Pontificia Universidad Católica del Perú
Escuela de Posgrado

Teoría de códigos sobre curvas algebraicas y aplicación de las bases de Gröbner

Tesis para optar el grado académico de
Magíster en Matemáticas

Autor
Aldo Arquimedes Salinas Encinas

Asesor
Hernán Neciosup Puican

Jurado
Christian Holger Valqui Haase
Percy Braulio Fernández Sánchez

Lima - Perú
Noviembre - 2020

Teoría de códigos sobre curvas algebraicas y aplicación de las bases de Gröbner[1]

Aldo Arquimedes Salinas Encinas

Tesis presentada a consideración del cuerpo docente de la Escuela de Posgrado, de la Pontificia Universidad Católica del Perú (PUCP), como parte de los requisitos para obtener el grado académico de Magíster en Matemáticas.

Miembros del Jurado:

_____

Dr. Christian Holger Valqui Haase.

(Presidente del jurado)

_____

Dr. Hernán Neciosup Puican.

(Asesor)

_____

Dr. Percy Braulio Fernández Sánchez.

(Tercer miembro)

Lima - Perú

Noviembre - 2020

[1] comentario si es necesario: version final con las correcciones del jurado

Resumen

Teoría de códigos sobre curvas algebraicas y aplicación de las bases de Gröbner

ArquiMEDES SALINAS ENCINAS

2020

Asesor: Hernán Neciosup Puican.
Título obtenido: Magíster en Matemáticas.

En la época que estamos viviendo, el manejo de la información toma una presencia muy importante en la toma de decisiones. La teoría de códigos surge en el mejoramiento de la transmisión de datos, desde las primeras computadoras hasta las super computadoras que tenemos hoy en día; no pasó mucho tiempo para que se establecieran las bases teóricas que sustentaran el desarrollo vértiginoso que se ha dado hasta hoy.

Empezando como simples subconjuntos, los códigos cobraron fuerza al ser vistos como subespacios vectoriales de dimensión finita. Lógicamente, al estar íntimamente ligadas el álgebra con la geometría; no es de extrañarse el surgimiento, con la ayuda de la teoría de cuerpo de funciones algebraicas, de los códigos algebro-geométricos o mejor conocidos como códigos de Goppa.

La teoría de códigos es una gran área de investigación, que con ayuda de la tecnología se complementan en busca de mejoras.

En este trabajo de tesis, estudiaremos los códigos algebro-geométricos para la codificación y la aplicación de las bases de Gröbner para la decodificación de los mismos.

Abstract

Code theory on algebraic curves and application of the Gröbner bases

Arquimedes Salinas Encinas

2020

Adviser: Hernán Neciosup Puican.
Obtained title: Magíster en Matemáticas.

At the time that we are living, information management takes a very important presence in decision making. Code theory arises in the improvement of the transmission of data, from the first computers to the super computers we have today; it didn't take long for me to know establish the theoretical bases that would sustain the vertiginous development that has given until today.

Starting as simple subsets, the codes gained momentum when viewed as finite-dimensional vector subspaces. Logically, being intimately linked algebra with geometry; no wonder the emergence, with the help of the field theory of algebraic functions, of the algebro-geometric codes or better known as Goppa codes.

The theory of codes is a large area of research, which with the help of tecnology, they complement each other in search of improvements.

In this thesis work, we'll study the alegbro-geometric codes for the coding and the application of bases Gröbner for the decoding of them.

A mis padres Benigno y Evelia,
a mis preciosas hijas Abigail y
Natalia.

Índice general

Agradecimientos

Antes de todo quiero agradecer a Dios, por la familia que me ha dado, los amigos y familiares que siempre están pendiente de mi. Gracias a Dios tengo una segunda oportunidad de seguir al lado de mi familia, y hacer lo que más me apasiona estudiar.
Quiero agradecer enormemente a la PUCP, por haber sido una segunda casa y brindarme el privilegio de enriquecer mi formación académica, y apoyarme frente al problema de salud.
A mis padres Benigno y Evelia por su apoyo incondicional, su constancia, motivación y esfuerzo en todo momento por salir adelante ante cualquier adversidad, el amor que en todo momento me dan.
A mi esposa, Flor, por su apoyo como pareja, las palabras de motivación, a mis hijas Abigail y Natalia que son el motor para seguir adelante, ser mejor cada día, por su amor incondicional que siempre tienen para mí.
A mis hermanos Riquelmer, César y Luis que en todo momento me alentaron a terminar lo que uno empieza, su infinito apoyo por todo lo que vienen haciendo por mí.
Un agradecimiento muy especial a mis profesores Percy Férnandez, Hérnan Neciosup, Nancy Saravía y Jesús Zapata, que en todo momento me apoyarón, con sus enseñanzas dentro y fuera de las aulas. Son ejemplo para seguir adelante y continuar por este maravilloso mundo que son las Matemáticas.
Finalmente, también agradecer a los jurados los doctores: Christian Valqui Haase, Percy Fernández Sanchéz y Hernán Neciosup Puican que gracias a sus observaciones se ha podido mejorar la presente Tesis.

Introducción

Hoy en día en que la información es cada vez más importante y, su dependencia de los datos que se envía son relevantes muchas veces en la toma de decisiones, los errores de transmisión pueden tener consecuencias muy graves. Imaginemos que deseamos enviar una información, (por ejemplo una transacción de $ 1000), y ésta no llega del todo correcta a su destino (por ejemplo, llega $ 100 000), esto causaría muchas dificultades. También podemos considerar este otro ejemplo, imaginemos que tenemos un robot para desactivar explosivos, si el robot se controla de manera remota, y enviamos la instrucción de "cortar el cable rojo" mediante (100) pero en cambio recepciona la información (010) que significa "cortar el cable verde", este error ocasiona una explosión.

En 1947 Richard W. Hamming desarrolla la teoría de codificación usando equipos de transmisión mecánica en los laboratorios de los teléfonos Bell. A la postre esto vendría a ser el inicio de la teoría de códigos, y en 1950 publica un artículo [2] para crear códigos que detectan y corrigen errrores. Después se denominaron códigos de Hamming. En 1948, Claude Shannon publicó A Mathematical Theory of Communication, un artículo en dos partes: uno en julio y el otro en octubre [3] en la revista técnica de sistemas Bell, y después en 1949 publica su libro The Mathematical Theory of Communication [Sha01].

El código binario de Golay se desarrolló en 1949. Es un código de corrección de errores capaz de corregir hasta tres errores en cada palabra de 24 bits y detectar un cuarto, estos códigos fueron usados por el explorador Voyager para transmitir fotografías coloridas de Jupiter y Saturno.

Golay, Hamming y Shanon fueron los grandes pioneros que iniciaron este trabajo,

[2] Hamming, R. W. (1950). Error detecting and error correcting codes. The Bell system technical journal, 29(2), 147-160.

[3] Shannon, Claude E. (October 1948). "A Mathematical Theory of Communication". Bell System Technical Journal. 27 (4): 623–666. doi:10.1002/j.1538-7305.1948.tb00917.x

ellos desarrollaron estudios e ideas que son usadas hasta nuestros días, como la comunicación móvil (por ejemplo, celulares), la compresión de datos (por ejemplo, DVD, Blueray), también comunicación vía satelite, procesamiento de imágenes digitales, entre otras.

La idea en general consiste en ver la fiabilidad de los canales de transmisión, mecanismos para detectar y corregir errores; por el cual se usaban los códigos lineales binarios.

Posteriormente, en la década de los 70, V. D. Goppa, en su investigación se dió cuenta que podía asociar códigos con ciertos divisores de cuerpos de funciones algebraicas y en los ochenta (Goppa 1981), presenta una nueva construcción de códigos lineales a partir de curvas algebraicas definidas sobre cuerpos finitos F_q (denominados códigos algebro-geométrico, o códigos geométricos de Goppa). Para esto se usan la evaluacion de espacio de funciones sobre curvas algebraicas. El Teorema de Riemann-Roch [4] proporciona buenas estimaciones para algunas propiedades de los códigos.

Por ejemplo, si queremos codificar un mensaje a usando un alfabeto A, para obtener un código C de longitud fija n sobre un cuerpo finito F_q, primero debemos elegir una curva algebraica X definida sobre F_q, aplicamos el Teorema de Riemann-Roch para construir un espacio $L(D)$ asociado al divisor racional D de X, y así obtener una matriz generadora G,

$$a \xrightarrow{\text{codificación}} aG.$$

Su estructura geométrica permite de manera especifica algoritmos de decodificación, que en sí viene hacer la parte de la recuperación de la información,

$$a \xrightarrow{\text{codificación}} aG \xrightarrow{\text{decodificación}} a.$$

Dados los problemas relacionados con estos códigos, una formulación polinómica es natural, y por eso las bases de Gröbner encuentran un campo de aplicación. Los códigos algebro-geométricos son un gran campo de investigación y en los últimos años se han desarrollado muchos algoritmos de decodificación, buscando optimizar su recuperación de la información.

[4] Goppa, Valerii Denisovich. "Codes associated with divisors". Problemy Peredachi Informatsii 13.1 (1977): 33-39.

Este trabajo consiste en seis capítulos distribuidos de la siguiente manera:

Capítulo 1, presentamos conceptos necesarios para el desarrollo de la tesis, desde cuerpos finitos, hasta campo de funciones racionales.

Capítulo 2, definimos divisor de una curva, después definimos y probamos el Teorema de Riemann-Roch, que será una parte importante en la unión de conceptos del capítulo 1 y el capítulo 3.

Capítulo 3, definimos lo que es un código algebro-geométrico, vemos lo que es un código lineal, y algunos códigos como: Reed-Muller, Reed-Solomon y los códigos de Goppa. Aquí se muestra como una palabra código codificada es enviada y después decodificada.

Capítulo 4, por lo expuesto en el capítulo 3, vemos que hay una necesidad de definir muchos puntos racionales, y disminuir la raíz q (tasa de información). Definimos lo que es un automorfismo y su uso en los códigos de Goppa, que será usado en el capítulo 5.

Capítulo 5, describimos el rol importante que juegan las bases de Gröbner al momento de decodificar un mensaje recibido. Ésto será desarrollado vía módulos.

Capítulo 6, se indica algunas conclusiones del trabajo de tesis, como también algunas ideas para seguir investigando.

Aldo Arquimedes Salinas Encinas
Lima, Perú.
2020

Capítulo 1

Preliminares

La geometría algebraica nació con el descubrimiento de las coordenadas cartesianas, y consistio, en principio, en el estudio de propiedades particulares de subconjuntos de R^2 y R^3 definidos por ecuaciones polinomiales respecto a las coordenadas, y se desarrolló basicamente en la búsqueda de invariantes con respecto a algunas transformaciones del plano o del espacio; problemas de intersecciones entre curvas, y también el estudio de familias de puntos sobre una curva, o familia de curvas en una superficie. En este capítulo, presentaremos conceptos y propiedades básicas de la geometría algebraica útiles para este trabajo de tesis.

1.1 Cuerpos finitos

Los cuerpos que tienen una cantidad finita de elementos (denominados cuerpos finitos) juegan un rol importante en algunas de las ramas de la matemática como por ejemplo: teoría de números, teoría de Galois, Geometría proyectiva, etc. Sin embargo una de las aplicaciones más importantes, esencialmente se da en la codificación de la información dígital.

Estructura de cuerpos finitos

Dado p un número primo, las clases residuales módulo p del anillo Z forman un cuerpo, al cual lo denotaremos Z/pZ o por F_p.
Un cuerpo es llamado cuerpo finito si solo contiene un número finito de elementos.

Ejemplo 1.1. Determinemos todos los elementos del cuerpo F_7.

Es evidente que al ser 7 un número primo sus únicos residuos módulo 7, son 0,1,2,3,4,5,6; por lo tanto

$$F_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}.$$

Observar que hemos calculado el cuerpo con elementos de manera aditiva; podemos calcular el cuerpo F_7 como un grupo multiplicativo, consideramos un elemento no nulo $\bar{3} \in F_7$.

$$F_7 = \{\bar{0}, \bar{3}, \bar{3}^2, \bar{3}^3, \bar{3}^4, \bar{3}^5, \bar{3}^6\}.$$

Vamos a efectuar sus residuos módulo 7,

$\bar{3} = \bar{3} \bmod 7$

$\bar{3}^2 = \bar{2} \bmod 7$

$\bar{3}^3 = \bar{6} \bmod 7$

$\bar{3}^4 = \bar{4} \bmod 7$

$\bar{3}^5 = \bar{5} \bmod 7$

$\bar{3}^6 = \bar{1} \bmod 7$

obtenemos lo siguiente:

$$F_7 = \{\bar{0}, \bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}, \bar{1}\}.$$

Los ejemplos más familiares de cuerpos finitos vienen hacer los cuerpos F_p, con p primo.

Del ejemplo 1.1, podemos notar que a partir de un elemento $\bar{3} \in F_7$ como grupo multiplicativo, también es un grupo es cíclico.

Teorema 1.2. Sea k cualquier cuerpo y G un subgrupo finito del grupo multiplicativo de k. Entonces G es cíclico.

Prueba. Supongamos que $|G| = n$. Para cada divisor d de n consideremos el conjunto G_d formado por los elementos de G que tienen orden d. Supongamos que uno de estos conjuntos G_d no sea vacío, es decir, existe $y \in G_d$. Entonces el subgrupo generado por y está contenido en el subgrupo formado por los elementos de G que cumplen $x^d = 1$, es decir,

$$\langle y \rangle \checkmark \{x \in G \mid x^d = 1\}.$$

Pero el orden del grupo $\langle y \rangle$ es d, y hay a lo más d raices de $x^d - 1 = 0$, por lo tanto $\langle y \rangle = \{x \in G \mid x^d = 1\}$, lo cual implica $G_d \checkmark \langle y \rangle$, es decir, G_d es el conjunto de

generadores del grupo $\langle y \rangle \cong Z/dZ$, y por lo tanto $|G_d| = \$(d)$. Hemos probado que para cada divisor d de n, se tiene que G_d es vacío o tiene cardinalidad $\$(d)$. Entonces

$$n = \#G = \sum_{d|n} \#G_d \leq \sum_{d|n} \$(d) = n,$$

y se sigue que la desiguadad es una igualdad, lo cual implica que para todo $d|n$, se tiene $|G_d| = \$(d)$. En particular para el divisor $d = n$, se tiene $|G_n| = \$(n) > 0$, lo cual demuestra que G_n es no vacío, es decir, existe al menos un elemento de orden n, que genera a todo el grupo G. Esto demuestra que G es cíclico. □

Como consecuencia inmediata resulta el siguiente corolario.

Corolario 1.3. El grupo multiplicativo de un cuerpo finito es cíclico.

Otros ejemplos de cuerpos finitos son:

Ejemplo 1.4. $k = F_2[X]/\langle X^2 + X + 1 \rangle$ es un cuerpo que tiene cuatro elementos. Es evidente que k es un cuerpo, ya que $X^2 + X + 1$ es un polinomio irreducible en $F_2[X]$, notamos además que $X^2 + X + 1$ es un polinomio de segundo grado en $F_2[X]$, por lo que al hallar el resto con cualquier polinomio $P \in F_2[X]$ sólo se obtendrá polinomios de la forma $aX + b$ con $a, b \in F_2$. Tenemos cuatro opciones para (a, b) y obtenemos que

$$k = F_2[X]/\langle X^2 + X + 1 \rangle = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}\}.$$

Observación 1.5. Se puede probar que hay un único cuerpo F_4 con cuatro elementos y se tiene $F_4 \cong F_2[X]/\langle X^2 + X + 1 \rangle$

+	0	1	α	α + 1
0	0	1	α	α + 1
1	1	0	α + 1	α
α	α	α + 1	0	1
α + 1	α + 1	α	1	0

x	0	1	α	α + 1
0	0	0	0	0
1	0	1	α	α + 1
α	0	α	α + 1	1
α + 1	0	α + 1	1	α

Cabe indicar que $1 = \overline{1}$, $X = \alpha$.

Definición 1.6. (Característica de un cuerpo)
Diremos que un cuerpo k tiene característica n, $\text{char}(k) = n$, si n es el menor número natural tal que $\underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}} + 1 = 0$. Si esta suma fuese distinta de cero, diremos que su característica es cero.

Ejemplo 1.7. De los ejemplos anteriores podemos deducir:

- $\mathrm{char}(F_7) = 7$.
- $\mathrm{char}(F_2[X]/\langle X^2 + X + 1\rangle) = 2$.
- $\mathrm{char}(Q) = \mathrm{char}(R) = \mathrm{char}(C) = 0$.
- $\mathrm{char}(F_2(X)) = 2$, note que $F_2(X)$ es un cuerpo infinito.

Observación 1.8. Tener presente que $F_2(X)$ representa el cuerpo de fracciones del dominio $F_2[X]$, que será visto en la página 23.

Cuerpo primo

Definición 1.9. El subcuerpo primo del cuerpo k es la intersección de todos los subcuerpos de k.
Diremos que k es un cuerpo primo si coincide con su subcuerpo primo.

Ejemplo 1.10. El cuerpo Q de los racionales es un cuerpo primo de Q.

Proposición 1.11. Sea k un cuerpo primo, se verifica una y solo una de las siguientes propiedades:

1. El cuerpo k tiene característica cero, y k es isomorfo a Q.
2. El cuerpo k tiene característica $p > 0$, el homomorfismo $\$: Z \to k$ es sobreyectivo y, k es isomorfo a F_p.

Como p es primo, F_p es un cuerpo primo, entonces F_p no admite subcuerpos; además F_p tiene exactamente p elementos.

Proposición 1.12. Si la característica de un cuerpo k es distinta de cero, entonces esta debe ser un número primo.

Prueba. Supongamos que el cuerpo k tiene característica $n > 0$, y además que n no sea un número primo, por lo tanto existen naturales $n_1, n_2 < n$ tales que podemos factorizarlo como $n = n_1.n_2$. Entonces

$$(n_1 1)(n_2 1) = (n_1 n_2)1 = n1 = 0, \qquad \text{pues } n = \mathrm{char}(k).$$

Además, como k es un cuerpo, también es un dominio, por lo que no tiene divisores de cero, luego $n_1 1 = 0$ ó $n_2 1 = 0$, eso implicaría que existe un natural menor que n

que cumple dicha condición, lo cual es una contradicción, por ser n el menor número natural con esta condición. □

Definición 1.13. Sea k un cuerpo. Un cuerpo F es una **extensión** de k, si k es subcuerpo de F. Denotaremos a esta extensión de k como F|k ó F : k.

Definición 1.14. Sea k un cuerpo, diremos que la extensión F|k es:

- Simple, si F = k(↵) con ↵ 2 F.
- Algebraica, si para todo ↵ 2 F, ↵ es algebraico sobre k, es decir, existe un polinomio no nulo P 2 k[X] tal que P(↵) = 0.
- Trascendente, si no es algebraica, es decir, si existe algún elemento ↵ 2 F de modo que no existe polinomio P 2 k[X] tal que ↵ sea raízde P .

Si un cuerpo finito tiene característica p, con p primo, éste contiene a F_p. Recordemos que si F es un cuerpo que contiene otro cuerpo k (en nuestro caso F_p), entonces F es una extensión de k.

Proposición 1.15. Si F es una extensión de k, entonces F es un espacio vectorial sobre k.

Prueba. Es fácil ver que (F, +) es un grupo abeliano. Por otro lado, podemos definir una multiplicación por escalar

$$\cdot : k \to F \times F$$

de la siguiente manera

$$(h, l) \mapsto h.f$$

para todo h 2 k y f 2 F. Por lo tanto, F es un espacio vectorial sobre k. □

Proposición 1.16. Toda extensión finita es algebraica.

Prueba. Consideremos la extensión F|k finita y ↵ 2 F. Como F|k es una extensión finita, por la proposición 1.15 es un espacio vectorial, necesariamente de dimensión finita digamos dim(F) = n, y por lo tanto existe una combinación lineal no trivial nula entre los elementos 1, ↵, $↵^2$, ··· , $↵^n$; es decir; existen L_i 2 k tal que $0 \leq i \leq n$

$$L_n ↵^n + L_{n-1} ↵^{n-1} + \cdots + L_1 ↵ + L_0 = 0.$$

Si consideramos el polinomio $P(X) = L_n X^n + L_{n-1} X^{n-1} + \cdots + L_1 X + L_0$, es claro que P 2 k[X], tal que P(↵) = 0, por lo tanto F|k es algebraica. □

Definición 1.17. (Algebraicamente cerrado)
Sea F un cuerpo, diremos que F es algebraicamente cerrado, si no existen extensiones algebraicas propias de F. Es decir, si $L|F$ es una extensión algebraica, esto obliga a que $L = F$.

Ejemplo 1.18. El cuerpo $F = C$ es algebraicamente cerrado.

Proposición 1.19. Todo cuerpo algebraicamente cerrado es infinito.

Prueba. Supongamos que el cuerpo es finito, es decir, $k = \{a_1, a_2, \ldots, a_n\}$. Consideremos el polinomio $f(X) = (X - a_1)(X - a_2) \cdots (X - a_n) + 1 \in k[X]$, con $f(a) = 1 \neq 0$ para todo $a \in k$, por lo que podemos afirmar que f no tiene raíces en k, luego k no sería algebraicamente cerrado. □

Definición 1.20. (Grado de una extensión)
Sea $F|k$ una extensión de cuerpos. Si la dimensión de F como espacio vectorial sobre k es finita, ($\dim_k F = n$), entonces diremos que F es una extensión finita de grado n sobre k. Denotemos por $[F : k] := \dim_k F$ al grado de la extensión.

Ejemplo 1.21. El grado de la extensión $C|R$ es dos, es decir, $[C : R] = 2$.

Lema 1.22. Sea F un cuerpo finito conteniendo un subcuerpo L con q elementos. Entonces F tiene q^m elementos, donde $m = [F : L]$.

Prueba. Por la proposición 1.15, F es un espacio vectorial sobre L, finito dimensional, pues F es finito. Denotaremos dicha dimensión $[F : L] = m$, y entonces F tiene una base sobre L que consiste de m elementos $\emptyset_1, \emptyset_2, \cdots, \emptyset_m$.
Cada elemento de F puede ser representado de manera única en la forma $k_1\emptyset_1 + k_2\emptyset_2 + \cdots + k_m\emptyset_m$ ($k_1, k_2, \cdots, k_m \in L$), como cada $k_i \in L$ y L tiene q elementos entonces cada k_i puede tomar q valores, así F debe tener q^m elementos. □

Teorema 1.23. Si F es un cuerpo finito, entonces F tiene característica $p > 0$ con p primo, y el número de elementos de F es p^n donde n es el grado de la extensión de F sobre un subcuerpo primo.

Prueba. Por la proposición 1.12, como F es un cuerpo finito, F es de característica p, con p primo. Sea L el subcuerpo primo de F. Aquí L no es isomorfo a Q, pues Q tiene característica cero y es infinito, así que L es isomorfo a F_p para algún primo p, así L tiene p elementos.
Sea $n = [F : L]$, por el lema 1.22 podemos concluir que F tiene p^n elementos. □

Teorema 1.24. Sea k un cuerpo finito y sean $\alpha_1, \ldots, \alpha_r$ elementos algebraicos sobre k (pertenecientes a alguna extensión del cuerpo k). Entonces existe algún $\alpha \in k(\alpha_1, \ldots, \alpha_r)$ de modo que

$$k(\alpha) = k(\alpha_1, \ldots, \alpha_r).$$

Prueba. Consideremos $F = k(\alpha_1, \ldots, \alpha_r)$, es el menor cuerpo que contiene a k y también a los elementos $\alpha_1, \ldots, \alpha_r$. Es evidente que F es una extensión finita de k, como k es un cuerpo finito, entonces F es también un cuerpo finito.
Del corolario 1.3, el grupo multiplicativo del cuerpo F es cíclico, y supongamos que α es su generador.
Es trivial que $F \supseteq k(\alpha)$, además $k(\alpha)$ es el menor cuerpo que contiene al cuerpo k y a α, por lo tanto $k(\alpha) \supseteq F$. Como consecuencia se tiene $k(\alpha) = F$. □

Definición 1.25. (Cuerpo de descomposición)
Sea $P \in k[X]$ un polinomio con coeficientes en el cuerpo k. Sea F una extensión de k. Diremos que:

1. P se descompone en F, si P se descompone en producto de factores lineales en F, es decir:

$$P(X) = c(X - a_1)(X - a_2)\cdots(X - a_n) \in F[X], \quad c \in k, \quad a_i \in F.$$

2. F es el cuerpo de descomposición de P, si P se descompone en F y no existe un cuerpo intermedio L de modo que

$$k \subseteq L \subseteq F,$$

y tal que P sea descompuesto en factores lineales en L.

Ejemplo 1.26. Sea $P(X) = (X^2-2)(X^2-3) \in Q[X]$. El cuerpo de descomposición será $F = Q(\sqrt{2}, \sqrt{3})$ y además su grado $[F : Q] = 4$.
En el cuerpo F, se tiene

$$P(X) = (X + \sqrt{2})(X - \sqrt{2})(X + \sqrt{3})(X - \sqrt{3}) \in F[X],$$

se puede probar que no existe ningún cuerpo intermedio que descomponga a P.

Ejemplo 1.27. Sea $P(X) = X^4 + 4 \in Q[X]$, observamos que el polinomio es reducible, $P(X) = (X^2 + 2X + 2)(X^2 - 2X + 2)$. El cuerpo de descomposición será $F = Q(i + 1)$ y además su grado $[F : Q] = 2$.

Ejemplo 1.28. Si consideremos el polinomio $P(X) = X^3 - 3 \in Q[X]$, dado que $P(X) = (X - \sqrt[3]{3})(X^2 + \sqrt[3]{3}X + \sqrt[3]{9})$, el cuerpo $Q(\sqrt[3]{3})$ no es su cuerpo de descomposición, pero $Q(\sqrt[3]{3}, \sqrt[3]{3}i)$ si es su cuerpo de descomposición.

Proposición 1.29. Sea $q = p^n$. Entonces $F = F_p$ es el cuerpo de descomposición del polinomio $X^q - X$ sobre F_p.

Prueba. Tenemos que F es un F_p-espacio vectorial de dimensión finita, digamos $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ es una F_p-base, esto es,

$$F = \alpha_1 F_p \alpha_2 F_p \cdots \alpha_n F_p = (F_p, F_p, \cdots, F_p)$$
$$\underbrace{\qquad\qquad}_{n \text{ veces}}$$

así, $|F| = p^n$. Además $(F^* = F \setminus \{0\}, \cdot)$ es un grupo ciclico de orden $p^n - 1$, entonces todo elemento de F^* satisface la ecuación

$$X^{p^n - 1} - 1 = 0.$$

Luego, todo elemento de F es raíz del polinomio $X^{p^n} - X = 0$, haciendo $q = p^n$ obtenemos $X^q - X = 0 \in F_p[X]$. En consecuencia $F|F_p$ es algebraico y $[F : F_p] = n$. Por lo tanto, F es el cuerpo de descomposición de $X^{p^n} - X$. □

Observación 1.30. Si F es el cuerpo de descomposición de $P(X) \in F[X]$, entonces $F = k(\lambda_1, \ldots, \lambda_n)$, donde λ_i son las raíces de $P(X)$ y $F|k$ es una extensión finita, su grado está acotado por $n!$, siendo n el grado de $P(X)$.

Teorema 1.31 (Kronecker). Sea k un cuerpo y $P(X) \in k[X] \setminus k$, entonces existe un cuerpo K, conteniendo a todos los subcuerpos de k, donde P es completamente factorizable en una extensión de k.

Prueba. Una demostración completa del teorema se puede observar en [Rot05, pág 299] □

Clausura algebraica

Por el teorema fundamental del álgebra, todo polinomio de grado n con coeficientes en C posee exactamente n raíces reales o complejas contadas con multiplicidad, es decir, todo polinomio se puede expresar como el producto de n polinomios lineales, del teorema 1.31 tenemos que siempre existe un cuerpo donde el polinomio se factoriza en polinomios lineales. Nos preguntamos si existe un cuerpo F extensión de un cuerpo k, donde cualquier polinomio con coeficientes en F se factorice en polinomios lineales sobre F, a tal cuerpo se le denomina clausura algebraica.

Definición 1.32. Una clausura algebraica de un cuerpo k es una extensión algebraica F de k formada por un cuerpo algebraicamente cerrado, al cual denotaremos por $\overline{k}$.

Teorema 1.33. Todo cuerpo k siempre posee su clausura algebraica.

Prueba. La demostración se puede ver en [Mil03]. □

Ejemplos 1.34. Sea k un cuerpo con $\text{char}(k) > 0$, entonces su clausura algebraica $\overline{k}$ será un cuerpo infinito numerable, por ejemplo para $k = F_p$, su clausura algebraica $\overline{k}$ es la unión de los F_{p^n}, con $n \leq 1$.
Si k es un cuerpo con $\text{char}(k) = 0$, entonces su clausura algebraica $\overline{k}$ tendrá la misma cardinalidad, por ejemplo para el cuerpo $k = R$, su clausura algebraica será $\overline{k} = C$.

1.2 Curvas algebraicas

Las curvas algebraicas son variedades algebraicas de dimensión uno. En esta sección, estudiaremos brevemente las curvas algebraicas sobre un cuerpo k algebraicamente cerrado; para mayores detalle al respecto ver [FW69].

Curvas afines

Sea k un cuerpo y, consideremos el producto cartesiano n veces de k,

$$A^n(k) = \underbrace{k \times \cdots \times k}_{n \text{ veces}}.$$

El conjunto $A^n(k)$ es denominado el n-espacio afín sobre k, el cual puede ser escrito de la siguiente manera

$$A^n_k = \{(x_1, x_2, \ldots, x_n) : \ x_1, x_2, \ldots, x_n \in k\}.$$

Los elementos $(x_1, \ldots, x_n)$ de A^n_k se denominan puntos.
Para $n = 1$, A^1_k se denomina **recta afín**.
Para $n = 2$, A^2_k se denomina **plano afín**.
Para $n = 3$, A^3_k se denomina **espacio afín**.

Definición 1.35. (Conjunto Algebraico)
Un conjunto algebraico afín sobre A^n_k es un conjunto de la forma:

$$V(S) = \{(a_1, \ldots, a_n) \in A^n_k : f(a_1, \ldots, a_n) = 0, \ \forall f \in S\}, \text{ donde } S \subseteq k[X_1, \ldots, X_n] \setminus \{k\}.$$

Propiedad 1.36. Sea S un subconjunto de $k[X_1, \ldots, X_n]$, tenemos:

1. $V(S) = V(I)$, donde I es un ideal generado por S.
2. Si $(I_\lambda)_\lambda$ una familia de ideales de $k[X_1, \ldots, X_n]$ entonces
$$V\left(\sum_\lambda I_\lambda\right) = \bigcap_\lambda V(I_\lambda).$$
3. Si $I \subseteq J$ entonces $V(J) \subseteq V(I)$.
4. Si I, J son ideales de $k[X_1, \ldots, X_n]$ entonces
$$V(I \cdot J) = V(\{f.g : f \in I, g \in J\}) = V(I) \cup V(J).$$
5. $V(0) = A^n_k$, $V(1) = \emptyset$.
6. $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$.

De las propiedades anteriores, se puede observar que los conjuntos algebraicos afines, son conjuntos cerrados de una topología sobre k^n. Estos conjuntos son de la forma $V(I)$, esta topología se denomina topología de Zariski.

Definición 1.37. (Ideales asociados a conjuntos de A^n_k)
Sea $X \subseteq A^n_k$ un conjunto. El siguiente conjunto

$$I(X) = \{f \in k[X_1, \ldots, X_n] : f(x) = 0, \ \forall x \in X\}$$

es un ideal de $k[X_1, \ldots, X_n]$.

Definición 1.38. Un conjunto algebraico $V \neq \emptyset$ en A^n_k es reducible, si existen conjuntos algebraicos $V_1, V_2 \subsetneq V$ tal que $V = V_1 \cup V_2$.
Los conjuntos que no son reducibles se denominan irreducibles.

Propiedad 1.39. Sea X una curva plana dada por $f(X, Y) = 0$ con $f \in k[X, Y]$. Diremos que X es irreducible sobre k, si f es un polinomio irreducible en el anillo $k[X, Y]$, y además $V(f)$ es infinito.

Diremos también que X es absolutamente irreducible, o geométricamente irreducible, si f es irreducible en $\bar{k}[X, Y]$, donde $\bar{k}$ es la clausura algebraica de k

Ejemplo 1.40. El polinomio $F = Y^2 + X^2(X-1)^2$ es irreducible en $R[X, Y]$, pero $V(F) = \{(0, 0), (1, 0)\}$ es reducible en R^2, pues

$$V(F) = V(Y, X(X-1)) = V(Y) \cup V(X(X-1)) = V(Y, X) \cup V(Y, X-1).$$

Notemos que $F = (Y + iX(X-1))(Y - iX(X-1))$ en $C[X, Y]$ lo que muestra que F es reducible en $C[X, Y]$.

Proposición 1.41. Un conjunto algebraico V es irreducible si y solo si $\mathbf{I}(V)$ es un ideal primo.

Prueba. La demostración se encuentra en [FW69, pág 15] y también en [1]. □

Las siguientes propiedades muestran la relación entre ideales y conjuntos algebraicos.

Propiedad 1.42.

1. Si $X \to Y \subseteq A_k^n$ entonces $\mathbf{I}(Y) \to \mathbf{I}(X)$.
2. $\mathbf{I}(\emptyset) = k[X_1, \ldots, X_n]$ y $\mathbf{I}(A_k^n) = (0)$ siempre que k es un cuerpo infinito.
3. $S \to \mathbf{I}(V(S))$, para $S \to k[X_1, \ldots, X_n]$ y $X \to V(\mathbf{I}(X))$ para $X \to A_k^n$.
4. $\mathbf{I}(X)$ es un ideal radical, para $X \to k[X_1, \ldots, X_n]$.
5. $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

Prueba. La demostración se puede ver en [dlPM07]. □

Definición 1.43. Un subconjunto $X \to A_k^2$ es una curva algebraica afín o simplemente una curva, si existe un polinomio no constante $f \in k[X, Y]$ tal que $X = V(f)$.

Ejemplo 1.44. Sea $f(X, Y) = X^2 - Y^2 - 1 = 0$ (una cónica), sobre el cuerpo $k = Z_3$. Se desea calcular el conjunto

$$V(f) = \{(a_1, a_2) : \ f(a_1, a_2) = 0\}.$$

Para a_2 hay solo tres posibilidades 0, 1 y 2, veamos: $a_2 = 0 \Longrightarrow a_1 = 1$ ó $a_1 = 2$. Si $a_2 = 1$ ó $a_2 = 2$ no existe a_1 tal que $f(a_1, a_2) = 0$, por lo tanto $V(f) = \{(1, 0), (2, 0)\}$.

[1] Introducción a la geometría algebraica de Maximiliano Riddick, Paula Vizzarri

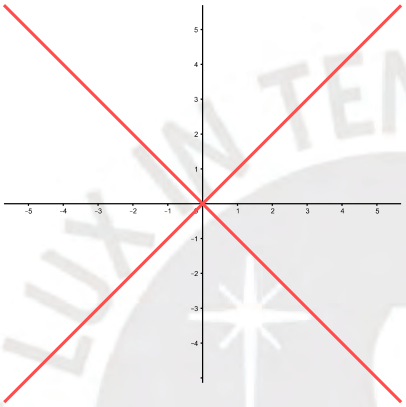
Ejemplos 1.45. Algunas curvas planas afines:

a) Los ceros del polinomio lineal $f(X, Y) = aX + bY + c$ con $(a, b) \neq (0, 0)$ forman una línea afín.

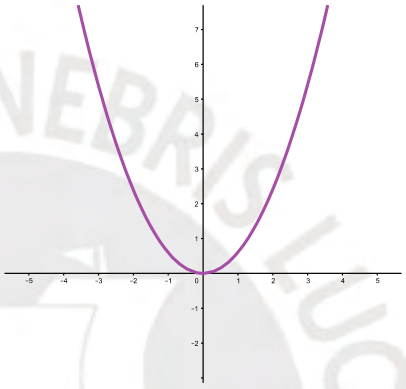
b) El conjunto de los ceros de un polinomio cuadrático

$$f(X, Y) = aX^2 + bXY + cY^2 + dX + eY + g, \qquad a, b, c, d, e, g \in k; (a, b, c) \neq (0, 0, 0)$$

es llamado curva cuadrática.

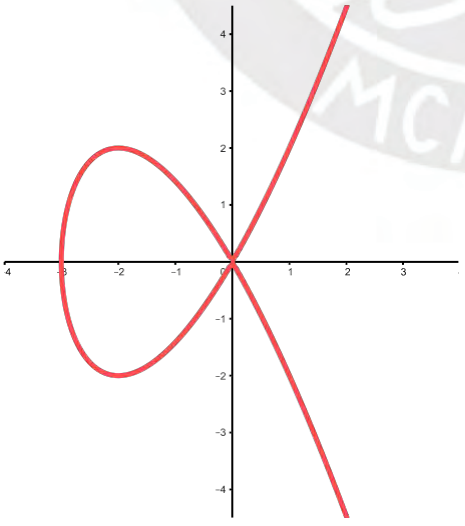


(a) $Y^2 - X^2 = 0$
Par de líneas

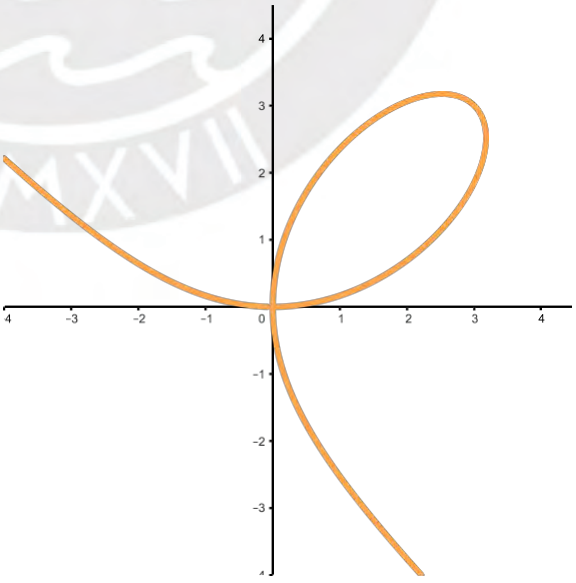


(b) $Y - aX^2 = 0;\ a > 0$
Parabóla

c) El conjunto de los ceros de un polinomio de grado 3 es llamado curva cúbica.

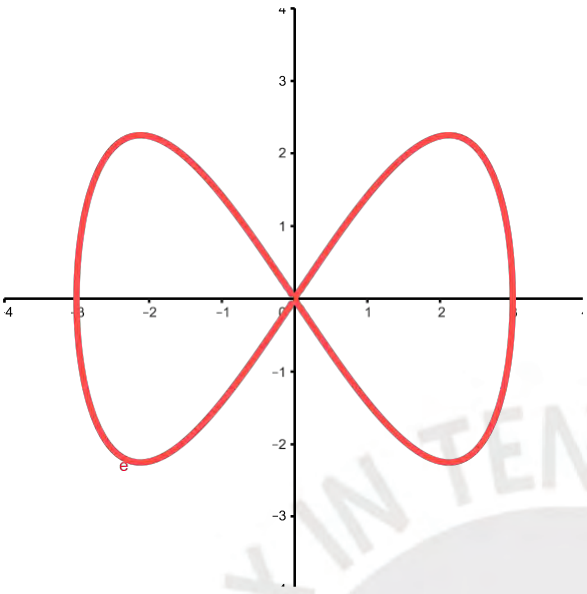


(c) $Y^2 - X^3 - X^2 = 0$
cúbica de Tschirnhausen

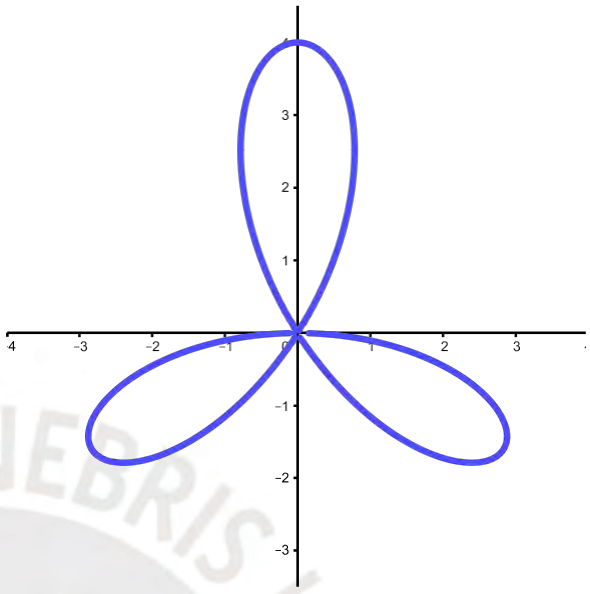


(d) $X^3 + Y^3 - 3aXY = 0;\ a > 0$
Folium de Descartes

d) El conjunto de los ceros de un polinomio de grado 4 es llamado curva cuártica.



