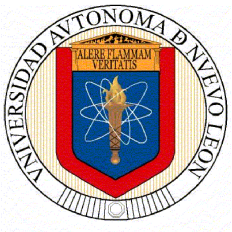
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

POSGRADO EN CIENCIAS CON ORIENTACIÓN EN MATEMÁTICAS



GENERALIZACIÓN DEL GRUPO DE PUNTOS EN UNA CURVA ELÍPTICA CON BASE EN QUASIGRUPOS PARA CRIPTOGRAFÍA

Por

ABRAHAM ALEJANDRO PUENTE RODRÍGUEZ

Como requisito parcial para obtener el Grado de

MAESTRÍA EN CIENCIAS con Orientación en Matemáticas

Agosto, 2026

APROBACIÓN

GENERALIZACIÓN DEL GRUPO DE PUNTOS EN UNA CURVA ELÍPTICA CON BASE EN QUASIGRUPOS PARA CRIPTOGRAFÍA

Aprobación de la Tesis

Dr. Pablo Cesar Rodríguez Ramírez

Asesor de la Tesis

Dra. Perla Marlene Viera González

Dra. Alison Garza Alonso

Dr. Alvaro Eduardo Cordero Franco

Subdirector de Estudios de Posgrado

AGRADECIMIENTOS

Le tengo todo el agradecimiento del mundo a mis padres que me dieron la vida y las oportunidades para llegar a donde he llegado. Mis hermanos que conmigo se han desarrollado.

Ustedes me dieron todo lo que debieron de tener y más.

Compañeros que me acompañaron en todos los momentos de aburrimiento y sosiego, en instantes tediosos y consejos superfluos; aun así, no los olvido. Amigos algunos de ellos. Como parvadas de aves, estudiantes conmigo, esclavos forzados, extranjeros en un comité.

Y claro, mi asesor el Dr. Pablo Cesar Rodríguez Ramírez, el cual durante todo este trabajo me ha apoyado, sin sus ideas nunca hubiera terminado. A los miembros del comité por sus sugerencias y el tiempo que me prestaron para obtener un trabajo sólido.

DEDICATORIA

A mis padres, por su apoyo incondicional.

A mi asesor, por su buena guía.

A mi amada, por su gran amabilidad.

Al Médico César por mostrarme el lexapro.

A mí mismo, por nunca ceder; la necedad me ha bendecido.

RESUMEN

Se propuso extender la *ley de grupo* en *curvas elípticas* con base a *quasigrupos*, esto con el objetivo de ofrecer una *estructura algebraica base no asociativa* para trabajar en criptografía. Es bien sabido que una operación binaria definida sobre una superficie suave generalmente induce un *loop conmutativo* [4]. Por tanto generamos una superficie mediante la *revolución* de una curva elíptica, con ello se desarrolló un quasigrupo cuya operación es una *extensión* para la ley de grupo en *curvas elípticas* al coincidir con esta cuando se fijan *órbitas* de elementos y se trabaja localmente sobre ellas. Asimismo se estudiaron algunas propiedades de la estructura desarrollada de interés criptográfico.

Índice general

Índice de figuras

NOMENCLATURA

$\mathbb{R}$	Conjunto de los números reales.
$\mathbb{Q}$	Conjunto de los números racionales.
$\mathbb{Z}$	Conjunto de los números enteros.
$\mathbb{R}^n$	Espacio euclidiano de dimensión n.
$\mathbb{Q}^n$	Espacio racional de dimensión n.
$\mathbb{Z}^n$	Espacio discreto de dimensión n.
$\mathbb{N}$	Conjunto de los números naturales.
$\mathbb{A}$	Espacio afín.
$\mathbb{A}^n$	Espacio afín de dimensión n.
$\mathbb{A}(K)$	Espacio afín sobre K.
$\mathbb{A}(K)^n$	Espacio afín de dimensión n sobre K.
$\mathbb{P}^n$	Espacio proyectivo de dimensión n.

$\mathbb{P}^n(K)$	Espacio proyectivo de dimensión n sobre K.
$T_P X$	Espacio tangente a P en X.
$\|x\|$	Norma euclidiana del vector x.
$\|A\|$	Cardinalidad del conjunto A.
$\cup$	Unión de conjuntos.
$\cap$	Interseccion de conjuntos.
$\vee$	Disyunción de predicados.
$\wedge$	Conjunción de predicados.
a^λ	Inverso izquierdo.
a^μ	Inverso por ambos lados.
a^ρ	Inverso derecho.
$\to$	Mapeo.
$\mapsto$	Aplicación de un mapeo.
PCOM	Posgrado en Ciencias con Orientación en Matemáticas.
UANL	Universidad Autónoma de Nuevo León.

CAPÍTULO 1

INTRODUCCIÓN

1.1 Antecedentes

En la criptografía y su historia hay un paradigma que tiene bastante relevancia, a menudo conocido como *criptografía con curvas elípticas*. En su desarrollo histórico identificamos dos fundadores independientes: Koblitz y Miller. En particular, Koblitz [8] se inspiró en los trabajos de Diffie y Hellman sobre la *criptografía de llave pública* y un *intercambio de llaves* usando el *problema del logaritmo discreto* [5]. Además, del algoritmo de factorización entera desarrollado por Lenstra usando *curvas elípticas* [7]. Con estos dos referentes propusieron un *grupo* basado en los puntos racionales de una curva elíptica, el cual se utilizaría en el problema del logaritmo discreto. Abreviamos esta problemática como *ECDLP* (Elliptic Curve Discrete Logarithm Problem).

Esta idea fue despreciada en su momento debido a la poco usual abstracción geométrica que representaba su propuesta; sin embargo, eso cambió después al comprender algunas de las ventajas que este método suponía. Por cierto, Diffie y Hellman utilizaban el problema del logaritmo discreto sobre *enteros modulares* para intercambiar llaves; sin embargo, luego de un tiempo se hallaron algoritmos que atacaban este problema con cierta eficacia. Solo por mencionar algunos bastante reconocidos: el *cálculo de índices* y el algoritmo *Pollard rho para logaritmos discretos*. Retomando el punto, algoritmos como el cálculo de índices y Pollard rho se vieron ineficaces al tratar con el *ECDLP*. Respectivamente, el primero no se podía adaptar

a la estructura y el segundo era ineficaz bajo ciertos supuestos en los parámetros.

Hay más historia sobre este paradigma que se puede encontrar en [32]; este es un artículo de *Koblitz* que describe el desarrollo histórico de las *curvas elípticas*. Mencionamos solo un poco para entender que este paradigma surgió al proponer una estructura alternativa poco usual. Estos trabajos han inspirado a otros que han tratado de generalizar o extender la estructura de *curva elíptica*, como se puede hallar en [37]; aquí, Alberto Sonnino y Giorgio Sonnino presentan una extensión en superficies de dimensiones grandes, una reducción de recursos computacionales, y ofrecen resistencia a ciertos ataques, etc. También en [31], Bruen y Hirschfeld definen una nueva ley de grupo sobre curvas elípticas con propiedades geométricas y combinatorias.

Las estructuras algebraicas se han aplicado en gran medida a la criptografía, frecuentemente estructuras como *grupos*, *anillos*, *campos* e incluso *espacios vectoriales*. Sin embargo, en las últimas décadas se ha propuesto usar conceptos de teorías relativamente nuevas e incluso no algebraicas. Ejemplos de ello son algunos trabajos de Vladimir Shpilrain en donde utiliza *álgebra tropical* [34]. Ademas también propone esquemas basados en conceptos de *procesos estocásticos* como en [44], este articulo presenta una primitiva criptográfica con errores basada en caminatas aleatorias la cual ofrece un supuesto de seguridad interesante y nuevo. Nuestro interés, sin embargo, se cierne sobre las *estructuras no asociativas* como *quasigrupos* o *loops*. Estos trabajos son recientes e incluso libros sobre su aplicación en *criptografía* no han de tener polvo en las estanterías. Asimismo, hay algunos trabajos de Shcherbacov que hablan explícitamente sobre su uso, como [26] ó [19].

El trabajo criptográfico sobre estructuras no asociativas como *quasigrupos*, *loops* y *neo-campos* es reciente e interesante debido a la incertidumbre del impacto que estas puedan tener en la *criptografía*.

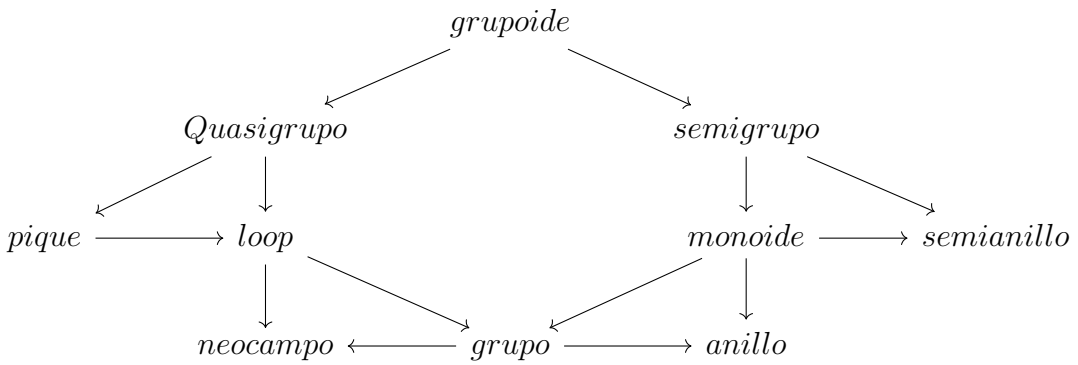


Diagrama 1: Estructuras no asociativas y asociativas

1.2 Motivación

Lo que se desea desarrollar con este trabajo es una estructura algebraica inspirada en curvas elípticas que se espera tenga buenas propiedades para la criptografía. Por esta misma razón, se trabajó con una estructura poco estudiada. Tampoco caemos en la ingenuidad de pensar que el hecho de que aún no haya ataques hace que este método sea seguro; claro que no. Eso es similar a alguien que cree saber manejar porque nunca ha tenido ninguna dificultad al volante, pero solo cuando se presentan problemas podemos analizar debilidades que pasan desapercibidas en un primer instante. Deseamos no solo proponer esta estructura, sino también hacer ver que tiene propiedades adecuadas, así como Koblitz tomó las *curvas elípticas* (anteriormente desarrolladas por Jacobi) y las trajo a la criptografía como *estructuras ideales*. Claro que es distinto, dado que no tenemos la fundamentación que ya se tiene con *curvas elípticas*. Pero, igualmente, la mezcla de los conceptos *algebraicos no asociativos* y *geométricos* no se ha desarrollado mucho en criptografía.

Sin ninguna intención de despreciar este trabajo, apenas hemos fundamentado lo suficiente la parte geométrica para definir una operación, un muy pequeño fragmento de la parte algebraica, y aún queda mucho por estudiar y aplicar de ello.

1.3 Justificación

Aunque la necesidad de crear y actualizar nuevos algoritmos de seguridad constantemente, o el hecho de que esto aún no se haya hecho, pudieran parecer buenas justificaciones, hay más razones por las cuales comenzar a trabajar el tema en este contexto. Empezando por hacer notar las actuales *futuras vulnerabilidades* de la *criptografía* con curvas elípticas y, más aún, de cierto paradigma en *teoría de grupos*. *Peter Shor* logró construir un *algoritmo cuántico* que resuelve dos de las instancias más importantes (para la criptografía) del *problema del subgrupo escondido*; es decir, da un ataque efectivo a *problemas* muy usados en la criptografía, entre ellos el *problema del logaritmo discreto*, los *problemas de factorización* y la búsqueda de *órbitas*. Es decir, sistemas criptográficos como *RSA* (Rivest Shamir Adleman), *ElGamal* y otros.

Si nos preguntamos ahora por qué se siguen usando, la respuesta es obvia: todavía no hay computadoras cuánticas con la suficiente capacidad para ejecutar algoritmos como el de *Peter Shor* [9]. Sin embargo, se espera que lleguen, y cuando lo hagan, tales criptosistemas dejarán de ser seguros. Más aún, esto no significa del todo el fin de la *criptografía basada en grupos*; este algoritmo resulta ser muy efectivo solo en *grupos conmutativos finitos* y funciona parcialmente en aquellos no conmutativos, es decir, no está definido para todos.

Por este mismo hecho, hay quienes tratan de *migrar* a otro tipo de *grupos*, tal y como sucede en [50], donde se busca desarrollar y proponer problemas sobre grupos *post-cuánticos*, es decir, resistentes a los posibles ataques que puedan provenir de las *computadoras cuánticas*. Pensamos entonces que una alternativa, similar al espíritu de las *curvas elípticas* pero, con una estructura resistente a los ataques actuales (debido a que aún está en proceso la adaptación de estos a las estructuras no asociativas, aunque algunos ya lo han logrado), representa una buena oportunidad de desarrollo. Incluso si nuestra propuesta resulta ser débil, aún hay mucha *teoría algebraica no*

asociativa que podemos implementar sobre lo ya desarrollado.

1.4 Objetivos

El principal fin de este trabajo es desarrollar una generalización o extensión de la estructura algebraica definida sobre *curvas elípticas* para su uso en la criptografía. Para eso, siempre se debe no proponer un fin como absoluto, sino particionar el mismo por los medios para llegar a él y tratar de percibir a cada uno de estos como un fin absoluto. Entonces, con esto en mente, tenemos los siguientes objetivos en su respectivo orden.

- Buscar y consultar trabajos, artículos ó similares sobre el tema de investigación en cuestión.
- Crear una bibliografía no demasiado amplia, sino concisa respecto a lo que se desea, para comparar, ver qué se tiene, qué falta y qué se puede hacer.
- Tomar una idea concisa con base en lo ya estudiado, desarrollarla siguiendo procedimientos permisibles, pero no del todo restrictivos. Como tal, todo lo que no esté expresamente prohibido es una posibilidad.
- Estudiar los resultados obtenidos, comparar con lo esperado, con lo conocido y, asimismo, estudiar si existen casos degenerados.
- Fundamentar lo obtenido, analizar problemas abiertos o caminos por los cuales extenderse para llegar a nuevos resultados.
- Delimitar lo obtenido y bien fundamentado de aquello posiblemente justificable para tener resultados concisos, correctos y, a su vez, posibles líneas de investigación.
- Discutir lo obtenido con respecto a lo que ya se tenía, las diferencias y ventajas obtenidas, además de los posibles desarrollos.

- Concluir con un producto limpio, fundamentado y conciso. Asimismo, enunciar algunas líneas de investigación quizá no triviales.

Estos objetivos son bastante generales y podemos perdernos en ellos; es por tanto que señalamos como objetivos principales:

- Construir y fundamentar una superficie para definir una estructura algebraica operacional.
- Desarrollar una operación sobre la superficie que defina un quasigrupo conmutativo.
- Estudiar propiedades de interés criptográfico, al menos las suficientes para que esto sea adaptable a problemas criptográficos.

1.5 Organización

El trabajo se organiza en 4 capítulos: *Introducción*, *Preliminares*, *Desarrollo* y *Conclusión*. El primer capítulo se compone de 4 secciones (no se hará detalle sobre las secciones de *Introducción*):

- *Estructuras Algebraicas*.
- *Geometría Algebraica*.
- *Curvas Elípticas*.
- *Criptografía*.

Siendo la primera sección muy extensa, esto se debe a la introducción de estructuras no asociativas, además de las asociativas. Por lo mismo, se trató de no extender más el trabajo en las demás secciones y dejar solo lo más fundamental.

El segundo capítulo se compone por 3 secciones:

- *Construcción de una Superficie.*
- *Ley de Composición.*
- *Propiedades Algebraicas.*

Y el último capítulo se compone por 2 secciones.

