Construcción de curvas algebraicas maximales sobre cuerpos finitos

escrito por

JOSÉ DAVID VILLANUEVA GARCÍA

Tutores

Milagros Izquierdo Barrios

Antonio F. Costa González

Facultad de Ciencias

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Trabajo presentado para la obtención del título de
Máster Universitario en Matemáticas Avanzadas de la UNED.
Especialidad Geometría y Topología.

OCTUBRE 2018

Abstract

Abstract:

Este trabajo describe la construcción de curvas maximales sobre cuerpos finitos, cubiertas por curvas hermitianas. Existe un gran interés en las curvas algebraicas sobre cuerpos finitos con muchos puntos racionales, ya que son utilizadas para la construcción de códigos correctores de errores, es decir, añadir información redundante a un mensaje con el propósito de ser recuperado en el caso de producirse errores . Explicamos las herramientas necesarias para abordar este tema, como parte de la Teoría de Anillos y Cuerpos, y analizamos el artículo On Certain Subcovers of the hermitian Curve, escrito por Arnaldo Garcá, Motoko Q. Kawakita y Shinji M, donde se detalla un método para la construcción de estas curvas maximales.

Al final del trabajo, se presentan varias tablas describiendo diferentes representaciones de algunos cuerpos finitos y las tablas de los puntos racionales de las curvas maximales que hemos obtenido aplicando el método descrito en el artículo. Todas estas tablas han sido obtenidas mediante la ejecución de un programa desarrollado en JAVA, ad-hoc, el cual puede ser generalizado para cualquier cuerpo finito y la evaluación de sus puntos en cualquier curva dada.

Abstract:

This thesis surveys the construction of maximal curves over finite fields covered by Hermitian curves. Currently there is a great interest in algebraic curves over finite field which have many rational points, because they are widely used for the construction of error correcting codes, that means, adding redundant data to a message in order to be recovered even when errors are introduced. We explain the necessary tools to address this topic, like part of the Ring and Field Theory and we analyze the paper titled On Certain Subcovers of the Hermitian Curve, written by Arnaldo García, Motoko Q. Kawakita and Shinji M, where it is explained in detail one method to construct such that maximal curves.

At the end of this thesis, we present some tables describing different representations of finite fields, and some tables containing the rational points of the maximal curves obtained by using the method described in that paper. All these tables have been generated through the execution of one application developed in JAVA programming language, ad-hoc, which could be generalized to get any finite field and for the evaluation of its points in any given curve.

Keywords: Group, Ideal, Field, Nullstellensatz, Variety, Rational function field, Curve, Field extensions, Riemann-Roch Theorem, Ramification, Covering, Hasse-Weils bound

Dedicatoria y agradecimientos

A Mi padre Antonio.

Cuando de niño dejaba de realizar mis tareas escolares, me animabas y exigías dedicación a los estudios. Ya de adulto, todavía me parece escuchar tu voz de ánimo cuando en ciertos momentos de la realización de esta tesis me sentía cansado o con ganas de abandonar.

“Un buen padre vale por cien maestros".

(Jean Jacques Rousseau).

Quisiera dar mi más sincero agradecimiento a Milagros Izquierdo por orientarme desde el primer día en la dirección correcta para desarrollar este trabajo, enseñarme a ser más cuidadoso y por haberme mostrado la manera de afrontar la investigación en Matemáticas.

También quisiera dar las gracias a mi esposa Myriam por su paciencia y ánimos durante todos estos meses.

NOMENCLATURE

$K\mathbb{A}^n$ Espacio afín de dimensión n sobre el cuerpo K

$K\mathbb{P}^n$ Espacio proyectivo de dimensión n sobre el cuerpo K

$[F:K]$ Grado de una extensión finita de cuerpos

$\#\mathscr{C}(\mathbb{F}_\ell)$ Número de puntos racionales de una curva proyectiva sobre el cuerpo $\mathbb{F}$

$\Gamma(V)$ Anillo de coordenadas de la variedad V

$\mathbb{F}_q$ Cuerpo finito de orden q

$\mathbb{P}(F)$ Conjunto de plazas del cuerpo de funciones algebraicas F

$\mathscr{H}$ Curva Hessiana

$\mathscr{K}$ Divisor canónico un cuerpo de funciones

$\mathscr{O}$ Anillo local

$\mathscr{O}^\times$ Grupo formado por las unidades del anillo de valuación $\mathscr{O}$

$\mathscr{C}$,$\mathscr{F}$ Curva plana afín y proyectiva

$\mathscr{H}$ Curva hermitiana

$\mathscr{P}$ Función de Weierstrass

$\overline{K}$ Clausura algebraica del cuerpo K

$\sum$ Esfera de Riemann

$deg(P)$ Grado de la plaza P

$div(F)$ Grupo de divisores de F

F/K Extensión de cuerpos

g Género de un cuerpo de funciones

I Ideal

$I(V)$ Ideal de la variedad V

K Cuerpo

$K(X)$ Cuerpo de funciones racionales

$K[X]$ Anillo de polinomios en la indeterminada X sobre el cuerpo K

P Plaza

R Anillo

$Rad(I)$ Radical del ideal I

V Variedad / Conjunto algebraico

$v()$ Valuación discreta

$Z[i]$ Enteros de Gauss

TABLA DE CONTENIDOS

ÍNDICE DE CUADROS

TABLA **Página**

Índice de figuras

Figura **Página**

CAPÍTULO 1

INTRODUCCIÓN

Las curvas siempre han sido de gran interés para los matemáticos, y el origen de su estudio de manera sistemática se remonta a la antigua Grecia, donde matemáticos como Euclides o Diofanto se planteaban y resolvían muchas cuestiones sobre muchos tipos de curvas. Algunas de estas curvas, como las cónicas, pertenecen a la categoría de lo que hoy denominamos como curvas algebraicas. El caso de las curvas algebraicas definidas sobre cuerpos finitos es quizás el que más se ha estudiado y desarrollado en los últimos años, debido a sus aplicaciones en campos como la criptografía o la ingeniería.

La Teoría de Códigos Correctores tuvo su inicio en las investigaciones de los matemáticos Golay, Hammig y Shannon, en los Laboratorios Bell, en la década de 1940. Al mismo tiempo, los matemáticos Hessel y Weil hallaban una fórmula para acotar el número de puntos racionales de una curva algebraica sobre un cuerpo finito. Las curvas que cumplen esta igualdad se denominan curvas maximales. Estas curvas son las que tienen el máximo número de puntos racionales de acuerdo con la fórmula de Hessel-Weil.

Posteriormente, en la década de los 70 del siglo pasado, el matemático ruso V. D. Goppa se dio cuenta de que, asociando códigos con ciertos divisores de cuerpos de funciones algebraicas, es decir curvas planas, se pueden construir gran cantidad de códigos, y construye códigos lineales (o llamados códigos Algebraico-Geométricos).

A partir de ese momento, se despierta entre matemáticos un gran interés por las curvas sobre cuerpos finitos, y la construcción de curvas definidas sobre $\mathbb{F}_q$ con muchos puntos racionales respecto a su género, debido a las aplicaciones que tienen éstas en la Teoría de Códigos. Por lo tanto, durante las últimas décadas, los códigos Algebraico-Geométricos han sido un gran campo de investigación.

Un código corrector de errores es un subespacio de un cuerpo finito $\mathbb{F}_{q^n}$, es decir, es un espacio

vectorial de $k < n$ dimensiones sobre $\mathbb{F}_q$. Son ampliamente utilizados en muchas situaciones las cuales tienen como característica común que la información procedente de alguna fuente se transmite por un canal de comunicación ruidoso a un receptor. Lo que hará Goppa será construir un método que permite definir códigos con buenas propiedades a partir de curvas definidas sobre cuerpos finitos. El Teorema de Riemann-Roch proporciona buenas estimaciones para estas propiedades de los códigos.

Una de las cosas más interesante desde el punto de vista de la criptografía y los códigos correctores, es que la curva tenga muchos puntos racionales con respecto a su género, ya que usando este tipo de curvas se pueden construir códigos correctores de calidad.

También se usan curvas algebraicas sobre cuerpos finitos en el protocolo Bitcoin, específicamente el algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm) para la creación de las claves privadas y públicas. Este algoritmo es una variante del clásico algoritmo DSA (Digital Signature Algorithm), que usa la critografía asimétrica o de clave pública. La criptografía utilizando curvas elípticas es mucho más rápida y proporciona un nivel de seguridad superior. Por ejemplo, una clave de 256 bits basada en la criptografía de las curvas elípticas, puede dar el mismo nivel de seguridad que una clave de 2048 bits generada con el clásico algoritmo RSA, con la ventaja adicional de que se puede reducir el espacio de almacenamiento y el de transmisión de la clave.

Resumen de los capítulos

Capítulo 2

En este capítulo revisaremos importantes conceptos para el posterior desarrollo del trabajo, como el concepto de anillo, anillo local, anillo de valuación, anillo noetheriano y cuerpos. Uno de los conceptos más importantes es el de extensión algebraica de cuerpos, ya que veremos las curvas como cubiertas de la recta proyectiva (cubiertas que corresponden a extensiones sobre cuerpos de funciones, los llamados cuerpos de funciones algebraicas).

Capítulo 3

En este capítulo explicamos el concepto de curvas planas y de variedades. En la primera parte nos centraremos en variedades y curvas afines, mientras que en la segunda parte veremos las variedades y curvas definidas en el plano proyectivo. Un concepto importante en este capítulo es el Nullstellensatz, tanto para curvas afines como proyectivas, un resultado muy importante que relaciona dos grandes campos de las matemáticas como son la Geometría y el Álgebra.

Capítulo 4

En este capítulo se introducen los conceptos de cuerpos de funciones algebraicas, plazas (que serán los puntos de las curvas), puntos racionales y el Teorema de Riemann-Roch, que une las propiedades algebraicas y topológicas de una curva.

Capítulo 5

En el capítulo 5, introducimos el concepto de ramificación y hablaremos sobre curvas como cubiertas de la recta proyectiva. Estas cubiertas están definidas por morfismos entre curvas y

veremos algunos ejemplos como el de las funciones meromorfas y las funciones elípticas.

Capítulo 6

En este capítulo construiremos extensiones de cuerpos finitos y curvas algebraicas maximales sobre estos cuerpos, siguiendo el método explicado en el artículo On Certain Subcovers of the Hermitian Curve, de los autores Arnaldo García, Motoko Q. Kawakita y Shinji Miura. Explicamos los pasos seguidos en el artículo para obtener las cubiertas y obtenemos curvas maximales que son cubiertas por una determinada curva hermitiana.

Finalmente, damos las tablas de todos los puntos racionales de las curvas maximales obtenidas en el Capítulo 6 sobre sus respectivos cuerpos, y construimos los cuerpos F_{16}, F_{64} y F_{81} a partir de algunos de sus polinomios primitivos, dando la tabla con su representación numérica y en forma de potencia de una raíz primitiva.

También proporcionamos el código fuente en el lenguaje de programación JAVA que ha sido utilizado para la obtención de las tablas descritas anteriormente.

CAPÍTULO 2

CONCEPTOS PRELIMINARES

Empezaremos estudiando en esta sección las propiedades generales de los grupos, anillos y cuerpos, conceptos básicos en toda teoría algebraica. A partir de estos conceptos, definiremos las variedades, las curvas y, en capítulos posteriores, las plazas en curvas. Las siguientes definiciones pueden encontrarse en [2] y [18].

2.1. Grupos, anillos y cuerpos

Definición 2.1. Un **grupo** es un conjunto de elementos $\{g_1, g_2, \dots\}$ dotados de una ley de composición $\cdot$ (multiplicación), que a cada par ordenado $g_i, g_j \in G$ le asigna otro elemento $g_i \cdot g_j$ de forma tal que se satisfacen las siguientes propiedades:

1. La ley de composición es interna, es decir si $g_i, g_j \in G$, entonces $g_i \cdot g_j \in G$ (cierre) .
2. Para todo $g_i, g_j, g_k \in G$, $g_i \cdot (g_j \cdot g_k) = (g_i \cdot g_j) \cdot g_k$ (asociativa).
3. Existe un único elemento, denotado usualmente e, con la propiedad de que para todo $g_i \in G$, $e \cdot g_i = g_i \cdot e = g_i$ (elemento unidad).
4. Para cada g_i existe un único elemento g_i^{-1} tal que $g_i^{-1} \cdot g_i = g_i \cdot g_i^{-1} = e$ (elemento inverso).

Si la ley de composición interna es conmutativa, decimos que el grupo es un grupo abeliano.

Ejemplo 2.1. Sea el grupo cíclico C_{15}, y sea $a = 2$ el generador del grupo. Podemos representarlo como

$$C_{15} = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, a^{15} = 1\}$$

donde tenemos que la tabla de multiplicación viene dada por la ecuación $a^4 = a^3 + 1$.

$$a, a^2 = 4, a^3 = 8, a^4 = 9, a^5 = 11, a^6 = 15, a^7 = 7, a^8 = 14, a^9 = 5, a^{10} = 10, a^{11} = 13,$$

$$a^{12} = 3, a^{13} = 6, a^{14} = 12, a^{15} = 1.$$

Los respectivos valores numéricos vienen dados por la representación binaria de los números del 1 al 15.

Ejemplo 2.2. $\mathbb{Q}^* = (\mathbb{Q}^* \setminus \{0\})$, con el producto habitual, es un grupo abeliano.

Ejemplo 2.3. Sea $Q_8 = \{1, -1, j, -j, k, -k, l, -l\}$ el grupo de los cuaterniones, cuya multiplicación $\cdot$ está determinada por: $(-1)\cdot(-1) = 1$, $j^2 = k^2 = l^2 = -1$, $j \cdot k = l$, $k \cdot j = -j \cdot k$, $k \cdot l = j = -l \cdot k$, $l \cdot j = k = -j \cdot l$, con la regla usual de los signos. Tenemos que $(Q_8, \cdot)$, es un grupo no abeliano.

Ejemplo 2.4. Sea el conjunto de los números reales $\mathbb{R}$ y sea $\mathbb{R}[X]$ el conjunto de polinomios en la indeterminada X con coeficientes reales. Entonces $(\mathbb{R}[X], +)$ es un grupo abeliano, donde $+$ representa la suma habitual de polinomios, es decir, la suma se hace término a término.

Las siguientes definiciones y conceptos básicos sobre anillos pueden encontrarse en [18].

Definición 2.2. Un anillo unitario (o anillo con uno) R es un conjunto dotado con dos operaciones cerradas, $+$ y $\cdot$ (suma y multiplicación), de modo que se verifican las siguientes propiedades:

1. R es un grupo abeliano con respecto a la suma $+$.
2. La multiplicación $\cdot$ es una operación asociativa en R.
3. Existe un elemento 1 no nulo tal que para todo $a \in R$, $1 \cdot a = a \cdot 1 = a$. Este elemento es el uno de anillo.
4. Se cumplen las leyes distributivas, es decir para todo $a, b, c \in R$,

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

Se dice que el anillo R es conmutativo si la operación de multiplicación es conmutativa. A partir de este momento, salvo que digamos lo contrario, todos los anillos serán conmutativos.

Ejemplo 2.5. $\mathbb{Z}_p$, con p primo es un anillo con uno.

Definición 2.3. Un elemento no nulo en un anillo unitario R se denomina **unidad** si tiene inverso multiplicativo, es decir, el elemento $a \in R$ es una unidad, si existe un elemento $b \in R$ tal que $a \cdot b = 1$. El conjunto formado por las unidades del anillo junto con la multiplicación forman un grupo abeliano.

Ejemplo 2.6. El conjunto $\mathbb{Z}$, con las operaciones usuales de suma y multiplicación, forman un anillo conmutativo unitario, con elemento unidad 1 y -1.

Ejemplo 2.7. Sea el conjunto $M = \{3n \mid n \in \mathbb{Z}\}$ el conjunto de todos los enteros múltiplos de 3. Junto con las operaciones de suma y multiplicación usuales, forman un anillo. Sin embargo, este anillo carece de elemento uno, por lo que no es **un anillo con uno**.

Ejemplo 2.8. Sea K un cuerpo (ver definición 2.7) y el anillo de polinomios en una indeterminada $K[X]$. Las unidades de $K[X]$ son las unidades de K, es decir $K \setminus \{0\}$.

Definición 2.4. Sea R un anillo. Un elemento $q \in R$, $q \neq 0$, es **irreducible**, si q no es unidad, y si $q = ab$, entonces a ó b son unidades.

Ejemplo 2.9. a) Sea R un anillo conmutativo. El conjunto de polinomios en la indeterminada X con coeficientes en el anillo R es el conjunto de todas las sumas formales finitas

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

donde X es un nuevo elemento.
En el conjunto de polinomios definimos una suma y un producto:
Sean $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, $g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$ dos polinomios. Supongamos que $m \leq n$ y tomamos $b_i = 0$ para todo $n \geq i > m$. Con este convenio definimos

$$f + g = (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$
$$f \cdot g = a_n b_n X^n + m + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1)X + a_0 b_0.$$

Tenemos entonces que el conjunto $R[X]$ con las dos operaciones definidas forma un anillo conmutativo que se llama anillo de polinomios en X con coeficientes en R.

El elemento neutro para la suma es el polinomio nulo, $p(X) = 0$, y el uno del anillo es el polinomio $p(X) = 1$.

b) De acuerdo a la definición anterior, un polinomio f en el anillo $R[X_1, X_2, \cdots, X_n]$ de polinomios en las indeterminadas $X_1, X_2, \cdots, X_n$ es **reducible** si existen dos polinomios no constantes f_1, f_2 en $R[X_1, X_2, \cdots, X_n]$ con $f = f_1 \cdot f_2$. En caso contrario, decimos que f es irreducible.

- El grado de un monomio $X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n}$ es $r_1 + r_2 + \cdots + r_n$.
- Un polinomio es homogéneo si todos sus términos tienen el mismo grado.
- El grado de un polinomio f es el grado más grande de todos sus términos. Lo denotamos por $degf$.

Ejemplo 2.10. Sea el polinomio $f = y^3 + xy^2 + x^2(x - y) \in \mathbb{R}[x, y]$. El grado de cada monomio es 3, por lo que el polinomio es homogéneo.

Definición 2.5. En un anillo A, un elemento $a \in A$ no nulo es un **divisor de cero** si existe otro elemento $b \in A$ tal que $a \cdot b = 0$.

Ejemplo 2.11. El anillo de los números enteros $\mathbb{Z}$ no tiene divisores de cero. Sin embargo, en el anillo $\mathbb{Z} \times \mathbb{Z}$, donde la suma y el producto se realizan sumando y multiplicando componentes, tenemos que $(0,1) \times (1,0) = (0,0)$, por lo que ambos $(0,1)$ y $(1,0)$ son divisores de cero.

Definición 2.6. Sea R un anillo. Se dice que R es un **dominio integral** (DI) si para todo $a, b \in R$, si $a \cdot b = 0$, entonces $a = 0$ ó $b = 0$.
Es decir, un dominio integral es un anillo que no tiene ningún divisor de cero.

Ejemplo 2.12. El conjunto $\mathbb{Z}[i] = \{r + si \mid r, s \in \mathbb{Z}\}$, llamado enteros de Gauss, junto a las operaciones de suma y multiplicación habituales en los números complejos, forman un **anillo con uno conmutativo**, que además es dominio integral.

Ejemplo 2.13. Sea el anillo $\mathbb{M}(2)$ de las matrices 2×2 con las operaciones de suma y multiplicación habituales. Tenemos que

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

por lo que el $\mathbb{M}(2)$ es un anillo con uno, pero no es un dominio integral, al tener divisores de cero.

A partir de ahora, salvo que digamos lo contrario, consideramos que todos los anillos son unitarios.

Definición 2.7. Un **cuerpo** K es un anillo tal que $K \setminus \{0\} = K^\times$ es un grupo abeliano con respecto a la multiplicación, llamado grupo multiplicativo. Un cuerpo K se dice que es finito (o cuerpo de Galois) si consta de un conjunto finito de elementos.

Se llama **característica** de K ($charK$) al menor número natural p tal que $p \cdot 1 = 0$. Si este número no existe, diremos que K tiene característica cero.

Ejemplo 2.14. $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Q}$ con las operaciones de suma y multiplicación habituales son cuerpos y tienen característica cero. El conjunto de los enteros módulo p, $\mathbb{Z}_p = \mathbb{F}_p$ con p primo y con las operaciones de suma y multiplicación modulares habituales, forman un cuerpo con característica p.

Sin embargo, $\mathbb{Z}_4 = \{0,1,2,3\}$, junto con las operaciones de suma y multiplicación modulares habituales, no es un cuerpo, ya que el elemento 2 no es unidad.

Ejemplo 2.15. El cuerpo $\mathbb{F}_4 = \{0,1,2,3\}$ con la suma habitual y la tabla de multiplicación dada por $2^2 = 3$, $3^2 = 2$ y $2 \cdot 3 = 1$ es un cuerpo de cuatro elementos de característica 2.

También el cuerpo $\mathbb{F}_{16}$ con la suma habitual y la multiplicación dada en el ejemplo 2.1 es un cuerpo de orden 16 y característica 2.

Definición 2.8. Sea K un cuerpo. Si $f(X), g(X) \in K[X]$ son dos polinomios, los elementos de la forma $h(X) = \frac{f(X)}{g(X)}$, con $g(X) \neq 0$, forman un cuerpo con la suma y multiplicación habituales. Se denomina **cuerpo de funciones racionales** en X sobre el cuerpo K, y lo denotamos por $K(X)$.

Ejemplo 2.16. Los números racionales $\mathbb{Q}$ son el cuerpo de las fracciones del dominio integral de los enteros $\mathbb{Z}$. Como cada número racional es una clase de equivalencia, tenemos que puede representarse por diferentes fracciones, obviamente todas equivalentes entre si. Hay, sin embargo, una fracción que es especialmente simple en cada clase, la fracción reducida. Este es un ejemplo de los llamados **cuerpos de fracciones** que veremos posteriormente.

Ejemplo 2.17. El cuerpo de funciones racionales $K(X)$ definido anteriormente, es un cuerpo de fracciones.

2.1.1. Cuerpos de fracciones de un dominio integral

Si A es un DI, construiremos un cuerpo que contendrá a A y que estará formado por las "fracciones" de elementos de A . Tal cuerpo se llama el **cuerpo de las fracciones de** A .

Definición 2.9. sea A un domino integral. Se denomina **cuerpo de fracciones** de A al mínimo cuerpo que contiene al dominio.
Dicho cuerpo siempre existe.

Ejemplo 2.18. Considerando el cuerpo de fracciones $Z(i)$ de los enteros de Gauss definidos anteriormente, tenemos el siguiente isomorfismo

$$Z(i) \simeq \{c + di \mid c, d \in \mathbb{Q}\}.$$

Ejemplo 2.19. Sea A un dominio integral y el anillo de polinomios en dos indeterminadas $A[X,Y]$, el cual es un dominio integral al serlo A. Definimos su cuerpo de fracciones $K(X,Y)$ como

$$K(X,Y) = \left\{ \frac{P(X,Y)}{Q(X,Y)} \mid P, Q \in K(X,Y), Q \neq 0 \right\}.$$

2.1.2. Ideal

El concepto de ideal generaliza el estudio de la divisibilidad del conjunto de los números enteros $\mathbb{Z}$. Podemos consultar los conceptos de esta sección en [18].

Definición 2.10. sea un anillo R y un subconjunto $I \subset R$. Se dice que I es un **ideal** del anillo A si cumple las siguientes condiciones:

1. $(I, +)$ es un subgrupo de $(R, +)$.
2. Para todo $a \in I$ y todo $b \in R$, $a \cdot b \in I$.

3. La unidad multiplicativa $1 \in I$ si y sólo si $I = R$

Si $a \in R$, el ideal generado por a es el conjunto $(a) = \{ra \mid r \in R\}$.
Si $I \neq \{0\}, R$, decimos que I es un ideal propio del anillo R.
Si I es generado por un único elemento, decimos que I es un **ideal principal** del anillo R.

Ejemplo 2.20. Sea el anillo conmutativo $(\mathbb{Z}_4, +, \cdot)$, siendo la suma y la multiplicación modulares habituales . Es fácil comprobar que los ideales de $\mathbb{Z}_4$ son $I_1 = \{0\}$, $I_2 = \{0,2\}$ y $I_3 = \mathbb{Z}_4$. Vemos que I_2 es un ideal propio de $\mathbb{Z}_4$.

Ejemplo 2.21. El ideal $I = (6,10) \subset \mathbb{Z}$ es principal, ya que es fácil probar que $I = (2)$.

Definición 2.11. Sea R un anillo conmutativo e I un ideal de R. Se dice que I es **maximal** si I es un ideal propio y no está estrictamente contenido en ningún otro ideal propio.

Ejemplo 2.22. El ideal $I = (2) \subset \mathbb{Z}$ es maximal, ya que si intentamos "añadir" a I un número impar, $2n+1$, entonces, también debería estar $(2n+1) + (-n)2 = 1$, y por lo tanto todo $\mathbb{Z}$.

Ejemplo 2.23. El ideal $I = (9) \subset \mathbb{Z}$ no es maximal, ya que $(9) \nsubseteq (3) \nsubseteq \mathbb{Z}$.

Ejemplo 2.24. Sea el anillo de polinomios sobre el cuerpo $\mathbb{R}[X]$. Sea el ideal generado por el polinomio $p(X) = X^2 + 1$, el cual es irreducible Entonces $\mathbb{R}[X]/(p(X))$ es un cuerpo isomorfo al cuerpo de los números complejos $\mathbb{C}$. Esbozamos la demostración que puede ser consultada completa en [8].

El polinomio $p(X) \in \mathbb{R}[X]$ es irreducible, por lo que el ideal (p) constituido por los múltiplos de $p(X)$ es ideal maximal del anillo $\mathbb{R}[X]$. Definimos las operaciones de suma y producto en $\mathbb{R}[X]/p(X)$ de la siguiente forma:

Para toda clase de polinomios $[p_1(X) + (p)]$, $[p_2(X) + (p)] \in \mathbb{R}[X]/p(X)$, las operaciones suma y multiplicación están bien definidas:

$$[p_1(X) + (p)] + [p_2(X) + (p)] = [p_1(X) + p_2(X)] + (p)$$

$$[p_1(X) + (p)] \cdot [p_2(X) + (p)] = [p_1(X) \cdot p_2(X)] + (p).$$

Obviamente, $\mathbb{R}[X]/p(X)$ tiene estructura de cuerpo con las operaciones definidas, y los elementos de $\mathbb{R}[X]/p(X)$ pueden representarse por pares de números reales (a,b) ya que cada clase de equivalencia tiene un representante q de la forma $a + bx$. Así, el cuerpo $\mathbb{R}[X]/p(X)$ es isomorfo al cuerpo de los números complejos $\mathbb{C}$, es decir, $a + bx \leftrightarrow (a,b)$.

Definición 2.12. Sea el anillo de polinomios $R[X_1, X_2, \cdots, X_n]$. Si $f_1, f_2, \cdots, f_s \in R[X_1, X_2, \cdots, X_n]$ entonces el **ideal generado por los polinomios** $f_1, f_2, \cdots, f_s$ es:

$$(f_1, f_2, \cdots, f_s) = \sum_{i=1}^{s} h_i f_i : h_1, h_2, \cdots, h_s \in R[X_1, X_2, \cdots, X_n].$$

En el caso particular de un solo polinomio f, tenemos que

$$(f) = fR[X_1, X_2, \cdots, X_n] = \{fh : h \in R[X_1, X_2, \cdots, X_n]\} = \{g \in R[X_1, X_2, \cdots, X_n] : f \mid g\}.$$

En general, dado un dado un anillo R y un ideal $I \subset R$, podemos establecer la relación de equivalencia $a, b \in R$, $a \sim b \leftrightarrow a - b \in I$ que establece el conjunto cociente R/I, que hereda la estructura de anillo.

Definición 2.13. Sea R un anillo unitario e I un ideal de R. Se dice que I es un **ideal primo** si se cumple la siguiente propiedad: si el producto de dos elementos del anillo R pertenece al ideal I, entonces alguno de los dos elementos pertenece a I, es decir, si

$$a, b \in R, a \cdot b \in I \Longrightarrow a \in I \text{ ó } b \in I.$$

Si un elemento $a \in R$ genera un ideal primo, diremos que a es **primo**. Por o tanto, tenemos que si el elemento p es primo para todo $a, b \in R$ tal que $p | a \cdot b$, entonces $p | a$ ó $p | b$.