(e) $X^2(1-X^2)-Y^2=0$
Lemniscate de Bernoulli



(f) $(X^2+Y^2)^2+3X^2Y-Y^3=0;\ a>0$
Rosa de tres hojas

Ejemplo 1.46. Consideremos la curva Hermitiana $X: f = X^{q+1} + Y^{q+1} + 1 = 0$, donde $q = p^2$, siendo p primo. Observe que f puede ser expresado como $f = a_0 + a_{q+1}Y^{q+1}$, con $a_{q+1} = 1$ y $a_0 = 1 + X^{q+1} \in k[X]$.
Si $\bar{k}$ es un cuerpo de caracter´ıstica $p = 2$, entonces:

$$a_0 = X^{q+1} + 1 = X^{q+1} - 1 = (X-1)^{q} X^i.$$

Aplicamos el criterio de Eisenstein [2]. Notemos que $(X-1)$ divide a a_0, pero no a a_{q+1} y $(X-1)^2$ no divide a a_0, por lo tanto f es absolutamente irreducible.
Si $\bar{k}$ no es un cuerpo de caracter´ıstica 2, entonces existe un r tal que $q = 2r-1$, as´ı:

$$a_0 = X^{q+1} + 1 = X^{2r} + 1 = (X^r+1)(X^r-1) = (X^r+1)(X-1)^{r-1} X^i.$$

[2]Sea R un DFU con cuerpo de fracciones F y sea $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$. Supongamos que existe $p \in R$ primo tal que:

(i) $p \nmid a_n$ y, $p|a_i$ para $i = 0, 1, \ldots, n-1$.

(ii) $p^2 \nmid a_0$.

Entonces, $P(X)$ es irreducible en $F[X]$ (como consecuencia también lo es en $R[X]$).

Nuevamente, aplicamos el criterio de Eisenstein. Se tiene que $(X-1)$ divide a a_0, pero no a a_{q+1} y $(X-1)^2$ no divide a a_0, por lo tanto f es absolutamente irreducible.

Ejemplo 1.47. Sea X una curva, dada por $f = X^2 + Y^2 - 3XY$, esta curva es irreducible en $Q[X, Y]$. Pero es reducible sobre $Q(\sqrt{5})[X, Y]$, puesto que

$$X^2 + Y^2 - 3XY = \left(X - \frac{3}{2}Y + \frac{\sqrt{5}}{2}Y\right)\left(X - \frac{3}{2}Y - \frac{\sqrt{5}}{2}Y\right).$$

Curvas proyectivas

La geometría proyectiva ha tenido su mayor desarrollo en el siglo XIX y al principio del siglo XX. Consiste en homogenizar las curvas afines agregando puntos en el infinito, ver [BK12].

Definición 1.48. Diremos que un polinomio $F \in k[X_0, X_1, \ldots, X_n]$ es homogéneo de grado d, si todos sus monomios tienen grado d.

Ejemplo 1.49. Ejemplos de polinomios homogéneos
$F(X_0, X_1, X_2) = X_1^2 - 5X_0X_2$.
$G(X_0, X_1) = X_0^4 + 4X_0^3X_1 - 3X_1^4$.
$H(X_0, X_1, X_2) = X_1 - 3X_2 - 5X_0$.

Proposición 1.50. Dado un polinomio $F \in k[X_0, X_1, \ldots, X_n]$ homogéneo de grado d entonces se cumple que:

$$F(\lambda X_0, \ldots, \lambda X_n) = \lambda^d F(X_0, \ldots, X_n)$$

en $k[X_0, X_1, \ldots, X_n]$ con $\lambda \in k^*$. (k es un cuerpo algebraicamente cerrado).

Observación 1.51. Hay que tener presente que lo contrario no es cierto, puesto que $\lambda \in k$ depende del cuerpo k, por ejemplo, si consideremos $k = Z_p$, y el polinomio

$$F[X] = X^p - X \in k[X].$$

Es evidente que no es homogéneo, pero cumple que $F(\lambda X) = \lambda^p F(x)$.

Corolario 1.52. Si k es un cuerpo infinito, $F \in k[X_0, \ldots, X_n]$ es homogéneo de grado d si y solo si para cada $\lambda \in k^*$ se cumple

$$F(\lambda X_0, \ldots, \lambda X_n) = \lambda^d F(X_0, \ldots, X_n).$$

Definición 1.53. El espacio proyectivo, $P^n(k)$, se define como

$$P^n_k := \frac{A^{n+1}_k - \{0\}}{\sim} = \{[x_0 : \cdots : x_n] : (x_0, \ldots, x_n) \in A^{n+1}_k - \{0\}$$

con la relación de equivalencia $(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n)$, donde $\lambda \in k^*$.

Ejemplo 1.54. Veamos:

- Los puntos $[1 : 2 : 3]$ y $[2 : 4 : 6]$ representan la misma coordenada en P^2_k, pues $(1, 2, 3) \sim (\lambda \cdot 1, \lambda \cdot 2, \lambda \cdot 3)$, donde $\lambda = 2$, es decir, $[2 : 4 : 6] = [1 : 2 : 3]$.
- $[x_0 : x_1 : x_2] = 1\left[\frac{x_1}{x_0} : \frac{x_2}{x_0}\right]$, para $x_0 \neq 0$ en P^2_k
- $[x^0_0 : x^1_1] = 1\left[\frac{x_1}{x_0}\right]$, para $x_0 \neq 0$ en P^1_k

En general, observemos para $x_i \neq 0$

$$[x_0 : \cdots : x_i : \cdots : x_n] = \left[\frac{x_0}{x_i} : \cdots : 1 : \cdots : \frac{x_n}{x_i}\right]$$

$$P^n_k = \{[x_0 : \cdots : x_n] : x_n \neq 0\} \cup \{[x_0 : \cdots : x_{n-1} : 0] : (x_0, \ldots, x_{n-1}) \in A^n_k - \{0\}\}$$

$$P^n_k = \underbrace{\{[x_0 : \cdots : x_{n-1} : 1]\}}_{A^k_n \text{ finito}} \cup \underbrace{\{[x_0 : \cdots : x_{n-1} : 0] : (x_0, \ldots, x_{n-1}) \in A^n_k - \{0\}\}}_{P^{n-1}_k \text{ infinito}}$$

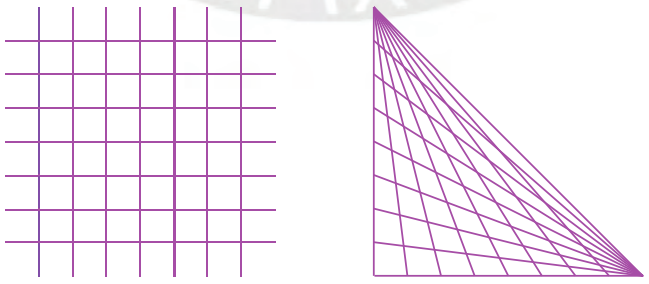
Para $n = 1$,

$$P^1_k = \{[x_0 : x_1] : (x_0, x_1) \in A^2_k - \{0\}\} = \underbrace{\{[x_0 : 1]\}}_{A^1_k} \cup \underbrace{\{[x_0 : 0] : x_0 = 0\}}_{=[1:0]=1}$$

denominado línea proyectiva sobre el cuerpo k.

Para $n = 2$, $P^2_k = \underbrace{\{[x_0 : x_1 : 1]\}}_{A^2_k} \cup \underbrace{\{[x_0 : x_1 : 0] : (x_0, x_1) \in A^2_k - \{0\}\}}_{P^1_k}$

A este último se le denomina plano proyectivo sobre un cuerpo k, que consiste de todas las lineas en k^3 que pasan por el origen.



Plano proyectivo real

Ejemplo 1.55. Si $k = R$, a P^2_k se denomina plano proyectivo real. Es el conjunto de todas las rectas en R^3 que pasan a través del origen $(0, 0, 0)$.

Podemos afirmar que:

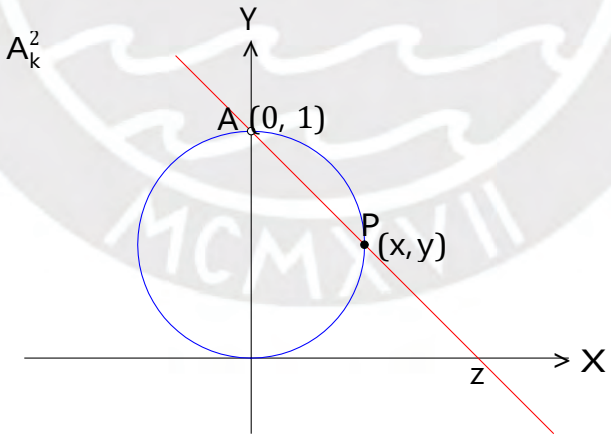
1. Un elemento de P^n_k (llamado un punto), es definido por el conjunto de todas las líneas que pasan a través de $(0, 0, \ldots, 0) \in A^{n+1}_k$.
2. El origen $[0 : \cdots : 0]$ no está definido en P^n_k.
3. A cada punto de P^n_k le corresponde $[x_0 : \cdots : x_n]$ con no todos los $x_i = 0$.
4. Cualquier punto $[x_0 : x_1 : \cdots : x_n] \in P^n_k$ determina una única línea en A^{n+1}_k, dada por $[x_0 : x_1 : \cdots : x_n] = \{(Lx_0, Lx_1, \ldots, Lx_n) : L \in k^*\}$.
5. Hay una biyección que hace corresponder a cada punto del proyectivo de la forma $[1 : x_1 : x_2 : \cdots : x_n] \in P^n_k$ un punto $(x_1, x_2, \cdots, x_n)$ del afín A^n_k.

Para una extensión finita F de k, se tiene el conjunto

$$P^n(F) = \{[x_0, x_1, \ldots, x_n] \in P^n : x_i \in F \text{ para } i = 0, 1, \ldots, n\},$$

denominado F-racional.

Ejemplo 1.56. Sea $S = \{(x, y) \in R^2 : x^2 + y^2 - y = 0\}$. Si P es cualquier punto de S distinto de $A = (0, 1) \in S$,

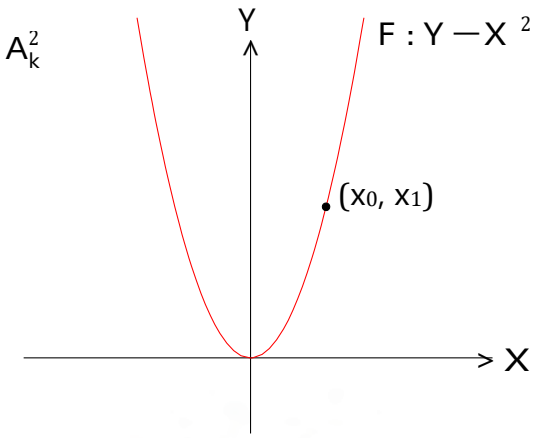


es claro del gráfico que

$$x^2 = y - y^2 \Longrightarrow \frac{x}{y} = \frac{1 - y}{x} = \frac{1}{z},$$

tomemos la coordenada proyectiva de P como $[z : zx]$, donde z es la abscisa del punto en el cual la recta AP intersecta al eje X, y z es cualquier número real no nulo. Para la coordenada proyectiva de A tomemos $[0 : z]$, con $z \neq 0$.

Ejemplo 1.57. Consideremos en el plano afín la curva X: $F = Y - X^2$,



Consideremos $(x_0, x_1) \in X$, es claro que cumple $x_0^2 = x_1$. Vamos a ver la expresión de X en P^2_k:

$$P^2_k = \{[x_0 : x_1 : 1]\} \cup \{[x_0 : x_1 : 0] : (x_0, x_1) \in A^2_k \setminus \{0\}\}.$$

$\{[x_0 : x_1 : 1]\} \simeq A^2_k$, $\{[x_0 : x_1 : 0] : (x_0, x_1) \in A^2_k \setminus \{0\}\} \simeq P^1_k$

Podemos cambiar el abierto del afín A^2_k, considerando $(x_0, x_1) \in A^2_k \setminus \{0\}$,

$$\begin{cases} x_1 = \frac{1}{y_1} \\ x_0 = \frac{y_0}{y_1} \end{cases} \Rightarrow \quad x_1 = x_0^2, \quad \frac{1}{y_1} = \frac{y_0^2}{y_1^2} \Longrightarrow y_1 = y_0^2$$

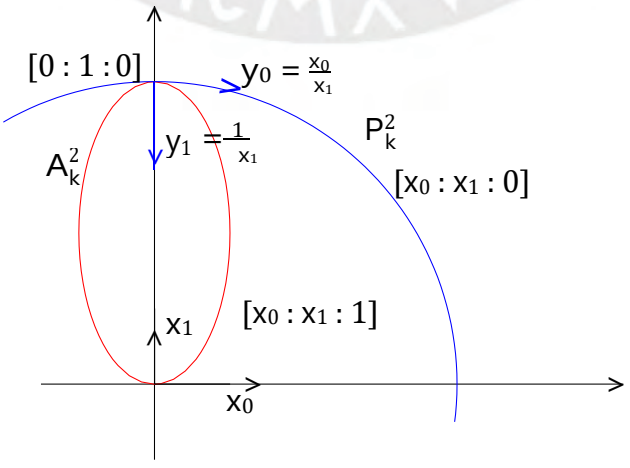
Podemos observar que $(y_0, y_1) \in X$ distinto de $(0, 0)$.

Si consideramos en el proyectivo P^2_k un punto de la curva $[x_0 : x_1 : 1]$, para $x_1 \neq 0$

$$[x_0 : x_1 : 1] = \left[\frac{x_0}{x_1} : 1 : \frac{1}{x_1}\right] = [y_0 : 1 : y_1],$$

tenemos $[y_0 : 1 : y_1]$, para $y_1 \neq 0$ representa al mismo punto de la curva en el proyectivo.

Representemos el gráfico de la curva X en el plano proyectivo.



La curva en el proyectivo, sería $F^{\sim}: ZY - X^2 = 0$.

Observación 1.58. Notemos que $P^2_k = U_0 \cup U_1 \cup U_2$, donde

$$U_i = \{(x_0, x_1, x_2) \in A^2_k - \{0\} : x_i \neq 0\}.$$

Lema 1.59. Sea $f \in k[X_1, \ldots, X_n]$ un polinomio no homogéneo (no constante) de grado d, entonces todos los polinomios homogéneos cuyo deshomogeneneizado (respecto a X_0) es f son de la forma $X_0^a F(X_0, X_1, \ldots, X_n)$, para algún $a \leq 0$, tal que:

$$F(X_0, X_1, \ldots, X_n) = X_0^d f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right).$$

Ejemplo 1.60. Consideremos el siguiente polinomio

$$f(X_1, X_2, X_3) = X_1^2 X_2 X_3 - 4X_2 X_3^2 + 5X_2^4 - 2X_1 + 7.$$

Notamos que su grado es 4, aunque no es un polinomio homogéneo, calculemos:

$$f\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}, \frac{X_3}{X_0}\right) = \frac{X_1^2}{X_0^2}\frac{X_2}{X_0}\frac{X_3}{X_0} - 4\frac{X_2}{X_0}\frac{X_3^2}{X_0^2} + 5\frac{X_2^4}{X_0^4} - 2\frac{X_1}{X_0} + 7.$$

Multiplicamos por X_0^4, obtenemos:

$$F(X_0, X_1, X_2, X_3) = X_0^4 f\left(\frac{X_1}{X_0}, \ldots, \frac{X_3}{X_0}\right) = X_1^2 X_2 X_3 - 4X_2 X_3^2 X_0 + 5X_2^4 - 2X_1 X_0^3 + 7X_0^4,$$

un polinomio homogéneo de grado 4.

Observación 1.61. Todo polinomio no homogéneo de grado d, $f(X_1, \ldots, X_n)$ siempre se puede separar como suma de polinomios homogéneos.

Ejemplo 1.62. Dado el polinomio no homogéneo de grado 3,

$$f(X_1, X_2, X_3) = X_1^3 - 2X_2 X_3^2 + X_2^2 - X_1 X_3 + 5X_1 + 2X_3 + 7X_1 X_2 X_3 - 3,$$

podemos expresarlo como:

$$f(X_1, X_2, X_3) = \underbrace{X^3 - 2X_2 X^2 + 7X_1 X_2 X_3}_{f_3} + \underbrace{X^2 - X_1 X_3}_{f_2} + \underbrace{5X_1 + 2X_3}_{f_1} + \underbrace{-3}_{f_0},$$

donde f_i son polinomios de grado i.

Prueba. Del lema 1.59

Consideremos el polinomio f, expresado como suma

$$f(X_1,\ldots,X_n) = f_0(X_1,\ldots,X_n) + f_1(X_1,\ldots,X_n) + \cdots + f_d(X_1,\ldots,X_n),$$

donde cada f_i son polinomios homogéneos de grado i $(i = 0, \ldots, d)$, observe que:

$$X_0^d f_i\left(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}\right) = X_0^{d-i}\left[X_0^i f_i\left(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}\right)\right] = X_0^{d-i}\underbrace{f_i(X_1,\ldots,X_n)}_{\text{grado } i},$$

es un polinomio de grado d para cada i, luego,

$$X_0^d f\left(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}\right) = X_0^d \underbrace{f_0\left(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}\right)}_{\text{grado } d} + \cdots + X_0^d \underbrace{f_d\left(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}\right)}_{\text{grado } d}.$$

Obtenemos así un polinomio homogéneo de grado d,

$$F(X_0,X_1,\ldots,X_n) = X_0^d f\left(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}\right) \in k[X_0,X_1,\ldots,X_n].$$

Por lo tanto, considerando $e \leq d$, podemos encontrar todos los polinomios homogéneos que homogenizan al polinomio f, como $X_0^a F(X_0, X_1, \ldots, X_n)$, donde $a = e - d$. □

Observación 1.63. Este resultado nos dice que todo polinomio no homogéneo f de n indeterminadas se puede homogenizar como un polinomio homogéneo F de $n + 1$ indeterminadas.

Lema 1.64. Sea $f \in k[X, Y]$ y $F \in k[X, Y, Z]$ la homogenización de f. Entonces

$$f \text{ es irreducible} \iff F \text{ es irreducible}$$

Prueba. Mostraremos utilizando su equivalencia lógica, es decir,

$$f \text{ es reducible} \iff F \text{ es reducible}$$

Consideremos F reducible, por lo tanto existen polinomios H, G tal que $F = H.G$, como F es homogéneo se tiene que H, G son homogéneos.
Deshomogenizando se tiene

$$f = F(X, Y, 1) = H(X, Y, 1).G(X, Y, 1) = h \cdot g.$$

Por lo tanto f es reducible, de manera similar se demuestra lo recíproco. □

Lema 1.65. *(Relación de Euler)*

Si $F \in k[X_1, X_2, \ldots, X_n]$ es un polinomio homogéneo de grado d entonces se cumple la siguiente relación

$$X_1\frac{\partial F}{\partial X_1}(X_1,\ldots,X_n) + \ldots + X_n\frac{\partial F}{\partial X_n}(X_1,\ldots,X_n) = dF(X_1,\ldots,X_n).$$

Puntos racionales sobre una curva algebraica

Sea X una curva proyectiva contenida en P^n_k, definida sobre k. Un punto sobre X es un punto racional (sobre k) si posee coordenadas $[x_0 : x_1 : \cdots : x_n] \in P^n_k$ tal que $x_0, x_1, \ldots, x_n \in k$.

Ejemplo 1.66. Sea $f(X, Y) = Y - X^2$. La curva plana afín $X : f = 0$, consiste de los puntos (t, t^2) para $t \in k$. La clausura proyectiva de X es $\hat{X} : F = YZ - X^2$ cuyos puntos son de la forma $[t : t^2 : 1]$, con un único punto al infinito $[0 : 1 : 0]$. Sobre F_2, los únicos puntos racionales de $\hat{X}$ son $[0 : 1 : 0]$, $[1 : 1 : 1]$ y $[0 : 0 : 1]$.

Ejemplo 1.67. Sea $f(X, Y) = Y^2 - X^3$. La clausura proyectiva de $X : f = 0$ es $\hat{X} : F = ZY^2 - X^3$ y tiene un único punto al infinito $[0 : 1 : 0]$. Sobre F_2, los puntos racionales de $\hat{X}$ son $[0 : 1 : 0]$, $[0 : 0 : 1]$ y $[1 : 1 : 1]$.

Ejemplo 1.68. Dada la curva afín $X : f = x^{q+1} + y^{q+1} + 1$. La clausura proyectiva es definida por $\hat{X} : F = X^{q+1} + Y^{q+1} + Z^{q+1}$ tiene $q + 1$ puntos en el infinito, basta tomar $Z = 0$ e $Y = 1$, por lo que quedaría $X^{q+1} + 1 = 0$, que tiene $q + 1$ raíces $\beta_1, \beta_2, \ldots, \beta_{q+1}$, de donde $[\beta_i : 1 : 0] \in \hat{X}$ son los puntos al infinito sobre k, otros puntos racionales sobre k podrían ser $[0 : 1 : w_i] \in \hat{X}$.

Curvas no singulares

Definición 1.69. Sea $X \subseteq A^n_k$ una curva afín, y sean $f_1, f_2, \ldots, f_m \in \bar{k}[X_1, \ldots, X_n]$ el conjunto de generadores del ideal $I(X)$. Entonces X se dirá no singular (regular, o suave) en un punto P de X si la matriz Jacobiana $m \times n$ en P tiene rango $n - 1$.

$$\left(\frac{\partial f_i}{\partial x_j}(P) \right)_{1 \leq i \leq m,\ 1 \leq j \leq n}$$

En otro caso, se dirá X es una curva singular en P.

Definición 1.70. (Punto Singular)
Sea X una curva afín o proyectiva dada por $F = 0$ y P un punto cualesquiera de la curva, diremos que X es una curva singular en P o que P es un punto singular, si todas las derivadas parciales se anulan en P.

La curva X es no singular en P, o P es un punto no singular (simple) de X, si al menos una de las derivadas anteriores es no nula, en este caso diremos que existe una línea tangente en P.

Ejemplo 1.71. La curva plana dada por $f(X, Y) = Y^2 - X$ no tiene puntos singulares, en efecto:

$f_X = -1$

$f_Y = 2Y$

Es evidente que al menos una de las derivadas anteriores es no nula.

Ejemplo 1.72. Consideremos la curva $H = Y^q Z - Y Z^q + X^{q+1} - X^2 Z^{q-1}$ sobre F_q, veamos que es no singular.

Busquemos los puntos singulares de la curva, para ello tenemos:

$H_X = X^q - 2XZ^{q-1} = 0$

$H_Y = -Z^q = 0$

$H_Z = Y^q + X^2 Z^{q-2} = 0$

Después de resolver el sistema se tiene el único punto $[0 : 0 : 0]$, pero no es punto del plano proyectivo.

Por lo tanto H es una curva no singular.

Ejemplo 1.73. La curva $F = Y^2 Z - X^3 + XZ^2$ no tiene puntos singulares. En efecto,

$F_X = -3X^2 + Z^2 = 0$

$F_Y = 2YZ = 0$

$F_Z = Y^2 + 2XZ = 0$

Tenemos dos casos para $YZ = 0$, por lo que:

Si $Y = 0$ entonces $XZ = 0$ y $-3X^2 + Z^2 = 0$, si $X = 0$ o $Z = 0$ tendríamos que $[0 : 0 : 0]$ lo cual no es posible.

Si $Z = 0$ entonces $-3X^2 = 0$ y $Y^2 = 0$, si $X = 0$ e $Y = 0$ tendríamos que $[0 : 0 : 0]$ lo cual no es posible.

Por lo tanto F no tiene puntos singulares.

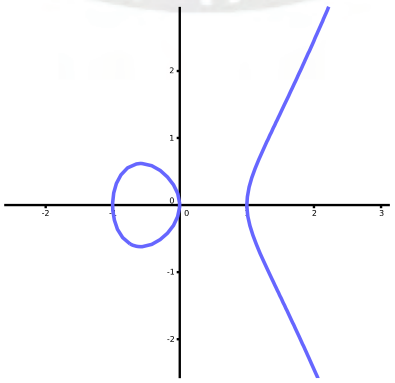


Figura 1.1: Curva afín $Y^2 = X^3 - X$

Ejemplo 1.74. Consideremos la curva afín $Y^2 = X^3 - X$ y sus puntos racionales sobre k, son $P_1 = [0 : 0 : 1]$, $P_2 = [1 : 0 : 1]$, $P_3 = [-1 : 0 : 1]$ y $P_1 = [0 : 1 : 0]$.
Vamos a determinar si los puntos P_i son simples o no, y determinamos la(s) recta(s) tangente en cada punto.
Para el punto $P_1 = [0 : 0 : 1] \in P^2_k$, en el plano afín $A^2_k : f(X, Y) = Y^2 - X^3 + X$ el $(0, 0)$ es un punto simple con recta tangente $X = 0$.
Para el punto $P_2 = [1 : 0 : 1] \in P^2_k$, en el plano afín $A^2_k : f(X, Y) = Y^2 - X^3 + X$ el $(1, 0)$ es un punto simple con recta tangente $X = 1$, para determinar la recta tangente realizaremos el desarrollo de Taylor alrededor de P_2.

$$f(X, Y) = -2(X - 1) - 3(X - 1)^2 + Y^2 - (X - 1)^3.$$

Para el punto $P_3 = [-1 : 0 : 1] \in P^2_k$, en el plano afín $A^2_k : f(X, Y) = Y^2 - X^3 + X$ en $(-1, 0)$ es un punto simple con recta tangente $X = -1$, para determinar la recta tangente realizaremos el desarrollo de Taylor alrededor de P_3.

$$f(X, Y) = -2(X + 1) + 3(X + 1)^2 + Y^2 - (X + 1)^3.$$

Observación 1.75. (Desarrollo de Taylor)
Sea $f \in k[X, Y]$ un polinomio de grado d y P un punto de coordenadas (a, b), consideramos su desarrollo de Taylor alrededor de P como:

$$f = \sum_{k=0}^{d} \sum_{u+v=k} \frac{1}{u!v!} \frac{\partial^k f(P)}{\partial X^u \partial Y^v} (X - a)^u (Y - b)^v = P_0 + P_1 + \cdots + P_d,$$

donde P_i es un polinomio homogéneo de grado i.

Definición 1.76. (Multiplicidad de una curva)
El orden o multiplicidad de una curva $X \to_k A^2$, $X : f = 0$ en el punto P, se define como:

$$\mathrm{ord}_P(f) = \min\{i \in \{0, 1, \ldots, d\} : f_i(P) \neq 0\}.$$

Donde d es el grado del polinomio f, f_i es el polinomio homogéneo contenido en f de grado i.
También dicho entero se denomina orden de X en P, se denota $\mathrm{ord}_P(X)$.

Ejemplo 1.77. Dada la curva $F = Y^2Z - X^3 - X^2Z$, donde dos de sus puntos son: $P_1 = [0 : 0 : 1]$ y $P_2 = [-1 : 0 : 1]$.

Para $p_1 = (0, 0)$, tenemos su curva afín $f = \underbrace{Y^2}_{f_2} - \underbrace{X^2}_{f_2} + \underbrace{X^3}_{f_3}$, así $ord_{p_1}(f) = 2$.

Para $p_2 = (-1 : 0)$, tenemos su curva afín

$$f = \underbrace{-(X+1)}_{f_1} + \underbrace{Y^2 + 2(X+1)^2}_{f_2} - \underbrace{(X+1)^3}_{f_3}.$$

Así, el punto $p_2 = (-1, 0)$ tiene $ord_{p_2}(f) = 1$.

1.3 Cuerpo de funciones racionales

Un cuerpo de funciones gobierna los aspectos del álgebra abstracta de una curva algebraica. En esta seccion, presentaremos aspectos básicos de un cuerpo de funciones.

El cuerpo de fracciones de $k[X_1, \cdots, X_n]$ se indica por $k(X_1, \cdots, X_n)$ y se denomina cuerpo de las funciones racionales de n variables sobre k.

$$k(X_1, \ldots, X_n) := \left\{ \frac{f}{g} : f, g \in k[X_1, \ldots, X_n], g \neq 0 \right\}.$$

Cuerpo de funciones racionales sobre un conjunto algebraico

Sea X una curva, $V = V(X) \dashrightarrow P^n_k$ un conjunto algebraico, además consideremos $I = \mathbf{I}(V)$ ideal homogéneo.

Estudiaremos el cuerpo de funciones asociados a una curva algebraica, por lo que el cuerpo no necesariamente es algebraicamente cerrado.

Definición 1.78. (Anillo de coordenadas)

Dada la curva plana $X : f = 0$ sobre el cuerpo algebraicamente cerrado F, definimos el anillo de coordenadas como:

$$F[X] := \frac{F[x, y]}{(f)}.$$

Si consideramos X sobre k (k cuerpo algebraicamente cerrado), entonces

$$k[X] := \frac{k[x, y]}{I}.$$

Definición 1.79. (Anillo Local)

Sea V definido como antes, definimos el anillo local en $p \in V$ como

$$\mathcal{O}_p(V) := \left\{ \frac{f}{g} : \quad g(p) \neq 0 \right\}.$$

Consideramos el campo de funciones racionales sobre V

$$k(V) = \left\{ \frac{F}{G} : F, G \in k[V] \text{ polinomios homogéneos del mismo grado, } G \neq 0 \right\}.$$

Observación 1.80. Sea X una curva, $V = V(X) \subseteq P^n_k$ un conjunto algebraico, entonces

$$k[V] \subseteq O_p(V) \subseteq k(V).$$

Definición 1.81. (Puntos no singulares, curva no singular)
Un punto $p \in V$ es no singular, si para toda $f \in k[C]$, o bien $f \in O_p(V)$ o $\frac{1}{f} \in O_p(V)$.

Proposición 1.82. Sea $C : f(X, Y) = 0$ una curva afín, y sea $P = (a, b) \in C$. Si $f_Y(P) = 0$ entonces $\frac{Y - b}{X - a} \in O_P(C)$.

Prueba. En efecto, consideremos, sin pérdida de generalidad que, $P = (0, 0)$, entonces podemos escribir

$$f(X, Y) = cX + dY + X^2 f_1(X) + Y^2 f_2(Y) + XY f_3(X, Y), \qquad (1.1)$$

para algún $c, d \in k$ y $f_1, f_2, f_3 \in k[X, Y]$.
Calculemos f_X, f_Y:
$f_X(X, Y) = c + 2X f_1(X) + X^2 f_1'(X) + Y f_3(X, Y) + XY f_3'(X, Y) \longrightarrow f_X(P) = c,$
$f_Y(X, Y) = d + 2Y f_2(X) + Y^2 f_2'(X) + X f_3(X, Y) + XY f_3'(X, Y) \longrightarrow f_Y(P) = d.$
Por condición del enunciado, $f_Y(P) = d \neq 0$, reagrupando convenientemente de (1.1)

$$Y(d + Y f_2(Y) + X f_3(X, Y)) = f(X, Y) - X(c + X f_1(X)).$$

Como $f \not\equiv 0$ en P, se tiene

$$\frac{Y}{X} = \frac{-c - X f_1(X)}{d + Y f_2(Y) + X f_3(X, Y)} \in O_P(C).$$

□

Valoración discreta

Proposición 1.83. Sea R un dominio que no es un cuerpo. Son equivalentes:

a) R es noetheriano, local y el ideal maximal es principal.

b) $\exists t \in R$ irreducible tal que $\forall z \in R, z \neq 0$ existe una unidad $u \in R$ y $n \in Z_{\geq 0}$ tal que $z = ut^n$.

Prueba. Sea $m \to R$ ideal maximal y sea $m = (t)$, $t \in R$, luego t es irreducible. Sea $z \in R$, $z \neq 0$

- Si $z \in R$ es una unidad, $z = zt^0$.
- Si $z \in R$ no es una unidad tenemos que $z \in m$ entonces $z = z_1 t$, $z_1 \in R$, como R es Noetheriano $\exists n$ tal que $z = z_n t^n$, con $z_n \in R$ una unidad.

Recíprocamente, considere $m = (t) \to R$ ideal maximal, por lo tanto todo elemento $z \in R$ que no es unidad está en m, esto es, $z = ut^n$, $n > 0$, $z \in m$. □

Definición 1.84. (Anillo de valoración discreta)
Un dominio R que satisface cualquiera de las condiciones de la proposición 1.83 es llamado anillo de valoración discreta. El elemento $t \in R$ es llamado parámetro de uniformización de R y n es llamado orden de $z \in R$.

Ejemplo 1.85. Sea $k[[X]]$ anillo de series de potencias

$$m = \{f \in k[[X]] : f(0) = 0\},$$

donde $f = a_0 + a_1X + a_2X^2 + \cdots$, así $f(0) = a_0$, por lo tanto

$$f = X^n(a_n + a_{n+1}X + \cdots), \quad a_n \neq 0 \text{ y } a_0 = a_1 = \cdots = a_{n-1} = 0.$$

Definimos la aplicación sobreyectiva,

$$\begin{aligned} \nu : k[[X]] &\to \mathbb{Z} \\ f &\mapsto \nu(f) = n. \end{aligned}$$

Definición 1.86. Una valoración discreta para un cuerpo k, es una función sobreyectiva, $\nu : k^* \to \mathbb{Z} \cup \{\infty\}$ que satisface las siguientes condiciones:

1. $\nu(z) = \infty$ si y solo si $z = 0$.
2. $\nu(yz) = \nu(y) + \nu(z)$ para todo $y, z \in k^*$.
3. $\nu(y + z) \geq \min(\nu(y), \nu(z))$ para todo $y, z \in k^*$.

Proposición 1.87. Sea R un dominio entero y K su cuerpo de fracciones. Si R es un anillo de valoración discreta, entonces su ideal maximal m es el conjunto $\{x \in K : \nu(x) > 0\}$.

Prueba. Veamos que $\nu(1) = 0$, en efecto, dado que $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$, luego $\nu(1) = 0$. Además, $0 = \nu(1) = \nu(x \cdot x^{-1}) = \nu(x) + \nu(x^{-1})$, luego $\nu(x^{-1}) = -\nu(x)$.

Ahora como R es un anillo de valoración discreta de ν, se tiene que todos los elementos de R, cumplen $\nu(x) \leq 0$. Así, si u es una unidad de R, se cumple que $\nu(u) \leq 0$ y $\nu(u^{-1}) = -\nu(u) \leq 0$, es decir, todas las unidades de R cumplen que $\nu(u) = 0$.

Esto es, si $\nu(x) = 0$ con $x \in R$, se tiene que $\nu(x^{-1}) = 0$, en efecto, $0 = \nu(1) = \nu(x \cdot x^{-1}) = \nu(x) + \nu(x^{-1})$, entonces $\nu(x^{-1}) = 0$, como R es un anillo de valoración se tiene que $x^{-1} \in R$, esto es x es una unidad de R.

Si definimos $m = \{x \in K : \nu(x) > 0\}$, entonces $R - m$ solo tiene unidades de R, por lo tanto m es un ideal maximal. □

Sea R un anillo de valoración discreta y K su cuerpo cociente. Todo elemento $z \in K$ se puede expresar en función del parámetro uniformizador de la siguiente manera. Si

$$z = \frac{x}{y}, \text{ con } x, y \in R, y \text{ es no nulo,}$$

$$z = \frac{u_1 t^n}{u_2 t^m} = u t^r, \quad r = n - m \in Z,$$

donde r es llamado orden del elemento z. Si $r > 0$, entonces z es un cero, y si $r < 0$, z es un polo.

$K = \{z \in K : \text{ord}(z) \in Z\}$.

$R = \{z \in K / \text{ord}(z) \leq 0\}$.

$m = \{z \in K / \text{ord}(z) > 0\}$.

De la proposición 1.82 se tiene el siguiente teorema.

Teorema 1.88. Sea $C : f(X, Y) = 0$ una curva afín y sea $P = (a, b) \in C$. Si $f_Y(P) \neq 0$ entonces $X - a$ es un parámetro de uniformización en P, y si $f_X(P) \neq 0$, entonces $Y - b$ es un parámetro de uniformización en P. Además P es singular si y solo si $f_X(P) = f_Y(P) = 0$.

Ejemplo 1.89. Consideremos la curva Hermitiana $C : F = X^5 + Y^5 + Z^5 = 0$ definida sobre F_2. Claramente C es no singular, consideremos la curva afín $A^2_{F_2}$ $f = x^5 + y^5 + 1$ y como

$$f_x = 5x^4 = 0 \wedge f_y = 5y^4 = 0 \Longrightarrow P = (0, 0).$$

Pero $P = [0 : 0 : 1] \in C$. En $Q = (0, 1) \in C$, notamos que $f_y(Q) = \frac{\partial f}{\partial y}(Q) \neq 0$ entonces x es un parámetro de uniformización para Q, sea $y + 1 = \frac{x^5}{1 + y + y^2 + y^3 + y^4} = ux^5$,

donde $u = \frac{1}{1 + y + y^2 + y^3 + y^4}$ es una unidad en $O_Q(C)$,

por lo tanto $\mathrm{ord}_Q(y + 1) = \mathrm{ord}_Q\left(\frac{1}{1+y+y^2+y^3+y^4}\right) + \mathrm{ord}_Q(x^5) = 5\mathrm{ord}_Q(x) = 5$.

Ejemplo 1.90. Consideremos la curva proyectiva plana no singular

$$C : f = YZ - X^2 = 0.$$

El único punto en el infinito es $[0 : 1 : 0] \in C$. Examinaremos el orden de $Z/X \in k(C)$. Sea $x_y = X/Y$ y $z_y = Z/Y$, tenemos $f(x_y, 1, z_y) = z_y - x_y^2$,

$$\frac{\partial f}{\partial z_y} = 1 \neq 0,$$

sea $Q = (0, 0)$. Así x_y es el parámetro de uniformización de $O_Q(C)$. Tenemos $z_y/x_y = x_y^2/x_y = x_y$.

Así, $\mathrm{ord}_Q(Z/X) = \mathrm{ord}_Q(z_y/x_y) = \mathrm{ord}_Q(x_y) = 1$ implica $\mathrm{ord}_Q(X/Z) = -1$, es evidente dado que el único polo de X/Z debe ser $Z = 0$ y este se dá para Q que es el único punto con $Z = 0$.

Ejemplo 1.91. Consideremos la misma curva C del ejemplo anterior (1.90) definido sobre F_2. Claramente $P = [1 : 1 : 1] \in C$.

Consideremos $f(x_z, y_z, 1) = y_z - x^2$, donde $y_z = Y/Z$ y $x_z = X/Z$,

$$\frac{\partial f}{\partial y_z} = 1 = 0,$$

sea $p = (1, 1)$, así $x_z - 1$ es el parámetro de uniformización de $O_p(C)$, veamos $y_z - 1 = x_z^2 - 1 = (x_z - 1)^2$, por lo que $\mathrm{ord}_p(y_z - 1) = 2\mathrm{ord}_p(x_z - 1) = 2$.

