo de constantes, ω' se caracteriza por la condición

$$\omega_P(Tr_{F'/F}(y)) = \sum_{P'|P} \omega'_{P'}(y)$$

para todo $P \in \mathbb{P}_F$ e $y \in F'$

Anteriormente habíamos visto la existencia de un diferencial Weil específico η del cuerpo de funciones racionales $K(x)/K$ que está determinado únicamente por las siguientes propiedades: el divisor de η es $(\eta) = -2P_\infty$, y $\eta_{P_\infty}(x^{-1}) = -1$ (P_∞ es el polo de x en $K(x)$, y η_{P_∞} es la componente local de η en P_∞).

Sea F/K un CFA. Definimos la aplicación:

$$\delta: \begin{cases} F \longrightarrow \Omega_F \\ x \longmapsto \delta(x) \end{cases}$$

de la siguiente manera: si $x \in F \backslash K$ es un elemento separante de F/K hacemos

$$\delta(x) := Cotr_{F'/F}(\eta)$$

donde $\eta \in \Omega_{K(x)}$ es el diferencial Weil de $K(x)/K$ caracterizado anteriormente. Para un elemento no separante $x \in F$ definimos $\delta(x) \coloneqq 0$. Llamamos a $\delta(x)$ el diferencial Weil de F/K asociado a x.

Nótese que $\delta(x) \neq 0$ si x es separante, luego cada diferencial Weil $\omega \in \Omega_F$ se puede escribir como $\omega = z \cdot \delta(x)$ con $z \in F$.

Teorema [20]: supongamos que F/K es un CFA sobre un cuerpo perfecto K, y $x \in F$ es un elemento separante:

1) La aplicación $\delta: F \longrightarrow \Omega_F$ definida anteriormente es una derivación de F/K.

2) Para cada $y \in F$ se cumple:

$$\delta(y) = \frac{dy}{dx} \cdot \delta(x)$$

3) La aplicación

$$\mu: \begin{cases} \Delta_F \longrightarrow \Omega_F \\ zdx \longrightarrow z \cdot \delta(x) \end{cases}$$

es un isomorfismo del módulo de diferenciales Δ_F en Ω_F. Este isomorfismo es compatible con las derivaciones $d: F \longrightarrow \Delta_F$ y $\delta: F \longrightarrow \Omega_F$, esto significa que $\mu \circ d = \delta$.

4) Si $P \in \mathbb{P}_F$ es un *place* de F/K de grado uno y $\omega = z \cdot \delta(x) \in \Omega_F$, el componente local de ω en P viene dado por:

$\big(z \cdot \delta(x)\big)_P(u) = res_P(uzdx)$ en particular $\big(z \cdot \delta(x)\big)_P(1) = res_P(zdx)$

5) Si $\omega = z \cdot \delta(t) \in \Omega_F$ y t es un elemento primo del *place* P, se cumple entonces que $v_P(\omega) = v_P(z)$

Una consecuencia inmediata de este teorema es:

Corolario (**teorema del residuo**): sea F/K un CFA sobre un cuerpo algebraicamente cerrado, y sea $w \in \Delta_F$ un diferencial de F/K. Entonces $res_P(w) = 0$ para casi todos los *places* $P \in \mathbb{P}_F$ y

$$\sum_{P\in\mathbb{P}_F} res_P(w) = 0$$

Como consecuencia del teorema anterior hemos identificado el módulo de diferenciales Δ_F con el módulo Ω_F de diferenciales Weil de F/K. Esto significa que un diferencial $\omega = zdx \in \Delta_F$ es lo mismo que el diferencial Weil $\omega = z \cdot \delta(x) \in \Omega_F$ (donde $x \in F$ es separante y $z \in F$). En otras palabras:

$$\Delta_F = \Omega_F \quad \text{y} \quad zdx = z \cdot \delta(x)$$

Si $0 \neq \omega \in \Delta_F$ y t es un elemento primo del *place* $P \in \mathbb{P}_F$, podemos escribir $\omega = zdt$ con $z \in F$, y definimos

$$v_P(\omega) \coloneqq v_P(z) \quad \text{y} \quad (\omega) \coloneqq \sum_{P\in\mathbb{P}_F} v_P(\omega)\, P$$

La definición de $v_P(\omega)$ es independiente de la elección del elemento primo y es compatible con la identificación de Δ_F y Ω_F. Luego (ω) es justo el divisor del diferencial Weil correspondiente ω.

Como un caso especial e importante de los teoremas anteriores, obtenemos la siguiente fórmula para el divisor de un diferencial $\omega = zdx \neq 0$:

$$(zdx) = (z) + (dx) = (z) - 2(x)_\infty + Diff(F/K(x))$$

un caso particular de esta fórmula es

$$(dx) = -2(x)_\infty + Diff(F/K(x))$$

donde:

$$Diff(F'/F) \coloneqq \sum_{P\in\mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'$$

y

$$d(P'|P) \coloneqq -v_P(t)$$

3.3 CURVAS ALGEBRAICAS Y CUERPOS DE FUNCIONES

Como parte final de este capítulo, vamos a aplicar la teoría de los CFA, vista en las secciones 3.1 y 3.2, al estudio de las curvas algebraicas. Analizaremos las relaciones entre curvas algebraicas y cuerpos de funciones algebraicas. Para ello recurrimos de nuevo a nuestro texto de referencia para el estudio de los CFA: *"Henning Stichtenoth, Algebraic Function Fields and Codes"* [20].

Asumimos que K es un cuerpo algebraicamente cerrado.

El espacio afín n-dimensional $\boldsymbol{A}^n = \boldsymbol{A}^n(K)$ está formado por el conjunto de todas las n-tuplas de elementos de K. Un elemento $P = (a_1, \dots, a_n) \in \boldsymbol{A}^n$ es un punto, y $a_1, \dots, a_n$ son las coordenadas de P.

Sea $K[X_1, \dots, X_n]$ el anillo de polinomios en n variables sobre K. Un subconjunto $V \subseteq \boldsymbol{A}^n$ es un **conjunto algebraico** si existe un conjunto $M \subseteq K[X_1, \dots, X_n]$ tal que

$$V = \{P \in \boldsymbol{A}^n | \, F(P) = 0 \;\; para\ todo\ F \in M\}$$

Dado un conjunto algebraico $V \subseteq \boldsymbol{A}^n$, el conjunto de polinomios

$$I(V) = \{F \subseteq K[X_1, \dots, X_n] | \, F(P) = 0\ para\ todo\ P \in V\}$$

se denomina el **ideal** de V. Evidentemente $I(V)$ es un ideal en $K[X_1, \dots, X_n]$, y puede ser generado por un número finito de polinomios $F_1, \dots, F_r \in K[X_1, \dots, X_n]$. Luego tenemos

$$V = \{P \in \boldsymbol{A}^n | \, F_1(P) = \dots = F_r(P) = 0\}$$

Un conjunto algebraico $V \subseteq \boldsymbol{A}^n$ se denomina **irreducible** si no puede ser escrito como $V = V_1 \cup V_2$, donde $V_1\ y\ V_2$ son subconjuntos algebraicos propios de V. Equivalentemente, V es irreducible si y solo si el ideal correspondiente $I(V)$ es un ideal primo.

Una **variedad afín** es un conjunto algebraico irreducible $V \subseteq \boldsymbol{A}^n$.

El **anillo de coordenadas** de una variedad afín V es el anillo de clases de equivalencia $\Gamma(V) = K[X_1, \dots, X_n]/I(V)$. Como $I(V)$ es un ideal primo, $\Gamma(V)$ es un

dominio de integridad. Cada $f = F + I(V) \in \Gamma(V)$ induce una función $f: V \longrightarrow K$ haciendo $f(P) \coloneqq F(P)$ para $P \in V$. El cuerpo cociente

$$K(V) = Quot(\Gamma(V))$$

se denomina el cuerpo de funciones racionales (o cuerpo de funciones) de V. Contiene a K como subcuerpo. La dimensión de V es el grado de transcendencia de $K(V)/K$.

Para un punto $P \in V$ consideramos el anillo local

$$\mathcal{O}_P(V) = \left\{ f \in K(V) |\, f = \frac{g}{h} \; con \; g, h \; \in \Gamma(V) \; y \; h(P) \neq 0 \right\}$$

cuyo cuerpo de fracciones es $K(V)$, y su ideal máximal y único es

$$\mathrm{M}_P(V) = \left\{ f \in K(V) |\, f = \frac{g}{h} \; con \; g, h \; \in \Gamma(V) \; y \; h(P) \neq 0 \; y \; g(P) = 0 \right\}$$

$\mathcal{O}_P(V)$ es el **anillo local de V en P**. Para $f = {}^{g}/_{h} \in \mathcal{O}_P(V)$ con $h(P) \neq 0$, el valor de f en P se define como

$$f(P) \coloneqq {}^{g(P)}\Big/_{h(P)}$$

Estas definiciones de anillo local y su ideal maximal de una variedad afín son equivalentes a los conceptos de anillo de valuación y *place* (respectivamente) para el caso de cuerpos de funciones algebraicas (*páginas 27 a 29 de este texto*).

Variedades proyectivas: en el conjunto $\boldsymbol{A}^{n+1} \backslash \{0, \dots, 0\}$ definimos la relación de equivalencia $\sim$ mediante:

$(a_0, a_1, \dots, a_n) \sim (b_0, b_1, \dots, b_n) :\Leftrightarrow$ existe un elemento $0 \neq \lambda \in K$ tal que $b_i = \lambda a_i$ para $0 \leq i \leq n$.

La clase de equivalencia de $(a_0, a_1, \dots, a_n)$ con respecto a $\sim$ se denota por $(a_0 : a_1 : \dots : a_n)$. El **espacio proyectivo n-dimensional $\boldsymbol{P}^n = \boldsymbol{P}^n(K)$** es el conjunto de todas las clases de equivalencia:

$$\boldsymbol{P}^n = \{(a_0 : a_1 : \ldots : a_n) |\ a_i \in K, no\ todos\ los\ a_i = 0\ \}$$

Un elemento $P = (a_0 : a_1 : \ldots : a_n) \in \boldsymbol{P}^n$ es un punto y $a_0, a_1, \ldots, a_n$ se denominan las **coordenadas homogéneas** de P.

Un **monomio** de grado d es un polinomio $G \in K[X_0, \ldots, X_n]$ de la forma

$$G = a \cdot \prod_{i=0}^{n} X_i^{d_i} \quad \text{con } 0 \neq a \in K \quad \text{y} \quad \sum_{i=0}^{n} d_i = d$$

Un polinomio F es un **polinomio homogéneo** si F es la suma de monomios del mismo grado. Un ideal $I \subseteq K[X_0, \ldots, X_n]$ generado por un polinomio homogéneo de denomina **ideal homogéneo**.

Sea $P = (a_0 : a_1 : \ldots : a_n) \in \boldsymbol{P}^n$ y $F \in K[X_0, \ldots, X_n]$ un polinomio homogéneo. Decimos que $F(P) = 0$ si $F(a_0 : a_1 : \ldots : a_n) = 0$. Esto tiene sentido, pues como $F(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = \lambda^d \cdot F(a_0, a_1, \ldots, a_n)$ (con $d = degF$), se tiene que $F(a_0, a_1, \ldots, a_n) = 0 \Leftrightarrow F(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = 0$

Un subconjunto $V \subseteq \boldsymbol{P}^n$ es un **conjunto proyectivo algebraico** si existe un conjunto de polinomios homogéneos $M \subseteq K[X_0, \ldots, X_n]$ tales que

$$V = \{P \in \boldsymbol{P}^n |\ F(P) = 0\ para\ todo\ F \in M\}$$

El ideal $I(V) \subseteq K[X_0, \ldots, X_n]$ que es generado por todos los polinomios homogéneos F que cumplen $F(P) = 0$ se denomina ideal de V, que es un ideal homogéneo. Los conjuntos proyectivos algebraicos irreducibles se definen como en el caso afín, de nuevo $V \subseteq \boldsymbol{P}^n$ es irreducible si y solo si $I(V)$ es un ideal homogéneo y primo en $K[X_0, \ldots, X_n]$. Una **variedad proyectiva** es un conjunto proyectivo algebraico irreducible.

Dada una variedad no nula $V \subseteq \boldsymbol{P}^n$, se define su anillo de coordenadas homogéneas por

$$\Gamma_h(V) = K[X_0, \ldots, X_n]/I(V)$$

que es un dominio de integridad que contiene a K. Un elemento $f \in \Gamma_h(V)$ se denomina **forma** de grado d si $f = F + I(V)$ para algún polinomio homogéneo $F \in K[X_0, \ldots, X_n]$ con $degF = d$. El cuerpo de funciones de V de define como

$$K(V) \coloneqq \left\{\frac{g}{h} \mid g, h \in \Gamma_h(V) \; son \; formas \; del \; mismo \; grado \; y \; h \neq 0\right\}$$

que es un subcuerpo de $Quot(\Gamma_h(V))$, el cuerpo cociente de $\Gamma_h(V)$.

Como vimos anteriormente, la dimensión de V es el grado de transcendencia de $K(V)$ sobre K.

Sea $P = (a_0 \colon a_1 \colon \ldots \colon a_n) \in V$ y $f \in K(V)$. Escribimos $f = {}^{g}/_{h}$ donde $g = G + I(V), h = H + I(V) \in \Gamma_h(V)$ y G, H son polinomios homogéneos de grado d.

Como

$$\frac{G(\lambda a_0, \lambda a_1, \ldots, \lambda a_n)}{H(\lambda a_0, \lambda a_1, \ldots, \lambda a_n)} = \frac{\lambda^d \cdot G(a_0, a_1, \ldots, a_n)}{\lambda^d \cdot H(a_0, a_1, \ldots, a_n)} = \frac{G(a_0, a_1, \ldots, a_n)}{H(a_0, a_1, \ldots, a_n)}$$

podemos definir $f(P) \coloneqq G(a_0, a_1, \ldots, a_n)/H(a_0, a_1, \ldots, a_n) \in K$ si $H(P) \neq 0$. Decimos entonces que f está definida en P y denominamos a $f(P)$ el valor de f en P. El anillo

$$\mathcal{O}_P(V) = \{f \in K(V) \mid f \; está \; definida \; en \; P\} \subseteq K(V)$$

es un anillo local con ideal maximal

$$\mathrm{M}_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}$$

Recubrimiento de variedades proyectivas por variedades afines: para $0 \leq i \leq n$ consideramos la aplicación $\varphi_i \colon \boldsymbol{A}^n \longrightarrow \boldsymbol{P}^n$ dada por

$$\varphi_i(a_0, \ldots, a_{n-1}) = (a_0 \colon \ldots \colon a_{n-1} \colon 1 \colon a_i \colon \ldots \colon a_{n-1})$$

que es una biyección de $\boldsymbol{A}^n$ en el conjunto

$$U_i = \{(c_0 \colon \ldots \colon c_n \in \boldsymbol{P}^n \mid c_i \neq 0\}$$

y $\boldsymbol{P}^n = \bigcup_{i=0}^{n} U_i$. Luego $\boldsymbol{P}^n$ se recubre por $n+1$ copias del espacio afín $\boldsymbol{A}^n$ (no es una unión disjunta).

Sea $V \subseteq \boldsymbol{P}^n$ una variedad proyectiva, entonces $V = \cup_{i=0}^{n}(V \cap U_i)$. Supongamos que $V \cap U_i \neq 0$, tenemos que

$$V_i \coloneqq \varphi_i^{-1}(V \cap U_i) \subseteq \boldsymbol{A}^n$$

es una variedad afín, y el ideal $I(V_i)$ viene dado por

$$I(V_i) = \left\{F\left(X_0, \dots, X_{i-1,}1\,, X_{i+1}, \dots, X_n\right| F \in I(V)\right\}$$

Por conveniencia a partir de ahora nos vamos a restringir al caso $i = n$ (y $V \cap U_n \neq 0$). El complemento $H_n = \boldsymbol{P}^n \backslash U_n = \{(a_0 \colon \dots \colon a_n) \in \boldsymbol{P}^n |\, a_n = 0\}$ se denomina hiperplano del infinito, y los puntos $P \in V \cap H_n$ son los **puntos** de V **en el infinito**.

Existe un K-isomorfismo natural α desde $K(V)$ (el cuerpo de funciones de la variedad proyectiva V) en $K(V_n)$ (el cuerpo de funciones de la variedad afín $V_n = \varphi_n^{-1}(V \cap U_n)$). Este isomorfismo se define de la siguiente manera: sea $f = {}^{g}/_{h} \in K(V)$, donde $g, h \in \Gamma_h(V)$ son formas del mismo grado y $h \neq 0$. Escogemos polinomios homogéneos $G, H \in K[X_0, \dots, X_n]$ que representan a g resp. h. Sea $G_* = G(X_0, \dots, X_{n-1,}1)$ y $H_* = H(X_0, \dots, X_{n-1}, 1) \in K[X_0, \dots, X_{n-1}]$. Sus clases de equivalencia en $\Gamma(V_n) = K[X_0, \dots, X_{n-1}]/I(V_n)$ son g_* resp. h_*. Entonces $\alpha(f) = {}^{g_*}/_{h_*}$. Bajo este isomorfismo el anillo local de un punto $P \in V \cap V_n$ se mapea al anillo local de $\varphi_n^{-1}(P) \in V_n$, luego ambos anillos locales son isomorfos.