- Discusión.
- Conclusión.

Preliminares es bastante extenso, pero hace que el trabajo de desarrollo sea corto debido a todos los conocimientos implícitos. Con esto, tenemos un diagrama breve del contenido y su organización.

CAPÍTULO 2

PRELIMINARES

Necesitaremos algunos conceptos fundamentales para discernir *quasigrupos* de *grupos*, así como entender cómo el primero funge como generalización del segundo. Después de esto, introduciremos conceptos fundamentales de *geometría algebraica*. Con estos conocimientos podremos hablar del grupo de puntos en una *curva elíptica*, para luego establecer la teoría que sustenta las propiedades de estas curvas y cómo son utilizadas en cifrados. Finalmente, presentaremos brevemente algunos fundamentos de criptografía con el fin de tener claro a qué nos referimos por *primitiva criptográfica*, *problema difícil* y *estructura base* en criptografía.

2.1 Estructuras Algebraicas

Las estructuras algebraicas asociativas han gozado de una atención constante por parte de la comunidad científica. Desde luego, quien ha estudiado matemática, física, química, ingeniería o alguna otra área afín se ha encontrado con los conceptos de *grupo*, *campo* y *espacio vectorial*, solo por mencionar los más conocidos. Otros no tanto, pero aun así escuchados rara vez son: *monoide*, *anillo* y *módulo*. Sin embargo, si se pregunta por alguna estructura no asociativa, lo más que se puede esperar es que se haga mención de álgebras no asociativas. Hay mucho más que esto y la poca atención que han recibido las estructuras no asociativas las convierte hoy en conceptos libres de teoría criptoanalítica en comparación con los grupos, desarrolladas por unos

pocos, pero con la suficiente riqueza estructural para implementarse en criptografía.

Definición 2.1. Sea C un conjunto, llamamos entonces *operación binaria* al mapeo

$$\oplus : C \times C \longrightarrow C$$

donde la evaluación en un elemento cualquiera se denota como

$$\oplus(c_1, c_2) = c_1 \oplus c_2 = c_3$$

En la actualidad, a un conjunto con una operación binaria se le suele llamar *magma*; pero, dado nuestro contexto, preferimos referirnos a tal estructura como *grupoide*, siendo este un término ahora usado para una estructura en *teoría de categorías*. Con esta aclaración esperamos disipar toda ambigüedad.

Con esto, procedemos a hablar de algunas propiedades que a menudo son consideradas por su uso y aplicación.

Definición 2.2. Sea $(C, \oplus)$ *grupoide*, entonces decimos que se tiene

- *asociatividad*, sí

$$(x \oplus y) \oplus z = x \oplus (y \oplus z) \ , \ \forall x, y, z \in C$$

- *divisibilidad*, sí

$$\forall a, b \in C \ (\exists! \, x, y \in C \mid x \oplus a = b = a \oplus y)$$

- *conmutatividad*, sí

$$x \oplus y = y \oplus x \, , \, \forall x, y \in C$$

- *neutro*, sí

$$\exists!\, e \in C \ (e \oplus x = x \oplus e = x \,,\, \forall x \in C)$$

Observación 2.3. Será usual ver durante este trabajo expresiones como $\forall x(P)$. Esto es solo una forma de expresar cómo el cuantificador universal $\forall$ *actúa* sobre una variable x que satisface el predicado P. De igual manera se procederá con el cuantificador existencial $\exists$. No siempre se utilizará esta estructura (por motivos puramente estéticos).

Observación 2.4. La *conmutatividad* es una propiedad que siempre se tomará por cierta, a menos que se exprese lo contrario. Algunas de estas propiedades, juntas, pueden llegar a implicar otras y, de tenerse, formar una estructura deseable. Asimismo, puede que se satisfagan de forma parcial, es decir, en subconjuntos particulares.

Observación 2.5. Una cosa que no se considera por el momento es la cantidad de elementos que se tienen. Pero este concepto será importante más adelante, por lo que, a partir de este momento, cuando se considere la cantidad de elementos en una estructura algebraica, llamamos a esta *orden*. Si el orden es no *infinito*, entonces la estructura en contexto se dice *finita*.

Definición 2.6. Sea $(C, \oplus)$ *grupoide*, llamamos a este

- *semigrupo*, sí se tiene *asociatividad*.
- *quasigrupo*, sí se tiene *divisibilidad*.
- *monoide*, sí es un *semigrupo* con *neutro*.
- *loop*, sí es un *quasigrupo* con *neutro*.
- *grupo*, sí es un *monoide* con *divisibilidad* o un *loop* con *asociatividad*.

Quizá sea algo obtuso a la vista, por lo que el siguiente diagrama da una mejor perspectiva de estas estructuras y su jerarquía.

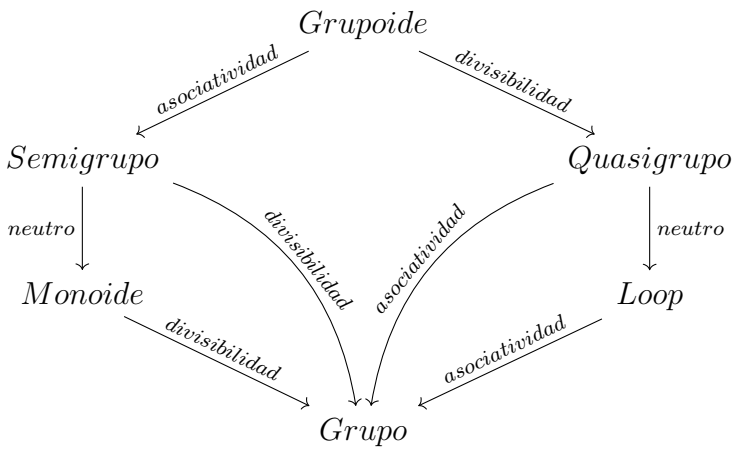


Diagrama 2: Estructuras con una operación

Hay otras propiedades respecto al *orden* de algunas estructuras, iniciamos entonces con aquellas que poseen asociatividad.

Definición 2.7. Sea G *grupo* y $C \subseteq G$ un subconjunto que funge como grupo con la operación de G. Entonces a este se le llama un *subgrupo*.

Observación 2.8. Sí G es finito entonces cualquier *subgrupo* de este también lo es. Mas aun, si el *grupo* es finito, entonces es más fácil hablar de un conjunto que *genere* a G.

Definición 2.9. Sea G *grupo*, si existen $r_1, \ldots, r_n \in G$ tales que

$$G = \{r_1^{\alpha_1} \cdots r_n^{\alpha_n} \mid \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}$$

Entonces se dice que G es generado por $\{r_1, \ldots, r_n\}$ y denotamos este conjunto como $\langle r_1, \ldots, r_n \rangle$. Sí $G = \langle r \rangle$ con $r \in G$. Entonces G se dice *cíclico*.

Observación 2.10. Los *subgrupos* de un *grupo* también pueden ser *generados* por algún subconjunto del mismo *subgrupo*.

Proposición 2.11. Sea G *grupo* y $S \subseteq G$ un subconjunto, entonces el conjunto

$$\{s_1^{\alpha_1} \cdots s_n^{\alpha_n} \mid \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}$$

forma un *subgrupo* y decimos que este es *generado por* S. Denotamos este por $\langle S \rangle$

Demostración. Véase [23] □

Ejemplo 2.12. Considerando los enteros sin el 0 es decir, $\mathbb{Z}-\{0\}$ con la multiplicación usual, esto forma un *grupo* usualmente llamado *grupo multiplicativo de* $\mathbb{Z}$. Además, dado un elemento como $4 \in \mathbb{Z}$, este forma un *subgrupo* que está compuesto por las potencias de r.

$$\langle 4 \rangle = \{4^{\alpha} \mid \alpha \in \mathbb{Z}\}$$

si consideramos $\mathbb{Z}$ con la suma usual se tiene un *grupo*, algo particular en este es que todos sus *subgrupos* son *cíclicos*. Esto debido a la existencia de un *máximo común divisor*.

$$\langle 4, 6 \rangle = \{4r_1 + 6r_2 \mid r_1, r_2 \in \mathbb{Z}\}$$

sin embargo, en este grupo está $4(-1) + 6(1) = 2$, por tanto

$$\langle 4, 6 \rangle = \langle 2 \rangle$$

De aquí podemos hablar de algunas relaciones entre *subgrupos* y *grupos* cuando estos son finitos.

Definición 2.13. Sea G *grupo* y $e, a \in G$ siendo e el *neutro*. Si existe $k \in \mathbb{Z}$ con $a^k = e$, llamamos a este *exponente* de a. Al mínimo *exponente* positivo de a se llama *orden* del elemento a. Denotamos este por $|a|$.

Observación 2.14. Una pregunta es si existe un exponente común para todo $g \in G$.

Definición 2.15. Sea G *grupo*. Entonces si existe $m \in \mathbb{Z}$ tal que

$$a^m = e\,,\ \forall a \in G$$

Entonces llamamos a este *exponente* de G. Sin embargo, al mínimo *exponente* positivo

de G lo llamamos *orden*, por lo que nos referimos a este de forma explícita por sus propiedades.

Proposición 2.16. Sea G *grupo* y $a \in G$. Entonces k es un *exponente* de a sí y solo si k es divisible por $|a|$. De igual forma, esto sucede para G y sus exponentes.

Demostración. Véase [21] □

Teorema 2.17. Sea G un *grupo finito*. Entonces

- Siendo $m = max\{|a| \mid a \in G\}$, este coincide con el *minimo exponente* positivo de G.
- El *mínimo exponente* de G coincide con su *orden* sí y solo si G es cíclico.

Demostración. Véase [21] □

Observación 2.18. El resultado anteriormente mencionado se aplica únicamente a *grupos conmutativos finitos*. No se hace énfasis en la conmutatividad, ya que esta es una propiedad que asumimos a lo largo de este trabajo, como se indicó en teorema 2.4. No obstante, consideramos pertinente señalarlo explícitamente.

Teorema 2.19 (Lagrange)**.** Sea G *grupo finito*. Entonces

- El *orden* de cualquier *subgrupo* en G divide al *orden* de G.
- El *orden* de cualquier *elemento* en G divide al *orden* de G.
- Sí A es un *grupo conmutativo finito* con k divisor de $|A|$, entonces hay un *subgrupo* de *orden* k en A.

Demostración. Véase [21] □

Teorema 2.20. Sea G *grupo*.

- Sí $|G| = p$ primo, entonces G es cíclico.

- Sí $H \subseteq G$ *subgrupo* con G cíclico, entonces H también es cíclico.
- Sí G es finito, este es cíclico sí y solo si su *mínimo exponente positivo* coincide con $|G|$

Demostración. Véase [21] □

Esto es suficiente para procedimientos próximos. Agregamos ahora algunos conceptos de *quasigrupos* y *loops* que serán necesarios y, con esto, entender el contraste con estructuras asociativas. Sin embargo, con la no asociatividad se suelen emplear *mapeos*, por lo que introducimos el concepto brevemente.

Definición 2.21. Sean A y B dos conjuntos, llamamos *mapeo* a una relación donde a cada elemento de a se asigna un único de b.

$$\begin{aligned} f : A &\to B \\ a &\mapsto f(a) \end{aligned}$$

si tenemos múltiples mapeos como $f : A \to B$ y $g : B \to C$, entonces podemos definir la composición de estos por $g(f) : A \to C$. Usualmente se denota por $(f \circ g)$

$$A \xrightarrow{f} B \xrightarrow{g} C \qquad A \xrightarrow[f\circ g]{} C$$

Diagrama 3: Composición de mapeos

Observación 2.22. Usualmente, un *mapeo* no nos da todo B, es decir, $f(A) \subseteq B$. Cuando esto sí ocurre o todo valor de b está únicamente determinado por algún valor de a, se consideran casos particulares. Por simplicidad, se suele llamar *dominio* a A y *rango* a B.

Definición 2.23. Sea $f : A \to B$ un *mapeo*, entonces el conjunto

$$\{b \in B \mid \exists a \in A\,,\ f(a) = b\}$$

se suele llamar *imagen* de f y se denota por $Im(f)$. Además, el mapeo se dice

- *inyectivo*, sí
$$\forall b \in Im(f) \mid f(a_1) = b = f(a_2) \Rightarrow a_1 = a_2$$
- *sobreyectivo*, sí $Im(f) = B$
- *biyectivo*, sí f es *inyectiva* y sobreyectiva.

Definición 2.24. Sea $f : A \to B$ un *mapeo*, entonces definimos el mapeo

$$f^{-1} : Im(f) \to A$$
$$b \mapsto a$$

donde $f(b) = a$. Usualmente se llama a este *mapeo inverso* de f y se tiene el siguiente diagrama.

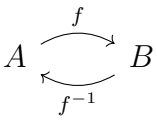


Diagrama 4: mapeo inverso

Observación 2.25. Usualmente cuando no se tiene una *biyección*, esta se puede obtener restringiendo el *dominio* o *rango* del *mapeo* en contexto.

Observación 2.26. Notemos que el hecho de decir que existe una biyección entre dos conjuntos A y B, implica decir que estos tienen la misma *cardinalidad*, es decir, la misma *cantidad* de elementos. No ahondaremos mucho en este tema dado que se extiende más allá de los límites del trabajo. Denotamos la cardinalidad de un conjunto A por $|A|$.

Todo el contenido siguiente es siguiendo el trabajo de [11].

Definición 2.27. Sea G *grupoide* y $a \in G$ fijo. Considerando los *mapeos*

$$L(a)x = a \cdot x \ , \ R(a)x = x \cdot a \tag{2.1}$$

los llamamos *mapeos de traslación izquierda* y *derecha* respectivamente, siendo $x \in G$ cualquier elemento.

Observación 2.28. Usualmente los autores aplican estos mapeos por el lado derecho, pero para tener cierta homogeneidad en escritura lo hacemos por el lado izquierdo. Estos se adaptan bien a la teoría ya establecida.

Definición 2.29. Sea G *grupoide*, llamamos a este *quasigrupo* sí los mapeos

$$L(a) : G \to G \ , \ R(a) : G \to G$$

son biyecciones para cualquier $a \in G$.

Observación 2.30. Debido a que se asume conmutatividad realmente solo necesitamos uno de estos *mapeos*, pero creemos que vale la pena poner los conceptos como se presentan formalmente en [11] Otra forma de entender esto es que se tiene un *quasigrupo* sí y solo si dados dos elementos de una terna x, y, z, el tercero está únicamente determinado. Con esto tenemos algunas propiedades.

Proposición 2.31. Sea Q un *quasigrupo*, entonces $\forall\ a, x, y \in Q$ se tiene

- *ley de cancelación izquierda*

$$ax = ay \Rightarrow x = y$$

- *ley de cancelación derecha*

$$xa = ya \Rightarrow x = y$$

Demostración. Véase [11] □

Observación 2.32. Debido a que asumimos conmutatividad desde teorema 2.4, realmente solo con tener una de estas propiedades la otra ya está determinada. Algo que quizá no se ha notado es que a pesar de no tener un *neutro*, se tienen *neutros locales*, esto debido a la condición de divisibilidad. Es decir, dado $a \in Q$, existe $e_a \in Q$ tal que $e_a a = a$.

Es claro que se trabaja con *traslaciones* en *quasigrupos*, pero hay una confusión cuando se piensa un poco sobre la *biyeccion* que estos definen. El que exista $L(a)$ y su inversa $L(a)^{-1}$ no implica que esta última funge como *traslación* es decir, que exista b tal que $L(b) = L(a)^{-1}$. Inspirados en esto [11] o [1] definen con estos mapeos inversos dos nuevas *operaciones*.