Ejemplo 2.25. Sea $p(X) = X^2 - 1 \in \mathbb{Q}[X]$ y el ideal que genera $I = \left(X^2 - 1\right)$. Sean $q(X), h(X) \in \mathbb{Q}[X]$ con $q(X) = X + 1$ y $h(X) = X - 1$. Tenemos entonces que I no es primo, ya que $p(X) = q(X)h(X)$ y ninguno de los factores $q(X)$, $h(X)$ pertenecen a I.

Ejemplo 2.26. a) Todo ideal maximal es primo. Por ejemplo, el ideal $I = (X - 1)$ del anillo de polinomios $\mathbb{Q}[X]$ es un ideal maximal y, por lo tanto, primo.

b) Sea K un cuerpo. En general, si $p(X) \in K[X]$ es irreducible, el ideal $(p(X))$ es maximal y, por lo tanto, primo.

Recordemos que un ideal principal es un ideal que es generado por un sólo elemento.

Definición 2.14. Un **dominio de ideales principales** (DIP) es un dominio integral en el que todos sus ideales son principales.

Ejemplo 2.27. Si R es un cuerpo, el anillo de polinomios $R[X]$ en una indeterminada es un DIP.

Ejemplo 2.28. El anillo de polinomios $R[X_1, \cdots, X_n]$ en n indeterminadas nunca es un DIP para $n \geq 2$, ya que $\left(X_{1,} X_2\right)$ no puede estar generado por un elemento ya que X_i no es unidad.

Una de las propiedades fundamentales del anillo de los números enteros es que todo entero se expresa de manera única como un producto de números primos. Esta propiedad se generaliza en forma natural a los dominios integrales, originándose as así el concepto de dominio de factorización única.

Definición 2.15. Un **dominio de factorización única** (DFU) es un dominio integral en el que se cumplen las siguientes dos condiciones:

1. Todo elemento irreducible es primo.

2. Todo elemento no nulo que no sea unidad es producto de elementos irreducibles.

Ejemplo 2.29. Sea K un cuerpo. En el anillo $K[X]$ los polinomios irreducibles son los elementos primos del anillo. Además, $K[X]$ es un dominio de factorización única, al ser un dominio de ideales principales.

Ejemplo 2.30. Tenemos que un dominio de ideales principales es un dominio de factorización única, y éste es un domino de integral.

Ejemplo 2.31. $DI \not\Rightarrow DFU$, por ejemplo: $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5}, a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$.

Ejemplo 2.32. $DFU \not\Rightarrow DIP$: por ejemplo $\mathbb{Z}[X]$ (al ser el anillo $\mathbb{Z}$ un DFU).

Definimos ahora un tipo de ideales con un papel relevante en el estudio de las curvas.

Definición 2.16. Sea I un ideal de un anillo R. Definimos el **radical** de I como $Rad(I) = \{a \in R : a^n \in I \text{ para algún entero } n > 0\}$. Un ideal I se llama **ideal radical** si $I = Rad(I)$.

Ejemplo 2.33. a) El radical del ideal (4) de los enteros múltiplos de 4 es (2).

b) Sea un cuerpo K. En el anillo $K[X]$ de polinomios, sea el ideal $I = \left(X^2\right)$. Tenemos entonces que $X^2 \in I$ pero $X \notin I$, por lo que I no es un ideal radical.

De acuerdo con la definición, tenemos que:

Proposición 2.1. Todo ideal primo es un ideal radical (ver[18]).

Demostración. Supongamos que I es un ideal primo. Por definición, tenemos que $I \subset Rad(I)$.

Probemos ahora la inclusión contraria. Sea $a \in Rad(I)$. Por definición, existe un entero positivo n tal que $a^n \in I$.

Ahora probemos por inducción que $a \in I$. Para el caso base $n = 1$ es trivial. Supongamos, como hipótesis de inducción, que si $a^k \in I$ entonces $a \in I$, para $k > 1$. Tenemos que probar que cuando $n = k + 1$, si $a^{k+1} \in I$ entonces $a \in I$. Tenemos que el producto $a^{k+1} = a \cdot a^k$, pertenece al ideal primo I, por lo que tenemos que ó bien $a \in I$ ó $a^k \in I$. Si se da el primer caso, ya estaría probado. Si se da el segundo caso, por la hipótesis de inducción, tenemos que también $a \in I$. Por lo tanto $Rad(I) \subset I$, es decir, $I = Rad(I)$, por lo que I es un ideal radical. □

Sin embargo, un ideal radical en general no es un ideal primo. Sea un cuerpo K. En el anillo $K[X]$ de polinomios, sea el ideal $I = \left(X^2 - 1\right)$. Claramente, I es un ideal radical ya que $I = Rad(I)$. Sin embargo I no es primo, ya que tomando $(X + 1), (X - 1) \in R[X]$, podemos escribir $\left(X^2 - 1\right) = (X + 1) \cdot (X - 1)$ y $(X + 1) \notin I$, $(X - 1) \notin I$.

2.1.3. Anillo noetheriano

Finalizamos esta sección con un teorema fundamental en la teoría de curvas algebraicas.

Las condición que hace a un anillo ser noetheriano es una condición de finitud, equiparable a la dimensión finita en los espacios vectoriales. Un anillo será noetheriano si todos sus ideales son finitamente generados.

Definición 2.17. Se dice que un anillo R es **noetheriano** si satisface las tres condiciones equivalentes siguientes:

1. Cada conjunto no vacío de ideales en R tiene un elemento maximal.
2. Cada cadena ascendente de ideales en R es estacionaria, es decir, la cadena de ideales $I_1 \subseteq I_2 \subseteq \cdots$ termina, por lo que existe un entero M tal que $I_M = I_{M+1}$.
3. Cada ideal en R es de generación finita.

La demostración de la equivalencia de las tres condiciones anteriores puede encontrarse en [15].

Ejemplo 2.34. Sea un cuerpo K. Entonces los únicos ideales de K son $\{0\}$ y K, finitamente generados por 0 y 1 respectivamente, luego K es un anillo noetheriano.

Ejemplo 2.35. Sea el anillo $\mathbb{Z}[i] = \{r + si \mid r, s \in \mathbb{Z}\}$ de los números enteros de Gauss. Este un anillo noetheriano.

Ejemplo 2.36. El anillo de los números enteros $\mathbb{Z}$ es noetheriano, pues cada sucesión ascendente de ideales es estacionaria, porque si $a \in \mathbb{Z}$ con $a \neq 0$, entonces tenemos que

$$\cdots \subset (a^n) \cdots \subset \left(a^3\right) \subset \left(a^2\right) \subset (a).$$

El Teorema de la Base de Hilbert es muy importante, ya que nos proporciona un gran número de anillos noetherianos.

La demostración del siguiente teorema se puede consultar en [9] .

Teorema 2.1. (Teorema de la Base de Hilbert) Si R es un anillo noetheriano, entonces el anillo de polinomios $R[X]$ también lo es. En particular, si K es un cuerpo, entonces el anillo de polinomios en n variables $R[X_1, X_2, \cdots, X_n]$ es también noetheriano.

Corolario 2.1. Sea K un cuerpo. Cualquier ideal I del anillo noetheriano $K[X_1, X_2, \cdots, X_n]$ es finitamente generado, por lo que $I = (S)$ para un cierto conjunto finito de polinomios $S \subset K[X_1, X_2, \cdots, X_n]$.

2.2. Extensiones de cuerpos

En esta sección estamos interesados en cuerpos de funciones racionales (en dos variables) porque dan la geometría de la curva (plana). Y también estamos interesados en extensiones de cuerpos, porque da lo que se llamará **cubiertas de curvas**.

Definición 2.18. Sea un cuerpo K. Un cuerpo F se dice que es una **extensión** de K si K es un subcuerpo de F.

Si F es una extensión de K entonces F es un espacio vectorial sobre el cuerpo K y a su dimensión la llamaremos grado de la extensión de F sobre K, denotada por $[F:K]$, que puede ser finito o infinito.

Sea ahora una extensión F/K y $\alpha \in F$. Decimos que elemento α es **algebraico** sobre K si existe un polinomio $f(X) \in K[X]$ tal que $f(\alpha) = 0$. En otro caso decimos que α es **trascendente**.

Ejemplo 2.37. Todo $\alpha \in K$ es algebraico pues $f(X) = X - \alpha \in K[X]$ es no nulo y $f(\alpha) = 0$. Sin embargo, los números π y e son trascendentes sobre $\mathbb{Q}$.

2.2.1. Extensión algebraica

Definición 2.19. Diremos que extensión F/K es una **extensión algebraica** de K si todo elemento de F es algebraico sobre K.
Toda extensión finita es algebraica sobre K.

Ejemplo 2.38. Obtención de cuerpos finitos por cocientes de polinomios irreducibles. En el Anexo 1 se puede consultar el método general detallado para la construcción de cuerpos finitos.

Sean $p = 2$ y $n = 3$. Vamos a construir el cuerpo finito de 8 elementos como una extensión de grado 3 sobre $\mathbb{F}_2$. Como $p = 2$, trabajaremos en el conjunto $\mathbb{F}_2[x]$ de polinomios, con coeficientes en $\mathbb{F}_2$. Como $n = 3$, el polinomio irreducible que vamos a emplear para la operación de multiplicación tendrá grado 3. Tomaremos el polinomio $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Para definir el cuerpo, necesitamos el conjunto y sus dos operaciones.

- El conjunto, en este caso, estará formado por los polinomios de $\mathbb{Z}_2[x]$ de grado menor que 3. Es decir:

$$\mathbb{F}_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

- La operación de suma es la operación habitual de polinomios. Es fácil comprobar que esta operación es cerrada, asociativa y conmutativa, tiene elemento neutro (el polinomio nulo), y que todos los elementos tienen simétrico (en este caso, como los coeficientes están en $\mathbb{F}_2$, cada polinomio es simétrico a si mismo). Por lo tanto, $\mathbb{F}_8$ con la suma, tiene estructura de grupo conmutativo.

- Para la segunda operación no podemos utilizar el producto habitual de polinomios, porque no es una operación cerrada. De forma similar a como hacemos en la aritmética modular habitual, tomaremos el producto módulo el polinomio $f(x)$ que hemos elegido antes.

Por lo tanto, el producto de dos clases residuales será el resto de dividir entre el polinomio $f(x)$. En este caso vemos que:

$\left(x^2+1\right)\left(x^2+x\right) = x^4+x^3+x^2+x$. La división euclídea de este producto entre $f(x)$ es $x^4+x^3+x^2+x = \left(x^3+x^2+1\right)x+x^2$. El resto es x^2, por lo que $\left(x^2+1\right)\left(x^2+x\right) = x^2$.

Como el resto de los productos que podemos hacer tiene grado menor que el grado de $f(x)$, que es 3, por lo que es un polinomio en $\mathbb{F}_8$. Además, es asociativo, conmutativo y tiene elemento neutro, el polinomio 1 (ver Cuadro 1).

.	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

Cuadro 2.1: Tabla de la multiplicación en $\mathbb{F}_8$

Así pues, el conjunto $\mathbb{F}_8 \setminus \{0\}$, con la operación producto módulo $f(x)$, tiene estructura de grupo conmutativo. Es fácil comprobar que este producto es distributivo respecto de la suma, por lo que $\mathbb{F}_8$ es un cuerpo.

Tal y como hemos construido el cuerpo, hablamos del cuerpo cociente $\mathbb{F}_2[x]/(f(x))$. El hecho de que $f(x)$ sea un polinomio irreducible es determinante para la existencia de los elementos inversos. Si este polinomio no fuera irreducible, hablaríamos del anillo cociente $\mathbb{F}_2[x]/(f(x))$. Esta construcción es la misma que la del ejemplo 2.24.

Recordemos que el grupo multiplicativo de $\mathbb{F}_{q^n}$ es cíclico y tiene orden q^n-1. Las construcciones de curvas que tratamos aquí se basan en el hecho de que si $n=2$, entonces $q^2-1=(q-1)(q+1)$.

Ejemplo 2.39. Sea el cuerpo $\mathbb{F}_2 = \{0,1\}$. Para extender este cuerpo a $\mathbb{F}_4$ utilizamos el polinomio $y^2 = y+1$; de la misma forma extendemos $\mathbb{F}_4$ a $\mathbb{F}_{16}$ usando el mismo polinomio. Este ejemplo junto con el ejemplo 2.1 son ejemplos de **extensiones cuadráticas**.

Se denomina polinomio mínimo de un elemento $\alpha \in F$ al polinomio mónico p de menor grado tal que $p(\alpha) = 0$.

Definición 2.20. Sea F/K una extensión algebraica. Un elemento $\alpha \in F$ es **separable** sobre K si su correspondiente polinomio mínimo en $K[X]$ es separable, es decir, si todas las raíces de este

polinomio son distintas. Entonces F/K es una **extensión algebraica separable** si todo $\alpha \in F$ es separable sobre K.

Ejemplo 2.40. Veamos un ejemplo de un polinomio que no es separable. Sea $F = \mathbb{F}_q(x)$ el cuerpo de funciones racionales con coeficientes en el cuerpo $\mathbb{F}$ y q elementos. En $F[y]$, consideramos el polinomio $y^p - x$. Supongamos que t es una raíz de $y^p - x$ en alguna extensión de F, tenemos que $t^p - x = 0$, es decir, $t^p = x$. Como el el cuerpo tiene característica p, tenemos que $(y-t)^p = y^p - t^p = y^p - x$, por lo que t es la única raíz de $y^p - x$. De hecho, se puede probar que $y^p - x$ es irreducible sobre F, por lo que la raíz t pertenece a alguna extensión estrictamente más grande que F. Observamos que sobre un cuerpo de característica 0, todos los polinomios irreducibles son separables.

Definición 2.21. Un cuerpo K se dice que es **algebraicamente cerrado** si cada polinomio con coeficientes en K, contiene una raíz en K.

Ejemplo 2.41. El cuerpo de los números reales no es algebraicamente cerrado, ya que el polinomio $X^2 + 1$ no tiene raíces en los reales.

Definición 2.22. Sea K un cuerpo. La **clausura algebraica** de K, denotada como $\overline{K}$, es el cuerpo algebraicamente cerrado más pequeño que contiene a K. Siempre existe y es única, salvo isomorfismos. Si $p(X)$ es un polinomio en el cuerpo $K[X]$, la clausura algebraica $\overline{K}$ contiene los ceros de $p(X)$.

Ejemplo 2.42. La clausura algebraica del cuerpo de los reales $\mathbb{R}$ es $\mathbb{C}$, ya que todo polinomio con coeficientes reales tiene sus ceros en los complejos.

Ejemplo 2.43. El cuerpo $\mathbb{C}$ de los números complejos contiene las raíces de todo polinomio con coeficientes en el cuerpo $\mathbb{Q}$ de los números racionales. Sin embargo $\mathbb{C}$ no es una clausura algebraica de $\mathbb{Q}$ ya que no se cumple la condición de minimalidad.

La clausura algebraica de los números racionales,$\overline{\mathbb{Q}}$, consiste en el conjunto de los números algebraicos sobre $\mathbb{Q}$, que es un subcuerpo de $\mathbb{C}$.

La demostración del siguiente ejemplo puede encontrarse en [15].

Ejemplo 2.44. La clausura algebraica de $\mathbb{F}_q$ es $\bar{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$.

La siguiente definición ha sido extraída de [14].

Definición 2.23. Sea $f(X) \in K[X]$ un polinomio mónico de grado $d \geq 1$. El polinomio

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i)$$

se descompone en factores lineales sobre alguna extensión de cuerpos F/K . 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 la característica de K es cero, todos los polinomios irreducibles son separables. Si la $charK = p > 0$, un polinomio irreducible es separable si y sólo si $a_i \neq 0$ para algún $i \not\equiv 0 mod p$.

2.2.2. Anillo local y anillo de valuación

Los anillos locales y los anillos de valuación son la forma algebraica de definir puntos.

Definición 2.24. Sea $\mathcal{O}$ un anillo conmutativo. Se dice que $\mathcal{O}$ es un **anillo local** si tiene un único ideal maximal.

Proposición 2.2. Sea K un cuerpo y sea $\mathcal{O}$ un anillo de valuación del cuerpo F/K. Se cumplen las siguientes propiedades:

1. $\mathcal{O}$ es un anillo local, es decir, que tiene un único ideal maximal, $\mathcal{M} = \mathcal{O} \setminus \mathcal{O}^{\times}$.
2. Dado $x \in F$, $x \neq 0$, tenemos que $x \in M \iff x^{-1} \notin \mathcal{O}$.

Una forma más visual de entender los anillos locales es definirlos como anillos de valuación discreta.

Definición 2.25. Una **valuación discreta** de un cuerpo K es una aplicación $v : K \to \mathbb{Z} \cup \{\infty\}$ con las siguientes propiedades:

1. $v(x) = \infty \iff x = 0$, $x \in K$.
2. Para todo $x, y \in K$, $v(xy) = v(x) + v(y)$.
3. Para todo $x, y \in K$, $v(x+y) \geq min\{v(x), v(y)\}$.

El subconjunto de $K : \mathcal{O} = \{0\} \cup \{r \in K \mid v(r) \geq 0\}$ tiene estructura de anillo, denominado **anillo de valuación o anillo de valuación discreta** de K.

Ejemplo 2.45. Sea $K(X)$ el cuerpo de funciones racionales en la variable X sobre el cuerpo K . Si $p(X) \in K[X]$ es un polinomio irreducible dado, entonces todo elemento $\alpha \in K$ se puede escribir de manera única como

$$\alpha = p(X)^r \frac{f(X)}{g(X)}$$

con $f(X), g(X) \in K[x]$, $p(X) \nmid fg$ y $r \in \mathbb{Z}$. Definimos entonces $v(\alpha) = r$ y $v(0) = \infty$.

El anillo local asociado al polinomio mónico irreducible $p(X)$ es:

$$\mathcal{O}_{p(X)} = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in K[X], p(X) \nmid g(X) \right\}.$$

Si consideramos cualquier otro polinomio, digamos $q(X) \in K(X)$, en lugar de $p(X)$, esto da lugar a un anillo de valuación diferente $\mathcal{O}_{q(X)}$ en el cuerpo de funciones racionales $K(X)$.
Con esta definición de $\mathcal{O}_{p(X)}$, las unidades en este anillo de valuación están dadas por aquellos elementos que satisfacen, no sólo que $p(X) \nmid g(X)$, sino también que $p(X) \nmid f(X)$. Por lo tanto, los elementos que no son unidades satisfacen que $p(X) \nmid g(X)$ y $p(X) \mid f(X)$. Es decir $\mathcal{O}_{p(X)}$ es un anillo local.

Ejemplo 2.46. Valuación p-adic Si $n \in \mathbb{Z}$, la **valuación *p*-adic** es el exponente de la mayor potencia de p que divide a n, y se denota por $v_p(n)$.
Si $r = \frac{a}{b}$ es racional, su valuación p-adic se define como $v_p(r) = v_p(a) - v_p(b)$. Veamos algunos ejemplos:

- La valuación 7-adic de 7 es 1. Por lo tanto, la de 14 también es 1, así como la de $21, 28, 35, 42$ ó 56.
- Sin embargo, la valuación 7-adic de 49 es 2, la misma que la de 98.
- La valuación 7-adic de 343 es 3.
- La valuación 2-adic de un entero es 0 si y sólo si es impar, y es al menos 1 si y sólo si es par, al menos 2 si y sólo si el entero es múltiplo de 4, y así sucesivamente.
- La valuación 7-adic de $\frac{1}{2}$ ó $\frac{8}{3}$ es 0, mientras que la de $\frac{7}{3}$ ó $\frac{14}{5}$ es 1
- La valuación 7-adic de $\frac{48}{49}$ es -2.

Definimos ahora el **valor absoluto *p*-adic** de un número racional r como $|r|_p = p^{-v_p(r)}$.
Por ejemplo, $|p|_p = \frac{1}{p}$, $|1|_p = 1$ y $|2p|_p = \frac{1}{p}$ si p es impar.
Definimos ahora la **distancia *p*-adic** de dos números racionales r_1, r_2 como $|r_2 - r_1|_p$. Los racionales $\mathbb{Q}$ no son completos con respecto a esta distancia, es decir, todas las sucesiones de Cauchy no son convergentes.

La demostración del siguiente teorema puede encontrarse en [21] Teorema 1.1.6.

Teorema 2.2. Sea $\mathcal{O}$ un anillo de valuación del cuerpo F/K y sea P su único ideal maximal. Entonces:

- P es un ideal principal.
- Si $P = t\mathcal{O}$ entonces cada $z \in F$ con $z \neq 0$ tiene una representación única de la forma $z = t^n u$, para algún $n \in \mathbb{Z}$ y $u \in \mathcal{O}^\times$ (unidades del anillo de valuación de $\mathcal{O}$).
- $\mathcal{O}$ es un dominio de ideales principales. Mas precisamente, si $P = t\mathcal{O}$ y $\{0\} \neq I \subseteq \mathcal{O}$ es un ideal, entonces $P = t^n\mathcal{O}$ para algún $n \in \mathbb{N}$.

Cuando decimos $P = t\mathcal{O}$, en geometría estamos hablando de la coordenada t, la coordenada local.

Por lo tanto, **los anillos de valuación son anillos locales**, como en los ejemplo 2.45 y 2.46.

Ejemplo 2.47. Sea S el cuerpo formado por las series formales de Laurent sobre un cuerpo K. Un elemento no nulo de S tiene la forma $f = \sum_{i=r}^{\infty} a_i X^i$ donde $a_i \in K$ y $r \in \mathbb{Z}$, con $a_r \neq 0$.
Entonces podemos escribir $f = a_r X^r g$, donde g pertenece al anillo $R = K[X]$ de las series de potencias formales sobre el cuerpo K. Además, el término constante de g es 1, por lo que g, y a su vez f, pueden ser invertidos. Por lo tanto, R es un anillo de valuación de K.

La demostración de la siguiente Proposición se pude encontrar también en [13].

Proposición 2.3. Un anillo R es local si y sólo si los elementos no invertibles de R forman un ideal.

Demostración. $\Rightarrow$ Sea A un anillo local y sea M su único ideal maximal. Como M es un ideal propio, entonces no tiene elementos invertibles. Tenemos que ver entonces que todos los elementos no invertibles pertenecen a M, lo que es equivalente a decir que todos los elementos que no pertenecen a M son invertibles.

Sea un elemento $a \notin M$. Entonces, $a\mathcal{O} \subsetneq M$, y como todo ideal propio está contenido en un ideal maximal, tenemos que $a\mathcal{O} = \mathcal{O}$, por lo que a es invertible.
$\Leftarrow$ Sea ahora el ideal S formado por todos los elementos de $\mathcal{O}$ que no son invertibles. Entonces, para todo ideal propio I de $\mathcal{O}$, $I \subset S$, ya que en I sólo hay elementos no invertibles. Entonces S es un ideal maximal y es único. □

CAPÍTULO 3

CURVAS

3.1. Variedades afines sobre un cuerpo K

Al conjunto solución de un sistema de ecuaciones algebraicas lo llamamos variedad afín. En esta sección estudiamos sus propiedades básicas y su relación con los ideales.
La mayoría de conceptos relativos a curvas descritos en esta sección en esta sección pueden consultarse en [22] y [5] .

3.1.1. Variedades afines

Definición 3.1. Sea K un cuerpo. Un **espacio afín** sobre K es una terna $(E,V,+)$ formada por un conjunto no vacío E, un K-espacio vectorial V y una operación $+$,

$$E \times V \xrightarrow{+} E,$$

$$(P,v) \longmapsto P+v$$

tales que para cualquiera $P,Q \in E$ y $u,v \in V$ se verifican las siguientes condiciones:

1. $P+0=P$.
2. $(P+u)+v=P+(u+v)$.
3. Existe un único $w \in V$ tal que $P+w=Q$.

Ejemplo 3.1. El **plano afín lineal** $K\mathbb{A}^2$ es un par $(\mathscr{P},\mathscr{L})$ donde
$\mathscr{P}=\{(X,Y) \mid X,Y \in K\}$
$\mathscr{L}=\{l=aX+bY+c \mid a,b,c \in K,(a,b) \neq (0,0)\}$
y un punto $P=(X,Y)$ pertenece a la linea $l=aX+bY+c$ si $ax+by+c=0$.

Sabemos que el espacio n-dimensional afín $\mathbb{A}^n = K\mathbb{A}^n$ es el conjunto de todas las n-tuplas de elementos del cuerpo K. Un elemento $P = (a_1, \cdots, a_n) \in \mathbb{A}^n$ es un punto, y a $a_1, \cdots, a_n$ son las coordenadas del punto P.

Definición 3.2. Sea $K[X_1, \cdots, X_n]$ el anillo de polinomios de n variables sobre el cuerpo K. Entonces $V \subseteq K\mathbb{A}^n$ es un **conjunto algebraico** si existe un conjunto $M \in K[X_1, \cdots, X_n]$ tal que

$$V(M) = \{P \in K\mathbb{A}^n \mid f(P) = 0 \text{ para todo } f \in M\}.$$

Ejemplo 3.2. El círculo $C = \{(cost, sent) \in \mathbb{R}^2 \mid t \in [0, 2\pi]\}$ es un conjunto algebraico ya que C es el conjunto de soluciones del polinomio $X^2 + Y^2 - 1 = 0$.

Definición 3.3. Sea un cuerpo K y un conjunto algebraico V. El conjunto de polinomios que se anulan en V forman un ideal y se denomina ideal de V

$$I(V) = \{f \in K[X_1, \cdots, X_n] \mid f(P) = 0 \text{ para todo } P \in V\}.$$

Como $I(V)$ es un ideal de $K[X_1, \cdots, X_n]$ generado por un conjunto finito de polinomios $f_1, \cdots, f_n \in K[X_1, \cdots, X_n]$, tenemos que

$$V(M) = \{P \in K\mathbb{A}^n \mid f_1(P) = \cdots = f_n(P) = 0 \text{ para todo } f_i \in M, i = 1, \cdots, n\}.$$

Es decir, tenemos una "función" V que envía ideales de $K[X_1, \cdots, X_n]$ a conjuntos algebraicos, y una "función" I que envía subconjuntos de $K\mathbb{A}^n$ a ideales de $K[X_1, \cdots, X_n]$.

Definición 3.4. Un conjunto algebraico M se dice que es **irreducible** si no es unión de dos conjuntos algebraicos más pequeños. En caso contrario se dice que M es **reducible**.

Observación: La definición anterior es equivalente a decir que M es irreducible si y sólo si el correspondiente ideal $I(M)$ es un ideal primo.

En los siguientes tres ejemplos consideramos el cuerpo de los números reales.

Ejemplo 3.3. La circunferencia dada por la ecuación $X^2 + Y^2 - 1 = 0$ es irreducible.

Ejemplo 3.4. La parábola $Y = X^2$ es reducible, al ser el producto de dos rectas.

Ejemplo 3.5. La curva elíptica dada por la ecuación $Y^2 - X^3 + aX + b = 0$, con $4a^3 + 27b^2 \neq 0$, es irreducible.

Definición 3.5. Sea K un cuerpo. Una **variedad afín (variedad)** es un conjunto algebraico irreducible $V \in K\mathbb{A}^n$.

Ejemplo 3.6. $K\mathbb{A}^n$ es una variedad, ya que $I(K\mathbb{A}^n) = (0)$ es un ideal primo. Si $f \in K[X_1, \cdots, X_n]$ es un polinomio irreducible, entonces $V((f))$ es una variedad , ya que $K[X_1, \cdots, X_n]$ es un dominio de factorización única denominada superficie si $n = 3$, o hipersuperficie si $n > 3$.

Como un caso particular, si $f \in K[X,Y]$ es un polinomio irreducible de grado d, entonces $V((f))$ es una curva afín plana (que veremos en la siguiente sección) de grado d, definida por la ecuación $f(X,Y) = 0$.

La demostración del siguiente Teorema la podemos encontrar en [5], sección 1.7.