El **cierre proyectivo de una variedad afín**: para un polinomio $F = F(X_0, \dots, X_{n-1}) \in K[X_0, \dots, X_{n-1}]$ de grado d hacemos

$$F^* = X_n^d \cdot F(\tfrac{X_0}{X_n}, \dots, \tfrac{X_{n-1}}{X_n}) \in K[X_0, \dots, X_n]$$

F^* es un polinomio homogéneo de grado d en $n + 1$ variables.

Consideremos ahora una variedad afín $V \subseteq \boldsymbol{A}^n$ y su ideal correspondiente $I(V) \subseteq K[X_0, \dots, X_{n-1}]$. Definimos una variedad proyectiva $\bar{V} \subseteq \boldsymbol{P}^n$ de la siguiente manera:

$$\bar{V} = \{P \in \boldsymbol{P}^n |\, F^*(P) = 0 \;\; para\; todo\; F \in I(V)\}$$

Esta variedad $\bar{V}$ se denomina el cierre proyectivo de V. Se puede recuperar V desde $\bar{V}$ mediante:

$$V = \varphi_n^{-1}(\bar{V} \cap U_n) = (\bar{V})_n$$

En consecuencia los cuerpos de funciones de V y $\bar{V}$ son isomorfos de forma natural y V y $\bar{V}$ tienen la misma dimensión.

Sean $V \subseteq \boldsymbol{P}^m$ y $W \subseteq \boldsymbol{P}^n$ variedades proyectivas. Supongamos que $F_0, \dots, F_n \in K[X_0, \dots, X_m]$ son polinomios homogéneos con la propiedades siguientes:

1) $F_0, \dots, F_n$ tienen el mismo grado.

2) No todos los F_i están en $I(V)$.

3) Para todo $H \in I(W)$ se cumple que $H(F_0, \dots, F_n) \in I(W)$.

Sea $Q \in V$ y asumimos que $F_i(Q) \neq 0$ para al menos un $i \in \{0, \dots, n\}$ (por 2) tal punto existe). Entonces el punto $(F_0(Q) \colon \dots \colon F_n(Q)) \in \boldsymbol{P}^n$ se encuentra en W. Sea $(G_0, \dots, G_n)$ otra n-tupla de polinomios homogéneos que satisfacen las tres condiciones anteriores. Decimos que $(F_0, \dots, F_n)$ y $(G_0, \dots, G_n)$ son equivalentes si

4) $F_i G_j \equiv F_i G_j mod I(V)$ para $0 \leq i, j \leq n$.

la clase de equivalencia de $(F_0, \dots, F_n)$ con relación a la relación de equivalencia se denota por

$$\phi = (F_0 \colon \dots \colon F_n)$$

a ϕ se le llama **aplicación racional** de V a W.

Una aplicación racional $\phi = (F_0 \colon \dots \colon F_n)$ es regular (o definida) en el punto $P \in V$ si existen polinomios homogéneos $G_0, \dots, G_n \in K[X_0, \dots, X_m]$ tales que $\phi = (G_0 \colon \dots \colon G_n)$ y $G_i(P) \neq 0$ para al menos un i. Definimos entonces

$$\phi(P) = (G_0(P) \colon \dots \colon G_n(P)) \in W$$

que está bien definida por 1) y 2).

Dos variedades $V_1 \, y \, V_2$ son **biracionalmente equivalentes** si existen aplicaciones racionales $\phi_1 \colon V_1 \longrightarrow V_2$ y $\phi_2 \colon V_2 \longrightarrow V_1$ tales que $\phi_1 \circ \phi_2$ y $\phi_2 \circ \phi_1$ son la aplicación

identidad en V_2 y V_1 respectivamente. Se cumple que V_1 y V_2 son biracionalmente equivalentes si y solo si sus cuerpos de funciones $K(V_1)$ y $K(V_2)$ son K-isomorfos (*ver* [20]).

Una aplicación racional $\phi: V \longrightarrow W$ que es regular en todos los puntos $P \in V$ se denomina un **morfismo**. Se llama isomorfismo si existe un morfismo $\psi: W \longrightarrow V$ tal que $\phi \circ \psi$ y $\psi \circ \phi$ son la identidad en W y V respectivamente. En este caso se dice que V y W son isomorfas. Isomorfismo implica equivalencia biracional, pero lo contrario no es cierto en general.

Pasamos al estudio de las curvas, de gran transcendencia en nuestro trabajo, para ello seguimos apoyándonos en [20].

Curvas algebraicas: una curva algebraica proyectiva (afín) V es una variedad proyectiva (afín) de dimensión uno. Esto significa que el cuerpo $K(V)$ de funciones racionales en V es un cuerpo de funciones algebraicas de una variable.

Un punto $P \in V$ es **no singular** (o simple) si el anillo local $\mathcal{O}_P(V)$ es un anillo de valuación discreta (i.e. $\mathcal{O}_P(V)$ es un dominio de ideales principales con un ideal maximal y único $\neq 0$, que es lo que denominamos *place*). Solo existe un número finito de puntos singulares en una curva. La curva V se denomina no singular si todos los puntos $P \in V$ son no singulares.

Una **curva plana afín** es una curva afín $V \subseteq \boldsymbol{A}^2$. Su ideal $I(V) \subseteq K[X_0, X_1]$ es generado por un polinomio irreducible $G \in K[X_0, X_1]$ (que es único hasta un factor constante). Por el contrario, dado un polinomio irreducible $G \in K[X_0, X_1]$, el conjunto $V = \{P \in \boldsymbol{A}^2 |\ G(P) = 0\}$ es una curva plana afín y G genera el correspondiente ideal $I(V)$. Un punto $P \in V$ es no singular si y solo si

$$G_{X_0}(P) \neq 0 \quad \text{o} \quad G_{X_1}(P) \neq 0 \ \text{ (o ambas)}$$

donde $G_{X_i} \in K[X_0, X_1]$ es la derivada parcial de G con respecto a X_i (criterio de *Jacobi*).

De la misma manera, el ideal de una **curva plana proyectiva** $V \subseteq \boldsymbol{P}^2$ está generado por un polinomio homogéneo irreducible $H \in K[X_0, X_1, X_2]$. Un punto $P \in V$ es no singular si y solo si $H_{X_i}(P) \neq 0$ para al menos una $i \in \{0, 1, 2\}$.

Si $V = \{P \in \boldsymbol{A}^2 | \, G(P) = 0\}$ es una curva plana afín (con un polinomio irreducible $G \in K[X_0, X_1]$ de grado d), el cierre proyectivo $\bar{V} \subseteq \boldsymbol{P}^2$ es el conjunto de ceros del polinomio homogéneo $G^* = X_2^d \cdot G(\frac{X_0}{X_2}, \frac{X_1}{X_2})$.

Aplicaciones entre curvas: vamos a considerar la aplicación racional $\phi: V \longrightarrow W$ donde V y W son curvas proyectivas. Se cumple lo siguiente:

1) ϕ está definida en todos los puntos no singulares $P \in V$. Luego si V es una curva no singular entonces ϕ es un morfismo.

2) Si V es no singular y ϕ no es la aplicación constante, entonces ϕ es sobreyectiva.

Sea V una curva proyectiva. Existe entonces una curva proyectiva no singular V' y un morfismo biracional $\phi': V' \longrightarrow V$. El par (V', ϕ') es único en el sentido siguiente: dada otra curva no singular V'' y un morfismo biracional $\phi'': V'' \longrightarrow V$, existe entonces un único isomorfismo $\phi: V' \longrightarrow V''$ tal que $\phi' = \phi'' \circ \phi$. De esta manera se define a V' (más precisamente, al par (V', ϕ')) como el **modelo no singular de $\boldsymbol{V}$**.

Si $\phi': V' \longrightarrow V$ es el modelo no singular de V y $P \in V$ es no singular, existe un único $P' \in V'$ con $\phi'(P') = P$; para un punto singular $P \in V$ el número de $P' \in V'$ con $\phi'(P') = P$ es finito (puede ser uno).

La curva asociada a un cuerpo de funciones algebraicas: partiendo de un cuerpo de funciones algebraicas de una variable F/K, existe una curva proyectiva no singular V (única hasta isomorfismos) cuyo cuerpo de funciones $K(V)$ es (K-isomorfo) F. Se puede construir V de la siguiente forma: elegimos $x, y \in F$ tales que $F = K(x, y)$. Sea $G(X, Y) \in K[X, Y]$ el polinomio irreducible que cumple $G(x, y) = 0$. Sea $W = \{P \in \boldsymbol{A}^2 | \, G(P) = 0\}$ y $\bar{W} \subseteq \boldsymbol{P}^2$ el cierre proyectivo de W. Sea V el modelo no singular de $\bar{W}$; entonces $K(V) \simeq F$.

Sea V una curva proyectiva no singular y $F = K(V)$ su cuerpo de funciones. Existe una correspondencia uno a uno entre los puntos $P \in V$ y los *places* de F/K, dada por

$$P \mapsto M_P(V)$$

que es el ideal maximal del anillo local $\mathcal{O}_P(V)$. Esta correspondencia hace posible la traducción de definiciones y resultados obtenidos mediante la teoría de CFA a las curvas algebraicas (y viceversa). Damos varios ejemplos:

1) El género de una curva V es el género de cuerpo de funciones $K(V)$.

2) Un divisor de V (*como hemos visto en la sección 3.1, páginas 29 y 30*) es una suma formal $D = \sum_{P \in V} n_P P$ donde $n_P \in \mathbb{Z}$ y casi todos los n_P son nulos. El grado de D es $degD = \sum_{P \in V} n_P$. Los divisores de V forman un grupo aditivo $Div(V)$.

3) El orden de una función racional en el punto $P \in V$ se define como $v_P(f)$, donde v_P es la valuación discreta de $K(V)$ correspondiente al anillo de valuación $\mathcal{O}_P(V)$.

4) El divisor principal (f) de una función racional $0 \neq f \in K(V)$ es $(f) = \sum_{P \in V} v_P(f)P$. El grado de un divisor principal es cero.

5) Los divisores principales forman un subgrupo $Princ(V)$ del grupo de divisores $Div(V)$. El grupo cociente $Jac(V) = Div^0(V)/Princ(V)$, donde $Div^0(V)$ es el grupo de divisores de grado cero se denomina ***Jacobiano*** de V.

6) Para $D \in Div(V)$, el espacio $\mathcal{L}(D)$ se define como en el caso de cuerpos de funciones. Es un espacio vectorial de dimensión finita sobre K. Su dimensión viene dada por el teorema de Riemann-Roch.

Sea $\overline{K} \supseteq K$ el cierre algebraico de K, se dice que una variedad afín $V \subseteq \boldsymbol{A}^n(\overline{K})$ está definida sobre K si su ideal $I(V) \subseteq \overline{K}[X_1, \dots, X_n]$ puede ser generado por polinomios $F_1, \dots, F_r \in K[X_1, \dots, X_n]$. Si V está definido sobre K, el conjunto

$$V(K) = V \cap \boldsymbol{A}^n(K) = \{P = (a_1, \dots, a_n) \in V | \; todos \; los \; a_i \; \in K\}$$

se denomina el **conjunto de los puntos $\boldsymbol{K}$-racionales de $\boldsymbol{V}$**.

De forma similar, una variedad proyectiva $V \subseteq \boldsymbol{P}^n(\overline{K})$ está definida sobre K si $I(V)$ está generado por polinomios homogéneos $F_1, \dots, F_r \in K[X_0, \dots, X_n]$. Un punto $P \in V$ se denomina K-racional si existen coordenadas homogéneas $a_0, \dots, a_n$ de P que pertenecen a K, y definimos

$$V(K) = \{P \in V | \; P \; es \; K - \text{racional}\}$$

Sea $V \subseteq \boldsymbol{A}^n(\overline{K})$ una variedad afín definida sobre K. Definimos el ideal

$$I(V/K) = I(V) \cap K[X_1, \dots, X_n]$$

y el anillo de clases de equivalencia

$$\Gamma(V/K) = K[X_1, \dots, X_n]/I(V/K)$$

el cuerpo cociente

$$K(V) = Quot(\Gamma(V/K)) \subseteq \overline{K}(V)$$

es el **cuerpo de las funciones $\boldsymbol{K}$-racionales de $\boldsymbol{V}$**. La extensión de cuerpos $K(V)/K$ es finita y su grado de transcendencia es la dimensión de V. De la misma manera se define el cuerpo de funciones K-racionales de una variedad proyectiva.

Consideremos ahora dos variedades $V \subseteq \boldsymbol{P}^m(\overline{K})$ y $W \subseteq \boldsymbol{P}^n(\overline{K})$. Una aplicación racional $\phi: V \longrightarrow W$ está definida sobre K si existen polinomios homogéneos $F_0, \dots, F_n \in K[X_1, \dots, X_m]$ que satisfagan las condiciones vistas cuando definimos las aplicaciones racionales de forma que $\phi = (F_0: \dots : F_n)$.

Otra manera de describir los puntos K-racionales, las funciones K-racionales, etc. en una variedad que está definida sobre K es la siguiente: sea $Gal(\overline{K}/K)$ el grupo de *Galois* de $\overline{K}/K$ (*ver página 22*). La acción de $Gal(\overline{K}/K)$ en $\overline{K}$ se extiende de forma natural a una acción en los conjuntos $\boldsymbol{A}^n(\overline{K})$, $\boldsymbol{P}^n(\overline{K})$, $\overline{K}[X_1, \dots, X_n]$, V, $\Gamma(V)$, $\overline{K}(V)$, etc. Si consideramos una variedad proyectiva $V \subseteq \boldsymbol{P}^n(\overline{K})$ (definida sobre K), un punto $P = (a_0: \dots : a_n) \in V$ y un automorfismo $\sigma \in Gal(\overline{K}/K)$; entonces $P^\sigma = ({a_0}^\sigma: \dots : {a_n}^\sigma)$. Se comprueba fácilmente que

$$V(K) = \{P \in V |\ P^\sigma = P\ para\ todo\ \sigma \in Gal(\overline{K}/K)\}$$

$$K(V) = \{f \in \overline{K}(V) |\ f^\sigma = f\ para\ todo\ \sigma \in Gal(\overline{K}/K)\}$$

y así para el resto

Consideramos ahora una curva proyectiva $V \subseteq \boldsymbol{P}^n(\overline{K})$ que está definida sobre K (donde K es perfecto y $\overline{K}$ es el cierre algebraico de K). Tenemos entonces que el cuerpo $K(V)$ de funciones K-racionales en V es un cuerpo de funciones

algebraicas de una variable sobre K, y $\overline{K}(V)$ es la extensión de cuerpos constante de $K(V)$ con $\overline{K}$.

Un divisor $D = \sum_{P \in V} n_P P \in Div(V)$ está definido sobre K si $D^\sigma = D$ para todo $\sigma \in Gal(\overline{K}/K)$ (esto significa que $n_{P^\sigma} = n_P$ para todo $P \in V$). Los divisores de V definidos sobre K forman un subgrupo $Div(V/K) \subseteq Div(V)$. Para un divisor $D \in Div(V/K)$ el espacio $\mathcal{L}_K(D)$ viene dado por

$$\mathcal{L}_K(D) = K(V) \cap \mathcal{L}(D)$$

que es un espacio K-vectorial de dimensión finita, y su dimensión (sobre K) es igual a la dimensión de $\mathcal{L}(D)$ (sobre $\overline{K}$).

Un divisor $Q \in Div(V/K)$ con $Q > 0$ se denomina **divisor primo** de V/K si Q no puede escribirse como $Q = Q_1 + Q_2$, con divisores efectivos $Q_1,\ Q_2 \in Div(V/K)$. Se comprueba fácilmente que el grupo de divisores $Div(V/K)$ es el grupo abeliano libre generado por los divisores primos. Los divisores primos de V/K se corresponden con los *places* del cuerpo de funciones $K(V)/K$; bajo esta correspondencia, divisores primos de grado uno (i.e., puntos K-racionales) de V se corresponden con los *places* de $K(V)/K$ de grado uno.

4 CÓDIGOS ALGEBRAICO-GEOMÉTRICOS (CÓDIGOS AG)

4.1 FUNDAMENTOS DE LA TEORÍA DE CÓDIGOS AG

Iniciamos un nuevo capítulo donde vamos a describir la construcción debida a Goppa de códigos de corrección de errores mediante el uso de CFA. Comenzamos con una sección donde hacemos un resumen de los conceptos de la teoría de codificación, para pasar posteriormente a definir los códigos algebraico-geométricos (códigos AG) y desarrollar sus propiedades principales.

Como texto de referencia para esta sección nos hemos basado en [20].

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. Consideramos el espacio vectorial n-dimensional $\mathbb{F}_q^n$ cuyos elementos son n-tuplas $a = (a_1, \dots, a_n)$ con $a_i \in \mathbb{F}_q$.