Definición 2.33. Sea Q *quasigrupo* con $x, y \in Q$. consideramos entonces.

$$L(x)^{-1}y \ , \ R(y)^{-1}x \tag{2.2}$$

como operaciones entre x y y. Denotamos estas por $x\backslash y$ y x/y respectivamente. De igual forma, llamamos a estas *división izquierda* y *división derecha*.

Observación 2.34. Con *conmutatividad*, estas operaciones coinciden como solo una $x/y = y\backslash x$ esto es obvio considerando una interpretación no tan obvia de la *división izquierda* y *derecha* como.

$$x\backslash y = z = L(x)^{-1}y \Leftrightarrow x \cdot z = y \quad , \quad x/y = z = R(y)^{-1}x \Leftrightarrow z \cdot y = x \tag{2.3}$$

considerando entonces x/y y $y\backslash x$ se tiene la igualdad. Mas aun, estas *operaciones* con Q forman un *quasigrupo*. Usualmente $(Q, /)$ y $(Q, \backslash)$ son llamados *conjugados* o *parastrofes*.

Usualmente sí se trabaja con *quasigrupos*, se hace considerando las *parastrofes* por su utilidad e incluso podemos definir un *loop* en base a sus operaciones.

Definición 2.35. Sea $(G, \cdot, /, \backslash)$ un conjunto con tres operaciones binarias tales que

- $a \cdot (a\backslash b) = b\,,\ (b/a) \cdot a = b \quad \forall a, b \in G$
- $a\backslash(a \cdot b) = b\,,\ (b \cdot a)/a = b \quad \forall a, b \in G$
- $a\backslash a = b/b \quad \forall a, b \in G$

entonces este se dice *loop*

Observación 2.36. Este hecho es trivial por lo que no se presenta como una *proposición*, incluso así se halla en [11]

También podemos hablar de subestructuras sin ningún problema, sin embargo, no se tendrán algunas de las propiedades que hay en *grupos*.

Definición 2.37. Sea Q *quasigrupo*. Dado $H \subseteq Q$ no vació, sí este es un *quasigrupo* con la operación de Q. Entonces se llama a H *subquasigrupo*.

Hablar de quasigrupos generados es distinto aquí debido a que no hay una forma constructiva.

Teorema 2.38. Sea Q *quasigrupo*, $S \subseteq Q$ un subconjunto no vació y T un conjunto no vació de *subquasigrupos* en Q con $S \subseteq H$ siempre y cuando $H \in T$. Entonces $\bigcap_{H \in T} H$ es un *subquasigrupo* de Q con $S \subseteq \bigcap_{H \in T} H$.

Demostración. Véase [11] □

Observación 2.39. este mismo resultado funciona para *loops*, pero debe notarse que T es un conjunto que contiene *subquasigrupos* no todos.

Sí consideramos Q *quasigrupo* con S y T como en el teorema anterior, pero ahora suponemos que T tiene todos los *subquasigrupos* de Q tales que $S \subseteq H$ con

$H \in T$. Claramente $T \neq \emptyset$ dado que $Q \in T$. Entonces por el teorema anterior, $\bigcap_{H \in T} H$ es un *quasigrupo* con $S \subseteq \bigcap_{H \in T} H$ y a esta intersección se denota por $\langle S \rangle$.

Definición 2.40. Sea Q *quasigrupo*, $S \subseteq Q$ no vació y T el conjunto de todos los *subquasigrupos* en Q tales que $S \subseteq H$ siempre y cuando $H \in T$. Entonces el *subquasigrupo* $\langle S \rangle$ es llamado el *subquasigrupo generado por* S.

Observación 2.41. Es correcto pensar en $\langle S \rangle$ como el *subquasigrupo* pequeño que contiene a S. Si ocurre que $\langle S \rangle = Q$, decimos que S genera a Q. Si se tiene $S = \{a\}$ denotamos $\langle S \rangle$ por $\langle a \rangle$. Y en caso de tener $\langle a \rangle = Q$, se dice que Q es *monogénico*.

Una cosa que quizá nunca consideramos como una *propiedad* sino como una construcción natural son las potencias, y es que estas mismas funcionan gracias a la asociatividad.

$$a^n \cdot a^m \overset{?}{=} a^{n+m}$$

Definición 2.42. Sea Q *quasigrupo*, este se dice con *potencias asociativas* sí $(a, \cdot)$ forma un *grupo* para toda $a \in Q$.

Observación 2.43. Aunque en general esta es la definición de tener *potencias asociativas*, en *teoría de quasigrupos* a menudo se encuentra uno con que demostrar una propiedad puede hacerse demostrando una identidad algebraica. Por ejemplo; en el caso de *potencias asociativas* donde solo es necesario demostrar que se tiene la *propiedad de alternancia*

$$y(x \cdot x) = (y \cdot x)x$$

Si se quiere ver algo más de este tema véase [42].

Algo que tampoco se satisface es el *teorema de Lagrange*.

Definición 2.44. Sea G un *loop* finito y $H \subseteq G$ *subloop*. Entonces H se satisface una *propiedad tipo Lagrange* sí $|H|$ divide $|G|$.

Que un *subloop* satisfaga una *propiedad tipo Lagrange* nos da algo similar a lo que se tenía en *grupos*, tenemos entonces dos *propiedades*.

Definición 2.45. Sea G *loop finito*. Entonces G satisface la *propiedad débil de Lagrange* sí todo *subloop* tiene la *propiedad tipo Lagrange*.

Definición 2.46. Sea G *loop finito*. Entonces G satisface la *propiedad fuerte de Lagrange* sí todo *subloop* tiene la *propiedad débil de Lagrange*.

Tomando $K \subseteq H \subseteq G$ donde G es un *loop* y los otros elementos *subloops* respectivamente. Los siguientes diagraman muestran la relación de divisibilidad que hay entre sus respectivos ordenes.

Diagrama 5: Lagrange débil y fuerte respectivamente.

Observación 2.47. Existen *loops finitos* que satisfacen la *propiedad débil de Lagrange* sin llegar a satisfacer la *propiedad fuerte*.

Un concepto de interés en *grupoides*, *quasigrupos* y *loops* es el *grado* de asociatividad que se tiene, esto usualmente se ve contando las *ternas asociativas*.

Definición 2.48. Sea G un *grupoide* y $a \in G$. Entonces a se dice *nuclear* sí $L(a \cdot x) = L(x)L(a)$. Y al conjunto de *elementos nucleares*

$$N = \{a \in G \mid a(x \cdot y) = (a \cdot x)y \, , \, \forall x, y \in G\}$$

se suele llamar *núcleo* de G.

Observación 2.49. Esta definición usualmente es un poco más extensa, sin embargo, debido a la *conmutatividad* se reduce a algo más simple. Es análoga entonces para *quasigrupos* y *loops*, pero en cuanto a algunas propiedades y relaciones difiere. Para las dos últimas estructuras mencionadas el *núcleo* forma un *subgrupo*, mientras este sea no vació.

Usualmente estudiar la *cardinalidad* del *núcleo* sirve para darnos una idea de *que tan asociativa* es nuestra estructura. Lo siguiente es considerar otra *propiedad* que usualmente se toma por algo *natural* en *grupos*. Procedemos notando primero que la existencia de un *inverso único* no se debe a la divisibilidad por si sola sino además a la existencia del *neutro*. Es decir, sin este se pueden tener *inversos locales*, pero estos no son como tal *elementos* sino *propiedades*.

Definición 2.50. Sea Q un *quasigrupo*, sí se satisface que

$$\exists J : Q \to Q \mid a \mapsto a^{\mu} \wedge a^{\mu}(a \cdot x) = x \, , \, \forall x \in Q$$

donde J es una *biyeccion*. Entonces se dice que Q tiene la *propiedad del inverso*.

Observación 2.51. De nuevo, gracias a la conmutatividad algunas definiciones se reducen. Usualmente cuando se tiene esta propiedad se dice que Q es un *quasigrupo I.P* (*propiedad de inversos*). Cuando ocurre esto se tiene una solución a la ecuación $ax = b$, siendo esta $x = a^{\mu}b$. Asimismo, al considerar $L(a)^{-1}$, esto es lo mismo que $L(a^{\mu})$. Debemos notar que a^{μ} no es un *inverso* en el sentido de *grupos*, sino un elemento que satisface ciertas propiedades que no involucran un *neutro*.

Teorema 2.52. Sea G un *loop* con la *propiedad del inverso*. Entonces $a^{\mu} = a^{-1}$ donde $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Demostración. Véase [11] □

Con esto claro, procedemos a hablar de estructuras con dos operaciones. Estas serán fundamentales para definir el espacio donde vive el *lugar geométrico*.

Definición 2.53. Sea C un conjunto con dos operaciones binarias $\oplus$ y $\otimes$. Sí se satisface que

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)\,,\ \forall x, y, z \in C$$

entonces decimos que se tiene distributividad de $\otimes$ sobre $\oplus$.

Definición 2.54. Sea C un conjunto con dos operaciones $\oplus$ y $\otimes$. Entonces llamamos a este

- *anillo*, sí es un *grupo* con $\oplus$, un *monoide* con $\otimes$ y además satisface distributividad de $\otimes$ sobre $\oplus$.
- *campo*, sí es un *grupo* con ambas operaciones y además satisface *distributividad* de $\otimes$ sobre $\oplus$.

Observación 2.55. Formalmente no se exige que un anillo sea *monoide* con $\otimes$ sino simplemente un *semigrupo*. Sin embargo, bajo este contexto es lo común, por ello nuestra definición. Además, los neutros de $\oplus$ y $\otimes$ se representan por $0, 1$ respectivamente.

Denotamos de esta forma los elementos debido a una relación intrínseca entre estas estructuras abstractas y las naturales ya conocidas. Para entender esta relación procedemos a definir unos cuantos conceptos que nos permitirá entender similitudes entre estructuras con operación.

Definición 2.56. Sean $(C, +)$ y $(C', \oplus)$ dos grupoides. Dada $f : (C, +) \to (C', \oplus)$, tenemos

$$\begin{array}{ccc} C \times C & \xrightarrow{+} & C \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ C' \times C' & \xrightarrow{\oplus} & C' \end{array}$$

Diagrama 6: Homomorfismo entre grupoides

Y sí $(f \times f) \circ \oplus = (+) \circ f$, entonces se llama *homomorfismo* a f y decimos

que el diagrama *conmuta*. Además de la propiedad

$$f(a+b) = f(a) \oplus f(b)$$

, sí f es *biyectiva* y un *homomorfismo*, se le llama *isomorfismo*.

Observación 2.57. *MacLane* [3] usa esta definición para definir los objetos conocidos como *morfismos*. Sin embargo, esto lo hace en un contexto categórico, para alejarnos de ello usamos el termino *homomorfismo* dado que se representa lo *mismo*.

Podemos preguntarnos ahora que sucede con estructuras más complejas, y el hecho es que se siguen teniendo *homomorfismos* siempre que estos sean *mapeos* que respetan la *estructura*.

Definición 2.58 (homomorfismo de anillos)**.** Sean $(A, +, \cdot)$ y $(B, \oplus, \otimes)$ anillos. Dado $f : A \to B$, entonces este se llama *homomorfismo de anillos* sí f respeta la estructura, es decir, para todos $a, b \in A$

$$f(a+b) = f(a) \oplus f(b) \ , \ f(a \cdot b) = f(a) \otimes f(b) \ , \ f(1_A) = 1_B$$

por lo que f es homomorfismo respecto a las operaciones.

Observación 2.59. La condición $f(1_A) = 1_B$ es necesaria considerando

$$f(1_A) = f(1_A \cdot 1_A) = f(1_A) \otimes f(1_A) = f(1_A)^2$$

de donde entonces intuimos que el único elemento de B tal que $b = b^n$, $\forall n \in \mathbb{Z}^+$ es 1_B, por tanto, $f(1_A) = 1_B$

Con estos conceptos vemos que hay una relación directa entre $\mathbb{Z}$ y cualquier *anillo* dada como se sigue.

Definición 2.60. Sea $\mathbb{Z}$ el *anillo* de enteros y $(A, \oplus, \otimes)$ *anillo*. Definimos el mapeo.

$$f : \mathbb{Z} \to A$$

$$n \mapsto n_A$$

donde

$$n_A = \begin{cases} \underbrace{1_A \oplus \cdots \oplus 1_A}_{n} & n > 0 \\ 0_A & n = 0 \\ \underbrace{(-1_A) \oplus \cdots \oplus (-1_A)}_{-n} & n < 0 \end{cases}$$

Proposición 2.61. Sea A *anillo* y f como en la definición anterior. Entonces f es un *homomorfismo de anillos*.

Demostración. Véase [3] □

Observación 2.62. Notemos entonces que debido a este homomorfismo, tenemos de cierta forma una copia del anillo $\mathbb{Z}$ dentro de A. Cuando no haya ambigüedad nos referimos por n a n_A. Ahora podemos manejar expresiones como $2 \otimes a = a \oplus a$ y $-a = (-1_A) \otimes a$. Además denotamos ahora las operaciones $\oplus, \otimes$ por $+, \cdot$ respectivamente. Donde usualmente $\cdot$ se *expresará* con la *yuxtaposición* de elementos cuando no haya ambigüedad.

Proposición 2.63. Para cada *anillo* A hay exactamente un *homomorfismo de anillos* $f : \mathbb{Z} \to A$.

Demostración. Véase [3]. □

Definición 2.64. Sea $(R, \oplus, \otimes)$ *anillo* y $x, y \in R$ elementos no nulos. Entonces estos se dicen

- *divisores de* 0, sí $x \otimes y = 0$.
- *unidades*, sí $x \otimes y = 1$, denotamos estos elementos por u.
- *asociados*, sí $\exists u \in R \mid x \otimes u = y$

Observación 2.65. Una cosa que no debe confundirse es el *neutro* de $\otimes$ con una *unidad* cualquiera. Las unidades no fungen como *neutro* necesariamente. , hay elementos que no son *unidades* ni *neutros*. Al conjunto de todas las *unidades* lo denotamos por $R^{\times}$.

Los anillos también se diferencian cuando sus elementos son todos alguno de estos dos tipos.

Definición 2.66. Sea R *anillo*. Entonces este se dicen un

- *dominio entero*, sí no contiene *divisores de* 0.
- *campo*, sí todos los elementos de $R^* = R - \{0\}$ son *unidades*.

Observación 2.67. Usualmente en el segundo caso de la anterior definición se dice *anillo con división*. Pero dado que se tiene *conmutatividad*, se dice *campo*. Es decir, la diferencia entre un concepto u otro es la *conmutatividad*.

Para continuar con estructuras elaboradas necesitaremos algunos conceptos de matemática discreta. Por tanto, haremos una sutil digresión en el tema.

Definición 2.68. Sea C un conjunto, entonces decimos que $r \subseteq C \times C$ es una *relación binaria* en C. Y denotamos $(x, y) \in C$ por xry

Las siguientes son propiedades que tendremos en consideración.

Definición 2.69. Sea C un conjunto con una relación $\sim$, entonces esta se dice

- *reflexiva*, sí $a \sim a$, $\forall a \in C$
- *anti-reflexiva*, sí $a \not\sim a$, $\forall a \in C$

- *simétrica*, sí $a \sim b \Rightarrow b \sim a$
- *asimétrica*, sí $a \sim b \Rightarrow b \not\sim a$
- *transitiva*, sí $a \sim b\,,\, b \sim c \Rightarrow a \sim c$
- *antisimétrica*, sí $a \sim b\,,\, b \sim a \Rightarrow a = b$

Observación 2.70. Con estos conceptos podemos formalizar relaciones ya conocidas, una de ellas el *orden* en *polinomios* con coeficientes reales, viendo algunas relaciones bajo el *orden monomial* se tiene

$$\begin{array}{lll} x^2 + 2x \geq x^2 + 2x & x^2 + 2x \leq x^2 + 2x & \textit{reflexiva} \\ & \Rightarrow & \\ x^2 + 2x \leq x^3 + 2x & x^3 + 2x \leq x^4 - 4 & x^2 + 2x \leq x^4 - 4 \end{array}$$

es decir, el orden $\leq$ es una *relación reflexiva* y *transitiva*. Este tipo de relación suele ser llamado *preorden* y, sí se tiene *antisimetría*, se llama *orden parcial*.