Teorema 3.1. Sea un cuerpo K y sea V un conjunto algebraico en $K\mathbb{A}^n$. Entonces existen variedades únicas $V_1, \cdots, V_m$ tales que $V = V_1 \cup \cdots \cup V_m$ y $V_i \not\subset V_j$ para $i \neq j$.

Es decir, dado un ideal J en el anillo de polinomios $K[X_1, \cdots, X_n]$, la variedad $V(J)$ definida por este ideal consiste en todas las n-tuplas $(a_1, \cdots, a_n) \in K\mathbb{A}^n$ tal que $f(x) = 0$ para todo f en J.

En [4] podemos encontrar ejemplos parecidos al siguiente, usando las llamadas Bases de Groebner:

Ejemplo 3.7. Sea el conjunto algebraico $V\left(X^2 - YZ, XZ - X\right)$. Su descomposición en componentes irreducibles viene dada por:

$$V\left(X^2 - YZ, XZ - X\right) = V\left(X^2 - YZ\right) \cap V(X(Z-1)) =$$

$$= V\left(X^2 - YZ\right) \cap (V(X) \cup V(Z-1)) =$$

$$= V\left(X, X^2 - YZ\right) \cup V\left(Z-1, X^2 - YZ\right) =$$

$$= \left[V\left(X^2 - YZ\right) \cap V(X)\right] \cup \left[V\left(X^2 - YZ\right) \cup V(Z-1)\right] =$$

$$= V(X,Y) \cup V(X,Z) \cup \left(Z-1, X^2 - YZ\right).$$

3.1.2. Nullstellensatz

La siguiente proposición es una versión del teorema Nullstellensatz que veremos más adelante.

Proposición 3.1. Sea un cuerpo K. Para todo conjunto algebraico $M \subset K\mathbb{A}^n$, $I(M)$ es un ideal radical. De manera equivalente, si $J \subset K[X_1, \cdots, X_n]$ no es un ideal radical entonces no existe ningún subconjunto $M \subset K\mathbb{A}^n$ tal que $J = I(M)$.

Lo que dice la proposición anterior es que es posible que dado un ideal J de $K[X_1, \cdots, X_n]$ y un conjunto algebraico $M \subset K\mathbb{A}^n$, no siempre ocurrirá que $J = I(M)$. Lo probamos con el siguiente ejemplo.

Ejemplo 3.8. Consideremos el ideal $\left(X^2\right) \subset \mathbb{C}[X]$. Supongamos que existe un conjunto $V \subset \mathbb{C}\mathbb{A}^1$ no vacío tal que $\left(X^2\right) = I(V) := \{f \in \mathbb{C}[X] \mid f(P) = 0 \text{ para todo } P \in V\}$. Sea $P \in X$. Como $X^2 \in I(X)$ tenemos que $X^2(0) = 0$, por lo que $V = \{0\}$. Pero $I(\{0\}) = (X)$. Por lo tanto la conclusión es que $\left(X^2\right)$ no es el ideal de ningún conjunto de puntos.

Del ejemplo anterior, tenemos la siguiente propiedad: sea $C \subset K\mathbb{A}^n$, $I(C) = \{f \in K[X_1, \cdots, X_n] \mid f(P) = 0 \text{ para todo } P \in C\}$. Supongamos que $f^n(P) \in I(C)$ para algún $n > 0$ y sea $P \in C$. Entonces $f^n(P) = 0$, y como K no tiene divisores de cero, es $f(P) = 0$, por lo que $f \in I(C)$.

Tenemos entonces que si un ideal J de $K[X_1, \cdots X_n]$ no es radical no puede ser el ideal de un conjunto de puntos de $K\mathbb{A}^n$. Pero, ¿todo ideal radical es el ideal de un conjunto de puntos?. Esto es cierto para cuerpos algebraicamente cerrados, es decir, si J es radical, entonces J es el ideal de puntos de la variedad $V(J)$.

El Nullstellensatz es un teorema muy importante, porque muestra una relación entre la geometría y el álgebra: las soluciones de un sistema de ecuaciones polinomiales son objetos geométricos y los ideales y radicales son objetos algebraicos.

La prueba del siguiente Teorema la podemos encontrar en [5], sección 1.7:

Teorema 3.2. (Nullstellensatz) Sea J un ideal en $K[X_1, \cdots, X_n]$, con K un cuerpo algebraicamente cerrado. Entonces $I(V(J)) = Rad(J)$.

Lo que nos dice el teorema es que si q es un polinomio de $K[X_1, \cdots X_n]$ que se anula en la variedad $V(J)$, es decir, $q(P) = 0$ para todo $P \in V(J)$, entonces existe un número natural n tal que $q^r \in J$.

Como para cualquier conjunto algebraico M, $V(I(M)) = M$, y para todo ideal radical J tenemos que $I(V(J)) = J$, el siguiente colorario es cierto:

Corolario 3.1. Las correspondencias V e I inducen las siguientes biyecciones (consultar la definición de la Topología de Zariski en [17]):

$$\begin{array}{ccc} \{\text{ideales J} \subset K[X_1, \cdots, X_n]\} & \longleftrightarrow & \{\text{subconjuntos Zariski cerrados M} \subset K\mathbb{A}^n\} \\ \cup & & \cup \\ \{\text{ideales radicales}\} & \longleftrightarrow & \{\text{subconjuntos algebraicos}\} \\ \cup & & \cup \\ \{\text{ideales primos}\} & \longleftrightarrow & \{\text{subconjuntos algebraicos irreducibles}\} \end{array}$$

Ejemplo 3.9. Sea K un cuerpo. Un ideal maximal J del anillo $K[X_1, \cdots, X_n]$ corresponde a un subconjunto cerrado minimal de $K\mathbb{A}^n$, que debe ser un punto (pues los puntos no contienen ningún subconjunto cerrado propio), digamos $P = (a_1, \cdots, a_n)$. Esto muestra que todo ideal maximal de A es de la forma $(X_1 - a_1, \cdots, X_n - a_n)$ para algunos $a_1, \cdots, a_n \in K$.

En otras palabras, el Nullstenllensatz identifica el conjunto de ideales maximales del anillo $K[X_1,\cdots,X_n]$ con los puntos del espacio afín $K\mathbb{A}^n$.

Observación**:** Si el cuerpo con el que estamos trabajando no es algebraicamente cerrado, puede suceder que los resultados anteriores no se cumplan.

Ejemplo 3.10. Sabemos que $\mathbb{R}[X]/\left(X^2+1\right)\cong\mathbb{C}$, pero el ideal maximal $\left(X^2+1\right)$ no es de la forma que hemos establecido en el ejemplo anterior. Más aún, todo ideal maximal en el anillo $\mathbb{R}[X]$ se puede expresar como $\left(X^2+1\right)$, $a\in\mathbb{R}$ o como $\left(X^2+aX+b\right)$, donde $a,b\in\mathbb{R}$ son tales que $a^2-4b<0$.

3.1.3. Anillo de coordenadas afines

Las demostraciones y algunos ejemplos de esta sección las podemos encontrar en [12].

Definición 3.6. Sea K un cuerpo y V una variedad. El anillo de coordenadas afines de V es el anillo de clases residuales $\Gamma(V)=K[X_1,\cdots,X_n]/I(V)$.

Observación: tenemos que V es una variedad afín en un cuerpo algebraicamente cerrado, por lo que $I(V)$ es primo. Entonces tenemos que $\Gamma(V)$ es un dominio integral.

Ejemplo 3.11. Si $V=K\mathbb{A}^1$, entonces tenemos entonces la recta afín. Dado un punto $P\in K\mathbb{A}^1$, el anillo local asociado asociado a P es $\mathcal{O}_P$ (ver ejemplo 2.45). Su cuerpo de funciones es el cuerpo de funciones racionales.

El cuerpo de funciones racionales de V, que denotamos por $K(V)$ contiene a K como subcuerpo, es el cuerpo de fraciones del dominio integral $\Gamma(V)$ (ver sección 2.1.1). Sea $P\in V$, y consideramos el anillo local

$$\mathcal{O}_P=\left\{f\in K(V)\mid f=\tfrac{g}{h},g,h\in\Gamma(V),h(P)\neq 0\right\}.$$

Entonces los conceptos de $\mathcal{O}_P$ (anillo local) y M_P (ideal maximal) **de una variedad afín extienden los conceptos de anillo de valuación (ver ejemplo 2.45) y plaza (que definiremos posteriormente para cuerpos de funciones algebraicas)**, respectivamente.

Ejemplo 3.12. Anillo coordenado afín de la parábola. Sea V el conjunto algebraico de los puntos con ecuación $Y=X^2$, es decir, V es el conjunto de ceros del polinomio $f(X,Y)=Y-X^2$. El anillo coordenado $\Gamma(V)=K[X,Y]/I(V)$ de V es isomorfo a un anillo de polinomios de una variable sobre el cuerpo K, donde $K[X,Y]$ es el anillo de polinomios sobre el cuerpo K en las indeterminadas X e Y.

Consideramos ahora el homomorfismo

$$\varphi:K[X,Y]/I(V)\to K(t).$$

Parametrizando la curva la parábola usando el elemento transcendental t, tenemos que $f(t)=\left(t,t^2\right)$, por lo que la coordenada local viene dada por

$t = \frac{y}{x}$. En el caso de que $x = 0$, tenemos que $t = 0$.

Ejemplo 3.13. Si consideramos $V(X^3 - Y^2)$. En el caso en que K es un cuerpo de característica cero se tiene $I(V(X^3-Y^2)) = (X^3-Y^2)$, y por tanto $\Gamma[V(X^3-Y^2)] = K[X,Y]/(X^3-Y^2)$. Sin embargo si $K = \mathbb{F}_2$, entonces $\Gamma[V(X^3-Y^2)] = \mathbb{F}_2[X,Y]/(X+Y, Y^2+Y) \cong \mathbb{F}_2[Y]/(Y^2+Y) \cong \mathbb{F}_2 \times \mathbb{F}_2$.

3.1.4. Curvas afines planas

Definición 3.7. Sea K un cuerpo algebraicamente cerrado, $f \in K[X,Y]$ el anillo de polinomios en el cuerpo K y $K\mathbb{A}^2$ el plano afín.
Definimos la curva afín plana como el conjunto $\mathscr{F} = v_a(f) = \{(X,Y) \in K\mathbb{A}^2 \mid f(X,Y) = 0\}$.
Tenemos además que:

- Una componente de la curva afín $\mathscr{F} = v_a(f)$ es una curva afín $\mathscr{G} = v_a(q)$ de tal forma que q divide a f.
- Una curva afín $\mathscr{F} = v_a(f)$ es irreducible cuando no tiene componentes propios, es decir, cuando f es irreducible.
- Si $f = f_1^{n_1} f_2^{n_2} \cdots f_n^{n_n}$ con cada f_i irreducible, entonces $\mathscr{F} = v_a(f)$ tiene componentes $\mathscr{F}_i = v_a(f_i)$ con multiplicidad n_i para $i = 1, \cdots, n$.

Ejemplo 3.14. Si consideramos el polinomio $f(X,Y) = X^3Y - X^2 + XY^3 - XY - Y^2 + 1$, vemos fácilmente que es no es irreducible, ya que es la unión de dos conjuntos algebraicos, una hipérbola y un círculo en la misma ecuación, es decir, $f(X,Y) = (XY-1)\left(X^2+Y^2-1\right)$.

Así, el polinomio $f(X,Y) = (XY-1)\left(X^2+Y^2-1\right)$ tiene dos componentes, que corresponden los dos factores irreducibles de f (Figura 3.1).

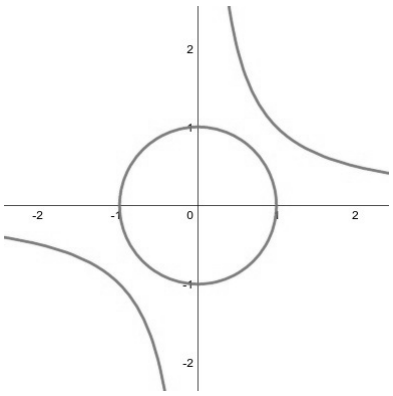

Figura 3.1: Componentes irreducibles

Definición 3.8. Sea una curva afín plana $\mathscr{F} = v(f)$ y P un punto de ella. Clasificamos el punto P de la siguiente forma:

- P se denomina un punto simple de $\mathscr{F}$ si $\frac{\partial f}{\partial X}|_P \neq 0$ y $\frac{\partial f}{\partial Y}|_P \neq 0$.

- P se denomina múltiple o singular si no es un punto simple.

Una curva que solo contenga puntos simples se la denomina curva no-singular.
Llamamos recta tangente de $\mathscr{F}$ en un punto $P=(x,y)$ a la recta $l_p = \frac{\partial f}{\partial X}|_P (X-x) + \frac{\partial f}{\partial Y}|_P (Y-y)$.

Ejemplo 3.15. Sea la curva de la Figura 3.2, $f(X,Y) = Y^2 - X^3 + X$:

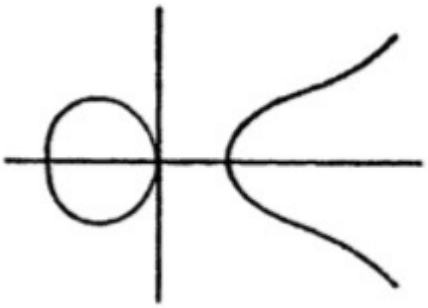

Figura 3.2: Curva no-singular

Un simple cálculo prueba que la Figura 3.2 es una curva no-singular, y que el término lineal de la ecuación de la curva es precisamente la recta tangente a la curva en $P=(0,0)$. Sin embargo, sea la curva mostrada en la Figura 3.3, $f(X,Y) = \left(X^2+Y^2\right)^3 + 3X^2Y - Y^3$.

En este caso, tenemos que en el punto $P=(0,0)$, $\frac{\partial f}{\partial X}|_P = 0$ y $\frac{\partial f}{\partial Y}|_P = 0$, por lo que P es único punto singular de la curva mostrada. El término de grado más bajo es
$3X^2Y - Y^3 = Y\left(\sqrt{3}X - Y\right)\left(\sqrt{3}X + Y\right)$, la cual determina unas rectas que pueden ser llamadas tangentes en el punto $(0,0)$.

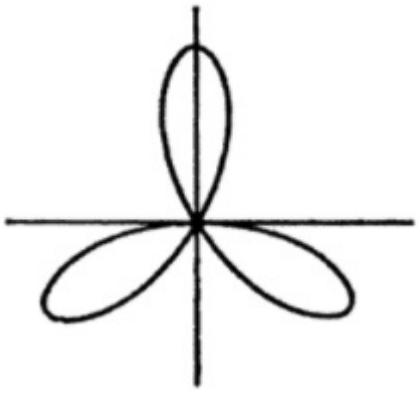

Figura 3.3: Punto singular

3.2. Variedades proyectivas sobre un cuerpo K

Empezamos definiendo la relación de equivalencia " $\sim$ " en $\mathbb{A}^{n+1} \setminus \{0\}$ diciendo que $(X_0, X_2, \cdots, X_n) \sim \left(X_0^{'}, X_2^{'}, \cdots, X_n^{'}\right)$ si existe un $\lambda \in K$, $\lambda \neq 0$,
tal que $(X_0, X_2, \cdots, X_n) = \lambda \left(X_0^{'}, X_2^{'}, \cdots, X_n^{'}\right)$, esto es, dos puntos pertenecen a la misma clase de equivalencia si están en la misma línea que pasa por el origen.

Definición 3.9. El espacio proyectivo de n-dimensiones sobre el cuerpo K es
$K\mathbb{P}^n = (K^{n+1} \setminus \{0\}/\sim)$, el conjunto de clases de equivalencia con respecto a $\sim$. Denotamos los elementos de $K\mathbb{P}^n$ por $(X_0 : X_2 : \cdots : X_n)$ (coordenadas homogéneas).
Por lo tanto, los puntos del espacio proyectivo $K\mathbb{P}^n$ son las rectas vectoriales del espacio vectorial K de dimensión $n+1$.

Definición 3.10. El **plano proyectivo** real $\mathbb{RP}^2$ surge al añadir al plano $\mathbb{R}^2$ un punto por cada familia de rectas paralelas. Estos puntos se llaman puntos en el infinito. Por lo tanto tenemos:

- Los puntos con la tercera coordenada no nula, llamados puntos finitos. Cada punto finito tiene una representación única en la forma $(a : b : 1)$, y por lo tanto el conjunto de punto finitos puede ser identificado con el plano $z = 1$ en el espacio afín $\mathbb{R}^3$ (ver Figura 3.4).
- Los puntos con la tercera coordenada igual a 0 son llamados puntos en el infinito. Tendrán la forma $(a : 1 : 0)$ o $(1 : 0 : 0)$.

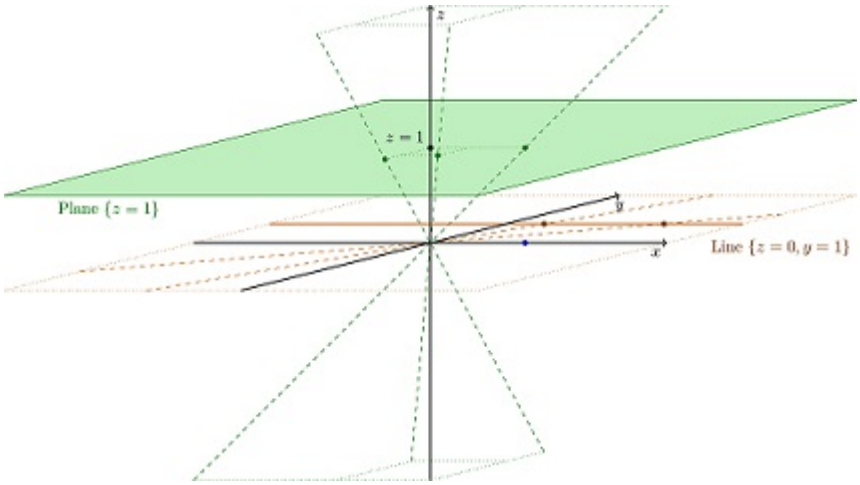

Figura 3.4: Plano proyectivo

Imágen de libre disposición: https://i.stack.imgur.com/Rfkzx.png

Ejemplo 3.16. Sea $f^*(Z, Y, Z) = X^2 - Y^2 - Z^2$. Veamos cómo se describe el conjunto de puntos en $\mathbb{RP}^2$ que satisfacen $X^2 - Y^2 - Z^2 = 0$.

Los puntos finitos corresponden a $Z = 1$, es decir cuando $X^2 - Y^2 = 1$, una hipérbola afín con asíntotas de ecuación $X = \pm Y$, y los puntos en el infinito corresponden a $Z = 0$, es decir los puntos de la forma $(1:1:0)$ y $(-1:1:0)$.

Ejemplo 3.17. La línea proyectiva compleja y la Esfera de Riemann

La recta proyectiva es el conjunto de $\mathbb{C}^2$ de los pares (α, β) de números complejos, no ambos nulos, junto con la relación de equivalencia $(\alpha, \beta) = (\lambda\alpha : \lambda\beta)$ con λ un número complejo no nulo. El plano complejo $\mathbb{C}$, con coordenada ζ puede ser aplicado en la línea proyectiva por la aplicación $\zeta \mapsto (\zeta : 1)$. Otra copia del plano complejo $\mathbb{C}$ con coordenada ξ se puede aplicar en la línea proyectiva como $\xi \mapsto (1 : \xi)$.

Estas dos cartas complejas cubren la línea proyectiva. Para valores no nulos ξ y ζ la aplicación

$$(1:\xi) = \left(\tfrac{1}{\xi} : 1\right) \to (\zeta : 1) = \left(1 : \tfrac{1}{\zeta}\right)$$

implica que las funciones de transición de coordenadas son $\zeta = \frac{1}{\xi}$ y $\xi = \frac{1}{\zeta}$. Por lo tanto,

la recta proyectiva compleja $\mathbb{CP}^1$ y la Esfera de Riemann $C \cup \{\infty\} = \hat{C}$ son equivalentes.

3.2.1. Variedades proyectivas

Podemos encontrar las ideas y algunos ejemplo de esta sección en [4] y [22] .

Definición 3.11. Sea $K[X_0, \cdots, X_n]$ el anillo de polinomios de $n+1$ variables sobre el cuerpo K. Entonces $V \subseteq K\mathbb{P}^n$ es un **conjunto proyectivo algebraico** si existe un conjunto de polinomios homogéneos $M \subset K[X_0, \cdots, X_n]$ tal que

$$V = \{P \in K\mathbb{P}^n \mid f(P) = 0 \text{ para todo } f \in M\}.$$

Definición 3.12. Una variedad proyectiva es un conjunto proyectivo algebraico irreducible $V \in K\mathbb{P}^n$.

Definición 3.13. Sea una variedad V. Se denomina ideal homogéneo de V, $I(W)$, al conjunto de polinomios homogéneos que se anulan en V, es decir,

$$I(V) = \{f \in K[X_0, \cdots, X_n] \mid f(P) = 0 \text{ para todo } P \in V\}.$$

3.2.2. Nullstellensatz para curvas proyectivas

Al igual que en el caso de curvas afines, veamos el Teorema Nullstellensatz equivalente para curvas proyectivas, cuya demostración podemos consultar en [5].

Teorema 3.3. Nullstellensatz Sea J un ideal homogéneo en $K[X_0, \cdots, X_n]$. Si $f \in S^h$, con $degf > 0$, es tal que $f(P) = 0$ para todo $P \in V(J)$ en $K\mathbb{P}^n$, entonces existe $q > 0$ tal que $f^q \in I$.

Demostración. Consideramos a $V(J)$ como una variedad en $K\mathbb{A}^{n+1}$ y sea H el conjunto de todos los elementos homogéneos de J. Tomamos $P=(a_0,\cdots,a_n)\in V(J)$. Como para todo $g\in J$ tenemos que $g(P)=0$, en particular para todo $g\in H$, $g(P)=0$, esto significa que $(a_0:\cdots:a_n)\in V(J)\subseteq K\mathbb{P}$, por lo que $f(a_0:\cdots:a_n)=f(a_0,\cdots,a_n)$, por lo que f se anula en todos los puntos de $K\mathbb{A}^{n+1}\subset K\mathbb{A}^n$. Ahora aplicamos el Nullstellensatz en su versión afín y vemos que existe $q>0$ tal que $f^q\in J$. □

3.2.3. Curvas proyectivas planas

Podemos encontrar las definiciones y más ejemplos de la siguiente sección en [22] .

Polinomio homogéneo

Definición 3.14. Sea un polinomio $f\in K[X,Y]$ de grado d. El polinomio homogéneo $f^*\in f[X_0,X_1,X_2]$ asociado al polinomio f viene dado por $X=\frac{X_1}{X_0},Y=\frac{X_2}{X_0},f^*(X_0:X_1:X_2)=X_0^d f\left(\frac{X_1}{X_0},\frac{X_2}{X_0}\right)$.

Dado el polinomio $f\in K[X,Y]$, la curva proyectiva plana de ecuación afín $f(X,Y)=0$, o ecuación homogénea $f^*(X_0,X_1,X_2)=0$ es

$\mathscr{F}=V(f^*)=\{(X_0:X_1:X_2)\in K\mathbb{P}_2(K)\mid f^*(X_0,X_1,X_2)=0\}$.

El grado de la curva es el grado del polinomio homogéneo.

Ejemplo 3.18. Sea la curva definida por el polinomio el polinomio $f(X,Y)=Y^2-X^3-aX^2+bX+c$. Entonces, el polinomio homogéneo asociado a f es $f^*(X_0,X_1,X_2)=X_0^3\left(\frac{X_2^2}{X_0^2}-\frac{X_1^3}{X_0^3}-a\frac{X_1^2}{X_0^2}+b\frac{X_1}{X_0}+c\right)=X_2^2X_0-X_1^3-aX_1^2X_0+bX_1X_0^2+cX_0^3$. El grado de la curva definida por el polinomio homogéneo es 3.

En este caso, los puntos finitos, cuando $X_0=1$, corresponden a la curva elíptica afín $X_2^2=X_1^3-aX_1^2+bX_1+c$, y los puntos en el infinito, cuando $X_0=0$ son $X_1^3=0\longleftrightarrow X_1=0$, un único punto, el punto $(0:0:1)$.

Es decir, lo que hacemos es rellenar los monomios de grado inferior al máximo con la potencia correspondiente de X_0 para que todos los monomios queden del grado del polinomio.

Ejemplo 3.19. Sea la curva elíptica definida por el polinomio homogéneo $X_1^2X_2=X_0^3+aX_0X_2^2+bX_2^3$. Representamos esta curva en el espacio proyectivo.

Haciendo $X_2=1$, tenemos que $X_1^2=X_0^3+aX_0+b$, por lo que la representación de la curva elíptica será la misma que en plano afín, pero "proyectada" en el plano $X_2=1$.

Si $X_2=0$, el único punto que satisface la ecuación es el $(0:1:0)$. Justamente este es el punto que no puede ser representado en el plano afín, el punto en el infinito P_∞ de la recta proyectiva $X_2=0$ (Figura 3.5).

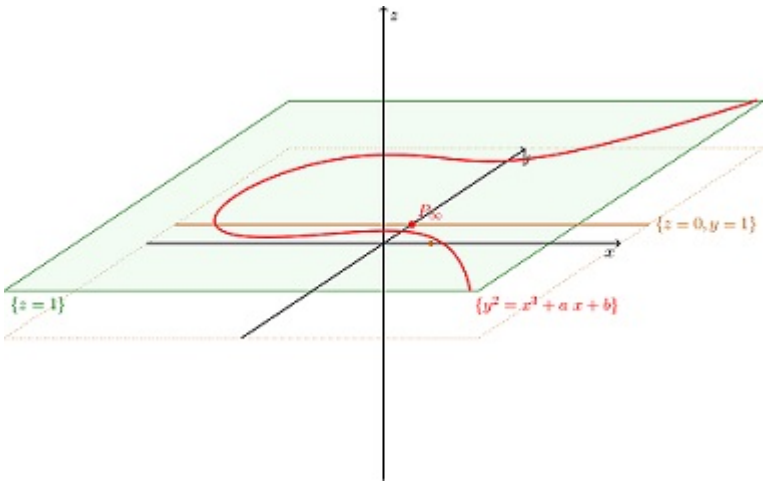

Figura 3.5: Curva Elíptica

Imágen de libre disposición: https://i.stack.imgur.com/PAqsA.png

Definición 3.15. Si f^* un polinomio homogéneo, un punto $P=(X_0:X_1:X_2)$ de $\mathscr{F}$ es singular si $\frac{\partial f^*}{\partial X_0}=\frac{\partial f^*}{\partial X_1}=\frac{\partial f^*}{\partial X_2}=0$. En otro caso, el punto P es un punto simple y la tangente en P es $\frac{\partial f^*}{\partial X_0}\,|_P\, X_0+\frac{\partial f^*}{\partial X_1}\,|_P\, X_1+\frac{\partial f^*}{\partial X_2}\,|_P\, X_2$.

Multiplicidad

Las siguientes definiciones y conceptos pueden encontrarse en [23] y [11] .

Consideramos en esta sección que trabajamos con cuerpos cerrados.

Sean dos curvas $C_1=V(f_1)$ y $C_2=V(f_2)$, de grado n y m respectivamente, pertenecientes a $K\mathbb{P}_2$. Entonces, si el cuerpo K es cerrado, tenemos que las curvas siempre se van a cortar en, al menos, un punto.

Si las dos curvas no tienen componentes en común, se cortarán en, como máximo, nm puntos.

Supongamos ahora que cada uno de esos puntos de intersección no son puntos singulares de C_1 y C_2, y que las líneas tangentes en esos puntos en son distintas en las dos curvas. Denotamos la **multiplicidad de la intersección en el punto** p de las dos curvas como: $mul_p(C_1,C_2)$.

Uno de los resultados más importantes de la teoría de curvas algebraicas proyectivas es el **Teorema de Bezout**, que proporciona el número de puntos de intersección de dos curvas, en función de los grados de las mismas.

La demostración del Teorema de Bezout puede ser consultada en [11].