Para $a = (a_1, \dots, a_n)$ y $b = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ sea

$$d(a, b) \coloneqq |\{i;\ a_i \neq b_i\}|$$

esta función d se denomina la **distancia de *Hamming*** en $\mathbb{F}_q^n$. El **peso** de un elemento $a \in \mathbb{F}_q^n$ se define como:

$$wt(a) \coloneqq d(a, 0) = |\{i;\ a_i \neq 0\}|$$

Se puede verificar de forma sencilla que la distancia de Hamming es un métrica en $\mathbb{F}_q^n$. En particular, se cumple la desigualdad triangular para todo $a, b, c \in \mathbb{F}_q^n$:

$$d(a, c) \leq d(a, b) + d(b, c)$$

Un **código** C (sobre el alfabeto $\mathbb{F}_q$) es un subespacio linear de $\mathbb{F}_q^n$; los elementos de C se denominan **palabras del código**. Denominamos a n la **longitud** de C y $dim C$ (como espacio $\mathbb{F}_q$-vectorial) la **dimensión** de C. Un código $[n, k]$ es un código de longitud n y dimensión k.

Se define la **distancia mínima** $d(C)$ de un código $C \neq 0$ como:

$$d(C) \coloneqq min\{d(a,b)|\ a,b\ \in C\ y\ a \neq b\} = min\{wt(c)|\ 0 \neq c \in C\}$$

Un código $[n,k]$ código con distancia mínima d se denota como un código $[n,k,d]$.

Sea C un código $[n,k]$ sobre $\mathbb{F}_q$. Una **matriz generadora** de C es una matriz $k \times n$ cuyas filas constituyen un base de C.

Se define el **producto interior canónico** en $\mathbb{F}_q^n$ por:

$$\langle a,b\rangle \coloneqq \sum_{i=1}^{n} a_i b_i$$

para $a = (a_1, \dots, a_n)$ y $b = (b_1, \dots, b_n) \in \mathbb{F}_q^n$

Si $C \subseteq \mathbb{F}_q^n$ es un código entonces:

$$C^{\perp} \coloneqq \left\{u \in \mathbb{F}_q^n |\ \langle u,c\rangle = 0\ para\ todo\ c \in C\right\}$$

se llama el **código dual** de C. El código C se denomina **auto-dual** (resp. auto ortogonal) si $C = C^{\perp}$ (resp. $C \subseteq C^{\perp}$).

Es conocido del álgebra lineal que el dual de un código $[n,k]$ es un código $[n, n-k]$, y que $(C^{\perp})^{\perp} = C$. En particular, la dimensión de un código auto-dual de longitud n es $n/2$.

Una matriz generadora H de $C^{\perp}$ se denomina **matriz de comprobación de paridad** para C.

Se demuestra fácilmente que una matriz de comprobación de paridad H de un código C $[n,k]$ es una matriz $(n-k) \times n$ de rango $(n-k)$, y que:

$$C = \left\{u \in \mathbb{F}_q^n |\ H \cdot u^t = 0\right\}$$

(donde u^t denota el transpuesto de u). Luego un matriz de comprobación de paridad "comprueba" si un vector $u \in \mathbb{F}_q^n$ es una palabra del código o no.

Uno de los problemas básicos de la teoría de codificación algebraica es construir códigos sobre un alfabeto determinado $\mathbb{F}_q$ cuya dimensión y distancia mínima son grandes en comparación con su longitud. Sin embargo existen ciertas restricciones. En otras palabras, si la dimensión de un código es grande (con relación a su longitud), entonces su distancia mínima es pequeña. La restricción más simple es la siguiente:

(Límite de Singleton). Para un código $[n, k, d]$ se cumple:

$$k + d \leq n + 1$$

demostración: consideremos el subespacio lineal $E \subseteq \mathbb{F}_q^n$ dado por

$$E \coloneqq \{(a_1, \dots, a_n) \in \mathbb{F}_q^n | \; a_i = 0 \; para \; todo \; i \geq d\}$$

cada $a \in E$ tiene peso $\leq d - 1$, luego $E \cap C = 0$. Como $dimE = d - 1$ se obtiene:

$$k + (d - 1) = dimC + dimE = \dim(C + E) + \dim(C \cap E) = \dim(C + E) \leq n$$

Códigos con $k + d = n + 1$ son óptimos en cierto sentido; tales códigos se denominan **códigos $\boldsymbol{MDS}$** (*maximum distance separable codes*).

En general es un problema de mayor dificultad encontrar límites inferiores para la distancia mínima de un código dado (o una clase de códigos dada). Solo en pocos casos de clases son conocidos. Una de las razones por el interés en los códigos AG es que para esta gran clase de códigos se obtiene un buen límite inferior para la distancia mínima.

Los códigos AG fueron introducidos por V.D. Goppa en [6]. Como una motivación para la construcción de dichos códigos vamos a estudiar primero los **códigos Reed-Salomon** sobre $\mathbb{F}_q$. Esta clase importante de códigos ha gozado de gran popularidad durante un largo periodo de tiempo. Los códigos AG son una generalización natural de estos códigos. Para su estudio utilizamos como referencia el texto de Stichtenoth [20].

Sea $n = q - 1$ y $\beta \in \mathbb{F}_q$ un elemento primitivo del grupo multiplicativo $\mathbb{F}_q^\times$; i.e. $\mathbb{F}_q^\times = \{\beta, \beta^2, \dots, \beta^n = 1\}$. Para un entero k con $1 \leq k \leq n$ consideramos el espacio vectorial k-dimensional:

$$\mathcal{L}_k \coloneqq \{f \in \mathbb{F}_q[X] | \; degf \leq k - 1\}$$

y la aplicación de evaluación $ev: \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ dada por

$$ev(f) \coloneqq (f(\beta), f(\beta^2), \dots, f(\beta^n)) \in \mathbb{F}_q^n$$

obviamente esta aplicación es $\mathbb{F}_q$-linear e inyectiva, porque un polinomio no nulo $f \in \mathbb{F}_q[X]$ de grado $< n$ tiene menos de n ceros. Luego:

$$C_k \coloneqq \{(f(\beta), f(\beta^2), \dots, f(\beta^n)) | \, f \in \mathcal{L}_k\}$$

es un $[n, k]$ sobre $\mathbb{F}_q$; se denomina código RS (Reed-Salomon). El peso de una palabra de código $0 \neq c = ev(f) \in C_k$ viene dado por:

$$wt(c) = n - |\{i \in \{1, \dots, n\}; f(\beta^i) = 0\}| \geq n - degf \geq n - (k-1)$$

luego la distancia mínima d de C_k satisface la desigualdad $d \geq n + 1 - k$. Por otro se cumple que $d \leq n + 1 - k$, por el límite de Singleton. Por lo tanto los códigos RS son códigos MDS sobre $\mathbb{F}_q$. Se observa sin embargo que los códigos RS son cortos en comparación con el tamaño del alfabeto $\mathbb{F}_q$, pues $n = q - 1$.

Introducimos ahora la noción de código AG. Establecemos cierta notación que va a ser válida para esta sección:

$F/\mathbb{F}_q$ es un CFA de género g

$P_1, \dots, P_n$ son *places* distintas dos a dos de $F/\mathbb{F}_q$ de grado 1

$D = P_1 + \dots + P_n$

G es un divisor de $F/\mathbb{F}_q$ tal que $suppG \cap suppD = 0$

El código algebraico-geométrico (o **código AG**) $C_{\mathcal{L}}(D, G)$ asociado a los divisores D y G se define por:

$$C_{\mathcal{L}}(D, G) \coloneqq \{(x(P_1), \dots, x(P_n)) | \, x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

Esta definición tiene sentido (*estamos usando la notación de las secciones 3.1 y 3.2 para las valuaciones y divisores*) ya que para $x \in \mathcal{L}(G)$ se cumple que $v_{P_i}(x) \geq 0 \;\; (i = 1, \dots, n)$ pues $suppG \cap suppD = 0$. La clase de equivalencia $x(P_i)$ de x módulo P_i es un elemento del cuerpo de clases de equivalencia de P_i. Como $degP_i = 1$, esta grupo de clases de equivalencia es $\mathbb{F}_q$, luego $x(P_i) \in \mathbb{F}_q$.

Consideremos ahora la aplicación de evaluación $ev_D: \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ dada por:

$$ev_D(x) \coloneqq (x(P_1), \dots, x(P_n)) \in \mathbb{F}_q^n$$

Esta aplicación de evaluación es $\mathbb{F}_q$-linear y $C_{\mathcal{L}}(D,G)$ es la imagen de $\mathcal{L}(G)$ mediante esta aplicación. La analogía con los códigos RS es obvia. De hecho, escogiendo adecuadamente el CFA $F/\mathbb{F}_q$ y los divisores D y G, se comprueba con facilidad que los códigos RS son un caso especial de códigos AG.

Aunque la definición de los códigos AG parezca, en ciertos sentido, artificial, el teorema que veremos a continuación mostrará por qué estos códigos son interesantes: se pueden calcular (o al menos estimar) sus parámetros n, k y d mediante el teorema de Riemann-Roch, y se puede obtener un límite inferior no trivial para la distancia mínima en el caso de una configuración de carácter general.

Teorema (*ver* [20]): $C_{\mathcal{L}}(D,G)$ es un código $[n,k,d]$ con parámetros

$$k = \ell(G) - \ell(G-D) \text{ y } d \geq n - degG$$

Corolario: supongamos que el grado de G es estrictamente menor que n. Entonces la aplicación de evaluación $ev_D: \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D,G)$ es inyectiva y se cumple:

1) $C_{\mathcal{L}}(D,G)$ es un código $[n,k,d]$ con

$$d \geq n - degG \quad \text{y} \quad k = \ell(G) \geq degG + 1 - g$$

luego

$$k + d \geq n + 1 - g$$

2) Adicionalmente, si $2g - 2 < degG < n$, entonces $k = degG + 1 - g$

3) Si $\{x_1, \ldots, x_k\}$ es una base de $\mathcal{L}(G)$, entonces la matriz

$$M = \begin{pmatrix} x_1(P_1) & \cdots & x_1(P_n) \\ \vdots & \ddots & \vdots \\ x_k(P_1) & \cdots & x_k(P_n) \end{pmatrix}$$

es una matriz generadora de $C_{\mathcal{L}}(D,G)$.

Demostración del corolario: por asunción tenemos que $\deg(G-D) = degG - n < 0$, luego $\mathcal{L}(G-D) = 0$. Como $\mathcal{L}(G-D)$ es el núcleo de la aplicación de evaluación, es una aplicación inyectiva. El resto de aserciones son consecuencias triviales del teorema anterior y el de Riemann-Roch.

Se observa que el límite inferior para la distancia mínima visto anteriormente:

$$k + d \geq n + 1 - g$$

es muy similar al límite superior de Singleton, si ponemos ambos límites juntos, vemos que para $degG < n$,

$$n + 1 - g \leq k + d \leq n + 1$$

se observa que $k + d = n + 1$ si F es un CFA de género $g = 0$. Luego los códigos AG construidos mediante un cuerpo de funciones racionales $\mathbb{F}_q(z)$ son siempre códigos MDS.

El entero $d^* \coloneqq n - degG$ se denomina la **distancia de diseño** del código $C_{\mathcal{L}}(D, G)$.

El teorema anterior establece que la mínima distancia d de un código AG no puede ser inferior que su distancia de diseño.

Se puede asociar otro código con los divisores G y D utilizando componentes locales de diferenciales de Weil. Vamos a recordar la notación introducida en la sección 3.1. Para un divisor $A \in Div(F)$, $\Omega_F(A)$ es el espacio de diferenciales de Weil ω con $(\omega) \geq A$, que es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión finita $i(A)$ (índice de especialidad de A). Para un diferencial de Weil ω y un *place* $P \in \mathbb{P}_F$, la aplicación $\omega_P: F \longrightarrow \mathbb{F}_q$ define la componente local de ω en P.

Sean G y $D = P_1 + \ldots + P_n$ los divisores definidos anteriormente (i.e., los P_i son *places* de grado uno distintas dos a dos y $suppG \cap suppD = 0$). Entonces definimos el código $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ por

$$C_\Omega(D, G) \coloneqq \left\{ \left(\omega_{P_1}(1), \ldots, \omega_{P_n}(1) \right) \mid \omega \in \Omega_F(G - D) \right\}$$

se denomina también a $C_\Omega(D, G)$ un código AG. La relación entre los códigos $C_{\mathcal{L}}(D, G)$ y $C_\Omega(D, G)$ la explicaremos a continuación.

Teorema [20]: $C_\Omega(D, G)$ es un código $[n, k', d']$ con parámetros:

$$k' = i(G - D) - i(G) \quad \text{y} \quad d' \geq degG - (2g - 2)$$

bajo la hipótesis adicional $degG > 2g - 2$, se tiene

$$k' = i(G - D) \geq n + g - 1 - degG$$

si además $2g - 2 < degG < n$ entonces

$$k' = n + g - 1 - degG$$

Análogamente al caso de los códigos $C_{\mathcal{L}}(D,G)$, el entero $degG-(2g-2)$ se denomina la distancia de diseño de $C_{\Omega}(D,G)$.

Existe una relación estrecha entre los códigos $C_{\mathcal{L}}(D,G)$ y $C_{\Omega}(D,G)$, para encontrarla, trasladamos los resultados de la sección 3.1 al ejemplo de códigos AG obtenidos a partir de CFA.

Así, tenemos los siguientes resultados (*ver* [20]):

Teorema: los códigos $C_{\mathcal{L}}(D,G)$ y $C_{\Omega}(D,G)$ son respectivamente duales:

$$C_{\Omega}(D,G)=C_{\mathcal{L}}(D,G)^{\perp}$$

Lema: existe un diferencial de Weil η tal que

$$v_{P_i}(\eta)=-1 \quad \text{y} \quad \eta_{P_i}(1)=1 \quad \text{para } i=1,\dots,n$$

Proposición: sea η un diferencial de Weil tal que $v_{P_i}(\eta)=-1$ y $\eta_{P_i}(1)=1$ para $i=1,\dots,n$. Entonces

$$C_{\mathcal{L}}(D,G)^{\perp}=C_{\Omega}(D,G)=C_{\mathcal{L}}(D,H) \quad \text{con} \quad H\coloneqq D-G+(\eta)$$

Corolario: supongamos que existe un diferencial de Weil η tal que

$$2G-D\leq(\eta) \quad \text{y} \quad \eta_{P_i}(1)=1 \quad \text{para } i=1,\dots,n$$

entonces el código $C_{\mathcal{L}}(D,G)$ es auto-ortogonal; i.e., $C_{\mathcal{L}}(D,G)\subseteq C_{\mathcal{L}}(D,G)^{\perp}$.

si

$$2G-D=(\eta) \quad \text{y} \quad \eta_{P_i}(1)=1 \quad \text{para } i=1,\dots,n$$

entonces el código $C_{\mathcal{L}}(D,G)$ es auto-dual.

Demostración del corolario: la asunción $2G-D\leq(\eta)$ es equivalente a $G\leq D-G+(\eta)$, luego la proposición anterior implica

$$C_{\mathcal{L}}(D,G)^{\perp}=C_{\mathcal{L}}\big(D,D-G+(\eta)\big)\supseteq C_{\mathcal{L}}(D,G)$$

esto prueba la primera aserción. Si asumimos la igualdad $2G-D=(\eta)$ entonces se cumple que $G=D-G+(\eta)$, por lo tanto

$$C_{\mathcal{L}}(D,G)^{\perp}=C_{\mathcal{L}}\big(D,D-G+(\eta)\big)=C_{\mathcal{L}}(D,G)$$

Se dice que dos códigos $C_1, C_2 \subseteq \mathbb{F}_q^n$ son **equivalentes** si existe un vector $a = (a_1, \dots, a_n) \in (\mathbb{F}_q^{\times})^n$ tal que $C_2 = a \cdot C_1$; i.e.,

$$C_2 = \{(a_1 c_1, \dots, a_n c_n) | \ (c_1, \dots, c_n) \in C_1\}$$

Evidentemente códigos equivalentes tienen la misma dimensión y la misma distancia mínima. Sin embargo, esta equivalencia no preserva todas las propiedades interesantes de un código. Por ejemplo, códigos equivalentes pueden tener grupos de automorfismos no isomorfos.

Proposición:

1) Supongamos que G_1 y G_2 son divisores con $G_1 \sim G_2$ y $suppG_1 \cap suppD = suppG_2 \cap suppD = 0$. Entonces los códigos $C_{\mathcal{L}}(D, G_1)$ y $C_{\mathcal{L}}(D, G_2)$ son equivalentes. Lo mismo se cumple para $C_{\Omega}(D, G_1)$ y $C_{\Omega}(D, G_2)$.

2) Al contrario, si un código $C \subseteq \mathbb{F}_q^n$ es equivalente a $C_{\mathcal{L}}(D, G)$ (resp. $C_{\Omega}(D, G)$) entonces existe un divisor $G \sim G'$ tal que $suppG' \cap suppD = 0$ y $C = C_{\mathcal{L}}(D, G')$ (resp. $C = C_{\Omega}(D, G')$).

4.2 MÁS ACERCA DE CÓDIGOS AG

Como ampliación del estudio de los códigos algebraico-geométricos, en esta sección trataremos principalmente la representación de los códigos $C_\Omega(D,G)$ basada en los residuos de diferenciales y los automorfismos de códigos AG; constituyendo estos últimos uno de los objetivos de este trabajo. Con este propósito, aplicaremos los conceptos de los CFA estudiados en la sección 3.2 de este texto, relativos a los diferenciales de CFA y sus residuos.

Como texto de referencia para esta sección nos hemos basado en [20].