Definimos con esto, una relación bastante útil por como hace de cierta forma una diferenciación de elementos en un conjunto.

Definición 2.71. Sea C un conjunto con una relación $\sim$, sí es *reflexiva*, *simétrica* y *transitiva*. Entonces llamamos a $\sim$ una *relación de equivalencia* en C.

No todos los elementos son equivalentes (puede suceder pero ese caso no es de interés bajo este contexto). Por tanto. podemos definir conjuntos de elementos que son equivalentes entre sí.

Definición 2.72. Sea C un conjunto con una relación de equivalencia $\sim$ y $a \in C$. Entonces definimos

$$[a] = \{b \in C \mid a \sim b\}$$

y llamamos a este conjunto, *clase de equivalencia* del elemento a.

Usualmente cuando se define una relación de equivalencia en un conjunto, a su vez se induce una partición sobre el conjunto.

Definición 2.73. Sea C un conjunto y $\{S_i\}_{i\in I}$ una colección de subconjuntos en C. Sí

- $S_i \cap S_j = \emptyset\,,\ \forall i \neq j$
- $\bigcup_{i\in I} S_i = C$

entonces llamamos a $\{S_i\}_{i\in I}$ una *partición* de C.

En resumen, dada una relación de equivalencia $\sim$ en un conjunto C. Esta induce una *partición* de C en *clases de equivalencia*. Algo no tan obvio es que dada una *partición* $\pi = \{S_i\}_{i\in I}$ de C, podemos inducir una *relación de equivalencia* por

$$a \sim_\pi b \iff a, b \in S_i \in \pi$$

Usualmente nos referimos al conjunto de todas las clases de equivalencia en C bajo $\sim$ por $C/\sim$.

Con estos conceptos regresamos al tema principal.

Definición 2.74. Sea R *anillo* y $I \subseteq R$ *subgrupo* respecto a $\oplus$. Entonces sí

$$\forall a \in R(a \otimes b \in I\,,\ \forall b \in I)$$

llamamos a I un *ideal* de R.

Observación 2.75. Esta propiedad particular que se exige a un ideal es, similar a la propiedad del 0 en los reales de ser *absorbente* bajo la multiplicación usual, es decir, que $0 \cdot x = 0\,,\ \forall x \in \mathbb{R}$. Usualmente para decir que I es un ideal, decimos que es *subgrupo* y *absorbente*. Otra forma valida seria definir este como un *subgrupo* cerrado bajo $\otimes$.

Hay además un detalle y es que un *ideal* en general no contiene el 1, de lo contrario es *trivial*, dado que si $1 \in I$, entonces $I = R$.

Hallar ideales puede resultar complicado, pero siempre podemos generarlos como se sigue.

Definición 2.76. Sea R *anillo* y $C \subseteq R$ un subconjunto. Entonces definimos

$$\langle C \rangle = \{r_1 c_1 + \cdots + r_n c_n \mid r_i \in R\,,\, c_i \in C\,,\, i = 1, 2, \ldots, n = |C|\}$$

llamamos a este *ideal generado por* C y decimos que es *finitamente generado*.

Observación 2.77. En general, C no contiene al 1, de lo contrario tenemos un *ideal trivial*. En caso de que tenga solo un elemento $C = \{r\}$ escribimos el ideal generado por este como $\langle r \rangle$.

La propiedad de ser *ideal* en un *anillo* es algo que se preserva bajo ciertas operaciones. Sean $A, B \subseteq R$ ideales, entonces

$$A \cap B = \{x \mid x \in A \wedge x \in B\}\ ,\ A + B = \{a + b \mid a \in A,\, b \in B\}$$

también son ideales de R. Usamos además el símbolo $+$ para hacer una distinción entre la operación de elementos $\oplus$ y conjuntos $+$.

Observación 2.78. Anteriormente se mencionó un concepto interesante que es el de ser *finitamente generado* como ideal. La pregunta es sí esto sucede para todos los ideales o incluso para todos los *anillos*. La respuesta es que no. Pero se puede probar incluso cuando sucede.

Definición 2.79. Sea R un anillo donde todos sus *ideales* son *finitamente generados*. Entonces este se dice *Noetheriano*.

Teorema 2.80. Sea R un *anillo Noetheriano*. Entonces toda *cadena ascendente de*

ideales se *estaciona*. Es decir

$$I_0 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

donde $I_{n+1} = I_n$. Con n entero.

Observación 2.81. Esto nos da herramientas útiles para adelante hablar sobre *variedades algebraicas*.

De aquí, tenemos el siguiente concepto

Definición 2.82. Sea $I \subseteq R$ un ideal y $r \in R$ un elemento fijo. Entonces definimos la *clase lateral* de I en R como subgrupo dado r por

$$r + I = \{r \oplus a \mid a \in I\}$$

Observación 2.83. Debemos mencionar que el concepto de *clase lateral* es propio de *grupos*, por esto mismo el énfasis en la anterior definición. Algo que además se debe observar es que no hacemos distinción entre clases laterales *izquierdas* o *derechas* dado que toda estructura en este trabajo se asume *conmutativa* a excepción de que se exprese lo contrario.

Este concepto es interesante dado que nos permite construir una *relación de equivalencia* en R.

Definición 2.84. Sean $x, y \in R$ e $I \subseteq R$ un ideal. Entonces

$$x \sim y \iff x + I = y + I$$

una condición equivalente es pedir que $x \ominus y \in I$.

Observación 2.85. Recordando que una *relación de equivalencia* induce una *partición* en el conjunto donde se define. Tenemos que $\sim$ particiona R en *clases de equivalencia*,

que forman todas las *clases laterales* de I en R.

Definición 2.86. Sea R *anillo*, $I \subseteq R$ un ideal y $\sim$ como en la definición anterior. Entonces al conjunto

$$R \,/\sim = \{r + I \mid r \in R\}$$

lo llamamos, el *cociente de R por I* y se suele denotar por R/I. Sus elementos también se denotan por $[r] = r + I$.

Observación 2.87. Hay varias formas de referirse a los elementos de R/I dado que estos fungen como *clases de equivalencia*, *clases laterales* o incluso, debido a la condición $x \ominus y \in I$, también suelen llamarse *clases residuales*. Algo que debemos notar es que se puede dotar de operaciones a R/I mediante las ya definidas en R, donde además I funge como un *neutro*.

Definición 2.88. Sea $(R, \oplus, \otimes)$ *anillo* e $I \subseteq$ un *ideal*. Entonces R/I es un *anillo* con las operaciones

$$[x] + [y] = [x \oplus y]\,,\ \forall [x], [y] \in R/I$$
$$[x] \cdot [y] = [x \otimes y]\,,\ \forall [x], [y] \in R/I$$

y usualmente se llama *anillo cociente* $(R/I, +, \cdot)$.

Observación 2.89. En las operaciones estamos operando los *representantes* de las clases. Pero no importa que otro elemento de una clase tomemos, las operaciones siguen estando bien definidas, es decir, sean $x, x' \in [x]$ donde $[x], [y] \in R/I$, entonces

$$[x] + [y] = [x'] + [y]$$

Toda esta información resulta digerible con el siguiente ejemplo.

Ejemplo 2.90. Sea $(\mathbb{Z}, +, \cdot)$ el anillo de enteros y $3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}$ un ideal.

Entonces podemos considerar su cociente $\mathbb{Z}/3\mathbb{Z}$ donde por definición, sus elementos son de la forma

$$-1+3\mathbb{Z}=\{\dots,-4,-1,2,\dots\} \qquad 2+3\mathbb{Z}=\{\dots,-1,2,5,\dots\}$$

$$0+3\mathbb{Z}=\{\dots,-3,0,3,\dots\} \qquad 3+3\mathbb{Z}=\{\dots,0,3,6,\dots\}$$

$$1+3\mathbb{Z}=\{\dots,-2,1,4,\dots\} \qquad 4+3\mathbb{Z}=\{\dots,1,4,7,\dots\}$$

es evidente entonces que $-1+3\mathbb{Z}=2+3\mathbb{Z}$ y al igual esto sucede con cada línea. Por tanto, observando que varios elementos se repiten en un ciclo, tenemos $\mathbb{Z}/3\mathbb{Z}=\{[0],[1],[2]\}$.

Observación 2.91. Usualmente a este *anillo cociente* se le llamar *anillo de enteros residuales* o *anillo de enteros modulo* 3. Esto debido a que de cierta forma estamos clasificando los enteros $\mathbb{Z}$ en base a su residuo al dividir por 3.

Los *ideales* también pueden tener ciertas propiedades que describen además su estructura, mencionamos algunas de interés a continuación.

Definición 2.92. Sea R *anillo* e I un ideal, decimos que este es

- *primo*, sí
$$\forall a,b\in R(a\otimes b\in I)\Rightarrow a\in I\vee b\in I$$
- *maximal*, sí dado J ideal de R
$$I\subseteq J\subseteq R\Rightarrow J=R\vee I=J$$
- *radical*, sí
$$a\in R\mid a^r\in I\,,\,r\in\mathbb{Z}\Rightarrow a\in I$$

Observación 2.93. Debemos notar que hay una relación de orden entre ideales respecto a la contención. Considerando esto tenemos que un ideal maximal funge como elemento maximal respecto a la relación de contención y los ideales primos fungen como elementos primos respecto al producto de ideales.

Por este último hecho se tiene una definición análoga de un ideal primo; dados I, J, P ideales de R con P primo. Entonces

$$IJ \subseteq P \Rightarrow I \subseteq P \vee J \subseteq P$$

Asimismo, un *ideal maximal* es *primo*, el converso es falso generalmente. También todo *ideal primo* es *radical*. Aunque esto último no es tan obvio dado la forma en que lo expresamos como *condición*.

Definición 2.94. Sea R *anillo* y $I \subseteq R$ un *ideal*. Entonces el conjunto

$$\{r \in R \mid \exists n \in \mathbb{Z} \ , r^n \in I\} \tag{2.4}$$

usualmente es llamado *ideal radical* de I. Denotamos este por $\sqrt{I}$

Con esto podemos hablar de algunos elementos particulares y su relación con estas estructuras.

Definición 2.95. Sea R *anillo* y $p \in R$ no nulo. Sí p no es una *unidad* y no tiene *divisores propios*, es decir, no existen $a, b \in R$ tal que $p = ab$ donde a y b se llaman *divisores* de p. Entonces p se dice *irreducible*.

Observación 2.96. Una condición necesaria y suficiente para que p sea irreducible, es decir que en el caso donde $p = a \cdot b$, entonces a o b es una *unidad*. Si un elemento es irreducible no necesariamente funge como *primo*. Algo por mencionar es que cuando b divida a p, denotamos esto por $b|p$.

Definición 2.97. Sea R *anillo* y $p \in R$ no nulo. Sí p no es una *unidad* y siempre que $p|ab$ se tiene que $p|a$ o $p|b$, entonces p se dice *primo*.

Teorema 2.98. Sea R *anillo* y $p \in R$ no nulo.

- Sí p es *primo*, entonces es *irreducible*.
- p es *primo* sí y solo si $\langle p \rangle$ es un *ideal primo* no nulo.

Demostración. Puede consultarse el [21] o [30]. □

Considerando los cocientes de un *anillo* por algún ideal con las propiedades antes mencionadas, se tiene lo siguiente.

Teorema 2.99. Sea R *anillo*. $P, M \subseteq R$ ideales donde P es primo y M maximal. Entonces

- R/P es un *dominio entero*.
- R/M es un *campo*.

Demostración. Véase [30]. □

Observación 2.100. Algo que debemos notar es que al hacer *cociente* por un *ideal maximal*, los únicos ideales que quedan son el *generado* por 0 y 1. Por tanto los *campos* siempre tiene solo 2 ideales siendo estos $\langle 0 \rangle$ y $\langle 1 \rangle$.

Estos resultados dan de hecho estructuras con las cuales se suele trabajar bastante. En concreto, con *anillos de enteros modulares* que bajo ciertas condiciones en el cociente, son *campos* y se llaman *campos de enteros modulares*.

Ejemplo 2.101. Sea $\mathbb{Z}$ el anillo de enteros. Considerando los ideales $4\mathbb{Z}$ y $8\mathbb{Z}$, observamos que $8\mathbb{Z} \subseteq 4\mathbb{Z}$. Esto dado que todos los múltiplos de 8 son también

múltiplos de 4, el converso no es veraz. Por tanto, si nos situamos en el número pequeño que genera múltiplos de $4, 6, 8$ o cualquier otro par, tenemos el 2. Es decir

$$\cdots \subseteq 8\mathbb{Z} \subseteq 4\mathbb{Z} \subseteq 2\mathbb{Z}$$

e incluso en otras cadenas el $2\mathbb{Z}$ es la cota superior de la cadena creciente de contenciones. Por tanto, $2\mathbb{Z}$ es un *ideal maximal*. Esto no es una coincidencia sino debido a que 2 es primo. Entonces siempre que se tenga $p\mathbb{Z}$ con p primo, se tiene un *ideal maximal* y aun, $\mathbb{Z}/p\mathbb{Z}$ un campo por el teorema anterior.

Observación 2.102. Usualmente en campos finitos no se tienen *raíces cuadradas*. Cuando un elemento $r \in \mathbb{Z}/p\mathbb{Z}$ sea tal que $\exists x \in \mathbb{Z}/p\mathbb{Z}$ con $x^2 = r \ (mod\, p)$ este se dice un *residuo cuadrático*. Usualmente para esto se usa el símbolo de Legendre

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \exists x \mid x^2 = r \ mod(p) \\ 0 & r = 0 \\ -1 & en\ otro\ caso. \end{cases}$$

Observación 2.103. Los *ideales primos* de este anillo son de la forma $p\mathbb{Z}$ con p primo, además del generado por el $\langle 0 \rangle$. Esto último ocurre debido a que $\mathbb{Z}$ es un *dominio entero* por lo que no hay *divisores de* 0. El tener la propiedad de un *orden finito* en la *aditividad* no es algo particular de estos campos.

Definición 2.104. Sea $(K, +, \cdot)$ un *campo*, sí el *orden* en la *aditividad* del 1 no es infinita, entonces se dice que K es de *característica* n donde

$$n = \underbrace{1 + 1 + \cdots + 1}_{n} = 0$$

de lo contrario, se dice que el *campo* es de *característica* 0.

Observación 2.105. Es claro que los racionales $\mathbb{Q}$ fungen como un *campo de característica* 0. Esta definición también funciona para *anillos* donde de hecho $\mathbb{Z}$ es un *anillo de característica* 0. Mas aun, cuando se habla de este concepto, está restringido si se tiene un *dominio entero* o un *campo*.

Teorema 2.106. Sea A un *dominio entero*. Entonces su característica es 0 o un *número primo* es decir, un *campo finito* tiene *característica prima*.

Con esto, procedemos a entrar en *anillos de polinomios*.

Definición 2.107. Sea R *anillo*. Entonces un *polinomio* en las *variables* $x_1, \ldots, x_n$ sobre R es una expresión como

$$f(x_1, \ldots x_n) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x \alpha$$

donde $a_\alpha \in R$ para $\alpha \in \mathbb{N}^n$ y $a_\alpha \neq 0$ para una cantidad finita de $\alpha \in \mathbb{N}^n$. Asimismo, dos polinomios

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \ ; \ g = \sum_{\beta \in \mathbb{N}^n} b_\beta x^\beta$$

son iguales sí y solo si $a_\alpha = b_\beta \, , \, \forall \alpha, \beta \in \mathbb{N}^n$

Observación 2.108. El lugar donde están los coeficientes puede ser también un *campo*. Dependiendo de donde estén se tienen ciertas propiedades o elementos. En este contexto se trabajarán usualmente sobre un campo K.