Si hubiéramos tomado $f(1, y_x, z_x) = y_x z_x - 1$, donde $y_x = Y/X$ y $z_x = Z/X$,

$$\frac{\partial f}{\partial y_x}(p) = 1 \neq 0,$$

entonces $z_x - 1$ es el parámetro de uniformización,

$$y_x - 1 = \frac{1 - z_x}{z_x} \Longrightarrow \mathrm{ord}_p(y_x - 1) = \mathrm{ord}_p(1 - z_x) - \mathrm{ord}_p(z_x) = 1 - 0 = 1.$$

Ejemplo 1.92. Consideremos la curva $C : F = Y^2Z - X^3 - XZ^2 = 0$. Es evidente que $P = [0 : 0 : 1] \in C$ es un punto no singular, pues

$$\frac{\partial F}{\partial X}(P) \neq 0.$$

Consideramos la curva $f(x, y) = y^2 - x^3 - x$, donde $x = X/Z$ e $y = Y/Z$. Aquí y es el parámetro de uniformización, por lo que $ord_{(0,0)}(y) = 1$. Sea $p = (0, 0)$, veamos que $ord_p(x) = 2$,

$$x = \frac{y^2}{x^2 + 1} \Longrightarrow ord_p(x) = ord_p(y^2) = 2ord_p(y) = 2.$$

Notemos que $\frac{1}{x^2+1}$ es una unidad en $O_p(C)$.

Veamos también que $ord_p(2y^2 - x) = 2$. En efecto, como $2x^2 + 1$ es una unidad en $O_p(C)$ y además $2y^2 - x = 2x^3 + x$, se tiene

$$ord_p(2y^2 - x) = ord_p(x) = 2.$$

Ejemplo 1.93. Consideramos la curva $X : F = X^3 + Y^3 + Z^3 = 0$ sobre el cuerpo F_2, es claro que $Q = [0 : 1 : 1] \in X$, además

$$F_X(Q) = 0, F_Y(Q) \neq 0, F_Z(Q) \neq 0.$$

Entonces $t = \frac{X}{Z}$ es un parámetro local de $O_Q(X)$, por lo tanto $ord_{(1,1)}(t) = 1$.

- Si consideramos la función $f = \frac{X}{Y+Z} \in F_2(X)$, es evidente que Q es el único polo para f, por lo que buscaremos una forma equivalente cerca a Q. Se tiene

$$f = \frac{X}{Y + Z} = \frac{X(Y^2 + YZ + Z^2)}{Y^3 + Z^3} = t^{-2}\left(\frac{Y^2 + YZ + Z^2}{Z^2}\right).$$

Notemos que el segundo factor es una unidad en $O_Q(X)$, por lo que $ord_{(1,1)}(f) = -2$, es decir, f tiene un polo de orden 2 en Q.

- Si consideramos la función $g = \frac{Y}{Y+Z}$, es evidente que Q es el único polo para g, por lo que buscaremos una forma equivalente cerca a Q. Se tiene

$$g = \frac{Y}{Y + Z} = \frac{Y(Y^2 + YZ + Z^2)}{Y^3 + Z^3} = t^{-3}\left(\frac{Y^3 + Y^2Z + YZ^2}{Z^3}\right).$$

Notemos que el segundo factor es una unidad en $O_Q(X)$, por lo que $ord_{(1,1)}(g) = -3$, es decir, g tiene un polo de orden 3 en Q.

Números de intersección

Definición 1.94. Sean F y G dos curvas planas y $P \in A^2$ un punto. Definimos el número de intersección de F y G en P como

$$I_P(F,G) := \dim_k \mathcal{O}_P(A^2)/\langle F, G\rangle.$$

Definición 1.95. Diremos que las curvas F y G se cortan en un sentido estricto en P, si F y G no tienen ninguna componente común que pase por P.

Definición 1.96. Diremos que las curvas F y G se cortan transversalmente en P, si el punto P es simple en las dos curvas F y G, y la recta tangente de F en P es distinta a la recta tangente de G en P.

Teorema 1.97. Dadas F, G curvas planas afines. Entonces existe una única multiplicidad de intersección $I_P(F,G)$, que satisface las siguientes propiedades:

i) $I_P(F,G) = I_P(G,F)$.

ii) Si F y G se cortan en el sentido estricto en P, entonces $I_P(F,G)$ es un entero no negativo; y si tienen una componente en común, $I_P(F,G) = \infty$.

iii) $I_P(F,G) = 0$ si y sólo si $P \notin F \cap G$.

iv) Si T es un cambio de coordenadas afín en A^2 y $T(P) = Q$, entonces $I_P(F,G) = I_Q(F^T, G^T)$.

v) $I_P(F,G) \geq m_P(F)m_P(G)$, la igualdad ocurre si F y G no tienen líneas tangentes en común en P.

vi) Si $F = \prod F_i^{r_i}$ y $G = \prod G_j^{s_j}$, entonces $I_P(F,G) = \sum_{i,j} r_i s_j I_P(F_i, G_j)$.

vii) $I_P(F,G) = I_P(F, G + AF)$ para cualquier $A \in k[X,Y]$.

Prueba. La prueba se puede ver en [Ful08, pág 37]. □

Ejemplo 1.98. El siguiente ejemplo fue tomado del libro de Fulton [Ful08, pág 40]. Vamos a calcular $I_P(F,G)$ considerando $F = (X^2+Y^2)^2 + 3X^2Y - Y^3$, $G = (X^2+Y^2)^3 - 4X^2Y^2$ y el punto $P = [0:0:1] \in P^2_k$ o simplemente

$P = (0, 0) \in A^2_k$ Podemos deshacernos de la peor parte de G, reemplazando G por $G - (X^2 + Y^2)F$,

$$\begin{aligned} G - (X^2 + Y^2)F &= (X^2 + Y^2)^3 - 4X^2Y^2 - (X^2 + Y^2)[(X^2 + Y^2)^2 + 3X^2Y - Y^3] \\ &= -4X^2Y^2 - (X^2 + Y^2)(3X^2Y - Y^3) \\ &= Y(X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y \\ &= YE, \end{aligned}$$

donde $E = (X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y$. Reemplazamos E por E + 3F,

$$\begin{aligned} E + 3F &= (X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y + 3((X^2 + Y^2)^2 + 3X^2Y - Y^3) \\ &= (X^2 + Y^2)[Y^2 - 3X^2 + 3(X^2 + Y^2)] + 5X^2Y - 3Y^3 \\ &= Y[5X^2 - 3Y^2 + 4Y(X^2 + Y^2)] \\ &= YH, \end{aligned}$$

donde $H = 5X^2 - 3Y^2 + 4Y(X^2 + Y^2)$. Entonces

$$I_P(F, G) = I_P(F, YE) = I_P(F, Y^2H) = 2I_P(F, Y) + I_P(F, H).$$

Por otro lado, $I_P(F, Y) = I_P(X^4, Y) = 4$ y $I_P(F, H) = m_P(F)m_P(H) = 6$, por consiguiente se tiene $I_P(F, G) = 14$.

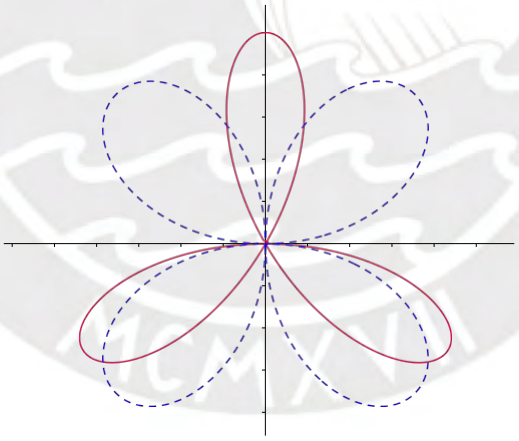


Figura 1.2: Las curvas afines F y G

Ejemplo 1.99. Sea X la cuártica de Klein $F = X^3Y + Y^3Z + Z^3X$, consideremos tres puntos $P = [0 : 0 : 1]$, $Q = [0 : 1 : 0]$ y $R = [1 : 0 : 0]$.

Sea L_1 la recta con ecuación $X = 0$. Es evidente que L_1 intersecta a X en los puntos P y Q, veamos

Tomamos la curva X el afın $Z = 1$, $f = X^3Y + Y^3 + X$, consideremos el punto

$P = (0, 0)$ en el afín, entonces

$I_P(X, L_1) = I_P(Y^3, X) = 3$, es decir, la multiplicidad de X con L_1 es 3.

Tomamos la curva X el afín $Y = 1$, $f = X^3 + Z + Z^3X$, consideremos el punto $Q = (0, 0)$ en el afín, entonces

$I_Q(X, L_1) = I_Q(Z, X) = 1$, es decir, L_1 no es tangente a X en el punto Q.

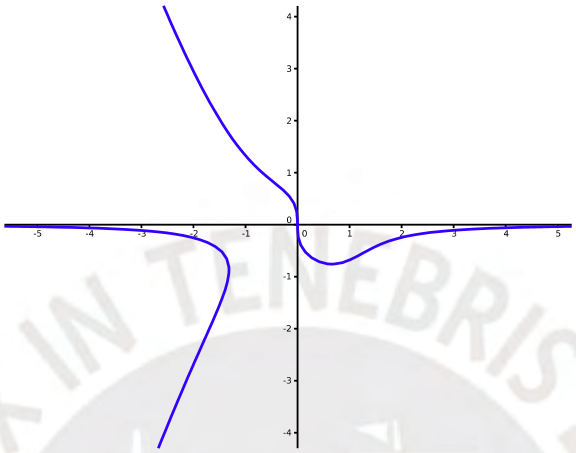


Figura 1.3: Las curvas afín de F

Teorema 1.100. *(Teorema de Bézout)*

Sean F y G dos curvas proyectivas de grados m y n respectivamente. Asumimos que F y G no tienen componentes en común. Entonces

$$\sum_{P} I_P(F, G) = mn.$$

Prueba. La demostración se puede ver en [Wal50, pág 59]. □

Una aplicación del teorema de Bézout nos muestra que si F es una curva irreducible de grado n y m_P es la multiplicidad de F en P, entonces

$$\sum_{P \in \mathbb{P}^2} \frac{m_P(m_P - 1)}{2} \leq \frac{n(n-1)}{2}.$$

El siguiente teorema mejora aún más la cota.

Teorema 1.101. Si F es una curva irreducible de grado n y m_P es la multiplicidad de F en P. Entonces

$$\sum_{P \in \mathbb{P}^2} \frac{m_P(m_P - 1)}{2} \leq \frac{(n-1)(n-2)}{2}.$$

Prueba. La demostración se puede ver en [Wal50, pág 65]. □

Capítulo 2

Teorema de Riemann-Roch

En este capítulo estudiamos el espacio y Teorema de Riemann-Roch, propuesto por Bernhard Riemann y su estudiante Gustav Roch en 1857. El teorema de Riemann-Roch es un teorema que relaciona el análisis complejo y la geometría algebraica con el género topológico, para el cálculo de la dimensión del espacio de funciones meroformas. Estos juegan un rol muy importante en el desarrollo del capítulo 3, al momento de construir los códigos lineales, el cálculo del rango y la distancia mínima de este tipo de códigos.

2.1 Divisor de una curva algebraica

Vamos a ver la importancia de los conceptos mencionados en el capítulo anterior, por ejemplo, veremos como una curva proyectiva regular puede ser recuperada desde su cuerpo de fracciones racionales, esto es, los puntos de la curva se recuperaran a partir de las valoraciones en el cuerpo.

Hay que tener presente que todo polinomio $f \in k[X]$, está determinado de manera única (salvo una constante), por sus ceros (raíces), contando sus multiplicidades $\nu_1, \ldots, \nu_n \in A_k$, es decir,

$$f(X) = c(X - x_1)^{\nu_1} \ldots (X - x_n)^{\nu_n}.$$

De igual manera, las funciones racionales $f(X) = \dfrac{P(X)}{Q(X)}$, con $P, Q \in k[X]$, están determinadas de manera única, por sus ceros y polos, es decir,

$$f(X) = c\frac{(X - x_1)^{\nu_1} \ldots (X - x_n)^{\nu_n}}{(X - y_1)^{\varnothing_1} \ldots (X - y_m)^{\varnothing_m}}. \tag{2.1}$$

Donde $x_1, \ldots, x_n$ representan los ceros, con sus multiplicidades $\lambda_1, \ldots, \lambda_n$, y $y_1, \ldots, y_m$ representan los polos con sus multiplicidades $\emptyset_1, \ldots, \emptyset_m$, respectivamente.

Definición 2.1. (Divisor de una curva)
Consideremos X una curva proyectiva no singular (irreducible). Un divisor de X es una suma formal

$$D = Div(X) = \sum_{P \in X} n_P P, \; n_P \in Z,$$

donde $n_P = 0$ para casi todo P.

Observación 2.2. Dado $z \in k(X)$ no nulo,

$$(z) = div(z) = \sum_{Q \in X} ord_Q(z).Q, \quad ord_Q(z) \in Z.$$

Denotaremos por:
$(z)_0 = \sum_{Q \in X} ord_Q(z).Q$, el divisor de ceros de z. $(ord_Q(z) \leq 0)$
$(z)_1 = \sum_{Q \in X} -ord_Q(z).Q$, el divisor de polos de z. $(ord_Q(z) < 0)$
$(z) = (z)_0 - (z)_1$, es denominado divisor principal.
Entonces $div(z) = (z)_0 - (z)_1$.
Además es fácil notar que:
$div(z.z') = div(z) + div(z')$
$div(z^{-1}) = -div(z)$

Ejemplo 2.3. Del ejemplo 1.99, tenemos la cuártica de Klein $F = X^3Y + Y^3Z + Z^3X$, y los puntos $P = [0 : 0 : 1]$, $Q = [0 : 1 : 0]$ y $R = [1 : 0 : 0]$.
En el ejemplo observamos que la recta L_1 intersecta a X, de aquí $X \cdot L_1 = 3P + Q$.
Sea L_2 la recta con ecuación $Y = 0$, de manera similar se obtiene $X \cdot L_2 = 3R + P$.
Sea L_3 la recta con ecuación $Z = 0$, de manera similar se obtiene $X \cdot L_3 = 3Q + R$.
Adicionalmente, podemos considerar: $x = X/Z$ e $y = Y/Z$, por lo que tenemos:
$div(x) = X \cdot L_1 - X \cdot L_3 = 3P + Q - (3Q + R) = 3P - 2Q - R$.
$div(y) = X \cdot L_2 - X \cdot L_3 = 3R + P - (3Q + R) = 2R + P - 3Q$.

Ejemplo 2.4. Sea $X = P^1_k$ la recta proyectiva. Sea $\varphi \in k(X)$, es decir, $\varphi = \frac{P}{Q}$, donde P y Q son dos polinomios homogéneos en $k[X, Y]$ del mismo grado. Sin perdida de generalidad, podemos suponer que P, Q no tienen factores en común, de manera

similar que en la ecuación (2.1), sean

$$P(X,Y) = X^{\alpha}Y^{\beta}\prod_i (X - a_iY)^{r_i},$$
$$Q(X,Y) = X^{\gamma}Y^{\delta}\prod_j (X - b_jY)^{s_j}.$$

Donde $\alpha, \beta, \gamma, \delta, r_i, s_j$ son enteros no negativos, $a_i, b_j \in k$ y $a_i \neq b_j$ para todo par (i, j). Como P y Q no tienen factores en común, entonces $\alpha\gamma = 0$ y $\beta\delta = 0$.

Para el punto racional $P_1 = [0 : 1]$ se tiene

$$\varphi = \frac{X^{\alpha}\prod_i (X - a_i)^{r_i}}{X^{\gamma}\prod_j (X - b_j)^{s_j}} = X^{\alpha-\gamma}\prod (X - a_i)^{r_i}(X - b_j)^{-s_j}, \quad \text{el único divisor es } X$$

Para el punto racional $P_2 = [1 : 0]$ se tiene

$$\varphi = \frac{Y^{\beta}\prod_i (1 - a_iY)^{r_i}}{Y^{\delta}\prod_j (1 - b_jY)^{s_j}} = Y^{\beta-\delta}\prod (1 - a_iY)^{r_i}(1 - b_jY)^{-s_j}, \quad \text{el único divisor es } Y$$

Para los puntos racionales $P_3 = [a_i : 1]$ se tiene

$$\varphi = \frac{X^{\alpha}\prod_i (X - a_i)^{r_i}}{X^{\gamma}\prod_j (X - b_j)^{s_j}} = X^{\alpha-\gamma}\prod (X - a_i)^{r_i}(X - b_j)^{-s_j}, \quad \text{el único divisor es } X - a_i$$

Para los puntos racionales $P_4 = [1 : b_j]$ se tiene

$$\varphi = \frac{Y^{\beta}\prod_i (1 - a_iY)^{r_i}}{Y^{\delta}\prod_j (1 - b_jY)^{s_j}} = Y^{\beta-\delta}\prod (1 - a_iY)^{r_i}(1 - b_jY)^{-s_j}, \quad \text{el único divisor es } 1 - b_jY$$

Por lo tanto,

$$\operatorname{div}(\varphi) = (\alpha - \gamma)[0 : 1] + (\beta - \delta)[1 : 0] + \sum_i r_i\,[a_i : 1] - \sum_j s_j\,[1 : b_j].$$

Ejemplo 2.5. Dada la cúbica irreducible $X : F = Y^2Z - X(X - Z)(X - LZ)$, $L \in k$, $L \neq 0, 1$. Sean $x = X/Z$, $y = Y/Z$, $z = \frac{1}{x} \in k(X)$, donde X, Y, Z son las coordenadas homogéneas de P^2_k

- Calculemos $\operatorname{div}(x)$

Para $X = 0$, tenemos $Y^2Z = 0$, con puntos racionales:

$[0 : 0 : 1]$ de multiplicidad $m = 2$ y $[0 : 1 : 0]$ de multiplicidad $m = 1$. Luego el divisor de los ceros de X es:

$$(x)_0 = 2[0 : 0 : 1] + [0 : 1 : 0].$$

Para $Z = 0$ tenemos $-X^3 = 0$, con punto racional: $[0 : 1 : 0]$ de multiplicidad $m = 3$. Luego,

$$(x)_1 = 3[0 : 1 : 0].$$

Por lo tanto, $\text{div}(x) = (x)_0 - (x)_1 = 2[0:0:1] - 2[0:1:0]$.

- Calculemos div(y)

Para $Y = 0$ tenemos $X(X - Z)(X - LZ) = 0$, con puntos racionales:

$[0:0:1]$ de multiplicidad $m = 1$, $[1:0:1]$ de multiplicidad $m = 1$ y $[L:0:1]$ de multiplicidad $m = 1$. Luego el divisor de ceros de Y es:

$$(y)_0 = [0:0:1] + [1:0:1] + [L:0:1]$$

Para $Z = 0$ tenemos $-X^3 = 0$, el punto racional es:

$[0:1:0]$ de multiplicidad $m = 3$.

$$(y)_1 = 3[0:1:0]$$

Por lo tanto, $\text{div}(y) = (y)_0 - (y)_1 = [0:0:1] + [1:0:1] + [L:0:1] - 3[0:1:0]$.

Ejemplo 2.6. Dada la curva irreducible $X : F = X^3 + Y^3 - Z^3 = 0$ definida en P^2_C. Vamos a calcular el divisor de $f = \frac{Y}{X}$.

Pasando al afín A^2_C, y calculando el divisor de f

$\text{div}(f) = [1:0:1] + [\omega:0:1] + [\omega^2:0:1] - [0:1:1] - [0:\omega:1] - [0:\omega^2:1]$, donde $\omega = e^{2\pi i/3}$ es la raíz primitiva de la raíz cúbica de la unidad.

Definición 2.7. (Grado de un divisor)

Dado D un divisor, definimos el grado del divisor D, como la suma de los coeficientes n_P, es decir

$$\text{grad}(D) = \text{grad}\left(\sum_{P \in X} n_P P\right) = \sum_{P \in X} n_P.$$

Ejemplo 2.8. De los ejemplos 2.4, 2.6, tenemos:

$\text{grad}(\omega) = (\infty - \sqrt{}) + (\emptyset - y) + \sum_i \omega_i - \sum_j \mu_j$; y

$\text{grad}(f) = 0$.

Un divisor $D = \sum_{P \in X} n_P P$, se dirá efectivo o positivo, cuando todos los $n_P \leq 0$ y se denota por $D \leq 0$.

Definición 2.9. Consideremos $D = \sum_{P \in X} n_P P$, definimos el soporte de D como

$$\text{supp}(D) = \{P \in P^n_k : n_p \neq 0\}.$$

Definición 2.10. Consideremos $D = \sum_{P \in X} n_P P$ y $D' = \sum_{P \in X} m_P P$. Diremos que $D \leq D'$ si y solo si $n_p \leq m_P$.

Ejemplo 2.11. Dada la cúbica $F = Y^2Z - X^3 - 2XZ^2 + 3Z^3 = 0$, dos puntos racionales de grado uno serán $P_1 = [2 : 3 : 1]$ y $P_2 = [1 : 0 : 1]$, entonces $D = 5P_1 - 7P_2$ es un divisor de la curva (cualquier combinación lineal de ellos es un divisor de la curva). Además, el soporte de D es $supp(D) = \{P_1, P_2\}$.

Proposición 2.12. Sea $z, z' \in K(X)$, ambos no nulos. Entonces $div(z) = div(z')$ si y sólo si $z = Lz'$ para algún $L \in K$.

Proposición 2.13. Dos divisores D, D' son linealmente equivalentes $D \sim D'$, si $D' = D + div(z)$ para algún $z \in K(X)$.

2.2 Espacio de Riemann-Roch

A partir de esta sección $K = K(X)$, representa el espacio de funciones.

Definición 2.14. (Espacio de Riemann-Roch)
Sea X una curva regular y $Div(X)$ el conjunto de divisores de X.
Si $D = \sum_{P \in X} n_P P$ es un divisor de X, el espacio de Riemann-Roch asociado a D, denotado por $L(D)$, se define como:

$$L(D) := \{f \in K^* / div(f) + D \geq 0\} \cup \{0\},$$

o equivalentemente, se puede expresar como:

$$L(D) := \{f \in K^* / ord_P(f) \geq -n_P, \quad \forall P \in X\} \cup \{0\}.$$

La dimensión de $L(D)$ es denotado por $l(D)$.

Ejemplo 2.15. Del ejemplo 2.5, en la curva $X : F = Y^2Z - X(X - Z)(X - LZ)$, tenemos $ord_Q(x) = -2$, $ord_Q(y) = -3$ y $l(n(z)_0) = 2n$, donde $Q = [0 : 1 : 0]$. En efecto, consideremos el afín $Y = 1$,

$$f = z_y - x_y(x_y - z_y)(x_y - Lz_y), \text{ donde } x_y = \frac{X}{Y} \; y \; z_y = \frac{Z}{Y}.$$

Es claro observar que $x_y = \frac{x}{y}$ y $z_y = y^{-1}$.
Como $f_{z_y}(Q) = 1 \neq 0$, se tiene que x_y es parámetro de uniformización, por lo que $ord_Q(x_y) = 1$.

$$z_y = \frac{1}{1 + (L+1)x_y^2 - Lx_y z_y} x_y^3, \text{ donde } \frac{1}{1 + (L+1)x_y^2 - Lx_y z_y} \in \mathcal{O}_Q(X)$$

luego, $ord_Q(z_y) = 3ord_Q(x_y) = 3$. Así,
$ord_Q(z_y) = ord_Q(y^{-1}) = 3$, entonces $ord_Q(y) = -3$.
$ord_Q(x_y) = ord_Q(x) - ord_Q(y) = 1$, entonces $ord_Q(x) = -2$.
$I_Q(F, X) = I_Q(Z - X(X - Z)(X - LZ), X) = I_Q(Z, X) = 1$
$I_Q(F, Z) = I_Q(Z - X(X - Z)(X - LZ), Z) = I_Q(-X^3, Z) = 3$, Q es un punto de inflexión.
Consideremos, $D = n(z)_0 = 2nQ$, como $L(D) = \{f \in K^* / div(f) \leq -2n.Q\}$, además

$$ord_Q(x^i y^j) = i.ord_Q(x) + j.ord_Q(y) = -2i - 3j \leq -2n. \qquad (2.2)$$

De la relación $y^2 = x(x-1)(x-L)$, todo $f \in K[x, y]$, es decir, $L(D) \to K[x, y]$ tiene un representante cuyos monomios son de la forma x^i e $x^i y$.
Para $j = 0$, en la ecuación (2.2), se tiene $0 \leq 2i \leq 2n$, obtenemos $n + 1$ valores posibles, $1, x, x^2, \ldots, x^n$.
Para $j = 1$, en la ecuación (2.2), se tiene $0 \leq 2i + 3 \leq 2n$, obtenemos $n - 1$ valores posibles, $y, xy, \ldots, x^{n-2}y$. Una base para $L(D)$ es,

$$\{1, x, x^2, \ldots, x^n, y, xy, \ldots, x^{n-2}y\} \text{ — } l(D) = 2n.$$

Proposición 2.16. El espacio de Riemann-Roch $L(D)$ es un espacio vectorial sobre el cuerpo k.

Prueba. Dados $f_1, f_2 \in L(D)$ entonces se cumple $div(f_i) + D \leq 0$, $i = 1, 2$ esto es,

$$ord_P(f_i) + n_P \leq 0; \quad \forall P \in X, \ i = 1, 2,$$

donde $D = \sum_{P \in X} n_P.P$.

Luego, $ord_P(f_1 + f_2) = n \leq \min\{ord_P(f_1), ord_P(f_2)\} \leq -n_P$.
$f_i = t^{n_i}u_i$, con $u_i \in O_P^*(X)$, $i = 1, 2$ ht$i = m$, entonces
$f_1 + f_2 = t^{n_1}u_1 + t^{n_2}u_2 = t^n u, \quad n \leq \min\{n_1, n_2\}$.
Como,

$$t^{n_1}u_1 = t^{n_1}(L_1 + \cdots), \quad L_1 = 0,$$
$$t^{n_2}u_2 = t^{n_2}(L_2 + \cdots), \quad L_2 = 0.$$

Por lo tanto, $div(f_1 + f_2) + D > 0$, esto implica $f_1 + f_2 \in L(D)$.
Dado $L \in k^*$, $f \in L(D)$,

$$div(Lf) + D = div(f) + D > 0, \quad \text{luego } Lf \in L(D).$$

□

Proposición 2.17. $L(D) \neq \{0\} \Leftrightarrow D \sim D'$ para algún $D' \geq 0$.

Prueba. Supongamos que $L(D) \neq \{0\}$. Entonces existe $f \in K^*$ tal que $\operatorname{div}(f) + D \geq 0$, haciendo $D' = \operatorname{div}(f) + D$ y por la proposición 2.13, se tiene $D \sim D'$.

Recíprocamente, si $D \sim D'$ con $D' \geq 0$ entonces existe $f \in K^*$ tal que $-D \leq D' - D = \operatorname{div}(f)$ entonces $f \in L(D)$. □

Proposición 2.18. Si $D \leq D'$ entonces $L(D) \subseteq L(D')$ y

$$\dim_k \frac{L(D')}{L(D)} \leq \operatorname{grad}(D' - D).$$

Prueba. Como $D \leq D'$, entonces $D' = D + P_1 + \cdots + P_s$,

$$L(D) \subseteq L(D + P_1) \subseteq L(D + P_1 + P_2) \subseteq \cdots \subseteq L(D')$$

Afirmación: Sea $L(D) \subseteq L(D + P)$, entonces $\dim_k \left(\frac{L(D+P)}{L(D)} \right) \leq 1$.

En efecto, sea $D = \sum_{P \in X} n_P . P$, consideremos t el parámetro de uniformización en $O_P(X)$. Definamos la aplicación lineal

$$\varphi : L(D + P) \to k$$
$$f \longmapsto \varphi(f) = (t^{n_P + 1} f)(P).$$

Claramente, φ está bien definida, como si $f \in L(D + P)$ entonces $\operatorname{div}(f) + D + P \geq 0$, es decir, $\operatorname{ord}_P(f) \geq -n_P - 1$.

Además, $\operatorname{Nu}(\varphi) = L(D)$, por lo que tenemos

$$\tilde{\varphi} : \frac{L(D + P)}{\operatorname{Nu}(\varphi)} \to \operatorname{Im}(\varphi),$$

de donde, $\dim_k \left(\frac{L(D+P)}{L(D)} \right) \leq \dim_k(\operatorname{Im}(\varphi)) = 1$.

De la afirmación, se tiene $\dim_k \frac{L(D')}{L(D)} \leq \operatorname{grad}(D' - D)$. □

Proposición 2.19. Para cualquier divisor D, existe $D_0 \geq 0$ tal que $l(D) \leq \operatorname{grad}(D_0) + 1$.

Prueba. Por la proposición 2.18,

$$l(D_0) - l(0) = \dim_k \frac{L(D_0)}{L(0)} \leq \operatorname{grad}(D_0).$$

Por otro lado, si $D_0 \leq D$ es trivial. Ahora si $D \leq D_0$ se sigue

$$l(D) \leq l(D_0) \leq \text{grad}(D_0) + 1.$$

□

Proposición 2.20. Sea $x \in K$, $x \notin k$. Sea $Z = (x)_0$ el divisor de los ceros de x, y sea $n = [K, k(x)]$. Entonces

a) $Z = (x)_0$ es un divisor efectivo de grado n.

b) Existe una constante γ tal que $l(r(x)_0) \leq rn - \gamma$ para todo r.

Prueba. La demostración lo puede ver en [FW69, pág. 100]. □

De todo lo anterior, tenemos:

- Si $D = 0$ divisor nulo, entonces $L(0) = k \Rightarrow l(0) = 1$.
- $D \sim D' \Rightarrow l(D) = l(D')$ y $\text{grad}(D) = \text{grad}(D')$.
- para todo $D \leq 0$ tenemos $l(D) \leq \text{grad}(D) + 1$.
- Si $\text{grad}(D) < 0$ entonces $L(D) = \{0\}$ y por lo tanto $l(D) = 0$.
- Si $\text{grad}(D) = 0$ entonces, si D es principal $l(D) = 1$, caso contrario $l(D) = 0$.

Ejemplo 2.21. Sea $X = P^1$ y $t = X_1/X_2 \in K(X)$, donde X_1, X_2 son coordenadas homogéneas de P^1.

- Como $t = X_1/X_2$, tenemos $(t)_0 = [0 : 1]$ y $(t)_1 = [1 : 0]$, luego

$$\text{div}(t) = (t)_0 - (t)_1 = [0 : 1] - [1 : 0].$$

- Consideremos los polinomios homogéneos del mismo grado,

$$f = \prod_{P_i \in P^1} (b_i X_1 - a_i X_2)^{n_i} \quad \text{y} \quad g = \prod_{Q_j \in P^1} (d_j X_1 - c_j X_2)^{m_j}$$

con f y g primos entre sí en $K[X]$.

Observe que $P_i = [a_i : b_i]$ y $Q_j = [c_j : d_j]$ son las raíces de f y g respectivamente, por lo tanto

$$\text{div}(f/g) = \sum_{P_i \in P^1} n_i P_i - \sum_{Q_j \in P^1} m_j Q_j = \sum_{P_i \in P^1} n_i [a_i : b_i] - \sum_{Q_j \in P^1} m_j [c_j : d_j].$$

- El divisor div(f/g) tiene grado cero. En efecto, recordemos que $\frac{f}{g} \in K(X)$ son cocientes de polinomios del mismo grado. Entonces

$$grad(div(f/g)) = grad(f) - grad(g) = 0.$$

- Tenemos que $(t)_0 = [0 : 1]$ son los divisores de ceros de t.
Sea $D = n(t)_0 = n[0 : 1]$,

$$L(D) = \{h \in K(X) \ / \ ord_P(h) \leq -ord_P(D)\}.$$

El único polo de $h \in L(D)$ es $[1 : 0]$ y es de orden a lo más n, luego

$$L(D) = \left\{ h = \frac{F}{X_2^n} \in K(X) \ / \ F \in k[X_1, X_2] \text{ homogéneos de grado } n \right\} \cup \{0\}$$

Consideremos el polinomio homogéneo $F = \sum_{i=0}^{n} a_i X_1^i X_2^{n-i}$, así el espacio L(D) tiene como base al conjunto,

$$1, \frac{X_1}{X_2}, \cdots, \frac{X_1^n}{X_2^n} \xrightarrow{t=X_1/X_2} \{1, t, \cdots, t^n\}.$$

Por lo tanto, $l(D) = n + 1$.

Ejemplo 2.22. En el ejemplo 1.93 vimos que $f = \frac{X}{Y+Z}$ tiene un polo de orden 2 en $Q = [0 : 1 : 1]$, pero la curva $X : X^3 + Y^3 + Z^3 = 0$ tiene otros dos ceros con multiplicidad 1, $P_1 = [0 : \omega : 1]$ y $P_2 = [0 : \omega^2 : 1]$, donde $\omega = e^{\frac{\pi i}{3}}$. Es claro que Q es el único polo, como $f(P_1)$ y $f(P_2)$ están bien definidos, entonces

$$div(f) = P_1 + P_2 - 2Q, \ grad(div(f)) = 0$$

Consideremos $D = 2Q$; como $dim_k(L(D)) = 2$, entonces $\{1, f\}$ es una base para L(D).

Definición 2.23. Sea X una curva algebraica regular, tal que $D \in Div(X)$, definimos:
$\delta(D) = grad(D) - l(D), \ D \in Div(X)$.
$g = máx\{1 + \delta(D) \ / \ D \in Div(X)\}$.

Consideramos $i(D) = g - 1 - \delta(D)$, conocido como el índice de especialidad de D.

Teorema 2.24. *(Teorema de Riemann)*
Sea X una curva algebraica. Existe una constante g tal que $\delta(D) \leq g - 1$ para todos los divisores D.

Prueba. Tenemos:

i. $\delta(0) = \text{grad}(0) - l(0) = -1$, por lo tanto $g \leq 0$, (existe g).

ii. Si $D \sim D'$ entonces $\delta(D) = \delta(D')$.

iii. Si $D \leq D'$ entonces $\delta(D) \leq \delta(D')$.

Sea $x \in K$, $x \notin k$ y sea γ el menor valor entero que verifica la proposición 2.20, existe γ tal que $\delta(rZ) = \text{grad}(rZ) - l(rZ) \leq \gamma$ para todo r, además como $rZ \leq (r+1)Z$, de la parte (iii) $\delta(rZ) \leq \delta((r+1)Z)$, podemos deducir que:

iv. $\delta(rZ) = \gamma$ para todo $r > 0$ suficientemente grande.

v. Para todo divisor D, existe un divisor $D' \sim D$, y un entero $r \leq 0$ tal que $D' \leq rZ$.

Necesitamos probar esta última afirmación, es decir, $D' \leq rZ$, para tal caso consideremos: $Z = \sum_P n_P . P$, $D = \sum_P m_P . P$.

Deseamos probar $D' = D - \text{div}(f)$, es decir, necesitamos probar $m_p - \text{ord}_P(f) \leq r n_P$ para todo P.

Sea $y = x^{-1}$ y $T = \{P \in X \ / \ m_P > 0 \ y \ \text{ord}_P(y) \leq 0\}$.

Consideremos, $f = \prod_{P \in T} (y - y(P))^{m_P}$, tenemos dos casos:

- Si $\text{ord}_P(y) \leq 0$ tenemos:

$$\text{ord}_P(f) \leq m_P \Longrightarrow m_P - \text{ord}_P(f) \leq 0 \leq r n_P,$$

- Si $\text{ord}_P(y) < 0$ entonces $n_P > 0$, por lo tanto:

$$m_P - \text{ord}_P(f) < 0 \leq r n_P,$$

luego para r suficientemente grande se tiene $\delta(D) = \delta(D') \leq \delta(rZ) = \gamma$, bastará considerar para terminar la prueba, $\gamma = g - 1$, por lo tanto, $\delta(D) \leq g - 1$. □

Definición 2.25. (Género de una curva)

El entero no negativo g es denominado género de una curva proyectiva no singular X sobre k;

$$g = \text{máx}\{1 + \delta(D) \ / \ D \in \text{Div}(X)\}.$$

Para más detalles, revisar [LA15], [ASS99].

Observación 2.26. Del teorema 2.24 (teorema de Riemann), $i(D) = 0$ para todo D de grado suficientemente grande, además

$$i(0) = g - 1 - \delta(0) = g - 1 - (-1) = g.$$

La topología ha jugado y juega un rol muy importante en la geometría, y la geometría de las curvas tienen una interpretacion topológica de las mismas, mediante el género. El siguiente resultado, relaciona el género con el grado de una curva.

Teorema 2.27. *(Fórmula de Julius Plücker)*
Si $X : f = 0$ es una curva proyectiva plana irreducible no singular, entonces el genero de X es dado por la fórmula

$$g = \frac{(d-1)(d-2)}{2},$$

donde $d = \text{grad}(f)$.

Prueba. La prueba se puede ver en el libro [ASS99, pág 200]. □

Ejemplo 2.28. Sea $X : F = X^2 - XZ + YZ$ una curva proyectiva irreducible, de grado $d = 2$, es evidente que es una curva no singular, por lo tanto su género es $g = 0$, topológicamente representa una esfera.

Ejemplo 2.29. Consideremos la curva $X : F = Y^2Z - X^3 + XZ^2$, no singular en $P^2(C)$. Por el Teorema 2.27 el género de X es $g = \frac{(3-1)(3-2)}{2} = 1$. Topológicamente $X : F = 0$, representa un toro.

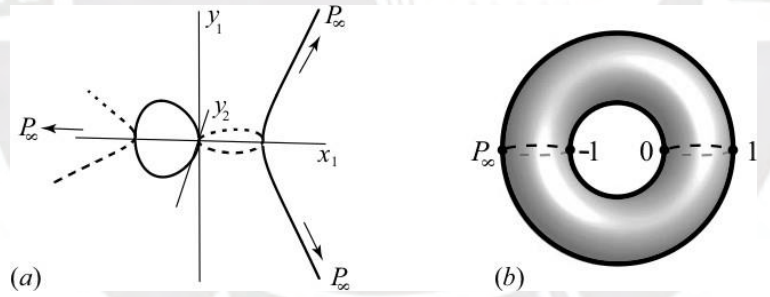


Figura 2.1: Interpretación (a) algebraica, (b) topológica

El siguiente resultado generaliza la fórmula de Julius Plücker del género de una curva $X \dashrightarrow P^2_k$ de grado d.

Teorema 2.30. *(Fórmula de Plücker generalizada)*
Si $X : f = 0$ es una curva proyectiva plana, entonces el género de X es dado por la fórmula

$$g = \frac{(d-1)(d-2)}{2} - \sum_{p_i \in Sing(X)} \frac{r_{p_i}(r_{p_i}-1)}{2}. \tag{2.3}$$

Donde $r_{p_i} \in Z_{>0}$ es la multiplicidad de p_i.

Prueba. Ver detalle de la prueba en [KK92, pág. 86]. □

Ejemplo 2.31. Considere la curva plana $X : F = X^4 + X^2YZ + Y Z^3$, de grado $d = 4$ y singularidad en el punto $P_1 = [0 : 1 : 0]$, de multiplicidad $r_1 = 3$, con tres tangentes distintas $Z = 0$, $X + Yi = 0$ y $X - Yi = 0$ con multiplicidad 1, reemplazando en la fórmula de la ecuación (2.3), tenemos:

$$g = \frac{(4-1)(4-2)}{2} - \frac{3(3-1)}{2} = 0.$$

Divisores canónicos

Consideremos una curva afín suave X en A^2 definida por la ecuación $f(x, y) = 0$, y $P = (a, b)$ un punto en X. Sea T_P la recta tangente a X en P definida por

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0.$$

Consideremos al conjunto $\Omega[X]$ de todas las aplicaciones que están asociadas a cada punto $P \in X$ (un elemento de T_P^*).