Sea $P \in \mathbb{P}_F$ un *place* de grado uno y $\omega \in \Omega_F$ un diferencial Weil. Con anterioridad identificamos Ω_F con el módulo de diferenciales Δ_F. Con esta identificación las componentes locales de ω en el *place* P pueden ser calculadas mediante el residuo de ω en P, pues $\omega_P(u) = res_P(u\omega)$ para todo $u \in F$. En particular, se cumple que $\omega_P(1) = res_P(\omega)$. De esta manera tenemos la siguiente descripción alternativa del código $C_\Omega(D,G)$.

Proposición:

$$C_\Omega(D,G) = \left\{ \left(res_{P_1}(\omega), \dots, res_{P_n}(\omega) \right) \mid \omega \in \Omega_F(G-D) \right\}$$

Ésta es la representación más comúnmente usada en la literatura para definir el código $C_\Omega(D,G)$.

En la sección anterior vimos que el código $C_\Omega(D,G)$ puede también escribirse como $C_\mathcal{L}(D,H)$, donde $H = D - G + (\eta)$, siendo η un diferencial con $v_{P_i}(\eta) = -1$ y $\eta_{P_i}(1) = 1$ para $i = 1, \dots, n$. Utilizando conceptos descritos en la sección 3.2, podemos construir fácilmente el diferencial η.

Proposición: sea t un elemento de F tal que $v_{P_i}(t) = -1$ para $i = 1, \dots, n$.
Entonces se cumple lo siguiente:

1) El diferencial $\eta := {dt}/{t}$ satisface $v_{P_i}(\eta) = -1$ y $res_{P_i}(\eta) = 1$ para $i = 1, \dots, n$.

2) $C_\Omega(D,G) = C_\mathcal{L}(D, D - G + (dt) - (t))$.

Demostración: como t es un elemento primo de $P \coloneqq P_i$, la expansión P-adic en series de potencias de $\eta = {dt}/{t}$ con respecto a t es: $\eta = \frac{1}{t}dt$, luego $v_P(\eta) = -1$ y $res_P(\eta) = 1$. El segundo punto del teorema se obtiene sin dificultad de esto último y de lo visto en la sección previa.

Corolario: supongamos que $t \in F$ es un elemento primo para todos los *places* $P_1, \dots, P_n$.

1) Si $2G - D \leq ({dt}/{t})$ entonces el código $C_{\mathcal{L}}(D, G)$ es auto ortogonal; i.e.,

$$C_{\mathcal{L}}(D, G) \subseteq C_{\mathcal{L}}(D, G)^{\perp}$$

2) Si $2G - D = ({dt}/{t})$ entonces $C_{\mathcal{L}}(D, G)$ es auto-dual.

Automorfismos de códigos AG: el grupo simétrico $\mathcal{S}_n$ (cuyos elementos son permutaciones del conjunto $\{1, \dots, n\}$) actúa en el espacio vectorial $\mathbb{F}_q^n$ mediante

$\pi(c_1, \dots, c_n) \coloneqq (c_{\pi(1)}, \dots, c_{\pi(n)})$ para $\pi \in \mathcal{S}_n$ y $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$.

El grupo de automorfismos de un código $C \subseteq \mathbb{F}_q^n$ se define como

$$Aut(C) \coloneqq \{\pi \in \mathcal{S}_n | \, \pi(C) = C\}$$

Obviamente $Aut(C)$ es un subgrupo de $\mathcal{S}_n$. Muchos códigos interesantes tienen un grupo de automorfismos no trivial. A continuación estudiaremos los automorfismos de códigos AG que son inducidos por automorfismos del cuerpo de funciones correspondiente.

Sea $F/\mathbb{F}_q$ un cuerpo de funciones y $Aut(F/\mathbb{F}_q)$ el grupo de automorfismos de F sobre $\mathbb{F}_q$ (i.e., $\sigma(a) = a$ para $\sigma \in Aut(F/\mathbb{F}_q)$ y $a \in \mathbb{F}_q$, *ver página* 22). El grupo $Aut(F/\mathbb{F}_q)$ actúa en $\mathbb{P}_F$ de la siguiente manera: $\sigma(P) \coloneqq \{\sigma(x) | \, x \in P\}$

Las valuaciones v_P y $v_{\sigma(P)}$ correspondientes están relacionadas de la forma:

$$v_{\sigma(P)}(y) = v_P(\sigma^{-1}(y)) \quad \text{para todo } y \in F$$

además se cumple que $deg\sigma(P) = degP$ puesto que σ induce un isomorfismo en el cuerpo de clases de equivalencia de P y $\sigma(P)$ dado por:

$$\sigma\big(z(P)\big) \coloneqq \sigma(z)(\sigma(P))$$

la acción de $Aut\big(F/\mathbb{F}_q\big)$ en $\mathbb{P}_F$ se extiende a una acción en el grupo de divisores haciendo:

$$\sigma(\sum n_P P) \coloneqq \sum n_P \sigma(P)$$

Como hemos hecho anteriormente, consideramos divisores $D = P_1 + \cdots + P_n$ y G de $F/\mathbb{F}_q$, donde $P_1, \dots, P_n$ son *places* distintos de grado uno y $suppG \cap suppD = 0$.

Definimos:

$$Aut_{D,G}(F/\mathbb{F}_q) \coloneqq \{\sigma \in Aut\big(F/\mathbb{F}_q\big) |\, \sigma(D) = D \;\; y\, \sigma(G) = G\}$$

Obsérvese que un automorfismo $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$ no necesita fijar los *places* $P_1, \dots, P_n$, pero genera una permutación de $P_1, \dots, P_n$. Se demuestra fácilmente que

$$\sigma\big(\mathcal{L}(G)\big) = \mathcal{L}(G)$$

para $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$, ya que $\sigma(G) = G$. Vamos a ver ahora que todo automorfismo $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$ induce un automorfismo en el código correspondiente $C_{\mathcal{L}}(D, G)$.

Proposición [20]:

1) $Aut_{D,G}(F/\mathbb{F}_q)$ actúa en el código $C_{\mathcal{L}}(D, G)$ de la siguiente forma:

$$\sigma\Big(\big(x(P_1), \dots, x(P_n)\big)\Big) \coloneqq \big(x\big(\sigma(P_1)\big), \dots, x\big(\sigma(P_n)\big)\big)$$

   (para $x \in \mathcal{L}(G)$). Esto genera un homomorfismo de $Aut_{D,G}(F/\mathbb{F}_q)$ en $Aut(C_{\mathcal{L}}(D, G))$.

2) Si $n \geq 2g + 2$, el homomorfismo anterior es inyectivo. Luego $Aut_{D,G}(F/\mathbb{F}_q)$ puede considerarse como un subgrupo de $Aut(C_{\mathcal{L}}(D, G))$.

5 CURVAS $C_{a,b}$

En este capítulo vamos a describir las propiedades generales de las curvas $C_{a,b}$, que constituyen una amplia clase de curvas algebraicas, entre las que se incluyen, por ejemplo, las curvas elípticas, hiperelípticas y superelípticas. Dichas curvas han sido estudiadas por numerosos investigadores debido a sus interesantes propiedades (*ver* [21], [18], [2], [4], [7], [15], [13]).

Como paso previo a su estudio, incluiremos secciones introductorias relativas a conceptos como las superficies de Riemann, los espacios recubridores de una variedad, teoría de ramificación y tipos de curvas algebraicas, que emplearemos a la hora de describir las propiedades de las curvas $C_{a,b}$.

5.1 SUPERFICIES DE RIEMANN

En primer lugar, conviene reseñar la estrecha relación existente entre las superficies de Riemann y las curvas algebraicas complejas. Podemos decir que una superficie de Riemann compacta se puede ver como una curva algebraica en el espacio proyectivo (de hecho son lo mismo debido al functor de Riemann); también es sabido que dos curvas son biracionalmente equivalentes si y solo si las superficies de Riemann correspondientes tienen la misma estructura compleja. Asimismo, el cuerpo de funciones meromorfas definidas sobre una superficie de Riemann es el cuerpo de funciones algebraicas (racionales) de la curva, como veremos en la sección 5.3. Esto es el functor de Riemann. También existe equivalencia entre las aplicaciones holomorfas entre superficies de Riemann y los morfismos entre curvas.

Para presentar estas ideas nos hemos apoyado en los apuntes de la asignatura "*Superficies de Riemann*" de la UNED [23], donde se puede encontrar una buena exposición de los temas tratados en esta y subsiguientes secciones.

Una **superficie de Riemann** S es un espacio topológico de tipo Hausdorff de dimensión real 2, al que se le ha dotado de un recubrimiento de abiertos $\{V_\alpha\}_{\alpha\in J}$ y para cada uno de ellos un homeomorfismo $\phi_\alpha: V_\alpha \longrightarrow U_\alpha$ con un abierto U_α de $\mathbb{C}$, de forma que para cada dos abiertos V_α, V_β con intersección no vacía, la aplicación entre abiertos de $\mathbb{C}$ denominada función de transición

$$\phi_\beta \circ {\phi_\alpha}^{-1}: \phi_\alpha(V_\alpha \cap V_\beta) \longrightarrow \phi_\beta(V_\alpha \cap V_\beta)$$

es un isomorfismo **holomorfo**.

El conjunto $\{(V_\alpha, \phi_\alpha), \alpha \in J\}$ se denomina atlas (formado por cartas) complejo sobre S y se dice que define una estructura analítica o una estructura de superficie de Riemann sobre S.

El homeomorfismo ϕ_α permite trasladar a V_α cualquier estructura dada en U_α; por ejemplo, la coordenada compleja z en U_α proporciona una función $z_\alpha = z \circ \phi_\alpha$ que llamaremos coordenada en V_α respecto el recubrimiento dado.

Ejemplos:

1) La recta proyectiva compleja $\boldsymbol{P}^1$ recibe también el nombre de **esfera de Riemann** por el siguiente motivo: consideremos el espacio euclidiano $\mathbb{R}^3$ dotado de las coordenadas (x, y, z) donde identificamos con $\mathbb{C}$ al plano coordenado (x, y). Consideremos ahora la esfera unidad S^2 formada por los puntos (x, y, z) tales que $x^2 + y^2 + z^2 = 1$. Denotemos con p_∞ al polo norte de la esfera y con p_0 al polo sur. Tomemos las cartas S, $V = S - \{p_\infty\}$ y $V' = S - \{p_0\}$. Sobre ellas se define $\phi: V \longrightarrow \mathbb{C}$ como la proyección estereográfica de S^2 desde el polo norte y $\phi': V' \longrightarrow \mathbb{C}$ como la proyección estereográfica desde el polo sur, seguida de la conjugación compleja. Se cumple que si $v \in V \cap V'$ y $\phi(v) = z$, entonces $\phi'(v) = 1/z$, con lo que la función de transición es $z \longmapsto 1/z$.

2) Sean e_1 y e_2 dos números complejos linealmente independientes sobre $\mathbb{R}$ y consideremos el grupo de traslaciones en $\mathbb{C}$ generado por ellos:

$$G = \{z \longmapsto z + me_1 + ne_2 \,|\, m, n \in \mathbb{Z}\}$$

el conjunto cociente del plano $\mathbb{C}$ por la acción de este grupo, $S = \mathbb{C}/G$ se denomina toro complejo. Topológicamente es un toro de dimensión real 2 homeomorfo con su topología cociente a un producto de circunferencias

$$S \simeq \mathbb{R}e_1/\mathbb{Z}e_1 \times \mathbb{R}e_2/\mathbb{Z}e_2$$

Vamos a definir ahora una estructura de superficie de Riemann sobre S. Consideramos la proyección canónica $\pi: \mathbb{C} \longrightarrow S$. Dado un punto p_0 sobre S sea z_0 una de sus antiimágenes por π. Sea D un disco abierto centrado en z_0 lo suficientemente pequeño para que todos sus traslados por la acción de G: $D_{mn} = D + me_1 + ne_2$ sean disjuntos dos a dos. Denotemos con z a la

coordenada compleja en D. La coordenada compleja en cada uno de los D_{mn} es $z + me_1 + ne_2$. Puesto que D no corta a ninguno de sus trasladados, $U = \pi(D)$ es isomorfo a D y en él definimos la coordenada z, que asigna a cada punto de U el mismo valor complejo que la coordenada del plano usual asigna al correspondiente punto de D.

Sea p'_0 otro punto de S y sea U' el entorno abierto análogo al definido antes para p a partir de un disco D' tomado en una de las antiimágenes de p'_0. Sea q un punto en $U \cap U'$. Todas las antiimágenes de q están en $\cup D_{mn}$ y en $\cup D'_{mn}$, con lo que un disco de la primera familia $D + me_1 + ne_2$ corta a uno de la segunda $D' + m'e_1 + n'e_2$. Como la coordenada en el primero es $z + me_1 + ne_2$ y en el segundo $z + m'e_1 + n'e_2$, el cambio de coordenadas en $U \cap U' = \pi(D_{mn} \cap D'_{mn})$ viene dado pues por una traslación, con lo que es trivialmente holomorfo.

Dotado de esta estructura de superficie de Riemann, S recibe el nombre de superficie de Riemann elíptica definida por el grupo G. Para un estudio más avanzado de las superficies de Riemann elípticas ver [8] (*página 70*)

Dada una función compleja $f: S \longrightarrow \mathbb{C}$, diremos que es **holomorfa** en un punto $p \in S$, si para cualquier carta $\{V_\alpha, \phi_\alpha\}$ del atlas que lo contenga, la función

$$f \circ {\phi_\alpha}^{-1}: U_\alpha \longrightarrow \mathbb{C}$$

es holomorfa en un entorno de $\phi_\alpha(p)$.

Una función f definida en un abierto U de S se dice que es holomorfa en U cuando es holomorfa en cada uno de sus puntos. El conjunto de todas las funciones holomorfas en U es un anillo.

Llamaremos función **meromorfa** f en una superficie de Riemann S a toda función holomorfa en un abierto U de complemento discreto. Los puntos de $S - U$ se llaman puntos singulares de f. Dado un punto singular p, podemos encontrar un entorno V de p tal que en $V^* = V - \{p\}$ no haya otros puntos singulares de f. Podemos suponer que sobre V existe una coordenada z que representa a este abierto en un disco D centrado en el origen en el plano $\mathbb{C}$ y que $z(p) = 0$. Tenemos las siguientes posibilidades (*ver* [23]):

1) Si f está acotada en un entorno de p, este punto es una singularidad evitable y puede adjuntarse al abierto U en el que f es holomorfa.

2) Si $\lim_{z\to p}|f(z)| = \infty$, entonces el punto p es un polo de f, y en el abierto V^* podemos escribir

$$f(z) = \frac{a_{-m}}{z^m} + \ldots + \frac{a_{-1}}{z} + \sum_{n=0}^{\infty} a_z z^n$$

donde m es un entero positivo; se dice entonces que p es un **polo de orden $\boldsymbol{m}$** de f.

3) Llamamos $ord_p f$ al orden de la función f en el punto p; diremos que $ord_p f = m$ (resp. $-m$) si la función f tiene un cero (res. polo) de orden m en p. La función $ord_p f$ produce valuaciones discretas (*ver página* 55).

4) Las funciones meromorfas constituyen un CFA.

Sabemos que [23]:

Una función meromorfa f sobre una superficie de Riemann S conexa verifica el principio de prolongación analítica: si es nula en un abierto no vacío $V \subset S$ entonces es idénticamente nula en S.

Una **1-forma diferencial** sobre una superficie de Riemann S es una asignación a cada carta local (U, z) con $z = x + iy$ de una expresión de la forma

$$\psi = f(z)dx + g(z)dy$$

donde f y g son funciones diferenciables con valores complejos.

Una 1-forma diferencial holomorfa ω en S es una forma diferencial que en cada abierto coordenado V por la coordenada local z se expresa en la forma $\omega = f(z)dz$ con f holomorfa en V. Una 1-forma diferencial sobre S diremos que es meromorfa si es holomorfa en una abierto U de complemento discreto en S. Los puntos de $S\backslash U$ se denominan puntos singulares de ω. Estamos definiendo, desde el estudio de las superficies de Riemann, las diferenciales de Weil de un CFA vistas en las secciones 3.1 y 3.2 de este trabajo.

Una aplicación $f: S \longrightarrow S'$ entre superficies de Riemann se llama holomorfa si para cada coordenada local $\{U, z\}$ sobre S y cada coordenada local $\{V, s\}$ sobre S' con $U \cap f^{-1}(V) \neq 0$, la aplicación

$$s \circ f \circ z^{-1}: z(U \cap f^{-1}(V)) \longrightarrow s(V)$$

es una función holomorfa entre abiertos del plano complejo.

En particular, una función con valores complejos sobre una superficie de Riemann S $f: S \longrightarrow \mathbb{C}$ es holomorfa si $f \circ z^{-1}: z(U) \longrightarrow \mathbb{C}$ es holomorfa para para cada carta local (U, z) sobre S.