Teorema 3.4. Teorema de Bezout: Sean dos curvas proyectivas C_1 y C_2, de grado n y m respectivamente, las cuales no tienen componentes en común. Entonces, tienen nm puntos de intersección, contando sus multiplicidades, es decir:

$$\sum_{p\in C_1\cap C_2} mul_p(C_1,C_2)=nm.$$

Ahora, para encontrar los puntos de intersección es muy útil el concepto de **resultante**, el cuál puede ser consultado en [23].

Ilustramos estos conceptos con el siguiente ejemplo:

Ejemplo 3.20. Consideramos las siguientes variedades proyectivas: el círculo unidad $C_1 = V\left(X^2+Y^2-Z^2=0\right)$ y la cúbica $C_2 = V\left(Y^2Z-X^3+X^2Z+XZ^2-Z^3=0\right)$ (ver Figura 3.6).

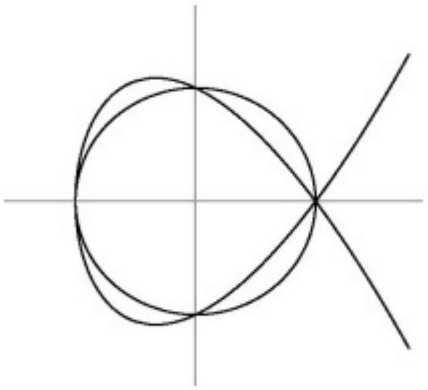

Figura 3.6: Variedades proyectivas

Como el punto $(0:0:1)$ no pertenece a ninguna de las dos curvas, el resultante con respecto a Z es:

$$P(X,Y,) = \left(X^2+Y^2\right)Z^0-(0)Z^1-(1)Z^2$$

$$Q(X,Y) = \left(X^3\right)Z^0+\left(-X^2-Y^2\right)Z^1-(X)z^2+(1)Z^3$$

$$\begin{vmatrix} X^2+Y^2 & 0 & -1 & 0 & 0 \\ 0 & X^2+Y^2 & 0 & -1 & 0 \\ 0 & 0 & X^2+Y^2 & 0 & -1 \\ X^3 & -X^2-Y^2 & -X & 1 & 0 \\ 0 & X^3 & -X^2-Y^2 & -X & 1 \end{vmatrix} = -X^2Y^4.$$

Por lo tanto, o tenemos que $X=0$ ó $Y=0$.

- Si $X=0$, tenemos que $Y^2-Z^2=0$ y $Z(Y^2-Z^2)=0$, lo que nos da los puntos $(0:1:1)$ y $(0:-1:1)$.
- Si $Y=0$, tenemos que $X^2-Z^2=0$ y $X^3-X^2Z-XZ^2+Z^3=(X-Z)(X^2-Z^2)=0$, lo que nos da los puntos$(1:0:1)$ y $(-1:0:1)$.

Por lo tanto, tenemos cuatro puntos de intersección en el plano afín, $(0,1)$, $(0,-1)$, $(1,0)$ y $(-1,0)$.

Observamos que el factor $X^2 = 0$ corresponde a los dos puntos de intersección$(0,1)$ y $(0,-1)$, mientras que el factor $Y^4 = 0$ corresponde a los dos puntos $(-1,0)$ y $(1,0)$, ambos con multiplicidad 2. Vemos que no hay intersección en el infinito.

3.2.4. Transformaciones proyectivas

Los siguientes conceptos sobre transformaciones proyectivas pueden ser consultados en [3].

Sean V, W espacios vectoriales de la misma dimensión $n+1, n \in \mathbb{Z}$ sea $T : V \to W$ una aplicación lineal. Si el núcleo de T es igual a $\{0\}$, será inyectiva (y suprayectiva al tener la misma dimensión) y la imagen de un subespacio de V dimensión k es un subespacio de W también de dimensión k. En este caso T induce una aplicación $\tau : V\mathbb{P}^n \to W\mathbb{P}^n$definida por $\tau([u]) = [T(u)]$.

Definición 3.16. Una transformación proyectiva de $V\mathbb{P}^n$ a $W\mathbb{P}^n$ es una aplicación inducida por una transformación $T : V \to W$ lineal e invertible. Si $\lambda \neq 0$ entonces T y λT inducen la misma transformación proyectiva.

Las propiedades de las curvas proyectivas tales como el grado, la multiplicidad de los puntos singulares o la multiplicidad de contacto de una tangente , son covariantes, es decir, son invariantes bajo transformaciones proyectivas.

Sean $V \subseteq K\mathbb{P}^m$ y $W \subseteq K\mathbb{P}^n$ variedades proyectivas y sean $f_0, \cdots, f_n \in K[X_0, \cdots, X_m]$ polinomios del mismo grado los cuáles cumplen las siguientes propiedades:

1. No todos los f_i pertenecen a $I(V)$.
2. Para todo $H \in I(W)$ tenemos que $H(f_0, \cdots, f_n) \in I(W)$.

Sea $Q \in V$ y supongamos que $f_i(Q) \neq 0$ para como mínimo un $i \in \{0, \cdots, n\}$ (que por 1. sabemos que existe). Entonces, tenemos que el punto $(f_0(Q) : \cdots : f_n(Q)) \in K\mathbb{P}^n$ está en W. Sea otra tupla de polinomios homogéneos $g_0, \cdots, g_n \in K[X_0, \cdots, X_m]$ que satisfacen las dos condiciones anteriores.

Definición 3.17. Decimos que las tuplas de polinomios $(f_0, \cdots, f_n), (g_0, \cdots, g_n)$ son **equivalentes** si $f_i g_j \equiv f_i g_j \bmod I(V)$ para $0 \leq i, j \leq n$. La clase de equivalencia de $(f_0, \cdots, f_n)$ se denota por

$$\phi = (F_0 : \cdots : F_n).$$

A la aplicación ϕ se la denomina **aplicación racional** de V a W.

Definición 3.18. Una aplicación racional $\phi = (f_0 : \cdots : f_n)$ se denomina **aplicación regular** en el punto $a \in V$ si existen polinomios homogéneos $g_0, \cdots, g_n \in K[X_0, \cdots, X_m]$ tales que $\phi = (g_0 : \cdots : g_n)$ y $g_i(a) \neq 0$ para al menos un i.

Definimos entonces $\phi(a) = (g_0(a) : \cdots : g_n(a)) \in W$, aplicación que está bien definida por el punto 1 de las dos condiciones anteriores.

Ejemplo 3.21. Sea la aplicación racional $f : \mathbb{P}^2 \to \mathbb{P}^2$ dada por $f = \left(x-1 : xy^2 : z^3\right)$. Esta aplicación es regular en todos los puntos excepto en el punto $[1:0:0]$ donde $2x^2 = xyz = z^3 = 0$.

Definición 3.19. Se dice que dos variedades V_1 y V_2 son **biracionalmente equivalentes** si existen aplicaciones racionales $\phi_1 : V_1 \to V_2$ y $\phi_2 : V_2 \to V_1$ tales que las composiciones $\phi_1 \circ \phi_2$ y $\phi_2 \circ \phi_1$ son la aplicación identidad en V_2 y V_1, respectivamente.

3.2.5. Curva Hessiana

Podemos encontrar la definición y más ejemplos de curvas Hessianas en [22].

Definición 3.20. Sea $\mathscr{F} = V(F(X_0, X_1, X_2))$ una curva proyectiva de grado d. Escribiendo $F_i = \frac{\partial F}{\partial X_i}$, $F_{ij} = \frac{\partial^2 F}{\partial X_i \partial X_j}$ tenemos que si

$$H(X_0, X_1, X_2) = \begin{vmatrix} F_{00} & F_{01} & F_{02} \\ F_{01} & F_{11} & F_{12} \\ F_{02} & F_{12} & F_{22} \end{vmatrix}$$

es no nulo, la curva proyectiva $\mathscr{H} = V(H(X_0, X_1, X_2))$ es la curva Hessiana de F, y tiene grado $3(d-2)$.

La demostración de la siguiente proposición puede consultarse en [22].

Proposición 3.2. Si p es la característica del cuerpo K y d es el grado del polinomio dado por la función $f(X,Y)$, donde $X = \frac{X_1}{X_0}$ e $Y = \frac{X_2}{X_0}$, tenemos que si $d \not\equiv 1 \,(mod\, p)$ y $\mathscr{F} = V(f(X,Y))$, entonces $\mathscr{H} = V(h(X,Y))$, donde

$$h(X,Y) = (f_X)^2 f_{YY} + (f_Y)^2 f_{XX} - 2 f_X f_Y f_{XY} - d(d-1)^{-1}\left(f_{XX} f_{YY} - (f_{XY})^2\right) f.$$

Ejemplo 3.22. Estudiando los puntos de inflexión de $\mathscr{F}$, es decir, la intersección de $\mathscr{F}$ y H , el último término del anterior polinomio puede ser omitido. De esta manera, ya no es necesario tener en cuenta la condición $d \not\equiv 1 \,(mod\, p)$.

Ejemplo 3.23. Sea la curva irreducible en un cuerpo con característica 3, $f = X_0^2 X_2 - X_1^3$. Sus derivadas parciales son: $\frac{\partial f}{\partial X_0} = 2X_0X_2$, $\frac{\partial f}{\partial X_1} = -3X_1^3$, $\frac{\partial f}{\partial X_2} = X_0^2$.
Si hacemos $X_0 = 0$ (la recta de puntos del infinito), sustituyendo en la curva tenemos que $X_1 = 0$, por lo que el único punto en el infinito es la singularidad $(0:0:1)$. Además, tenemos que $H(X_0, X_1, X_2) = 0$.
Si deshomogeneizamos tomando $X = \frac{X_1}{X_0}$, $Y = \frac{X_2}{X_0}$, nos queda la curva $Y = X^3$, que son los puntos finitos al haber tomado $X_0 \neq 0$. Tenemos claramente un punto de inflexión en $P = (0,0)$, ya que en este punto la recta tangente es $Y = 0$ y corta a la curva con multiplicidad 3.

Por ser un cuerpo de característica 3 se cumple que $(m+n)^3 = m^3+n^3$. Por lo tanto, para cualquier punto de la curva (a,b) se cumple que $b = a^3$ por lo que

$$Y - X^3 = Y - X^3 - \left(b - a^3\right) = Y - b - (X-a)^3$$

por lo que podemos escribir $(Y-b) = (X-a)^3$, por lo que (a,b) es un punto de inflexión, es decir, todo punto de la curva es un punto de inflexión.

CAPÍTULO 4

CUERPO DE FUNCIONES ALGEBRAICAS

En esta sección retomamos las extensiones algebraicas de cuerpos para aplicarlas a las curvas, por lo que estamos interesados en los conceptos explicados en la sección 2.2 (extensiones de cuerpos) y en la sección 3.2.3, es decir, estamos considerando curvas planas proyectivas.

Los cuerpos de funciones algebraicas son extensiones algebraicas del cuerpo de funciones racionales, como podemos ver en la siguiente definición:

Definición 4.1. Sea $K(X)$ el cuerpo de funciones racionales en la variable X sobre el cuerpo K . Un cuerpo de funciones algebraicas F/K de una variable sobre un cuerpo K, es una extensión de cuerpos $K \subseteq F$ tal que F es una extensión algebraica finita de $K(X)$ para algún elemento $X \in F$ trascendente sobre K.

Ejemplo 4.1. El ejemplo más sencillo de cuerpo de funciones algebraicas es el propio **cuerpo de funciones racionales**, donde F/K es racional si $F = K(X)$ para algún $X \in F$ trascendente sobre K.
El subconjunto $\tilde{K} = \{z \in F : z$ es algebraico sobre $K\}$ es un subcuerpo de F.

Ejemplo 4.2. Sea K un cuerpo algebraicamente cerrado. Tenemos que el cuerpo de funciones algebraicas $K[X,Y]/\left(Y^2 - X^3 + aX + b\right) = K(X)[Y]/\left(Y^2 - X^3 + aX + b\right)$ es una extensión de grado 3 de $K(X)$. Es el cuerpo de funciones racionales de la curva elíptica definida por $Y^2 - X^3 + aX + b = 0$. Veamos entonces cómo construir el cuerpo de funciones racionales de curvas como un cuerpo de funciones algebraicas sobre un cuerpo K.

Sea K un **cuerpo** y $K[X]$ el **anillo de polinomios** en una indeterminada sobre el cuerpo K. Sea $K(X)$ el **cuerpo de funciones racionales** en X sobre K.

En general, el cuerpo de funciones racionales de una curva $\mathscr{C}$ es una extensión algebraica finita (cuyo grado es el grado de la curva) del cuerpo de funciones racionales $K(X)$, dada por un polinomio $f(X,Y) \in K(X)[Y]$:

$$K(\mathscr{C}) = K(X)[Y]/(f(X,Y)).$$

Sea $\mathrm{K}\mathbb{A}^2$ el espacio afín sobre el cuerpo K. Dado un polinomio $f(X,Y) \in K[X,Y]$ tenemos una curva algebraica afín sobre el cuerpo K (como vimos la sección 3.1.3)

$$\mathscr{C} = \{(X,Y) \in K\mathbb{A}^2 \mid f(X,Y) = 0\}.$$

El ideal de la variedad $\mathscr{C}$ es

$$I(\mathscr{C}) = \{f(X,Y) \in K[X,Y] \mid f(p) = 0, \forall p \in \mathscr{C}\}.$$

Así, el **anillo de coordenadas locales de** $\mathscr{C}$ viene dado por el cociente

$$\Gamma(\mathscr{C}) = K[X,Y]/I(\mathscr{C}) = K(X)[Y]/I(\mathscr{C}).$$

y es el anillo de funciones polinómicas en $\mathscr{C}$. Además, este anillo es un **dominio integral**, por lo que podemos considerar su **cuerpo de fracciones:**

$$K(\mathscr{C}) = \left\{ \tfrac{g(X,Y)}{h(X,Y)} \mid g(X,Y), h(X,Y) \in \Gamma(\mathscr{C}), h(X,Y) \neq 0 \right\}$$

que es precisamente el cuerpo de funciones racionales de la curva.

Ejemplo 4.3. Consideremos las líneas $\ell = V(f)$ para $f(X,Y) = Y - mX - b$. Tenemos entonces que el anillo de coordenadas locales de ℓ es

$$\Gamma(\ell) = K[X,Y]/(f) = K(X)[Y]/(f).$$

Si $g \in K[X,Y]$, los representantes de las clases residuales $g + (f)$ son polinomios en $K[X,Y]$.

Podemos reemplazar cada Y en g por $mX + b$. Por lo tanto, los elementos de $\Gamma(\ell)$ pueden ser escritos como $g(X) + (f)$ para algunos polinomios en X. Además, si tenemos que
$g(X) + (f) = h(X) + (f)$, esto significa que $g(X) - h(X)$ es divisible por $f(X,Y) = Y - mX - b$, lo cual sólo es posible si $g = h$.

Por último, tenemos que la aplicación $\Gamma(\ell) \to K[X]$ definida por $g(X) + (f) \mapsto g(X)$ es un isomorfismo entre anillos, por lo que $\Gamma(\ell) \simeq K[X]$.

Ejemplo 4.4. Sea la parábola $\mathscr{C} = V(f)$, donde $f(X,Y) = Y - X^2$. El anillo de coordenadas locales de esta parábola viene dado por

$$\Gamma(\mathscr{C}) = K[X,Y]/(f) = K(X)[Y]/(f).$$

Entonces, cualquier elemento $g(X,Y)+\left(Y-X^2\right)$ puede ser representado por un polinomio en X ya que podemos reemplazar cualquier Y por X^2 sin modificar la clase residual. En particular, tenemos que $g(X,Y)+\left(Y-X^2\right)=g\left(X,X^2\right)+\left(Y-X^2\right)$. De nuevo, la aplicación $\Gamma(\mathscr{C})\mapsto K[X]$ definida por $g(X,Y)+(Y-X^2)\mapsto g(X,X^2)$ es un isomorfismo de anillos. Claramente es sobreyectiva, ya que cada $h\in K[X]$ es imagen de $h+\left(Y-X^2\right)$. Probamos ahora que es inyectiva. Sean g y f dos polinomios tales que $g\left(X,X^2\right)=f\left(X,X^2\right)=0$. entonces, como polinomio en $K[X,Y]$, ambos tienen a $Y-X^2$ como divisor, por lo que pertenece al ideal $\left(Y-X^2\right)$, el cual representa al 0 en el anillo de coordenadas locales.

Ejemplo 4.5. Sea $\mathscr{C}=V(f)$, donde $f(X,Y)=X^2+Y^2-1$. El anillo de coordenadas locales de esta circunferencia es:

$$\Gamma(\mathscr{C})=K[X,Y]/(f)=K(X)[Y]/(f).$$

Por ejemplo, el polinomio $g(X,Y)=X^4+X^2Y+XY^2$ tiene su imagen $g+(f)$ en $\Gamma(\mathscr{C})$. Vemos que $g+(f)=X^4+X^2Y+X(1-X^2)+(f)=X^4-X^3+X+X^2Y+(f)$.
En general, cada elemento $g+(f)$ se puede escribir en la forma
$g(X,Y)+(f)=h_1(X)+Yh_2(X)+(f)$, ya que siempre podemos reemplazar Y^2 por $1-X^2$.
En este caso, $\Gamma(\mathscr{C})$ no puede ser isomorfo a $K[X]$, ya que $K[X]$ es un dominio de factorización única y $\Gamma(\mathscr{C})$ no lo es. Tenemos que $Y^2+(f)=(1-X)(1+X)+(f)$, y los elementos $Y+(f)$, $1+X+(f)$ y $1-X+(f)$ son irreducibles.

Ejemplo 4.6. Sea C la curva cúbica definida por el polinomio $f(X,Y)=Y^2-X^3+aX+b$. El anillo de coordenadas en este caso es:

$$\Gamma(\mathscr{C})=K[X,Y]/(f)=K(X)[Y]/(f).$$

En general, cada elemento $g+(f)$ se puede escribir en la forma
$g(X,Y)+(f)=h_1(X)+Yh_2(X)+(f)$, ya que siempre podemos reemplazar Y^2 por X^3-aX-b.

La aplicación $\Gamma(\mathscr{C})\mapsto K[X]$ definida por $g(X,Y)+(f)\mapsto g(X,X^3-aX-b)$ no es inyectiva.

4.1. Plazas

Sabemos que un anillo de valuación es un anillo local. Ahora estamos interesados en anillos de evaluación dentro de cuerpos de funciones algebraicas. Tenemos presente los ejemplos de cuerpos de funciones vistos al principio de esta sección. Además, a partir de ahora, el cuerpo K es cuerpo algebraicamente cerrado.

Los conceptos de esta sección pueden ser consultados en [19] y [21]

Recordemos que si $\mathscr{C}$ es una curva e $I(\mathscr{C})$ su ideal, el anillo de coordenadas de $\mathscr{C}$ se define por el cociente:

$$\Gamma(\mathscr{C}) = K[X,Y]/I(\mathscr{C}) = K(X)[Y]/I(\mathscr{C})$$

donde la Y es la nueva coordenada local de la extensión, y su cuerpo de funciones racionales es (ver ejemplo 2.45):

$$K(\mathscr{C}) = \left\{ \tfrac{g(X,Y)}{h(X,Y)} \mid g(X,Y), h(X,Y) \in \Gamma(\mathscr{C}), h(X,Y) \neq 0 \right\}.$$

Es decir, como hemos visto anteriormente los cuerpos de funciones racionales de una curva son cuerpos de funciones algebraicas.

Definición 4.2. Se denomina **plaza** P del cuerpo de funciones F/K al ideal maximal de algún anillo de valuación $\mathscr{O}_P$ de F/K. Cualquier elemento $t \in P$ tal que $P = t\mathscr{O}_P$ se denomina elemento primo (o parámetro local) para P.

Sea K un cuerpo, p un polinomio irreducible sobre $K(X)$, F una extensión algebraica de $K(X)$ sobre el polinomio p, y una curva $\mathscr{C}$ definida por el polinomio $p(X,Y) = 0$. Establecemos en F la siguiente relación de equivalencia: decimos que $z = \frac{f}{g}$ es equivalente a $z - \frac{rq}{h}$, donde $r \nmid h$. El conjunto de todas las funciones racionales de la forma $\left\{z - \frac{rq}{h}\right\}$ es un cuerpo, que es justamente el cuerpo de funciones racionales de la curva $\mathscr{C}$, $K(\mathscr{C})$. Entonces cada clase de equivalencia $[z]$ será una plaza.

El siguiente ejemplo está extraído de [19].

Ejemplo 4.7. Cuerpo de Funciones Racionales. En el caso del cuerpo de funciones racionales podemos definir el anillo de valuación correspondiente a un polinomio mónico irreducible $p(X) \in K[X]$ como sigue (ver también ejemplo 2.45):

$$\mathscr{O}_{p(X)} = \left\{ \tfrac{f(X)}{g(X)} \mid f(X), g(X) \in K[X], p(X) \nmid g(X) \right\}.$$

Si consideramos cualquier otro polinomio, digamos $q(X) \in K(X)$, en lugar de $p(X)$, esto da lugar a un anillo de valuación diferente $\mathscr{O}_{q(X)}$ en el campo de funciones racionales $K(X)$.

Con esta definición de $\mathscr{O}_{p(X)}$, las unidades en este anillo de valuación están dadas por aquellos elementos que satisfacen, no sólo que $p(X) \nmid g(X)$, sino también que $p(X) \nmid f(X)$. Por lo tanto, los elementos que no son unidades satisfacen que $p(X) \nmid g(X)$ y $p(X) \mid f(X)$.

Continuando con el ejemplo 4.7 (ver [19]), definimos los conceptos de cero y polo en una plaza P dada por un polinomio $p(X)$:
Sea $z_1 = \frac{h_1(X)}{g_1(X)} = \frac{(p(X))^2 f_1(X)}{g_1(X)}$ donde $p(X) \nmid f_1(X)$ y $p(X) \nmid g_1(X)$. Entonces los ceros del polinomio $p(X)$ son también **ceros** de la función z_1. Tenemos que $\frac{f_1(X)}{g1(X)}$ es una unidad del anillo de valuación $\mathscr{O}_{p(X)}$. Por lo tanto, en este caso podemos decir que la plaza $P_{p(X)}$ es un **cero** de z_1.
Tomamos ahora una función diferente $z_2 = \frac{f_2(X)}{s_2(X)} = \frac{f_2(X)}{(p(X))^3 g_2(X)}$ donde $p(X) \nmid f_2(X)$ y

$p(X) \nmid g_2(X)$. Entonces los ceros del polinomio $p(X)$ crean **polos** para z_2. En este caso, la plaza $P_{p(X)}$ se denomina **polo** de z_1.

Definimos ahora la plaza en el infinito del cuerpo de funciones racionales $K(X)$ como:

$$P_\infty = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in K[X], deg\, f(X) < deg\, g(X) \right\}.$$

El anillo de valuación determinado por esta plaza es:

$$\mathcal{O}_\infty = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in K[X], deg\, f(X) \leq deg\, g(X) \right\}.$$

Recordemos que si K es un cuerpo de números algebraicos y p un polinomio irreducible sobre el cuerpo de funciones racionales $K(X)$, el cuerpo de funciones racionales de una curva $\mathscr{C}$ es una extensión algebraica de $K(X)$ sobre el polinomio p. Este polinomio define la curva, cuyos puntos son aquellos donde se anula p. Veamos cómo están relacionados los conceptos de plaza y los puntos (a,b) de una curva $\mathscr{C}$, con $a,b \in K$ y $p(a,b) = 0$.

Sabemos que el cuerpo de funciones racionales de la curva $\mathscr{C}$ es $K(\mathscr{C}) = K(X)[Y]/(p(X,Y))$. Podemos entonces escribir cualquier elemento $q \in K(\mathscr{C})$ como $q = \frac{A(X,Y)}{B(X,Y)}$ donde $A, B \in \Gamma(\mathscr{C})$, el anillo de coordenadas de la curva. Tenemos entonces que

$$\mathcal{O}_{(a,b)} = \left\{ q \in K(\mathscr{C}) \mid q = \frac{A(X,Y)}{B(X,Y)}, B(a,b) = 0 \right\}$$

$$P_{(a,b)} = \left\{ q \in K(\mathscr{C}) \mid q = \frac{A(X,Y)}{B(X,Y)}, A(a,b) = 0 \right\}$$

que son el anillo de valuación y su plaza P correspondiente.

Ilustramos esto con el siguiente ejemplo:

Ejemplo 4.8. sea el cuerpo $K = \mathbb{R}$.

a) Supongamos que $p(X,Y) = Y^2 - X^4 + 1$. Tomamos $a = \frac{1}{X}$ y $b = -1 + \frac{Y}{X^2}$. Tenemos que $p(1,0) = 0$. Por lo tanto tenemos que $A(X,Y) = a^4 + b^2 + 2b = 0 = p(1,0)$, como se comprueba fácilmente.

b) Supongamos que $p(X,Y) = X^3 + Y^3 - XY = 0$. Tomando $a = X - \frac{1}{2}$ y $b = Y - \frac{1}{2}$, tenemos que $p\left(\frac{1}{2}, \frac{1}{2}\right) = 0$ y $A(X,Y) = 4a^3 + 6a^2 + a + 4b^3 + 6b^2 + b - 4ab = 0 = p\left(\frac{1}{2}, \frac{1}{2}\right)$.

En ambos casos, $A(X,Y)$ determina una plaza para el correspondiente punto (a,b).

El conjunto de plazas de F/K se denota por $\mathbb{P}(F)$. Podemos omitir el cuerpo base K, pues para cada plaza P de F/K se puede probar que $\overline{K} \subseteq \mathcal{O}_P$.

Definición 4.3. Sea F un cuerpo de funciones algebraicas sobre un cuerpo K. Sea $P \in \mathbb{P}(F)$ una plaza y la valuación $v_P : F \to \mathbb{Z} \cup \{\infty\}$, la cual asociamos a la plaza de la siguiente manera: sea t un elemento primo para P. Entonces todo $z \in F$ con $z \neq 0$ tiene una representación única $z = t^n u$ con $u \in \mathcal{O}^\times$ y $n \in \mathbb{Z}$. Definimos entonces $v_P(z) := n$ y $v_P(0) := \infty$.

Definición 4.4. ceros y polos. Sea $z \in F$ y una plaza $P \in \mathbb{P}(F)$.

- Decimos que P es un **cero** de z si $v_P(z) = m > 0$, $m \in \mathbb{Z}$. Entonces P es un **cero de orden** m.
- Decimos que P es un **polo** de z si $v_P(z) = m < 0$, $m \in \mathbb{Z}$. Entonces P es un **polo de orden** m.

En la sección 2 definimos lo que era un anillo de valuación discreta. La demostración del siguiente Teorema la podemos encontrar en [21] Teorema 1.1.13.

Teorema 4.1. Sea F/K un cuerpo de funciones algebraicas. Para una plaza $P \in \mathbb{P}(F)$, la función v_P definida anteriormente es una valuación discreta de F/K. Más aún, tenemos que:

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

Tenemos que el cuerpo de constantes $\overline{K}$ de F/K se cumple que $\overline{K} \in \mathcal{O}$ y $\overline{K} \cap M$.

Además, un elemento $x \in F$ es elemento primo de P si y sólo si $v_P(x) = 1$. Recíprocamente, si v es una valuación discreta de F/K, entonces el conjunto $P = \{z \in F \mid v(z) > 0\}$ es una plaza de F/K y $\mathcal{O}_P = \{z \in F \mid v_P(z) > 0\}$ es el anillo de valuación correspondiente.
Cada anillo de valuación $\mathcal{O}$ de F/K es un subanillo maximal y propio de F.

Definición 4.5. Sea $P \in \mathbb{P}(F)$. Tenemos entonces que $F_P := \mathcal{O}_P/P$ es el cuerpo de clases residuales de P. La función

$$F \to F_P \cup \{\infty\}$$

$$x \mapsto x(P)$$

se denomina función de clases residuales. Para todo $x \in \mathcal{O}_P$, denotamos por $x(P)$ a la clase de residuos módulo P, y para $x \in F \setminus \mathcal{O}_P$ definimos $x(P) = \infty$.

La demostración del siguiente teorema puede encontrase en [21].