Definición 2.32. Un elemento $\omega \in \Omega[X]$ es llamado una forma diferencial regular (en la curva X) si cada punto $P \in X$ tiene una vecindad U tal que en esta vecindad, ω puede ser representada como $\omega = \sum_{i=1}^{n} f_i dg_i$, donde todas las funciones f_i y g_i son regulares en U.

Las formas diferenciales regulares en X forman un $k[X]$-módulo, el cual denotamos por $\Omega(X)$. Este módulo es generado por elementos de df, donde $f \in k[X]$, con las relaciones:

- $d(f + g) = df + dg$.
- $d(fg) = fdg + gdf$.
- $d(c) = 0$, donde $c \in k$.

para una extensión de las formas diferenciales racionales, debemos agregar la relación $d(f/g) = (gdf - fdg)/g^2$.
Consideraremos el par (U, w), donde U es un conjunto afín no vacío y w tiene la forma gdf en U. Diremos que (U, w), (V, Ω) son equivalentes, si $w = \Omega$ en el conjunto $U \cap V$. Una clase de equivalencia por esta relación es llamada una forma diferencial racional.

Sea X una curva proyectiva no singular, K su espacio de funciones. Sea $\Omega = \Omega_k(K)$ el espacio de las diferenciales de K sobre k; los elementos $\omega \in \Omega$ también son denominados diferenciales en X.

Ejemplo 2.33. El ejemplo se ha tomado de [HVLP98, pág. 17]. Consideremos la curva X en P^2 dada por $X^3 + Y^3 + Z^3 = 0$ (con char(k) $\neq 3$), definimos los conjuntos:

$$U_x = \{(x : y : z) \in X : \ y = 0, \ z \neq 0\}$$

$$U_y = \{(x : y : z) \in X : \ x \neq 0, \ z \neq 0\}$$

$$U_z = \{(x : y : z) \in X : \ x \neq 0, \ y \neq 0\}.$$

Como no hay puntos en X con dos coordenadas iguales a cero, entonces U_x, U_y y U_z cubren X. Podemos observar que

$$d\left(\frac{x}{z}\right) = d\left(\frac{y}{z}\right) = \frac{z\,dx - x\,dz}{z^2} = \frac{z\,dy - y\,dz}{z^2}.$$

De aquí, $w := \left(\frac{y}{z}\right)^2 d\left(\frac{x}{y}\right) = \frac{y}{z} d\left(\frac{x}{z}\right) - \frac{x}{z} d\left(\frac{y}{z}\right)$ está en U_x.

No es difícil comprobar las otras dos representaciones:

$$\eta := \left(\frac{z}{x}\right)^2 d\left(\frac{y}{x}\right) \text{ en } U_y, \quad \theta := \left(\frac{x}{y}\right)^2 d\left(\frac{z}{y}\right) \text{ en } U_z.$$

Podemos notar que η y θ coinciden en $U_y \cap U_z$. Consideremos la curva en $U_y \cap U_z$

$$\left(\frac{x}{z}\right)^3 + \left(\frac{y}{z}\right)^3 + 1 = 0 \Longrightarrow \left(\frac{x}{z}\right)^2 d\left(\frac{x}{z}\right) + \left(\frac{y}{z}\right)^2 d\left(\frac{y}{z}\right) = 0.$$

Tengamos presente, $d\left(\frac{z}{x}\right) = -\left(\frac{z}{x}\right)^2 d\left(\frac{x}{z}\right)$ reemplazando en lo anterior se tiene $\eta = \theta$.

Teorema 2.34. El espacio Ω tiene dimensión 1 sobre K; en una vecindad de un punto P con un parámetro local t ($O_P(X)$). Un diferencial w puede ser representado como $w = f\,dt$, donde f es una función racional.

Prueba. Ver detalle de la prueba en [1]. □

Proposición 2.35. Sea K un cuerpo de funciones en una variable sobre k, O un anillo de K de valoración discreta, y t un parámetro de uniformización de O. Si $f \in O$, entonces $\frac{df}{dt} \in O$.

Prueba. Ver detalle de la prueba en [MONL12, pag.51]. □

[1] Teorema de Riemann-Roch, Abraham Martin del Campo Sanchez, pág. 69

Definición 2.36. Sea $\omega \in \Omega$, $\omega \neq 0$ y $P \in X$. Definimos el orden de ω en P como $ord_P(\omega)$. Considerando t un parámetro de uniformización de $O_P(X)$, escribimos $\omega = fdt$, con $f \in K$. Se define $ord_P(\omega) = ord_P(f)$. Veamos que esta definición no depende de la elección del parámetro de uniformización t, consideremos otro parámetro de uniformización, por ejemplo u tal que $fdt = gdu$, entonces $f/g = \frac{du}{dt} \in O(X)$, ahora por la proposición 2.35, $g/f \in O(X)$, por consiguiente $ord_P(f) = ord_P(g)$.

Definición 2.37. Si $0 \neq \omega \in \Omega$, se define el divisor de ω, como

$$div(\omega) = \sum_{P \in X} ord_P(\omega) \cdot P.$$

Definición 2.38. (Divisores Canónicos)
Definimos $W = div(\omega)$, como el divisor canónico de w.

Definición 2.39. Sea D un divisor en una curva X. Definimos el espacio

$$\Omega(D) = \{\omega \in \Omega(X) / \ div(\omega) - D \geq 0\} \cup \{0\},$$

y denotemos por $i(D)$ la dimensión de $\Omega(D)$ sobre k, el cual hemos definido como el índice de especialidad de D (ver definición 2.23, pág. 40).

Observación 2.40. Si ω' es otra diferencial no nula de Ω, entonces $\omega' = f\omega$, $f \in K$, luego $div(\omega') = div(f) + div(\omega)$, y por tanto $div(\omega') \sim div(\omega)$. Recíprocamente, si $W \sim W'$ entonces $W' = div(f) + W$, y $W' = div(f\omega)$.

De la observación 2.40, los divisores canónicos constituyen una clase de equivalencia respecto a la equivalencia lineal. En particular, todos los divisores canónicos tienen el mismo grado.

Corolario 2.41. Si $\ell(D) = g - 1$ y $W \leq D$ entonces $\ell(W) = g - 1$.

Prueba. Del teorema de Riemann tenemos $\ell(W) \leq g - 1$, ademas como $W \leq D$ entonces $\ell(W) \leq \ell(D) = g - 1$.
Por lo que se concluye que $\ell(W) = g - 1$. □

Definición 2.42. Sea P un punto en X, t un parámetro local en P y $w = fdt$ (la función f puede ser escrita como $\sum_i a_i t^i$). Definimos el residuo de w en el punto P, como $Res_P(w) = a_{-1}$.

Observación 2.43. Esta definición algebraica 2.42 del residuo no depende de la elección del parámetro local.

Teorema 2.44. Si w es una diferencial en una curva proyectiva regular X, entonces

$$\sum_{P \in X} \mathrm{Res}_P(w) = 0.$$

Antes de probar el teorema de Riemann-Roch, probaremos el siguiente teorema de Dualidad.

Teorema 2.45 (Dualidad). Para cualquier divisor D y divisor canónico $W = \mathrm{div}(\omega)$, la aplicación lineal

$$\begin{aligned} \$: \ L(W - D) &\to \Omega(D) \\ f &\mapsto \$(f) = f\omega \end{aligned}$$

es un isomorfismo de k-espacios vectoriales.

Prueba. Para cualquier $f \in L(W - D)$ no nulo y $\omega \in \Omega(D)$ se tiene

$$\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega) \geq -(W - D) + W = D.$$

Así, tenemos $\mathrm{div}(f\omega) \geq D$, por lo tanto $f\omega \in \Omega(D)$, y como $\mathrm{im}(\$) \to \Omega(D)$, $\mathrm{Nu}(\$) = \{0\}$, $\$$ es inyectiva.
Es claro que si $f, g \in L(W - D)$ y $L \in k$ entonces $f + g \in L$ y $Lf \in L(W - D)$, $\$(f + g) = (f + g)\omega = f\omega + g\omega = \$(f) + \$(g)$, $\$(Lf) = (Lf)\omega = L(f\omega) = L\$(f)$, así $\$$ es una aplicación lineal. Veamos que $\$$ es suryectiva, sea $\omega' \in \Omega(D)$ no nulo, por la observación 2.40, $\omega' = f\omega$ para algún $f \in K^*$,

$$\mathrm{div}(f) + W = \mathrm{div}(f) + \mathrm{div}(\omega) = \mathrm{div}(f\omega) = \mathrm{div}(\omega') \geq D.$$

Así $\mathrm{div}(f) \geq -(W - D)$, por lo tanto $f \in L(W - D)$, además $\omega' = \$(f)$, esto garantiza que $\$$ es suryectiva, en consecuencia $\$$ es un isomorfismo. □

Lema 2.46. Para cualquier divisor $D \in \mathrm{Div}(X)$, tenemos que $\dim(\Omega(D)) = i(D)$.

Prueba. Del Teorema Dualidad, se obtiene que $i(D) = \dim(\Omega(D)) = l(W - D)$. □

2.3 Teorema de Riemann-Roch

Teorema 2.47. *(Teorema de Riemann-Roch)*
Sea X una curva proyectiva no singular. Para cualquier divisor $D \in Div(X)$,

$$l(D) - l(W - D) = grad(D) + 1 - g,$$

donde W es un divisor canónico de X y g el género de X.

Prueba. Del lema 2.46, se obtuvo que $i(D) = l(W-D)$, donde $i(D) = g-1-6(D)$ es el ´ındice de especialidad.
Usando la definición 2.23, reemplazando $i(D) = g-1-grad(D) + l(D)$, obtenemos

$$l(W - D) = g - 1 - grad(D) + l(D).$$

□

Ejemplo 2.48. Consideremos la diferencial dx en la l´ınea proyectiva P^1, entonces dx es regular en los puntos $P_a = [a : 1]$, como $x - a$ es un parámetro local en P_a y $dx = d(x - a)$. Sea $Q = [1 : 0]$ el punto en el infinito, entonces $t = 1/x$ es un parámetro local. Consideremos la 1-forma $\omega = dx$ sin ceros ni polos en la parte afín $X_2 = 1$ y $\omega = dx = -t^{-2}dt$, así $ord_q(\omega) = ord_Q(dx) = -2$, por lo tanto $W = div(\omega) = -2Q$ es un divisor canónico, su grado $grad(W) = -2$, en consecuencia $l(W) = 0$. Aplicando el teorema de Riemann-Roch, $g = 0$.
Por lo tanto, la l´ınea proyectiva P^1 tiene genero cero.

Como consecuencia del teorema de Riemann-Roch tenemos los siguientes corolarios.

Corolario 2.49. Si W es un divisor canónico, entonces $l(W) = g$.

Prueba. Usando el teorema de Riemann-Roch, tomaremos $D = 0$, así $L(D)$ consiste solo de constantes, por lo tanto $l(D) = 1$ y $grad(D) = 0$. Reemplazando en el resultado del teorema

$$l(W - 0) = l(0) + g - 1 - grad(0), \longrightarrow l(W) = g$$

□

Corolario 2.50. El grado de una clase canónica es $2g - 2$.

Prueba. Usando el teorema de Riemann-Roch, consideramos $D = W$ y $l(0) = 1$,

$$l(W - W) = l(W) + g - 1 - \text{grad}(W), \Rightarrow \text{grad}(W) = 2g - 2.$$

□

Observación 2.51.

- Observe que $L(W - D) = 0$, siempre que $\text{grad}(W - D) < 0$. En este caso tendr´ıamos que $L(D) = \text{grad}(D) + 1 - g$.
- Nos gustaria encontrar condiciones sobre el divisor D, tal que $L(W - D) = 0$.

Corolario 2.52. Si $\text{grad}(D) > 2g - 2$, entonces $l(W - D) = 0$.

Prueba. Del teorema de Riemann-Roch se tiene que
$l(D) = l(W - D) + \text{grad}(D) + 1 - g$, también
$l(W - D) = l(W - (W - D)) + \text{grad}(W - D) + 1 - g$, sumando ambos resultados se tiene

$$\text{grad}(W - D) = 2g - 2 - \text{grad}(D) < 2g - 2 - (2g - 2) = 0.$$

Como $\text{grad}(W - D) < 0$ entonces $l(W - D) = 0$. □

Lema 2.53. Si $\text{grad}(D) > 2g - 2$, entonces $l(D) = \text{grad}(D) + 1 - g$.

Prueba. Es consecuencia directa del corolario 2.52, reemplazando en el teorema de Riemann-Roch

$$l(D) = \text{grad}(D) + 1 - g.$$

□

El siguiente teorema demuestra que los divisores canónicos son únicos.

Teorema 2.54. Supongamos que $g_o \in Z$ y $W_0 \in \text{Div}(X)$ satisfacen

$$l(D) - l(W_0 - D) = \text{grad}(D) + 1 - g_0;$$

para todo divisor $D \in \text{Div}(X)$. Entonces $g_0 = g$ y $W_0 = W$.

Prueba. - Consideremos $D = 0$, reemplazando en la hipótesis

$$l(0) - l(W_0) = \text{grad}(0) + 1 - g_0 \longrightarrow l(W_0) = g_0.$$

- Consideremos $D = W_0$ reemplazando en la hipótesis

$$l(W_0) - l(0) = \text{grad}(W_0) + 1 - g_0 \Longrightarrow \text{grad}(W_0) = 2g_0 - 2.$$

- Consideremos un divisor D tal que $\text{grad}(D) > \text{máx}\{2g-2, 2g_0-2\}$, ahora por el lema 2.53 se tiene

$$l(D) = \text{grad}(D) + 1 - g; \text{ y por hipótesis } l(D) = \text{grad}(D) + 1 - g_0.$$

De donde se concluye que $g = g_0$.

- Consideremos ahora $D = W$, reemplazando en la hipótesis que $g_0 = g$ y considerando los Corolarios 2.49 y 2.50,

$$l(W) - l(W_0 - W) = \text{grad}(W) + 1 - g, \text{ entonces } l(W_0 - W) = 1.$$

Como $\text{grad}(W_0 - W) = 0$, tenemos que $W_0 - W$ es principal, por ende $W_0 = W$□

Observación 2.55. Para el espacio de Riemann-Roch $L(D)$, deseamos encontrar todas las funciones cuyo divisor D cumplan el lema 2.53. La razón es que esto nos permitirá el proceso de codificar que veremos en siguiente capítulo.

Ejemplo 2.56. Del ejemplo 1.90, se tiene la curva $F = YZ - X^2$, además considerando $Q = [0 : 1 : 0] \in P^2$, o $Q = (0, 0) \in A^2$ y $\text{ord}_Q(x) = -1$. Sea $D = mQ$, donde $\text{grad}(D) = m$ y siendo m cualquier entero positivo.
Por la fórmula de Plücker $g = 0$, se cumple la condición del lema 2.53, por lo tanto $l(mQ) = m + 1 - 0 = m + 1$.
Así, $\text{ord}_Q(x^i) = -i \leq -m \Rightarrow 0 \leq i \leq m$, y obtenemos una base para $L(mQ)$

$$\{1, x, x^2, \ldots, x^m\}.$$

Ejemplo 2.57. Del ejemplo 1.89, se tiene la curva $F = X^5 + Y^5 + Z^5$, además considerando $Q = [0 : 1 : 1] \in P^2$, o $Q = (0, 1) \in A^2$,
$\text{ord}_Q(x) = 1$, $\text{ord}_Q(y) = 0$ y $\text{ord}_Q(y + 1) = 5$

$$\text{ord}_Q\left(\frac{x^i y^j}{(y+1)^{i+j}}\right) = i\,\text{ord}_Q(x) + j\,\text{ord}_Q(y) - (i+j)\,\text{ord}_Q(y+1) = -(4i + 5j) \leq -11.$$

Sea $D = 11Q$, $\text{grad}(D) = 11$, utilizando la fórmula de Plücker se tiene que $g = 6$, se cumple la condición del lema 2.53, por lo tanto $l(11Q) = 11 + 1 - 6 = 6$.
Calculemos $L(D) = L(11Q)$, teniendo el resultado $4i + 5j \leq 11$.
Para $j = 0$ se tiene $0 \leq 4i \leq 11$, se obtiene $i = 0, 1, 2$

$$1, y\frac{x}{+1}, \frac{x^2}{(y+1)^2}.$$

Para $j = 1$ se tiene $0 \leq 4i + 5 \leq 11$, se obtiene $i = 0, 1$

$$y\frac{y}{+1}, \frac{xy}{(y+1)^2}.$$

Para $j = 2$ se tiene $0 \leq 4i + 10 \leq 11$, se obtiene $i = 0$

$$\frac{y^2}{(y+1)^2}.$$

Una base para $L(11Q)$ es,

$$\overrightarrow{1, y\frac{x}{+1}, \frac{y}{y+1}, \frac{xy}{(y+1)^2}, \frac{x^2}{(y+1)^2}, \frac{y^2}{(y+1)^2}}^{\Sigma}.$$

Ejemplo 2.58. Consideremos la curva Hermitiana de segunda forma definida por $F = X^3 + Y^2Z + YZ^2$, la cual es una curva regular, con el único punto en el infinito $Q = [0 : 1 : 0] \in P^2$, o $Q = (0, 0) \in A^2$, considerando $x_y = \frac{X}{Y}$ y $z_y = \frac{Z}{Y}$; x_y es parámetro de uniformización por lo tanto $ord_Q(x_y) = 1$, así $ord_Q(z_y) = 3$.
Consideremos $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$.

$ord_Q(x) = ord_Q\left(\frac{x_y}{z_y}\right) = ord_Q(x_y) - ord_Q(z_y) = 1 - 3 = -2.$

$ord_Q(y) = ord_Q(z_y^{-1}) = -ord_Q(z_y) = -3.$

Sea $D = 5Q$, $grad(D) = 5$, utilizando la fórmula de Plücker se tiene que $g = 1$, se cumple la condición del lema 2.53, por lo tanto $l(5Q) = 5 + 1 - 1 = 5$.

$ord_Q(x^iy^j) = iord_Q(x) + jord_Q(y) = -2i - 3j \leq -5.$

Calculemos $L(D) = L(5Q)$, teniendo $2i + 3j \leq 5$

Para $j = 0$ se tiene $0 \leq 2i \leq 5$, se obtiene $i = 0, 1, 2$

$$1, x, x^2.$$

Para $j = 1$ se tiene $0 \leq 2i + 3 \leq 5$, se obtiene $i = 0, 1$

$$y, xy.$$

Una base para $L(5Q)$ es,

$$\{1, x, y, xy, x^2\}.$$

Capítulo 3

Códigos álgebro-geométricos

Imaginemos que tenemos un robot para desactivar explosivos, si el robot se controla de manera remota, y enviamos la instrucción de "cortar el cable rojo" mediante (100) pero en cambio recepciona la información (010) que significa "cortar el cable verde", este error ocasiona una explosión.

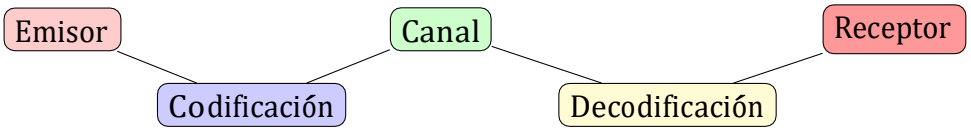
Los canales que se usan para transmitir la información, suelen ocasionar distorciones; generalmente por la presencia de interferencia o ruido, este problema es resuelto por el denominado código detector o corrector de errores, inventado por Richard Hamming. Los datos codificados de Hamming puede detectar errores de un bit y corregirlos.

Los códigos correctores son tan importantes en la teoría de códigos, debido a que además de codificar un mensaje también son capaces de corregir errores producidos por la transimisión de los mismos, asegurando el envió y recepción del mensaje correcto.

En esta sección sentaremos las bases de la definición de un código, la codificación y la decodificación. Estos conceptos junto con sus propiedades serán de mucha utilidad en el desarrollo del capítulo 5 a la hora de describir los mismos en terminos de estructuras modulares.

Definiciones básicas

Primero debemos considerar el siguiente proceso de la transmisión de la información.



Definición 3.1. Un Alfabeto es un conjunto finito $A = \{a_1, \ldots, a_q\}$, donde sus elementos son denominados símbolos, y al número q la raíz de A.

Una palabra o n-cadena es una sucesión de elementos de A de longitud n, por ejemplo sea a una sucesión en A entonces,

$$a = a_{i_1} a_{i_2} \ldots a_{i_n}, \quad a_{i_k} \in A.$$
$$\underbrace{\qquad\qquad}_{\text{longitud } n}$$

Ejemplo 3.2. Considerando nuestro alfabeto $A = \{a, b, c, d, \ldots, z\}$ el cual llamaremos 27-ario, denotemos por $|A| = q = 27$ la raíz. Elegimos los elementos: $a_{i_1} = c$, $a_{i_2} = u$, $a_{i_3} = b$, $a_{i_4} = o$ en A, una palabra será $a_{i_1} a_{i_2} a_{i_3} a_{i_4}$ ="cubo".

Denotemos por A^n el conjunto de todas las n-cadenas, y A^* el conjunto de todas las palabras sobre el alfabeto A, es decir $A^* = \bigcup_{n \in \mathbb{N}} A^n$.

Definición 3.3. Un código sobre un alfabeto A es un subconjunto C de A^*.

Si $q = 2$ se dirá que el código es binario, si $q = 3$ código ternario, así sucesivamente. Últimamente hay un gran interés por los códigos cuaternarios ($q = 4$) debido a que poseen algunas mejoras con respecto de los códigos binarios.

Observación 3.4. Debemos tener presente que la longitud puede ser variable, por lo que solo trataremos código de longitud fija, denominados código de bloque.

Ejemplo 3.5. El siguiente código $C = \{1, 10, 11, 101, 0101, 11110\}$ se denomina código binario de longitud variable.
El código $C = \{001, 101, 110, 010\}$ se denomina código binario de longitud fija, o código binario de bloque.

Definición 3.6 (Codificación). La codificación es el proceso por el cual cada mensaje, antes de ser enviada al receptor, se transforma en una sucesión de palabras de código.

Consideramos el mensaje $m = a_1 a_2 \cdots a_r \in A^r$ del cual separamos el mensaje en bloques de longitud $k < r$, como

$$m = (a_1 \cdots a_k) \cdot (a_{k+1} \cdots a_{2k}) \cdot \ldots \cdot (a_{r-k+1} \cdots a_r).$$

Cada uno de los bloques se codificará de manera natural e independiente mediante una aplicación $c : A^k \longrightarrow A^n$

$$c(m) = c(a_1 \cdots a_k) \cdot c(a_{k+1} \cdots a_{2k}) \cdot \ldots \cdot c(a_{r-k+1} \cdots a_r).$$

El conjunto $C := \mathrm{Im}(c)$ formará un código que será utilizado de aquí en adelante.

Definición 3.7 (Decodificación). La decodificación viene hacer el proceso final antes de llegar el mensaje al receptor, quizas la parte más delicada de todo el proceso.

Notemos que entre la codificación y la decodificación esta el canal el cual puede haber ruido, por lo que el mensaje no llegue del todo correcto.

Ejemplo 3.8. Consideremos el código binario C sobre el alfabeto $A = \{0, 1\}$ y supongamos que deseamos enviar los siguientes mensajes:

ROJO, VERDE, AZUL.

Podemos definir algunos códigos, en la siguiente tabla:

Código	Longitud	ROJO	VERDE	AZUL
C_1	2	10	01	11
C_2	3	100	010	110
C_3	4	1100	0110	0011

Representaremos un codigo de longitud fija n, y tamaño M como (n, M)-código q-ario.

Definición 3.9. El tamaño de un código C se define como $M := |C|$.

Ejemplo 3.10. Por ejemplo consideremos el alfabeto $A = \{0, 1, 2\}$, sean los códigos C_1, C_2 (sobre un código ternario) del alfabeto A.

$$C_1 = \{20, 11, 01\}, \qquad C_2 = \{010, 201, 110, 011, 220\}$$

Por lo tanto, C_1 es un $(2, 3)$-código y C_2 es un $(3, 5)$-codigo.

Definición 3.11. (Tasa de información)
La tasa de información de un (n, M)-código q-ario C, se define como:

$$R = R_q(C) = \frac{\log_q(M)}{n}.$$

Esta tasa representa el porcentaje de dígitos que guardan la información del mensaje original sobre el total de d´ıgitos transmitidos.

Ejemplo 3.12. Sean los códigos binarios C_1, C_2 sobre el alfabeto $A_1 = \{0, 1\}$ y los códigos ternarios C_3 y C_4 sobre el alfabeto $A_2 = \{0, 1, 2\}$.

$$C_1 = \{0, 1\}, \qquad C_2 = \{01, 10, 11\}$$

$$C_3 = \{20, 11, 01\}, \qquad C_4 = \{010, 201, 110, 011, 220\}\ .$$

La tasa de información para los códigos C_1 y C_2 son respectivamente $R_2(C_1) = \log_2(2) = 1$, $R_2(C_2) = \log_2(3)/2 \nearrow 0{,}7925$ y la tasa de información para los códigos C_3 y C_4 son $R_3(C_3) = \log_3(3)/2 = 0{,}5$, $R_3(C_4) = \log_3(5)/3 \nearrow 0{,}4883$.

Por ejemplo, podemos interpretar 0.4883, como: por cada bit de cada palabra del código C_4 llega 48.83 % bit de la información actual.

Observación 3.13. Es evidente observar que si $A_q \dashrightarrow A_r$ con $q < r$ entonces tomando a C como un (n, M)-código q-ario sobre A_q,

$$R_q(C) = \frac{\log_q(M)}{n} > \frac{\log_r(M)}{n} = R_r(C).$$

Podemos pensar que si q es el mínimo posible entonces la tasa de información será lo máximo posible, lo cual no es cierto en general.

Definición 3.14. (Distancia y peso de Hamming)

Consideremos dos palabras de igual longitud $a = a_1 \ldots a_n$ y $b = b_1 \ldots b_n \in A^n$, la distancia de Hamming entre a y b, se define como el número de coordenadas en que a y b difieren.

$$d : A^n \rightarrowtail A^n \blacksquare [0, n] \dashrightarrow \mathbb{N},$$

$d(a, b) := \#\{i : a_i \neq b_i\}$, se verifica inmediatamente que $d(a, b)$ es una métrica en A^n.

El peso de Hamming se define como el número de coordenadas no nulas.

$$w(a) := d(a, 0) = \#\{i : a_i = 0\}.$$

Del ejemplo 3.12 consideremos, en el código C_4, dos palabras $a = 201$ y $b = 220$, por lo tanto $d(a, b) = 2$, $w(a) = 2$ y $w(b) = 2$.

Definición 3.15. Dado un código C, se define la distancia de C como la menor distancia no nula entre sus palabras.

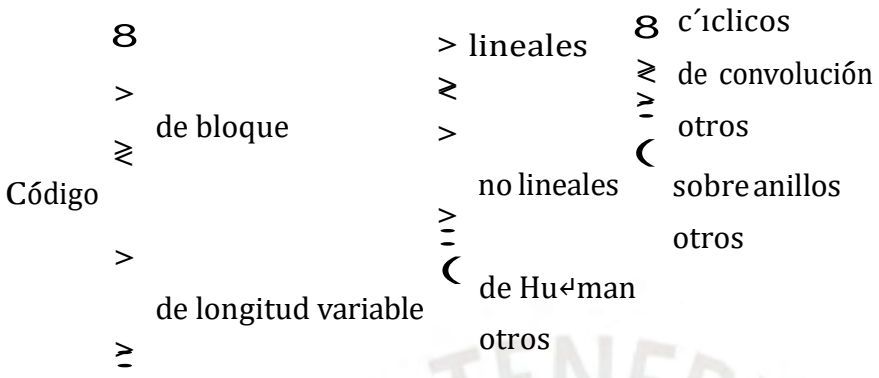
$$d(C) := \min\{d(a, b) : a, b \in C \text{ y } a \neq b\}.$$

Definición 3.16. Dado un código C, se define el peso de C como:

$$w(C) := \min\{w(c) : c \neq 0;\ c \in C\}.$$

Códigos correctores

Hay una variedad de tipos de códigos autocorrectores, los cuales los podemos clasificar de forma básica, teniendo presente la estructura del código:



Las familias más conocidas de estos códigos, hasta la actualidad son:

- Códigos lineales: de Hamming, de Hamming extendidos, simplex, de Golay, de Reed-Muller y de Goppa geométricos.
- Códigos cíclicos: BCH, de Reed-Solomon, de residuos cuadráticos y de Goppa clásicos.
- Códigos no-lineales: Hadamard, Kerdock, Justesen y Preparata.

Uno de los objetivos de la teoría de códigos, es maximizar la tasa de transmisión. Dentro de las familias de códigos más utilizados son los códigos lineales.

3.1 Códigos lineales

Los códigos lineales y cíclicos son los más importantes por su simplicidad. No solo poseen buenas propiedades, sus algoritmos son eficientes para la codificación y decodificación. A partir de este momento asumiremos que el alfabeto es el cuerpo finito $A = F_q$ o de Galois, con $q = p^m$ elementos, donde p primo.

Observación 3.17. El alfabeto A en general será considerado como un cuerpo, aunque podría ser un anillo.

Definición 3.18. Un código lineal q-ario de longitud n y rango k, es un subespacio vectorial $C \checkmark A^n$ de dimensión k.

Denotaremos a un código lineal de longitud n, dimensión k y de distancia mínima d como $[n, k, d]_q$-código, o simplemente $[n, k]_q$-codigo.

Matriz generatriz y matriz de control

El objetivo es encontrar una forma sistemática de generar códigos lineales, como también métodos rápidos, eficientes de codificación y decodificación de mensajes, por ello introduciremos la matriz generatriz G y la matriz de control H, así como su relación entre ellas. Codificar un mensaje es multiplicar matrices, por ejemplo $aG = c$, donde a es una palabra de información; decodificar consiste en resolver el sistema $aG = x$, donde el objetivo es hallar a, siendo x el mensaje recibido.

Definición 3.19. Sea C un $[n, k]_q$-codigo. Llamaremos **matriz generatriz** o matriz generadora $G \in F_q^{k \times n}$ de C, a la matriz de tamaño $k \times n$ y rango k cuyas filas forman una base de C, es decir,

$$G = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix} = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix},$$

donde, $g_1, g_2, \cdots, g_k$ son linealmente independientes.

Dada la aplicación lineal inyectiva

$$\begin{aligned} \varphi : F_q^k &\to F_q^n \\ x &\mapsto C = \varphi(x) = xG. \end{aligned}$$

La matriz asociada a la aplicación lineal φ de tamaño $k \times n$ es la matriz generatriz G.

Ejemplo 3.20. Considere la aplicación $\varphi : F_2^4 \to F_2^7$ y el siguiente código lineal binario en F_2^7, definido por

$$\varphi(x_1, x_2, x_3, x_4) = (x_1 + x_3, x_1, x_2, x_2 + x_3, x_2 + x_3 + x_4, x_4, x_1 + x_2 + x_4)$$

Es claro que la longitud del código es 7, y su dimensión es 4, por lo que tendremos un $[7, 4]_2$-código. Observe que

$$\varphi(1, 0, 0, 0) = (1, 1, 0, 0, 0, 0, 1), \quad \varphi(0, 1, 0, 0) = (0, 0, 1, 1, 1, 0, 1),$$
$$\varphi(0, 0, 1, 0) = (1, 0, 0, 1, 1, 0, 0), \quad \varphi(0, 0, 0, 1) = (0, 0, 0, 0, 1, 1, 1).$$

Por lo tanto, su matriz generatriz será

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

Ejemplo 3.21. Consideremos el cuerpo F_2, y el subespacio $L \to F_2^4$ generado por

$$L = h(1, 0, 0, 1), (0, 1, 0, 1), (0, 0, 1, 1)i$$

La matriz generadora del código L es

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

A partir de la matriz generatriz $G \in F_2^{3\to 4}$, para codificar un mensaje $a \in F_2^3$ bastará con multiplicar el mensaje por dicha matriz, es decir,

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

Esto genera un código binario C con parámetros $[4, 3]_2$ (o simplemente $[4, 3]$).

Teorema 3.22. Sea C un $[n, k]_q$-código. La matriz generatriz G siempre existe, y tiene rango k, es decir, $C = \{aG : a \in F_q^k\}$.

Prueba. De la definición 3.18 se tiene que C es un espacio vectorial de dimensión k, consideremos una base $\{c_1, c_2, \ldots, c_k\}$, donde $c_i = \sum_{j=1}^{n} c_{ij} e_j$, para $c_{ij} \in F_q$, siendo $\{e_1, e_2, \ldots, e_n\}$ es la base canónica de F_q^n.
Sea $a \in F_q^k$, veamos que $aG \in C$, en efecto

$$\begin{aligned} aG = (aG^1, \cdots, aG^n) &= \left(\sum_{i=1}^{k} a_i c_{i1}, \ldots, \sum_{i=1}^{k} a_i c_{in} \right) \\ &= \sum_{i=1}^{k} a_i \underbrace{(c_{i1}, \ldots, c_{in})}_{\{z}} \\ &= \sum_{i=1}^{k} a_i \sum_{j=1}^{n} c_{ij} e_j \\ &= \sum_{i=1}^{k} a_i c_i \in C. \end{aligned}$$

□

La matriz generatriz G dá una manera fácil de codificar palabras F_q^k, a cada palabra $a \in F_q^k$, se codifica como $aG \in F_q^n$.

Ejemplo 3.23. Del ejemplo (3.21), codificamos

$$000 \longrightarrow 0000,\quad 001 \longrightarrow 0011,\quad 010 \longrightarrow 0101,\quad 100 \longrightarrow 1001,$$
$$110 \longrightarrow 1100,\quad 011 \longrightarrow 0110,\quad 101 \longrightarrow 1010,\quad 111 \longrightarrow 1111$$

Luego,

$$C = \{0000, 0011, 0101, 1001, 1100, 0110, 1010, 1111\}$$

Es fácil comprobar que la distancia es $d = 2$.

Definición 3.24. Un $[n, k]$-código q-ario se dirá *sistemático* si existen k coordenadas $i_1, i_2, \ldots, i_k$ tal que al restringir las palabras código a estas coordenadas se obtienen todas las q^k palabras de longitud k.

Ejemplo 3.25. El código del ejemplo (3.23), es sistemático en todas sus coordenadas, por ejemplo para la coordenada 1, se tiene el código

$$C^{-} = \{000, 011, 101, 001, 100, 110, 010, 111\}$$

podemos verificarlo en la siguiente tabla,

Ejemplo del código lineal $[4, 3]_2$			
Mensaje	Palabra código	coordenada 1	coordenada 2
000	0000	0000	0000
001	0011	0011	0011
010	0101	0101	0101
100	1001	1001	1001
110	1100	1100	1100
011	0110	0110	0110
101	1010	1010	1010
111	1111	1111	1111

Definición 3.26. Una matriz generadora $G \in F_q^{k \times n}$ se dice que está en su forma estándar si es de la forma $G = (I_k|A)$, donde I_k es la matriz identidad de orden k y A es una matriz de orden $k \times (n - k)$.

Ejemplo 3.27. Del ejemplo 3.21, podemos observar que las tres primeras columnas de la matriz generatriz G, forman una submatriz identidad I_3.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$ Es decir G está en su forma estándar.

Es interesante observar que, si G está en su forma estándar, entonces C es sistemático, por lo que $aG = a(I_k|A) = (a|aA)$,

a codifica $aG = (a, aA)$ decodifica a.

Observación 3.28. Todo código lineal posee una matriz generatriz G, pero no es única. Podemos realizar operaciones elementales (método de Gauss Jordan) para expresar G en su forma escalonada; por ejemplo si consideramos el código lineal con n = 4 y k = 2 y su matriz generatriz

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

Definición 3.29. Dos códigos C_1 y C_2 de una misma longitud n sobre F_q, son equivalentes, si existe una permutación de sus índices $\{1, 2, \ldots, n\}$ tal que $C_2 = \{\sigma(x) | \ x \in C_1\}$.

Proposición 3.30. Todo código lineal C es equivalente a un código C' cuya matriz generatriz está en su forma estándar.

Prueba. Sea C el código lineal, por el teorema 3.22, C admite matriz generatriz G. Ahora sea $E = (E^1, \ldots, E^n)$ la matriz escalón reducida por filas de G (E^j son matrices columnas), además consideremos las coordenadas $i_1, i_2, \ldots, i_k$ donde están los 1's de E, es decir, si $i_1 = 3$ entonces $E^3 = (1, 0, \ldots, 0)^t$. Consideramos la permutación $\sigma = (ki_k) \cdots (2i_2)(1i_1) \in S_n$.
Por lo que $G' = (E^{\sigma(1)}, \ldots, E^{\sigma(n)})$, obteniendo $G' = (I_k|A)$ y $C' = F_q^n G' = C$ □

Existe otra manera de describir a los códigos lineales y es mediante su matriz de control, para ello nuestro objetivo será mostrar que: un mensaje x, a ser codificado, satisface $xG = y$ si y solo si existe una matriz H tal que $Hy^t = 0$.

Definición 3.31. Sea C un $[n, k]_q$-codigo, diremos que H es una matriz de control de C, o también matriz de chequeo de paridad, si para todo vector $y \in F_q^n$ se verifica que $y \in C$ si y solo si $Hy^t = 0$. Es decir,

$$C = \{y \in F_q^n / \ Hy^t = 0\}.$$

De la definición, podemos notar que la matriz de control H tendrá tamaño $(n-k)\times n$ y rango $n-k$.

Observe que podemos tener la matriz de control en su forma canónica $H = \begin{pmatrix} B & | & I_{n-k} \end{pmatrix}$. En efecto, si consideramos el cuerpo F_2, se tiene

$$\underbrace{\begin{pmatrix} I_k & | & A \end{pmatrix}}_{\text{matriz generatriz}} \quad \underbrace{\begin{pmatrix} A^t & | & I_{n-k} \end{pmatrix}}_{\text{matriz de control}}$$

Ejemplo 3.32. Consideremos G la matriz generatriz estándar del código de Hamming $[7, 4]_2$-código,

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} I_4 & | & A \end{pmatrix}.$$

Su matriz de control canónica, será

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} A^t & | & I_3 \end{pmatrix}.$$

Es fácil observar que $GH^t = 0$.

Proposición 3.33. Sean G y H la matriz generatriz estándar y la matriz de control canónica respectivamente en F_2, entonces $GH^t = 0$.

Prueba. Consideremos,

$G = (g_{ij})_{k\times n}$ la matriz generatriz estándar,

$H = (h_{ij})_{(n-k)\times n}$ la matriz de control canónica. Entonces

$M = GH^t = (m_{ij})_{k\times(n-k)}$, donde

$$\begin{aligned} m_{ij} &= \sum_{r=1}^{n} g_{ir}h_{rj} \\ &= \sum_{r=1}^{k} g_{ir}h_{rj} + \sum_{r=k+1}^{n} g_{ir}h_{rj}\, a_{i(r-k)}\delta_{(r-} \\ &= \sum_{r=1}^{k} \delta_{ir}a_{rj} + {}_{r=k+1}{}^{k)j} \\ &= a_{ij} + a_{ij} \\ &= 2a_{ij} = 0. \end{aligned}$$

donde,

$$6_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Por lo tanto, $GH^t = 0$. □

Teorema 3.34. Sea C un $[n, k]_q$-código. Sean G y H la matriz generatriz estándar y la matriz de control canónica en F_q respectivamente. Para todo vector $y \in F_q^n$ se verifica que $y \in C$ si y solo si $Hy^t = 0$.