Se cumple [23]:

Sea $f: S \longrightarrow S'$ un morfismo holomorfo entre superficies de Riemann. Dado $p \in S$ sea $q = f(p)$. Existen entonces cartas locales (U, z) sobre S y (V, w) sobre S' con $z(p) = 0$ y $w(q) = 0$ tales que $f(U) \subset V$ y de tal forma que en esas coordenadas locales f se expresa de la forma:

$$w = f(z) = z^k \text{ para algún entero } k \geq 1.$$

Sea S una superficie de Riemann. Entonces toda función meromorfa f sobre S define un morfismo holomorfo (que denotamos con la misma f) en la esfera de Riemann

$$f: S \longrightarrow \boldsymbol{P^1}$$

Recíprocamente, todo morfismo holomorfo en la esfera de Riemann $S \longrightarrow \boldsymbol{P^1}$ define una función meromorfa sobre S.

Este morfismo se define de la siguiente manera: si $P(f)$ es el conjunto de polos de la función meromorfa f, en el abierto $S - P(f)$ f define una función holomorfa que suponemos valorada en el abierto afín $U(= \mathbb{C})$ de $\boldsymbol{P^1}$. Prolongamos esta aplicación a un morfismo $f: S \longrightarrow \boldsymbol{P^1}$ que asigna a cada polo p de f el punto ∞ de $\boldsymbol{P^1}$. Esta aplicación es continua pues

$$f(p) = \infty = \lim_{z \to p} f(z)$$

y se demuestra que es un morfismo holomorfo entre superficies de Riemann.

5.2 RECUBRIDORES DE UNA VARIEDAD Y TEORÍA DE RAMIFICACIÓN

A continuación vamos a describir brevemente los conceptos básicos de la teoría de recubridores y ramificación de una variedad en general, que nos serán de utilidad en el capítulo siguiente, debido principalmente al hecho de que los morfismos entre superficies de Riemann son recubridores ramificados.

Como texto de referencia para esta sección seguimos apoyándonos en los apuntes de la UNED de la asignatura "*Superficies de Riemann*" [23] y en la sección 2.3 del capítulo de preliminares.

Espacios recubridores: dada una aplicación continua $\pi: Y \longrightarrow X$ entre espacios topológicos que suponemos conexos, localmente euclidianos y *Hausdorff,* decimos que π es un **recubridor** si cada punto $P \in X$ tiene un entorno abierto U tal que $\pi^{-1}(U)$ es la unión de una familia de abiertos $\{V_i\}$, disjuntos dos a dos y cada uno de ellos homeomorfo a U por la aplicación π. Un abierto como U recibe el nombre de abierto trivializante del recubridor.

Ejemplo: Si llamamos a S^1 a la circunferencia unidad en el plano euclidiano o, alternativamente, al conjunto de números complejos de módulo unidad: $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, la aplicación

$$\pi: \begin{cases} \mathbb{R} \longrightarrow S^1 \\ x \longmapsto e^{2\pi i x} \end{cases}$$

es un recubridor. Se observa que π aplica biyectivamente el intervalo $V = (-\frac{1}{4}, \frac{1}{4})$ en el intervalo $U = (-\frac{\pi}{2}, \frac{\pi}{2})$ de S^1 y que es un homeomorfismo. Además se cumple que $\pi^{-1}(U) = \cup_n V_n$, donde $V_n = (n - \frac{1}{4}, n + \frac{1}{4})$.

En nuestro texto de referencia [23] se encuentra una buena exposición de los siguientes resultados:

Sea $\pi: Y \longrightarrow X$ un recubridor, p_0 un punto de X y $\gamma: [0,1] \longrightarrow X$ un camino con origen en p_0, $\gamma(0) = p_0$. Para cada punto $q_0 \in \pi^{-1}(p_0)$ existe un único camino $\hat{\gamma}: [0,1] \longrightarrow Y$ con origen en q_0 tal que $\pi \circ \hat{\gamma} = \gamma$. Denominamos a ese camino **levantamiento o elevación** de γ al recubridor π.

Una aplicación continua $\phi: [0,1] \times [0,1] \longrightarrow X$ admite una elevación al recubridor $\Phi: [0,1] \times [0,1] \longrightarrow Y$, y ésta es única si fijamos $\Phi(0,0)$.

Sea $\pi: Y \longrightarrow X$ un recubridor y γ_0, γ_1 dos caminos en X que son homótopos con origen en p y extremo en q. Si $\widehat{\gamma_0}$ y $\widehat{\gamma_1}$ son sus levantamientos respectivos con origen común en un punto p' con $\pi(p') = p$, entonces estos caminos tienen el mismo extremo q' y además son homótopos entre sí.

Sea $f: Y \longrightarrow X$ un recubridor, $y_0 \in Y$ y $f(y_0) = x_0$, entonces el morfismo $f_*: \pi_1(Y, y_0) \longrightarrow \pi_1(X, x_0)$ entre grupos fundamentales es inyectivo.

Teorema [23]: toda variedad conexa X admite un recubridor $\pi: Y \longrightarrow X$ por una variedad simplemente conexa.

Demostración: fijemos un punto $x_0 \in X$. Vamos a llamar Y al conjunto de todas las clases de homotopía de curvas en X con origen en x_0 y extremo en cualquier punto. De esta manera, si $\gamma: [0,1] \longrightarrow X$ es un camino tal que $\gamma(0) = x_0$ y $\gamma(1) = x$, se tiene que γ define un punto en Y que denotaremos por x_γ (identificamos caminos en X con origen común con puntos en el espacio Y). Definimos ahora $\pi: Y \longrightarrow X$ como $\pi(x_\gamma) = x$. Como X es conexa por caminos (todo espacio topológico conexo es conexo por caminos) entonces π es suprayectiva.

Dotamos a Y de estructura de espacio topológico de la siguiente manera: dado un punto $x \in X$ tomamos un entorno $U(x)$ suyo homeomorfo a $\mathbb{R}^n$. Dado un punto $x_\gamma \in \pi^{-1}(x)$, sea $\widetilde{U}(x_\gamma)$ el conjunto de todos los puntos z_ξ tales que $z \in U(x)$ y $\xi \sim c \cdot \gamma$, donde c es un camino en $U(x)$ uniendo x con z. Puesto que el grupo de lazos con base en x es trivial en $U(x)$ (es homeomorfo a $\mathbb{R}^n$), es fácil ver que a cada punto $z \in U(x)$ le corresponde un único punto en $\widetilde{U}(x_\gamma)$.

Tomaremos como base de la topología de Y a la familia de todos los abiertos $\widetilde{U}(x_\gamma)$.

Vamos a ver que Y es *Hausdorff* y que π es un recubridor. Dados dos puntos x_γ y y_ξ de Y, si $x \neq y$ es obvio que éstos tienen entornos disjuntos. Si $x = y$, entonces $[\gamma] \neq [\xi]$. Tomando el entorno $U(x)$ anterior se tiene que $\widetilde{U}(x_\gamma)$ y $\widetilde{U}(x_\xi)$ son disjuntos. En caso contrario existirían caminos c y c' en $U(x)$ con $c \cdot \gamma \sim c' \cdot \xi$, luego $\gamma \sim c^{-1} \cdot c' \cdot \xi \sim \xi$, en contra de lo supuesto. El mismo argumento prueba que π es un recubridor.

Vamos a ver ahora que Y es conexa. Si denotamos con $[x_0]$ la clase de homotopía del camino constante x_0, veamos que todo punto x_γ puede unirse a $[x_0]$ por un camino en Y.

Pero antes necesitamos el siguiente resultado:

Proposición: la elevación del camino γ al recubridor Y con origen en $[x_0]$ es el camino que une los puntos $[x_0]$ y x_γ.

Demostración: para cada α con $0 \leq \alpha \leq 1$ definimos el camino $f_\alpha: [0,1] \longrightarrow X$ mediante $f_\alpha(t) = \gamma(\alpha t)$. Definimos también una aplicación $\tilde{\gamma}: [0,1] \longrightarrow Y$ escribiendo $\tilde{\gamma}(\alpha) = [f_\alpha]$. Se tiene $\tilde{\gamma}(0) = [x_0]$ y $\tilde{\gamma}(1) = [f_1] = [\gamma] = x_\gamma$. Además $\pi \circ \tilde{\gamma}(\alpha) = \pi[f_\alpha] = f_\alpha(1) = \gamma(\alpha)$.

Volviendo a la demostración del teorema vamos a ver que el grupo fundamental de Y es la identidad. Sea pues $\tilde{\gamma}$ un lazo con origen en $[x_0]$, entonces $\gamma = \pi \circ \tilde{\gamma}$ es un lazo en x_0 y por ser Y un recubridor de X existe una única elevación de γ a Y con origen en $[x_0]$. Tal elevación ha de ser el propio $\tilde{\gamma}$. Como acabamos de ver $\tilde{\gamma}(\alpha) = [f_\alpha]$ y como $\tilde{\gamma}(0) = \tilde{\gamma}(1)$ se tiene que $[x_0] = [\gamma]$. Pero si $\gamma \sim x_0$ también $\tilde{\gamma} \sim [x_0]$, con lo que todo elemento $\tilde{\gamma} \in \pi_1(Y, [x_0])$ es homótopo al lazo constante.

El recubridor $\pi: Y \longrightarrow X$ definido anteriormente recibe el nombre de **recubridor universal** de la variedad conexa X.

Teorema [23]: sean $\pi: Y \longrightarrow X$ y $\phi: Z \longrightarrow X$ dos recubridores de la variedad X, y se supone que Z es simplemente conexo. Fijados los puntos $x_0,\ y_0,\ z_0$ con $\pi(y_0) = x_0,\ \phi(z_0) = x_0$, entonces existe un único recubridor $\Phi: Z \longrightarrow Y$, tal que $\pi \circ \Phi = \phi$ (es decir, un recubridor simplemente conexo recubre a su vez a cualquier otro recubridor).

Corolario: dos recubridores simplemente conexos $Y,\ Z$ de la variedad X son homeomorfos.

Corolario: si una variedad X es simplemente conexa, todo recubridor $\pi: Y \longrightarrow X$ por una variedad conexa Y es un homeomorfismo.

Sea $\pi: Y \longrightarrow X$ un recubridor. Llamaremos grupo de automorfismos de π al grupo que denotaremos $Aut_X(Y)$ formado por aquellos homeomorfismos $f: Y \longrightarrow Y$ tales que $\pi \circ f = \pi$.

Si Y es conexa y $f \in Aut_X(Y)$ es tal que fija un punto $y \in Y$, entonces $f = Id_Y$.

Ejemplos:

1) En el caso visto en la sección anterior de las superficies de Riemann elípticas S definidas por el grupo o retículo G, la proyección canónica $\pi: \mathbb{C} \longrightarrow S$ es un recubridor universal, donde el grupo de traslaciones del retículo G genera el grupo de automorfismos del recubrimiento.

2) La ecuación definida por funciones racionales con coeficientes en el cuerpo $\mathbb{F}_9$: $y^2 = \frac{(x^9+x^3)}{(x^3+2x)}$ es un recubridor de grado 2 sobre la esfera de Riemann.

Teorema [23]: sea X una variedad conexa y sea $\pi: Y \longrightarrow X$ su recubridor universal. Fijado un punto $x_0 \in X$, el grupo fundamental $\pi_1(X, x_0)$ es isomorfo al grupo de automorfismos del recubridor π, y opera transitivamente y sin puntos fijos en cada fibra de π.

Sean ahora S y W superficies de Riemann conexas y $\phi: S \longrightarrow W$ un morfismo holomorfo no constante. Sea p un punto en S y $q = \phi(p)$. Elegimos coordenadas locales z y w en sendos entornos de p y q en las cuales ϕ tiene la forma

$$w = z^r$$

(ya vimos en la sección de superficies de Riemann que siempre era posible definir las coordenadas locales de esta forma).

El entero r se denomina **multiplicidad** de ϕ en $p \in S$. Este punto será llamado de **ramificación** si $r > 1$, en cuyo caso $q = \phi(p)$ se llamará valor de ramificación de ϕ.

Esto equivale a decir que si en términos de ciertas coordenadas locales la aplicación ϕ se describe por una función holomorfa $w = f(z)$, el punto $p \in S$ es un punto de ramificación de multiplicidad r cuando $f'(p) = \ldots = f^{r-1)}(p) = 0$ y $f^{r)}(p) \neq 0$. Supondremos además que S es compacta. De esta forma, como ϕ es no constante, los puntos de ramificación son aislados, luego constituyen un conjunto finito en S. Denotemos con W' al complemento en W de los valores de ramificación y sea S' su antiimagen. Entonces se cumple que la restricción $\phi: S' \longrightarrow W'$ es un isomorfismo local en cada punto de S'. Cuando además esta restricción es un recubridor se dice que $\phi: S \longrightarrow W$ es un **recubridor ramificado**.

Tenemos el siguiente resultado:

Teorema [23]: todo morfismo holomorfo no constante $\phi: S \longrightarrow W$ entre superficies de Riemann compactas conexas es un recubridor ramificado.

Demostración: manteniendo las mismas notaciones del párrafo anterior, vamos a probar que $\phi: S' \longrightarrow W'$ es un recubridor. Sea q un punto de W'. Este punto solo puede tener un número finito de antiimágenes $p_1, \dots, p_m$ (pues ϕ es isomorfismo local y S es compacto). Como ϕ es un isomorfismo local en cada p_i, podemos suponer que existen entornos disjuntos V_i de p_i que se aplican por ϕ en entornos U_i de q. Tomando $U = U_1 \cap \dots \cap U_m$ entonces $\phi^{-1}(U)$ consiste en la unión de los abiertos disjuntos $V'_i = V_i \cap \phi^{-1}(U)$, cada uno de ellos aplicados por ϕ sobre U.

En consecuencia $\phi: S' \longrightarrow W'$ es un recubridor. El número n de antiimágenes de cada punto $q \in W'$ es siempre el mismo, pues este número es una función localmente constante sobre W' al ser esta conexa.

En particular, toda función meromorfa no constante sobre una superficie de Riemann S define un recubridor ramificado en la esfera de Riemann $\boldsymbol{P^1}$.

El número m de hojas del recubridor $\phi: S' \longrightarrow W'$ recibe el nombre de **grado del morfismo** ϕ.

Seguidamente veremos que m no solo coincide con el número de antiimágenes por ϕ de cualquier punto de W', sino que cualquier valor de ramificación q de ϕ tiene también m antiimágenes, contando cada uno de estos puntos con la multiplicidad adecuada.

Teorema [23]: el morfismo $\phi: S \longrightarrow W$ toma cada valor $q \in W$ es mismo número de veces, y este número es m, el grado de ϕ.

Corolario: si f es una función meromorfa definida en una superficie de Riemann compacta S, entonces su número de ceros es igual a su número de polos, contando cada cero y polo según indica su multiplicidad.

Ejemplos:

1) Sea una aplicación holomorfa $f: \boldsymbol{P^1} \longrightarrow \boldsymbol{P^1}$ que en el abierto U de la variable z se expresa como:

$$f(z) = \frac{z}{z^3 + 2}$$

Es claro que f es una función racional de grado 3. Vamos a estudiar la ramificación en U. Como $f'(z) = \frac{2(1-z^3)}{(z^3+2)^2}$, los puntos en los que $f'(z) = 0$ son $1,\ \omega,\ \omega^2$, donde $\omega = e^{\frac{2\pi i}{3}}$ y, por tanto, estos puntos son los puntos de ramificación en el abierto U. Estudiemos el primero; el valor de ramificación es $f(1) = 1/3$. El conjunto $f^{-1}(1/3)$, esto es, el conjunto de soluciones de la ecuación: $\frac{z}{z^3+2} = \frac{1}{3}$ es $f^{-1}(1/3) = \{-2,1,1\}$; así tenemos que $z = 1$ es un punto de ramificación con multiplicidad 2. El análisis con ω y ω^2 es similar.

Como $\lim_{z\to\infty} f(z) = 0$, la función f aplica un entorno del punto $\{\infty\}$ en un entorno del $\{0\}$. Tomando la carta $J(z) = 1/z$, la expresión de f es

$$f \circ J(z) = \frac{z^2}{1 + 2z^3}$$

que tiene un cero doble en $z = 0$, con lo que $\{\infty\}$ es un punto de ramificación de f. De hecho $f^{-1}(0) = \{\infty, \infty, 0\}$.

2) Consideramos la superficie de Riemann X de la curva proyectiva que en las coordenadas homogéneas de $\boldsymbol{P^2}$ se expresa como $t_0^3 + t_1^3 + t_2^3 = 0$. Dado el morfismo

$$\pi\colon \begin{cases} X \longrightarrow \boldsymbol{P^1} \\ (t_0, t_1, t_2) \mapsto (t_0, t_1) \end{cases}$$

Vamos a calcular sus puntos de ramificación: la antiimagen de un punto de coordenadas (t_0, t_1) está formada por los puntos (t_0, t_1, t_2) con $t_2 = \sqrt[3]{-(t_0^3 + t_1^3)}$. Esto produce tres puntos distintos en $\pi^{-1}(t_0, t_1)$ salvo que $t_0^3 + t_1^3 = 0$. De esta forma si ω es tal que $\omega^3 = -1$, los puntos de ramificación pueden escribirse con las coordenadas homogéneas $(t_0, -t_0, 0), (t_0, \omega t_0, 0), (t_0, \omega^2 t_0, 0)$ que proporcionan los tres puntos $(1, \omega, 0), (1, \omega^2, 0), (1, -1, 0)$.