Teorema 4.2. Sea P una plaza de F/K y sea $\mathcal{O}_P$ su anillo de valuaciones. Tenemos que P es un ideal maximal de , el anillo de clases residuales $\mathcal{O}_P/P$ es un cuerpo que contiene una copia isomorfa de K. Además, el cuerpo de clases residuales F_P es isomorfo a la extensión algebraica de K.

4.2. Puntos racionales

Definición 4.6. Definimos el grado de una plaza P como $degP = [F_P : K]$. Una plaza de grado uno, se dice que es una **punto racional** de F/K. El grado de una plaza siempre es finito.

Consideremos una plaza P, F/K una extensión de un cuerpo K y F_P su cuerpo de clases residuales.

Ejemplo 4.9. Sea una curva $\mathscr{C}$ definida por un polinomio $p(X,Y) \in K(X,Y)$. Las plazas racionales de $\mathscr{C} = V(p)$ no son otra cosa que las raíces de p que están en K. Observamos que este conjunto puede ser vacío, por ejemplo si $p(X,Y) = X^2 + Y^2$ y $K = \mathbb{Q}$.

Ejemplo 4.10. Sea la curva $\mathscr{C}$ definida por el polinomio $p(X,Y) = Y^{10} - X^3 - 77X$ en el cuerpo $\mathbb{F}_{81}$. Algunos puntos racionales de $\mathscr{C}$ son $(76,71)$ y $(27,60)$. Todos los puntos racionales en $\mathbb{F}_{81}$ de esta curva pueden consultarse en la Tabla 7.10.

La demostración de la siguiente proposición puede encontrarse en [21] Proposición 1.1.15.

Proposición 4.1. Sea un cuerpo K y una extensión algebraica F/K. Si P es una plaza de F/K y $X \in P$ con $x \neq 0$, entonces

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

Observamos que para el caso en que $degP = 1$ tenemos que $F_P = K$ y la función de clases residuales aplica F en $K \cup \{\infty\}$. En particular, cuando K es algebraicamente cerrado, todas las plazas son de grado uno, por lo que se puede considerar a cada elemento como una función

$$r : \mathbb{P}(F) \to K \cup \{\infty\}$$

$$P \mapsto r(P).$$

La proposición anterior da lugar al siguiente corolario, cuya demostración se puede encontrar en [21], Corolario 1.3.4.

Corolario 4.1. En un cuerpo de funciones algebraica F/K todo elemento $z \in F$ con $z \neq 0$ tiene una cantidad finita de ceros y de polos.

Ejemplo 4.11. Sobre el cuerpo de funciones $\mathbb{F}_3$, busquemos las plazas racionales de la curva definida por la ecuación afín $Y^2 = X^3 - X + 1$.

La correspondiente ecuación de la curva proyectiva viene dada por $Y^2Z = X^3 - XZ^2 + Z^3$. Haciendo $Z = 0$, tenemos que $X^3 = 0$, es decir, la única plaza en el infinito es $P_\infty = (0:1:0)$.

Por otro lado, para cada par $(a,b) \in \mathbb{F}_3 \times \mathbb{F}_3$ tal que $b^2 = a^3 - a + 1$, tendremos una plaza $P_{(a,b)}$ de grado 1. Estas plazas racionales son los puntos

$$P_1 = (0,1), P_2 = (0,2), P_3 = (1,1), P_4 = (1,2), P_5 = (2,1) \text{ y } P_6 = (2,2).$$

4.3. Divisores y grupo de divisores

Como hemos mencionado en la introducción, la idea Goppa se basó en asociar los divisores de cuerpos de funciones algebraicas con los códigos. Como veremos, los divisores son conjuntos de plazas, y la parte de valuación positiva de las plazas están dadas por polinomios que son múltiplos de otros polinomios.

Consideremos un cuerpo K, F el cuerpo de funciones algebraicas sobre K y $\mathbb{P}(F)$ el conjunto de plazas de F. Suponemos a partir de ahora que el cuerpo base K es algebraicamente cerrado en el cuerpo de funciones F, es decir, $\overline{K} = K$.

Definición 4.7. Se denomina grupo de divisores de la extensión F/K al grupo abeliano libre generado por las plazas de F, y lo denotamos por $div(F)$, es decir,

$$div(F) = \{\sum_{P\in\mathbb{P}(F)} n_P P : n_P \in \mathbb{Z} \text{ con } n = 0, \text{ salvo un número finito}\}.$$

A los elementos de $div(F)$ se les denominan divisores de F/K. Por lo tanto, los divisores son cualquier combinación lineal de plazas.

Si $D = \sum_{P\in\mathbb{P}(F)} n_P P \in div(F)$, definimos el soporte de D como

$$suppD := \{P \in \mathbb{P}(F) : n_P \neq 0\}.$$

Abusando de la notación, dada una curva $\mathscr{C}$ con cuerpo de funciones racionales F diremos que un divisor de F es un divisor de la curva.

Ejemplo 4.12. Sobre el cuerpo $\mathbb{Q}$, sea la ecuación de la curva afín dada por $Y^2 = X^3 + 2X - 3$. Dos plazas racionales de grado 1 son $P_1 = (2,3)$, $P_2 = (1,0) \in \mathbb{P}(F)$. Entonces, tenemos que $D = 5(P_1) - 7(P_2)$ es un divisor de la curva. El soporte de D es $suppD = \{P_1, P_2\}$. En $div(F)$ definimos un orden parcial de la siguiente forma: si $D_1, D_2 \in div(F)$, entonces $D_1 \leq D_2$ si y solo si $v_P(D_1) \leq v_P(D_2)$ para todo $P \in \mathbb{P}(F)$. Si $D_1 \leq D_2$ y $D_1 \neq D_2$, escribiremos $D_1 < D_2$.
Un divisor D se denomina **positivo (o efectivo)** si $D \geq 0$.

Definición 4.8. Definición: Se define el grado de un divisor D como

$$degD = \sum_{P\in\mathbb{P}(F)} v_P(D) degP.$$

Por el Corolario anterior, sabemos que todo elemento no nulo $z \in F$ tiene una cantidad finita de ceros y polos en $\mathbb{P}(F)$. Entonces, la siguiente definición tiene sentido:

Definición 4.9. Sea $z \in F$ con $z \neq 0$ y denotemos por Z al conjunto de ceros y por N al conjunto de polos de z en $\mathbb{P}(F)$. Entonces definimos:

- $(z)_0 := \sum_{P\in Z} v_P(z)P$, denominado divisor de ceros del elemento z,

- $(z)_\infty := \sum_{P \in N} (-v_P(z))P$, denominado divisor de polos del elemento z,
- $(z) := (z)_0 - (z)_\infty$, denominado divisor principal del elemento z.

Puede consultarse la demostración del siguiente Teorema en [21] Teorema 1.4.11.

Teorema 4.3. Sea $z \in F \setminus K$. Entonces $deg(z)_0 = deg(z)_\infty = [F : K(z)]$. En particular, todos los divisores principales tienen grado cero.

4.4. Teorema de Riemann-Roch

El Teorema de Riemann-Roch para curvas algebraicas es muy importante ya que en él se basa la Teoría de Números sobre curvas, pues relaciona las propiedades de las curvas de naturaleza puramente algebraica, con las propiedades de naturaleza topológica y geométrica.
Los conceptos y definiciones de esta sección pueden ser consultados en [19] , [21] y [5].

Definición 4.10. Sea $D \in div(F)$. Definimos el espacio de Riemann-Roch asociado a D por

$$\mathscr{L}(D) = \{x \in F : v_P(x) \geq -D\} \cup \{0\}.$$

El espacio de Riemann-Roch es un espacio vectorial de dimensión finita sobre K, cuya dimensión se denota como $\ell(D)$.

Dado un divisor $D \in div(F)$, el entero $\ell := dim\mathscr{L}(D)$ se denomina **dimensión del divisor** D.

En esta sección nos basamos en [19].

Definimos en esta sección el concepto de género g de una curva, el cuál puede ser definido tanto para curvas singulares como para no singulares. Nos centraremos en las curvas no singulares. Desde el punto de vista topológico, una curva proyectiva no singular en $\mathbb{P}^2$ puede ser vista como una superficie isomorfa a una esfera con g asas. Este número g de asas es el **género** de la curva. Sea ahora un polinomio $p(X,Y)$ de grado d. Entonces el género de la curva proyectiva plana no singular definida por p, está relacionada con el grado d del polinomio por la fórmula de Plücker:

$$g = \tfrac{1}{2}(d-1)(d-2).$$

Ejemplo 4.13. las curvas de Fermat. En el plano proyectivo, sea la curva algebraica definida en coordenadas homogéneas por el polinomio:

$$f^*(X,Y,Z) = X^n + Y^n - Z^n.$$

En el plano afín, la curva viene dada por el polinomio

$$f(X,Y) = X^n + Y^n - 1.$$

Esta es una curva no singular, y su género viene dado por

$$g = \tfrac{1}{2}(d-2)(d-1).$$

Si $n+2$, tenemos una cónica, con género 0, y el género es uno en el caso de que $n=3$, es decir, para una curva elíptica.

El siguiente ejemplo puede ser consultado en [22] Sección 12.3.

Ejemplo 4.14. curvas hermitianas. Un caso particular de las curvas de Fermat son las curvas hermitianas. Una curva hermitiana es una curva plana irreducible sobre el cuerpo $\mathbb{F}_{q^2}$, con $q = p^h$ con p primo, dada por:

$$V\left(Y^{q+1} - X^q - X\right).$$

En el Teorema 12.24 de [22] podemos consultar la demostración de que esta curva es no singular y tiene género $g = \frac{1}{2}q(q-1)$.

Ejemplo 4.15. sea la curva $\mathscr{C}$ definida por el polinomio $p(X,Y) = Y^5 - X^2 - X$ sobre el cuerpo $\mathbb{F}_{16}$. Esta curva tiene género $g(\mathscr{C}) = \frac{q(degQ-1)}{2} = 2$ y algunos de sus puntos racionales (los cuáles calcularemos posteriormente) son $P = (2,11)$ y $Q = (3,13)$ por lo que cualquier combinación lineal de ellos es un divisor de la curva $\mathscr{C}$.

Otra forma equivalente de definir el género g, para curvas no singulares, viene dada por la siguiente definición:

Definición 4.11. Se define el genero g de un cuerpo de funciones F/K como

$$g = max\{deg(D) - \ell(D) + 1 : D \in div(F)\}.$$

Un divisor con $degD = 2g-2$, donde g es el género de la curva se denomina **divisor canónico**, $\mathscr{K}$. El género es uno de los invariantes mas importantes de un cuerpo de funciones, y podemos verificar que existe y que es un numero entero no negativo (consultar [21] Proposición 1.4.14).

Enunciamos el Teorema de Riemann-Roch el cual, dado el género de una curva, nos proporciona la dimensión del espacio de un divisor.

La demostración del Teorema de Riemann-Roch puede encontrarse en [21] Teorema 1.5.15.

Teorema 4.4. Teorema de Riemann-Roch: Sea $\mathscr{K}$ un divisor canónico de F/K. Entonces, para cada divisor $D \in div(F)$ tenemos que

$$\ell(D) = deg(D) + 1 - g + \ell(\mathscr{K} - D).$$

Ilustramos el Teorema de Riemann-Roch con el siguiente ejemplo:

Ejemplo 4.16. Como veremos en la sección 5, el conjunto de soluciones de una curva elíptica sobre $\mathbb{C}$ es topológicamente equivalente a un toro. Por lo tanto, el género g de una curva elíptica es 1. Sea la curva elíptica $\mathscr{C}$ definida por el polinomio $p(X,Y) = Y^2 - X^3 - 1$ sobre $\mathbb{C}$.

Consideremos ahora una función z perteneciente al cuerpo de funciones de la curva $\mathscr{C}$. Sabemos que $v_P(z) = n$ si z tiene un cero de orden n en P (n puede ser negativo si en lugar de un cero es un polo). Por lo tanto, comprobando todos los ceros y los polos de esta función, podemos construir un divisor a partir de z, que denotaremos por $div(z)$. Por ejemplo, sea $z = x-2$. Entonces tenemos que $z = 0$ si $x = 2$, lo cual ocurre para los puntos $Q = (2,3)$ y $Q' = (2,-3)$, comprobando fácilmente que son ceros simples. Entonces tenemos que $v_Q(z) = v_{Q'}(z) = 1$. Además, z tiene un polo de orden 2 en el punto ∞, por lo que $v_\infty(z) = -2$. Teniendo ya todos los polos y los ceros, podemos ver que $div(z) = (Q) + (Q') - 2(\infty)$.

Para el espacio de Riemann-Roch $\mathscr{L}(D)$, lo que queremos es encontrar todas las funciones cuyo divisor sea el negativo de, al menos, otro divisor. Por ejemplo, si tomamos $D = (Q) + (Q')$, lo que estamos diciendo es que sólo permitimos funciones las cuales tengan polos simples en Q y Q' y en ningún otro punto. Es fácil comprobar que se genera un espacio vectorial complejo.

Por ejemplo, la función $g = \frac{1}{x-2}$ está en este espacio (al igual que cualquier múltiplo de ella en el espacio vectorial). Por lo tanto tenemos un sólo elemento en la base, por lo que $\ell(D) \geq 1$. Podemos comprobar también que $h = \frac{x}{x-2}$ también pertenece al espacio y en este caso $\ell(D) = 2$. Todas las funciones no constantes tienen polos, por lo que si el grado de D es negativo, entonces $\ell(D) = 0$.

Por lo tanto, el Teorema de Riemann-Roch puede ser visto como la definición del género y también para obtener $\ell(D)$. Ahora, para el divisor canónico $\mathscr{K}$ tenemos que $deg\mathscr{K} = 2g-2$ lo que implica que $deg(\mathscr{K} - D) = -2$, por lo que al ser negativo $\ell(\mathscr{K} - D) = 0$, cumpliéndose la igualdad dada por el Teorema de Riemann-Roch.

CAPÍTULO 5

CUBIERTAS

Los conceptos topológicos de la esta sección pueden consultarse en [1]. Además, nos basamos en [19], [10] , [17] y [14]

Tenemos presente en esta sección las definiciones de aplicación regular y variedades birracionalmente equivalentes dadas en la sección 3.2.4.

Recordemos también que cualquier curva dada es una cubierta de la recta proyectiva del cuerpo base utilizado. Los cuerpos de funciones algebraicas corresponden a cubiertas de curvas. Lo que nos interesa, y veremos en la siguiente sección, es encontrar métodos para, dada una curva con muchos puntos racionales, calcular cubiertas de ella obteniendo otras curvas con más puntos racionales para el correspondiente cuerpo; y al contrario, obtener curvas con muchos puntos racionales sabiendo que están cubiertas por otras curvas (subcubiertas), en nuestro caso, curvas hermitianas. Como ya sabemos, las curvas hermitianas son maximales, por lo que las subcubiertas también serán maximales.

En [10] podemos encontrar la demostración de la siguiente proposición.

Proposición 5.1. Se denomina **morfismo** a una aplicación racional $\phi : V \to W$ que es regular en todos los puntos $a \in V$. Se denomina **isomorfismo** si existe un morfismo $\psi : W \to V$ tal que $\phi \circ \psi$ y $\psi \circ \phi$ son la aplicación identidad en W y V, respectivamente. Decimos entonces que V y W son isomorfas.

Notar que isomorfismo implica equivalencia biracional pero, en general, lo contrario no es cierto.

Los conceptos de esta sección pueden encontrarse en [19].

Sean C_1 y C_2 dos curvas algebraicas con cuerpos de funciones F_1 y F_2, respectivamente. Entonces, C_1 es una cubierta de C_2 si podemos definir un **morfismo** $p : C_1 \to C_2$ entre las dos curvas. Esto se corresponde al morfismo $F_1 \to F_2$ entre los cuerpos de funciones donde F_1 es una **extensión** de F_2. Además, el grado de la cubierta está dado por el grado de la extensión de cuerpos del cuerpo de funciones de la curva que se recubre, C_2, a la cubierta C_1, es decir, $[F_1 : F_2] = n$, por lo que el grado de la cubierta de C_2 es también n.

Ejemplo 5.1. Sea un cuerpo K y consideremos la línea proyectiva $\mathrm{K}\mathbb{P}^1$, la cual es obtenida añadiendo a la línea afín $K\mathbb{A}^1$ un punto en el infinito. Entonces, tenemos que considerar las funciones del cuerpo de funciones racionales $K(X)$, donde X es un elemento trascendente. Por lo tanto, el anillo de coordenadas proyectivas (homogéneas) es obtenido mediante el anillo cociente

$$K[X,Y]/\left(\tfrac{1}{X} - Y\right) = K\left[X, \tfrac{1}{X}\right] = K[X].$$

Consideremos ahora la curva $\mathscr{C}$ definida por el polinomio $p(X,Y) = 2X^2Y^2$. Tenemos que el cuerpo de funciones de esta curva es una extensión de grado 8 de $K(X)$, por lo que $[F : K(X)] = 8$.

Si consideramos la cubierta de la línea proyectiva $\mathrm{K}\mathbb{P}^1$ por la curva $\mathscr{C}$, vemos que es de grado 8, ya que el grado de la cubierta coincide con el grado de la extensión de cuerpos $F/K(X)$.

5.1. Funciones meromorfas y elípticas

Como ejemplo de cubiertas de curvas tenemos las funciones meromorfas y elípticas, donde utilizamos la estructura compleja de la curva para dotarla de una estructura algebraica.

Las siguientes definiciones y conceptos se pueden consultar en [10].

Definición 5.1. Sea f una función definida en el plano complejo $\mathbb{C}$. Un número complejo t es un **periodo** de f si

$$f(z+t) = f(z)$$

para todo $z \in \mathbb{C}$.A la función f se la denomina **función periódica** de periodo $t \neq 0$.

Definición 5.2. Retículo Sean w_1, w_2 números complejos tales que $\frac{w_1}{w_2}$ no es un número real. Se define **retículo** como:

$$L = \{mw_1 + nw_2 \mid n, m \in \mathbb{Z}\}.$$

En [10] podemos encontrar la demostración de que un retículo es un grupo aditivo de $\mathbb{C}$, y abeliano, por lo tanto, normal. En el mismo libro, podemos también consultar la definición de **región fundamental**.

Definición 5.3. Una función **meromorfa** del plano complejo en la esfera de Riemann $f : \mathbb{C} \to \sum$ es **elíptica** con respecto a un retículo $L \subseteq \mathbb{C}$ si f es doblemente periódica respecto a L, es decir, si

$$f(z+t) = f(z) \text{ para todo } z \in \mathbb{C}, t \in L,$$

por lo que cada $t \in L$ es un periodo de f.

Sean ahora las funciones doblemente periódicas, es decir, las funciones elípticas, con periodos w_1 y w_2 para x e y, respectivamente ($z = x + iy, x, y \in \mathbb{R}$). Estas funciones están definidas en una región fundamental que es un paralelogramo P de lados $[0, w_1] \times [0, w_2]$, con los puntos de los lados paralelos identificados entre sí. Tenemos que este paralelogramo es el cociente de $\mathbb{C}$ por el retículo L. Visto de manera topológica, el paralelogramo P con las identificaciones descritas es un toro T, es decir,

$$T = \mathbb{C}/L.$$

Definición 5.4. Función de Weierstrass. Dado un retículo L, la función $\mathscr{P}$ de Weierstrass asociada se define como:

$$\mathscr{P}(z) = z^{-2} + \sum_{w \in L - \{0\}} \left((z-w)^{-2} - w^{-2} \right).$$

Su derivada es

$$\mathscr{P}'(z) = -2 \sum_{w \in L} (z-w)^{-3}.$$

La demostración de que la función de Weierstrass es una función meromorfa con periodos w_1, w_2 se puede consultar en [10].

Las funciones doblemente periódicas están definidas en T, son meromorfas en T, y están generadas por la función de Weierstrass y su derivada. Por lo tanto **las funciones meromorfas en un toro complejo determinado por el retículo L coinciden con las funciones meromorfas doblemente periódicas en $\mathbb{C}$, es decir, con las funciones elípticas.**

Recordemos que dada una función $F : X \to Y$ entre superficies de Riemann, $p \in X$ es un punto de ramificación de F si $mult_p(F) > 1$.

Por otro lado, en [20] sección 3.15, se demuestra que las funciones $\mathscr{P}$ y $\mathscr{P}'$ inducen **cubiertas ramificadas** $\mathscr{P} : T \to \sum$ y $\mathscr{P}' : T \to \sum$ del toro en la esfera de Riemann.

Tenemos que la función $\mathscr{P}$ es trascendente en $\mathbb{C}(z)$, por lo que hace de **coordenada local,** pero la función $\mathscr{P}'$ es algebraica sobre $\mathbb{C}(z)$, ya que es la raíz del polinomio $w^2 = z^3 + az + b$. De esta

forma, tenemos que $F = \mathbb{C}(z)[w]/\left(w^2 - z^3 - az - b\right)$ **es una extensión de grado 3**, $[F : \mathbb{C}(z)] = 3$. La extensión es la extensión de la cubierta $\mathscr{P}$.

Denotemos por V a la curva $w^2 - z^3 - az - b$. Tenemos entonces que la extensión F es un cuerpo de funciones racionales, precisamente las funciones racionales del anillo coordenado de la curva V, cuyo ideal es el generado por V, $I = \left(w - z^3 - az - b\right)$.

Entonces la curva V es una cubierta de $\sum$ con función cubierta $\mathscr{P}$. Por tanto la curva V es el toro T. El cuerpo de funciones meromorfas de T es el cuerpo de funciones racionales de la curva V. Además, podemos identificar cada punto (plaza) en V con un punto en T. La curva se llama elíptica porque sus funciones racionales son funciones elípticas.

5.2. Ramificación

Los conceptos de esta sección pueden ser consultados en [19] y [22].

En Análisis Complejo se estudia el concepto de ramificación en Superficies de Riemann. Este concepto de traduce ahora a ramificación en curvas sobre cuerpos finitos.

Consideremos ahora dos curvas algebraicas C y C', con F y F' sus correspondientes cuerpo de funciones, y donde C' es una cubierta de C, es decir, F'es una extensión algebraica de F.

Definición 5.5. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}\left(F'\right)$ dos plazas. Decimos que Q **divide** a P, o que Q **está encima** de P si $P \subset Q$, y lo denotaremos por $Q|P$.

La demostración de la siguiente proposición se puede encontrar en [21] (Proposición 3.1.4):

Proposición 5.2. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}\left(F'\right)$ dos plazas. $Q|P$ es equivalente a la existencia de un número entero $e \geq 1$ tal que $v_Q(z) = e v_P(z)$ para todo $z \in F$, siendo v_Q y v_P las respectivas valuaciones. Además $Q \cap F = P$.

La siguiente definición puede ser consultada en [21] (Definición 3.1.5).

Definición 5.6. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}\left(F'\right)$ dos plazas. Se denomina **índice de ramificación** $e(Q|P)$ de Q sobre P al único entero $e(Q|P) := e$ que satisface

$$v_Q(x) = e v_P(x).$$

Decimos que $Q|P$ está ramificado si $e(Q|P) > 1$. Si $e(Q \mid P) = 1$ decimos que $Q|P$ no ramifica. Entonces una plaza $P \in \mathbb{P}(F)$ está ramificada en F'/F si existe un $Q \in \mathbb{P}\left(F'\right)$ tal que $Q|P$ ramifica. En caso contrario, decimos que P no ramifica en F'/F.

Definición 5.7. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}\left(F'\right)$ dos plazas. Se denomina **grado relativo** de Q sobre P a $\left[F'_Q : F_P\right]$, denotado por $f(Q|P)$, es decir, $f(Q|P) := \left[F'_Q : F_P\right]$.

Si F'/F es una extensión algebraica separable y $Q \in \mathbb{P}\left(F'\right)$ entonces la restricción $Q \cap F$ de Q a F es una plaza de F.

Igualdad fundamental

Se pueden consultar los conceptos de esta sección en [21]:

Teorema 5.1. Igualdad fundamental Si F/F' es una extensión finita de cuerpos de funciones y $P \in \mathbb{P}(F)$ entonces

$$\sum_{\substack{Q \in \mathbb{P}(F') \\ Q|P}} e(Q|P) f(Q|P) = [F' : F].$$

La demostración del Teorema anterior puede ser consultada en [21] Teorema 3.1.11.

La igualdad fundamental proporciona información importante sobre cómo calcular el valor de $f\left(P'_i|P\right)$ una vez conocido el índice de ramificación y el grado de la extensión. En particular, si $f\left(P'|P\right) = 1$ sabemos que el grado de la plaza P' que está por encima de la plaza P tiene el mismo grado que P. Por lo tanto (si P es una plaza racional entonces es de grado 1), entonces, si el grado relativo is$f\left(P'|P\right) = 1$, P' también es una plaza racional ($degP' = 1$). Por lo tanto, si tenemos que el grado relativo es $f\left(P'|P\right) = 1$, lo que nos interesa es que P se divida completamente, es decir, cuando hay $[F' : F] = n$ plazas sobre P con $e\left(P'|P\right) = f\left(P'|P\right) = 1$, o cuando P es totalmente ramificado, es decir, $e\left(P'|P\right) = n = [F' : F]$ con $f\left(P'|P\right) = 1$.

Ejemplo 5.2. en el ejemplo de la Figura 5.1 podemos ver las plaza P_1 y P_2 cubiertas por otras plazas. La plaza P_1 está cubierta por la plaza P'_{1_1}, la cual es totalmente ramificada. Sin embargo, la plaza P_2 está cubierta por las plazas P'_{2_1}, la cual es ramificada (pero no totalmente ramificada) y la plaza P'_{2_2}, la cual no está ramificada. tenemos entonces que:

- Plaza P_1: está cubierta por la plaza P'_{1_1}, la cual está completamente ramificada ya que es la única que está por encima de la plaza P_1. Entonces, $e\left(P'_{1_1}|P_1\right) = [F' : F] = 3$, y $f\left(P'_{1_1}|P_1\right) = 1$. Por lo tanto,

$$\sum_{i=1}^{n} e\left(P'_i|P\right) f\left(P'_i|P\right) = 1 + 1 + 1 = 3.$$

- Plaza P_2: está cubierta por las plazas P'_{2_1} y P'_{2_2}. La plaza P'_{2_1} está ramificada, pero no totalmente ramificada. Entonces, en este caso $e\left(P'_{2_1}|P_2\right) = 2$ y $f\left(P'_{2_1}|P_2\right) = 1$. La plaza P'_{2_2} no está ramificada, por lo que $e\left(P'_{2_2}|P_2\right) = 1$ y $f\left(P'_{2_2}|P_2\right) = 1$. Entonces,

$$\sum_{i=1}^{n} e\left(P'_i|P\right) f\left(P'_i|P\right) = (2 \cdot 1) + (1 \cdot 1) = 3.$$

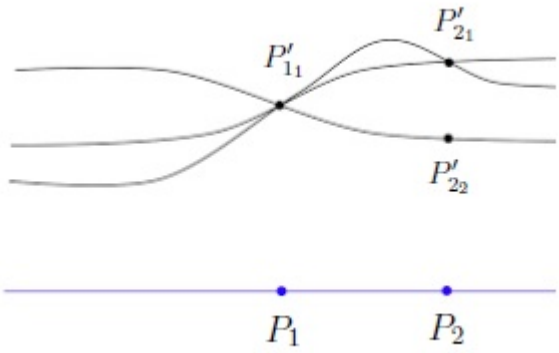

Figura 5.1: Cubierta

CAPÍTULO 6

CURVAS CUBIERTAS POR CURVAS HERMITIANAS

En esta sección estudiamos el artículo [7] y nos basaremos también en los artículos [20] y [6].

Analizaremos el artículo [7], de Arnaldo García, Motoko Q. Kawatika y Shinji Miura (2006)) On Certain Subcovers of the Hermitian Curve, Communications in Algebra, 34:3, 973-982, DOI: 10.1080/00927870500441940. En este artículo se presenta una construcción para obtener ecuaciones explícitas para ciertas curvas que están cubiertas por curvas hemitianas, por lo que las curvas obtenidas son maximales.

Junto con el artículo [7] se da un método para obtener curvas con ecuación $Y^{q+1} = aX + X^m$, es decir se da un método de obtención del exponente m.