Prueba. La prueba es inmediata de la definición 3.31 y la proposición 3.33. □

Definición 3.35. Si C es un $[n, k]_q$-codigo, el conjunto

$$C^? = \{x \in F_q^n / x \cdot c = 0 \text{ para todo } c \in C\}$$

es llamado código dual de C.

Teorema 3.36. Sea C un $[n, k]_q$-código, entonces se cumple:

1. Si G es una matriz generadora de C, entonces

$$C^? = \{x \in F_q^n / xG^? = 0\} = \{x \in F_q^n / Gx^? = 0\}.$$

2. $C^?$ es un $[n, n-k]_q$-código.

3. $(C^?)^? = C$.

Prueba. (1) Sea $x \in C^?$, de la definición 3.35 se cumple que $x \cdot c = 0$ para todo $c \in C$, por lo tanto

$$0 = x \cdot c = xc^? = x(G^?a^?) = (xG^?)a^?, \qquad (3.1)$$

para algún $a \in F_q^k$.

En la ecuación (3.1), si $xG^? = 0$ entonces $x \in C^?$. Probaremos su recíproco, es decir, si $x \in C^?$ entonces $xG^? = 0$. En efecto, como $(xG^?)a^? = 0$ para algún $a \in F_q^k$. Consideremos la base canónica, podemos expresar en particular $a = e_1, e_2, \ldots, e_k$, se tendría $0 = (Gx^?)e_i^? = (xG^?)_i$ para $1 \leq i \leq k$, por lo tanto $xG^? = 0$.

(2) De la definición 3.35, es claro que $C^?$ es un subespacio de F_q^n. Por (1) podemos considerar a $C^?$ como el espacio solución del sistema lineal homogéneo $xG^? = 0$ que tiene k ecuaciones y n incógnitas. Luego, como G tiene rango k, hay $n-k$ variables

libres, por lo tanto $\dim C^{\perp} = n - k$, es decir, $C^{\perp}$ es un $[n, n-k]_q$-codigo.
(3) Se tiene que $C \to (C^{\perp})^{\perp} = \{x \in F_q^n / x \cdot c' = 0\}$ para todo $c' \in C^{\perp}$. Pero

$$\dim(C^{\perp})^{\perp} = n - (n-k) = k = \dim C,$$

luego $C = (C^{\perp})^{\perp}$. □

Definición 3.37. Diremos que un código lineal es autodual cuando coincide con sigo mismo, es decir, $C^{\perp} = C$.

Proposición 3.38. *(Cota de Singleton)* Sea C un $[n, k, d]_q$-código, se cumple que

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

Prueba. Consideremos el subespacio lineal $L \subseteq_q F^n$, definido por

$$L := \{(x_1, x_2, \ldots, x_n) \in F_q^n / \ x_i = 0, \ \forall i \leq d\}.$$

Sea $a \in L$, de la definición 3.14 se tiene que el peso de Hamming es $w(a) \leq d-1$, por lo que $\dim(L \cap C) = 0$. Utilizando la fórmula de Grassmann [1], se tiene

$$\dim(C) + \dim(L) = \dim(C + L) + \dim(C \cap L) = \dim(C + L).$$

Por lo que $k + (d-1) = \dim(C + L) \leq n$. □

Ejemplo 3.39. Algunos ejemplos para ilustrar la proposición:
En el código $[11, 6, d]_q$-código se cumple $d \leq 11 - 6 + 1 = 6$.
Un $[11, k, 7]_q$-código cumple $k \leq 11 - 7 + 1 = 5$.
Un $[n, 8, 7]_q$-código cumple $n \leq 8 + 7 - 1 = 14$.
No existen códigos de la forma $[n, n-1, 3]_q$-codigos, pues debería cumplir
$n \leq (n-1) + 3 - 1 = n + 1$ (—■ —).

Proposición 3.40. *(Cota Gilbert-Varshamov)* Sea n, k y d enteros con la condición, $1 \leq k < n$, $2 \leq d \leq n$, y

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k},$$

entonces, existe un código lineal $[n, k]$ sobre F_q con distancia mínima al menos d.

[1] Sea V un espacio vectorial de dimensión finita, y sean V_1 y V_2 subespacios de V. Entonces

$$\dim(V_1 + V_2) = \dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2)$$

Prueba. Ver la demostración en el libro [NX09, pág. 151]. □

Definición 3.41. Los códigos que satisfacen la igualdad de la cota de Singleton ($k+d = n+1$) son llamados códigos MDS (códigos de máxima distancia separable).

Observación 3.42. Si G es la matriz generadora de un código MDS, entonces cualesquiera k columnas de G son linealmente independientes.

Observación 3.43. El código dual de un código MDS es también un código MDS.

Decodificación

Sea C un código lineal. Decodificar es la operación inversa de codificar, es decir, un decodificador es una aplicación

$$D : F_q^n \longrightarrow C \cup \{?\},$$

tal que $D(c) = c$ para todo $c \in C$. Sea y la palabra recibida, entonces $D(y)$ es la palabra código o ?, si ocurre esto último nuestra codificación falla.
La decodificación por detección de error es como sigue. Sea H la matriz de chequeo de paridad del código C, la salida del decodificador es:

$$D(y) = \begin{cases} y, & yH^t = 0 \\ ?, & yH^t \neq 0 \end{cases}$$

Sea $c \in C \subseteq F^n{}_q$ la palabra código con distancia mínima d transmitida sobre un canal con ruido e información recibida y, entonces diremos que el error ocurrido es $e = y - c$, por lo tanto

$$y = c + e.$$

Definición 3.44. Sea C un $[n, k, d]_q$-codigo con matriz control H, por lo tanto $cH^t = 0$ para todo $c \in H$. Después, recibiendo $y \in F_q^n$, definimos el vector síndromes del mensaje y como:

$$s(y) = yH^t \in F_q^{n-k}.$$

Ejemplo 3.45. Considerando la matriz de control H del ejemplo 3.32, y la tabla 3.1.
Supongamos que recibimos el mensaje $y = (0, 0, 1, 1, 1, 0, 1) \in F_2^7$, entonces su vector s´ındrome de y es

$$s(y) = yH^t = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}.$$

Observe que, $s(y) = (0, 1, 1)$, se encuentra en la cuarta fila de la tabla 3.1. Por lo tanto, asumimos por error el vector $e = (0, 0, 1, 0, 0, 0, 0)$ y como consecuencia obtenemos la palabra código $c = y - e = (0, 0, 1, 0, 1, 0, 1)$.

Error	Síndrome
(0,0,0,0,0,0,0)	(0,0,0)
(1,0,0,0,0,0,0)	(1,1,1)
(0,1,0,0,0,0,0)	(1,1,0)
(0,0,1,0,0,0,0)	(0,1,1)
(0,0,0,1,0,0,0)	(1,0,1)
(0,0,0,0,1,0,0)	(1,0,0)
(0,0,0,0,0,1,0)	(0,1,0)
(0,0,0,0,0,0,1)	(0,0,1)

Cuadro 3.1: Tabla error-síndrome

3.2 Códigos de Reed-Muller

Uno de los códigos lineales más conocidos son los **códigos de Reed-Muller**. Estos códigos forman parte de los códigos detectores y correctores de errores. El primero en realizar su construcción fue Muller. Un estudio en detalle y una sencilla decodificación lo hace Reed. Posteriormente, estos fueron generalizados a cualquier cuerpo finito; por su características, tienen una rica variedad en propiedades algebraicas, mayor detalle revisar [DADlH17].

Definición 3.46. Para $0 \leq r \leq m$, el código de Reed-Muller de orden r y longitud 2^m, denotado por $R(r,m)$, se define como el espacio

$$R(r,m) = \{(u, u+v) \in F_2^{2m} : u \in R(r, m-1),\ v \in R(r-1, m-1)\},$$

satisfaciendo las siguientes propiedades:

1. $R(0,m) = \{\underbrace{0\ldots0}_{2^m}, \underbrace{1\ldots1}_{2^m}\}$,
2. $R(m,m) = F_2^{2m}$,
3. si $0 < r < m$ entonces, $R(r,m) = R(r, m-1)\ R(r-1, m-1)$.

Ejemplo 3.47. Para $m \leq 2$, tenemos los codigos de Reed-Muller

- $m = 0$, $R(0,0) = \{0, 1\}$.
- $m = 1$, $R(0,1) = \{00, 11\}$, $R(1,1) = F_2^2 = \{00, 01, 10, 11\}$.
- $m = 2$, $R(0,2) = \{0000, 1111\}$, $R(2,2) = F_2^4$.

Del item 3 de la definición 3.46 tenemos

$$R(1,2) = R(1,1)\quad R(0,1) = \{(u, u+v) \in F_2^4 : u \in R(1,1), v \in R(0,1)\}.$$

Luego las palabras códigos son,

↤ Para $v = 00$ y $u \in R(1,1)$, tenemos $(u, u+v)$:

$$(00, 00+00), (01, 01+00), (10, 10+00), (11, 11+00).$$

↤ Para $v = 11$ y $u \in R(1,1)$, tenemos $(u, u+v)$:

$$(00, 00+11), (01, 01+11), (10, 10+11), (11, 11+11).$$

$$R(1,2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}.$$

Observación 3.48. Del ejemplo 3.47 para $m = 3$,

$$R(0,3) = \{00000000, 11111111\},\ R(3,3) = F_2^6,$$

faltaría los no triviales, que se puede calcular del item 3, de la definición 3.46.

- $R(1,3) = R(1,2)\ R(0,2)$.

- $R(2,3) = R(2,2)\ R(1,2)$.

Proposición 3.49. Sean r, m como en la definición 3.46, para el cuerpo F_2, la matriz generatriz de $R(r, m)$, está dada por bloques de manera recursiva en función de las matrices generadoras de menor orden $G(r, m-1)$ y $G(r-1, m-1)$, es decir,

$$G(r,m) = \begin{pmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{pmatrix}.$$

Siendo,

$$G(0,m) = \underbrace{1\ 1 \cdots 1}_{2^m} \quad \text{y} \quad G(m,m) = \begin{pmatrix} \underbrace{0\ 0 \cdots 0}_{2^m-1} & 1 \\ G(m-1,m) & \end{pmatrix}.$$

Ejemplo 3.50. Vamos a construir $G(2, 3)$

$$G(2,3) = \begin{pmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{pmatrix},$$

donde $G(1,1) = \begin{pmatrix} G(0,1) \\ 0\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $G(0,1) = (1\ 1)$.

$$G(1,2) = \begin{pmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

$$G(2,2) = \begin{pmatrix} G(1,2) \\ 0\ 0\ 0\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

$$G(2,3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

3.3 Códigos de Reed-Solomon

Definición 3.51. Consideremos el siguiente subespacio L_r de F_q.

$$L_r := \{f \in F_q[x] / \deg(f) \leq r\} \cup \{0\}.$$

Definamos $F_q^* = \{\alpha_1, \ldots, \alpha_{q-1}\}$ y elegimos un entero k tal que $1 \leq k \leq q-1$. Entonces el código Reed-Solomon $RS(k, q)$ está definido por

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

Si consideramos la transformación lineal $\varphi : L_{k-1} \to F_q^{q-1}$, la imagen de esta transformación es

$$\varphi(f) = (f(\alpha_1), \ldots, f(\alpha_{q-1})).$$

Los parámetros de $RS(k, q) = Im(\varphi)$ son: $n = q-1$, $\dim(C) = k$, y $d = n-k+1$, ver definición 3.18.

Teorema 3.52. Los códigos Reed-Solomon son MDS.

Prueba. De las hipótesis tenemos que la distancia mínima d de un código C satisface la desigualdad $d \leq n+1-k$. Además, de la cota de Singleton, $d \leq n+1-k$ de donde se cumple la igualdad, mayor detalle de la prueba, revisar [MONL12]. □

Ejemplo 3.53. Un ejemplo muy popular del código Reed-Solomon es $RS(223, 255)$ con 8-bit de símbolos, de donde los parámetros son:

- Tamaño bit de símbolo: $s = 8$ bits.
- Tamaño de bloque: $n = 2^s - 1 = 2^8 - 1 = 255$ bytes palabras clave (obs. que $q = 2^8$).
- Tamaño del mensaje: k símbolos, así $k = 223$ bytes son datos.
- Tamaño de paridad: $2t = n - k = 32 \longrightarrow$ 32 bytes son símbolos de paridad.
- Errores a corregir: $t \longrightarrow$ 16 bytes errores a corregir.
- Distancia mínima: $d_{min} \leq 2t + 1 = 33$ bytes de símbolos.

Observamos que, con $s = 8$ bits, se pueden generar como máximo una longitud de $n = q - 1 = 255$ bytes de símbolos, y el decodificador puede corregir 16 bytes de errores en símbolos de la palabra clave.

Ejemplo 3.54. Sea X la línea proyectiva P^1 sobre F_{q^m}. Sea $n = q^m - 1$. Sabemos que $P_0 = [0 : 1]$, $P_1 = [1 : 0]$ y definimos el divisor $B = P_1 + P_2 + \cdots + P_n$, donde $P_j = [\alpha^j : 1]$, con $j = 1, \ldots, n$, siendo α es la raíz n-énesima primitiva de la unidad; definimos $D = aP_0 + bP_1$, con $a, b \leq 0$.

Por el teorema de Riemann-Roch, $L(D)$ tiene dimensión $a + b + 1$, inmediatamente se sigue que

$$L(D) = \left\{ x \in F_q(x) / (x) + (a) \geq 0 \right\}.$$

Consideremos el código $C_L(B, D)$, con matriz generatriz que tiene por filas $(\alpha^i, \alpha^{2i}, \ldots, \alpha^{ni})$ con $-a \leq i \leq b$.

Es fácil chequear que $(c_1, c_2, \ldots, c_n)$ es una palabra código en $C_L(B, D)$ si y solo si $\sum_{j=1}^{n} c_j (\alpha^l)^j = 0$ para todo l con $a < l < n - b$. A $C_L(B, D)$ es un código de Reed-Solomon.

3.4 Códigos cíclicos

En está sección haremos una breve descripción de los códigos cíclicos.

Definición 3.55. Un $[n, k, d]_q$ código lineal C es un código cíclico si al final después de permutar las palabras sigue siendo cíclico, esto es,

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Podemos notar que por definición, un código lineal C es cíclico si es cerrado por el desplazamiento cíclico.

Para describir propiedades algebraicas de un código cíclico, necesitamos introducir una nueva estructura. Podemos identificar de manera natural $c = (c_0, c_1, \ldots, c_{n-1})$ como un polinomio de una variable $c(x) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$, esto permite definir un código cíclico como un ideal.

Definición 3.56. Un código cíclico es un ideal en $F_q[X]/\langle X^n - 1 \rangle$. La F_q-base para este anillo está formado por los monomios $1, X, \ldots, X^{n-1}$.

De la definición 3.56

$$\begin{aligned} x(c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}) &= c_0 X + c_1 X^2 + \ldots + c_{n-1} X^n \mod (X^n - 1) \\ &= c_{n-1} + c_0 X + \ldots + c_{n-2} X^{n-1}. \end{aligned}$$

Teorema 3.57. Sea C un código cíclico de longitud n. Entonces:

1. Existe un único polinomio mónico $g(X)$ de grado mínimo en C. Además, este polinomio genera C, es decir, $C = \langle g(X) \rangle$.
2. $g(X) | X^n - 1$.

3. Si $gr(G) = r$, entonces C tiene dimensión $n - r$. Más aún

$$C = \langle g(X) \rangle = \{r(X)g(X) : gr(g) < n - r\}.$$

4. Si $g(X) = g_0 + g_1X + \ldots + g_rX^r$, entonces $g_0 = 0$ y C tiene matriz generadora

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots\cdots & \cdots & g_r & \ddots & \cdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots\cdots & \cdots & g_r \end{pmatrix}$$

Prueba. La prueba lo puede encontrar en [Pod, pág. 76], como también en [Sal09, pág. 55]. □

Ejemplo 3.58. Consideremos el codigo $C = \langle 1 + X \rangle$ en $F_2[X]/\langle X^3 - 1 \rangle$, del teorema 3.57 $\dim C = 3 - 1 = 2$ y C está formado por los múltiplos de $1 + X$:

$$0,\ 1 + X,\ X(1 + X) = X + X^2,\ (1 + X)(1 + X) = 1 + X^2.$$

Luego,

$$C = \{0, 1 + X, 1 + X^2, X + X^2\} = \{000, 110, 101, 011\}.$$

Notemos que,

$$\langle 1 + X^2 \rangle = \{0, 1 + X^2, X(1 + X^2), (1 + X)(1 + X^2)\} = \{0, 1 + X^2, 1 + X, X + X^2\} = C.$$

Observación 3.59. Algunos códigos cíclicos son: códigos de Hamming, códigos BCH y los códigos de residuos cuadráticos, que son muy utilizados para encriptación.

3.5 Códigos de Goppa

Los códigos clásicos de Goppa fueron introducidos por Valery Denisovich Goppa [Gop70], matemático Soviético-Ruso, quién descubrió la relación entre la geometría algebraica y los codigos. Estos códigos son un tipo general de códigos lineales de Reed-Solomon, que se construyen usando una curva algebraica X sobre un cuerpo finito F_q, de la siguiente manera:

1. Elegimos un cuerpo finito F_q.

2. Elegimos una curva plana proyectiva no singular X sobre F_q.

3. Tomamos n puntos distintos F_q-racionales

$$P = \{P_1, \ldots, P_n\} \subset X(F_q) \text{ en } X.$$

4. Elegimos un divisor D en X, tal que $P \cap \text{supp}(D) = \emptyset$, además

$$2g - 2 < \text{grad}(D) < n.$$

5. Finalmente, el código Goppa es

$$C_L(P, D) := \{(f(P_1), \ldots, f(P_n)) / \ f \in L(D)\}.$$

3.6 Función código

La idea de Goppa es que un código puede ser construido evaluando funciones que pertenecen al espacio de Riemann-Roch en un conjunto de puntos racionales. En esta sección usaremos el espacio de Riemann-Roch para codificar nuestro código, como lo visto en el capítulo 2.

Definición 3.60. (Función código)
Sea X una curva proyectiva irreducible no singular sobre un cuerpo finito F_q, $P_1, P_2, \ldots, P_n$ puntos racionales distintos (sobre X), $B = P_1 + P_2 + \cdots + P_n$ un divisor asociado, y D un divisor tal que $0 < \text{grad}(D) < n$, con soporte disjunto al soporte de B, es decir,

$$\text{supp}(D) \cap \{P_i : \ i = 1, \cdots, n\} = \emptyset.$$

La función código de B en D, es la imagen de $L(D)$ bajo la aplicación

$$\begin{aligned} ev : L(D) &\longrightarrow F_q^n \\ f &\longmapsto ev(f) = (f(P_1), f(P_2), \ldots, f(P_n)). \end{aligned}$$

Notar que toda $f \in L(D)$ está definida en P_i $(\text{ord}_{P_i}(f) \leq 0)$, $i = 1, \ldots, n$; por lo que $f(P_i) \in F_q$.

Definición 3.61. Considerando las condiciones de la definición 3.60, denotemos por $C_L(B, D)$ el código algebro-geométrico (AG) de B y D, definido como la imagen de la aplicación evaluación, es decir,

$$C = C_L(B, D) := \{(f(P_1), f(P_2), \ldots, f(P_n)) \in F_q^n \ / \ f \in L(D)\}.$$

El núcleo de la aplicación ev está contenido en $L(D - B)$.

Observación 3.62. El requerimiento de pedir que $supp(D) \cap supp(B) = \emptyset$, es necesario y práctico.

Supongamos que $supp(D') \cap supp(B) = \emptyset$ y $m \in \mathbb{Z}^+$. Si $D = D' + mP_i$, entonces una función en $L(D)$ debe tener un polo en P_i, entonces $f(P_i)$ no está definido. De otro lado, si $D = D' - mP_i$ entonces cualquier función en $L(D)$ evaluado en P_i será cero. Entonces, cada palabra de código tiene un cero en la posición i, por lo que podemos borrarlo de está posición y no afecta la distancia mínima del código.

Proposición 3.63. La aplicación evaluación ev definida en 3.60 es inyectiva.

Prueba. Sea $f \in Nu(ev)$, es decir, $ev(f) = 0$ entonces $f(P_i) = 0$, $i = 1, 2, \ldots, n$, por lo tanto, el coeficiente de cada P_i en $div(f)$ es al menos 1.

Además, como $P \cap supp(D) = \emptyset$ y $B = P_1 + \cdots + P_n$ tenemos que $div(f) + D - B \leq 0$, por lo tanto $f \in L(D-B)$. Dado que $grad(D) < n$ entonces $grad(div(D-B)) < 0$ por lo tanto $L(D - B) = \{0\}$, por lo que se tiene que $f = 0$. □

Observación 3.64. Notemos que $f \in Nu(ev)$ si y solo si $f(P_i) = 0$ para $i = 1, \ldots, n$, por lo tanto $ord_{P_i}(f) \leq 1$. Así, $div(f) - \sum_{i=1}^{n} P_i \leq 0$, dado que $f \in L(D)$ y f tiene un cero en cada uno de los P_i, entonces

$$f \in L(D - \sum_{i=1}^{n} P_i) = L(D - B).$$

Por lo tanto,

$$Nu(ev) = \{f \in L(D) / ord_{P_i}(f) > 0,\ i = 1, \ldots, n\} = L(D - B),$$

por ende $dim(Nu(ev)) = l(D - B)$.

Observación 3.65. Como $L(D)$ es un espacio vectorial, el código $C_L(B, D)$ es lineal.

Teorema 3.66. El código $C_L(B, D)$ es un $[n, k, d]_q$-código lineal cuyos parámetros son:

1. longitud $n = dim(B)$,
2. rango $k = l(D) - l(D - B)$,
3. la distancia mínima es $d \leq n - grad(D)$.

Prueba. Ya que los puntos de B son racionales, la longitud del código $C_L(B, D)$ es la misma que el grado de B, así $n = \dim(B)$. De la definición 3.61 se tiene que $C_L(B, D) = \mathrm{Im}(ev)$, aplicamos el primer teorema de isomorfismos para espacios vectoriales

$$k := \dim(C_L(B, D)) = \dim(\mathrm{Im}(ev)) = \dim(L(D)) - \dim(\mathrm{Nu}(ev)).$$

Por definición tenemos que $\dim(L(D)) = l(D)$, y de la observación 3.64 se tiene:

$$k = l(D) = l(D) - l(D - B).$$

Considerando g el género de la curva X y además sea $2g - 2 < \mathrm{grad}(D) < n$, por el teorema de Riemann-Roch $k = \mathrm{grad}(D) + 1 - g = l(D) - l(D - B)$.
Sea $ev(f) = (f(P_1), \ldots, f(P_n)) \in C$ una palabra de peso mínimo d, es decir, $w(ev(f)) = d > 0$ entonces $ev(f)$ tiene exactamente d coordenadas no nulas. Sin pérdida de generalidad, asumimos que $f(P_i) \neq 0$, $i = 1, \ldots, d$ y $f(P_{d+1}) = \cdots = f(P_n) = 0$, así $f \in L(D - P_{d+1} - \cdots - P_n)$, dado que $f \neq 0$, se tiene

$$\mathrm{div}(f) + D - P_{d+1} - \cdots - P_n \geq 0,$$

sabemos que $\mathrm{grad}(f) = 0$, así que $\mathrm{grad}(D) - (n - d) = \mathrm{grad}(D - P_{d+1} - \cdots - P_n) \geq 0$, por ende $d \leq n - \mathrm{grad}(D)$. □

Corolario 3.67. Supongamos que el grado de D es estrictamente menor que n. Entonces la aplicación evaluación $ev : L(D) \to C_L(B, D)$ es inyectiva y tenemos:

1. $C_L(B, D)$ es un $[n, k, d]_q$-código con

   $$d \geq n - \mathrm{grad}(D) \text{ y } k = \dim(D) \leq \mathrm{grad}(D) + 1 - g,$$

   por lo tanto, $k + d \leq n + 1 - g$.

2. Si adicionalmente, $2g - 2 < \mathrm{grad}(D) < n$, entonces $k = \mathrm{grad}(D) + 1 - g$.

3. Si $\{f_1, f_2, \ldots, f_k\}$ es una base de $L(D)$ entonces la matriz

   $$G = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{pmatrix},$$

   es una matriz generadora para $C_L(B, D)$ de orden $k \times n$.

Observación 3.68. Realizando operaciones elementales en fila, si es necesario, intercambiando columnas, podemos tomar a G de la forma

$$G' = [I_k \quad P],$$

donde I_k es la matriz identidad de orden $k \times k$ y P es alguna matriz de orden $k \times (n - k)$.

Ejemplo 3.69. Del ejemplo 1.93 y ejemplo 2.22, $D = 2Q$ donde $Q = [0 : 1 : 1]$, es fácil hallar los otros puntos racionales de X.

	Q	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	0	0	0	1	α	α^2	1	α	α^2
y	1	α	α^2	0	0	0	1	1	1
z	1	1	1	1	1	1	0	0	0

Del ejemplo 2.22 encontramos que $L(D) = \{h, f\}$, con $h = 1$ y $f = \frac{x}{y+z}$ sobre F_2 y también sobre F_4. Considerando $B = P_1 + \cdots + P_8$, esto nos lleva a la siguiente matriz generatriz para $C_L(B, D)$

$$G = \begin{pmatrix} h(P_1) & h(P_2) & h(P_3) & h(P_4) & h(P_5) & h(P_6) & h(P_7) & h(P_8) \\ f(P_1) & f(P_2) & f(P_3) & f(P_4) & f(P_5) & f(P_6) & f(P_7) & f(P_8) \end{pmatrix},$$

obteniendo

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 \end{pmatrix}.$$

De la matriz generatriz G se tiene que la distancia de mínima es $d = 6$, $n = 8$ y $k = 3$.

Ejemplo 3.70. Del ejemplo 1.93 consideremos $D = 3Q$ donde $Q = [0 : 1 : 1]$, en el ejemplo 3.68 hallamos los 9 puntos racionales de X.

La dimensión de $L(D)$ es $l(D) = 3$, encontramos que $L(D) = \{h, f, g\}$, con $h = 1$, $f = \frac{x}{y+z}$ y $g = \frac{y}{y+z}$ sobre F_2 y también sobre F_4. Considerando $B = P_1 + \cdots + P_8$, esto nos lleva a la siguiente matriz generatriz para $C_L(B, D)$

$$G = \begin{pmatrix} h(P_1) & h(P_2) & h(P_3) & h(P_4) & h(P_5) & h(P_6) & h(P_7) & h(P_8) \\ f(P_1) & f(P_2) & f(P_3) & f(P_4) & f(P_5) & f(P_6) & f(P_7) & f(P_8) \\ g(P_1) & g(P_2) & g(P_3) & g(P_4) & g(P_5) & g(P_6) & g(P_7) & g(P_8) \end{pmatrix},$$

obteniendo

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha^2 & \alpha & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

De la matriz generatriz G se tiene que la distancia de mínima es $d = 5$, $n = 8$ y $k = 4$.

Definición 3.71. Una definición simple de los códigos de Goppa es que son el dual de $C_L(B, D)$. Usualmente lo denotaremos por

$$C_\Gamma(B, D) = C_L^?(B, D).$$

Lema 3.72. Sea $2g - 2 < \text{grad}(D) < n$, d y d^0 la distancia mínima de $C_L(B, D)$ y $C_\Gamma(B, D)$ respectivamente, entonces

1. $n - \text{grad}(D) \leq d \leq n - \text{grad}(D) - g$.
2. $\text{grad}(D) - 2g + 2 \leq d^0 \leq \text{grad}(D) - g + 2$.

Prueba. Ver la demostración en [Zam07, pág. 15]. □

Definición 3.73. Definimos el código $C_\Gamma(B, D) \checkmark F_q^n$ por

$$C_\Gamma(B, D) = \{(\text{Res}_{P_1}(!), \ldots, \text{Res}_{P_n}(!))/\ ! \in \Gamma(D - B)\}.$$

Teorema 3.74. $C_\Gamma(B, D)$ es un $[n, k^\diamond, d^\diamond]_q$-código con parámetros

$$k^\diamond = i(D - B) - i(D) \quad \text{y} \quad d^\diamond \leq \text{grad}(D) - (2g - 2).$$

Bajo la hipótesis adicional de que $\text{grad}(D) > 2g - 2$, tenemos que $k^\diamond = i(D - B) \leq n + g - 1 - \text{grad}(D)$. Más aún, si $2g - 2 < \text{grad}(D) < n$ entonces

$$k^\diamond = n + g - 1 - \text{grad}(D).$$

Prueba. De la definición 3.71, $C_\Gamma(B, D) = C_L^?(B, D)$.
$i(D - B) - i(D) = \ell(D) - \ell(D - B) = n - k = k^\diamond$.
Del lema 3.72, $d^0 \leq \text{grad}(D) - (2g - 2)$.
Del teorema 3.36 y del teorema 3.66, se sigue

$$k^\diamond = n - k = n - (\text{grad}(D) + 1 - g) \longrightarrow k^\diamond = n + g - 1 - \text{grad}(D).$$

□

Ejemplo 3.75. Del ejemplo 2.58, $D = aQ$ donde $Q = [0 : 1 : 0]$, es fácil hallar los otros puntos racionales de X, sobre $F_4 = F_2(\alpha) = \{0, 1, \alpha, \alpha^2\}$, donde $\alpha^2 + \alpha + 1 = 0$.

	Q	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	0	0	0	1	1	α	α	α^2	α^2
y	1	0	1	α	α^2	α	α^2	α	α^2
z	0	1	1	1	1	1	1	1	1

Sea $B = P_1 + \cdots + P_8$, tenemos que $d^\perp \leq a - (2g - 2)$, Consideramos el código $C_\Omega(B, D)$, con distancia mínima $d^\perp = a$, entonces $a = 5$, $k^\perp = 8 + 1 - 1 - a = 3$, esto nos lleva a la siguiente matriz generatriz para $C_\Omega(B, D)$

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ x(P_1) & x(P_2) & x(P_3) & x(P_4) & x(P_5) & x(P_6) & x(P_7) & x(P_8) \\ y(P_1) & y(P_2) & y(P_3) & y(P_4) & y(P_5) & y(P_6) & y(P_7) & y(P_8) \\ xy(P_1) & xy(P_2) & xy(P_3) & xy(P_4) & xy(P_5) & xy(P_6) & xy(P_7) & xy(P_8) \\ x^2(P_1) & x^2(P_2) & x^2(P_3) & x^2(P_4) & x^2(P_5) & x^2(P_6) & x^2(P_7) & x^2(P_8) \end{pmatrix},$$

obteniendo:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \end{pmatrix}.$$

De la matriz generatriz G se tiene que la distancia de mínima es $d = 4$, $n = 8$ y $k = 5$.

Número de puntos racionales sobre una curva algebraica

Goppa establece una relación entre las curvas algebraicas sobre cuerpos finitos y los códigos correctores de errores, habiendo así un mayor interés hacia la construcción de curvas definidas sobre F_q con muchos puntos racionales respecto a su género. Por las aplicaciones que tienen estas curvas en la teoría de códigos, enunciaremos algunos resultados sobre cotas, sin demostrar, los cuales se pueden revisar en detalle [NX01] y [Sti09].

Denoratemos en adelante $\#X(F_q)$ como la cantidad de puntos racionales sobre la curva X.

Teorema 3.76. *(Cota de Hasse-Weil)*
Sea X una curva proyectiva no singular irreducible, de género g sobre un cuerpo F_q con q elementos, el número de puntos racionales satisface:

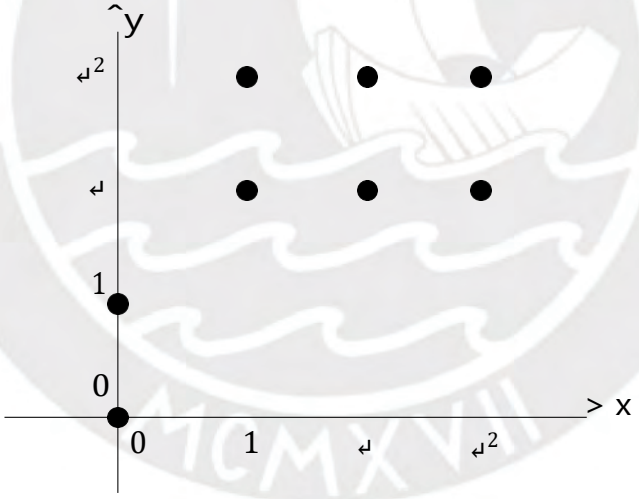
$$|\#X(F_q) - (q+1)| \leq \lfloor 2g\sqrt{q} \rfloor.$$

A las cotas de Hasse-Weil también se le conoce como la hipótesis de Riemann para curvas sobre cuerpos finitos.

Ejemplo 3.77. Dada la curva Hermitiana $X : F = X^{q+1} + Y^q Z + Y Z^q$, plana no singular de grado $q+1$, su género es $g = q(q-1)/2$. Adicionalmente X tiene $q^3 + 1$ puntos F_{q^2}-racionales. Hay q^3 puntos afines y $Q = [0 : 1 : 0]$ punto en el infinito. Usando la cota de Hasse-Weil se tiene el máximo número de puntos posibles

$$|\#X(F_{q^2})| \leq q^2 + 1 + 2gq = 1 + q^2 + q(q-1)q = q^3 + 1.$$

Si consideramos $q = 2$, tenemos el ejemplo 3.75, mostraremos una imagen que visualiza dicho ejemplo.



Consideremos un código de longitud n. Sea $f \in L(D)$ que tiene peso d, entonces f se anula en $n-d$ puntos, por lo tanto $\text{grad}(D)-(n-d) \leq 0$ (un divisor tiene al menos polos y ceros), es decir, $d \leq n - \text{grad}(D)$, para garantizar d positivo, asumamos que $\text{grad}(D) < n$. Como $B = \sum_{i=1}^{n} P_i$ es evidente $\text{grad}(D - B) < 0$ entonces $Nu(ev) = L(D - B)$, y la dimensión k del código viene dado por el teorema de Riemann-Roch $l(D) \leq \text{grad}(D) + (1-g)$, así

$$d \leq n - \text{grad}(D) \quad y \quad k \leq \text{grad}(D) + 1 - g.$$

En particular, usando la cota de Singleton $k + d \leq n + 1$, encontramos

$$1 + \frac{1-g}{n} \leq \frac{k}{n} + \frac{d}{n} \leq 1 + \frac{1}{n}.$$

Por lo tanto, un buen código (uno con $\frac{k}{n}$ y $\frac{d}{n}$ grande), del cual surge una curva de género pequeño con un gran número de puntos racionales.

Ejemplo 3.78. Consideremos la cuártica de Klein $X : F = X^3Y + Y^3Z + XZ^3$ definida en el plano proyectivo F_2, la curva tiene género $g = (4-1)(4-2)/3 = 3$, tiene tres puntos racionales $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1] \in X(F_2)$ y son los únicos puntos sobre el cuerpo F_{2^k} $(k \leq 1)$ con $XYZ = 0$.
Consideremos ahora la curva sobre $F_8 = F_2(\alpha)$, con $\alpha^3 + \alpha + 1 = 0$, entonces α genera un grupo multiplicativo F_8^*. Si $(X, Y ; Z) \in X(F_8)$ con $XYZ \neq 0$, podríamos asumir que $Z = 1$, $Y = \alpha^i$ y $X = \alpha^{3i}\beta$ para algún $\beta \in F_8$, así tenemos

$$(\alpha^{3i}\beta)^3\alpha^i + (\alpha^i)^3 + \alpha^{3i}\beta = \alpha^{3i}(\beta^3 + \beta + 1) = 0.$$

De aquí podemos elegir $\beta \in \{\alpha, \alpha^2, \alpha^2 + \alpha\}$; de la cota de Hasse-Weil, se tiene

$$|\#X(F_8)| \leq 8 + 1 + \lfloor 6\sqrt{8} \rfloor = 25.$$

De donde, $\#X(F_8^*) = 21$, por lo tanto se tendría en total $\#X(F_8) = 24$.

Sea $N_q(g)$ el número máximo de puntos racionales de una curva de género g sobre F_q que se puede tener, es decir,

$$N_q(g) = \max_{X/F_q} \#X(F_q).$$

Como también una cantidad asintótica

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g} \leq 2\sqrt{q}.$$

Por muchos años después de que Weil probara estas conjeturas, esencialmente no hubo mucha investigación; aunque en muchos casos esta cota se ha mejorado grandemente.

Teorema 3.79. *(Cota de Serre)*
Sea X una curva proyectiva no singular, definida sobre F_q, de género g, tenemos:

$$|\#X(F_q) - (q + 1)| \leq g\lfloor 2\sqrt{q} \rfloor.$$

Como consecuencia inmediata se tiene $A(q) \leq \lfloor 2\sqrt{q} \rfloor$.

Prueba. Ver la demostración en [AP18]. □

Ejemplo 3.80. Del ejemplo anterior 3.78, se tiene que $g = 3$, $q = 8$. Por la cota de Hasse-Weil se tiene $|\#X(F_8)| \leq 25$, pero utilizando la cota de Serre, se ve una mejora

$$|\#X(F_8)| \leq 9 + \lfloor 2\sqrt{8} \rfloor = 24.$$

Que es exactamente la cantidad de puntos obtenidos en la cuártica de Klein.

Cuando el género es grande en comparación con el tamaño del cuerpo, una significante mejora se puede obtener debido a Ihara.

Teorema 3.81. *(Cota de Ihara)*
Sea X una curva proyectiva no singular, definida sobre F_q, de género g, tenemos:

$$|\#X(F_q)| \leq q + 1 + \frac{1}{2}\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} - g.$$

Y asintóticamente

$$A(q) \leq \frac{1}{2}\left(\sqrt{8q+1} - 1\right).$$

Aunque S. G. VlâdutV. G. Drinfel'd [VD83] mejora esta cota, mostrando que

$$A(q) \leq \sqrt{q} - 1.$$

Observación 3.82. Esta cota de Ihara es mejor que la de Hasse-Weil, cuando

$$2g\sqrt{q} > \frac{1}{2}\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} - g.$$

Agrupando y elevando al cuadrado

$$g^2(1 + 4\sqrt{q})^2 > (8q+1)g^2 + (4q^2 - 4q)g,$$

$$8g\sqrt{q}(1 + \sqrt{q}) > 4q(q-1) \Longrightarrow g > \frac{1}{2}\sqrt{q}(\sqrt{q} - 1).$$

Ejemplo 3.83. Para $g = 100$ y $q = 2$, la cota por Hasse-Weil sería $N_2(100) \leq 285$, pero por la cota de Ihara sería $N_2(100) \leq 159$.

Ejemplo 3.84. Sea $k = F_{7^2}$ y sea X la curva que denota la ecuación afín

$$Y^2 = X^7 - X,$$

su género viene dado por $g = \frac{7-1}{2} = 3$ (ver [FT96]). De la cota de Hasse-Weil se tiene $|\#X(F_{49})| \leq 50 + \lfloor 2(3)\sqrt{49} \rfloor = 92$, con un único punto en el infinito $Q = [0 : 1 : 0]$.

Un algoritmo de decodificación

Como ya hemos visto el uso de códigos algebro-geométricos, muchos han decidido buscar algoritmos de decodificación, para el cual se presentará el algoritmo-SV, que fué creado por A.N. Skorobogatov y S.G. Vladut en 1990, quienes introdujeron la noción de localizador de error.

Presentaremos el algoritmo-SV, el cual permitirá corregir sólo hasta $t' = \lfloor \frac{d^* - g}{2} \rfloor$ errores, donde $t^* = \frac{d^* - 1}{2}$, d^* es la distancia mínima asignada y g el género de la curva C proyectiva no singular.