Definición 2.109. Sea K *campo*. Entonces el conjunto de polinomios

$$\left\{ f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \mid a_\alpha \in R \right\}$$

forma un *anillo* con las operaciones usuales de suma y producto de polinomios, llamamos a este *Anillo de polinomios sobre* K y lo denotamos por $R[x_1, \ldots, x_n]$ o

$R[X]$ en un contexto claro.

Observación 2.110. Usualmente con *polinomios* en una sola variable se tiene un *orden parcial*.

Definición 2.111. Sean $m, f \in K[X]$ no nulos donde m es un monomio y f un polinomio. Entonces se llama

- *coeficiente* a $a_\alpha \in K$ donde $m = a_\alpha x^\alpha$ con $\alpha \in \mathbb{N}^n$, y lo denotamos por $C(m)$.
- *termino* a x^α donde $m = a_\alpha x^\alpha$ con $\alpha \in \mathbb{N}^n$, y lo denotamos por $T(m)$.
- *grado* a $\sum_{i=1}^n \alpha_i$ donde $m = a_\alpha x^\alpha$ y $\alpha = (\alpha_1, \ldots, \alpha_n)$ con $\alpha \in \mathbb{N}^n$, denotamos esto por
$$grd(m) = \sum_{i=1}^{n} \alpha_i$$
- *conjunto de monomios* a $\{m_i\}_{i<\infty}$ donde $f = \sum_i m_i$, y lo denotamos por $M(f)$.
- *conjunto de términos* a $\{T(m_i) \mid m_i \in M(f)\}$, y lo denotamos por $T(f)$.
- *coeficiente líder* a a_α donde $a_\alpha x^\alpha = max(M(f))$, y lo denotamos por $HC(f)$.
- *grado* a $max\{grd(m) \mid m \in M(f)\}$ y lo denotamos por $grd(f)$.

Observación 2.112. Un resultado útil de esto es que en general

$$grd(f \cdot g) = grd(f) + grd(g)$$

Corolario 2.113. Sea K un *campo* y $f \in K[x]$. Entonces $\alpha \in K$ es una *raíz* de f sí y solo si $x - \alpha$ es un divisor de $f(x)$ sobre K.

Observación 2.114. Usualmente se les llamara *factores* a los *divisores* de un polinomio, donde por *divisor* lo decimos en un sentido *algebraico*. Es decir, $f = q \cdot (x - \alpha)$

Los siguientes contenidos están formulados sobre polinomios en una *variable*. Esto debido a que formularlos sobre variables resulta *superfluo* en el contexto.

Corolario 2.115. Sea K un campo, dado $f(x) \in R[x]$ no nulo, entonces se tiene a lo $grd(f)$ raíces distintas de f en K.

Demostración. Véase [21]. □

Observación 2.116. De este enunciado y algunos conceptos anteriores podemos mencionar un teorema bastante importante para toda esta teoría.

Teorema 2.117 (Fundamental de Hilbert)**.** Sí R es *Noetheriano*. Entonces $R[X]$ también es *Noetheriano*.

Observación 2.118. Este teorema se puede extender a variables solo haciendo inducción sobre n. Y como los *campos* solo tienen dos *ideales* siendo estos $\langle 0 \rangle$ y $\langle 1 \rangle$. Estos siempre son *Noetherianos*.

Podemos pensar en sí f tiene todas sus raíces sobre algún *campo* particular. Para esto introducimos las *extensiónes de campos*.

Definición 2.119. Sean L y K campos tales que $K \subseteq L$. Entonces se llama *extensión* de K al campo L. Denotamos esto por L/K.

Los elementos de L no necesariamente son *raíces* en K. Cuando esto sucede les damos un nombre.

Definición 2.120. Sea L/K una *extensión de campos* y $a \in L$. Sí existe $f \in K[x]$ tal que $f(a) = 0$. Entonces a se dice *algebraico* sobre K. De lo contrario, se dice *trascendental*.

Definición 2.121. Sea L/K una *extensión de campos*. Sí cualquier $a \in L$ es *algebraico*. Entonces la *extensión* se dice *algebraica*.

Observación 2.122. Recordando teorema 2.113, entonces la factorización de $f(x)$ es relevante. Sin embargo, esto no siempre se puede hacer, comprobar cuando no es difícil. Afortunadamente existe una herramienta muy útil.

Teorema 2.123 (Criterio de Eisenstein)**.** Sea K un *campo* y $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$. Sí existe $p \in K$ *primo* tal que

$$p|a_i\,,\, 0 \leq i < n\ ,\ p \nmid a_n\ ,\ p^2 \nmid a_0$$

Entonces $f(x)$ es *irreducible*.

Observación 2.124. Entonces si tenemos $f(x) \in K[x]$ y una extensión L/K donde $\alpha \in L - K$ es algebraico, en concreto siendo este raíz de $f(x)$. Podemos decir que $f(x)$ tiene un factor sobre L. Siendo este el caso podemos preguntarnos si existe una *extensión* donde $f(x)$ se descomponga por completo en *factores lineales*

Usualmente hay unos cuantos resultados antes de llegar a esta parte, sin embargo, dentro del contexto no son necesarios por lo que los omitiremos.

Definición 2.125. Sea K un campo. Sí todo $f(x) \in K[x]$ tiene una raíz en K. Entonces decimos que este es *algebraicamente cerrado*. Denotamos esto por $\bar{K}$

Observación 2.126. Esta condición nos asegura una factorizacion completa de $f(x)$, dado que sí $f(x) \in K[x]$, entonces $f(x) = p(x)(x - \alpha_0)$, pero $p(x) \in K[x]$, por tanto, podemos continuar con el mismo procedimiento.

Definición 2.127. Sea L/K una *extensión algebraica* de campos, sí L es *algebraicamente cerrado*. Entonces L se dice una *cerradura algebraica* de K.

Teorema 2.128. Todo campo K tiene una *cerradura algebraica única*.

Demostración. Véase [30] □

2.2 Geometría Algébrica

Los lugares geométricos y su relación con el álgebra son de interés en esta sección, se definirán conceptos fundamentales como la topología de Zariski, los

conjuntos algebraicos y otros conceptos. Todo esto con el fin de poder dar fundamento a algunas de las propiedades en curvas elípticas asimismo, fundamentar nuestra propia teoría.

Definición 2.129. Sea $\mathbb{A}^n$ el conjunto de *n-tuplas* donde las componentes no tienen una *estructura definida*. Entonces llamamos este se dice el *espacio afín*.

$$\mathbb{A}^n = \{(x_1, \ldots, x_n) \mid x \in \mathbb{A}\}$$

Observación 2.130. El *espacio afín* es un intento por liberar las tuplas de estructuras algebraicas dado que el objetivo del estudio en este contexto es meramente de los lugares geométricos. Pero también podemos definir este sobre un *campo*.

$$\mathbb{A}^n(K) = \{(x_1, \ldots, x_n) \mid x \in K\}$$

Usualmente trabajamos sobre un *campo algebraicamente cerrado*.

Definición 2.131. Sea $\bar{K}$ un *campo algebraicamente cerrado* y $\mathcal{V} \subseteq \mathbb{A}^n(\bar{K})$ no vació. Entonces este se dice un *conjunto algebraico*, sí es el *lugar geométrico* asociado a un conjunto de polinomios, es decir, el conjunto de *ceros* a un *sistema de polinomios*.

Observación 2.132. Dado que $\mathcal{V}$ es un conjunto de puntos, podemos pensar en los *polinomios* que se anulan en ccV.

Definición 2.133. Sea $\mathcal{V} \subseteq \mathbb{A}^n(\bar{K})$ un *conjunto algebraico*, entonces definimos su *ideal* por

$$\mathcal{I}(\mathcal{V}) = \{f \in \bar{K}[X] \mid f(\alpha) = 0\,,\, \forall \alpha \in \mathbb{A}^n(\bar{K})\}$$

Observación 2.134. Algo trivial es que $\mathcal{I}(\mathbb{A}^n(\bar{K})) = \{0\}$. Igual que antes, dado un *ideal*, podemos pensar en su *conjunto algebraico*.

Definición 2.135. Sea $I \subseteq \bar{K}[X]$ un *ideal*, entonces definimos su *conjunto algebraico*

por

$$\mathcal{V}(I) = \{\alpha \in \mathbb{A}^n(\bar{K}) \mid f(\alpha) = 0\,,\, \forall f \in I\}$$

Observación 2.136. Algo trivial es que $\mathcal{V}(0) = \mathbb{A}^n(\bar{K})$. Cuando no haya ambigüedad sobre el *espacio afín* en cuestión se omitirá la escritura del *campo* sobre el cual radica.

Tenemos entonces algunas propiedades con estos *operadores*

Definición 2.137. Sea $\mathbb{A}^n$ el *espacio afín*. Entonces tenemos las siguientes propiedades

- $\mathcal{V}(I) \cup \mathcal{V}(J) = V(IJ)$
- $\mathcal{V}(I) \cap \mathcal{V}(J) = V(I + J)$

Observación 2.138. Con estas propiedades y estos conjuntos tenemos de hecho que el espacio afín forma una *topología* τ donde los *abiertos* (elementos de la topología) son $D(I) = \mathbb{A}^n - \mathcal{V}(I)$ es decir, se tiene

- $\emptyset, \mathbb{A}^n \in \tau$
- $\bigcup_I D(I) \in \tau$
- $D(I) \cap D(J) \in \tau$

donde la *unión* es *arbitraria* y la *intersección finita*.

Definición 2.139. Sea $\mathbb{A}^n$ con la topología antes mencionada, entonces esta se llama *topología de Zariski*.

Observación 2.140. Usualmente se trabaja con los *cerrados*, es decir, los *conjuntos algebraicos*. Esto debido a que tienen propiedades interesantes cuando son *irreducibles topológicamente*. Es decir, no existen dos *cerrados* V_1, V_2 tales que $\mathcal{V} = V_1 \cup V_2$

Definición 2.141. Sea $\mathbb{A}^n$ el *afín* y $\mathcal{V}$ un conjunto algebraico, si este es *irreducible*. Entonces llamamos a este *variedad algebraica*.

Observación 2.142. En general se trabaja con *variedades algebraicas* debido a que estas tienen propiedades interesantes como la siguiente.

Teorema 2.143. Sea $\mathcal{V} \subseteq \mathbb{A}^n$ un *conjunto algebraico*. Entonces este es una *variedad algebraica* sí y solo si su *ideal* asociado es *primo*.

Observación 2.144. Lo que esto quiere decir es que se tiene una correspondencia biyectiva entre *ideales primos* y *variedades algebraicas*. Para más información acerca de esto se puede consultar el [6].

Una concepto que a menudo se considera cuando hay objeto geométrico es la *dimensión*. En este contexto necesitamos de un concepto *topológico* para ello.

Definición 2.145. Un *espacio topología* X es llamado *Noetheriano* Sí este satisface la condición de *cadenas descendentes estacionarias* para *cerrados* es decir, para cualquier sucesión

$$Y_1 \supseteq \cdots \supseteq Y_n \supseteq Y_{n+1}$$

se tiene que $Y_n = Y_{n+1}$. Con n entero.

Observación 2.146. Esto y el hecho de que los operadores de *variedad* e *ideal* invierten contenciones, es decir

$$V_1 \subseteq V_2 \Rightarrow \mathcal{I}(V_2) \subseteq \mathcal{I}(V_1)$$
$$I_1 \subseteq I_2 \Rightarrow \mathcal{V}(I_2) \subseteq \mathcal{V}(I_1)$$

nos da paso al siguiente resultado

Teorema 2.147. Sea $\mathbb{A}^n$ el *afín*. Entonces todo *conjunto algebraico* puede ser expresado únicamente como la unión de *variedades algebraicas* sin que ninguna contenga a la otra.

Demostración. Véase [6]. □

Definición 2.148. Sea X un *espacio topológico*. Entonces llamamos *dimensión* de X a

$$dim(X) = Supp\{n \mid Z_0 \subset Z_1 \cdots \subset Z_n\}$$

donde $Z_i \neq Z_j$ sí $i \neq j$, cada Z_i es un *subconjunto cerrado* e *irreducible* de X

Observación 2.149. La *dimensión* en *variedades algebraicas* esta definida en base a su *dimensión topológica*. Procedemos ahora con algunos conceptos sobre suavidad.

Definición 2.150. Sea $\mathbb{A}^n$ el *afín* con $a \in \mathbb{A}^n$ y $f \in K[X]$. Entonces a la tupla

$$\nabla f(a) = \left(\frac{f}{x_1}(a), \ldots, \frac{f}{x_n}(a)\right)$$

la llamamos *gradiente* de f en a.

El gradiente nos ayudara a darle una caracterización a los planos tangentes.

Proposición 2.151. Sea $\mathcal{V} \subseteq \mathbb{A}^n$ una *variedad algebraica* y $a \in \mathcal{V}$. Entonces el *espacio tangente* en a esta dado por

$$T_a\mathcal{V} = \{v \in K^n \mid \nabla f(a) \cdot v = 0\,,\, \forall f \in \mathcal{I}(\mathcal{V})\}$$

donde "$\cdot$"denota el *producto punto entre vectores*.

Demostración. Véase [43] □

Con esto ya podemos hablar de otro aspecto que se cuida, y es tener operaciones bien definidas, para ello necesitamos suavidad.

Definición 2.152. Sea $\mathcal{V}$ una *variedad algébrica* y $a \in \mathcal{V}$. Entonces decimos que $\mathcal{V}$ es *suave* en a sí $dim(T_a\mathcal{V}) = dim(\mathcal{V})$. De lo contrario decimos que es singular. Además, llamamos *suave* a $\mathcal{V}$ si todo punto de $\mathcal{V}$ es suave. En otro caso decimos que $\mathcal{V}$ es singular.

Mas aun, podemos recurrir a un criterio para comprobar la suavidad.

Definición 2.153. Dados polinomios $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Entonces llamamos *Jacobiano* a la matriz

$$\begin{pmatrix} \frac{f_1}{x_1} & \cdots & \frac{f_1}{x_n} \\ \vdots & \ddots & \vdots \\ \frac{f_m}{x_1} & \cdots & \frac{f_m}{x_n} \end{pmatrix}$$

Proposición 2.154 (Criterio del Jacobiano)**.** Sea $\mathcal{V} \subseteq \mathbb{A}^n$ una *variedad algebraica irreducible* con $\mathcal{I}(\mathcal{V}) = \langle f_1, \cdots, f_m \rangle$. Entonces

$$T_a\mathcal{V} = ker(Jac_{f_1,\ldots,f_m}(a))$$

donde, $\mathcal{V}$ es singular en a sí y solo si

$$rk(Jac_{f_1,\ldots,f_m}(a)) < codim(\mathcal{V})$$

Observación 2.155. Aquí se habla de *codimensión*, este concepto es un *complemento* de la *dimensión*. Es decir $codim(\mathcal{V}) = n - \dim(V)$

Ejemplo 2.156. Por ejemplo, si se tuviera que $\mathcal{V} = \mathcal{V}(f)$ donde $f \in K[x_1, \ldots, x_n]$ es *irreducible*, considerando $\mathcal{I}(\mathcal{V}) = \langle f \rangle$. Tenemos $codim(\mathcal{V}) = 1$, dado que en general al ser $\mathcal{V}$ generada por un único polinomio irreducible f se tiene que $dim(\mathcal{V}(f)) = n - 1$. Por tanto el criterio del Jacobiano dice que la matriz

$$\begin{pmatrix} \frac{f}{x_1}(a) & \cdots & \frac{f}{x_n}(a) \end{pmatrix}$$

Es *singular* sí y solo si tiene *rango* 0. Es decir, $\mathcal{V}$ es singular en a sí y solo si

$$\frac{f}{x_1}(a) = \cdots = \frac{f}{x_n}(a) = 0$$

Procedemos ahora con algunos conceptos de geometría proyectiva.