Las curvas sobre cuerpos finitos con muchos puntos racionales son muy importantes para la Teoría de Códigos y la Criptografía. Las curvas que vienen dadas en forma explícita y que tienen muchos puntos racionales con respecto a su género, pueden ser usadas para construir correctores de errores lineales en la transmisión códigos.

En esta tesis hemos desarrollado un algoritmo para obtener las extensiones de los cuerpos tratados en el artículo. Además, una vez obtenidos los cuerpos, el algoritmo evalúa todas las coordenadas del cuerpo en las curvas obtenidas como ejemplos para hallar todos sus puntos racionales.

La cota de Hasse-Weil.

Se puede consultar la demostración de la cota de Hasse-Weil en [21] (Teorema 5.2.3).

El número de puntos racionales o plazas de grado uno de una curva sobre un cuerpo $\mathbb{F}_{q^n}$ está acotado y puede ser estimado por la cota de Hasse-Weil.

Sea una curva $\mathscr{C}$ una curva proyectiva sobre un cuerpo $\mathbb{F}_{q^n}$, g el género de $\mathscr{C}$ y $\#\mathscr{C}\left(\mathbb{F}_{q^n}\right)$ el número de puntos racionales de la curva. La cota de Hasse-Weil viene dada por la desigualdad

$$\#\mathscr{C}\left(\mathbb{F}_{q^n}\right) \leq q^n + 1 + 2g\sqrt{q^n}.$$

Definición 6.1. Sea $\mathscr{C}$ una curva sobre un cuerpo $\mathbb{F}_{q^n}$, donde $n = 2$. Decimos que la curva es **maximal** si se da la igualdad en la cota de Hasse-Weil, es decir, si

$$\#\mathscr{C}\left(\mathbb{F}_{q^2}\right) = q^2 + 1 + 2gq.$$

Por lo tanto, las curvas maximales tienen el mayor número posible de puntos racionales. Uno de los ejemplos más importantes de curvas maximales sobre $\mathbb{F}_{q^n}$, con $n = 2$, son las curvas hermitianas, que como hemos visto anteriormente, vienen dadas por la ecuación afín

$$\mathscr{H} \equiv y^{q+1} = x^q + x.$$

Ejemplo 6.1. Sea $\mathscr{H}$ una curva hermitiana sobre un cuerpo $\mathbb{F}_{q^2}$. Como hemos visto, su género viene dado por $g(\mathscr{H}) = \frac{1}{2}q(q-1)$ y $\mathscr{H}$ es una curva plana no singular con grado d, donde tenemos que $d = q + 1$. En [20] Ejemplo 6.3.6 tenemos la demostración de que las curvas hermitianas son maximales sobre $\mathbb{F}_{q^2}$ y, como veremos más adelante, el número de puntos racionales de una curva maximal en un cuerpo $\mathbb{F}_{q^2}$ viene dado por

$$\#\mathscr{H}\left(\mathbb{F}_{q^2}\right) = 1 + q^2 + 2q\,\tfrac{q(q-1)}{2} = 1 + q^3.$$

En el artículo [20] se prueba que la única curva maximal para el género dado es la curva hermitiana. Por otro lado, en [6] se prueba que si una curva es maximal, entonces es isomorfa a una curva definida por una ecuación de la forma $Y^{q+1} = X + X^m$, donde $m \leq q$, cuando se cumplen ciertas condiciones. En nuestro caso no siempre se cumplen estas condiciones, como por ejemplo en la primera curva obtenida en el Ejemplo 6.2, $y^9 = x^4 + x^2 + x$ sobre el cuerpo $\mathbb{F}_{64}$, donde utilizando el código fuente del Anexo 2, comprobamos que el número de puntos racionales para $m \leq q$ no coincide con el número de puntos racionales de la curva obtenida, por lo que no puede haber isomorfismo.

En el artículo estudiado [7], On Certain Subcovers of the Hermitian Curve, de los autores Arnaldo García, Motoko Q. Kawatika y Shinji Miura, se da un método basado en cubiertas de curvas para encontrar curvas maximales.

En el capítulo 5 hemos visto que las cubiertas de curvas son extensiones de cuerpos, por lo que el método trata de encontrar un cierto polinomio que factorice la curva hermitiana, es decir, encontrar el polinomio que da la extensión del cuerpo adecuada.

Por lo tanto, empezamos definiendo el concepto de divisibilidad por la izquierda de un polinomio.

Definición 6.2. Sea K un cuerpo y $B(X) \in K[X]$. Decimos que $B(X)$ es **divisible por la izquierda** si existen dos polinomios $f(X), g(X) \in K[X]$ tal que

$$B(X) = f(h(X)).$$

Sean $G(Y) \in K[Y]$ y $G(X) \in K[X]$ polinomios tales que el polinomio $G(Y) - G(X) \in K[X,Y]$ es absolutamente irreducible. Sea una curva hermitiana $\mathscr{H}$ sobre un cuerpo K dada por la ecuación afín

$$G(Y) = G(X).$$

La siguiente proposición se puede encontrar en la Proposición 1 del artículo estudiado [7].

Proposición 6.1. Sea una curva hermitiana $\mathscr{H}$ definida por el polinomio $y^{q+1} = x^q + x$. Sean G y B dos polinomios divisibles por la izquierda por los polinomios g y f, respectivamente. Entonces, la curva $\mathscr{H}$ es una cubierta de la curva dada por la ecuación

$$g(y) = f(x).$$

Para ver que $\mathscr{H}$ es una cubierta de la curva $\mathscr{C}$, tomamos la aplicación

$$\mathscr{H} \to \mathscr{C}$$

$$(\alpha, \beta) \mapsto (h_1(\alpha), h_2(\beta))$$

donde h_1 y h_2 son dos polinomios que dividen por la izquierda a f y a g, respectivamente.

Definición 6.3. Sea K un cuerpo perfecto de característica $p > 0$ (como por ejemplo $K = \mathbb{F}_\ell$). Se denomina **polinomio aditivo** a un polinomio de la forma

$$A(X) = \sum_{i=0}^{n} a_i X^{p^i} \in K[X],$$

el cual es separable si y sólo si $a_0 \neq 0$.

La demostración del siguiente Teorema es similar a la demostración del Algoritmo de la División de Euclides. El Teorema y el Corolario posterior están extraídos del artículo estudiado [7], Teorema 3:

Teorema 6.1. Algoritmo de la División. Sea K un cuerpo y sean $B(X)$ y $A(X)$ dos polinomios aditivos en $K[X]$ con $A \neq 0$. Entonces existen dos polinomios aditivos $Q(X), R(X) \in K[X]$ tal que

$$B(X) = Q(A(X)) + R(X) \text{ con } degR < degA.$$

Además, los polinomios $Q(X)$ y $R(X)$ son únicos.

Usamos las definiciones y la proposición anterior para construir curvas maximales sobre $\mathbb{F}_{q^n}$, con $n = 2$ tomando $\mathscr{H}$ como curva hermitiana. Estas curvas $\mathscr{H}$ son especialmente interesantes si $degB$ y $degG$ son relativamente primos, ya que de esta forma el polinomio $G(Y) - G(X)$ es absolutamente irreducible.

Tomemos entonces $G(Y) = Y^{q+1}$y $B(X) = X^q + X$. Sean $\mathscr{A}$ y $\mathscr{F}$ subgrupos aditivos de $\mathbb{F}_{q^2}$ y denotamos por

$$A(X) = \prod_{a \in \mathscr{A}} (X - a), B(X) = \prod_{a \in \mathscr{F}} (X - a).$$

Corolario 6.1. El Algoritmo de la División implica que $\mathscr{A} \subseteq \mathscr{F} \Leftrightarrow B(X) = Q(A(X))$.

Aplicando lo anterior para los subgrupos aditivos $\mathscr{A}$ del grupo $\mathscr{F} = \{a \in \mathbb{F}_{q^2} : a^q + a = 0\}$, obtenemos una curva maximal $\mathscr{C}$ sobre $\mathbb{F}_{q^2}$ con ecuación afín

$$y^{q+1} = Q(X)$$

donde $Q(A(X)) = X^q + X$, y la curva $\mathscr{H}$ definida anteriormente es hermitiana sobre $\mathbb{F}_{q^2}$.

La siguiente proposición y su demostración pueden consultarse en el artículo analizado [7], Proposición 4:

Proposición 6.2. Sea K un cuerpo y sean $\mathscr{A} \subseteq \mathscr{F}$ dos subgrupos aditivos de $\overline{K}$ tal que el grupo $\mathscr{F}$ está contenido en K. Sea $G(Y) \in K[Y]$ un polinomio tal que $p \nmid degG$ y sea $G(X) \in K[X]$ tal que se cumple el Corolario anterior. Entonces la curva algebraica $\mathscr{H}$ sobre K definida por

$$G(Y) = G(X)$$

es una cubierta de Galois de la curva algebraica $\mathscr{C}$ definida por

$$G(Y) = Q(X)$$

con un grupo de Galois isomorfo a $\mathscr{A}$.

Como el polinomio $Q(X)$es un polinomio separable aditivo en $\mathbb{F}_{q^2}$, el género de la curva $\mathscr{C}$ es

$$g(\mathscr{C}) = \frac{q(degQ-1)}{2}.$$

Vamos a construir curvas maximales sobre diferentes grupos utilizando este método, completando los detalles del artículo [7].

Utilizaremos las estructuras algebraicas estudiadas en los capítulos 2 y 3 sobre curvas, y el capítulo 4 para la extensión de los cuerpos finitos. Finalmente, utilizaremos el capítulo 5 para obtener las correspondientes subcubiertas de las curvas hermitianas.

Ejemplo 6.2. En el primer ejemplo del artículo se utiliza como polinomio de extensión $a^6+a^4+a^3+a+1=0$ para obtener el cuerpo $\mathbb{F}_{64}$, con a un elemento primitivo de $\mathbb{F}_{64}$.

La primera curva que se obtiene es utilizando el subgrupo aditivo $\mathscr{A}=\{0,1\}\subset\mathscr{F}=\left\{b\in\mathbb{F}_{64}:b^8+b=0\right\}$. Entonces,

$$A(X)=\prod_{a\in\mathscr{A}}(X-a)=X(X-1)=X^2+X.$$

En este caso es $\mathscr{C}$ viene definida por el polinomio $y^9=x^4+x^2+x$, por lo que $Q(X)=x^4+x^2+x$. Efectivamente, componiendo tenemos que $Q(A(X))=\left(X^2+X\right)^4+\left(X^2+X\right)^2+\left(X^2+X\right)=X^8+X$. Esta curva tiene género $g(\mathscr{C})=\frac{q(degQ-1)}{2}=12$, por lo que el número de puntos racionales es $\#\mathscr{C}=1+q^2+2qg(\mathscr{C})=257$ (ver tabla 7.8).

La segunda curva que se obtiene es utilizando como subgrupo aditivo

$$\mathscr{A}=\left\{0,1,a^9,a^{27}\right\}\subset\mathscr{F}=\left\{b\in\mathbb{F}_{64}:b^8+b=0\right\}.$$

Entonces, $A(X)=\prod_{a\in\mathscr{A}}(X-a)=X(X-1)\left(X-a^9\right)\left(X-a^{27}\right)=X^4+a^{25}X^2+a^{36}X$.

La curva que se obtiene en el ejemplo está definida por el polinomio $y^9=x^2+a^{27}x$, por lo que en este caso, $Q(X)=X^2+a^{27}X$. Efectivamente, componiendo nos queda:

$$Q(A(X))=X^8+X.$$

En este caso tenemos que el género $g(\mathscr{C})=\frac{q(degQ-1)}{2}=4$, por lo que el número de puntos racionales es $\#\mathscr{C}=1+q^2+2qg(\mathscr{C})=129$ (ver tabla 7.9).

Veamos otros ejemplos basados en el mismo método.

Ejemplo 6.3. Sea el cuerpo $\mathbb{F}_{16}$ obtenido como extensión del cuerpo $\mathbb{F}_4$, usando el polinomio $Y^4=Y+1$ y sea a una raíz. Entonces, el grupo $\mathbb{F}_{16}$ está formado por:

$$\mathbb{F}_{16}=\{0,1,a,a+1,a^2,a^2+1,a^2+a,a^2+a+1,a^3,a^3+1,$$

$$a^3+a,a^3+a+1,a^3+a^2,a^3+a^2+1,a^3+a^2+a,a^3+a^2+a+a\}.$$

Podemos representar el cuerpo mediante las diferentes potencias de a:

$0,1,a=2,a^2=4,a^3=8,$
$a=3=a+1,a^5=a^2+a=6,$
$a^6=a^3+a^2=12,a^7=a^3+a+1=11,$
$a^8=a^2+1=5,a^9=a^3+a=10,$

$a^{10} = a^2 + a + 1 = 7, a^{11} = a^3 + a^2 + a = 14,$
$a^{12} = a^3 + a^2 + a + a = 15,$
$a^{13} = 13 = a^3 + a^2 + 1,\ a^{14} = 9 = a^3 + 1, a^{15} = 1.$

Hay que tener en cuenta que si utilizamos otro polinomio primitivo distinto para construir el cuerpo, obtendremos un cuerpo que es isomorfo al que hemos calculado, pero no es el mismo cuerpo, por lo que los valores numéricos y la representación del cuerpo en potencias de la raíz primitiva serán distintos.

Sea el grupo $\mathscr{F} = \{b \in \mathbb{F}_{16} : b^4 + b = 0\} = \{0, 1, a^5, a^{10}\}$. Para este caso, tenemos que
$A(X) = F(X) = \prod_{a \in \mathscr{A}} (X - a) = X(X-1)\left(X - a^5\right)\left(X - a^{10}\right) =$
$= X^4 - \left(a^{10} + a^5 + 1\right)X^3 + \left(a^5 a^{10} + a^{10} + a^5\right)X^2 - a^5 a^{10} X = X^4 - X = X^4 + X.$

Como era de esperar utilizando el grupo $\mathscr{F}$, el polinomio $Q(X) = X$, es decir, el polinomio identidad.

Elijamos ahora un subgrupo $\mathscr{A} \subset \mathscr{F}$, $\mathscr{A} = \{0, 1\}$. En este caso tenemos que

$$A(X) = \prod_{a \in \mathscr{A}} (X - a) = X(X-1) = X^2 + X.$$

Tenemos que buscar un polinomio $Q(X) \in \mathbb{F}_{16}$ tal que $Q(A(X)) = X^4 + X$.

Claramente el polinomio $Q(X)$ tiene grado 2, por lo que podemos escribir el polinomio en la forma $Q(X) = X^2 + c_1 X + c_2$, con $c_1, c_2 \in \{0, 1\}$. Entonces,

$$Q(A(X)) = \left(X^2 + X\right)^2 + c_1\left(X^2 + X\right) + c_2 = X^4 + (1 + c_1)X^2 + c_1 X + c_2.$$

Por lo tanto, tomando $c_1 = 1$ y $c_2 = 0$, tenemos que $Q(A(X)) = X^4 + X$, por lo que $Q(X) = X^2 + X$. La curva maximal es entonces la curva $\mathscr{C}$ está definida por el polinomio

$$y^5 = x^2 + x.$$

El género de la curva es $g(\mathscr{C}) = \frac{q(degQ-1)}{2} = 2$ y el número de puntos racionales en $\mathbb{F}_{16}$ es: $\#\mathscr{C} = 1 + q^2 + 2qg(\mathscr{C}) = 33$ (ver tabla 7.7).

Ejemplo 6.4. Extendemos el cuerpo $\mathbb{F}_3$ a $\mathbb{F}_9$ utilizando el polinomio primitivo $Y^2 = Y + 1$. Si a es una raíz, tenemos que el cuerpo $\mathbb{F}_9$ viene dado por:

$$\mathbb{F}_9 = \{0, 1, 2, a, a+1, a+2, 2a, 2a+1, 2a+2\}.$$

Como tenemos que $a^2 = a + 1$, podemos representar el cuerpo como

$$\mathbb{F}_9 = \{0,1,2,a,a^2,a^3,a^4,a^5,a^6,a^7,a^8=1\}.$$

Escogemos ahora el grupo aditivo $\mathscr{F} = \{b \in \mathbb{F}_9 : b^3+b=0\} = \{0,1,a^2,a^6\}$.
Construimos el polinomio

$$A(X) = \prod_{a\in\mathscr{F}} (X-a) = X\left(X-a^2\right)\left(X-a^6\right) = X^3 + \left(a^2+a^6\right)X^2 + a^8X = X^3+X.$$

Por lo tanto $Q(X)$ es el polinomio identidad $Q(X)=X$.

Ejemplo 6.5. Extendemos el cuerpo $\mathbb{F}_9$ al cuerpo $\mathbb{F}_{81}$ utilizando el polinomio $Y^4 = 2Y+1$ que es primitivo. En este caso, obtenemos $\mathbb{F}_{81} = \{0,1,2,a,a^2,\cdots,a^{79},a^{80}=1\}$.

El grupo aditivo es $\mathscr{F} = \{b \in \mathbb{F}_{81} : b^9+b=0\} = \{0,1,a^5,a^{15},a^{25},a^{35},a^{45},a^{55},a^{65},a^{75}\}$.

Escogemos un subgrupo aditivo $\mathscr{A} = \{0,a^{35},a^{75}\}$. Entonces

$$A(X) = \prod_{a\in\mathscr{F}} (X-a) = X\left(X-a^{35}\right)\left(X-a^{75}\right) = X^3 + a^{30}X.$$

El polinomio $Q(X)$ debe ser un polinomio de grado 3 por lo que sea
$Q(X) = c_1X^3 + c_2X^2 + c_3X + c_4$, con $c_1,c_2,c_3,c_4 \in \{0,1,2\}$. Componiendo ambos polinomios tenemos que:

$$Q(A(X)) = c_1\left(X^3+a^{30}X\right)^3 + c_2\left(X^3+a^{30}X\right)^2 + \left(X^3+a^{30}X\right) + c_4 =$$

$$= c_1X^9 + c_2X^6 + c_2a^{70}X^4 + \left(c_1a^{10}+c_3\right)X^3 + c_2a^{60}X^2 + c_3a^{30}X + c_4.$$

El polinomio anterior debe ser igual a X^9+X, por lo que directamente tenemos que $c_2 = c_4 = 0$, quedando

$$Q(A(X)) = c_1X^9 + \left(c_1a^{10}+c_3\right)X^3 + c_3a^{30}X.$$

Entonces, debe ser $c_3a^{30}=1$, por lo que $c_3 = a^{50}$ y $c_1 = 1$.

Efectivamente, comprobamos que el término al cubo se anula, ya que $\left(c_1a^{10}+c_3\right) = \left(a^{10}+a^{50}\right) = 0$. Por lo tanto, la curva resultante $\mathscr{C}$ está definida por el polinomio $y^{10} = x^3 + a^{50}x$, con $g(\mathscr{C}) = \frac{q(degQ-1)}{2} = 9$.

El número de sus puntos racionales es $\#\mathscr{C} = 1+q^2+2qg(\mathscr{C}) = 244$ (ver tabla 7.10).

6.1. Implementación

La aplicación, desarrollada en el lenguaje de programación JAVA, se compone de tres clases:

1. **Clase Polinomio**: esta clase almacena en variables miembro los coeficientes del polinomio y su grado. Implementa las operaciones de suma, resta y multiplicación de polinomios, reducción de un polinomio en el caso de que haya algún coeficiente nulo y la evaluación de un polinomio en un punto dado. Además, ofrece métodos para obtener los coeficientes, el grado y el polinomio módulo el polinomio primitivo utilizado para la construcción del cuerpo (polinomio de corte). Finalmente, la clase sobrescribe el método para representar el polinomio como una cadena de texto, muy útil para visualizar los resultados en la consola.

2. **Clase PolinomioStruct**: esta clase almacena objetos de la clase Polinomio, su valor numérico y el valor de la potencia dado un elemento primitivo, además de todos los métodos para establecer y obtener estos valores. Estos objetos tienen sentido y son creados una vez que tenemos el polinomio primitivo y estamos construyendo el cuerpo ya que, evidentemente, el valor numérico y la potencia dependerán del polinomio primitivo usado para construir el cuerpo.

3. **Clase TablaPolinomios**: esta clase almacena un mapa de objetos de la clase PolinomioStruct, indexados por el valor numérico del polinomio. Un objeto de esta clase se construye mediante el número de elementos que tendrá el cuerpo y la base para la cuál se calcularan los módulos de los coeficientes. Una vez construido el objeto, se invocará al método Inicializar, proporcionando como parámetros el polinomio primitivo utilizado para construir el cuerpo. Por ejemplo, para el caso de $\mathbb{F}_{64}$, el polinomio primitivo que se utiliza para construir el cuerpo es: $a^6 + a^4 + a^3 + a + 1 = 0$. y la base es 2 ($64 = 2^6$). Esta clase proporciona los métodos para calcular las tablas de suma y multiplicación del cuerpo construido, que servirán posteriormente para calcular los puntos racionales de una curva.

Rutina principal: el método main, situado en la clase Polinomio, obtiene los puntos racionales de las curvas analizadas en la sección 6. Para ello hay que seguir los siguientes pasos en el siguiente orden:

1. Establecer el **número de elementos** que tendrá el cuerpo y la **base** (como espacio vectorial) para calcular el módulo de los coeficientes.

2. Construir el objeto TablaPolinomios con los dos parámetros anteriores.

3. Construir el polinomio de corte.

4. Inicializar el objeto TablaPolinomios anteriormente construido pasando como parámetro el polinomio de corte.

5. Obtener la tabla de suma y multiplicación del cuerpo construido.

A partir de este momento, al tener las tablas de multiplicación y suma ya podemos utilizarlas para evaluar los puntos del cuerpo en la curva que queramos, y así obtener los puntos racionales.

El programa puede ser utilizado para la construcción de cualquier cuerpo, con cualquier número de elementos y polinomio de corte, teniendo en cuenta el coste en tiempo del cálculo de la tabla multiplicación. El programa se ha probado con el cuerpo $\mathbb{F}_{16384}$ (2^{14}), utilizando como polinomio de corte el polinomio primitivo $x^{14}+x^5+x^3+x+1=0$, con un coste de 7,2 horas de computación.

Se pueden hacer mejoras en la aplicación, como por ejemplo implementar un algoritmo más rápido para calcular la tabla multiplicar en un cuerpo con muchos elementos. Aprovechando su diseño modular, se puede dotar a la aplicación de un interfaz de usuario gráfico donde el usuario tendría que introducir el número de elementos y el polinomio de corte en un formato preestablecido.

Pasamos a estudiar el tiempo de CPU de ejecución del programa para la generación de las tablas de suma y multiplicación de los diferentes cuerpos finitos. Para los primeros cuerpos, con un número pequeño de elementos, la ejecución del programa es casi inmediata. A medida que vamos incrementando el cuadrado de los elementos del cuerpo, el tiempo de ejecución va aumentando, como podemos ver en la siguiente lista:

1. Cuerpo $\mathbb{F}_{16}$: 17 milisegundos.
2. Cuerpo $\mathbb{F}_{64}$: 40 milisegundos.
3. Cuerpo $\mathbb{F}_{81}$: 42 milisegundos.
4. Cuerpo $\mathbb{F}_{256}$: 118 milisegundos.
5. Cuerpo $\mathbb{F}_{1024}$: 3,5 segundos.
6. Cuerpo $\mathbb{F}_{2048}$: 25,3 segundos.
7. Cuerpo $\mathbb{F}_{4096}$: 4,7 minutos.
8. Cuerpo $\mathbb{F}_{8192}$: 35,5 minutos.
9. Cuerpo $\mathbb{F}_{16384}$: 7,2 horas.

El código fuente del programa se puede encontrar en el Anexo 2.

Bibliografía

[1] J. Arregui Fernández.
Topología.
U.N.E.D Ediciones, 1988, Madrid.

[2] E. Bujalance, J.M. Etayo, and J.M. Gamboa.
Teoría elemental de grupos.
U.N.E.D Ediciones, 2002, Madrid.

[3] I. Cortazar.
Trabajo Fin de Máster: Superficies de Riemann compactas y Teorema de Riemann Roch.
U.N.E.D, 2012, Madrid.

[4] D.Cox, D. O´Shea, and J. Little.
Ideals, Varieties and Algorithms.
Springer-Verlag, 1997, Heidelberg.

[5] W. Fulton.
Algebraic Curves. An Introduction to Algebraic Geometry.
W. A. Benjamin, Inc., 2018, New York.

[6] A. García, R. Fuhrmann, and F. Torres.
On Maximal Curves.
Journal of Number Theory (1997) 67, 29-51.

[7] A. García, M. Q. Kawakita, and S. Miura.
On Certain Subcovers of the Hermitian Curve.
Communications in Algebra (2016) 34:3, 973-982.

[8] B. Garrett and M.L.Saunders.
Álgebra moderna.
Manuales Vicens-Vives, 1974, Barcelona.

[9] T.W. Hungerford.
Algebra.
Graduate Texts in Mathematics. Springer-Verlag, 1974, New York.

[10] G. A. Jones and D. Singerman.
Complex Functions: An Algebraic and Geometric Viewpoint.
Cambridge University Press, 1974, New York.

[11] F. Kirwan.
Complex Algebraic Curves.
Cambridge Univ. Press, 1992, Cambridge.

[12] E. Kunz.
Introduction to Commutative Algebra and Algebraic Geometry.
Birkh auser, 1985, Boston.

[13] I.G Macdonald and M. F. Atiyah.
Introduction to Commutative Algebra.
CRR Press Addison-Wesley Series in Mathematics, 1994, Massachusetts.

[14] V. Magdaleno Jiménez.
Trabajo Fin de Máster: sobre Códigos Algebraico-Geométricos Basados en Curvas C(a,b).
U.N.E.D., 2016, Madrid.

[15] B. R. McDonald.
Finite rings with identity (Pure and Applied Mathematics).
Marcel Dekker Inc., 1974, New York.

[16] Jesús Miranda García.
El anillo de polinomios sobre un cuerpo.
Universidad de Granada, 2006, Granada.
https://www.ugr.es/~jesusgm/Curso%202005-2006/Matematica%20Discreta/Polinomios.pdf.

[17] C.J. Moreno.
Algebraic Curves Over Finite Fields.
Cambridge Univ. Press, 1991, New York.

[18] J. M. Gamboa Mutuberría and J.M Ruiz Sancho.
Anillos y cuerpos conmutativos.
U.N.E.D Ediciones, 2002, Madrid.

[19] C. Rovi.
Master Thesis Algebraic Curves over Finite Fields.
U.N.E.D, 2010, Linkoping Universitet.

[20] H. G. Ruck and H. Stichtenoth.

A characterization of Hermitian function fields over finite fields.
J. Reine Angew. Math. (1994) 457, 185-188.

[21] H. Stichtenoth.
Algebraic function fields and codes.
Graduate Texts in Mathematics. Springer-Verlag, 2009, Berlin.

[22] F. Torres, G. Korchmáros, and J.W.P Hirschfeld.
Algebraic curves over a finite field.
Princeton Univ. Press, 2008, New Jersey.

[23] A. Uteshev and P. Bikker.
On the Bezout Construction of the Resultant.
J. Symbolic Computation (1999) 28, 45-88.

CAPÍTULO 7

ANEXO 1

7.1. Construcción de cuerpos finitos

Esta sección está basada en [16].
Sea p un número primo. Sabemos que $\mathbb{Z}/\mathbb{Z}_p$ es un cuerpo finito que tiene p elementos. De ahora en adelante lo denotaremos por $\mathbb{F}_p$. Sea ahora cualquier cuerpo finito F.

Denotando la suma de n copias del elemento 1 como $n \cdot 1 \in F$, al ser F finito, los elementos $n \cdot 1 \in F$ no pueden ser todos distintos, por lo que existe un $m < n$ tal que $n \cdot 1 = m \cdot 1$, por lo que $(m-n) \cdot 1 = 0$.

Si denotamos por a el número más pequeño tal que $a \cdot 1 = 0$, al ser F un cuerpo, debe ser $a = p$, es decir a debe ser primo. Por minimalidad, se sigue que p es el único primo que cumple esta propiedad y tenemos que $n \cdot 1 = 0$ si y sólo si n es múltiplo de p.
Además, los elementos $i \cdot 1$, $i = 0, 1, \cdots, p-1$ forman un subcuerpo de F, que es isomorfo a $\mathbb{F}_p$. Por lo tanto, todo cuerpo finito F puede verse como una extensión de un cuerpo $\mathbb{F}_p$.