3) Una superficie de Riemann compacta S se dice que es hiperelíptica si existe sobre ella una función meromorfa f con exactamente dos polos. Vamos a construir sobre S un automorfismo holomorfo σ tal que $\sigma^2 = Id$: podemos considerar a f como un morfismo holomorfo en la esfera de Riemann:

$$f: S \longrightarrow \boldsymbol{P^1}$$

Entonces, como la imagen inversa por f del punto del ∞ son dos puntos en S, se cumple también que la antiimagen de cualquier punto $p \in \boldsymbol{P^1}$ son dos puntos q_1 y q_2 (que en general siempre son distintos pero pueden ser el mismo punto). Definimos entonces $\sigma: S \longrightarrow S$ de la siguiente forma: dado $q \in S$ se calcula $f(q)$, entonces $f^{-1}(f(q))$ son dos puntos $\{q,\ q'\}$ y hacemos $\sigma(q) = q'$ (σ intercambia los puntos en cada fibra de f). Está claro que $\sigma^2 = Id$ y además σ es holomorfa, por ser conmutativo el diagrama

$$\begin{array}{ccc} S & \overset{\sigma}{\rightarrow} & S \\ f \searrow & & \swarrow f \\ & \boldsymbol{P^1} & \end{array}$$

y las propiedades elementales de la composición de funciones complejas: sobre un abierto coordenado σ es holomorfa ya que f lo es y $f \circ \sigma = f$.

4) Como ejemplo de superficies hiperelípticas tenemos la familia de curvas S con ecuación

$$y^2 = x^b - x$$

El morfismo dado por la proyección en la coordenada x sobre la esfera de Riemann

$$f: \begin{cases} S & \longrightarrow \boldsymbol{P^1} \\ (x, y) & \longmapsto x \end{cases}$$

es la función meromorfa f del ejemplo anterior. Dicho morfismo define una teselación cociente de tipo (3,4) sobre la esfera, que levanta a una teselación de tipo (3,8) en las superficies S, ver [3] (una teselación de tipo (3,8) es una teselación en una superficie donde en cada vértice se juntan 3 polígonos hiperbólicos de 8 lados cada uno (o el dual)).

5.3 FÓRMULA DE RIEMANN-HURWITZ.

Volvemos de nuevo al Teorema de Riemann-Roch, pero esta vez planteado desde un enfoque geométrico a partir del estudio de las superficies de Riemann compactas. El objetivo final es la obtención de la fórmula de Riemann-Hurwitz, que nos será de gran utilidad en el capítulo siguiente para el cálculo del género de una variedad algebraica.

Como ya hemos visto que las funciones meromorfas definidas sobre una superficie de Riemann forman un CFA, volvemos a reconsiderar las secciones 3.1 y 3.3, ahora para el caso especial de cuerpos de funciones meromorfas. Queremos reformular el Teorema de Riemann-Roch para funciones meromorfas.

Como texto de referencia para esta sección nos hemos basado, como en las secciones anteriores, en [23].

Los **divisores** (*ver concepto de divisor en sección 3.1, página 29*) sobre una superficie de Riemann S son los elementos del grupo libre generado sobre $\mathbb{Z}$ por los puntos de S.

Una función meromorfa f sobre S define un divisor sobre S como sigue: para un punto P de S denotamos como $ord_P f$ al orden de la función f en el punto P, escribiendo de esta manera: $D(f) = \sum_{P \in S} ord_P f \cdot P$. Sabemos que si $ord_P f > 0$ la función f tiene un cero en P, mientras que si $ord_P f < 0$ entonces f tiene un polo en P.

Dados dos divisores D y D' sobre S, diremos que son equivalentes y escribiremos $D \sim D'$ si existe una función meromorfa f tal que $D - D' = D(f)$.

Sea D un divisor sobre S. Se define el $\mathbb{C}$-espacio vectorial $\mathcal{L}_D$ de las funciones meromorfas que cumplen (*ver concepto de espacio de Riemann-Roch asociado a un divisor de la sección 3.1, página 30*)

$$\mathcal{L}_D = \{f \in \mathcal{M}(S) | \, D(f) + D \geq 0\}$$

donde $\mathcal{M}(S)$ es el conjunto de funciones meromorfas definido sobre una superficie de Riemann S.

Ejemplo: sea P un punto de S y consideramos el divisor P, entonces:

$$\mathcal{L}_P = \{f \in \mathcal{M}(S) |\, D(f) + P \geq 0\}$$

está formado por las funciones meromorfas sobre S con un único polo (y simple) en P.

Dada una diferencial meromorfa ω sobre una superficie de Riemann compacta X se define su divisor asociado de la siguiente forma (*ver concepto de divisor asociado a un diferencial de Weil en la sección 3.1, página 34*): dado un punto $P \in X$ sea (U, z) un entorno coordenado suyo. Sobre U la forma ω se escribe como $\omega = f(z)dz$ donde f es una función meromorfa de la coordenada local z. Se define el orden de ω en P como $ord_P\omega = ord_P f$. Así se define el divisor de ω sobre X como $D(\omega) = \sum_{P \in X} ord_P\omega \cdot P$.

Dos diferenciales meromorfas definen divisores equivalentes; esta clase de equivalencia de divisores se denomina **clase canónica** y la representamos por $\mathcal{K}$ (*véase concepto de divisor canónico y clase canónica de un CFA F/K en sección 3.1, página 35*).

Vamos a considerar el espacio vectorial $\mathcal{L}_{\mathcal{K}}$ asociado:

$$\mathcal{L}_{\mathcal{K}} = \{f \in \mathcal{M}(X) |\, D(f) + D(\omega) \geq 0\} = \{f \in \mathcal{M}(X) |\, D(f\omega) \geq 0\}$$

Que corresponde con el $\mathbb{C}$-espacio vectorial de las diferenciales holomorfas (sin polos) sobre X.

Si D es un divisor cualquiera sobre X, necesitamos interpretar también los elementos del $\mathbb{C}$-espacio vectorial $\mathcal{L}_{\mathcal{K}-D}$:

$$\mathcal{L}_{\mathcal{K}-D}(X) = \{f \in \mathcal{M}(X) |\, D(f) + D(\omega) - D \geq 0\} = \{f \in \mathcal{M}(X) |\, D(f\omega) - D \geq 0\}$$

podemos afirmar que $\mathcal{L}_{\mathcal{K}-D}$ se corresponde con el $\mathbb{C}$-espacio vectorial de las diferenciales meromorfas sobre X cuyo divisor asociado es múltiplo de D.

Teorema de Riemann-Roch [20], [23] (*véase sección 3.1, página 36*): Sea X una superficie de Riemann compacta de género g y D un divisor sobre ella, se cumple entonces que

$$dim_{\mathbb{C}}(\mathcal{L}_D) - dim_{\mathbb{C}}(\mathcal{L}_{\mathcal{K}-D}) = 1 - g + \deg(D)$$

Ejemplos:

1) Si $D = 0$ entonces $dim_{\mathbb{C}}(\mathcal{L}_D) = 1$, pues las únicas funciones meromorfas sin ceros ni polos son las funciones constantes. Por otra parte, si D es un divisor de grado negativo, entonces $dim_{\mathbb{C}}(\mathcal{L}_D) = 0$, pues si existiera una función meromorfa f con $D(f) + D \geq 0$ entonces $D(f) \geq -D$. Si tomamos grados: $0 \geq \deg(-D) > 0$, lo que es una contradicción.

2) Dada una superficie de Riemann compacta S de género g, vamos a calcular la dimensión del espacio de las diferenciales holomorfas sobre S: si tomamos $D = 0$ y aplicamos el teorema de Riemann-Roch:

$$1 - dim_{\mathbb{C}}(\mathcal{L}_{\mathcal{K}}) = 1 - g$$

con lo que la dimensión del espacio de las diferenciales holomorfas sobre S es g.

3) Dada una superficie de Riemann compacta S de género g, vamos a calcular el grado de la clase canónica $\mathcal{K}$: si tomamos si tomamos $D = \mathcal{K}$ y aplicamos el teorema de Riemann-Roch

$$dim_{\mathbb{C}}(\mathcal{L}_{\mathcal{K}}) - 1 = 1 - g + \deg(\mathcal{K})$$

como en el ejemplo anterior habíamos obtenido $dim_{\mathbb{C}}(\mathcal{L}_{\mathcal{K}}) = g$, se cumple que $\deg(\mathcal{K}) = 2g - 2$. Por ejemplo, si S es la esfera de Riemann, sabemos que el divisor de la diferencial meromorfa $\omega = dz$ es $(-2) \cdot \infty$, que es de grado -2, con lo que tenemos el resultado esperado, ya que en género de $\boldsymbol{P^1}$ es cero.

Fórmula de Riemann-Hurwitz [23]: sea $f: X \longrightarrow Y$ un morfismo de grado n entre superficies de Riemann compactas de géneros g_X y g_Y respectivamente. Para cada punto q sobre X sea $p = f(q)$ sobre Y. Elegimos coordenadas z y w centradas en q y p en las cuales f tiene la forma: $w = z^{v(q)}$, donde el entero $v(q)$ es la multiplicidad de f en q. Vimos que el punto q es de ramificación si $v(q) > 1$. Definimos el **divisor de ramificación** del morfismo f como

$$\mathcal{R} = \sum_{q \in X} (v(q) - 1) \cdot q$$

Si Ω es una diferencial holomorfa en la clase canónica $\mathcal{K}_Y$ de Y, entonces el *pull-back* $f^*\Omega$ define un elemento de la clase canónica $\mathcal{K}_X$. Procediendo en

coordenadas, si Ω en una carta local sobre Y coordenada por w se expresa como $\Omega = g(w)dw$, entonces $f^*\Omega = v(q)z^{v(q)-1} \cdot g(z^{v(q)})dz$, con lo que

$$ord_q(f^*\Omega) = v(q)ord_p(\Omega) + (v(q) - 1)$$

Que implica la relación entre los divisores sobre X: $\mathcal{K}_X = f^*(\mathcal{K}_Y) + \mathcal{R}$

El grado del divisor de ramificación $\mathcal{R}$ suele denotarse por R. De esta manera, si tomamos grados en la igualdad anterior tenemos

$$2g_X - 2 = n(2g_Y - 2) + R$$

Fórmula que se conoce como de Riemann-Hurwitz.

Ejemplo: sea S una superficie de Riemann compacta de tal forma que existe un morfismo holomorfo f: $\boldsymbol{P^1} \longrightarrow S$.

Vamos a calcular el género de S: si llamamos n al grado de f, aplicando la fórmula anterior:

$$-2 = n(2g_S - 2) + R$$

Como n y R son enteros no negativos, $2g_S - 2$ ha de ser negativo, con lo que $g_S = 0$.

Teorema [23], [20]: sea S una superficie de Riemann definida por un polinomio homogéneo $P(t_0, t_1, t_2)$ no singular de grado d en $\boldsymbol{P^2}(\mathbb{C})$. El género de S viene dado por

$$g = \frac{(d-1)(d-2)}{2}$$

Demostración: con un cambio de coordenadas proyectivas podemos suponer que la expresión de P en las coordenadas afines $x = {}^{t_1}/_{t_0}$, $y = {}^{t_2}/_{t_0}$ es

$$f(x, y) = y^d + \lambda_1(x)y^{d-1} + \ldots + \lambda_m(x)$$

Consideramos el morfismo

$$\pi: \begin{cases} S & \longrightarrow & \boldsymbol{P^1} \\ (x,y) & \longmapsto & x \end{cases}$$

en un punto $q \in S$ con ${}^{\partial f}/_{\partial y} \neq 0$, la x es coordenada local, y por tanto π aquí no está ramificada (pues el morfismo se expresa como $x = x$). Si ${}^{\partial f}/_{\partial y} = 0$ en un punto q, entonces ${}^{\partial f}/_{\partial x} \neq 0$, con lo que la y sirve como coordenada local.
De esta forma $\frac{\partial f}{\partial y} + \frac{\partial f}{\partial x}\frac{\partial x}{\partial y} = 0$. Si el orden del cero de ${}^{\partial x}/_{\partial y}$ en q, que es $v(q) - 1$ (pues el morfismo se expresa como $x = y^{v(q)}$), es igual al orden del cero de ${}^{\partial f}/_{\partial y}$ en q, esto es a la multiplicidad de la intersección de S con la curva $\left\{{}^{\partial f}/_{\partial y} = 0\right\}$ en q. Como ${}^{\partial f}/_{\partial y}$ es una curva de grado $d - 1$, el número de intersección con S es $d(d-1)$, de esta forma $\sum v(q) - 1 = d(d-1)$. Aplicando la fórmula de Riemann-Hurwitz:

$$2g - 2 = d(-2) + d(d-1)$$

de donde se obtiene el valor deseado para el género de S.

5.4 CURVAS ELÍPTICAS, HIPERELÍPTICAS Y SUPERELÍPTICAS

Como paso previo al estudio de las curvas algebraicas de tipo $C_{a,b}$, a continuación vamos a definir y presentar de forma somera sus propiedades más importantes, los tipos de curvas algebraicas elípticas, hiperelípticas y superelípticas, al estar todas ellas englobadas dentro de la familia superior de curvas tipo $C_{a,b}$.

Como referencia para esta sección nos hemos basado en diferentes artículos extraídos de la red Internet, principalmente la enciclopedia digital Wikipedia (*https://es.wikipedia.org/wiki/Wikipedia:Portada*)

Formalmente hablando, una **curva elíptica** es una curva proyectiva algebraica y regular (sin vértices ni intersecciones) de género uno definida sobre un cuerpo K, en la que existe un punto específico O, que denominamos punto en el infinito del plano proyectivo.

Recordemos la superficie de Riemann compacta definida por el conjunto cociente del plano $\mathbb{C}$ por la acción del grupo G (*ejemplo 2 de la página 70 de este texto*), que denominábamos toro complejo y que constituye un caso de curva elíptica compleja, donde G es el grupo fundamental de la curva como cociente ramificado del plano complejo $\mathbb{C}$.

Si la característica del cuerpo K no es ni 2 ni 3, toda curva elíptica sobre K puede escribirse mediante una ecuación cúbica de la forma

$$y^2 = x^3 + ax + b$$

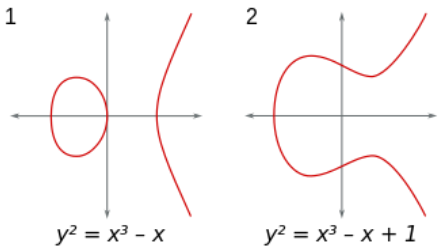
que es no singular, donde a y b son elementos de K tales que el polinomio del segundo miembro de la ecuación $x^3 + ax + b$ no tenga ninguna raíz doble. Si la característica de K es 2 o 3, harán falta más miembros en la ecuación.

Normalmente se define la curva como el conjunto de puntos (x, y) que satisfacen la ecuación anterior y tales que $x\ e\ y$ sean elementos que pertenecen al cierre algebraico de K. Los puntos de la curva en los que tanto x como y pertenecen a K se denominan puntos K-racionales (*ver puntos K-racionales de una variedad en página 55 del presente trabajo*).

Si añadimos el punto en el infinito obtenemos la versión proyectiva de la curva.

Ejemplo: sobre el cuerpo K de los números reales las siguientes expresiones definen curvas de tipo elíptico: $y^2 = x^3 - x$ y $y^2 = x^3 - x + 1$

cuyas representaciones gráficas de la parte real de las curvas son



Como hemos visto, la definición de curva elíptica requiere que la curva sea no singular. Geométricamente hablando, esto significa que su representación gráfica no tiene ni vértices o cúspides ni intersecciones o puntos aislados. Desde el punto de vista algebraico, si calculamos el discriminante $\Delta = -16(4a^3 + 27b^2)$, la curva es no singular si y solo si el discriminante no es igual a cero.

La representación gráfica (real) de una curva elíptica tiene dos componentes si el discriminante es positivo y un componente si es negativo. Por ejemplo, en los dos ejemplos anteriores, el discriminante en el primer caso es 64 y en el segundo -368.

Curvas **hiperelípticas**: en geometría algebraica, una curva hiperelíptica es una curva algebraica que viene dada por una ecuación de la forma

$$y^2 = f(x)$$

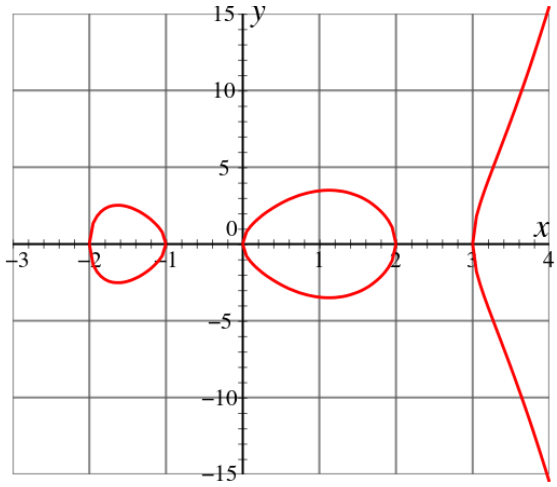
donde $f(x)$ es un polinomio de grado $n > 4$ con n raíces diferentes. Una función hiperelíptica es un elemento del cuerpo de funciones de dicha variedad.

En la página 79 vimos que una superficie de Riemann compacta era hiperelíptica si sobre ella estaba definida una función meromorfa con exactamente 2 polos.