Definición 2.157. Sea $\mathbb{A}^n$ el *Afín*. Considerando 0 la *tupla nula*, definimos el conjunto

$$\mathbb{P}^n = (\mathbb{A}^{n+1} - \{0\})/\sim \quad = \quad \{[X_1 : \cdots : X_{n+1}] \mid X_i \in K\} \tag{2.5}$$

donde

$$[X_1 : \cdots : X_{n+1}] = \{(Y_1, \ldots, Y_{n+1}) \mid (X_1, \ldots, X_{n+1}) \sim (Y_1, \ldots, Y_{n+1}) \iff X_i = \lambda Y_i \,,\, i = 1, \ldots, n+1\}$$

Y a este conjunto lo llamamos *espacio proyectivo estándar*. Sus elementos se suelen decir *coordenadas proyectivas*.

Observación 2.158. Puede llegar a pensarse que la definición es incorrecta debido al momento en donde establecemos el elemento nulo 0. Pero este no es propio de $\mathbb{A}^n$, sino que esta en todo afín de cualquier dimensión, por tanto el valor de 0 se adapta al contexto de las operaciones sin ambigüedad. Las coordenadas proyectivas suelen ser de mucha utilidad para resolver algunos problemas. Uno de sus usos es en la criptografía, sin embargo no exactamente con este espacio proyectivo, sino sobre uno más particular el cual utilizaremos para agilizar nuestras operaciones.

Definición 2.159. Sea $\mathbb{A}^n$ el *Afín*. Considerando 0 la *tupla nula*, definimos el conjunto

$$\mathbb{P}^n(\alpha_1, \ldots, \alpha_{n+1}) = (\mathbb{A}^{n+1} - \{0\})/\sim \quad = \quad \{[X_1 : \cdots : X_{n+1}] \mid X_i \in K\} \tag{2.6}$$

donde

$$[X_1 : \cdots : X_{n+1}] = \{(Y_1, \ldots, Y_{n+1}) \,|(X_1, \ldots, X_{n+1}) \sim (Y_1, \ldots, Y_{n+1}) \\ \iff X_i = \lambda^{\alpha_i} Y_i \,,\, i = 1, \ldots, n+1\}$$

Y a este conjunto lo llamamos *espacio proyectivo ponderado*. Sus elementos se suelen decir *coordenadas proyectivas*.

Observación 2.160. Esta es una definición formal la cual generaliza de cierta forma lo que hizo Jacobi [27] para optimizar operaciones sobre *curvas elípticas*. Este ligero cambio de perspectiva hace que se replanteen ciertos conceptos, pero tales cosas salen del contexto de este trabajo, si se desea ver algo más de esto se puede consultar [39]. Cuando no haya ambigüedad sobre $\mathbb{P}(\alpha_1, \ldots, \alpha_{n+1})$, se llamara a este $\mathbb{P}^n(\alpha)$. Algo que se debe notar es una intersección de elementos más no igualdad entre el *espacio proyectivo estándar* y el afín $\mathbb{A}$. Análogamente para $\mathbb{P}^n(\alpha)$ y $\mathbb{A}$.

Definición 2.161. Sea $\mathbb{P}^n$ el *proyectivo estándar*, considerando el mapeo

$$\phi : \mathbb{P}^n \longrightarrow \mathbb{A}^n$$
$$[X_1 : \cdots : X_{n+1}] \longmapsto (X_1/X_{n+1}, \ldots, X_n/X_{n+1})$$

se tiene una *inclusión* de un subconjunto $\mathbb{P}^n$ en $\mathbb{A}^n$, siempre y cuando $X_{n+1} \neq 0$, dado que hacemos una identificación de cada elemento en $\mathbb{P}^n$ con uno de $\mathbb{A}^n$ considerando

$$[X_1 : \cdots : X_n : X_{n+1}] = [X_1/X_{n+1} : \cdots : X_n/X_{n+1} : 1]$$

entonces a los puntos de $\mathbb{P}^n$ tales que $X_{n+1} \neq 0$ los llamamos *puntos proyectivos*. Los denotamos por

$$U_{n+1} = \{[X_1 : \cdots : X_{n+1}] \in \mathbb{P}^n \mid X_{n+1} \neq 0\} \simeq \mathbb{A}^n$$

Por el contrario, los elementos en $\mathbb{P}^n - U_{n+1}$ son llamados *puntos al infinito*.

Observación 2.162. La pregunta ahora es si podemos ir del *afín* al *proyectivo*, la respuesta es obvia, solo haciendo un proceso en reversa. Pero dejaremos hasta este punto las *coordenadas proyectivas ponderadas*, debido a que su uso solo es en cálculos más no para los siguientes desarrollos.

Definición 2.163. Sea $f \in K[X]$, se dice *homogéneo* de grado d sí

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)\,,\ \forall \lambda \in K$$

Definición 2.164. Sea $f \in K[X]$ con $grd(f) = d$, llamamos *homogeneización* al proceso de hallar $f^* \in K[X]$ donde

$$f^* = x_{n+1}^d \cdot f\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right)$$

Definición 2.165. Sea $\mathcal{V} \in\subseteq \mathbb{A}^n$ una *variedad algebraica*. Entonces consideramos su *encaje* en $\mathbb{P}^n$ mediante la *homogeneización* de sus *polinomios generadores*. Es decir, sea $\mathcal{V} = \langle f_1, \ldots, f_n \rangle$ entonces $\mathcal{V}^* = \langle f_1^*, \ldots, f_n^* \rangle$.

Observación 2.166. Una pregunta que puede surgir es si $\mathcal{V}^*$ seguirá siendo *topológicamente irreducible* y la respuesta es afirmativa dado que para esto, solo se necesita que el *ideal* asociado a la variedad sea *primo*. Y esto si sucede debido a que se preserva la *irreducibilidad algebraica* de los *generadores* incluso después de *homogeneizar*.

Entonces tenemos una *complementación* de *variedades algebraicas* con *variedades proyectivas*. Pero debido a una consideración de ligereza por secciones, no nos extenderemos más. Por tanto tenemos solo dos objetos más por enunciar.

Definición 2.167. Sea $\mathcal{V}$ una *variedad proyectiva* de *dimensión* $n-1$. Entonces llamamos a $\mathcal{V}$ una *hipersuperficie proyectiva*.

Observación 2.168. Respecto a la *dimensión*, esta sigue siendo la misma por como definimos el *encaje* en teorema 2.165

Teorema 2.169 (Teorema de Bézout)**.** Sean X, Y *hipersuperficies proyectivas* en $\mathbb{P}^2$ con grados d y e respectivamente. Considerando $X \cap Y = \{P1, \ldots, P_n\}$. Entonces

$$\sum_j i(X; Y; Pj) = de$$

Teorema 2.170. Lo que esto quiere decir es que, contando multiplicidades que puedan tener las componentes (la función $i(X, Z, P_j)$ con componente P_j) y sumando, estas dan como resultado *el producto de los grados* que es el número de intersecciones de ambas *hipersuperficies*.

Ejemplo 2.171. Consideremos dos *hipersuperficies proyectivas*, digamos $A = \mathcal{V}(Y - X)$ y $B = \mathcal{V}(Y^2Z = X^3 + bZ^2X + cZ^3)$ la primera es de grado 1 y la segunda grado 3. Entonces podemos tener 2 casos donde $A \cap B = \{P, Q, R\}$ o $A \cap B = \{P, P, R\}$. Aplicando teorema 2.169 tenemos que

$$1 + 1 + 1 = 3 = 1 \cdot 3 \quad , \quad 2 + 1 = 3 = 1 \cdot 3$$

2.3 Curvas Elípticas

Dado que mucha de la teoría usada en *curvas elípticas* ya fue establecida, esta sección será más corta que las demás.

Definición 2.172. Sean a_i elementos sobre un campo K, $i = 1, \ldots, 5$, llamamos *curva elíptica* al lugar geométrico E definido por

$$E\colon y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

Sin embargo, sí $char(K) \neq 2, 3$, esto es equivalente a

$$y^2 = x^3 + bx + c\,,\ \Delta = 4b^3 + 27c^2 \tag{2.7}$$

Observación 2.173. Algo que no se suele mencionar es que el discriminante Δ en teorema 2.172 se obtiene con el *criterio del Jacobiano* teorema 2.154. En lo que sigue se trabajara siempre con la curva $E/K : y^2 = x^3 + bx + c$ sobre K con $car(K) \neq 2, 3$.

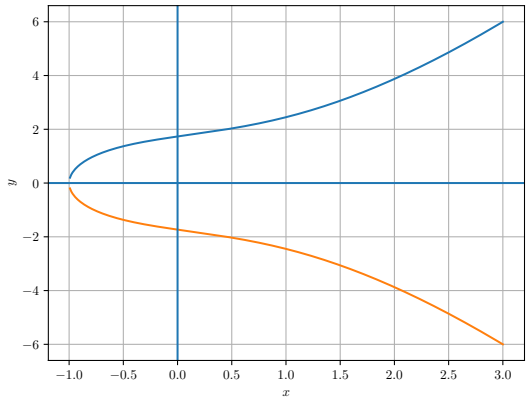


Figura 2.1: Gráfica de $y^2 = x^3 + 2x + 3$

Entonces procedemos a definir la *ley de grupo*.

Definición 2.174. Sea E/K una curva elíptica con un punto $\mathcal{O}$ diferenciado y la operación $\oplus$. Se sigue que

- *identidad* $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P\,,\ \forall P \in E$
- *inversos* Sí $P = (x, y) \in E \Rightarrow (x, y) \oplus (x, -y) = \mathcal{O}$. El punto $(x, -y)$ es denotado por $-P$ y es llamado *inverso de* P, asimismo este siempre está en E.
- Sean $P = (x_1, y_1), Q = (x_2, y_2) \in E$ donde $P \neq \pm Q$. Entonces $P \oplus Q = (x_3, y_3)$ donde

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad , \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

- Sea $P = (x_1, y_1) \in E$ donde $P \neq -P$. Entonces $P \oplus P = 2P = (x_3, y_3)$ donde

$$x_3 = \left(\frac{3x_1^2 + b}{2y_1}\right)^2 - 2x_1 \quad , \quad y_3 = \left(\frac{3x_1^2 + b}{2y_1}\right)(x_1 - x_3) - y_1$$

Observación 2.175. La propiedad de tener un tercer punto siempre está dada por teorema 2.169. El punto $\mathcal{O}$ que se menciona es un *punto al infinito*, es decir, un punto que vive en el *espacio proyectivo* más no en el *afín*. Es decir, el *polinomio homogéneo* asociado con E viene a ser $Y^2Z = X^3 + bXZ^2 + cZ^3$ de donde, considerando $Z = 0$ (los *puntos al infinito*) tenemos

$$Y^2Z = X^3 + bXZ^2 + cZ^3\,,\ Z = 0 \to X^3 = 0 \Leftrightarrow X = 0$$

de donde tenemos solo un *punto al infinito* $[0 : 1 : 0]$.

Proposición 2.176. Sea $(E, \oplus)$ el *grupo de puntos en una curva elíptica*. Entonces se tiene

- $\forall P, Q, R \in E$ *colineales*, $P \oplus Q \oplus R = \mathcal{O}$
- *conmutatividad*, es decir, $P \oplus Q = Q \oplus P\,,\ \forall P, Q \in E$

Algunas otras propiedades que son de interés en esta estructura es la *cardinalidad*. Esto debido a consideraciones de seguridad criptográfica y, asimismo de ello depende sí *grupo* generado por la *ley de grupo* $(\oplus)$ es isomorfo a estructuras con baja periodicidad como $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Este problema resulta tan importante que muchas estimaciones se han tratado de hacer sobre la *cardinalidad*. Así como el *intervalo de Hasse*

Teorema 2.177 (Hasse)**.** Sea E una curva elíptica sobre $\mathbb{F}_q = \mathbb{Z}/p^n\mathbb{Z}$ $(q = p^n)$. Entonces

$$q + 1 - 2\sqrt{q} \leq |\mathbb{F}_q| \leq q + 1 + 2\sqrt{q}$$

es llamado *intervalo de Hasse* y estima la cantidad de puntos en la curva sobre un *campo discreto*.

El otro ejemplo antes mencionado ya está generalizado.

Teorema 2.178. Sea E una curva elíptica sobre $\mathbb{F}$. Entonces $E(\mathbb{F}_q)$ es isomorfo a $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ donde n_1, n_2 son enteros positivos únicamente determinados tales que $n_2|n_1$ y $n_2|q-1$

Recordando, mencionamos el concepto de *coordenadas proyectivas ponderadas* debido a que *Jacobi* ya lo había utilizado con *curvas elípticas*, aunque no en el sentido de hoy sino con un fin computacional.

Ejemplo 2.179. Sea $P = [X_1 : Y_1 : Z_1] \in E$, con $P \neq -P$. Entonces $2P = (X_3 : Y_3 : Z_3)$ en coordenadas jacobianas viene dado por:

$$\begin{aligned} X_3 &= (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2, \\ Y_3 &= (3X_1^2 + aZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4, \\ Z_3 &= 2Y_1Z_1. \end{aligned}$$

nos limitamos a mostrar la duplicación de puntos.

Observación 2.180. Puede parecer una expresión más compleja, pero el hecho es que calcular *inversos* en $\mathbb{F}_p$ es pesado computacionalmente hablando, con lo que hizo *Jacobi* no se tiene que trabajar con esto (en el transcurso del cálculo) y lo que se efectúa son operaciones de suma y multiplicación, que en general resultan más ligeras. Pero al final si se tiene que hacer solo una inversión para volver a *coordenadas afines*.

2.4 Criptografía

La *criptografía* es el estudio del cifrado de la información, es normal por tanto que sus principales temas sean el *cifrado* y *descifrado* (no ataque) de mensajes. Estos *cifrados* se suelen clasificar en dos grandes ramas.

Definición 2.181. Sea π un *cifrado*, entonces decimos que este es

- De *llave privada* si cualesquiera dos individuos en un canal de comunicación comparten una misma *llave* secreta.
- De *llave publica* si cualesquiera dos individuos en un canal de comunicación tienen una *llave publica* y una *llave privada*.

Observación 2.182. Como ya se mencionó en la introducción, los *cifrados de llave publica* parecieran ser la solución, sin embargo, hasta ahora no ha habido uno que sea más efectivo que los *cifrados de llave privada* en juego actualmente. Esto dependiendo del tamaño de la llave. No es un parámetro estático y suele ser importante debido a que si no se tiene una suficiente cantidad y de forma que haya algún tipo de análisis que reduzca las opciones, podría hacerse un ataque de fuerza bruta.

Definición 2.183. Sea $\pi(m,k)$ un *cifrado*. Este funge como un mapeo

$$\pi : \mathbb{K}^r \times \mathbb{K}^l \to \mathbb{K}^n$$
$$(m,k) \mapsto c$$

usualmente $l \leq r$, un caso donde cuando se tiene igualdad es en el *one time pad*. K es algún espacio.

Asimismo, se define un *descifrado* que funge de cierta forma como una *función inversa*.

Definición 2.184. Sea $\pi^{-1}(m,k)$ un *descifrado*. Este funge como un mapeo

$$\pi : \mathbb{K}^r \times \mathbb{K}^l \to \mathbb{K}^n$$
$$(c,k) \mapsto m$$

también tenemos que usualmente $l \leq r$.