Por definición, F puede verse como un campo vectorial sobre $\mathbb{F}_p$, por lo que el número de elementos de F es p^n para algún n, de hecho $n = \left[F : \mathbb{F}_p\right]$.

Veamos cómo se puede demostrar la existencia y unicidad de cuerpos finitos usando polinomios.

Sea p un número primo y $q = p^n$, con $n \in \mathbb{N}$. El cuerpo de descomposición del polinomio $f(x) = x^q - x \in \mathbb{F}_p[x]$ es un cuerpo finito con q elementos. La unicidad de F_q se sigue de la unicidad

del cuerpo de descomposición de un polinomio y los elementos de F_q son las raíces de f, todas ellas distintas.
Ahora, para construir el cuerpo usamos polinomios irreducibles. Sea $f(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado n y suponemos que $f(x)$ es mónico, es decir, el coeficiente de x^n es 1, por lo que tenemos que:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Demostremos que el anillo cociente de el anillo de polinomios sobre el ideal maximal generado por $f(x)$, $F = \mathbb{F}_p[x]/(f(x))$, es un cuerpo de p^n elementos.

Sea X la imagen de x modulo $(f(x))$, el ideal generado por $f(x)$. Recordemos que $(f(x))$ no es más que el conjunto de polinomios en $\mathbb{F}_p[x]$ que son múltiplos de $f(x)$.
Tenemos que F es un espacio vectorial de dimensión n sobre $\mathbb{F}_p$, por lo que $|F| = p^n$. Los elementos de F se pueden expresar de manera única en la forma $v = \sum_{i=0}^{n-1} c_i X^i$, es decir, F es el conjunto de polinomios en $\mathbb{F}_p[x]$ de grado menor que n.

Por otro lado, las X^i, $i = 0, 1, \cdots, n-1$ son linealmente independientes, ya que de lo contrario $f(x)$ dividiría a un polinomio no nulo de grado menor que n, lo cual es imposible. Por lo tanto, todo elemento de F puede escribirse de forma única como polinomio de grado menor que n con coeficientes en $\mathbb{F}_p$.
Supongamos ahora que tenemos dos polinomios $h(X)$ y $g(X)$ tales que $g(X)h(X) = 0$. Esto quiere decir que $f(x)$ divide a $g(x)h(x)$, y como $f(x)$ es irreducible, entonces $f(x)$ divide a $g(x)$o a $h(x)$, por lo que tenemos que o bien $g(x) = 0$ o bien $h(x) = 0$.

Por lo tanto, esto demuestra que F es un dominio integral, es decir, que no tiene divisores de cero. Solo queda demostrar que todo elemento de F tiene un inverso multiplicativo. Sea $g(x)$ un polinomio no nulo de grado menor que n. Como $f(x)$ es irreducible, debe ser primo relativo a $g(x)$. Usando ahora el algoritmo de Euclides, encontramos polinomios $h(x)$ y $l(x)$ tales que

$$1 = g(x)h(x) + f(x)l(x).$$

Si ahora calculamos la expresión $mod(f(x))$ de la expresión anterior, tenemos que
$1 = g(X)h(X)$, por lo que hemos encontrado el inverso multiplicativo de $g(X) \in F$.
Denotamos ahora por $\mathscr{F}$ a la cerradura algebraica de $\mathbb{F}_p$, que suponemos que siempre existe de manera única. Esto quiere decir dos cosas:

- Todo elemento $a \in \mathscr{F}$ es algebraico sobre $\mathbb{F}_p$, es decir, satisface una ecuación polinomial con coeficientes en $\mathbb{F}_p$.

- $\mathscr{F}$ es algebraicamente cerrado, es decir, todo polinomio con coeficientes en $\mathscr{F}$ se descompone como producto de factores lineales sobre el mismo cuerpo.

Consideremos ahora el polinomio $X^{p^n} - X$ y supongamos la existencia de un cuerpo de p^n elementos. Como es un cuerpo finito, debe ser una extensión algebraica sobre $\mathbb{F}_p$, por lo que se puede considerar como un subcuerpo de $\mathscr{F}$.

Como el grupo multiplicativo de este cuerpo tiene $p^n - 1$ elementos, todo elemento no nulo v satisface $v^{p^n-1} = 1$, por lo que todo elemento de dicho cuerpo es la raíz de dicho polinomio. De esta manera, vemos que un cuerpo con p^n elementos queda determinado de manera única, si es que existe, como cierto subcuerpo de $\mathscr{F}$.

Por otro lado, el polinomio $X^{p^n} - X$ es separable, es decir, sus p^n raíces son distintas, por lo que al estar trabajando con un cuerpo, solo tenemos que demostrar que sumas, productos e inversos multiplicativos de las raíces, son también raíces. Para ello, usamos el siguiente resultado:

Definición 7.1. Automorfismo de Frobenius Sea $\mathscr{F}$ un cuerpo de característica p. Entonces la aplicación $\sigma(x) = x^p$, es un automorfismo de F en F^p. En el caso de que F sea un cuerpo finito, tenemos que $F^p = F$. El cuerpo fijado por σ es $\mathbb{F}_p$.

Podemos resumir lo dicho en el siguiente resultado:

Para todo primo p y todo número natural n existe un cuerpo con p^n elementos. Cada cerradura algebraica $\mathscr{F}$ de $\mathbb{F}_p$contiene exactamente un subcuerpo de p^n, consistiendo de las raíces del polinomio $X^{p^n} - X$. Denotaremos este cuerpo como $\mathbb{F}_{p^n}$.

Ejemplo 7.1. Para determinar si un polinomio $p(x) \in K[x]$ es o no irreducible, existen algoritmos de factorización, como el algoritmo de Berlekamp. Sin embargo, para polinomios de grado 2 y 3 podemos utilizar el siguiente resultado:

Sea $p(x) \in K[x]$, con el grado de p igual a 2 ó a 3. Entonces $p(x)$ es irreducible si, y sólo si, $p(x)$ no tiene raíces.

- El polinomio $p(x) = x^3 + 2x + 2 \in \mathbb{Z}_3[x]$es irreducible. Al ser de grado 3 basta ver que no tiene raíces. Evaluamos en los tres elementos de $\mathbb{Z}_3$ y vemos que $p(0) = 2$,$p(1) = 2$ y $p(2) = 2$.
- El polinomio de grado 4, $p(x) = x^4 + x^3 + x + 2 \in \mathbb{Z}_3[x]$ no tiene raíces ($p(0) = 2$, $p(1) = 2$, y $p(2) = 1$). Sin embargo no es irreducible, pues$p(x) = \left(x^2 + 1\right)\left(x^2 + x + 2\right)$.
- El polinomio $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ es irreducible. Al ser de grado 3 basta ver que no tiene raíces. Evaluamos en los tres elementos de $\mathbb{Z}_2$ y vemos que $p(0) = p(1) = 1$. Usaremos este polinomio en el ejemplo siguiente.

Ejemplo 7.2. Sea $p = 2$ y $n = 3$. Vamos a construir el cuerpo finito de 8 elementos. Como $p = 2$, trabajaremos en el conjunto $\mathbb{Z}_2[x]$ de polinomios, con coeficientes en $\mathbb{Z}_2$. Como $n = 3$, el polinomio irreducible que vamos a emplear para la operación de multiplicación tendrá grado 3.
Tomaremos el polinomio $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Para definir el cuerpo, necesitamos el conjunto y sus dos operaciones.

- El conjunto, en este caso, estará formado por los polinomios de $\mathbb{Z}_2[x]$ de grado menor que 3. Es decir:

$$\mathbb{F}_{p^n} = \mathbb{F}_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

- La operación de suma es la operación habitual de polinomios. Se puede comprobar fácilmente que esta operación es cerrada, conmutativa y asociativa, tiene elemento neutro (el polinomio nulo), y que todos los elementos tienen simétrico (en este caso, como los coeficientes están en $\mathbb{Z}_2$, cada polinomio es simétrico a si mismo). Por lo tanto, $\mathbb{F}_8$ con la suma, es un grupo conmutativo.

- Para la segunda operación no podemos utilizar el producto habitual de polinomios, porque no es una operación cerrada. De forma parecida a como se hace en la aritmética modular habitual, tomaremos el producto módulo el polinomio $f(x)$ escogido anteriormente. Por lo tanto, el producto de dos polinomios será el resto de dividir el polinomio entre el polinomio $f(x)$. En este caso vemos que:

  $(x^2+1)(x^2+x) = x^4+x^3+x^2+x$. La división euclídea de este producto entre $f(x)$ es $x^4 + x^3+x^2+x = (x^3+x^2+1)x+x^2$. El resto es x^2, por lo que $(x^2+1)(x^2+x) = x^2$.

  El resto de los productos que podemos hacer tiene grado menor que el grado de $f(x)$, que es 3, por lo que es un polinomio en $\mathbb{F}_8$. Además, es asociativo, conmutativo y tiene elemento neutro, el polinomio 1.

Por lo tanto, tenemos que $\mathbb{F}_8 - \{0\}$, con el producto módulo $f(x)$, tiene estructura de grupo conmutativo.
Comprobemos ahora que todos los elementos del grupo multiplicativo $\mathbb{F}_8 - \{0\}$ tienen inverso:

- El polinomio 1, como siempre ocurre con el elemento neutro de cualquier grupo, es inverso de sí mismo.

- Los polinomios x y x^2+x son inversos el uno del otro, porque $x(x^2+x) = x^3+x^2$, cuyo resto al dividirlo entre $f(x) = x^3+x^2+1$ es 1. Esto podemos verlo también de la siguiente forma: como $x^3+x^2+1 = 0$ porque el resto de dividir este polinomio entre sí mismo es 0, entonces $x^3+x^2 = 1$ (recordemos que en $\mathbb{Z}_2$ $-1 = 1$).

- Los polinomios $x+1$ y x^2 son también inversos el uno del otro, ya que $(x+1)x^2 = x^3+x^2 = 1$.

- Finalmente, los polinomios restantes x^2+1 y x^2+x+1 también son inversos el uno del otro: $(x^2+1)(x^2+x+1) = x^4+x^3+x^2+x+1 = (x^3+x^2+1)x+1 = 1$.

Así pues, el conjunto $\mathbb{F}_8 - \{0\}$, con la operación producto módulo $f(x)$, tiene estructura de grupo conmutativo. Es fácil comprobar que este producto es distributivo respecto de la suma, por lo que $\mathbb{F}_8$ es un cuerpo.

Tal y como hemos construido el cuerpo, hablamos del cuerpo cociente $\mathbb{Z}_2[x]/f(x)$. El hecho de que $f(x)$ sea un polinomio irreducible es determinante para la existencia de los elementos inversos. Si este polinomio no fuera irreducible, hablaríamos del anillo cociente $\mathbb{Z}_2[x]/f(x)$.

Ejemplo 7.3. Sea $p=3$ y $n=2$. Construimos el cuerpo finito de 9 elementos de la misma forma que antes, y tenemos que:

$$\mathbb{F}_{p^n} = \mathbb{F}_9 = \{0,1,2,x,2x,x+1,x+2,2x+1,2x+2\}.$$

Utilizamos el polinomio irreducible $f(x) = x^2+x+2$ para la operación de multiplicación, teniendo en cuenta esta vez que, usando la aritmética modular:

- $x^2 = \left(x^2+x+2\right)+(-x-2) = (-x-2) = 2x+1$.
- $x^3 = xx^2 = x(2x+1) = 2x^2+x = 2(2x+1)+x = 4x+2+x = 5x+2 = 2x+2$.
- $x^4 = xx^3 = x(2x+2) = 2x^2+2x = 2(2x+1)+2x = 4x+2+2x = 6x+2 = 2$.
- $x^5 = xx^4 = 2x$.
- $x^6 = xx^5 = 2x^2 = 2(2x+1) = 4x+2 = x+2$.
- $x^7 = xx^6 = x(x+2) = x^2+2x = (2x+1)+2x = 4x+1 = x+1$.
- $x^8 = xx^7 = x(x+1) = x^2+x = (2x+1)+x = 3x+1 = 1$.

Es decir, podemos representar el cuerpo como:

$$\mathbb{F}_9 = \left\{0,1,2,x,x^2x^3,x^4,x^5,x^6,x^7\right\}.$$

Ejemplo 7.4. Construyamos las tablas para el cuerpo $\mathbb{F}_9$ usando el polinomio irreducible X^2+1 de $\mathbb{F}_3$:

$$\mathbb{F}_9 = \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}.$$

.	1	2	x	$x+1$	x+2	$2x$	$2x+1$	$2x+2$
1	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Cuadro 7.1: Tabla de la multiplicación en $\mathbb{F}_9$

Si hacemos $x = 3$, nos quedan las siguientes tablas para la suma y multiplicación en el cuerpo:

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	8	2	0	1	5	3	4

Cuadro 7.2: Tabla de la suma en $\mathbb{F}_9$ con $x = 3$

.	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	6	8	7	3	5	4
3	3	4	2	5	8	1	4	7
4	4	8	5	6	1	7	2	3
5	5	7	8	1	3	4	6	2
6	6	3	1	7	4	2	8	5
7	7	5	4	2	6	8	3	1
8	8	4	3	7	2	5	1	6

Cuadro 7.3: Tabla de la multiplicación en $\mathbb{F}_9$ con $x = 3$

7.2. Tablas

En esta sección escribimos las tablas de los cuerpos finitos analizados en la sección 6. En ellas podemos ver los polinomios obtenidos, su valor numérico y su representación en potencias de un elemento primitivo a, dependiendo del polinomio primitivo utilizado para generar el cuerpo. Las tablas han sido obtenidas con una aplicación desarrollada en JAVA que describiremos posteriormente.

7.2.1. Tabla de $\mathbb{F}_{16}$

Polinomio primitivo: $a^4 = a + 1$.

Potencias de a	Polinomio	Valor numérico
a^0	1	1
a	x	2
a^2	x^2	4
a^3	x^3	8
a^4	$x+1$	3
a^5	x^2+x	6
a^6	x^3+x^2	12
a^7	x^3+x+1	11
a^8	x^2+1	5
a^9	x^3+x	10
a^{10}	x^2+x+1	7
a^{11}	x^3+x^2+x	14
a^{12}	x^3+x^2+x+1	15
a^{13}	x^3+x^2+1	13
a^{14}	x^3+1	9

Cuadro 7.4: Tabla de $\mathbb{F}_{16}$

7.2.2. Tabla de $\mathbb{F}_{64}$

Polinomio primitivo: $a^6 + a^4 + a^3 + a + 1 = 0$.

Potencias de a	Polinomio	Valor Numérico
a^0	1	1
a	x	2
a^2	x^2	4
a^3	x^3	8
a^4	x^4	16
a^5	x^5	32
a^6	$x^4 + x^3 + x + 1$	27
a^7	$x^5 + x^4 + x^2 + x$	54
a^8	$x^5 + x^4 + x^2 + x + 1$	55
a^9	$x^5 + x^4 + x^2 + 1$	53
a^{10}	$x^5 + x^4 + 1$	49
a^{11}	$x^5 + x^4 + x^3 + 1$	57
a^{12}	$x^5 + x^3 + 1$	41
a^{13}	$x^3 + 1$	9
a^{14}	$x^4 + 1x$	18
a^{15}	$x^5 + x^2$	36
a^{16}	$x^4 + x + 1$	19
a^{17}	$x^5 + x^2 + x$	38
a^{18}	$x^4 + x^2 + x + 1$	23
a^{19}	$x^5 + x^3 + x^2 + x$	46
a^{20}	$x^2 + x + 1$	7
a^{21}	$x^3 + x^2 + x$	14
a^{22}	$x^4 + x^3 + x^2$	28
a^{23}	$x^5 + x^4 + x^3$	56
a^{24}	$x^5 + x^3 + x + 1$	43
a^{25}	$x^3 + x^2 + 1$	13
a^{26}	$x^4 + x^3 + x$	26
a^{27}	$x^5 + x^4 + x^2$	52
a^{28}	$x^5 + x^4 + x + 1$	51
a^{29}	$x^5 + x^4 + x^3 + x^2 + 1$	61
a^{30}	$x^5 + 1$	33
a^{31}	$x^4 + x^3 + 1$	25
a^{32}	$x^5 + x^4 + x$	50
a^{33}	$x^5 + x^4 + x^3 + x^2 + x + 1$	63
a^{34}	$x^5 + x^2 + 1$	37
a^{35}	$x^4 + 1$	17
a^{36}	$x^5 + x$	34
a^{37}	$x^4 + x^3 + x^2 + x + 1$	31

Potencias de a	Polinomio	Valor Numérico
a^{38}	$x^5+x^4+x^3+x^2+x$	62
a^{39}	x^5+x^2+x+1	39
a^{40}	x^4+x^2+1	21
a^{41}	x^5+x^3+x	42
a^{42}	x^3+x^2+x+1	15
a^{43}	$x^4+x^3+x^2+x$	30
a^{44}	$x^5+x^4+x^3+x^2$	60
a^{45}	x^5+x+1	35
a^{46}	$x^4+x^3+x^2+1$	29
a^{47}	$x^5+x^4+x^3+x$	58
a^{48}	$x^5+x^3+x^2+x+1$	47
a^{49}	x^2+1	5
a^{50}	x^3+x	10
a^{51}	x^4+x^2	20
a^{52}	x^5+x^3	40
a^{53}	x^3+x+1	11
a^{54}	x^4+x^2+x	22
a^{55}	$x^5+x^3+x^2$	44
a^{56}	$x+1$	3
a^{57}	x^2+x	6
a^{58}	x^3+x^2	12
a^{59}	x^4+x^3	24
a^{60}	x^5+x^4	48
a^{61}	$x^5+x^4+x^3+x+1$	59
a^{62}	$x^5+x^3+x^2+1$	45

Cuadro 7.5: Tabla de $\mathbb{F}_{64}$

7.2.3. Tabla de $\mathbb{F}_{81}$

Polinomio primitivo: $a^4 = 2a + 1$.

Potencias de a	Polinomio	Valor Numérico
1	1	1
a	x	3
a^2	x^2	9
a^3	x^3	27
a^4	$2x+1$	7
a^5	$2x^2+x$	21
a^6	$2x^3+x^2$	63
a^7	x^3+x+2	32
a^8	x^2+x+1	13
a^9	x^3+x^2+x	39
a^{10}	x^3+x^2+2x+1	43
a^{11}	x^3+2x^2+1	46
a^{12}	$2x^3+1$	55
a^{13}	$2x+2$	8
a^{14}	$2x^2+2x$	24
a^{15}	$2x^3+2x^2$	72
a^{16}	$2x^3+x+2$	59
a^{17}	x^2+2	11
a^{18}	x^3+2x	33
a^{19}	$2x^2+2x+1$	25
a^{20}	$2x^3+2x^2+x$	75
a^{21}	$2x^3+x^2+x+2$	68
a^{22}	x^3+x^2+2	38
a^{23}	x^3+x+1	31
a^{24}	x^2+1	10
a^{25}	x^3+x	30
a^{26}	x^2+2x+1	16
a^{27}	x^3+2x^2+x	48
a^{28}	$2x^3+x^2+2x+1$	70
a^{29}	x^3+2x^2+2x+2	53
a^{30}	$2x^3+2x^2+x+1$	76
a^{31}	$2x^3+x^2+2x+2$	71
a^{32}	x^3+2x^2+2	47
a^{33}	$2x^3+x+1$	58
a^{34}	x^2+2x+2	17
a^{35}	x^3+2x^2+2x	51
a^{36}	$2x^3+2x^2+2x+1$	79
a^{37}	$2x^3+2x^2+2x+2$	80

Potencias de a	Polinomio	Valor Numérico
a^{38}	$2x^3+2x^2+2$	74
a^{39}	$2x^3+2$	56
a^{40}	2	2
a^{41}	$2x$	6
a^{42}	$2x^2$	18
a^{43}	$2x^3$	54
a^{44}	$x+2$	5
a^{45}	x^2+2x	15
a^{46}	x^3+2x^2	45
a^{47}	$2x^3+2x+1$	61
a^{48}	$2x^2+2x+2$	26
a^{49}	$2x^3+2x^2+2x$	78
a^{50}	$2x^3+2x^2+x+2$	77
a^{51}	$2x^3+x^2+2$	65
a^{52}	x^3+2	29
a^{53}	$x+1$	4
a^{54}	x^2+x	12
a^{55}	x^3+x^2	36
a^{56}	x^3+2x+1	34
a^{57}	$2x^2+1$	19
a^{58}	$2x^3+x$	57
a^{59}	x^2+x+2	14
a^{60}	x^3+x^2+2x	42
a^{61}	x^3+2x^2+2x+1	52
a^{62}	$2x^3+2x^2+1$	73
a^{63}	$2x^3+2x+2$	62
a^{64}	$2x^2+2$	20
a^{65}	$2x^3+2x$	60
a^{66}	$2x^2+x+2$	23
a^{67}	$2x^3+x^2+2x$	69
a^{68}	x^3+2x^2+x+2	50
a^{69}	$2x^3+x^2+x+1$	67
a^{70}	x^3+x^2+2x+2	44
a^{71}	x^3+2x^2+x+1	49
a^{72}	$2x^3+x^2+1$	64
a^{73}	x^3+2x+2	35
a^{74}	$2x^2+x+1$	22
a^{75}	$2x^3+x^2+x$	66
a^{76}	x^3+x^2+x+2	41
a^{77}	x^3+x^2+x+1	40
a^{78}	x^3+x^2+1	37
a^{79}	x^3+1	28

Cuadro 7.6: Tabla de $\mathbb{F}_{81}$

7.2.4. Tablas de puntos racionales

Presentamos las tablas de los puntos racionales obtenidos para los cuerpos y curvas maximales obtenidas en la sección 6.

Cuerpo $\mathbb{F}_{16}$ sobre la curva $\mathscr{C}$ definida por el polinomio $y^5 = x^2 + x$.

(0,0)	(2,7)	(3,3)	(4,4)	(4,14)	(5,9)	(6,10)	(7,8)
(1,0)	(2,11)	(3,7)	(4,5)	(5,4)	(5,14)	(6,12)	(7,10)
(2,2)	(2,13)	(3,11)	(4,6)	(5,5)	(6,1)	(6,15)	(7,12)
(2,3)	(3,2)	(3,13)	(4,9)	(5,6)	(6,8)	(7,1)	(7,15)
∞							

Cuadro 7.7: Puntos racionales de la curva definida por el polinomio $y^5 = x^2 + x$

Cuerpo $\mathbb{F}_{64}$ sobre la curva $\mathscr{C}$ definida por el polinomio $y^9 = x^4 + x^2 + x$.

(0,0)	(3,56)	(6,36)	(17,34)	(20,31)	(32,27)	(36,2)	(38,63)	(49,59)	(52,18)
(1,1)	(3,60)	(6,55)	(17,36)	(20,33)	(32,37)	(36,6)	(39,11)	(49,63)	(52,51)
(1,3)	(4,21)	(6,61)	(17,55)	(20,53)	(32,42)	(36,10)	(39,13)	(50,8)	(52,54)
(1,5)	(4,22)	(7,8)	(17,61)	(20,56)	(32,44)	(36,28)	(39,16)	(50,24)	(53,0)
(1,14)	(4,26)	(7,24)	(18,11)	(20,60)	(32,45)	(36,30)	(39,23)	(50,25)	(54,4)
(1,15)	(4,32)	(7,25)	(18,13)	(21,7)	(32,47)	(36,34)	(39,29)	(50,35)	(54,12)
(1,17)	(4,41)	(7,35)	(18,16)	(21,9)	(32,52)	(36,36)	(39,39)	(50,38)	(54,19)
(1,18)	(4,46)	(7,38)	(18,23)	(21,27)	(33,4)	(36,55)	(39,48)	(50,40)	(54,20)
(1,51)	(4,58)	(7,40)	(18,29)	(21,37)	(33,12)	(36,61)	(39,50)	(50,43)	(54,31)
(1,54)	(4,59)	(7,43)	(18,39)	(21,42)	(33,19)	(37,8)	(39,57)	(50,49)	(54,33)
(2,7)	(4,63)	(7,49)	(18,48)	(21,44)	(33,20)	(37,24)	(48,11)	(50,62)	(54,53)
(2,9)	(5,11)	(7,62)	(18,50)	(21,45)	(33,31)	(37,25)	(48,13)	(51,2)	(54,56)
(2,27)	(5,13)	(16,8)	(18,57)	(21,47)	(33,33)	(37,35)	(48,16)	(51,6)	(54,60)
(2,37)	(5,16)	(16,24)	(19,21)	(21,52)	(33,53)	(37,38)	(48,23)	(51,10)	(55,7)
(2,42)	(5,23)	(16,25)	(19,22)	(22,1)	(33,56)	(37,40)	(48,29)	(51,28)	(55,9)
(2,44)	(5,29)	(16,35)	(19,26)	(22,3)	(33,60)	(37,43)	(48,39)	(51,30)	(55,27)
(2,45)	(5,39)	(16,38)	(19,32)	(22,5)	(34,0)	(37,49)	(48,48)	(51,34)	(55,37)
(2,47)	(5,48)	(16,40)	(19,41)	(22,14)	(35,1)	(37,62)	(48,50)	(51,36)	(55,42)
(2,52)	(5,50)	(16,43)	(19,46)	(22,15)	(35,3)	(38,21)	(48,57)	(51,55)	(55,44)
(3,4)	(5,57)	(16,49)	(19,58)	(22,17)	(35,5)	(38,22)	(49,21)	(51,61)	(55,45)
(3,12)	(6,2)	(16,62)	(19,59)	(22,18)	(35,14)	(38,26)	(49,22)	(52,1)	(55,47)
(3,19)	(6,6)	(17,2)	(19,63)	(22,51)	(35,15)	(38,32)	(49,26)	(52,3)	(55,52)
(3,20)	(6,10)	(17,6)	(20,4)	(22,54)	(35,17)	(38,41)	(49,32)	(52,5)	∞
(3,31)	(6,28)	(17,10)	(20,12)	(23,0)	(35,18)	(38,46)	(49,41)	(52,14)	
(3,33)	(6,30)	(17,28)	(20,19)	(32,7)	(35,51)	(38,58)	(49,46)	(52,15)	
(3,53)	(6,34)	(17,30)	(20,20)	(32,9)	(35,54)	(38,59)	(49,58)	(52,17)	

Cuadro 7.8: Puntos racionales de la curva definida por el polinomio $y^9 = x^4 + x^2 + x$

Cuerpo $\mathbb{F}_{64}$ sobre la curva $\mathscr{C}$ definida por el polinomio $y^9 = x^2 + a^{27}x$.

(0,0)	(12,53)	(22,38)	(26,26)	(34,8)	(35,51)	(47,44)	(56,19)
(1,2)	(12,56)	(22,40)	(26,32)	(34,24)	(35,54)	(47,45)	(56,20)
(1,6)	(12,60)	(22,43)	(26,41)	(34,25)	(46,21)	(47,47)	(56,31)
(1,10)	(13,11)	(22,49)	(26,46)	(34,35)	(46,22)	(47,52)	(56,33)
(1,28)	(13,13)	(22,62)	(26,58)	(34,38)	(46,26)	(52,0)	(56,53)
(1,30)	(13,16)	(23,1)	(26,59)	(34,40)	(46,32)	(53,2)	(56,56)
(1,34)	(13,23)	(23,3)	(26,63)	(34,43)	(46,41)	(53,6)	(56,60)
(1,36)	(13,29)	(23,5)	(27,7)	(34,49)	(46,46)	(53,10)	(57,11)
(1,55)	(13,39)	(23,14)	(27,9)	(34,62)	(46,58)	(53,28)	(57,13)
(1,61)	(13,48)	(23,15)	(27,27)	(35,1)	(46,59)	(53,30)	(57,16)
(12,4)	(13,50)	(23,17)	(27,37)	(35,3)	(46,63)	(53,34)	(57,23)
(12,12)	(13,57)	(23,18)	(27,42)	(35,5)	(47,7)	(53,36)	(57,29)
(12,19)	(22,8)	(23,51)	(27,44)	(35,14)	(47,9)	(53,55)	(57,39)
(12,20)	(22,24)	(23,54)	(27,45)	(35,15)	(47,27)	(53,61)	(57,48)
(12,31)	(22,25)	(26,21)	(27,47)	(35,17)	(47,37)	(56,4)	(57,50)
(12,33)	(22,35)	(26,22)	(27,52)	(35,18)	(47,42)	(56,12)	(57,57)
∞							

Cuadro 7.9: Puntos racionales de la curva definida por el polinomio $y^9 = x^2 + a^{27}x$

Cuerpo $\mathbb{F}_{81}$ sobre la curva $\mathscr{C}$ definida por el polinomio $y^{10} = x^3 + a^{50}x$.