Proposición 3.85. Sea $d^* = \text{grad}(D) - (2g - 2)$ una distancia diseñada de $C_\Omega := C_\Omega(B, D)$. Sabemos que $d^* \leq d$, donde d representa la distancia mínima de C_Ω. Las siguientes afirmaciones son válidas:

a) Si G_1 y t satisfacen

$$\begin{aligned} &\text{Supp}(D_1) \cap \text{Supp}(B) = \emptyset, \\ &\text{grad}(D_1) < \text{grad}(D) - (2g-2) - t, \\ &l(D_1) > t, \end{aligned} \tag{3.2}$$

entonces $t \leq (d^* - 1)/2$.

b) Si $0 \leq t \leq (d^* - 1 - g)/2$ entonces existe un divisor D_1 tal que satisface la ecuación (3.2).

Prueba. La demostración lo puede ver en [Sti09, pág. 304]. □

Definición 3.86. (Localizador de error)

1. Sea $e = (e_1, \cdots, e_n) \in \mathbb{F}^n$. Si $e_i = 0$, entonces P_i es una posición de error para e.

2. Una función $\sigma \in K$ es un Localizador de error para e, si $\sigma(P_i) = 0$ para toda posición de error P_i de e.

Definamos el síndrome

$$S_b(f) := \sum_{j=1}^{n} b_j \cdot f(P_j),$$

siendo $b \in \mathbb{F}_q^n$ y $f \in L(D)$.

Lema 3.87. Si una función $\sigma \in K$ es un localizador de error para e, entonces $S_e(\sigma) = 0$.

Prueba. Si $\sigma \in K$ es un localizador de error para $e = (e_1, \cdots, e_n)$, entonces $e_i = 0$, de la definición 3.86 implica que $\sigma(P_i) = 0$, y es claro que

$$S_e(\sigma) = \sum_{j=1}^{n} e_j \cdot \sigma(P_j) = 0.$$

□

Consideremos las siguientes bases específicas:

$$\begin{aligned} &\{f_1, \ldots, f_m\} \text{ de } L(D), \\ &\{h_1, \ldots, h_l\} \text{ de } L(D_1), \\ &\{g_1, \ldots, g_k\} \text{ de } L(D - D_1). \end{aligned} \tag{3.3}$$

Tenga en cuenta que la elección de estas bases no depende del vector $y \in F_q^n$ que será decodificado, además es claro que, $h_i g_j \in L(D)$ para $1 \leq i \leq l$ y $1 \leq j \leq k$. Consideremos el siguiente sistema de ecuaciones lineales, el cual juega un rol esencial en el algoritmo de decodificación:

$$\sum_{i=1}^{n} S_y(h_i g_j) \cdot x_i = 0, \quad \text{para } j = 1, \ldots, k. \tag{3.4}$$

Algoritmo-SV

Entrada: Sea $y \in F_q^n$ un elemento dado

1. Encontrar una solución no trivial $(x_1, \ldots, x_n)$, del sistema (3.4), y sea $\sigma := \sum_{i=1}^{n} x_i z_i$ (Si (3.4) tiene sólo la solución trivial, no se puede decodificar y)

2. Determine $N(\sigma) = \{j : 1 \leq j \leq n, \text{ y } \sigma(P_j) = 0\}$. (Esto puede ser hecho por evaluación $\sigma(P_j) = \sum_{i=1}^{n} x_i z_i(P_j)$ para $j = 1, \ldots, n$.)

3. Si el sistema $\sum_{j \in N(\sigma)} f_\mu(P_j) \cdot z_j = S_y(f_\mu)$ para $\mu = 1, \ldots, m$ tiene solución única $(e_j)_{j \in N(\sigma)}$, fijamos $e := (e_1, \ldots, e_n)$ con $e_j = 0$ para $j \notin N(\sigma)$. (Si el sistema no es resoluble unicamente entonces no se puede decodificar y)

4. Comprueba si $c := y - e$ es un elemento de C_D (por el cálculo del síndrome $S_c(f_\mu)$ para $\mu = 1, \ldots, m$) y sea $wt(e) \leq t$. Si la respuesta es SI, decodificamos y en la palabra código c. Si la respuesta es NO, no podemos decodificar y.

Teorema 3.88. *(Skorobogatov-Vladut)*

a) Dado D_1 y t satisface (3.2) el algoritmo-SV decodifica todos los errores de peso $\leq t$.

b) Se puede elegir el divisor D_1 de tal manera que el algoritmo-SV decodifica todos los errores e de peso

$$wt(e) \leq (d^{\leftarrow} - 1 - g)/2,$$

donde $d^{\leftarrow} = grad(D) - (2g - 2)$ es la distancia diseñada de $C_{\mathbb{D}}$.

Prueba. La demostración lo puede ver en [Sti09, pág. 308]. □

Ejemplo 3.89. Considerando el ejemplo 3.75, este código corrige un error, consideremos c es la palabra clave enviada, e la palabra error, e y es la palabra recibida

$$\begin{aligned} c &= (1,1,1,1,1,1,1,1), \\ e &= (0,0,\hookleftarrow,0,0,0,0,0), \\ y &= (1,1,\hookleftarrow^2,1,1,1,1,1), \end{aligned}$$

tenemos las funciones de base: $\bullet_1 = 1, \bullet_2 = x, \bullet_3 = y, \bullet_4 = xy, \bullet_5 = x^2$.
Queremos un localizador de la forma

$$\$ = x_1\bullet_1 + x_2\bullet_2 + x_3\bullet_3 + x_4\bullet_4 + x_5\bullet_5.$$

Sea $\bullet_{i,j} = S_e(\bullet_i \bullet_j)$, note que $\bullet_{i,j} = \bullet_{j,i}$.

$$\bullet_{1,1} = S_e(\bullet_1\bullet_1) = \sum_{j=1}^{8} e_j \cdot \bullet_1^2(P_j) = e_3\bullet_1^2(P_3) = \hookleftarrow,$$

$$\bullet_{1,2} = S_e(\bullet_1\bullet_2) = \sum_{j=1}^{8} e_j \cdot \bullet_1\bullet_2(P_j) = e_3\bullet_1\bullet_2(P_3) = \hookleftarrow,$$

$$\bullet_{1,3} = S_e(\bullet_1\bullet_3) = \sum_{j=1}^{8} e_j \cdot \bullet_1\bullet_3(P_j) = e_3\bullet_1\bullet_3(P_3) = \hookleftarrow^2,$$

$$\bullet_{1,4} = S_e(\bullet_1\bullet_4) = \sum_{j=1}^{8} e_j \cdot \bullet_1\bullet_4(P_j) = e_3\bullet_1\bullet_4(P_3) = \hookleftarrow^2,$$

$$\bullet_{1,5} = S_e(\bullet_1\bullet_5) = \sum_{j=1}^{8} e_j \cdot \bullet_1\bullet_5(P_j) = e_3\bullet_1\bullet_5(P_3) = \hookleftarrow,$$

$$\bullet_{2,2} = S_e(\bullet_2\bullet_2) = \sum_{j=1}^{8} e_j \cdot \bullet_2^2(P_j) = e_3\bullet_2^2(P_3) = \hookleftarrow,$$

$$\bullet_{2,3} = S_e(\bullet_2\bullet_3) = \sum_{j=1}^{8} e_j \cdot \bullet_2\bullet_3(P_j) = e_3\bullet_2\bullet_3(P_3) = \hookleftarrow^2,$$

$$\bullet_{2,4} = S_e(\bullet_2\bullet_4) = \sum_{j=1}^{8} e_j \cdot \bullet_2\bullet_4(P_j) = e_3\bullet_2\bullet_4(P_3) = \hookleftarrow^2,$$

$$\bullet_{2,5} = S_e(\bullet_2\bullet_5) = \sum_{j=1}^{8} e_j \cdot \bullet_2\bullet_5(P_j) = e_3\bullet_2\bullet_5(P_3) = \hookleftarrow,$$

$$\bullet_{3,3} = S_e(\bullet_3 \bullet_3) = \sum_{j=1}^{8} e_j \cdot \bullet_3^2(P_j) = e_3 \bullet_3^2(P_3) = 1,$$

$$\bullet_{3,4} = S_e(\bullet_3 \bullet_4) = \sum_{j=1}^{8} e_j \cdot \bullet_3 \bullet_4(P_j) = e_3 \bullet_3 \bullet_4(P_3) = 1,$$

$$\bullet_{3,5} = S_e(\bullet_3 \bullet_5) = \sum_{j=1}^{8} e_j \cdot \bullet_3 \bullet_5(P_j) = e_3 \bullet_3 \bullet_5(P_3) = \lambda^2,$$

$$\bullet_{4,4} = S_e(\bullet_4 \bullet_4) = \sum_{j=1}^{8} e_j \cdot \bullet_4^2(P_j) = e_3 \bullet_4^2(P_3) = 1,$$

$$\bullet_{4,5} = S_e(\bullet_4 \bullet_5) = \sum_{j=1}^{8} e_j \cdot \bullet_4 \bullet_5(P_j) = e_3 \bullet_4 \bullet_5(P_3) = \lambda^2,$$

$$\bullet_{5,5} = S_e(\bullet_5 \bullet_5) = \sum_{j=1}^{8} e_j \cdot \bullet_5^2(P_j) = e_3 \bullet_5^2(P_3) = \lambda,$$

Tenemos el siguiente sistema

$$\begin{pmatrix} \lambda & \lambda & \lambda^2 & \lambda^2 & \lambda \\ \lambda & \lambda & \lambda^2 & \lambda^2 & \lambda \\ \lambda^2 & \lambda^2 & 1 & 1 & \lambda^2 \\ \lambda^2 & \lambda^2 & 1 & 1 & \lambda^2 \\ \lambda & \lambda & \lambda^2 & \lambda^2 & \lambda \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Una solución no trivial del sistema será $(x_1, x_2, x_3, x_4, x_5) = (1, 0, \lambda, 1, 0)$.

Por lo que, nuestro localizador de errores es $\$ = 1 + \lambda Y + XY$ y $P_3 = [1 : \lambda : 1], [0 : \lambda^2 : 1], [\lambda^2 : 1 : 1]$ son los únicos ceros posibles.

Ahora asumamos que sólo conocemos y, además $\$ = 1 + \lambda X + XY$ y $P_3 = [1 : \lambda : 1]$ como único cero. Podemos deducir que $e = (e_1, \cdots, e_8)$ debe tener $e_j = 0$ con la posible excepción de $e_3 = 0$.

$$\begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \end{pmatrix}(e_3) = \begin{pmatrix} e_3 \\ e_3\lambda \\ e_3\lambda^2 \end{pmatrix} = \begin{pmatrix} \lambda \\ \lambda^2 \\ 1 \end{pmatrix} \longrightarrow e_3 = \lambda,$$

esto nos dá el vector de errores $e = (0, 0, \lambda, 0, 0, 0, 0, 0)$, como consecuencia tenemos nuestra palabra código $c := y - e = (1, 1, 1, 1, 1, 1, 1, 1)$.

Capítulo 4

Automorfismos y estructuras modulares.

Un automorfismo es un endomorfismo que también es un isomorfismo, es decir, es un homeomorfismo biyectivo de un objeto en si mismo que conserva toda su estructura. El conjunto de todos los automorfimos de un objeto forma un grupo, denominado grupo de automorfismos.
Los resultados de este capítulo serán pieza clave a la hora de describir la codificación sistemática que estudiaremos en el capítulo 5.

Automorfismos

Un automorfismo, es una correspondencia que asocia cada elemento de un conjunto con un único elemento del mismo conjunto.
Consideremos el cuerpo k, un automorfismo del cuerpo k es una aplicación biyectiva $\sigma : k \to k$ que preserva todas las propiedades algebraicas de k, más precisamente, es un isomorfismo, esto es,

$$\sigma(a + b) = \sigma(a) + \sigma(b) \quad y \quad \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) \quad \forall a, b \in k. \tag{4.1}$$

Ejemplo 4.1. La conjugación compleja, es un automorfismo del cuerpo C. Si $\sigma : C \to C$ tal que $\sigma(a + bi) = a - bi \ \forall a, b \in R$, es claro que σ es una biyección, como, $\sigma(\sigma(z)) = z, \forall z \in C$, veamos que cumple la condición (4.1)
Sean $z_1 = a + bi$ y $z_2 = c + di$, con $a, b, c, d \in R$

$$\begin{aligned}\sigma(z_1 + z_2) &= \sigma((a + c) + (b + d)i)\\ &= (a + c) - (b + d)i\\ &= (a - bi) + (c - di)\\ &= \sigma(z_1) + \sigma(z_2).\end{aligned}$$

$$\begin{aligned}\sigma(z_1 \cdot z_2) &= \sigma((ac - bd) + (bc + ad)i)\\ &= (ac - bd) - (bc + ad)i\\ &= (a - bi) \cdot (c - di)\\ &= \sigma(z_1) \cdot \sigma(z_2).\end{aligned}$$

Ejemplo 4.2. El único automorfismo del cuerpo Q es la identidad.

El automorfismo de un cuerpo k forman un grupo, el grupo de automorfismos se denota como: Aut(k).

Ejemplo 4.3. Consideremos una extensión $F|k$, se define el grupo de Galois $G(F|k)$ como el grupo de automorfismos de F sobre k

$$Gal(F|k) = Aut_k(F) = \{\sigma : F \to \bar{k} / \ \sigma \text{ es una k-inmersión}\},$$

siendo el cardinal del grupo $|Gal(F/k)| = |Aut_k(F)| = [F : k]$.
Por ejemplo, consideremos el cuerpo $k = Q$ y su extensión $F = Q(i, \sqrt[4]{2})$, asi $[F : k] = 8$ y su grupo de automorfismos es

$$Gal(F|k) = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle \cong D_4,$$

donde $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\tau(i) = -i$ y $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$; $\quad i^2 = -1$, $\sqrt[4]{2}^4 = 2$.

Teorema 4.4 (Automorfismo de Frobenius). Sea k un cuerpo de característica p, entonces la aplicación $\sigma_p : k \to k$, donde $\sigma_p(x) = x^p$; $\forall x \in k$, es un automorfismo de k.

Prueba. Sean $x, y \in k$, por ser un cuerpo, $xy \in k$. Por lo tanto

$$\sigma_p(xy) = x^p y^p = \sigma_p(x)\sigma_p(y), \quad \sigma_p(1) = 1.$$

Igualmente $x + y \in k$ por lo tanto usando el Binomio de Newton

$$\sigma_p(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

Como $\binom{p}{i}$ es múltiplo de p con $i \neq 0, p$; entonces

$$\sigma_p(x + y) = x^p + y^p = \sigma_p(x) + \sigma_p(y),$$

σ_p es un homomorfismo de anillo con unidad.

Además σ_p es inyectivo, pues si $x \in k$ tenemos $0 = \sigma_p(x) = x^p$, entonces $x = 0$, dado que k es un cuerpo (no tiene elementos nilpotentes); σ_p es sobreyectivo porque toda aplicación inyectiva entre cuerpos del mismo cardinal lo es, por lo tanto esto demuestra que σ_p es un automorfismo.

Finalmente, como k tiene característica p, contiene a un cuerpo isomorfo a F_p. Así todo elemento de F_p es raíz de la ecuación $X^p - X = 0$, además dichas raíces son precisamente los elementos de k que quedan fijos por σ_p, lo que significa que F_p es el cuerpo fijo de σ_p. □

Observación 4.5. Del Teorema de Frobenius 4.4 se observa que para un cuerpo finito k de característica p, $\mathrm{Aut}(k)$ es un grupo cíclico.

Proposición 4.6. Sea F_q un cuerpo finito y sea $n > 1$ un entero. En una clausura algebraica de F_q existe un único cuerpo extensión F_q^n de grado n de F_q.

Prueba. Ver la demostración en [LREL19]. □

Teorema 4.7. Sean $n, m \leq 1$ enteros. Entonces F_{p^n} es un subcuerpo de F_{p^m} si y solo si $n|m$. En este caso la extensión F_{p^m}/F_{p^n} es cíclica y $\mathrm{Gal}(F_{p^m}/F_{p^n}) = \langle \sigma^n \rangle$.

Prueba. Supongamos que $F_{p^m} \supseteq F_{p^n} \supseteq F_p$. Entonces se tiene que $n = [F_{p^n} : F_p]$ divide $m = [F_{p^m} : F_p]$, en efecto,

$$[F_{p^m} : F_p] = [F_{p^m} : F_{p^n}].[F_{p^n} : F_p] \Rightarrow m = [F_{p^m} : F_{p^n}] \cdot n.$$

Supongamos ahora que n es un divisor de m, es decir, $m = dn$. El grupo $\mathrm{Gal}(F_{p^m}/F_{p^n}) = \langle \sigma^n \rangle$ es cíclico de orden n y posee un subgrupo único $H = \langle \sigma^n \rangle$ de orden d.

Sea $F = F_{p^n}^H$ el cuerpo fijo bajo H. Entonces $[F : F_p] = [G : H] = m$ y por lo tanto $|F| = p^m$. Por el teorema de Moore [LREL19] $F \cong F_{p^m}$. Además, $H = \mathrm{Gal}(F_{p^m}/F_{p^n})$. □

4.1 Automorfismos en códigos geométricos de Goppa

La investigación de grupo de automorfismo de códigos de Goppa fue iniciado por Stichtenoth [Sti90], quien considera el código $C(B, D)$ con $B = P_1 + P_2 + \cdots + P_n$ puntos de grado 1.

Definición 4.8. Dados D y D' divisores en X, diremos D, D' son B-equivalentes ($D \sim_B D'$), si existe un elemento $0 \neq u \in X$ tal que $D - D' = (u)$ con $u(P_i) = 1$ para $i = 1, 2, \ldots, n$.

Es claro que $\sim_B$ es una relación de equivalencia. Ahora asumamos que D y D' no contienen ningún punto racionales, en común $P_1, \ldots, P_n$, entonces tenemos

Lema 4.9. Si $D \sim_B D'$, entonces $C_L(B, D) = C_L(B, D')$.

Prueba. Se tiene $D \sim_B D'$, por lo tanto $D = D' + (u)$ con $u(P_i)$, para $i = 1, \ldots, n$. La aplicación

$$\begin{aligned} \mu : \ L(D) &\longrightarrow L(D') \\ f &\longmapsto \mu(f) = fu \end{aligned}$$

es un isomorfismo, de aquí

$$\begin{aligned} C_L(B, D') &= \{((fu)(P_1), \ldots, (fu)(P_n)) : \ f \in L(D)\} \\ &= \{(f(P_1)u(P_1), \ldots, f(P_n)u(P_n)) : \ f \in L(D)\} \\ &= \{(f(P_1), \ldots, f(P_n)) : \ f \in L(D)\} = C_L(B, D). \end{aligned}$$

□

Sabiendo que el grupo simétrico S_n actúa sobre F_q^n vía

$$\pi(a_1, \ldots, a_n) = (a_{\pi(1)}, \ldots, a_{\pi(n)}).$$

Entonces el grupo de automorfismo del código $C \hookrightarrow F_q^n$ está definido por

$$\mathrm{Aut}(C) = \{\pi \in S_n : \pi(C) = C\}.$$

De otro lado, consideramos el grupo $\mathrm{Aut}_{F_q}(X)$ del cuerpo de automorfismos del cuerpo de funciones algebraicas X sobre F_q. Este grupo actúa en los puntos de X vía

$$\mathrm{ord}_{\sigma(P)}(f) = \mathrm{ord}_P(\sigma^{-1}(f)).$$

Esta acción se extiende a la acción de $\mathrm{Aut}_{F_q}(X)$ en el grupo de divisores de X de la siguiente manera

$$\sigma\left(\sum n_P \cdot P\right) = \sum n_P \cdot \sigma(P),$$

de esto último podemos tener que $\sigma(L(A)) = L(\sigma(A))$, si P no es un polo de f tenemos $f(P) = (\sigma f)(\sigma P)$.

Dado X una curva irreducible proyectiva no singular sobre un cuerpo finito F_q, $C_L(B, D)$ un código de Goppa geométrico sobre la curva X, consideremos una colección de funciones $\{f_1, \ldots, f_k\}$ en $L(D)$, cuyas imágenes están en $L(D)/L(D - B)$; esto se prueba en los artículos [HLS95], [GK08] y [Wes98], que forman una base para este espacio cuya matriz generatriz es

$$G = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{pmatrix}.$$

El cálculo de esta matriz lo podemos observar en el corolario 3.67 y de la observación 3.68. Stichtenoth en [Sti90, pág. 114] define el siguiente grupo de automorfismo que cae en la curva X

$$\mathrm{Aut}_{F_q,B,D}(X) = \{\sigma \in \mathrm{Aut}_{F_q}(X) : \sigma(B) = B, \sigma(D) \sim_B D\}.$$

Observe que $\mathrm{Aut}_{F_q,B,D}(X)$ es un subgrupo de $\mathrm{Aut}_{F_q}(X)$. La condición $\sigma(D) \sim_B D$ en la definición de $\mathrm{Aut}_{F_q,B,D}(X)$ siempre puede ser reemplazado por la condición, mucho más simple, $\sigma(D) = D$ quedando

$$\mathrm{Aut}_{F_q,B,D}(X) = \{\sigma \in \mathrm{Aut}_{F_q}(X) : \sigma(B) = B, \sigma(D) = D\}.$$

Lema 4.10. Asumamos que $D = D_0 - D_1$ tal que $D_0 \leq 0$, $D_1 \leq 0$ y $\mathrm{grad}(D_0 + D_1) \leq n - 1$, entonces

$$\mathrm{Aut}_{F_q,B,D}(X) = \{\sigma \in \mathrm{Aut}_{F_q}(X) : \sigma(B) = B, \sigma(D) = D\}.$$

Prueba. La demostración de este lema se puede revisar en [Sti90, pág. 116]. □

Teorema 4.11. Sea $C_L(B, D)$ el código racional de Goppa con $1 \leq \mathrm{grad}(D) \leq n-3$. Entonces tenemos $\mathrm{Aut}(C_L(B, D)) = \mathrm{Aut}_{F_q,B,D}(X)$, es decir, cada automorfismo de $C_L(B, D)$ es inducido por una transformación lineal proyectiva.

La prueba depende esencialmente de los siguientes dos lemas.

Lema 4.12. Sean $C_L(B, D)$ y $C_L(B, D')$ códigos racionales de Goppa de longitud $n \leq 3$. Supongamos que $0 \leq \text{grad}(D) = \text{grad}(D') \leq n - 2$. Entonces $C_L(B, D) = C_L(B, D')$ si y solo si $D \sim_B D'$.

Prueba. La demostración se puede revisar en [Sti90, pág. 117-120]. □

Lema 4.13. Sea $C_L(B, D) = C_L(B', D')$ códigos racionales de Goppa de longitud n con $1 \leq \text{grad}(D) = \text{grad}(D') \leq n - 3$. Entonces existe un automorfismo $\sigma \in \text{Aut}_{F_q}(X)$ tal que $\sigma(B) = B'$.

Prueba. La demostración se puede revisar en [Sti90, pág. 117-120]. □

Asumiendo estos dos lemas, podemos demostrar el teorema 4.11.

Prueba. del Teorema 4.11

Tenemos que mostrar que cada automorfismo de $C_L(B, D)$ es inducido por un elemento de $\text{Aut}_{F_q,B,D}(X)$. Por lo tanto, consideramos una permutación $\pi \in S_n$ tal que

$$\pi(C_L(B, D)) = C_L(B, D).$$

Como $\pi(C_L(B, D)) = C_L(\pi(B), D)$, sabemos, del lema 4.13, que existe un automorfismo $\sigma \in \text{Aut}_{F_q}(X)$ con $\sigma(P_i) = P_{\pi(i)}$ para $i = 1, \ldots, n$. En particular, tenemos que $\sigma(B) = B$. De otro lado tenemos

$$\begin{aligned} C_L(\sigma(B), \sigma(D)) &= C_L(B, D), \\ &= C_L(\pi(B), D), \\ &= C_L(\sigma(B), D). \end{aligned}$$

Del lema 4.12, se concluye que $\sigma(D) \sim_B D$. Esto prueba que $\sigma \in \text{Aut}_{F_q,B,D}(X)$. □

Ejemplo 4.14. Ilustremos nuestro resultado con un ejemplo simple dado en [Sti90], Consideremos el cuerpo $F_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ y el cuerpo de funciones racionales $k = F_q(z)$. Para $i = 1, 2, \ldots, q$; sea P_i el cero de $z - \alpha_i$, y sea P_1 el polo de z. Consideremos el código racional de Goppa $C(B, kP_1)$ con $B = P_1 + P_2 + \ldots + P_q$ y $2 \leq k \leq q - 2$. Es fácil ver que $C(B, kP_1)$ es la extensión del código Reed-Solomon de longitud q y dimensión $k + 1$ sobre F_q. Así tenemos

$$\begin{aligned} \text{Aut}_{F_q,B,kP_1}(X) &= \{\sigma \in PGL(2, q) : \sigma(P_1) = P_1\}. \\ &= \{\sigma \in PGL(2, q) : \sigma(z) = az + b \text{ con } a, b \in F_q \text{ y } a \neq 0\}. \end{aligned}$$

Sin embargo, para $k = 0$ o $k = q - 2$, tenemos $\text{Aut}(C(B, kP_1)) = S_q$.

Ejemplo 4.15. Consideremos la curva Hermitiana[1] X sobre F_{q^2}, dada por la ecuación afín

$$X^{q+1} = Y^q + Y$$

del ejemplo 3.77 y de los artículos [BHHW98],[Lit07] tenemos que su género es $g = q(q-1)/2$ y por el teorema 3.76 cota de Hasse-Weil se tiene $q^3 + 1$ puntos F_{q^2}-racionales. Además, tiene un único punto en el infinito $Q = P_1 = [0 : 1 : 0]$. En particular sea B como la suma de los q^3 puntos afines F_{q^2}-racionales de X, es decir, $B = P_1 + P_2 + \cdots + P_{q^3}$.

Consideremos $x = \frac{X}{Z}$ y $y = \frac{Y}{Z}$, un punto simple de la forma $[0 : \alpha : 1]$ donde $\alpha^q + \alpha = 0$, hay exactamente q soluciones para $\alpha \in F_{q^2}$, así concluimos que x tiene q ceros y así q polos en el punto Q, por lo tanto $(x)_1 = qQ$, igualmente para el punto $[0 : 0 : 1]$ se obtiene una raíz simple de orden $q + 1$, esto implica que el orden del polo en Q es $q + 1$ es decir $(y)_1 = (q + 1)Q$. El semigrupo S del número de polos están generados por los divisores de qQ y $(q + 1)Q$, esto es,

$$S = \{aq + b(q + 1) : a, b \in N\}.$$

Una base para $L(mQ)$ viene dado por

$$\{x^i y^j : \ 0 \leq i,\ 0 \leq j \leq q-1 \text{ y } iq + j(q + 1) \leq m\}.$$

Sea λ un elemento primitivo de F_{q^2}. La aplicación

$$\begin{aligned} \sigma : \quad P^2 &\longrightarrow P^2 \\ [X : Y : Z] &\longmapsto [\lambda X : \lambda^{q+1} Y : Z], \end{aligned}$$

induce un automorfismo en la curva X, es fácil chequear que $[X : Y : Z] \in X$. Además, se cumple $X^{q+1} - Y^q Z - Y Z^q = 0$.

$$\sigma([X : Y : Z]) \Rightarrow (\lambda X)^{q+1} - (\lambda^{q+1} Y)^q Z - (\lambda^{q+1} Y) Z^q = \lambda^{q+1}(X^{q+1} - Y^q Z - Y Z^q) = 0.$$

El grupo de automorfismo del código de la curva Hermitiana $C_L(B, mQ)$, está dado por:

$$\mathrm{Aut}(C_L(B, mQ)) \cong \mathrm{Aut}_{F_{q^2}, B, mQ}(X).$$

El lector interesado puede seguir profundizando sobre curvas Hermitianas en el libro [Sti09].

[1] Tiersma prueba que la curva Hermitiana de Fermat $X^{r+1} + Y^{r+1} = Z^{r+1}$ y la curva $X^{r+1} = Y^r Z + Y Z^r$ son isomorfos. Remarks on codes from Hermitian curves, IEEE Trans. Inform. Theory IT-33 (l987), 605-609.

Observación 4.16. Del ejemplo 4.15, para ilustrar podemos tomar el caso $q = 2$, así el género es $g = 1$ y tendría 9 puntos afines F_4-racionales como se muestra en el gráfico del ejemplo 3.77, el automorfismo σ estaría dado por

$$\sigma([X : Y : Z]) = [\lambda X : Y : Z], \quad \text{recordando que } F_4 = F_2[\lambda]/\langle \lambda^2 + \lambda + 1 \rangle$$

Esté automorfismo permuta los 8 puntos afines F_4-racionales en cuatro orbitas, las dos primeras de longitud tres, y las otras dos de longitud uno

$$\begin{aligned} O_1 &= \{[1 : \lambda : 1], [\lambda : \lambda : 1], [\lambda^2 : \lambda : 1]\}. \\ O_2 &= \{[1 : \lambda^2 : 1], [\lambda : \lambda^2 : 1], [\lambda^2 : \lambda^2 : 1]\}. \\ O_3 &= \{[0 : 0 : 1]\}. \\ O_4 &= \{[0 : 1 : 1]\}. \end{aligned}$$

Capítulo 5

Aplicaciones con bases de Gröebner

5.1 Algunas estructuras algebraicas y bases de Gröbner

Las bases de Gröbner son unos de los resultados más importantes del álgebra computacional, por ende una herramienta fundamental. En la presente sección daremos una breve descripción de la teoría de bases de Gröbner que nos permitirá desarrollar el tema principal de está tesis, el cual es codificar y decodificar mediante módulos.

Las bases de Gröbner se inició con B. Buchberger a inicio de los años 1980; usando ideales. En este trabajo de tesis se desarrollará usando módulos.

A los lectores con el buen manejo de este tipo de estructuras podrían prescindir de esta sección y pasar a la sección 5.2.

Polinomios e ideales

Un monomio, es la colección de variables $X_1, X_2, \ldots, X_n$ como productos de la forma

$$X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n},$$

donde cada α_i son enteros no negativos (i = 1, ..., n).

Si consideramos $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in Z^n_{\geq 0}$ podemos reescribir un monomio como $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}$, donde su grado será $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Un polinomio será entonces una combinación lineal de monomios, es decir,

$$f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha X^\alpha, \qquad a_\alpha \in k.$$

Denotaremos por $k[X_1, \ldots, X_n]$ el anillo de polinomios en las variables $X_1, X_2, \ldots, X_n$.

Por ejemplo, el polinomio definido sobre Q

$$f(X_1, X_2, X_3) = 5X_1^3 X_2 - 2X_1 X_3^2 + \frac{1}{2} X_3 - 3,$$

podemos expresarlo como

$$f(X_1, X_2, X_3) = 5X^{(3,1,0)} - 2X^{(1,0,2)} + \frac{1}{2} X^{(0,0,1)} - 3X^{(0,0,0)},$$

de donde podemos calcular el grado de cada monomio

$X^{(3,1,0)}$ su grado es: $|(3, 1, 0)| = 3 + 1 + 0 = 4$,

$X^{(1,0,2)}$ su grado es: $|(1, 0, 2)| = 1 + 0 + 2 = 3$,

$X^{(0,0,1)}$ su grado es: $|(0, 0, 1)| = 0 + 0 + 1 = 1$,

$X^{(0,0,0)}$ su grado es: $|(0, 0, 0)| = 0 + 0 + 0 = 0$,

el monomio que tiene mayor grado es $X^{(3,1,0)}$, de donde su término des $5X^{(3,1,0)}$, por lo tanto f será un polinomio de 4 términos, y de grado 4.

Definición 5.1. Dado el polinomio

$$f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha X^\alpha, \qquad a_\alpha \in k.$$

Consideremos que $a_{\alpha_i} X^{\alpha_i}$ es el término que tiene mayor grado, definimos:

1. su coeficiente lider $cl(f) = a_{\alpha_i}$.
2. su monomio lider $ml(f) = X^{\alpha_i}$.
3. su término lider $tl(f) = a_{\alpha_i} X^{\alpha_i}$.

Orden monomial

Vamos a considerar al conjunto formado por todos los monomios en varias variables

$$T^n = \{X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} \mid \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}\}.$$

Definición 5.2. Definimos el orden monomial sobre T^n como un orden total $\succ$ que satisface:

a) $1 \succ X^{\alpha}$.

b) Si $X^{\alpha} \succ X^{\beta}$ entonces $X^{\gamma}X^{\alpha} \succ X^{\gamma}X^{\beta}$ para todo $X^{\gamma} \in T^n$.

Definición 5.3. (Orden lexicográfico)
Sean $\alpha, \beta \in Z^n_{\geq 0}$ y $X^{\alpha}, X^{\beta} \in T^n$

$$X^{\alpha} \succ_{lex} X^{\beta} \Leftrightarrow \begin{cases} \alpha = \beta \\ \text{ó} \\ \exists j \text{ tal que } \alpha_i = \beta_i \quad \forall i = 1, \ldots, j-1 \text{ y } \alpha_j < \beta_j \end{cases}.$$

Ejemplo 5.4. Dado el polinomio
$f(X, Y, Z) = X^3YZ - 5X^2Z^5 + 6Y^3Z^2 + 7XY^2Z^4$
Ordenando por orden lexicográfico
$X^{(0,3,2)} \succ_{lex} X^{(1,2,4)} \succ_{lex} X^{(2,0,5)} \succ_{lex} X^{(3,1,1)}$ o también podemos ordenar por sus multiindices $(0, 3, 2) < (1, 2, 4) < (2, 0, 5) < (3, 1, 1)$, según $\succ_{lex}$.
De donde:
Su coeficiente líder $cl(f) = 1$.
Su monomio líder $ml(f) = X^3YZ$.
Su término líder $tl(f) = X^3YZ$.

Definición 5.5. Orden lexicográfico graduado
Sean $\alpha, \beta \in Z^n_{\geq 0}$ y $X^{\alpha}, X^{\beta} \in T^n$

$$X^{\alpha} \succ_{lexg} X^{\beta} \Leftrightarrow \begin{cases} |\alpha| < |\beta| \quad , |\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n \\ \text{ó} \\ |\alpha| = |\beta| \text{ y } X^{\alpha} \succ_{lex} X^{\beta} \end{cases}.$$

Ejemplo 5.6. Dado el polinomio
$f(X, Y, Z) = 3X^2Y^2Z - 2X^3Z^2 + 7XY^3Z^3 - 5X^3Y^4$.
Calculemos el grado de f
$f = 3\underbrace{X^2Y^2Z}_{5} - 2\underbrace{X^3Z^2}_{5} + 7\underbrace{XY^3Z^3}_{7} - 5\underbrace{X^3Y^4}_{7}$.
Vemos que $|(1, 3, 3)| = |(3, 4, 0)| = 7$, entonces $X^{(1,3,3)} \succ_{lex} X^{(3,4,0)}$
De donde:
Su coeficiente líder $cl(f) = -5$.

Su monomio líder $ml(f) = X^3Y^4$.

Su término líder $tl(f) = -5X^3Y^4$.

Definición 5.7. Orden lexicográfico graduado inverso

Sean $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ y $X^\alpha, X^\beta \in T^n$

$$X^\alpha <_{grevlex} X^\beta \iff \begin{cases} |\alpha| < |\beta| \\ |\alpha| = |\beta| \text{ y en } \alpha - \beta \in \mathbb{Z}^n_{\geq 0} \text{ el primer elemento distinto de cero de derecha a izquierda es negativo.} \end{cases}$$

Ejemplo 5.8. Dado el polinomio

$f(X, Y, Z) = 2X^3Y^2Z^2 + 4X^2Z^3 - 3XY^3Z^2 - XY^3Z$.

Calculemos el grado de f

$f = 2X^3Y^2Z^2 + 4X^2Z^3 - 3XY^3Z^2 - XY^3Z$.

$\underbrace{\quad}_{6} \quad \underbrace{\quad}_{5} \quad \underbrace{\quad}_{4} \quad \underbrace{\quad}_{5}$

Ordenando por orden lexicográfico graduado inverso

$X^{(1,3,2)} >_{grevlex} X^{(3,1,2)} >_{grevlex} X^{(1,3,1)} >_{grevlex} X^{(2,0,3)}$ De

donde:

Su coeficiente líder $cl(f) = -3$.

Su monomio líder $ml(f) = XY^3Z^2$.

Su término líder $tl(f) = -3XY^3Z^2$.

Máximo común divisor y Mínimo común múltiplo

Sean $m_1 = X_1^{\alpha_1}X_2^{\alpha_2} \ldots X_n^{\alpha_n}$, $m_2 = X_1^{\beta_1}X_2^{\beta_2} \ldots X_n^{\beta_n} \in T^n$, diremos que m_1 divide a m_2 $(m_1|m_2)$, si $\alpha_i \leq \beta_i$ para todo $i = 1, \ldots, n$.

El máximo común divisor de m_1 y m_2 viene dado por

$$mcd(m_1, m_2) = X_1^{\min\{\alpha_1,\beta_1\}} \ldots X_n^{\min\{\alpha_n,\beta_n\}}$$

El mínimo común múltiplo de m_1 y m_2 viene dado por

$$mcm(m_1, m_2) = X_1^{\max\{\alpha_1,\beta_1\}} \ldots X_n^{\max\{\alpha_n,\beta_n\}}$$

Definición 5.9. Sea $f \in k[X_1, \ldots, X_n]$, definimos el soporte de f como:

$$Supp(f) = \{X^\alpha : a_\alpha \neq 0\}.$$

Donde $f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha X^\alpha$ y $X^\alpha \in T^n$.

Es fácil observar que, $Supp(f) = \emptyset$ si y solo si $f \neq 0$.

Definición 5.10. Sea $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$. Definimos el ideal generado por los polinomios $f_1, \ldots, f_s$ como

$$\langle f_1, \ldots, f_s \rangle = \{p_1 f_1 + \cdots + p_s f_s : p_i \in k[X_1, \ldots, X_n], \text{para } i = 1, 2, \ldots, s\}.$$

Por ejemplo, consideramos los polinomios,

$$f_1 = X^3 + Y^2 + 1,$$
$$f_2 = X^2 - Y^2 - 1.$$

El polinomio,

$$f = X^4 - Y^3 + YX^2 - Y^2 - Y - 1 = (X - 1)(X^3 + Y^2 + 1) + (X + Y)(X^2 - Y^2 - 1),$$

es un elemento del ideal $\langle f_1, f_2 \rangle$.

Proposición 5.11. Si $I = \langle f_1, \ldots, f_s \rangle$ es un ideal del anillo $k[X_1, \ldots, X_n]$. Entonces

i) $\langle f_1, \ldots, f_s \rangle = \langle mcd(f_1, \ldots, f_s) \rangle$.

ii) Si $s \leq 3$ entonces $\langle f_1, \ldots, f_s \rangle = \langle f_1, mcd(f_2, \ldots, f_s) \rangle$.

Ideales monomiales

Un **ideal monomial** en $k[X_1, \ldots, X_n]$ es un ideal generado por monomios. Esta clase de ideales es de nuestro interés, para el cálculo de las bases de Gröbner dado que reduce la dificultad del cálculo.

Ejemplo 5.12. El ideal $I = \langle X^2, Y^3 \rangle$ es monomial, además $2X^2 - Y^3 \in I$, es decir, los ideales monomiales contienen más que solo monomios, además el ideal $J = \langle 2X^2 - Y^3, Y^3 \rangle$ aunque no está definido por monomios, se puede verificar que $J = \langle X^2, Y^3 \rangle = I$.

Lema 5.13. *Lema de Dickson para ideales monomiales*
Los ideales monomiales son finitamente generado.

Prueba. Para demostrar este lema, utilizaremos un proceso inductivo sobre el número de variables (n).
Para $n = 1$, el conjunto viene dado por monomios que son potencias de X_1, podemos

considerar al ideal $I = \langle X^a \rangle$, donde $a \in \mathbb{N}$ es el número más pequeño.
Para $n > 1$, consideremos el conjunto

$$\mathbf{I} = \{X^{\alpha} \in k[X_1, \ldots, X_{n-1}] / X^{\alpha} X_n^b \in I \text{ para algún } b \leq 0\}.$$

Es claro que $\mathbf{I}$ es un ideal monomial, en efecto, sea $X^{\alpha} \in \mathbf{I}$ entonces $X^{\alpha} X_n^b \in I$ y consideremos el monomio X^{β} tal que $X^{\alpha} | X^{\beta}$, como I es ideal entonces $X^{\beta} X^b \in I$, así tenemos que $X^{\beta} \in \mathbf{I}$.