Ejemplo:

$$y^2 = x^5 - 2x^4 - 7x^3 + 8x^2 + 12x = x(x+1)(x-3)(x+2)(x-2)$$

Cuya gráfica de la parte real de la curva es la siguiente



Género de una curva hiperelíptica: el grado del polinomio determina el género de la curva: un polinomio de grado $2g+1$ o $2g+2$ determinan una curva hiperelíptica de género g. Cuando el grado es igual a $2g+1$ la curva se denomina hiperelíptica imaginaria (con un punto en el infinito), mientras que la de grado $2g+2$ es hiperelíptica real (con dos puntos en el infinito).

Mientras este modelo es la manera más simple de describir la curvas hiperelípticas, la ecuación tiene un punto singular en el infinito en el plano proyectivo. En consecuencia, para proporcionar una ecuación de una curva no singular se asume el modelo no singular en el sentido biraccional, en el que el punto del infinito es eliminado mediante el proceso de normalización denominado cierre proyectivo que describimos con anterioridad (*página 51*). Después de aplicar esta normalización nos encontramos con 2 espacios recubridores de la curva por dos gráficos afines. Uno es el ya visto $y^2 = f(x)$ y el otro viene dado por $v^2 = u^{2g+2} f(1/u)$.

Desde el punto de vista geométrico podemos considerar a una curva hiperelíptica como un espacio recubridor doblemente ramificado de la línea proyectiva o esfera de Riemann. La ramificación se produce en las raíces del polinomio f y, para n impar, en el punto del infinito. De esta manera se pueden unificar los casos $n = 2g+1$ y $n = 2g+2$, pues podemos hacer uso de un automorfismo en la línea proyectiva para sacar cualquiera de los puntos de ramificación del infinito.

Usando la fórmula de Riemann-Hurwitz obtenemos que la curva hiperelíptica de género g está definida por una ecuación de grado $n = 2g+2$: supongamos el morfismo biyectivo $f: \mathcal{X} \longrightarrow \boldsymbol{P}^1$ con grado de ramificación 2, donde $\mathcal{X}$ es una curva

de género g y $\boldsymbol{P}^1$ es la esfera de Riemann. Sean $g_1 = g$ y g_0 el género de $\boldsymbol{P}^1$ (que es 0). Si aplicamos la fórmula de Riemann-Hurwitz

$$2 - 2g_1 = degf(2 - 2g_0) - \sum_{s \in X}(e_s - 1)$$

Donde s recorre todos los puntos ramificados. El número de dichos puntos es finito, de valor n, luego $n = 2g + 2$. Para el caso de curvas hiperelípticas reales, con $n + 1$ puntos de ramificación, obtendríamos $n = 2g + 1$ de la misma manera.

Existen curvas hiperelípticas para cada género $g \geq 1$. Si el género de la curva es $g = 1$, la denominamos simplemente curva elíptica. Luego las curvas hiperelípticas son una generalización de las curvas elípticas.

Curvas superelípticas: una curva algebraica es superelíptica si viene expresada por una ecuación de la forma

$$y^m = f(x)$$

donde el exponente m es fijo y f es un polinomio de grado d. El caso $m = 2$ y $d > 4$ es la curva hiperelíptica vista anteriormente.

Ejemplo: la cuártica de Klein es una curva Q cuya ecuación es

$$y^7 = x(x^2 + 1)$$

es un curva superelíptica. La proyección en la coordenada x sobre la esfera de Riemann

$$\pi: \begin{cases} Q & \longrightarrow \boldsymbol{P^1} \\ (x, y) & \mapsto x \end{cases}$$

es una función meromorfa (recubridor ramificado) de grado 7.

5.5 CURVAS ADMISIBLES

En esta sección vamos a definir una clase de curvas que tienen algunas propiedades adicionales en sus divisores y que son de gran utilidad porque, bajo determinadas condiciones, su grupo de automorfismos es isomorfo al de los códigos AG basados en estas curvas. Veremos también en la siguiente sección que las curvas $C_{a,b}$ se enmarcan dentro de este tipo de curvas.

Como texto de referencia para esta sección nos hemos basado en [18], [21].

Sea $\mathbb{F}_q$ un cuerpo finito de tamaño q, $\mathcal{X}$ una curva algebraica de género $g \geq 2$ definida sobre $\mathbb{F}_q$ y F su cuerpo de funciones algebraicas.

Una curva $\mathcal{X}$ de género $g \geq 2$ se denomina **admisible** si satisface las siguientes propiedades:

1) Existe un punto racional P_∞ y dos funciones $x, y \in F$ tales que

$$(x)_\infty = kP_\infty, \ (y)_\infty = lP_\infty$$

y $k, l \geq 1$

2) Para $m \geq 0$, los elementos $x^i y^j$ con $0 \leq i$, $0 \leq j \leq k-1$ y $ki + lj \leq m$ forman una base del espacio de Riemann-Roch asociado al divisor $\mathcal{L}(m \cdot P_\infty)$.

Habíamos definido en la sección 4.2:

$$Aut_{D,G}(F/\mathbb{F}_q) \coloneqq \{\sigma \in Aut(F/\mathbb{F}_q) |\ \sigma(D) = D \ \ y\ \sigma(G) = G\}$$

y que todo automorfismo $\sigma \in Aut_{D,G}(F/\mathbb{F}_q)$ induce un automorfismo en el código correspondiente $C_{\mathcal{L}}(D, G)$:

$$\sigma\left(\left(x(P_1), \dots, x(P_n)\right)\right) \coloneqq \left(x\left(\sigma(P_1)\right), \dots, x\left(\sigma(P_n)\right)\right)$$

(para $x \in \mathcal{L}(G)$). Esto generaba un homomorfismo de $Aut_{D,G}(F/\mathbb{F}_q)$ en $Aut(C_{\mathcal{L}}(D,G))$.

También mostramos en 4.2 que, si $n \geq 2g+2$, el homomorfismo anterior es inyectivo. Con el siguiente teorema vamos a ver qué condiciones adicionales deben cumplirse para que este homomorfismo sea también suprayectivo en el caso de las curvas admisibles.

Teorema [21]: sea $\mathcal{X}$ una curva admisible sobre $\mathbb{F}_q$ de género g donde $l > k$. Asumimos también que $m \geq l$. Dado el divisor $D = \sum_{P \in J} P$, donde $J \subseteq \mathbb{P}_F \backslash \{P_\infty\}$, siendo $\mathbb{P}_F$ el conjunto de los *places* de $F/\mathbb{F}_q$ (*ver página* 28). Si

$$n > max\left\{2g+2, 2m, k\left(l + \frac{k-1}{\beta}\right), lk(1 + \frac{k-1}{m-k+1})\right\}$$

donde

$$\beta = min\{k-1, r | y^r \ \in \mathcal{L}(mP_\infty)\}$$

Entonces se cumple que

$$Aut(C_{\mathcal{L}}(D, mP_\infty)) \cong Aut_{D,mP_\infty}(\mathcal{X})$$

La demostración del teorema puede obtenerse de [21]

5.6 INTRODUCCIÓN A LAS CURVAS $C_{a,b}$

Pasamos por fin a hablar sobre las denominadas curvas $C_{a,b}$, que pertenecen a la familia de las curvas superelípticas. Las curvas $C_{a,b}$ son curvas algebraicas admisibles con propiedades muy interesantes. Con posterioridad veremos cómo estas propiedades son de utilidad para construir buenos códigos AG.

Como texto de referencia nos hemos basado en [18].

A lo largo de la sección K es un cuerpo algebraicamente cerrado de característica distinta de 2 y a, b dos enteros positivos primos entre sí.

Una curva $\mathcal{X}$ definida sobre K se llama **curva $C_{a,b}$** si es una curva plana no singular definida por la ecuación $f(x,y) = 0$, donde $f(x,y) \in K[x,y]$ tiene la forma:

$$f(x,y) = \alpha_{0,a}y^a + \alpha_{b,0}x^b + \sum_{ai+bj<ab} \alpha_{i,j}\, x^i y^j$$

para $\alpha_{0,a}$, $\alpha_{b,0} \in K$ no nulos

Proposición: sea $\mathcal{X}$ una curva $C_{a,b}$ definida sobre K. Entonces existe exactamente un *place* K-racional P_∞ en el infinito, que implica que el grado de P_∞ es uno. Además, los divisores polo de $x\ e\ y$ son $b \cdot P_\infty$ y $a \cdot P_\infty$, respectivamente. El género de $\mathcal{X}$ es

$$g(\mathcal{X}) = \frac{(a-1)(b-1)}{2}$$

Demostración: el cuerpo de funciones racionales de la curva $\mathcal{X}$ es el cuerpo cociente (o cuerpo de fracciones) del anillo de coordenadas de la curva (*ver página 48*):

$$K(\mathcal{X}) = Quot\big(\Gamma(\mathcal{X})\big) = Quot(K[x,y]/f(x,y))$$

Vamos a estudiar los *places* de ese cuerpo de funciones (*ver página 28 de este texto*). Al ser un cuerpo de funciones racionales se cumple que $degP_\infty = 1$, formando este place parte del conjunto de los puntos K–racionales de la curva (*página 55*).

Analizando el comportamiento en el infinito, se comprueba que $1/x$ y $1/y$ son elementos primos del ideal P_∞ , con lo que únicos divisores polo de la curva son:

$$(x)_\infty = \left(-v_\infty(x)\right) \cdot P_\infty \ = b \cdot P_\infty$$

$$(y)_\infty = \left(-v_\infty(y)\right) \cdot P_\infty \ = a \cdot P_\infty$$

Luego las curvas $C_{a,b}$ constituyen recubridores totalmente ramificados de grados a y b de la recta proyectiva $\boldsymbol{P}^1(K)$. Consideremos en primer lugar el recubridor de grado a $\pi_a: C_{a,b} \longrightarrow \boldsymbol{P}^1(K)$. Como el recubridor está totalmente ramificado, entonces hay $2g + a - 1$ puntos rama adicionales (teorema de *Riemann-Roch*). Luego el número total de puntos rama es

$$d_1 \coloneqq 2g + a = ab - b + 1 = b(a-1) + 1$$

aplicando la fórmula anterior del género de una curva $C_{a,b}$

La cubierta de grado b $\pi_b: C_{a,b} \longrightarrow \boldsymbol{P}^1(K)$ tiene lógicamente

$$d_2 \coloneqq a(b-1) + 1$$

Obtenida de la anterior por intercambio de los parámetros a y b (por simetría).

Corolario: todas la curvas hiperelípticas son curvas $C_{a,b}$

Demostración: como vimos anteriormente, toda curva hiperelíptica puede escribirse de la forma $y^2 = f(x)$ cumpliéndose que $degf = 2g + 1$. Tomando $a = 2$ y $b = 2g + 1$ queda demostrado.

A continuación volveremos sobre las curvas superelípticas que, como mostramos en la sección 5.4 son una clase de curvas mayor que la de las curvas

hiperelípticas. La siguiente proposición será de gran utilidad cuando vayamos a construir códigos AG desde curvas $C_{a,b}$.

Proposición [18]: sea $\mathcal{X}$ una curva $C_{a,b}$ definida mediante $f(X,Y)=0$ con $f(X,Y) \in F[X,Y]$, entonces

$$\left\{X^i Y^j \mid 0 \leq j \leq a-1, i \geq 0, ai+bj \leq m\right\}$$

es un base del espacio vectorial $\mathcal{L}(m \cdot P_\infty)$ sobre F, donde $m \in \mathbb{Z}_{\geq 0}$

Esta conclusión se obtiene de la definición de espacio de Riemann-Roch asociado a un divisor (*página 30*) perteneciente al grupo de divisores del cuerpo de funciones racionales de una curva:

$$\mathcal{L}(m \cdot P_\infty) \coloneqq \{x \in K(\mathcal{X}) \mid (x) \geq -m \cdot P_\infty\} \cup \{0\}$$

donde $K(\mathcal{X})$ es el cuerpo de fracciones del anillo de coordenadas $K[x,y]/f(x,y)$, siendo $f(x,y)$ el polinomio descrito anteriormente para definir una curva de tipo $C_{a,b}$.

Corolario: las curvas $C_{a,b}$ son curvas admisibles.

Habíamos visto en 5.4 que las curvas superelípticas se podían escribir con la ecuación afín $y^m = f(x)$ para un polinomio $f \in K[X]$.

El siguiente enunciado es una consecuencia inmediata de la definición de curva superelíptica:

Las curvas superelípticas son curvas $C_{a,b}$.

Corolario: las curvas superelípticas son curvas admisibles.

Grupos de automorfismos de curvas $C_{a,b}$: sea $\mathcal{X}$ una curva $C_{a,b}$ como la definida anteriormente. ¿Se puede determinar el grupo de automorfismos de $\mathcal{X}$ sobre K en términos de a y b? Para los casos de géneros $g = 2, 3$ estos grupos se pueden determinar gracias al trabajo previo de varios autores (*véase* [17] *para curvas de género* 2 *y* [11], [12] *para curvas superelípticas de género* 3*. En* [16] *se estudia el caso de curvas no hiperelípticas de género* 3). Para géneros más altos

los grupos se pueden determinar si la curva $C_{a,b}$ es hiperelíptica o superelíptica. En general no se conoce un algoritmo para determinar el grupo de automorfismos de una curva algebraica.

Lema: sea $\mathcal{X}$ una curva $C_{a,b}$ de género $g = 2$ definida sobre K. Se cumple entonces que $Aut(\mathcal{X})$ es isomorfo a uno de los grupos siguientes:

1) $p = 3$: $\mathbb{Z}_2, V_4, D_4, D_6, GL_2(3)$.

2) $p = 5$: $\mathbb{Z}_2, \mathbb{Z}_{10}, V_4, D_4, D_6, GL_2(3)$.

3) $p \geq 5$: $\mathbb{Z}_2, V_4, D_4, D_6, GL_2(3)$.

Para el caso $p = 2$ ver [17] para detalles. Para $g = 3$ consultar [11], [12]. Los grupos de automorfismos de curvas superelípticas sobre un cuerpo K con $charK \neq 2$ se determinan completamente en [11], [12] y las correspondientes ecuaciones se determinan en [14].

5.7 EL LOCUS DE CURVAS $C_{a,b}$ EN EL ESPACIOS DE MÓDULOS

Vamos a realizar ahora una breve introducción a los espacios de Hurwitz y su proyección en el espacio de módulos $\mathcal{M}_g$, los cuales describimos como parte inicial de esta sección.

Para ello nos basaremos en [9], [18].

Los espacios de módulos surgen de forma natural en los problemas de clasificación geométricos: en geometría algebraica un espacio de módulos de curvas algebraicas es una variedad algebraica cuyos puntos representan clases de isomorfía de curvas algebraicas. El problema más básico corresponde al módulo de curvas no singulares sobre un cuerpo K con un género fijo g. Para el caso concreto del cuerpo de los números complejos, este espacio de módulos clasifica las superficies de Riemann compactas de género g, ya que el functor de Riemann nos dice que una clase biracional de curvas complejas es una clase de estructura conforme (superficie de Riemann) de una superficie.

Se sabe [9] que una superficie de Riemann compacta S de género g se puede embeber de forma analítica en el espacio proyectivo $\boldsymbol{P^{g+1}}$, de tal manera que la imagen es una curva proyectiva compleja no singular de grado $2g+1$. La estructura algebraica resultante sobre S es canónica.

Como consecuencia de lo anterior tenemos que una superficie de Riemann compacta de género cero es isomorfa a $\boldsymbol{P^1}$ (esfera de Riemann vista en 5.1) y que una superficie de Riemann de género uno es isomorfa a una curva no singular en $\boldsymbol{P^2}$ de grado 3, es decir una curva elíptica (o toro).

¿Qué podemos decir del grupo de automorfismos de una superficie de Riemann compacta S de género g? Si $g=0$ entonces asumimos que $S \cong \boldsymbol{P^1}$ y $Aut(\boldsymbol{P^1})$ es el grupo de transformaciones lineales

$$z \longmapsto \frac{(az+b)}{(cz+d)}$$

con $ad-bc \neq 0$ (ver [23]).

Si $g=1$, vimos en la sección 5.1 que S es isomorfa a un toro complejo y por lo tanto $Aut(S)$ está definido por el grupo de traslaciones del retículo G.

Para el resto de géneros ($g \geq 2$) se cumple que $Aut(S)$ es finito.