(0,0)	(16,18)	(22,43)	(28,10)	(42,58)	(48,11)	(50,65)	(56,29)	(70,62)	(76,32)
(1,9)	(16,22)	(22,57)	(28,13)	(42,60)	(48,19)	(50,66)	(56,41)	(70,71)	(76,36)
(1,16)	(16,23)	(22,77)	(28,20)	(42,78)	(48,30)	(50,69)	(56,42)	(70,72)	(76,49)
(1,17)	(16,33)	(23,12)	(28,26)	(43,1)	(48,35)	(54,4)	(56,50)	(71,5)	(76,56)
(1,18)	(16,43)	(23,24)	(28,34)	(43,2)	(48,39)	(54,8)	(56,55)	(71,7)	(76,61)
(1,22)	(16,57)	(23,37)	(28,47)	(43,10)	(48,58)	(54,15)	(56,70)	(71,29)	(76,62)
(1,23)	(16,77)	(23,38)	(28,59)	(43,13)	(48,60)	(54,21)	(56,75)	(71,41)	(76,71)
(1,33)	(17,12)	(23,44)	(28,64)	(43,20)	(48,78)	(54,40)	(56,79)	(71,42)	(76,72)
(1,43)	(17,24)	(23,45)	(29,14)	(43,26)	(49,1)	(54,52)	(69,4)	(71,50)	(77,5)
(1,57)	(17,37)	(23,63)	(29,25)	(43,34)	(49,2)	(54,53)	(69,8)	(71,55)	(77,7)
(1,77)	(17,38)	(23,73)	(29,27)	(43,47)	(49,10)	(54,67)	(69,15)	(71,70)	(77,29)
(2,12)	(17,44)	(23,74)	(29,46)	(43,59)	(49,13)	(54,68)	(69,21)	(71,75)	(77,41)
(2,24)	(17,45)	(23,76)	(29,48)	(43,64)	(49,20)	(54,80)	(69,40)	(71,79)	(77,42)
(2,37)	(17,63)	(27,3)	(29,51)	(44,14)	(49,26)	(55,28)	(69,52)	(75,4)	(77,50)
(2,38)	(17,73)	(27,6)	(29,54)	(44,25)	(49,34)	(55,31)	(69,53)	(75,8)	(77,55)
(2,44)	(17,74)	(27,11)	(29,65)	(44,27)	(49,47)	(55,32)	(69,67)	(75,15)	(77,70)
(2,45)	(17,76)	(27,19)	(29,66)	(44,46)	(49,59)	(55,36)	(69,68)	(75,21)	(77,75)
(2,63)	(21,0)	(27,30)	(29,69)	(44,48)	(49,64)	(55,49)	(69,80)	(75,40)	(77,79)
(2,73)	(22,9)	(27,35)	(42,3)	(44,51)	(50,14)	(55,56)	(70,28)	(75,52)	∞
(2,74)	(22,16)	(27,39)	(42,6)	(44,54)	(50,25)	(55,61)	(70,31)	(75,53)	
(2,76)	(22,17)	(27,58)	(42,11)	(44,65)	(50,27)	(55,62)	(70,32)	(75,67)	
(15,0)	(22,18)	(27,60)	(42,19)	(44,66)	(50,46)	(55,71)	(70,36)	(75,68)	
(16,9)	(22,22)	(27,78)	(42,30)	(44,69)	(50,48)	(55,72)	(70,49)	(75,80)	
(16,16)	(22,23)	(28,1)	(42,35)	(48,3)	(50,51)	(56,5)	(70,56)	(76,28)	
(16,17)	(22,33)	(28,2)	(42,39)	(48,6)	(50,54)	(56,7)	(70,61)	(76,31)	

Cuadro 7.10: Puntos racionales de la curva definida por el polinomio $y^{10} = x^3 + a^{50}x$

CAPÍTULO 8

ANEXO 2

8.1. Código fuente

```
public class PolinomioStruct
{
 private int m_iValor;
 private int m_iPotencia;
 private Polinomio m_Polinomio;


 public PolinomioStruct(int iValor, int iPotencia, Polinomio polinomio){
  this.setM_iValor(iValor);
  this.setM_iPotencia(iPotencia);
  this.setM_Polinomio(polinomio);
 }

 /**
 * @return valor del polinomio.
 */
 public int getM_iValor() {
  return m_iValor;
 }

 /**
```

```
 * @param valor del polinomio.
 */
 public void setM_iValor(int m_iValue) {
  this.m_iValor = m_iValue;
 }

 /**
 * @return potencia del valor del polinomio
 */
 public int getM_iPotencia() {
  return m_iPotencia;
 }

 /**
 * @param potencia del valor del polinomio
 */
 public void setM_iPotencia(int iPower) {
  this.m_iPotencia = iPower;
 }

 /**
 * @return polinomio
 */
 public Polinomio getM_Polinomio() {
  return m_Polinomio;
 }

 /**
 * @param polinomio
 */
 public void setM_Polinomio(Polinomio polinomio) {
  this.m_Polinomio = polinomio;
 }
}

import java.util.HashMap;
import java.util.Map;
```

```
public class TablasPolinomios
{
 private Map<Integer,PolinomioStruct> m_PolinomioMapa = null;
 private int m_iNumeroElementosCuerpo;
 private int m_iBase;
 private int m_iPotencia;

 /**
 * La tabla de polinomios consta de un mapa de PolinomiosStruc indexados
 * por el valor del polinomio, la cantidad de elementos del
 * cuerpo y la base de los coeficientes.
 * @param cantidad de elementos del cuerpo.
 * @param base de los coeficientes.
 */
 public TablasPolinomios(int iNumeroElementosCuerpo, int iBase){
  m_PolinomioMapa = new HashMap<Integer, PolinomioStruct>();
  m_iNumeroElementosCuerpo = iNumeroElementosCuerpo;
  m_iBase = iBase;
 }

 /**
 * Crea todo lo necesaria sobre el cuerpo en la estructura de datos mapa.
 * @param  polinomio de corte del cuerpo.
 * @param  potencia a la que representa. Por ejemplo, si el polinomio de corte es
 * x^6=x^4+x^3+x^2+1, la potencia es 6.
 */
 public void Inicializar(Polinomio polinomio_corte){
  m_iPotencia = polinomio_corte.getGrado();

  int iCoefienteMayorPotencia = polinomio_corte.getCoeficientes()[m_iPotencia];

  Polinomio monomioMayorPotencia = new Polinomio(iCoefienteMayorPotencia, m_iPotencia);
  polinomio_corte = polinomio_corte.restar(monomioMayorPotencia);

  //Creamos los polinomios nulo y unidad, que forman parte de todos los cuerpos
  Polinomio polinomio_nulo = new Polinomio(0, 1);
  setEntrada(0, -1, polinomio_nulo);
```

```
Polinomio a_0 = new Polinomio(1, 0);
setEntrada(1, 0,  a_0);
System.out.println(1 + "-----a^0 = " + a_0.toString());

//Creamos los primeros iPotencia-1 polinomios de forma normal
for(int i=1; i<m_iPotencia; i++){
 Polinomio polinomio = new Polinomio(1, i);

 setEntrada(polinomio.evaluar(m_iBase), i, polinomio);
 System.out.println(polinomio.evaluar(m_iBase) + "-----a^"
         + i + " = " + polinomio.toString());
}

//Establecemos la entrada para el polinomio de corte.
setEntrada(polinomio_corte.evaluar(m_iBase), m_iPotencia, polinomio_corte);
System.out.println(polinomio_corte.evaluar(m_iBase)
        + "-----a^" + m_iPotencia + " = " + polinomio_corte.toString());

//Vamos multiplicando el polinomio actual por x, para obtener la
//siguiente potencia. A partir de ello, tenemos que evaluar si
//es necesario obtener mod del polinomio.
int iGrado = 0;
Polinomio polinomio_equis = new Polinomio(1, 1);
Polinomio current_pol = polinomio_corte;
for(int i=(m_iPotencia+1); i<=(m_iNumeroElementosCuerpo-2); i++){
 Polinomio new_pol = current_pol.multiplicar(polinomio_equis);
 current_pol = new_pol;
 iGrado = current_pol.getGrado();

 if(iGrado >= m_iPotencia){
  Polinomio new_pol_mod = null;
  new_pol_mod = new_pol.getModuloPolinomio(polinomio_corte, m_iPotencia, m_iBase);
  current_pol = new_pol_mod;
 }
 System.out.println(current_pol.evaluar(m_iBase)
         + "-----a^" + i + " = " + current_pol.toString());
 setEntrada(current_pol.evaluar(m_iBase), i, current_pol);
 new_pol = null;
```

```
 }

 System.out.println("End of New Field Calculation");
}

public void setEntrada(int iValor, int iPotencia, Polinomio polinomio){
 PolinomioStruct pStruct = new PolinomioStruct(iValor, iPotencia, polinomio);
 m_PolinomioMapa.put(iValor, pStruct);
}

/**
* Devuelve el valor de un polinomio, dada la potencia de un elemento
//primitivo por la que se representada.
* @param iPotencia del elemento primitivo.
* @return valor del polinomio.
*/
private int getValorNumericoPotencia(int iPotencia){
 int iIterPotencia         = -1;
 int i                                = 0;
 boolean bEncontrado = false;

 while( (bEncontrado == false) && (i<=m_iNumeroElementosCuerpo-1) ){
  iIterPotencia = m_PolinomioMapa.get(i).getM_iPotencia();

  if(iIterPotencia == iPotencia)
   bEncontrado = true;
  else
   i++;
 }
 return i;
}

/**
* Devuelve la tabla de la suma del cuerpo finito representado.
* @return tabla de la suma.
*/
public int[][] getTablaSuma(){
 int[][] iTablaSuma = new int[m_iNumeroElementosCuerpo][m_iNumeroElementosCuerpo];
```

```
 for(int i=0; i<=m_iNumeroElementosCuerpo-1; i++){
  Polinomio polinomio_fila = m_PolinomioMapa.get(i).getM_Polinomio();

  for(int j=0; j<=m_iNumeroElementosCuerpo-1; j++){
   Polinomio polinomio_columna = m_PolinomioMapa.get(j).getM_Polinomio();

   if(polinomio_fila.getGrado() == -1){
    int iValorSumar = polinomio_columna.evaluar(m_iBase);
    iTablaSuma[i][j] = iValorSumar;
    //System.out.print(iTablaSuma[i][j] + " ");
   }
   else{
    Polinomio polinomio_resultado = polinomio_fila.suma(polinomio_columna);
    polinomio_resultado.reducir();

    for (int k = 0; k <= polinomio_resultado.getGrado(); k++)
     polinomio_resultado.m_iCoeficientes[k] =
             (polinomio_resultado.m_iCoeficientes[k] % m_iBase);

    int iValue = polinomio_resultado.evaluar(m_iBase);
    iTablaSuma[i][j] = iValue;

    //System.out.print(iTablaSuma[i][j] + " ");
    //System.out.println("Tabla suma iteracion: i=" + i + ", j=" + j);
   }
  }
  //System.out.println();
 }
 return iTablaSuma;
}

/**
* Devuelve tabla de la multiplicar del cuerpo finito.
* Aprovechamos la forma en potencia para multiplicar y luego obtener
* el valor a partir de ella.
* @return tabla de multiplicar.
*/
```

```
 public int[][] getTableMultiplication(){
  int[][] iTablaMultiplication =
          new int[m_iNumeroElementosCuerpo][m_iNumeroElementosCuerpo];

  for(int i=0; i<=m_iNumeroElementosCuerpo-1; i++){
   int iPotenciaFila = m_PolinomioMapa.get(i).getM_iPotencia();
   int iValorTabla = 0;

   for(int j=0; j<=m_iNumeroElementosCuerpo-1; j++){
    if (iPotenciaFila == -1) {
     iTablaMultiplication[i][j] = iValorTabla;
     //System.out.print(iTablaMultiplication[i][j] + " ");
    }
    else{
     int iPotenciaColumna = m_PolinomioMapa.get(j).getM_iPotencia();

     if (iPotenciaColumna == -1)
      iTablaMultiplication[i][j] = iValorTabla;
     else{
      int iPotenciaBuscada =
              (iPotenciaFila + iPotenciaColumna) % (m_iNumeroElementosCuerpo-1);
      iValorTabla = getValorNumericoPotencia(iPotenciaBuscada);
      iTablaMultiplication[i][j] = iValorTabla;
     }
     //System.out.print(iTablaMultiplication[i][j] + " ");
     //System.out.println("Tabla multiplicacion iteracion: i=" + i + ", j=" + j);
    }
   }
   //System.out.println();
  }
  return iTablaMultiplication;
}

 public int getM_iNumeroElementosCuerpo() {
  return m_iNumeroElementosCuerpo;
  }

 public void setM_iNumeroElementosCuerpo(int m_iNumeroElementosCuerpo) {
```

```
  this.m_iNumeroElementosCuerpo = m_iNumeroElementosCuerpo;
 }

 public int getM_iBase() {
  return m_iBase;
 }

 public void setM_iBase(int m_iBase) {
  this.m_iBase = m_iBase;
 }
}
 /**
 * Esta clase representa un polinomio con coeficientes enteros.
 *
 * Incluye funciones para sumar, restar, multiplicar, dividir y obtener
 * mod otro polinomio.
 *
 * @author Jose David Villanueva Garcia.
 * @author UNED.
 */
public class Polinomio {
 public int[] m_iCoeficientes; // Coeficientes p(x) = sum { coeficientes[i] * x^i }
 private int m_iGrado; // Grado del polinomio (-1 para el polinomio nulo).

 /**
 * Inicializa un nuevo polinomio: ax^b
 * @param a Coeficiente principal
 * @param b Exponente
 * @throws IllegalArgumentException si {@code b} is negativo
 */
 public Polinomio(int a, int b) {
  if (b < 0)
   throw new IllegalArgumentException("El exponente no puede ser negativo: " + b);
  m_iCoeficientes = new int[b+1];
  m_iCoeficientes[b] = a;
  reducir();
 }
```

```
/**
* Precalcula el grado de el polinomio, en el caso de tener coeficientes .
* con valor cero (es decir, la longitud del array no esta relacionada
* necesariamente con el grado del polinomio).
*
*/
public void reducir() {
 m_iGrado = -1;
 for (int i = m_iCoeficientes.length - 1; i >= 0; i--){
  if (m_iCoeficientes[i] != 0) {
   m_iGrado = i;
   return;
  }
 }
}

/**
* Devuelve el grado de este polinomio.
* @return grado de este polinomio, -1 para el polinomio nulo.
*/
public int getGrado(){
 return m_iGrado;
}

/**
* Devuelve los coeficientes del polinomio.
* @return Array que contiene los coeficientes del polinomio.
*/
public int[] getCoeficientes(){
 return this.m_iCoeficientes;
}

/**
* Devuelve la suma de este polinomio y el polinomio del argumento.
*
* @param polinomio para sumar.
* @return polinomio cuyo valor es {@code (this(x) + pol(x))}.
*/
```

```
 public Polinomio suma(Polinomio pol){
  Polinomio polinom = new Polinomio(0, Math.max(this.m_iGrado, pol.m_iGrado));
  for (int i = 0; i <= this.m_iGrado; i++)
   polinom.m_iCoeficientes[i] += this.m_iCoeficientes[i];

  for (int i = 0; i <= pol.m_iGrado; i++)
   polinom.m_iCoeficientes[i] += pol.m_iCoeficientes[i];

  polinom.reducir();

  return polinom;
 }

 /**
 * Devuelve la resta de este polinomio y el polinomio del argumento.
 *
 * @param polinomio para restar.
 * @return polinomio cuyo valor es {@code (this(x) - pol(x))}.
 */
 public Polinomio restar(Polinomio pol){
  Polinomio polinom = new Polinomio(0, Math.max(this.m_iGrado, pol.m_iGrado));
  for (int i = 0; i <= this.m_iGrado; i++)
   polinom.m_iCoeficientes[i] += this.m_iCoeficientes[i];

  for (int i = 0; i <= pol.m_iGrado; i++)
   polinom.m_iCoeficientes[i] -= pol.m_iCoeficientes[i];

  polinom.reducir();

  return polinom;
}

 /**
 * Devuelve el producto de este polinomio y el polinomio del argumento.
 * El tiempo para ejecutar los bucles depende del grado del polinomio
 * mas alto.
 *
 * @param polinomio para multiplicar.
```

```
* @return polinomio cuyo valor es {@code (this(x) * pol(x))}.
*/
public Polinomio multiplicar(Polinomio pol){
 Polinomio polinom = new Polinomio(0, this.m_iGrado + pol.m_iGrado);
 for (int i = 0; i <= this.m_iGrado; i++){
  for (int j = 0; j <= pol.m_iGrado; j++){
   polinom.m_iCoeficientes[i+j] +=
           (this.m_iCoeficientes[i] * pol.m_iCoeficientes[j]);
  }
 }
 polinom.reducir();
 return polinom;
}

/**
* Devuelve el polinomio modulo el polinomio de corte
*
* @param polinomio de corte.
* @return polinomio cuyo valor es {@code (this(x) mod polinomio_corte)}
*/
public Polinomio getModuloPolinomio(Polinomio polinomio_corte,
       int iPotencia, int iBase){
 Polinomio pol_nuevo_modulo = null;

 //Coeficientes del polinomio actual.
 int iCoeficientes[] = getCoeficientes();

 //Obtenemos el coeficiente de la potencia mayor
 int iCoeficientePotenciaMayor = iCoeficientes[iPotencia];
 Polinomio polinomio_constante_potencia_mayor =
              new Polinomio(iCoeficientePotenciaMayor, 0);

 //Formamos el monomio correspondiente a la potencia mayor
 Polinomio monomio_potencia_mayor =
              new Polinomio(iCoeficientePotenciaMayor, iPotencia);

 //Multiplicamos tantas veces indique el monomio con la potencia mayor
 Polinomio pol_mult =
```

```
                polinomio_corte.multiplicar(polinomio_constante_potencia_mayor);

 //Quitamos del resultado el monomio de mayor potencia.
 Polinomio pol_orig_rest = restar(monomio_potencia_mayor);

 //Sumamos los polinomios, que ya son mod el polinomio de corte.
 pol_nuevo_modulo = pol_mult.suma(pol_orig_rest);
 int iCoeficienteArray = pol_nuevo_modulo.getCoeficientes().length;

 //Finalmente, calculamos los coeficientes del polinomio mod la base.

 for(int i=0; i<iCoeficienteArray; i++)
  pol_nuevo_modulo.m_iCoeficientes[i] =
              pol_nuevo_modulo.m_iCoeficientes[i] % iBase;

 pol_nuevo_modulo.reducir();
 iCoeficientes = null;
 return pol_nuevo_modulo;
}

/**
* Devuelve el resultado de evaluar el polinomio en x..
*
* @param x el punto en el que evaluamos el polinomio.
* @return numero entero cuyo valor es {@code (this(x))}
*/
public int evaluar(int x){
 int p = 0;
 for (int i = m_iGrado; i >= 0; i--)
  p = m_iCoeficientes[i] + (x * p);
 return p;
}

/**
* Devuelve el polinomio en texto.
* @return una cadena de texto representando el polinomio
* en el formato 4x^5 - 3x^2 + 11x + 5
*/
```

```
 @Override
 public String toString(){
  if (m_iGrado == -1)
   return "0";
  else if (m_iGrado == 0)
   return "" + m_iCoeficientes[0];
  else if (m_iGrado == 1)
   return m_iCoeficientes[1] + "x + " + m_iCoeficientes[0];
  String s = m_iCoeficientes[m_iGrado] + "x^" + m_iGrado;
   for (int i = m_iGrado - 1; i >= 0; i--){
    if (m_iCoeficientes[i] == 0)
     continue;
    else if (m_iCoeficientes[i] > 0)
   s = s + " + " + (m_iCoeficientes[i]);
   else if (m_iCoeficientes[i] < 0)
    s = s + " - " + (-m_iCoeficientes[i]);
   if (i == 1)
    s = s + "x";
   else if (i > 1)
    s = s + "x^" + i;
   }
  return s;
 }

public static void main(String[] args) {
 int iCountRationalPoints = 0;
 int iNumeroElementosCuerpo = 0; //Cantidad de elementos del cuerpo.
 int iBaseCoeficientes = 0; //Base de los coeficientes.

 /*****************************************************/
 /*Calculos para el cuerpo F16 (una curva)*/
 //Paso 1
 iNumeroElementosCuerpo = 16;
 iBaseCoeficientes = 2;
 //Paso 2
 TablasPolinomios polinomioMapaF16 =
        new TablasPolinomios(iNumeroElementosCuerpo, iBaseCoeficientes);
 //Paso 3 Polinomio de corte: a^4+x+1=0
```

```
Polinomio polinomio_corteF16 =
       new Polinomio(1,4).suma(new Polinomio(1, 1).suma(new Polinomio(1, 0)));
//Paso 4
polinomioMapaF16.Inicializar(polinomio_corteF16);
//Paso 5
int[][] additionTableF16 = polinomioMapaF16.getTablaSuma();
int[][] multiplicationTableF16 = polinomioMapaF16.getTableMultiplication();

for(int x=0; x<=iNumeroElementosCuerpo-1; x++){
 for(int y=0; y<=iNumeroElementosCuerpo-1; y++){
  //Esta curva es y^5=x^2+x
  int iValueYpowerFive = y;
  for(int k=1;k<=4;k++){
   iValueYpowerFive = multiplicationTableF16[iValueYpowerFive][y];
  }
  int iValueXsquare = multiplicationTableF16[x][x];
  int iValuePolynomialQ_X = additionTableF16[x][iValueXsquare];
  if(iValueYpowerFive == iValuePolynomialQ_X){
   iCountRationalPoints++;
   System.out.println(iCountRationalPoints +
                   ": Rational point: (" + x + "," + y + ")");
  }
 }
}

/*****************************************************/
/*Calculos para el cuerpo F64 (tenemos dos curvas)*/
//Paso 1
iNumeroElementosCuerpo = 64;
iBaseCoeficientes = 2;
//Paso 2
TablasPolinomios polinomioMapaF64 =
       new TablasPolinomios(iNumeroElementosCuerpo, iBaseCoeficientes);
//Paso 3 Polinomio de corte: x^6+x^4+x^3+x+1=0
Polinomio polinomio_corteF64 =
       new Polinomio(1,6).suma(new Polinomio(1, 4).suma(new Polinomio(1, 3).suma(new
Polinomio(1, 1).suma(new Polinomio(1, 0)))));
//Paso 4
```

```
polinomioMapaF64.Inicializar(polinomio_corteF64);
//Paso 5
int[][] additionTableF64 = polinomioMapaF64.getTablaSuma();
int[][] multiplicationTableF64 = polinomioMapaF64.getTableMultiplication();
iCountRationalPoints = 0;

for(int x=0; x<=iNumeroElementosCuerpo-1; x++){
 for(int y=0; y<=iNumeroElementosCuerpo-1; y++){
  //Esta curva es y^9=x^4+x^2+x
  int iValueYpowerNine = y;
  for(int k=1;k<=8;k++)
   iValueYpowerNine = multiplicationTableF64[iValueYpowerNine][y];

  int iValueXsquare = multiplicationTableF64[x][x];
  int iValueXPowerCube = multiplicationTableF64[iValueXsquare][x];
  int iValueXPowerFour = multiplicationTableF64[iValueXPowerCube][x];
  int iFirstSum = additionTableF64[iValueXPowerFour][iValueXsquare];
  int iValuePolynomialQ_X = additionTableF64[iFirstSum][x];
  if(iValueYpowerNine == iValuePolynomialQ_X) {
   iCountRationalPoints++;
   System.out.println(iCountRationalPoints +
                   ": Rational point: (" + x + "," + y + ")");
  }
 }
}

/*************************************************/
System.out.println("Siguiente curva");
iCountRationalPoints = 0;
for(int x=0; x<=iNumeroElementosCuerpo-1; x++){
 for(int y=0; y<=iNumeroElementosCuerpo-1; y++){
  //Esta curva es y^9=x^2+52x (y^9=x^2+a^27x)
  int iValueYpowerNine = y;

  for(int k=1;k<=8;k++)
   iValueYpowerNine = multiplicationTableF64[iValueYpowerNine][y];

  int iValueXsquare = multiplicationTableF64[x][x];
```

```
   int iValue52X = multiplicationTableF64[52][x];
   int iValuePolynomialQ_X = additionTableF64[iValueXsquare][iValue52X];
   if(iValueYpowerNine == iValuePolynomialQ_X){
    iCountRationalPoints++;
    System.out.println(iCountRationalPoints +
                    ": Rational point: (" + x + "," + y + ")");
   }
  }
 }

 /*****************************************************/
 /*Calculos para el cuerpo F81*/
 //Paso 1
 iNumeroElementosCuerpo = 81;
 iBaseCoeficientes = 3;
 //Paso 2
 TablasPolinomios polinomioMapaF81 =
        new TablasPolinomios(iNumeroElementosCuerpo, iBaseCoeficientes);
 //Paso 3 Polinomio de corte: x^4+2x+1=0
 Polinomio polinomio_corteF81 =
        new Polinomio(1,4).suma(new Polinomio(2, 1).suma(new Polinomio(1, 0)));
 //Paso 4
 polinomioMapaF81.Inicializar(polinomio_corteF81);
 //Paso 5
 int[][] additionTableF81 = polinomioMapaF81.getTablaSuma();
 int[][] multiplicationTableF81 = polinomioMapaF81.getTableMultiplication();
 iCountRationalPoints = 0;

 for(int x=0; x<=iNumeroElementosCuerpo-1; x++){
  for(int y=0; y<=iNumeroElementosCuerpo-1; y++){
   //Esta curva es y^10=x^3+77x
   int iValueYpowerTen = y;
   for(int k=1;k<=9;k++){
    iValueYpowerTen = multiplicationTableF81[iValueYpowerTen][y];
   }
   int iValueXsquare = multiplicationTableF81[x][x];
   int iValueXCube = multiplicationTableF81[iValueXsquare][x];
   int iRighSum = multiplicationTableF81[77][x];
```

```
   int iValuePolynomialQ_X = additionTableF81[iValueXCube][iRighSum];
   if(iValueYpowerTen == iValuePolynomialQ_X){
    iCountRationalPoints++;
    System.out.println(iCountRationalPoints +
                    ": Rational point:(" + x + ","+ y + ")");
   }
  }
 }

 /*************************************************/
 //TEST F_16384
 float tiempoInicio = System.currentTimeMillis();
 //Paso 1
 iNumeroElementosCuerpo = 16384;
 iBaseCoeficientes = 2;
 //Paso 2
 TablasPolinomios polinomioMapaF16384 =
        new TablasPolinomios(iNumeroElementosCuerpo, iBaseCoeficientes);
 //Paso 3 Polinomio de corte: x^14+x^5+x^3+x+1=0
 Polinomio polinomio_corteF16384 =
        new Polinomio(1,14).suma(new Polinomio(1,5).suma(new Polinomio(1,3).suma(new
 Polinomio(1, 1).suma(new Polinomio(1, 0)))));
 //Paso 4
 polinomioMapaF16384.Inicializar(polinomio_corteF16384);

 //Paso 5
 int[][] additionTableF16384 = polinomioMapaF16384.getTablaSuma();
 int[][] multiplicationTableF16384 = polinomioMapaF16384.getTableMultiplication();
 float totalTiempo = System.currentTimeMillis() - tiempoInicio;
 System.out.println("El tiempo de ejecucion en milisegundos es :"
         + totalTiempo + " miliseg");
 System.out.println();
 System.out.println("El tiempo de ejecucion en minutos es :"
         + ((totalTiempo/1000))/60 + " minutos");
 }
}
```