Por nuestra hipótesis inductiva $\mathbf{I} \to k[X_1, \ldots, X_{n-1}]$ es un ideal finitamente generado, es decir,

$$\mathbf{I} = \langle X^{\alpha_1}, X^{\alpha_2}, \cdots, X^{\alpha_r} \rangle.$$

Para cada X^{α_i} existe un $b_i \leq 0$ tal que $X^{\alpha_i} X_n^{b_i} \in I$, consideremos $0 \leq k < m$, donde $m = \max\{b_1, b_2, \ldots, b_r\}$.
Sea los ideales

$$I_k = \{X^{\alpha} \in k[X_1, \ldots, X_{n-1}] / X^{\alpha} X_n^k \in I\} \to k[X_1, \ldots, X_{n-1}].$$

Por hipótesis inductiva

$$I_k = \langle X^{\alpha_{1,k}} \ldots, X^{\alpha_{r_k,k}} \rangle, \text{ con } X^{\alpha_{i,k}} X_n^k \in I \quad \forall i = 1, \ldots, r_k.$$

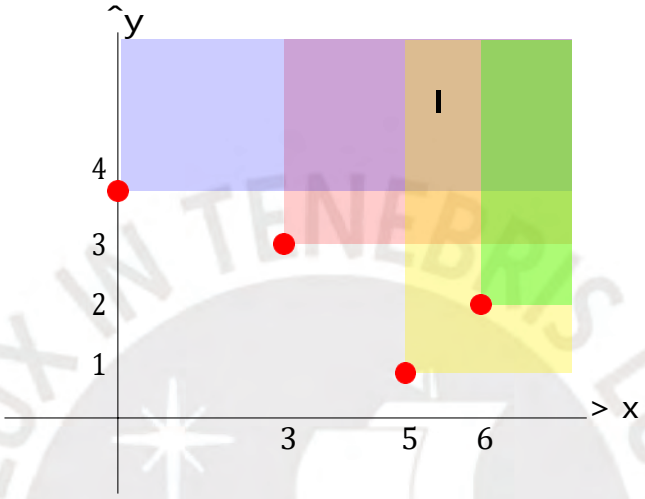
Consideremos $J = \langle X^{\alpha_{1,k}} X_n^k \ldots, X^{\alpha_{r_k,k}} X_n^k / k = 0, \ldots, m \rangle$, probaremos que $I = J$ donde $X^{\alpha_{j,m}} = X^{\alpha_j}$, $j = 1, \ldots, r$.
En efecto, para todo monomio $X^{\alpha} X_n^p \in I$, con $X^{\alpha} \in k[X_1, \ldots, X_n]$. Tenemos dos casos a considerar:

- Suponiendo que $p \leq m$, como $X^{\alpha} X_n^p \in I$ se tiene $X^{\alpha} \in \mathbf{I}$ entonces existe i tal que $X^{\alpha_i} | X^{\alpha}$, luego $X^{\alpha_i} X_n^{m_i} | X^{\alpha} X_n^p$ entonces $X^{\alpha} X_n^p \in J$.
- Supongamos que $p \leq m-1$, $X^{\alpha} \in I_K$ entonces existe $X^{\alpha_{p,i}} | X^{\alpha}$. Así $X^{\alpha_{p,i}} X_n^p | X^{\alpha} X_n^p$, esto es, $X^{\alpha} X_n^p \in J$.

Por lo tanto, $I \to J \to I$. □

Ejemplo 5.14. Tomemos el ideal $I = \langle Y^4, X^3Y^3, X^5Y, X^6Y^2 \rangle$. Se puede observar que si $X^a Y^b \in I$, entonces $X^{a+\alpha} Y^{b+\beta} \in I$ para toda $(\alpha, \beta) \in \mathbb{Z}^2_{\leq 0}$ es cual podemos calcularlo usando el software Singular,
además podemos visualizar a I en el siguiente diagrama

```
> ring R=0,(x,y),lp;
> ideal I=y^4,x^3*y^3,x^5*y,x^6*y^2;
> minbaseMon(I);
_[1]=y4
_[2]=x3y3
_[3]=x5y
>
```



Vemos que I está generado mínimimamente por $\{Y^4, X^3Y^3, X^5Y\}$.

Teorema 5.15. *Teorema de la Base de Hilbert*
Se cumple las siguientes propiedades:

i) Si I es un ideal de $k[X_1, \ldots, X_n]$, entonces existen polinomios $f_1, f_2, \ldots, f_s \in k[X_1, \ldots, X_n]$, tal que $I = \langle f_1, f_2, \ldots, f_s \rangle$.

ii) Si $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ es una cadena creciente de ideales en $k[X_1, \ldots, X_n]$, entonces existe un N tal que $I_N = I_{N+1} = I_{N+2} = \cdots$

Algoritmo de la división

Vamos a definir un algoritmo de la división en $k[X_1, \ldots, X_n]$, la idea básica que tiene el algoritmo es similar a la divisón clásica, cuando dividimos f por g, se busca cancelar términos de f usando el término lider de g.

Teorema 5.16. *Algoritmo de la división*
Consideremos la relación de orden $\prec$ en T^n y $g \in k[X_1, \ldots, X_n]$ no nulo. Entonces para todo $f \in k[X_1, \ldots, X_n]$ existen y son únicos $q, r \in k[X_1, \ldots, X_n]$ tal que $f = gq + r$ donde $r = 0$ ó $ml(g) \nmid m, \forall m \in Supp(r)$.

Prueba. Ver la prueba en [Sal09]. (ver también el siguiente ejemplo 5.17). □

Como parte de la prueba en [Sal09], se define

$$S(f) = \{m \in Supp(f) / ml(g) | m\}.$$

el cual será usado en el ejemplo 5.17.

Ejemplo 5.17. Sean los polinomios $f = XY^2 + 4XY - 3X^2$ y $g = X + 2Y + 1$ con orden c_{lexg} con $X < Y$.

Calculemos $ml(g) = Y$.

$S(f) = \{XY^2, 4XY\}$, calculamos $m_0 = máxS(f) = XY^2$, vamos a eliminar el término lider de f, mediante

$$f_1 = f - \frac{m_0}{tl(g)} \cdot g = XY^2 + 4XY - 3X^2 - XY^2 - \frac{X^2Y}{2} - \frac{XY}{2}.$$

Así, $f_1 = \frac{7XY}{2} - 3X^2 - \frac{X^2Y}{2}$, ahora calculamos

$S(f_1) = \{\frac{7XY}{2}, -\frac{X^2Y}{2}\}$, $m_1 = máxS(f_1) = -\frac{X^2Y}{2}$, eliminamos el término lider de f_1, mediante

$$f_2 = f_1 - \frac{m_1}{tl(g)} \cdot g = \frac{7XY}{2} - 3X^2 - \frac{X^2Y}{2} + \frac{X^2Y}{2} + \frac{X^3}{4} + \frac{X^2}{4}.$$

Así, $f_2 = \frac{7XY}{2} + \frac{X^3}{4} - \frac{11X^2}{4}$, ahora calculamos

$S(f_2) = \{\frac{7XY}{2}\}$, $m_2 = máxS(f_2) = \frac{7XY}{2}$, eliminamos el término lider de f_2, mediante

$$f_3 = f_2 - \frac{m_1}{tl(g)} \cdot g = \frac{7XY}{2} + \frac{X^3}{4} - \frac{11X^2}{4} - \frac{7XY}{2} - \frac{7X^2}{4} - \frac{7X}{4}.$$

Así, $f_3 = \frac{X^3}{4} - \frac{9X^2}{2} - \frac{7X}{4}$, ahora calculamos

$S(f_3) = \{\}$, eso indica que nuestro proceso ha terminado, por lo tanto

$$f = \frac{m_2 + m_1 + m_0}{tl(g)} \cdot g + f_3.$$

Así,

$q = \frac{m_2+m_1+m_0}{tl(g)} = \frac{7X}{4} - \frac{X^2}{4} + \frac{XY}{2}$

$r = f_3 = \frac{X^3}{4} - \frac{9X^2}{2} - \frac{7X}{4}$

Teorema 5.18. *(Algoritmo de la pseudodivisión)*

Consideremos la relación de orden c en T^n. Dados los polinomios no nulos $g_1, \ldots, g_s \in k[X_1, \ldots, X_n]$. Entonces para todo $f \in k[X_1, \ldots, X_n]$ existen los polinomios $q_1, \ldots, q_s, r \in k[X_1, \ldots, X_n]$ tal que:

$f = q_1g_1 + \cdots + q_sg_s + r$, donde $r = 0$ ó $ml(g_i) \nmid m, \forall m \in Supp(r)$ y $\forall i = 1, \ldots, s$.

Prueba. La construcción de $q_1, \ldots, q_s$ y r será por inducción.

Paso 0 tenemos $f = \sum_{j=1}^{s} q_j^0 g_j + r_0 + h_0$, donde $q_j^0 = 0 = r_0$ y $h_0 = f$ □

Paso k tenemos $f = \sum_{j=1}^{s} q_j^k g_j + r_k + h_k$,

Si $h_k = 0$ finaliza el algoritmo.

Si $h_k \neq 0$, consideramos los siguientes casos:

Caso 1 $\exists i_k$ tal que $ml(g_{i_k}) | ml(h_k)$

$$f = \sum_{j \neq i_k} q_j^k g_j + \left(q_{i_k}^k + \frac{tl(h_k)}{tl(g_{i_k})}\right) g_{i_k} + r_k + \left(h_k - \frac{tl(h_k)}{tl(g_{i_k})} g_{i_k}\right)$$

$$\underbrace{\sum_{j \neq i_k} q_j^k g_j + \left(q_{i_k}^k + \frac{tl(h_k)}{tl(g_{i_k})}\right)}_{q_j^{k+1}} g_{i_k} + \underbrace{r_k}_{r_{k+1}} + \underbrace{\left(h_k - \frac{tl(h_k)}{tl(g_{i_k})} g_{i_k}\right)}_{h_{k+1}}$$

$m_k = ml(h_k) > ml\left(h_k - \frac{tl(h_k)}{tl(g_{i_k})} g_{i_k}\right) = ml(h_{k+1}) = m_{k+1}$.

Caso 2 Si tenemos lo contrario del caso 1

$$f = \sum_{j=1}^{s} \underbrace{q_j^k}_{q_j^{k+1}} g_j + \underbrace{(r_k + tl(h_k))}_{r_{k+1}} + \underbrace{(h_k - tl(h_k))}_{h_{k+1}}$$

$m_k = ml(h_k) > ml\,(h_k - tl(h_k)) = ml(h_{k+1}) = m_{k+1}$.

Así, tenemos $m_0 > m_1 > \cdots$ por el principio del buen orden monomial c se tiene que la secuencia es finita, esto es, $\exists k_0$ talque $h_{k_0} = 0$. □

Ejemplo 5.19. Consideremos el orden lexicográfico graduado c_{lexg}, y los polinomios

$f = X^5 - X^3Y + XY^2 - X^2 + X + Y$.

$g_1 = X^2 - Y$, $ml(g_1) = X^2$.

$g_2 = Y^2 - X$, $ml(g_2) = Y^2$.

Realizamos el proceso de igual manera que la prueba

$$f = \underbrace{0}_{q_1^0} g_1 + \underbrace{0}_{q_2^0} g_2 + \underbrace{0}_{r_0} + \underbrace{f}_{h_0}$$

$ml(h_0) = ml(f) = X^5$, estamos en el caso 1, como $ml(g_1) | ml(h_0)$ entonces

$$f = \underbrace{\left(0 + \frac{X^5}{X^2}\right)}_{q_1^1} g_1 + \underbrace{0}_{q_2^1} g_2 + \underbrace{0}_{r_1} + \underbrace{(f - X^3 g_1)}_{h_1}$$

Así, tenemos $q_1^1 = X^3$, $q_2^1 = 0$, $r_1 = 0$ y $h_1 = XY^2 - X^2 + X + Y$.

$ml(h_1) = XY^2$, estamos en el caso 1, como, $ml(g_2) | ml(h_1)$

$$f = \underbrace{X^3}_{q_1^2} g_1 + \underbrace{\left(0 + \frac{XY^2}{Y^2}\right)}_{q_2^2} g_2 + \underbrace{0}_{r_2} + \underbrace{(h_1 - Xg_2)}_{h_2}.$$

Así, tenemos $q_1^2 = X^3$, $q_2^2 = X$, $r_2 = 0$ y $h_2 = X + Y$.

$ml(h_2) = X$, estamos en el caso 2, como, $ml(g_i) \nmid ml(h_2)$, $i = 1, 2$

$$f = \underbrace{X^3}_{q_1^3} g_1 + \underbrace{X}_{q_2^3} g_2 + \underbrace{(0 + X)}_{r_3} + \underbrace{(h_2 - X)}_{h_3} . X$$

Así, tenemos $q_1^3 = X^3$, $q_2^3 = X$, $r_3 = X$ y $h_3 = Y$.

$ml(h_3) = Y$, estamos en el caso 2, como, $ml(g_i) \nmid ml(h_3)$, $i = 1, 2$

$$f = \underbrace{X^3}_{q_1^4} g_1 + \underbrace{X}_{q_2^4} g_2 + \underbrace{(X + Y)}_{r_4} + \underbrace{(h_3 - Y)}_{h_4} . X$$

Así, tenemos $q_1^4 = X^3$, $q_2^4 = X$, $r_4 = X + Y$ y $h_4 = 0$.

Como $h_4 = 0$ el algoritmo término

$$f = X^3 g_1 + X g_2 + (X + Y).$$

Observación 5.20. Notemos que:

$$ml(f) = X^5 = máx\{\underbrace{ml(q_1^4)}_{X^3} ml(g_1), \underbrace{ml(q_2^4)}_{X^2} ml(g_2)\} = máx\{\underbrace{X^5}_{X^3}, \underbrace{XY^2}_{X^2}\}.$$

Corolario 5.21. Con el enunciado del algoritmo de pseudodivisión se tiene

$$ml(f) = máx\{ml(q_1)ml(g_1), \ldots, ml(q_s)ml(g_s)\}.$$

Observación 5.22. Lo mencionado en el corolario 5.21 no se cumple para cualquier expresión de f como combinación de los g_i más un polinomio.
Por ejemplo $Z + Y = 1(X^2 + Z + Y) + (-1)(X^2) + 0$.

$$ml(Z + Y) = Y, \quad ml(1(X^2 + Z + Y)) = X^2, \quad ml((-1)(X^2)) = X^2.$$

Definición 5.23. Fijemos un orden monomial c en $k[X_1, \ldots, X_n]$, sea el ideal $I \to k[X_1, \ldots, X_n]$. Una base de Gröbner para I (con respecto a c) es una colección finita de polinomios $G = \{g_1, g_2, \ldots, g_s\} \to I$ con la propiedad de que cada polinomio no nulo $f \in I$, $ml(f)$ es divisible por $ml(g_i)$ para algún i.

Ejemplos 5.24. Daremos algunos ejemplos de bases de Gröbner:

1. Sea $I = \langle f \rangle \to k[X]$. El conjunto $G = \{f\}$ es una base de Gröbner de I, en efecto, si $h \in I$ entonces existe un g tal que $h = f \cdot g$, de donde $ml(h) = ml(f) \cdot ml(g)$ por lo tanto $ml(g) | ml(h)$.

2. $I = \langle m_1, \ldots, m_r \rangle \subseteq k[X_1, \ldots, X_n]$, $m_i \in T^n$, entonces $G = \{m_1, \ldots, m_r\}$ es una base de Gröbner de I.
   Dado que si $f \in I$, $f = \sum_i g_i m_i$ $g_i \in k[X_1, \ldots, X_n]$. Sabemos que $m \in I$ $\forall m \in Supp(f)$. En particular $ml(f) \in I$, luego existe i tal que $ml(m_i) | ml(f)$.

3. Fijemos el orden lexicográfico graduado en $k[X, Y]$
   Sea $I = \langle Y^2 - X, XY - Y \rangle$, es claro que $X^2 - X \in I$, pues

$$X^2 - X = Y(XY - Y) - (X - 1)(Y^2 - X) \in I.$$

   El conjunto $G = \{Y^2 - X, XY - Y\}$ no es una base de Gröbner, pues $ml(X^2 - X) = X^2$ no es divisible por $ml(Y^2 - X) = Y^2$, ni $ml(XY - Y) = XY$.
   Si usamos el software Singular [DGPS19], veamos cuál es la base de Gröbner

```
> ring R=0,(x,y),dp;
> poly f1=y^2-x;
> poly f2=x*y-y;
> ideal I=f1,f2;
> ideal sI=groebner(I);
> sI;
sI[1]=y2-x
sI[2]=xy-y
sI[3]=x2-x
```

   este proceso, lo veremos en detalle en el ejemplo 5.31.

Teorema 5.25. Sea I un ideal no nulo de $k[X_1, \ldots, X_n]$ y fijemos un orden monomial c. Las siguientes proposiciones son equivalentes, para el subconjunto de polinomios no nulo $G = \{g_1, \ldots, g_s\} \subseteq I$.

i) G es una base de Gröbner para I.

ii) $f \in I$ si y solo si en la pseudodivisión de f por $g_1, \ldots, g_s$ el resto es cero.

iii) $f \in I$ si y solo si $f = \sum_{i=1}^{s} q_i g_i$ con $ml(f) = máx\{ml(q_i)ml(g_i) / i = 1, \ldots, s\}$.

iv) $\langle ml(G) \rangle = \langle ml(I) \rangle$, donde $ml(G) = \{ml(g_i) / i = 1, \ldots, s\}$ y $ml(I) = \{ml(f) / f \in I\}$.

Prueba. La prueba del teorema lo pueden revisar en el libro [AL94], [MGB07]. □

Cálculo de las bases de Gröbner

Definición 5.26. Sean $f, g \in k[X_1, \ldots, X_n]$ no nulos. Dado un orden monomial c, el **S-proceso** o **S-polinomio** de f y g es denotado por $S(f, g)$, como:

$$S(f, g) = \frac{m}{tl(f)} \cdot f - \frac{m}{tl(g)} \cdot g,$$

donde $m = mcm(ml(f), ml(g))$.

Ejemplo 5.27. Dados los polinomios $f = Y^5 - XY$, $g = XY^4 - XY^2$.

- Si usamos orden monomial c_{lex}

$f = Y^5 - XY$, $ml(f) = XY$, $tl(f) = -XY$.

$g = XY^4 - XY^2$, $ml(g) = XY^4$, $tl(g) = XY^4$.

$mcm(ml(f), ml(g)) = mcm(XY, XY^4) = XY^4$.

$$S(f, g) = -Y^3(Y^5 - XY) - (XY^4 - XY^2) = XY^2 - Y^8.$$

- Si usamos orden monomial c_{lexg}

$f = Y^5 - XY$, $ml(f) = Y^5$, $tl(f) = Y^5$.

$g = XY^4 - XY^2$, $ml(g) = XY^4$, $tl(g) = XY^4$.

$mcm(ml(f), ml(g)) = mcm(Y^5, XY^4) = XY^5$.

$$S(f, g) = X(Y^5 - XY) - Y(XY^4 - XY^2) = XY^3 - X^2Y.$$

Propiedad 5.28. Sean $f, g \in k[X_1, \ldots, X_n]$ no nulos. Fijemos un orden monomial c. El *S-polinomio* de f y g, $S(f, g)$ cumple:

1. $S(f, g) = -S(g, f)$.
2. Si f y g son monomios entonces $S(f, g) = 0$.
3. $ml(S(f,g) \subset mcm(ml(f), ml(g))$.

Teorema 5.29. *(Teorema de Buchberger)*
Fijemos un orden monomial c. El conjunto $G = \{g_1, \ldots, g_s\} \subset k[X_1, \ldots, X_n]$ es una base de Gröbner respecto a c, para el ideal $I = \langle g_1, \ldots, g_s \rangle$, si y solo si para todo $i \neq j$ el resto de los $S(g_i, g_j)$ divididos por la pseudodivisión por $g_1, \ldots, g_s$ es cero.

Prueba. La prueba lo pueden revisar en [AL94]. □

Teorema 5.30. *(Algoritmo de Buchberger)*
Fijemos un orden monomial c. Sea $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideal de $k[X_1, \ldots, X_n]$. Entonces una base de Gröbner respecto a c, puede construirse por un número finito de pasos del siguiente algoritmo.

Entrada: Los generadores de I: $f_1, \ldots, f_s$
Defina: $tt_0 = \emptyset$ y $tt_1 = \{f_1, \ldots, f_s\}$
Mientras $tt_{i-1} \neq tt_i$ realice:
1. Si $\exists f, g \in tt_i$ tal que el resto r de $S(f, g)$ divididos por la pseudodivisión con los elementos de tt_i, es distinto de cero entonces $tt_{i+1} = tt_i \cup \{r\}$.
2. Caso contrario, todos los restos de los S-procesos de los elementos de tt_i por la pseudodivisión con los elementos de tt_i es cero, entonces $tt_{i+1} = tt_i$.
Salida: Base de Gröbner $tt = \{g_1, \ldots, g_t\}$ para I.

Prueba. Siguiendo el algoritmo, definimos

$$G_0 = \emptyset \quad \text{y} \quad G_1 = \{f_1, \ldots, f_s\}.$$

Si $\exists f, g \in G_i$ tal que el resto r de $S(f, g)$ por la pseudodivisión con los elementos de G_i, es no nulo, entonces definimos $G_{i+1} = G_i \cup \{r\}$.
Caso contrario $G_{i+1} = G_i$. Si en algún paso del proceso k tenemos los restos de $S(f, g)$ por la pseudovisión con G_k, son ceros $\forall f, g \in G_k$ entonces G_k es una base de Gröbner por el Teorema de Buchberger, y el algoritmo término.
Suponiendo que no sucediera lo afirmado (que en alguna parte del proceso tenemos restos ceros) tendríamos una secuencia creciente estrictamente

$$G_1 \subset G_2 \subset G_3 \subset \cdots$$

Según el algoritmo $G_{i+1} = G_i \cup \{r\}$, $0 \neq r$ es el resto de $S(f, g)$ por G_i para algunos $f, g \in G_i$. Tenemos $ml(r) \in ml(G_{i+1})$ y $ml(g) \nmid m$, $\forall m \in Supp(r)$ y $\forall g \in G_i$. En particular $ml(r) \notin ml(G_i)$ entonces $ml(G_i) \subset ml(G_{i+1})$, luego

$$\langle ml(G_1) \rangle \subset \langle ml(G_2) \rangle \subset \cdots \subset \langle ml(G_j) \rangle \subset \cdots$$

Así $\left\langle \bigcup_{i=1}^{*} ml(G_i) \right\rangle^{+}$ no tiene un número finito de generadores contenidos en $S = \bigcup_{i=1} ml(G_i)$, el cual es una contradicción por el lema de Dickson. □

Ejemplo 5.31. Fijemos el orden monomial c_{lexg} y el ideal $I = \langle f_1, f_2 \rangle \to k[X, Y]$
$f_1 = Y^2 - X$, $ml(f_1) = Y^2$, $tl(f_1) = Y^2$.

$f_2 = XY - Y$, $\quad ml(f_2) = XY$, $\quad tl(f_2) = XY$.

Siguiendo el algoritmo: $G_0 = \emptyset$ y $G_1 = \{Y^2 - X, XY - Y\}$.

$S(f_1, f_2) = Y^2 - X^2$.

Realizamos la pseudodivisión de $S(f_1, f_2)$ con f_1 y f_2, de donde

$$S(f_1, f_2) = \underbrace{1}_{q_1} f_1 + \underbrace{0}_{q_2} f_2 + \underbrace{(-X^2 + X)}_{r}.$$

Como $r \neq 0$, por el algoritmo de Buchberger $G_2 = G_1 \cup \{r\} = \{f_1, f_2, r\}$.

Consideremos $f_3 = r$ entonces $G_2 = \{f_1, f_2, f_3\}$

$f_3 = -X^2 + X$, $\quad ml(f_3) = X^2$, $\quad tl(f_3) = -X^2$.

Calculemos $S(f_1, f_3)$ y la pseudodivisión con cada elemento de G_2.

- $S(f_1, f_3) = XY^2 - X^3$, ahora dividimos

$$S(f_1, f_3) = \underbrace{X}_{q_1} f_1 + \underbrace{0}_{q_2} f_2 + \underbrace{X}_{q_3} f_3 + \underbrace{0}_{r}.$$

Calculemos $S(f_2, f_3)$ y la pseudodivisión con cada elemento de G_2.

- $S(f_2, f_3) = 0$, quiere decir que ya es divisible, esto es,

$$S(f_2, f_3) = \underbrace{0}_{q_1} f_1 + \underbrace{0}_{q_2} f_2 + \underbrace{0}_{q_3} f_3 + \underbrace{0}_{r}.$$

- $S(f_1, f_2) = Y^2 - X^2$, de lo anterior cumple:

$$S(f_1, f_2) = \underbrace{1}_{q_1} f_1 + \underbrace{0}_{q_2} f_2 + \underbrace{1}_{q_3} f_3 + \underbrace{0}_{r}.$$

Por lo tanto $G_2 = \{f_1, f_2, f_3\}$ es una base de Gröbner de I.

Ejemplo 5.32. Usando los polinomios del ejemplo 5.27 y el orden monomial c_{lexg}

$f_1 = Y^5 - XY$, $\quad f_2 = XY^4 - XY^2$.

La base de Gröbner para el ideal $I = \langle f_1, f_2 \rangle$ es

$$G = \{XY^3 - X^2Y, X^2Y^2 - XY^2, X^3Y - X^2Y, Y^5 - XY\}.$$

Este ejemplo ha sido calculado con el software Singular.

Bases de Gröbner para submódulos

Un monomio sobre $A^m = (k[X_1, \ldots, X_n])^m$ es un elemento de la forma $m = X^\alpha e_j$, $j = 1, 2, \ldots, n$, $e_j = (0, 0, \ldots, \underbrace{1}_{\text{pos } j}, \ldots, 0)$.

```
> ring R=0,(x,y),dp;
> poly f1=y^5-x*y;
> poly f2=x*y^4-x*y^2;
> ideal I=f1,f2;
> ideal sI=groebner(I);
> sI;
sI[1]=xy3-x2y
sI[2]=x2y2-xy2
sI[3]=x3y-x2y
sI[4]=y5-xy
```

Consideremos el polinomio $f \in A^m$, de la siguiente forma

$$f = \sum_{\downarrow} c_{\downarrow} X^{\downarrow} e_{i_{\downarrow}}, \quad c_{\downarrow} \in k.$$

Denotemos por

$$M(f) = \{X^{\downarrow} e_{i_{\downarrow}} \mid c_{\downarrow} \neq 0\}.$$

El conjunto de los monomios no nulos de f, del siguiente ejemplo 5.33, será:

$$M(f) = \{X_1^2 e_1, X_1^5 X_3^6 e_1, X_1 X_2^2 X_3^3 e_2, X_3^9 e_2\}.$$

Vamos a considerar al conjunto formado por todos los monomios de $(k[X_1, \ldots, X_n])^m$ como:

$$M^{(n)} = \{X^{\downarrow} e_{j_{\downarrow}} / X^{\downarrow} \in T^n\}.$$

Ejemplo 5.33. Consideremos A^2, dado por $A = k[X_1, X_2, X_3]$.
Sea $f \in A^2$, $f = (2X_1^2 + 3X_1^5X_3^6, X_1X_2^2X_3^3 - 2X_3^9)$, podemos expresarlo como

$$f = 2(X^2, 0) + 3(X_1^5X_3^6, 0) + (0, X_1X_2^2X_3^3) - 2(0, X_3^9).$$

Por lo tanto, $f = 2X_1^2e_1 + 3X_1^5X_3^6e_1 + X_1X_2^2X_3^3e_2 - 2X_3^9e_2$.

Definición 5.34. Una relación de orden total es una relación de orden monomial en $M^{(n)}$ de A^n, si se cumple:

- $\forall\, m_1, m_2 \in M^{(n)}$ y $m_1 \neq m_2 \Rightarrow m.m_1 \neq m.m_2 \quad (\forall\, m_2 \in M^{(n)})$.
- (Principio del Buen Orden) Todo conjunto de $M^{(n)}$ tiene elemento mínimo.

En particular se definen dos nuevas ordenes monomiales, teniendo en consideración que $e_1 > e_2 > e_3 > \ldots$ (vectores canónicos).

Definición 5.35. (Término sobre posición, TSP)
Sean $\alpha, \beta \in \mathbb{Z}^n_{\leq 0}$ y $X^\alpha, X^\beta \in T^n$. Diremos que:

$$X^\alpha e_i \ c_{TSP} \ X^\beta e_j \quad \text{(están en relación de término sobre posición)} \quad \Leftrightarrow \quad \begin{cases} X^\alpha \ c \ X^\beta \\ \text{ó} \\ \alpha = \beta \ \wedge \ i > j \end{cases}$$

Ejemplo 5.36. Consideremos $A = k[X_1, X_2, X_3]$, con $e_1 > e_2 > e_3$ y los monomios $m_1 = X_1X_2^2X_3^3e_1$, $m_2 = X_1^2X_3^3e_2$ y $m_3 = X_1^2X_3^3e_1$ $(m_1, m_2, m_3 \in M(3))$

$$m_1 = X_1X_2^2X_3^3e_1 \ c_{TSP} \ X_1^2X_3^3e_2 = m_2.$$

$$m_2 = X_1^2X_3^3e_2 \ c_{TSP} \ X_1^2X_3^3e_1 = m_3.$$

Definición 5.37. (Posición sobre término, PST)
Sean $\alpha, \beta \in \mathbb{Z}^n_{\leq 0}$ y $X^\alpha, X^\beta \in T^n$. Diremos que:

$$X^\alpha e_i \ c_{PST} \ X^\beta e_j \quad \text{(están en relación de posición sobre término)} \quad \Leftrightarrow \quad \begin{cases} i > j \\ \text{ó} \\ i = j \ \text{y} \ X^\alpha \ c \ X^\beta \end{cases}$$

Ejemplo 5.38. Consideremos $A = k[X_1, X_2, X_3]$, con $e_1 > e_2 > e_3$ y los monomios $m_1 = X_1X_2^2X_3^3e_1$, $m_2 = X_1^2X_3^3e_2$ y $m_3 = X_1^2X_3^3e_1$ $(m_1, m_2, m_3 \in M(3))$

$$m_2 = X_1^2X_3^3e_2 \ c_{PST} \ X_1X_2^2X_3^3e_1 = m_1.$$

$$m_1 = X_1X_2^2X_3^3e_1 \ c_{PST} \ X_1^2X_3^3e_1 = m_3.$$

Observación 5.39. Para el presente trabajo usaremos el orden PST (Posición sobre término).

Definición 5.40. Sea $f = 0$ un elemento de A^m, entonces podemos escribir

$$f = a_1m_1 + a_2m_2 + \cdots + a_lm_l.$$

Donde $a_i \in F_q - \{0\}$ y m_i es un monomio de A^m para todo $i = 1, 2, \ldots, l$.

- El monomio líder de f en A^m, es

$$ml(f) = \text{máx}\{m/m \in M(f)\}.$$

Si considera $m_1 > m_2 > \cdots > m_l$ entonces $ml(f) = m_1$.

- El multigrado de $f \in A^m$, se define como

  $$\text{multigrad}(f) = \alpha = (\alpha_1, \alpha_2, \ldots), \quad \text{donde} \quad X^{\alpha} e_j \text{ es el monomio líder de } f.$$

- El término líder será $\text{tl}(f) = a_i m_i$, cuyo coeficiente líder es a_i, si consideráramos $m_1 > m_2 > \cdots > m_l$ entonces $\text{tl}(f) = a_1 m_1$ y el coeficiente l´ıder es a_1.

Ejemplo 5.41. Consideremos el polinomio en A^3, con $A = k[X, Y, Z]$

$$f = 3X^2Y\, e_1 - ZY^3 e_1 + 2X^3Y^5 e_2 - 5Z^3 e_3.$$

Considerando orden PST y el orden lexicográfico $X > Y > Z$; $e_1 > e_2 > e_3$

$$X^2Y\, e_1 >_{PST} ZY^3 e_1 >_{PST} X^3Y^5 e_2 >_{PST} Z^3 e_3.$$
$$\overbrace{\quad\quad}^{(2,1,0)} \qquad \overbrace{\quad\quad}^{(0,3,1)}$$

De donde

$\text{ml}(f) = X^2Y\, e_1$.

$\text{tl}(f) = 3X^2Y\, e_1$.

$\text{cl}(f) = 3$.

Teorema 5.42. *(Algoritmo de la división sobre módulos)*
Sea $f_1, \ldots, f_s \in A^m$, $f_i \neq 0$. Entonces $\forall f \in A^m$, $\exists q_1, \ldots, q_s \in A$ y $r \in A^m$ tal que $f = q_1 f_1 + \cdots + q_s f_s + r$ donde $r = 0$ ó $\text{ml}(f_i) \nmid m \; \forall m \in \text{Supp}(r)$, $i = 1, 2, \ldots, s$.

Prueba. La demostración puede ser revisada en [EH11]. □

Definición 5.43. Sea $m_1 = X^{\alpha} e_i$, $m_2 = X^{\beta} e_j$ dos módulos en A^m.
Definimos el MCM (mínimo común múltiplo para módulos) de m_1 y m_2 como:

$$\text{MCM}(m_1, m_2) = \begin{cases} 0 & , i \neq j \\ \text{MCM}(X^{\alpha}, X^{\beta}) & , i = j \end{cases}$$

Teorema 5.44. *(Teorema de la base de Hilbert)*
A^m es un A-módulo noetheriano, esto es, todo submódulo de A^m es finitamente generado.

Prueba. La demostración puede ser revisada en [AL94] (pág. 118). □

Definición 5.45. Sea $G = \{g_1, \ldots, g_t\}$ un conjunto de vectores no nulos contenidos en el submódulo $M \subset A^m$ ($A = k[X_1, \ldots, X_n]$) y c un orden monomial en A^m. Diremos que G es una base de Gröbner para M, respecto a c, si para todo $f \in M$ existe $i \in \{1, \ldots, t\}$ tal que $\text{ml}(g_i) | \text{ml}(f)$.

Observación 5.46. Veamos que:

$$\langle ml(M)\rangle = \langle ml(G)\rangle = \langle ml(g_1), \ldots, ml(g_t)\rangle \Longleftrightarrow M = \langle g_1, \ldots, g_t\rangle.$$

En efecto, sea $f \in M$ por el algoritmo de la división $\exists\, q_1, \ldots, q_t \in A$ y $r \in A^m$ tal que $f = q_1g_1 + \ldots + q_tg_t + r$, donde $r = 0$ ó $ml(g_i) \nmid m\ \forall m \in Supp(r)$, $i = 1, \ldots, t$.

- Si $r = 0$. $\checkmark$
- Si $r \neq 0$, $r = f - q_1g_1 - \ldots - q_tg_t \in M$, así que $ml(r) \in \langle ml(M)\rangle = \langle ml(G)\rangle$ por lo que $\exists i$ tal que $ml(g_i) \mid ml(r) (\Longleftarrow)$.

Por lo que $M = \langle g_1, \ldots, g_t\rangle$.

Ejemplo 5.47. Sea $M = \langle m_1e_{j_1}, \ldots, m_te_{j_t}\rangle$ submódulo monomial de A^m.
El conjunto $G = \{m_1e_{j_1}, \ldots, m_te_{j_t}\}$, $m_i \in T^n$ es una base de Gröebner para M. En efecto, dado $f \in M$ tenemos $f = \sum_{i=1}^{t} c_im_ie_{j_i}$, con $c_i \in k$.
Luego, $\exists i$ tal que $ml(f) = m_ie_{j_i}$. Por lo tanto G es una base de Gröebner de M.

Teorema 5.48. Sea M un submodulo de A^m, $G = \{g_1, \ldots, g_t\}$ subconjunto de M. Las siguientes afirmaciones son equivalentes:

1. G es una base de Gröebner.
2. $\langle ml(M)\rangle = \langle ml(G)\rangle$.
3. $f \in M$ si y solo sí el resto de la división de f por $g_1, \ldots, g_t$ es cero.
4. $f \in M$ si y solo sí $f = \sum_i q_ig_i$, $q_i \in A$ y $ml(f) = máx\{ml(q_ig_i) / \ i = 1, \ldots, t\}$.

Prueba. La demostración puede ser revisada en [EH11]. □

Corolario 5.49. El resto por la división de $g_1, \ldots, g_t$ ($G = \langle g_1, \ldots, g_t\rangle$) es único.

Prueba. Consideremos $\sum_i q^{(1)}g_i + r_1 = f = \sum_i q_i^{(2)}g_i + r_2$,
entonces $\sum_i (q_i^{(1)} - q_i^{(2)})g_i = r_1 - r_2$.

- $r_1 - r_2 = \sum_i (q_i^{(1)} - q_i^{(2)})g_i = 0$. $\checkmark$
- $r_1 - r_2 = \sum_i (q_i^{(1)} - q_i^{(2)})g_i = 0$, entonces $r_1 - r_2 \in \langle g_1, \ldots, g_t\rangle$, por lo que $\exists i$ tal que $ml(g_i) \mid ml(r_1 - r_2)$, así que $ml(r_1 - r_2) \in M(r_1) \cap M(r_2)$ $(\Longleftarrow)$ por ser G una base de Gröebner.

En consecuencia $r_1 = r_2$. □

Cálculo de las bases de Gröbner para submódulos

Definición 5.50. Fijemos un orden monomial en A^m y sea $f, g \in A^m$ no nulos, siendo $tl(f) = c_1 m_1 e_{j_1}$, $tl(g) = c_2 m_2 e_{j_2}$. El S-vector de f y g es denotado por $S(f, g)$, como:

$$S(f, g) = \begin{cases} \frac{m}{c_1 m_1} \cdot f - \frac{m}{c_2 m_2} \cdot g & ; j_1 = j_2 \\ 0 & ; j_i \neq j_2 \end{cases}$$

donde $m = MCM(tl(f), tl(g))$.

Ejemplo 5.51. Considere los polinomios en A^3, con $A = k[X, Y, Z]$.

$f = X^2Y\, e_1 + ZY^3 e_1 + X^3Y^5 e_2 + Z^3 e_3$.

$g = Xe_1 + YZe_1 + X^2Y\, e_2$.

Consideremos el orden lexicográfico y $X > Y > Z$ con $e_1 > e_2 > e_3$.

- Fijamos el orden monomial TSP en A^3.

$$\left.\begin{array}{l} tl(f) = X^3Y^5 e_2 \longrightarrow m_1 = X^3Y^5 \\ tl(g) = X^2Y\, e_2 \longrightarrow m_2 = X^2Y \end{array}\right\} MCM(m_1, m_2) = X^3Y^5.$$

$$S(f, g) = \frac{X^3Y^5}{X^3Y^5} \cdot f - \frac{X^3Y^5}{X^2Y} \cdot g = f - XY^4 g = X^2Y\, e_1 + ZY^3 e_1 - X^2Y^4 e_1 - XY^5 Ze_1 + Z^3 e_3.$$

- Fijamos el orden monomial PST en A^3

$$\left.\begin{array}{l} tl(f) = X^2Y e_1 \longrightarrow m_1 = X^2Y \\ tl(g) = Xe_1 \longrightarrow m_2 = X \end{array}\right\} MCM(m_1, m_2) = X^2Y.$$

$$S(f, g) = \frac{X^2Y}{X^2Y} \cdot f - \frac{X^2Y}{X} \cdot g = f - XY\, g = ZY^3 e_1 - XY^2 Ze_1 + X^3Y^5 e_2 - X^4Y^2 e_2 + Z^3 e_3.$$

Observación 5.52. Del ejemplo 5.51 consideramos los mismos polinomios en A^3, además el orden lexicográfico, $X > Y > Z$ con $e_3 > e_2 > e_1$ (notar este cambio)

Fijamos el orden monomial PST en A^3

$$\left.\begin{array}{l} tl(f) = Z^3 e_3 \longrightarrow m_1 = Z^3 \\ tl(g) = X^2Y\, e_2 \longrightarrow m_2 = X^2Y \end{array}\right\} S(f, g) = 0, \text{ pues } 3 \neq 2$$

Esto nos indica que S-vector es dependiente.