Denotamos por **espacio de módulos** $\mathcal{M}_g$ al conjunto de clases de isomorfismos de curvas no singulares de género g. De momento es solo eso, un conjunto, pero nuestro objetivo es dotar de alguna estructura adicional a $\mathcal{M}_g$ cuando $g \geq 2$. Existen varias aproximaciones, vamos a describir brevemente la aproximación original de Riemann, de carácter heurístico:

Método de Riemann para el cálculo del número de módulos: sabemos (*ver* [1]) que el espacio de recubridores $f: \mathcal{X} \longrightarrow \boldsymbol{P^1}$ con grado de ramificación d cuando $\mathcal{X}$ varía tiene dimensión $dim(\mathcal{M}_g) + 2d - g + 1$. Podemos calcular la dimensión de este espacio de otra forma: aplicando la fórmula de Riemann-Hurwitz, el número de puntos rama del recubridor sobre la esfera de Riemann es $2g + 2d - 2$; por el teorema de existencia de Riemann sabemos que existe un número finito de recubridores $f: \mathcal{X} \longrightarrow \boldsymbol{P^1}$ de grado d ramificados en los $2g + 2d - 2$ puntos. Luego el espacio de módulos parametrizando $2g + 2d - 2$ puntos distintos en la esfera de Riemann es el espacio cociente inducido por las clases de equivalencia de recubridores de tipo $\sigma = \{\sigma_1, \dots, \sigma_r\}$ (*ver espacios de Hurwitz en esta misma sección*), cuya dimensión es $r = 2g + 2d - 2$. Luego, igualando los dos términos:

$$dim(\mathcal{M}_g) + 2d - g + 1 = 2g + 2d - 2,$$

de donde obtenemos la dimensión del espacio de módulos

$$dim(\mathcal{M}_g) = 3g - 3.$$

Introducimos ahora los **espacios de Hurwitz**

Sea $\mathcal{X}$ una curva de género g y $f: \mathcal{X} \longrightarrow \boldsymbol{P^1}$ un recubrimiento de grado n con r puntos rama. Llamamos $q_1, \dots, q_r \in \boldsymbol{P^1}$ a los puntos rama. Sea $p \in \boldsymbol{P^1} \backslash \{q_1, \dots, q_r\}$**.** Elegimos lazos γ_i alrededor de q_i de forma que el grupo fundamental

$$\Gamma \coloneqq \pi_1(\boldsymbol{P^1} \backslash \{q_1, \dots, q_r\}, p) = \langle \gamma_1, \dots, \gamma_r \rangle, \ \ \gamma_1 \dots \gamma_r = 1$$

Siendo $\langle \gamma_1, \dots, \gamma_r \rangle$ una base de homotopía de Γ (cualquier conjunto de lazos que genera el grupo fundamental).

Vimos (*página 77*) que Γ actúa en cada fibra de $f^{-1}(p)$ de forma transitiva, induciendo un grupo transitivo G del grupo simétrico S_n (determinado por f hasta

conjugación en S_n). Se denomina **grupo de monodromía** de f. Las imágenes de $\gamma_1, \dots, \gamma_r$ en S_n forma una tupla de permutaciones $\sigma = \{\sigma_1, \dots, \sigma_r\}$ denominada **tupla de ciclos rama** de f. Llamamos a esa tupla la firma de f. Se dice que el recubrimiento $f: \mathcal{X} \longrightarrow \boldsymbol{P^1}$ es de tipo σ si tiene σ como tupla de ciclos rama relativa a una base de homotopía de $\boldsymbol{P^1} \backslash \{q_1, \dots, q_r\}$.

Dos espacios recubridores $f: \mathcal{X} \longrightarrow \boldsymbol{P^1}$ y $f': \mathcal{X}' \longrightarrow \boldsymbol{P^1}$ son débilmente equivalentes (resp. equivalentes) si existe un homeomorfismo $h: \mathcal{X} \longrightarrow \mathcal{X}'$ y un automorfismo analítico g: $\boldsymbol{P^1} \longrightarrow \boldsymbol{P^1}$ tal que $g \circ f = f' \circ h$ (resp. $g = 1$). Estas clases de equivalencia se denotan por $[f]_w$ (resp. $[f]$). El espacio de Hurwitz $\mathcal{H}_\sigma$ (resp. el espacio de Hurwitz simetrizado $\mathcal{H}_\sigma^S$) es el conjunto de clases de equivalencia débil (resp. clases de equivalencia) de recubridores de tipo σ. Este grupo induce en $\mathcal{H}_\sigma$ de forma natural una estructura de variedad cuasi proyectiva.

Sea $\mathcal{M}_g$ el espacio de módulos de las curvas de género g. Tenemos los siguientes morfismos

$$\begin{gathered} \mathcal{H}_\sigma \xrightarrow{\Phi_\sigma} \mathcal{H}_\sigma^S \xrightarrow{\bar{\Phi}_\sigma} \mathcal{M}_g \\ [f]_w \longrightarrow [f] \longrightarrow [\mathcal{X}] \end{gathered}$$

Cada componente de $\mathcal{H}_\sigma$ tiene la misma imagen en $\mathcal{M}_g$. Denotamos mediante

$$\mathcal{L}_g \coloneqq \bar{\Phi}_\sigma(\mathcal{H}_\sigma^S)$$

Decimos que el recubrimiento f o que la ramificación σ tiene dimensión de módulo $\delta \coloneqq dim \mathcal{L}_g$.

Volvamos a nuestro caso: sean a, b fijos; sabemos que $g = \frac{(a-1)(b-1)}{2}$. La curva genérica $C_{a,b}$ de género g tiene un recubrimiento de grado a $\pi_a: C_{a,b} \longrightarrow \boldsymbol{P}^1$ (resp. de grado b $\pi_b: C_{a,b} \longrightarrow \boldsymbol{P}^1$). La estructura de ramificación de $\pi_a: C_{a,b} \longrightarrow \boldsymbol{P}^1$ es $(a, 2, \dots, 2)$ donde el número de puntos rama es $d_a = b(a-1)+1$, como vimos en la sección anterior. Si $\mathcal{H}_a$ denota el espacio de Hurwitz de estos recubridores y $\mathcal{M}_a$ su imagen en $\mathcal{M}_g$ entonces la dimensión de $\mathcal{M}_a$ es $\delta_a \leq b(a-1)-2$. De forma similar se obtiene que la dimensión de $\mathcal{M}_b$ es $\delta_b \leq a(b-1)-2$. El espacio recubridor que nos interesa es el de menor grado.

Nuestro objetivo ahora es estudiar el espacio $\mathcal{M}_{a,b}$ para a, b fijos y en particular el caso $a = 3$ y $b = 4$. Para ello nos basamos en [18].

Ejemplo: sean $a = 3$ y $b = 4$, entonces el género de una curva $C_{a,b}$ es $g = 3$ y su ecuación es

$$Y^3 + \alpha_1 X^4 + \alpha_2 X^3 + \alpha_3 X^2 Y + \alpha_4 Y^2 X + \alpha_5 X^2 + \alpha_6 Y^2 + \alpha_7 XY + \alpha_8 X + \alpha_9 Y + \alpha_{10} = 0$$

Como la dimensión de $\mathcal{M}_3$ es 5 (estamos trabajando con las versiones afines de las curvas), entonces tiene que haber una "mejor" manera de escribir esta curva. El siguiente teorema nos ayudará en este sentido:

Teorema: toda curva de género 3 es una curva de tipo $C_{3,4}$. Se cumple además que toda curva $C_{3,4}$ definida sobre un cuerpo K es isomorfa a una curva con ecuación

$$f(x, y) = (x + b)y^3 + (cx + d)y^2 + (ex^2 + fx)y + x^3 + kx^2 + lx = 0$$

demostración (ver [18]).

Luego el espacio de las curvas de tipo $C_{3,4}$ se corresponde con el espacio de módulos $\mathcal{M}_3$. Es un problema interesante ver qué pasa con géneros superiores.

5.8 CÓDIGOS OBTENIDOS DE CURVAS TIPO $C_{a,b}$

En la última sección del capítulo de curvas $C_{a,b}$ vamos a dar un ejemplo (*extraído de* [18]) de códigos algebraico-geométricos construidos en base a curvas $C_{a,b}$. Estudiaremos la curva $y^3 = x^4 + 1$. Se trata de una curva de género $g = 3$ de tipo no hiperelíptica. Recordemos que un código AG $[n, k, d]$ con $d = n - k + 1$ se denomina *maximum distance separable code* o código MDS.

Sea $\mathcal{X}$ la curva con ecuación

$$y^3 = x^4 + 1$$

Definida sobre $\mathbb{F}_q$. Se trata de una curva de tipo $C_{3,4}$ cuyo género es $g = 3$. Para características $p \neq 2, 3$ el grupo de automorfismos de la curva es $C_4 \rtimes A_4$, cuya identidad en la librería *SmallGroup* del sistema de computación algebraica GAP es $(48, 33)$. Llamamos $\{P_1, \dots, P_n\}$ al conjunto de puntos racionales afines de $\mathcal{X}$ sobre $\mathbb{F}_q$. Sea $C = C_{\mathcal{L}}(D, G)$ el código AG, donde $n + 1$ es el número de puntos racionales de $\mathcal{X}$ y

$$G = mP_\infty, \qquad D = P_1 + \dots + P_n$$

Tenemos el resultado siguiente

Teorema: para el grupo de automorfismos $Aut(C)$ se tiene

1) Si $0 \leq m < 3$ o $m > n + 4$ entonces $Aut(C) \cong S_n$.
2) Si $n > 24$ y $4 \leq m < {}^{n}/_{2}$ entonces $Aut(C) \cong Aut_{D,mP_\infty}(\mathcal{X})$.

Demostración:

1) Si $0 \leq m < 3$ por la proposición de la página 94 sabemos que $(1, \dots, 1)$ es una base del espacio vectorial $\mathcal{L}(m \cdot P_\infty)$, luego $\ell(G) = 1$. Como $\ell(G - D) \geq 0$ entonces $dim C \geq 1$, que junto a $dim C = \ell(G) - \ell(G - D)$ nos da $dim C = 1$; por lo tanto $Aut(C) \cong S_n$.

Si $m > n + 4$ entonces $deg(G - D) > 2g - 2$. Luego $dimC = \ell(G) - \ell(G - D) = n$, con lo que C es todo el espacio y $Aut(C) \cong S_n$.

2) Teniendo en cuenta la notación definida para las curvas admisibles y el teorema de la página 91, tenemos $k = 3, l = 4,\ g = 3,\ \beta = 1, m \geq 4$. Para que se cumpla dicho teorema

$$n > max\left\{8, 2m, 18, 12(1 + \frac{2}{m-2})\right\}$$

Como $m \geq 4,\ 12(1 + \frac{2}{m-2}) \leq 24$. Luego cuando $n > 24$ y $4 \leq m < {}^{n}/_{2}$ el teorema aplica y tenemos $Aut(C) \cong Aut_{D,mP_\infty}(\mathcal{X})$.

Se puede comprobar que $C_{\mathcal{L}}(D, G)$ es un código MDS de tipo $[n, 1, n]$ cuando $0 \leq m < 3$ y MDS de tipo $[n, n, 1]$ cuando $m > n + 4$.

Ejemplo: sea $\mathcal{X}$ definida sobre $\mathbb{F}_{2^3}$. Tomamos $m = 4$; calculando con GAP (librería GUAVA) encontramos que $C_{\mathcal{L}}(D, G)$ es un código MDS de tipo $[8, 3, 6]$, cuya matriz generadora es

$$\begin{pmatrix} \alpha^5 & \alpha^3 & \alpha^6 & 1 & \alpha^4 & \alpha & \alpha^2 & 0 \\ \alpha^3 & \alpha^6 & \alpha^5 & 0 & \alpha^2 & \alpha^4 & \alpha & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Donde α es un elemento primitivo de $\mathbb{F}_{2^3}$. El grupo de automorfismos es $Aut(C) \cong \mathbb{Z}_{14}$.

6 CONCLUSIONES

Es un tema central de investigación, del cual hemos aportado alguna idea en este trabajo para el caso concreto de las curvas $C_{a,b}$, el hecho de que bajo determinadas condiciones, el grupo de automorfismos de los códigos algebraico-geométricos es isomorfo a un determinado subgrupo de automorfismos del cuerpo de funciones algebraicas asociado.

Todavía es una cuestión abierta la determinación de los grupos de automorfismos de códigos algebraico-geométricos obtenidos a partir de curvas tipo $C_{a,b}$ para cualquier característica del cuerpo base. Incluso la determinación del grupo de automorfismos de las curvas $C_{a,b}$ es una cuestión que está lejos de ser trivial.

Por otro lado, la determinación del locus de curvas $C_{a,b}$ definidas sobre $\mathbb{C}$ en el espacio de módulos $\mathcal{M}_g$ parece un problema de gran interés en sí mismo. Una curva $C_{a,b}$ genera espacios recubridores de grado a y b sobre la esfera de Riemann. El espacio de las curvas $C_{a,b}$ en $\mathcal{M}_g$ es la intersección de los espacios de Hurwitz de ambos recubridores. Hemos visto que el espacio $\mathcal{M}_3$ es el espacio de las curvas tipo $C_{3,4}$, pero para la generalización para cualquier a, b requiere un análisis cuidadoso de los espacios de Hurwitz correspondientes.

En los últimos años se ha realizado un importante avance para el caso de las curvas superelípticas. Las propiedades de este tipo de curvas son ampliamente conocidas y su grupo de automorfismos se ha determinado totalmente para todas las características, excepto para $p = 2$, gracias a los trabajos (*ver* [2]) de *R. Sanjeewa, T. Shaska, E. Bujalance, J. Cirre, G. Gamboa y G. Gromadzki (para la curvas hiperelípticas y trigonales); A. Wootton y A. Kontogeorgis (para las curvas superelípticas con grado p primo, general); G. Bartolini, A. Costa, T. Shaska y M. Izquierdo (para las curvas superelípticas reales).*

Todavía se desconoce si existe una relación precisa entre el grupo de automorfismos de un código algebraico-geométrico y el de la curva asociada, incluso para el caso de las curvas superelípticas, cuyo grupo de automorfismos es bien conocido.

Grandes progresos se han realizado también con relación al campo de aplicación de las curvas algebraicas sobre cuerpos finitos y sus cuerpos de funciones. Nueva áreas de aplicación se han abierto en los últimos años, como los "*stream ciphers*", "*hash functions*" y esquemas de autenticación en criptografía. En todos estos casos los métodos de la geometría algebraica han sido más exitosos que las aproximaciones clásicas. Sin embargo, hay que prestar especial atención a los últimos avances en las aplicaciones prácticas en el campo de la criptografía cuántica, materia que tan

solo hace unos años parecía restringida al mundo de la teoría, y que promete ser la solución definitiva al paradigma de las comunicaciones seguras, dada su naturaleza intrínseca de carácter infranqueable.

7 REFERENCIAS

[1] S. Abhyankar. Coverings of algebraic curves. Amer. J. Math., 79 (1957), 825-856.

[2] L. Beshaj, T. Shaska, and E. Zhupa (eds.), Advances on superelliptic curves and their applications. Based on the NATO Advanced Study Institute (ASI), Ohrid, Macedonia, 2014., Amsterdam

[3] H.S.M. Coxeter and W.O.J. Moser, Generators and Relations for Discrete Groups. Springer-Verlag, Berlin, Heidelberg, 1957.

[4] A. Elezi and T. Shaska, Quantum codes from superelliptic curves, Albanian J. Math. 5 (2011), no. 4, 175–191 (201305).

[5] J. M. Gamboa Mutuberría y J. M. Ruíz Sancho, Anillos y Cuerpos Conmutativos, Universidad Nacional a Distancia (UNED), Madrid 2002.

[6] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. 24, No. 1, 1981,pp. 170-172.

[7] M. Izquierdo and Tony Shaska, Cyclic curves over the reals (201501).

[8] G. A. Jones and D. Singerman. Complex Functions, and algebraic and geometric viewpoint. Cambridge University Press, Cambridge, 1988.

[9] E. Looijenga. A minicourse on Moduli of Curves. Lecture given at school on Algebraic Geometry, Trieste, 26 July – 13 August 1999.

[10] C. Munuera, A. Sepúlveda and F. Torres, Generalized Hermitian codes over *GF*(*qr*), preprint, 2009.

[11] R. Sanjeewa, Automorphism groups of cyclic curves defined over finite fields of any characteristics, Albanian J. Math. Vol. 3, Number 4, 2009, 131-160 (201301)

[12] R. Sanjeewa and T. Shaska, Determining equations of families of cyclic curves, Albanian J.Math. VOL 2, NO 3 (2008) (201301).

[13] F. Sebé, Algorithms for the Construction of Elliptic Curves with Given Cardinality, Master Thesis of Master en Matemáticas Avanzadas (UNED).

[14] T. Shaska, Subvarieties of the hyperelliptic moduli determined by group actions, SerdicaMath. Journal, No. 4, 355-374, 2006 (201302).

[15] T. Shaska and C. Shor, Weierstrass points of superelliptic curves (201502)

[16] T. Shaska and J. Thompson, On the generic curve of genus 3, Affine algebraic geometry, 2005, pp. 233–243.

[17] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus 2 function fields, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703-723.

[18] T. Shaska and Q. Wang, On the automorphism groups of some AG-codes based on *Ca*,*b* curves. *Serdica J. Comput.* 1 (2007), no. 2, 193–206.

[19] H. Stichtenoth, "A note on Hermitian codes over GF(*q*2)," IEEE Trans. Inf. Theory, vol. 34, no. 5, pt. 2, pp. 1345–1348, Sep. 1988, Coding techniques and coding theory.

[20] H. Stichtenoth, Algebraic Function Fields and Codes, second edition, Graduate Texts in Mathematics, 2009 Springer-Verlag Berlin Heidelberg.

[21] S. Wesemeyer, On the automorphism group of various Goppa codes, IEEE Trans. Inform. Theory 44 (1998).

[22] S. Yang, Improvements on parameters of algebraic-geometry codes from Hermitian curves. *IEEE Trans. Inform. Theory* 55 (2009), no. 1.

[23] Apuntes de la asignatura Superficies de Riemann, del Master en Matemáticas Avanzadas (especialidad Geometría y Topología) de la Universidad Nacional de Educación a Distancia (UNED).