Observación 2.185. Esta estructura también suele ser llamada *puerta trampa*. El termino viene de una analogía sobre entrar en un cuarto que tiene facilidad para meterse, pero no para salir a menos que se conozca algún detalle. No siempre sucede que las *dimensiones* del espacio de *mensajes* y *cifrados* coincida, esto es con fines de interrumpir diversos ataques.

Asimismo, π se podría pensar como un algoritmo pero esto es incorrecto, más que eso, es un proceso complejo dado que se encarga de codificar los datos y esconderlos, pero esto último lo hace con ayuda de otra herramienta de la que después se hablara. pueden ser criterios probabilísticos o teóricos. Como por ejemplo el que $\pi(m_1,k)$ *difiera considerablemente* de $\pi(m_2,k)$ cuando m_1 y m_2 son *similares*. Esto debido a que también se suelen hacer ataques analizando *distancias de palabras*. Un *ejemplo* de esto es la *distancia de Hamming*.

Definición 2.186. Sean $m_1, m_2 \in \mathbb{F}_2^k$, entonces llamamos *distancia de Hamming* a

$$H(m_1,m_2) = \sum_{i=1}^{k} \rho_i(m_1 + m_2)$$

donde ρ_i es el mapeo de proyección $\rho_i(x_1,\ldots,x_i,\ldots,x_k) = x_i$. Observemos como si en la entrada i para m_1 y m_2 se tienen caracteres iguales, Hamming da un 0. Sin embargo, cuando difieren se obtiene un 1. Por tanto $0 \leq H \leq k$ donde 0 significa una coincidencia perfecta y k una discrepancia completa.

De toda esta discusión puede entenderse entonces que la diferencia entre *llave*

privada y *llave publica* radica en el *cifrado*. Siendo estos

$$\pi(m,k) \mapsto c \quad , \quad \pi(m,k_s,k_p)$$

respectivamente. Observemos entonces que el de llave publica tiene que manejar dos llaves, la *publica* k_s (shared) y *privada* k_p (private).

Observación 2.187. Aun cuando *llave publica* tiene dos llaves, estas no necesariamente son *independientes*. Con esto nos referimos a que durante el *proceso* para *generar* las llaves, estas pueden crearse considerando información similar.

Asimismo, aun cuando podemos estar mucho tiempo pensando en un esquema casi perfecto para ocultar información, un error es tratar de esconder este esquema, el otro error se mencionará después de enunciar un principio basado en el primer error.

Definición 2.188 (Principio de Kerckhoff)**.** Sea π un cifrado. La *seguridad* del mismo no debe basarse en su desconocimiento.

Observación 2.189. Lo que Kerckhoff sugiere es natural después de todo, muchos sistemas de cifrado en la antigüedad fueron descifrados solo descubriendo su funcionamiento, el *Cesar* o *enigma*, aunque este último bajo otras condiciones. Hay otros principios de Kerckhoff, pero debido a la época en que los enuncio, todos los demás a excepción del mencionado son anticuados.

El segundo error es una reducción o *replanteamiento* del problema. No ahondaremos mucho en lo que una *reducción* significa dado que hay muchas formas de reducir un problema. Pero para intentar explicar esto, veamos un ejemplo.

Definición 2.190. Sea g una *raíz primitiva* de $\mathbb{F}_p$ (un *generador*) y $h \in \mathbb{F}_p$ no nulo. Llamamos *problema del logaritmo discreto* a hallar x tal que

$$g^x = h \ (mod\, p)$$

x es llamado *logaritmo discreto* de h en base g y usualmente es denotado por $log_g(h)$. A este problema lo denotamos por (DLP).

En un inicio Diffie y Hellman utilizaron este problema para un algoritmo que intercambia llaves. Lo que sucedió después fue una gran cantidad de ataques los cuales no atacaban directamente la suposición que hacía fuerte a este problema, un ejemplo de ello es el algoritmo *Shank´s Babystep-Giantstep* que se basa en crear dos listas con elementos y verificar *coincidencias*.

Observación 2.191. Usualmente se pueden hacer reducciones pero hasta ahora ninguna que logre reducir un problema de complejidad *exponencial* a *polinomial*. En caso de que sucediera quien lo haga seguro se llevaría un premio.

La criptografía es bastante extensa así que nos delimitamos a lo más fundamental. Para ubicarnos hay que dar un par de conceptos más. Comprendiendo que el *cifrado* es un proceso, nos adentramos en lo que está dentro.

Definición 2.192. Sea π un *cifrado*. Este es un *mapeo* de una *transformación algebraica* dependiente de una clave. Construido sobre una *primitiva criptográfica*

Es decir, el cifrado solo se encarga de transformar la información mediante una llave y alguna primitiva criptográfica.

Definición 2.193. Sea (k, h, S) la terna compuesta por h un problema difícil, k una clave y S una suposición de seguridad donde

$$S : K \times h \to [0, 1]$$

es un mapeo en función de *llave* $k \in J$ y *primitiva* $h \in H$, que da un *indicé* de que tan seguro es que el *problema difícil* realmente lo sea. Entonces llamamos a esta *primitiva criptográfica*.

Definición 2.194. Llamamos *problema difícil* a una determinada problemática cuya *solución* es tiene una gran complejidad en el aspecto computacional. Es decir, un *problema computacional parametrizado*.

Mas aun, estos problemas difíciles no salen de cualquier lugar sino en general de *estructuras algebraicas*

Definición 2.195. Sea P un problema difícil, este se define usualmente sobre una estructura algebraica. Llamamos a esta *estructura base*.

Puede parecer que nos estamos adentrando en el área más *simple* de la criptografía, sin embargo, hallar nuevas estructuras puede ser de utilidad. Un ejemplo de ello son las *curvas elípticas*

Ejemplo 2.196. Sea E una curva elíptica sobre $\mathbb{F}_q$ y $P \in E$ un elemento primitivo. Entonces dado $Q \in E$, al problema de hallar n tal que

$$nP = Q$$

se llama *problema del logaritmo discreto sobre curvas elípticas* $(ECDLP)$.

Observación 2.197. Cuando Koblitz trajo esta estructura a la criptografía, ataques que funcionaban con el (DLP) ya no lo hacían con el $(ECDLP)$. Algunos se adaptaron sin embargo no lograron obtener la misma eficacia que con (DLP).

CAPÍTULO 3

DESARROLLO

Dado que ya hemos dado las bases para trabajar sin ningún problema o retraso, iremos directo a construir nuestra *superficie* y analizar algunas propiedades geométricas de utilidad para desarrollar una *ley de composición*.

3.1 Construcción de una Superficie

El primer resultado que nos da paso a trabajar con todo esto es el siguiente.

Teorema 3.1. Sea S una *superficie cubica suave*. En general no puede definirse una estructura de *grupo algebraico* (*variedad algebraica que se comporta a la vez como grupo*) de forma *global*.

Demostración. Véase [4] □

Observación 3.2. Algo que si podemos obtener es al menos una *estructura de quasi-grupo*. [4].

Sea $E : y^2 = x^3 + bx + c$ una *curva elíptica*. Entonces podemos considerar la superficie generada por la rotación de E alrededor del eje X.

$$z^2 + y^2 = x^3 + bx + c$$

Sin embargo, esto no tiene la suficiente complejidad, dado que al rotar se tienen infinitas *simetrías* respecto a X. Por ello consideramos un término cruzado yz. De

donde obtenemos

$$z^2 + yz + y^2 = x^3 + bx + c$$

Esto esta bien, sin embargo, con parámetros en la izquierda se puede tener un espacio más grande de *superficies* lo cual es ideal cuando se quieren tomar parámetros aleatorios. Tenemos entonces

$$rz^2 + hyz + sy^2 = x^3 + bx + c \tag{3.1}$$

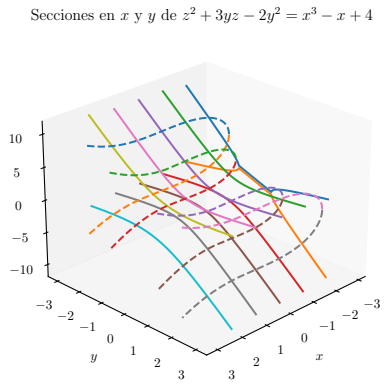


Figura 3.1: Gráfica de $z^2 + 3yz - 2y^2 = x^3 - x + 4$

Claro está que podemos preguntarnos si esto define una *variedad algebraica*. Considerando el grado de $|S| = 3$, supongamos que es reducible y consideremos este en $K[y, z][x]$. Entonces

$$S(x, y, z) = g \cdot h$$

con $|g| = 1$ y $|h| = 2$ de donde

$$S = (x + u(x, y))(x^2 + xv + w(x, y)) = x^3 + x^2(u + v) + x(w + uv) + wu$$

donde $u, v, w \in K[y, z]$. Igualando coeficientes con $x^3 + bx + (c - rz^2 - hyz - sy^2)$

tenemos

$$\begin{aligned} u + v &= 0 \\ w + uv &= b \\ wu &= c - rz^2 - hyz - sy^2 \end{aligned}$$

de donde $u = -v$, $w = b + u^2$ y $bu + u^3 = c - rz^2 - hyz - sy^2$. Tenemos entonces dos casos.

$$grd(u) \geq 1 \qquad\qquad grd(u) = 0$$

$$\Rightarrow u(x,y)^3 - rz^2 - hyz - sy^2 = 0 \qquad \Rightarrow u \in K$$

$$\Rightarrow \nexists u, v, w \qquad\qquad c - rz^2 - hyz - sy^2 = u$$

En ambos casos, o no se tiene soluciones o los coeficientes son constantes con lo cual se tiene una curva degenerada. Por tanto, S es irreducible.

Procedemos entonces a revisar *suavidad*.

Recordando el teorema 2.154, consideramos el Jacobiano de $S = rz^2 + hyz + sy^2 - x^3 - bx - c$

$$\begin{pmatrix} -3x^2 - b & 2sy + hz & 2rz + hy \end{pmatrix}$$

siendo $S = \mathcal{V}(rz^2 + hyz + sy^2 - x^3 - bx - c)$. una *variedad algebraica*, entonces $dim(S) = 2$ y $codim(S) = 1$ dado que $dim(\mathbb{A}^3) = 3$. Entonces el rango $rk < 1$, es decir

$$\frac{\partial S}{\partial x}(a) = \frac{\partial S}{\partial y}(a) = \frac{\partial S}{\partial z}(a) = 0$$

Asimismo, si $a = (x_0, y_0, z_0) \in S$, tenemos la ecuación extra $S\Big|_a = 0$. Procedemos entonces a resolver el sistema para hallar cuando se tienen singularidades

$$-3x_0^2 - b = 0 \tag{1}$$

$$2sy_o + hz_0 = 0 \tag{2}$$

$$2rz_0 + hy_0 = 0 \tag{3}$$

$$rz_0^2 + hy_0z_0 + sy_0^2 = x_0^3 + bx_0 + c \tag{4}$$

notemos que al multiplicar (2) y (3) por y_0, z_0 respectivamente y sumarlas se obtiene $2rz_0^2 + 2hy_0z_0 + 2sy_0^2 = 0$ de donde obtenemos

$$-3x_0^2 - b = 0 \tag{1}$$

$$x_0^3 + bx_0 + c = 0 \tag{2}$$

sustituyendo (1) en (2) se tiene $x_0^3 - 3x_0^2 + c = 0$. Entonces tenemos las ecuaciones

$$b = -3x_0^2 \tag{1}$$

$$c = 2x_0^3 \tag{2}$$

elevando (1) al cubo y (2) al cuadrado se tiene $\frac{b^3}{-27} = x_0^6 = \frac{c^2}{4}$. de donde obtenemos el discriminante

$$4b^3 + 27c^2 \neq 0$$

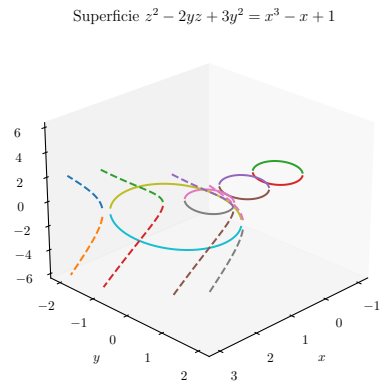


Figura 3.2: Gráfica de $z^2 - 2yz + 3y^2 = x^3 - x + 1$

Por el contrario, si nos concentramos en el sistema generado por (2) y (3) tenemos un sistema homogéneo. Procedemos por la *regla de Cramer*.

$$\begin{vmatrix} 2s & h \\ h & 2r \end{vmatrix} = 4rs - h^2 = \Delta s$$

Dado que este sistema es *homogéneo*. Tenemos una solución trivial o algo indeterminado. Mas aun, sí resolvemos esto por *Gauss* llegamos a la misma identidad, por tanto, pediremos que $h^2 - 4rs \neq 0$.

De aquí tenemos entonces las dos condiciones

$$4b^3 + 27c^2 \neq 0 \ , \ h^2 - 4rs \neq 0$$

bajo las cuales tendremos *suavidad*. Pero esto no es suficiente cuando se trabaja sobre $\mathbb{F}_p$, dado que se tiene un *caso degenerado* cuando $h^2 - 4rs = x$ siendo x un *residuo*

cuadrático. Por tanto, tenemos las tres condiciones

$$4b^3 + 27c^2 \neq 0 \qquad\qquad h^2 - 4rs \neq 0$$

$$h^2 - 4rs \neq x \ , \ \left(\frac{x}{p}\right) = 1$$

Observación 3.3. Recordemos que $\left(\frac{x}{p}\right)$ denota el símbolo de Legendre. teorema 2.102. El *caso degenerado* del cual se habla es de una degeneración en la parte *cuadrática* de $\mathcal{S}$ a un par de rectas.

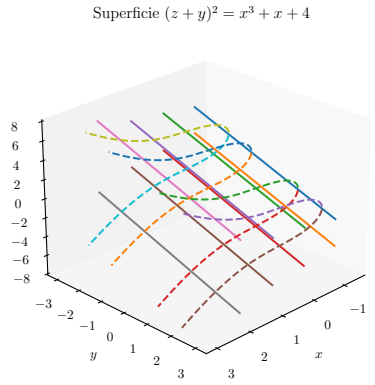


Figura 3.3: Gráfica de $z^2 + 2yz + y^2 = x^3 + x + 4$

Ahora procedemos a obtener el número de intersecciones entre nuestra superficie $\mathcal{S}$ y cualquier *recta* en *posición general*. Recordando teorema 2.169. Tenemos que $\mathcal{S}$ es una *variedad algebraica* de *dimensión* 2. Entonces esta es una *hipersuperficie proyectiva*. Análogamente, dada una recta ℓ en el espacio, esta es $\mathcal{V}(p_1, p_2) = \mathcal{V}(p_1) \cap \mathcal{V}(p_2)$ siendo p_1, p_2 planos. Entonces ya podemos aplicar *Bézout*.

$$\mathcal{V}(p_1) \cap \mathcal{V}(p_2) \cap \mathcal{V}(S) = 1 \cdot 1 \cdot 3 = 3$$

Por tanto, ℓ y S tienen intersecciones en exactamente 3 puntos.

Observación 3.4. La razón de porque expresamos ℓ como la intersecciones de dos

planos es debido a que ℓ no es una *hipersuperficie proyectiva*, Sin embargo, los planos p_1 y p_2 si lo son. Por cierto, se utilizo una forma equivalente de *Bézout* para múltiples *hipersuperficies proyectivas*.