Teorema 5.53. *(Teorema de Buchberger para submódulos)*

Sea M un submódulo de A^m y fijemos un orden monomial c sobre A^m. Sea el conjunto $G = \{g_1, \ldots, g_s\} \to M$ es una base de Gröbner de M respecto a c si y solo si los restos de la división de $S(g_i, g_j)$ $\forall i, j$ divididos por $g_1, \ldots, g_s$ es cero.

Prueba. La prueba es similar al caso de ideales, ver la demostración en [EH11]. □

Teorema 5.54. *(Algoritmo de Buchberger para submódulos)*
Fijemos un orden monomial c en A^m y sea M un submódulo de A^m generado por $f_1, f_2, \ldots, f_s$. Entonces una base de Gröbner respecto a c, puede construirse por un número finito de pasos del siguiente algoritmo.

Entrada: $F = \{f_1, \ldots, f_s\} \longrightarrow A^m$
Inicializamos: $tt := F$ y $G := \{\{f_i, f_j\} / f_i \neq f_j \in tt\}$
Mientras $G \neq \emptyset$; realice:
1. Elegimos $f, g \in G$.
2. Calculamos $S(f, g)$ y hallamos el resto r de la división de $S(f, g)$ por los elementos de tt.
3. Si $r \neq 0$ entonces $G := G \cup \{(u, r) / \forall u \in tt\}$ y $tt := tt \cup \{r\}$.
Salida: Base de Gröbner $tt = \{g_1, \ldots, g_t\}$ para M.

Prueba. La prueba es similar al caso de ideales, ver la demostración en [EH11]. □

Ejemplo 5.55. Consideremos los siguientes polinomios en A^3, donde $A = Q[X, Y]$.

$$f_1 = Y e_2 + X e_3,\ f_2 = X e_2 + (XY - X) e_3,\ f_3 = X e_1 + Y^2 e_2,\ f_4 = Y e_1 + X e_3.$$

Usaremos el orden lexicográfico, con $X > Y$, $e_1 > e_2 > e_3$, fijemos el orden monomial TSP. Calculemos la base de Gröbner para el submódulo $M = \langle f_1, f_2, f_3, f_4 \rangle$.
Sea $G = \{f_1, f_2, f_3, f_4\}$, tenemos $G = \{\{f_1, f_2\}, \{f_1, f_4\}, \{f_2, f_4\}\}$.
Calculemos los S-vector
$S(f_1, f_2) = Y f_1 - f_2 = (Y^2 - X) e_2 + X e_3 \xrightarrow{t} r = -X e_1 - (X + Y) e_2 = f_5$.
Ahora agregamos $G = G \cup \{f_5\}$.
$S(f_1, f_4) = f_1 - f_4 = -Y e_1 + Y e_2 \xrightarrow{t} r = -Y e_1 + Y e_2 = f_6$.
Ahora agregamos $G = G \cup \{f_6\}$.
$S(f_2, f_4) = f_2 - Y f_4 = -Y^2 e_1 + X e_2 - X e_3 \xrightarrow{t} r = 0$.
Los nuevos vectores f_5 y f_6 generarón un único S-vector
$S(f_5, f_6) = Y f_5 - X f_6 = (-2XY - Y^2) e_2 \xrightarrow{t} r = (-2XY - X - Y) e_2 = f_7$.
Ahora agregamos $G = G \cup \{f_7\}$.
Al agregar el vector f_7 se genera un único S-vector
$S(f_3, f_7) = 2X f_3 + Y f_7 = 2X^2 e_1 + (-XY - Y^2) e_2 \xrightarrow{t} r = (-2X^2 + \frac{1}{2}X + \frac{1}{2}Y) e_2 = f_8$.
Ahora agregamos $G = G \cup \{f_8\}$.
Al agregar el vector f_8 se generarón dos S-vectores
$S(f_3, f_8) = 2X^2 f_3 + Y^2 f_8 = 2X^3 e_1 + (\frac{1}{2}XY^2 + \frac{1}{2}Y^3) e_2 \xrightarrow{t} r = 0$.
$S(f_7, f_8) = X f_7 - Y f_8 = (-X^2 - \frac{3}{2}XY - \frac{1}{2}Y^2) e_2 \xrightarrow{t} r = 0$.
Por lo tanto, $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ es una base de Gröbner para M.

Definición 5.56. Una base de Gröbner $G = \{g_1, \ldots, g_t\} \to A^m$ es una base de Gröbner reducida si, para todo i, g_i es reducida con respecto a $G - \{g_i\}$ y $cl(g_i) = 1$; para todo $i = 1, \ldots, t$. Así, para todo i de términos no nulos en g_i es divisible por cualquier $ml(g_j)$ para cualquier $j \neq i$.

Teorema 5.57. Fijemos un orden monomial. Cada submódulo no nulo M de A^m tiene una única base de Gröbner reducida con respecto al orden monomial. Así las bases de Gröbner son efectivamente calculables una vez que M haya sido generado por un conjunto finito de vectores en A^m.

Ejemplo 5.58. Del ejemplo 5.55, hemos encontrado una base de Gröbner con el orden monomial TSP, $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ para M.

$f_1 = Y e_2 + \underline{Xe_3}$,
$f_2 = Xe_2 + \underline{XY e_3} - Xe_3$,
$f_3 = \underline{Xe_1} + Y^2 e_2$,
$f_4 = Y e_1 + \underline{Xe_3}$,
$f_5 = \underline{-Xe_1} - (X + Y)e_2$,
$f_6 = \underline{-Y e_1} + Y e_2$,
$f_7 = \underline{-2XY e_2} - (X + Y)e_2$,
$f_8 = \underline{-2X^2 e_2} + \frac{1}{2}(X + Y)e_2$.

Observemos que $ml(f_1)$ divide a $ml(f_2)$ y $ml(f_4)$ debemos eliminar f_2 y f_4 de G, aún así tenemos una base de Gröbner. Además $f_3 - \overset{t}{\blacksquare} r = (Y^2 - X - Y)e_2$, Por lo tanto tenemos una base reducida para M dada por $\{f_1, f_3^{\leftarrow}, f_5^{\leftarrow}, f_6^{\leftarrow}, f_7^{\leftarrow}, f_8^{\leftarrow}\}$, de donde

$f_1 = Y e_2 + Xe_3$,
$f_3^{\leftarrow} = (Y^2 - X - Y)e_2$,
$f_5^{\leftarrow} = Xe_1 + (X + Y)e_2$,
$f_6^{\leftarrow} = Y e_1 - Y e_2$,
$f_7^{\leftarrow} = (XY + \frac{1}{2}X + \frac{1}{2}Y)e_2$,
$f_8^{\leftarrow} = (X^2 - \frac{1}{4}X - \frac{1}{4}Y)e_2$.

5.2 Códificación usando estructuras de módulos

Los grupos simétricos S_n actuan sobre F_q^n por permutación entre sus vectores. Un automorfismo de permutación de un codigo lineal $C \to F_q^n$ es un elemento de S_n que aplica al conjunto de palabras en símismo.

Para la presente tesis consideraremos automorfismos de códigos Abelianos (conocidos también como códigos cíclicos ordinarios y los códigos cíclicos m-dimensional). Sea

C un código, este tiene un grupo Abeliano no trivial de automorfismos H; por simplicidad de notación podemos restringir al caso $H = \langle\sigma\rangle$ que es cíclico. Los códigos cíclicos son ejemplos más básicos, quienes no necesariamente actuán de manera transitiva en las componentes de una palabra.

Sea O_i, $i = 1, 2, \ldots, r$ las orbitas de las componentes de una palabra código c bajo la acción de H. Elegimos cualquier componente $c_{i,0}$ en la i-ésima orbita y las etiquetas de las componentes en cada orbita como $c_{i,j}$, donde $j = 0, \ldots, |O_i| - 1$. Con la convención de que el segundo índice es un módulo entero $|O_i|$, la acción de σ puede ser escrita como

$$\sigma(c_{i,j}) = c_{i,j+1} \quad \forall i = 1, \ldots, r, \ \text{y} \ j = 0, \ldots, |O_i| - 1.$$

Podemos considerar de aquí en adelante, P_t como el anillo de polinomios en una variable $F_q[t]$, podemos considerar también la base estándar e_i del módulo libre P_t^r. Entonces la estructura de una orbita de las componentes del código de palabras C determina el submódulo de P_t^r

$$\langle (t^{|O_i|} - 1)e_i : \ i = 1, \ldots, r\rangle.$$

Observe que el codigo C como subconjunto del módulo cociente

$$N = P_t^r / \langle (t^{|O_i|} - 1)e_i : \ i = 1, \ldots, r\rangle \tag{5.1}$$

vía la aplicación

$$\begin{aligned} \$: \ C &\to N \\ (c_{i,j}) &\mapsto \sum_{i=1}^{r} \sum_{j=0}^{|O_i|-1} c_{i,j} t^j e_i \bmod \langle (t^{|O_i|} - 1)e_i : \ i = 1, \ldots, r\rangle, \end{aligned} \tag{5.2}$$

satisface el siguiente Teorema.

Teorema 5.59. Sea C un código lineal de bloque sobre F_q con un grupo cíclico H de automorfismos y $\$, N$ como antes. Entonces $\$(C)$ tiene una estructura de un P_t-submódulo de N.

Prueba. De la misma definición dada en (5.2), es claro que $\$$ es lineal, por lo tanto $\$(C)$ es un F_q-vector subespacio de N. Por la definición de $\$$, si $c \in C$ es cualquier

palabra código, la multiplicación de $ por t

$$t \cdot \$(c) = \sum_{i=1}^{k} \left(\sum_{j=0}^{|G_i|-1} c_{i,j} t^{j+1} \right) e_i - \sum_{i=1}^{k} \left(\sum_{j=0}^{|G_i|-1} c_{i,j} t^{j} \right) e_i \bmod N.$$
$$= \$(\sigma^{-1}(c)).$$

Por hipótesis, esté es otro elemento de $(C). Por lo tanto $(C) es cerrado bajo la multiplicación por t, en consecuencia bajo la multiplicación de todos los polinomios en P_t. Se sigue que $(C) es un P_t-submódulo de N. □

Observación 5.60. Note que si el teorema aplica a un código C, este aplica también a su código dual $C^{\perp}$.

Un algoritmo para una codificación sistemática

Mostraremos ahora que la teoría de bases de Gröbner para módulos pueden ser aplicados para trabajar con estos códigos. Sea M(C) el submódulo de P_t^r correspondiente a $(C) → N bajo la aplicación

$$\Phi : P_t^r \to N,$$

donde N es el módulo cociente de (5.1). La observación clave aquí es que el algoritmo de la forma canónica con respecto a la base de Gröbner G para M(C), de acuerdo a cualquier orden de términos σ en P_t^r, puede ser usado para producir una codificación sistemática para C.

Teorema 5.61. Sea G una base de Gröbner para el módulo M(C) con respecto al orden de término σ en P_t^r. El algoritmo que se dá a continuación produce una palabra código c en todos los casos y nos dá una codificación sistemática para el código C.

Entrada: tt, *los términos no estándar* m_i, *información de simbolos* c_i.

Salida: c_i *una palabra código.*

1. $f = \sum c_i m_i$;

2. c:=f—*FormaCanonica*(f,tt);

Prueba. Como

$$\mathrm{FormaCanonica}(c) = \mathrm{FormaCanonica}(f - \mathrm{FormaCanonica}(f, G), G) = 0.$$

Se sigue que $c \in M(C)$, lo que significa que c representa una palabra código de C. La información de los símbolos aparecen como coeficientes de los términos no estándar en f, pero FormaCanonica(f, G) es una combinación lineal de términos estándar. El conjunto de términos estándar y no estándar son disjuntos, por lo tanto está codificación es sistemática, en el sentido que los símbolos de información aparecen sin alterar en un subconjunto en las entradas de palabras códigos. □

Observación 5.62. En este método descrito por el teorema 5.61, los coeficientes de los términos no estándar dá la información de la palabras códigos, y los coeficientes de los términos estándar son los chequeos de paridad.

Ejemplo 5.63. Considerando el ejemplo 4.15 y la observación 4.16, hemos considerado $q = 2$, de donde ordenamos los puntos en 4 orbitas, además para el código $C_L(B, 3Q)$ tenemos una base para $L(3Q)$, dada por $\{1, x, y\}$ y matriz generadora

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ x(P_1) & x(P_2) & x(P_3) & x(P_4) & x(P_5) & x(P_6) & x(P_7) & x(P_8) \\ y(P_1) & y(P_2) & y(P_3) & y(P_4) & y(P_5) & y(P_6) & y(P_7) & y(P_8) \end{pmatrix}.$$

así obtenemos

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}.$$

De aquí, si ordenamos los puntos F_4-racionales en H de acuerdo a las estructuras de las orbitas (O_1, O_2, O_3 y O_4) obtenemos

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 & 0 & 0 \\ \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & 0 & 1 \end{pmatrix}.$$

Como $n = 8$ y $k = 3$ la distancia mínima será $d = 5$ ($k + d \leq n + 1 - g$), tenemos un código con los parámetros $[n, k, d] = [8, 3, 5]$ sobre F_4.
Bajo la aplicación \$ dada en la ecuación (5.2), la primera fila $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$ le corresponde por ejemplo

$$\sum_{j=1}^{|G_i|-1} c_{ij}t^j = \begin{matrix} \overbrace{1\ t\ t^2}^{O_1} & \overbrace{1\ t\ t^2}^{O_2} & \overbrace{1}^{O_3} & \overbrace{1}^{O_4} \end{matrix}.$$

así, el elemento del módulo será $g_1 = (1 + t + t^2, 1 + t + t^2, 1, 1)$.
La segunda fila $(1 \; \lambda \; \lambda^2 \quad 1 \; \lambda \; \lambda^2 \quad 0 \quad 0)$ le corresponde

$$\sum_{j=1}^{|O_1|} c_{ij} t^j = \begin{matrix} 1 & \lambda t & \lambda^2 t^2 & 1 & \lambda t & \lambda^2 t^2 & 0 & 0 \end{matrix},$$

así, el elemento del módulo será $g_2 = (1 + \lambda t + \lambda^2 t^2, 1 + \lambda t + \lambda^2 t^2, 0, 0)$.
La tercera fila $(\lambda \; \lambda \; \lambda \quad \lambda^2 \; \lambda^2 \; \lambda^2 \quad 0 \quad 1)$ le corresponde

$$\sum_{j=1}^{|O_1|-1} c_{ij} t^j = \begin{matrix} \lambda & \lambda t & \lambda t^2 & \lambda^2 & \lambda^2 t & \lambda^2 t^2 & 0 & 1 \end{matrix},$$

así, el elemento del módulo será $g_3 = (\lambda + \lambda t + \lambda t^2, \lambda^2 + \lambda^2 t + \lambda^2 t^2, 0, 1)$.
Con respecto al orden monomial PST, la base de Gröbner reducida G para el submódulo de P_t^4 correspondiente a $(C) es:

$$\begin{aligned} g_1^{\leftarrow} &= (\lambda + t, \lambda + t, \lambda^2, \lambda^2), \\ g_2^{\leftarrow} &= (0, 1 + t + t^2, \lambda, \lambda^2), \\ g_3^{\leftarrow} &= (0, 0, 1 + t, 0), \\ g_4^{\leftarrow} &= (0, 0, 0, 1 + t). \end{aligned}$$

Por ejemplo, los elementos $g_1^{\leftarrow}, \ldots, g_4^{\leftarrow}$ es igual a la combinación lineal entre g_1, g_2 y g_3. Además, como estamos sobre $F_4 = F_2[\lambda]/\langle \lambda^2 + \lambda + 1 \rangle$,

$$\begin{aligned} g_1^{\leftarrow} &= \lambda^2 g_1 + g_2 &&= (\lambda + t, \lambda + t, \lambda^2, \lambda^2), \\ g_2^{\leftarrow} &= \lambda g_1 + g_3 &&= (0, 1 + t + t^2, \lambda, \lambda^2), \\ g_3^{\leftarrow} &= (1 + t)(g_1 + g_3) &&= (0, 0, 1 + t, 0), \\ g_4^{\leftarrow} &= (1 + t) g_3 &&= (0, 0, 0, 1 + t). \end{aligned}$$

De la codificación sistemática presentado en el teorema 5.61, consideremos:

- Información de posición: coeficientes de $t^2 e_1$, $t e_1$, $t^2 e_2$. X
- Chequear paridad: coeficientes de $e_1, t e_2, e_2, e_3, e_4$. X

Entonces para nuestra codificación, es suficiente calcular los residuos de la división por G. Para el orden c_{PST}, esto equivale a divisiones polinómicas ordinarias en cada componente. Por ejemplo, si deseamos codificar

$$f = (t + \lambda t^2, \lambda^2 t^2, 0, 0) = 1 \cdot t e_1 + \lambda \cdot t^2 e_1 + \lambda^2 \cdot t^2 e_2.$$

Podemos chequear que dividiendo primero por g_1, entonces g_2 resulta

$$\mathrm{FormaCanonica}(f, G) = (\leftarrow^2, \leftarrow, \leftarrow, \leftarrow^2).$$

Su correspondiente palabra código es

$$c = f - \mathrm{FormaCanonica}(f, G) = (\leftarrow^2 + t + \leftarrow t^2, \leftarrow + \leftarrow^2 t^2, \leftarrow, \leftarrow^2).$$

Como,

$$c = (\leftarrow^2 + t + \leftarrow t^2, \leftarrow + \leftarrow^2 t^2, \leftarrow, \leftarrow^2) = (\leftarrow + \leftarrow t)g_1 + 1 \cdot g_2 + 1 \cdot g_3 + 1 \cdot g_4 + 0,$$

si calculamos

$$\mathrm{FormaCanonica}(c) = \mathrm{FormaCanonica}(f - \mathrm{FormaCanonica}(f, G), G) = 0.$$

El teorema 5.61 nos indica que c representa una palabra código, y es una codificación sistemática para f.

Observación 5.64. Podemos notar que las curvas Hermitanas tiene muchos automorfismos además del subgrupo generado por o en el ejemplo 4.15. Aunque por [Sti09] hay también un subgrupo no abeliano $\overline{H}$ de orden $|\overline{H}| = (q^2 - 1)q^3$ en el grupo de automorfismo de la curva Hermitiana, que fija tanto el punto en el infinito Q, y el divisor B, por lo tanto induce automorfismos de $C_L(B, mQ)$ para todo m. Los elementos en este subgrupo pueden ser escrito como aplicaciones

$$\mathbb{Z}_{Z,6,\mu}([X : Y : Z]) = [\leftarrow X + 6Z : \leftarrow^{q+1} Y + \leftarrow 6^q X + \mu Z : Z],$$

donde $\leftarrow \in F_{q^2}$, y $[6 : \mu : 1]$ es cualquier punto afín F_{q^2}-racional en la curva. Note que

$$\mathbb{Z}_{Z,6,\mu}([0 : 0 : 1]) = [6 : \mu : 1],$$

esto implica que $\overline{H}$ actúa transitivamente en los puntos afínes F_{q^2}-racionales, o equivalentemente, que hay solo una orbita de puntos bajo $\overline{H}$.

Finalmente para los códigos geométricos de Goppa con otras clases de curvas, pero con número máximo de puntos racionales, y de género sobre F_q pueden ser tratados de manera similar a lo tratado para curvas Hermitianas.

5.3 Decodificación usando estructuras de módulos

Consideraremos el artículo [GR09], la decodificación algebraica de errores, ha sido estudiado por mucho tiempo, vamos a describir especifícamente un algoritmo de decodificación que depende del cálculo de las bases de Gröbner, mediante el "algoritmo FGLM-like" [OF07] (o técnicas similares vista en [Mor09]) en módulos de polinomios.

Sean S y S^0 A-submódulos del módulo libre A^m ($A = k[X_1, \ldots, X_n]$) tal que:

- $S^0 \subseteq S$.
- $S^0 = \{a \in S : L(a) = 0\}$, donde $L : S \longrightarrow k$ es un k-homomorfismo.

Como $S^0 = Nu(L)$, $\forall a, b \in S \setminus S^0$, los elementos

$$\left(b - \frac{L(b)}{L(a)}a\right) \quad \text{y} \quad \left(X_i b - \frac{L(b)}{L(a)}a\right).$$

están en S. Veamos

$$L\left(b - \frac{L(b)}{L(a)}a\right) = L(b) - \frac{L(b)}{L(a)}L(a) = 0,$$

$$L\left(X_i b - \frac{L(b)}{L(a)}a\right) = L(X_i b) - \frac{L(b)}{L(a)}L(X_i a) = 0,$$

de está última igualdad se tiene: $\dfrac{L(X_i b)}{L(b)} = \dfrac{L(X_i a)}{L(a)}$.

Por lo que, podemos afirmar que: para cualquier X_i, existe un $\emptyset_i \in k$ tal que $\forall c \in S$,

$$L((X_i - \emptyset_i)c) = 0. \tag{5.3}$$

En efecto, basta considerar por ejemplo $\emptyset_i = \dfrac{L(X_i b)}{L(b)}$.

Supongamos que conocemos una base ordenada de Gröbner $G = \{g_1, \ldots, g_r\}$ de S con respecto a cierto orden $\prec$. Queremos determinar una base G^0 de S^0. Está base se prueba en [OF02], tal base consiste de tres partes

$$G^0 = G_1 \cup G_2 \cup G_3.$$

Donde los g_i pueden ser construido dela siguiente manera:

$\leftarrow$ Si $L(g_h) = 0$ para todo $1 \leq h \leq r$, entonces $G \subseteq S^0 \subseteq S$, por lo tanto $S = S^0$. (En

este caso $G_1 = G$ y $G_2 = G_3 = ;$).

$\leftarrow$ Por otro lado, sea $L(g_h) = \hookleftarrow_h$ para $1 \leq h \leq r$, consideremos $h\leftarrow$ el menor h tal que $\hookleftarrow_{h\leftarrow} 6= 0$. Tenemos:

- $G_1 = \{g_h : 1 \leq h < h\leftarrow\}$, note que, $G_1 \dashrightarrow S^{\lozenge}$.
- Es claro que, $g_{h\leftarrow} \not\in S^{\lozenge}$, seguimos de (5.3) que, para cualquier entero i

$$(X_i - \emptyset_i)g_{h\leftarrow} = X_i \blacklozenge \frac{L(X_i g_{h\leftarrow})}{\hookleftarrow_{h\leftarrow}} g_{h\leftarrow} \in S^{\lozenge}.$$

  Por lo tanto, tenemos

$$G_2 = \{(X_i - \emptyset_i)g_{h\leftarrow} : 1 \leq i \leq n\}, \text{ note que, } G_2 \not\subset S^{\lozenge}.$$

- Para $h > h\leftarrow$, tenemos que $g_h - \frac{\hookleftarrow_h}{\hookleftarrow_{h\leftarrow}} g_{h\leftarrow} \in S^{\lozenge}$, finalmente tenemos

$$G_3 = \overrightarrow{\sum} g_h - \frac{\hookleftarrow_h}{\hookleftarrow_{h\leftarrow}} g_{h\leftarrow} : h\leftarrow < h \leq r \quad \text{nuevamente, } G_3 \not\subset S^{\lozenge}.$$

Se puede notar que, al asumir la base ordenada de Gröbner, se deduce que el término lider de un elemento $a \in S^{\lozenge}$ es divisible por el término lider de un elemento de $G^{\lozenge}$, si $h = h\leftarrow$. Entonces, podemos suponer que el término lider de $g_{h\leftarrow}$ es el único término lider de los elementos de la base g_h que dividen el término lider de a y demuestra que $X_n tl(g_{h\leftarrow})$ también divide $tl(a)$ para algún n.

Observación 5.65. Es posible aplicar los resultados previos para incrementar pasos a una situación más general. Sea $M_N \dashrightarrow \cdots \dashrightarrow M_l \dashrightarrow \cdots \dashrightarrow M_0$ submódulos de M A-módulo. Sea $\surd_l : M_l \longrightarrow k$ un k-homomorfismo tal que

$$Nu(\surd_l) = M_{l+1}. \tag{5.4}$$

Sea $H : A^m \longrightarrow M$ una función k-lineal tal que, para cualquier $1 \leq i \leq n$, existe un $y_i \in k$ tal que satisface

$$H(X_i b) = (X_i + y_s)H(b), \tag{5.5}$$

donde $b = (b_1, \cdots, b_m) \in A^m$. Supongamos que nuestros submódulos S y $S^{\lozenge}$ son respectivamente, el conjunto de elementos que satisface las siguientes congruencias

$$H(b) \cong 0 \bmod M_l.$$

y

$$H(b) \cong 0 \bmod M_{l+1}.$$

Puede revisar más en detalle [Sal09, pág. 199].

Enfoque de Sudan

Sea X una curva absolutamente irreducible, con género g sobre F_q. Denotemos $n+1$ F_q-puntos racionales de X por $P_1, \ldots, P_n$ y P_1. Definimos $L(lP_1)$ como el conjunto de las funciones racionales en X de P_1 cuyo $ord(P_1) \leq l$. Para $2g-1 \leq k < n$, 1-punto codigo $C_L(B, kP_1)$ puede ser definido como F_q-espacio vectorial

$$\{(f(P_1), \cdots, f(P_n)) : f \in L(kP_1)\}. \tag{5.6}$$

Para cualquier $l \leq 2g-1$ hay funciones $\$_{1,1}, \cdots, \$_{l-g+1,1}$, con orden de polos crecientes, que forman una base de $L(lP_1)$ (espacio vectorial). Así que el código definido por 5.6 tiene longitud n y dimensión $k-g+1$.

Sabemos por [HN99], [KV03] que para cualquiera de los puntos $P_i \neq P_1$, hay también una base para $L(lP_1)$ de funciones $\$_{1,i}, \cdots, \$_{l-g+1,i}$ con orden cero creciente en P_i. Hay un conjunto de constantes de conversión de base

$$\{6_{i,j_2,j_3} \in F_q : i \in [n], j_2, j_2 \in [l-g+1]\},$$

tal que para cualquier i, j_2

$$\$_{j_2,1} = \sum_{j_3} 6_{i,j_2,j_3} \$_{j_3,i}.$$

Sea $(z_1, \cdots, z_n)$ la palabra recibida. Definimos $s = \left\lfloor \frac{l-g}{k+g-1} \right\rfloor$. Consideremos el polinomio de la forma

$$Q(z) = \sum_{j_1=0}^{l-g+1-(k+g-1)j_1} \sum_{j_2=1} a_{j_1,j_2} \$_{j_2,1} z^{j_1},$$

se busca $Q(z)$ que tenga un cero de al menos multiplicidad r en cada punto (P_i, z_i), $1 \leq i \leq n$. Existe una solución $Q_M \in k[z]^{l-g+1}$ cuyos términos satisfacen

$$(1, k+g-1) - grad(z^{j_1} e_{j_2}) = (k+g-1)j_1 + (j_2 - 1) < l-g+1.$$

Todas las soluciones cuyos términos tienen está propiedad están contenidos en $k[z]^{l-g+1}$.

Este elemento podría ser el primero ordenado de la base de Gröbner, de la solución del módulo

$$\{b \in F_q[z]^{l-g+1} : H^{i,y_i}(b) \not\equiv 0 \bmod M_r, i = 1, \ldots, n\},$$

donde

$$M_r = \{f \in A^u : \text{coef. del término } t \text{ de } f \text{ son } 0,\ \forall t = z^{j_1} e_{j_2} \text{ con } j_1 + (j_2 - 1) < r\}.$$

Así, todos los requerimientos del algoritmo FGLM-like son satisfechos y el elemento mínimo producido es una solución al problema de interpolación.

De esta manera, es posible generar una secuencia de módulo descendente. Un elemento minimal de la solución del submódulo con respecto a $c_{k,w}$ donde $w = (0, 1, 2, \ldots, m - 1)$ corresponde a la solución requerida y, por lo tanto, es posible aplicar el algoritmo general.

Capítulo 6

Conclusiones

En la presente tesis, se ha abordado algunas curvas que generan códigos lineales, mediante el teorema de Riemann-Roch; pero se puede profundizar un poco más, con otro tipo de curvas, otros cuerpos finitos, como también se puede abordar los conceptos vía cohomología.

Se ha dado varias aplicaciones para poder explicar de manera clara los conceptos tratados, para que el lector pueda continuar con el trabajo ya iniciado, asimismo se puede profundizar la última parte de decodificación sobre módulos, y su aplicación mediante software como: Magma, Singular, etc.

Bibliografía

[AL94] William W. Adams and Philippe Loustaunau, An introduction to Gröbner bases, no. 3, American Mathematical Society, Graduate Studies in Mathematics., 1994.

[AM89] Michael Francis Atiyah and Ian Grant Macdonald, Introducción al álgebra conmutativa, Reverté, 1989.

[AP18] Miriam Abdón and Cícero Carvalho y Daniel Panario, Curvas sobre cuerpos finitos.

[ASS99] Enrique Arrondo, Juana Sendra, and J Rafael Sendra, Genus formula for generalized o↵set curves, Journal of Pure and Applied Algebra 136 (1999), no. 3, 199–209.

[Bac96] Eric Bach, Weil bounds for singular curves, Applicable Algebra in Engineering, Communication and Computing 7 (1996), no. 4, 289–298.

[BHHW98] Ian Blake, Chris Heegard, Tom Hoholdt, and Victor Wei, Algebraic-geometry codes, IEEE Transactions on Information Theory 44 (1998), no. 6, 2596–2618.

[BK12] Egbert Brieskorn and Horst Knörrer, Plane algebraic curves: Translated by John Stillwell, Springer Science & Business Media, 2012.

[Bom74] Enrico Bombieri, Counting points on curves over finite fields, Séminaire Bourbaki vol. 1972/73 Exposés 418–435, Springer, 1974, pp. 234–241.

[CG16] Adrián Cruz Guerra, Usando bases de Gröbner en teoría de códigos.

[CLO06] David A Cox, John Little, and Donal O'shea, Using algebraic geometry, vol. 185, Springer Science & Business Media, 2006.

[DADlH17] Andoni De Arriba De la Hera, Códigos Reed-Muller.

[dBP96] Mario de Boer and Ruud Pellikaan, Gröbner bases for error-correcting codes and their decoding, submitted to the bookSome tapas of computer algebra (1996).

[dBP99] _____, Gröbner bases for codes, Some Tapas of Computer Algebra, Springer, 1999, pp. 237–259.

[DGPS19] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR 4-1-2 A computer algebra system for polynomial computations, 2019.

[dlPM07] María Jesús de la Puente Muñoz, Curvas algebraicas y planas, Servicio Publicaciones UCA, 2007.

[EH11] Viviana Ene and Jürgen Herzog, Gröbner bases in commutative algebra, vol. 130, American Mathematical Soc., 2011.

[FT96] Rainer Fuhrmann and Fernando Torres, The genus of curves over finite fields with many rational points, manuscripta mathematica 89 (1996), no. 1, 103–106.

[Ful69] William Fulton, Algebraic curves, Université de Versailles, 1969.

[Ful08] _____, Curvas algebraicas, Reverté, 2008.

[FW69] William Fulton and Richard Weiss, Algebraic curves. an introduction to algebraic geometry.

[GK08] Massimo Giulietti and Gábor Korchmáros, On automorphism groups of certain Goppa codes, Designs, Codes and Cryptography 47 (2008), no. 1-3, 177–190.

[Gop70] Valerii Denisovich Goppa, A new class of linear correcting codes, Problemy Peredachi Informatsii 6 (1970), no. 3, 24–30.

[Gop88] Valerij Denisovič Goppa, Geometry and codes, Springer, 1988.

[GQ01] Arnaldo Garcia and Luciane Quoos, A construction of curves over finite fields, Acta Arithmetica - ACTA ARITHMET 98 (2001), 181–195.

[GR09] Eleonora Guerrini and Anna Rimoldi, Fglm-like decoding: from Fitzpatrick's approach to recent developments, Gröbner Bases, Coding, and Cryptography, Springer, 2009, pp. 197–218.

[HLS95] Chris Heegard, John Little, and Keith Saints, Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes, IEEE Transactions on Information Theory 41 (1995), no. 6, 1752–1761.

[HN99] Tom Høholdt and R Refslund Nielsen, Decoding hermitian codes with Sudan's algorithm, International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Springer, 1999, pp. 260–269.

[HP95] Tom Hoholdt and Ruud Pellikaan, On the decoding of algebraic-geometric codes, IEEE Transactions on Information Theory 41 (1995), no. 6, 1589–1614.

[HP10] W.Cary Hu↵man and Vera Pless, Fundamentals of error-correcting codes, Cambridge university press, 2010.

[HVLP98] Tom Høholdt, Jacobus H Van Lint, and Ruud Pellikaan, Algebraic geometry codes, Handbook of coding theory 1 (1998), no. Part 1, 871–961.

[JK06] David Joyner and Amy Ksir, Automorphism groups of some AG codes, IEEE Transactions on Information Theory 52 (2006), no. 7, 3325–3329.

[KB05] Ernst Kunz and Richard G Belsho↵, Introduction to plane algebraic curves, vol. 68, Springer, 2005.

[KK92] Frances Kirwan and Frances Clare Kirwan, Complex algebraic curves, vol. 23, Cambridge University Press, 1992.

[Köt96] Ralf Kötter, On algebraic decoding of algebraic-geometric and cyclic codes.

[KV03] Ralf Koetter and Alexander Vardy, Algebraic soft-decision decoding of Reed-Solomon codes, IEEE Transactions on Information Theory 49 (2003), no. 11, 2809–2825.

[LA15] Diego Lopez Alvarez, Género de curvas algebraicas, Master's thesis, 7 2015.

[Lan02] Serge Lang, Algebra revised third edition, Graduate Texts in Mathematics 1 (2002), no. 211, ALL–ALL.

[LAN03] Leocarlos BS Lima, Francisco M Assis, and Lirida AB Naviner, Decodificação de códigos algébraico-geométrico, Journal of Communication and Information Systems 18 (2003), no. 3.

[Leo09a] Douglas A. Leonard, A tutorial on AG code construction from a Gröbner basis perspective, Gröbner Bases, Coding, and Cryptography, Springer, 2009, pp. 93–106.

[Leo09b] _____, A tutorial on AG code decoding from a Gröbner basis perspective, Gröbner Bases, Coding, and Cryptography, Springer, 2009, pp. 187–196.

[Lin99] J.H. Van Lint, Introduction to coding theory, Springer, 1999.

[Lit07] John Little, Automorphisms and encoding of AG and order domain codes, volume from D1 Workshop on applications of Gröbner bases in coding theory and cryptography, RISC-Linz, 2007.

[LREL19] Juan Antonio Lopez Ramos and José Escoriza Lopez, Grupos, anillos y cuerpos, Grupos, Anillos y Cuerpos (2019), 1–86.

[MGB07] Edgar Martınez Moro, Carlos Munuera Gómez, and Diego Ruano Benito, bases de Gröbner: aplicaciones a la codificación algebraica, Instituto Venezolano de Investigaciones Cientıficas (2007).

[Mil03] James S. Milne, Fields and Galois theory, Courses Notes, Version 4 (2003).

[Mir95] Rick Miranda, Algebraic curves and Riemann surfaces, vol. 5, American Mathematical Soc., 1995.

[MONL12] Daniel Miguel Ortiz and Joel Nava Lara, Geometr´ıa algebraica aplicada a códigos, Ph.D. thesis, 2012.

[Mor93] Carlos Moreno, Algebraic curves over finite fields, no. 97, Cambridge University Press, 1993.

[Mor09] Teo Mora, The FGLM problem and Moeller's algorithm on zero-dimensional ideals, Gröbner Bases, Coding, and Cryptography, Springer, 2009, pp. 27–45.

[NX01] Harald Niederreiter and Chaoping Xing, Rational points on curves over finite fields: theory and applications, vol. 288, Cambridge University Press, 2001.

[NX09]_____, Algebraic geometry in coding theory and cryptography, Princeton University Press, 2009.

[OF02] Henry O'Keeↄe and Patrick Fitzpatrick, Gröbner basis solutions of constrained interpolation problems, Linear algebra and its applications 351 (2002), 533–551.

[OF07] Henry O'Keeↄe and Patrick Fitzpatrick, Gröbner basis approach to list decoding of algebraic geometry codes, Applicable Algebra in Engineering, Communication and Computing 18 (2007), no. 5, 445–466.

[Pod] Ricardo A Podestá, Introducción a la teoría de códigos autocorrectores.

[Rot05] Joseph J Rotman, A first course in abstract algebra, Prentice Hall, 2005.

[Rov10] Carmen Rovi, Algebraic curves over finite fields.

[S+15] Thiago Rodrigues da Silva et al., Bases de Gröbner e a geometria algébrica na teoria de códigos corretores de erros.

[Sak06] Shojiro Sakata, Applications of the BMS algorithm to decoding of algebraic codes, Workshop on Gröbner Bases in Cryptography, Coding Theory and Algebraic Combinatorics, Linz, Austria, 2006.

[Sak09] _____, The bms algorithm, Gröbner Bases, Coding, and Cryptography, Springer, 2009, pp. 143–163.

[Sal09] Massimiliano Sala, Gröbner bases, coding, and cryptography: a guide to the state-of-art, Gröbner Bases, Coding, and Cryptography, Springer, 2009, pp. 1–8.

[Sei68] Abraham Seidenberg, Elements of the theory of algebraic curves, vol. 6999, Addison-Wesley, 1968.

[Sha01] Claude Elwood Shannon, A mathematical theory of communication, ACM SIGMOBILE Mobile Computing and Communications Review 5 (2001), no. 1, 3–55.

[Ste12] Serguei A. Stepanov, Codes on algebraic curves, Springer Science & Business Media, 2012.

[Ste15] Ian Nicholas Stewart, Galois theory, CRC Press, 2015.

[Sti90] Henning Stichtenoth, On automorphisms of geometric Goppa codes, Journal of Algebra 130 (1990), no. 1, 113–121.

[Sti09] _____, Algebraic function fields and codes, vol. 254, Springer Science & Business Media, 2009.

[T+08] Guilherme Chaud Tizziotti et al., Codificação de certos codigos de Goppa geometricos utilizando a teoria de bases de Gröbner e codigos sobre a curva norma-traço.

[TO98] Fernando Eduardo Torres Orihuela, Sobre curvas maximales.

[VD83] Sergei Georgievich Vlăduţ and Vladimir Gershonovich Drinfeld, Number of points of an algebraic curve, Funktsional'nyi Analiz i ego Prilozheniya 17 (1983), no. 1, 68–69.

[VLVdG12] J. Van Lint and Gerard Van der Geer, Introduction to coding theory and algebraic geometry, vol. 12, Birkhäuser, 2012.

[Wal50] Robert J. Walker, Algebraic curves, 1950.

[Wes98] Stephan Wesemeyer, On the automorphism group of various Goppa codes, IEEE Transactions on Information Theory 44 (1998), no. 2, 630–643.

[XNL99] Chaoping Xing, Harald Niederreiter, and Kwok Yan Lam, A generalization of algebraic-geometry codes, IEEE Transactions on Information Theory 45 (1999), no. 7, 2498–2501.

[Zam07] Paolo Zampolini, Algebraic geometric codes on curves and surfaces, 2007.