Con esto tenemos casi todo resuelto, sin embargo, debemos considerar que, debido a que $\mathcal{S}$ es una *superficie cúbica*. Entonces puede contener a lo más 27 rectas (también pueden estar en el espacio proyectivo). Sin embargo, esto no es un problema dado que mientras se hagan cálculos, podemos verificar si en algún momento se tiene una recta. Guardar esta información y cuando se hagan operaciones hacer verificaciones rápidas. Esto dado que la complejidad para operar es a lo más *lineal*. Se hablará de esto después.

3.2 Ley de Composición

Procedemos ahora a desarrollar nuestra operación sobre $\mathcal{S}$. Dado que ya estamos en el *espacio*, procedemos de forma general tomando un punto $P \in \mathcal{S}$ y alguna dirección M que estará dada por el contexto.
Sea P un punto de la superficie generada por la ecuación

$$\mathcal{S} : rz^2 + hzy + sy^2 = x^3 + bx + c \tag{1}$$

donde $b, c, r, h, s \in K$ siendo K un **campo**.

Si P se mueve en una dirección M, consideramos la recta trazada por este movimiento $\ell(t) = P + Mt, \forall t$. Hallamos las intersecciones de esta recta con nuestra superficie

sustituyendo $\ell(t)$ en (1)

$$
\begin{aligned}
&r(p_3+m_3t)^2+h(p_2+m_2t)(p_3+m_3t)+s(p_2+m_2t)^2=(p_1+m_1t)^3+b(p_1+m_1t)+c\\
&\quad\Rightarrow r(p_3^2+2p_3m_3t+m_3^2t^2)+h(p_2p_3+t(p_2m_3+p_3m_2)+m_2m_3t^2)+s(p_2^2+2p_2m_2t+m_2^2t^2)\\
&\qquad-(p_1^3+3p_1^2m_1t+3p_1m_1^2t^2+m_1^3t^3+b(p_1+m_1t)+c)\\
&\quad=-t^3m_1^3+t^2(rm_3^2+sm_2^2+hm_2m_3-3p_1m_1^2)\\
&\qquad+t(2p_3m_3+2p_2m_2+hp_2m_3+hp_3m_2-3p_1^2m_1-bm_1)+C=0
\end{aligned}
$$

Notemos que como P está en $\mathcal{S}$, satisface (1), sustituyendo tenemos

$$rp_3^2+hp_2p_3+sp_2^2-p_1^3-bp_1-c=0$$

siendo esto C, se tiene que $C=0$. Obtenemos

$$-t^3m_1^3+t^2(rm_3^2+sm_2^2+hm_2m_3-3p_1m_1^2)+t(2p_3m_2+2p_2m_2+h(p_2m_3+p_3m_2)-3p_1^2m_1-bm_1)=0$$

Sabemos que $t=0$ es raíz, por tanto

$$-t^2m_1^3+t(rm_3^2+sm_2^2+hm_2m_3-3p_1m_1^2)+(2p_3m_2+2p_2m_2+h(p_2m_3+p_3m_2)-3p_1^2m_1-bm_1)=0$$

Considerando t_1 y t_2 asociados a puntos en $\ell\cap\mathcal{S}$, se tiene $(t-t_1)(t-t_2)=t^2-t(t_1+t_2)+t_1t_2=0$ siendo esto equivalente a (3), tenemos

$$t_1+t_2=\frac{rm_3^2+sm_2^2+hm_2m_3-3p_1m_1^2}{m_1^3}$$

De donde

$$t_1=\frac{rm_3^2+sm_2^2+hm_2m_3-3p_1m_1^2}{m_1^3}-t_2$$

donde el punto asociado a t_2 y este mismo valor se suponen conocidos. Por tanto,

hemos hallado todos los puntos de intersección entre ℓ y $\mathcal{S}$, el tercero de ellos dado por $P + M\lambda$ donde

$$\lambda = \frac{rm_3^2 + sm_2^2 + hm_2m_3 - 3p_1m_1^2 - t_2m_1^3}{m_1^3} \tag{3.2}$$

Observación 3.5. Cuando $m_1 = 0$ se anula el denominador. Esto mismo sucede cuando se trabaja con curvas elípticas, por lo mismo suele diferenciarse un punto como la identidad, usualmente el punto al infinito O debido a sus propiedades. Pero en nuestro caso eso no será posible, por tanto, nos restringimos a que nuestra operación sea *transversal* respecto a *secciones* generadas al fijar x.

Algo obvio es que cuando $P = Q$, el problema es tener un *plano tangente* en lugar de una *recta tangente*. Por tanto, al considerar tangencia a $\mathcal{S}$ en P, tenemos más de una dirección. Para resolver esta ambigüedad haremos uso de una *analogía*, pero antes, es necesario conocer al menos una simetría de nuestra superficie.

Dado que ahora nos encontramos en el espacio podemos considerar el uso de otras simetrías. Supongamos que hay una rotación en un ángulo θ respecto al eje X que resulta ser una simetría. Procedemos entonces a determinar si existe tal angulo. Considerando además que esta debe ser una *involución*.

Observación 3.6. Esta última exigencia no es trivial, esta condición *da vida* a las *curvas elípticas* y nuestra estructura no es la excepción. Esto se discutirá más adelante.

Sea ϕ_θ una rotación que fije x, entonces esta es de la forma

$$\phi_\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & \sin(\theta) \\ 0 & -\sin(\theta) & \cos(\theta) \end{pmatrix} \tag{3.3}$$

Sea $P = (x, y, z) \in \mathcal{S}$, entonces

$$\phi_\theta P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & \sin(\theta) \\ 0 & -\sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y\cos(\theta) + z\sin(\theta) \\ -y\sin(\theta) + z\cos(\theta) \end{pmatrix}$$

Sustituyendo en (1), simplificando e igualando coeficientes polinomiales obtenemos el siguiente sistema

$$s\cos^2(\theta) + r\sin^2(\theta) - h\sin(\theta)\cos(\theta) = s \tag{1}$$

$$2s\cos(\theta)\sin(\theta) - 2r\cos(\theta)\sin(\theta) - h\sin^2(\theta) + h\cos^2(\theta) = h \tag{2}$$

$$s\sin^2(\theta) + r\cos^2(\theta) + h\sin(\theta)\cos(\theta) = r \tag{3}$$

asociamos algunos términos, restamos (3) de (1) y utilizamos identidades trigonometricas, se tiene entonces

$$(s - r)\sin(2\theta) + h\cos(2\theta) = h \tag{1}$$

$$(s - r)\cos(2\theta) - h\sin(2\theta) = s - r \tag{2}$$

Resolviendo respecto a $\sin(2\theta)$ y $\cos(2\theta)$ por Cramer obtenemos

$$\Delta_s = \begin{vmatrix} s-r & h \\ -h & s-r \end{vmatrix} = h^2 + (s-r)^2 \neq 0$$

por otra parte

$$\Delta_{sin} = \begin{vmatrix} h & h \\ (s-r) & (s-r) \end{vmatrix} = 0 \ , \ \Delta_{cos} = \begin{vmatrix} s-r & h \\ -h & s-r \end{vmatrix} = h^2 + (s-r)^2$$

Por tanto tenemos como soluciones

$$\sin(2\theta) = 0 \ , \ \cos(2\theta) = 1$$

que es lo mismo que

$$\sin(\theta)\cos(\theta) = 0 \, , \, \cos^2(\theta) - \sin^2(\theta) = 1$$

de donde obtenemos soluciones para θ

$$\begin{aligned} \sin(\theta) = 0 \quad & \qquad \cos(\theta) = 0 \\ \Rightarrow \cos^2(\theta) = 1 \quad & \qquad \Rightarrow -\sin^2(\theta) = 1 \\ \Rightarrow \theta = \pi k \, , \, k \in \mathbb{Z} \quad & \qquad \nexists \theta \in (0, 2\pi) \end{aligned}$$

Por tanto, nuestra matriz de rotación está dada por

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

comprobamos que esta actúa como simetría sustituyendo $(x, -y, -z)$. La sustitución es trivial.

Cuando se trabaja con curvas elípticas y la duplicación de puntos, aplicamos una reflexión respecto al eje, la cual actúa como una simetría, algo que no se suele notar es que al considerar el punto simétrico junto con su tangente, las tangentes tienen la misma intersección con el eje X. Determinamos sí esto sucede en nuestro caso.

Considerando

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Recordamos que dados dos planos ℓ_1 y ℓ_2, la intersección de estos (en un caso general) es una recta, para probar que esta siempre corta al eje X basta hallar la intersección de ℓ_1 con X y ver que esta pertenece a ℓ_2.

Sea

$$T_P\mathcal{S} \coloneqq \left\{ X \in \mathbb{Q}^3 \,:\, \nabla\mathcal{S}\Big|_P \cdot (X - P) = 0 \right\} \tag{3.4}$$

el plano tangente a $\mathcal{S}$ en el punto $P \in \mathcal{S}$. Dadas las observaciones anteriores, solo necesitamos la intersección de $T_P\mathcal{S}$ con

$$X : \ell(t) = (1, 0, 0)t \, , \, \forall t \in \mathbb{R}$$

Sustituyendo X

$$\begin{aligned} & \nabla\mathcal{S}\Big|_P \cdot (t - p_1, -p_2, -p_3) = 0 \\ \Rightarrow & \left.\frac{\partial\mathcal{S}}{\partial x}\right|_P (t - p_1) - \left.\frac{\partial\mathcal{S}}{\partial y}\right|_P p_2 - \left.\frac{\partial\mathcal{S}}{\partial z}\right|_P p_3 = 0 \end{aligned}$$

Esto es

$$\begin{aligned} & (3p_1^2 + b)(t - p_1) + (2sp_2 + hp_3)p_2 + (2rp_3 + hp_2)p_3 = 0 \\ & \Rightarrow t = \frac{2(rp_3^2 + hp_3p_2 + sp_2^2)}{-(3p_1^2 + b)} + p_1 \\ & \Rightarrow t = \frac{2(p_1^3 + bp_1 + c) - p_1(3p_1^2 + b)}{-(3p_1^2 + b)} \\ & \Rightarrow t = \frac{p_1^3 - bp_1 - 2c}{3p_1^2 + b} \end{aligned}$$

Entonces $A = \left(\frac{p_1^3 - bp_1 - 2c}{3p_1^2 + b}, 0, 0\right)$ es nuestra intersección de $T_P\mathcal{S}$ con X.

Sustituyendo en $T_{\phi P}\mathcal{S}$

$$\begin{aligned} \nabla\mathcal{S}\Big|_{\phi P} \cdot (A - \phi P) &= 0 \\ &= \left.\frac{\partial\mathcal{S}}{\partial x}\right|_{\phi P} \left(\frac{p_1^3 - bp_1 - 2c}{3p_1^2 + b} - p_1\right) + \left.\frac{\partial\mathcal{S}}{\partial y}\right|_{\phi P} p_2 + \left.\frac{\partial\mathcal{S}}{\partial z}\right|_{\phi P} p_3 \\ &= (-3p_1^2 - b)\left(\frac{p_1^3 - bp_1 - 2c - p_1(3p_1^2 + b)}{3p_1^2 + b}\right) - (2sp_2 + hp_3)p_2 - (2rp_3 + hp_2)p_3 \\ &= p_1^3 - bp_1 - 2c - p_1(3p_1^2 + b) + 2sp_2^2 + hp_2p_3 + 2rp_3^2 + hp_2p_3 \\ &= p_1^3 - bp_1 - 2c - 3p_1^3 - bp_1 + 2(p_1^3 + bp_1 + c) = 0 \end{aligned}$$

Hallamos entonces que $A \in T_P\mathcal{S} \cap T_{\phi P}\mathcal{S}$. Por tanto, A es intersección de $T_P\mathcal{S}$ con X y un punto que nos dará una *orientación* para nuestra recta tangente a $\mathcal{S}$ por P.

Sea $\mathcal{S}/K$ el *lugar geométrico* de la curva $\mathcal{S}$ sobre el campo K (por simplicidad de escritura $\mathcal{S}$), con $P, Q \in \mathcal{S}$, y $x(P) \neq x(Q)$, definimos la operación binaria

$$\oplus \colon \mathcal{S} \times \mathcal{S} \longrightarrow \mathcal{S} \ \mid \ P \oplus Q = \phi(P + M\lambda) = R$$

Donde ϕ es la *rotación* usual, $M = Q - P$ y λ se define como

$$\lambda = \frac{rm_3^2 + sm_2^2 + hm_2m_3 - 3x_1m_1^2 - m_1^3}{m_1^3}$$

Observación 3.7. Esta condición se trabajará como algo implícito en los siguientes desarrollos por simplicidad de escritura.

Recordando que cuando se trabaja de forma computacional con curvas elípticas suelen usarse expresiones explicitas para las componentes de R, procederemos a obtener las expresiones correspondientes dada nuestra operación con ϕ siendo la rotación usual y $M = Q - P$ con $P = (x_1, y_1, z_1),\ Q = (x_2, y_2, z_2)$.

$$R = P \oplus Q = \phi(P + M\lambda) \Rightarrow R = \begin{pmatrix} x_3 = x_1 + (x_2 - x_1)\lambda \\ y_3 = -[y_1 + (y_2 - y_1)\lambda] \\ z_3 = -[z_1 + (z_2 - z_1)\lambda] \end{pmatrix} \tag{3.5}$$

de donde

$$x_3 = x_1 + (x_2 - x_1)\frac{rm_3^2 + sm_2^2 + hm_2m_3 - 3x_1m_1^2 - m_1^3}{m_1^3}$$

es decir

$$x_3 = x_1 + \frac{rm_3^2 + sm_2^2 + hm_2m_3}{m_1^2} - 3x_1 - (x_2 - x_1) = \frac{rm_3^2 + sm_2^2 + hm_2m_3}{m_1^2} - x_1 - x_2$$

considerando $\lambda = \frac{x_3 - x_1}{x_2 - x_1}$ obtenemos

$$x_3 = \frac{rm_3^2 + sm_2^2 + hm_2m_3}{m_1^2} - x_1 - x_2 \tag{1}$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \tag{2}$$

$$z_3 = \left(\frac{z_2 - z_1}{x_2 - x_1}\right)(x_1 - x_3) - z_1 \tag{3}$$

Estas expresiones son análogas al caso de curvas elípticas clásicas y de hecho cuando nos restringimos al plano $z = 0$ estas expresiones pasan a ser iguales.

Sean $P, Q \in \mathcal{S}$ tales que $P = Q$, procedemos a obtener expresiones explicitas tal y como hicimos con la suma de puntos distintos donde $M = A - P$ con $A = \left(\frac{x_1^3 - bx_1 - 2c}{3x_1^2 + b}, 0, 0\right)$, $P = (x_1, y_1, z_1)$.

$$R = P \oplus P = \phi(P + M\lambda) \Rightarrow R = \begin{pmatrix} x_3 = x_1 + m_1\lambda \\ \\ y_3 = -[y_1 + (-y_1)\lambda] \\ \\ z_3 = -[z_1 + (-z_1)\lambda] \end{pmatrix} \tag{3.6}$$

de donde

$$\begin{aligned} x_3 = x_1 + m_1\lambda &= x_1 + m_1\left(\frac{rm_3^2 + sm_2^2 + hm_2m_3 - 3x_1m_1^2}{m_1^3}\right) \\ &= x_1 + \frac{rm_3^2 + sm_2^2 + hm_2m_3 - 3x_1m_1^2}{m_1^2} \end{aligned}$$

es decir

$$x_3 = x_1 + \frac{rm_3^2 + sm_2^2 + hm_3m_2}{m_1^2} - 3x_1 = \frac{rm_3^2 + sm_2^2 + hm_3m_2}{m_1^2} - 2x_1$$

esto pareciera no ser una forma análoga a la duplicación de puntos en curvas elípticas, sin embargo, recordemos que $M = A - P$, por tanto

$$x_3 = \frac{rz_1^2 + sy_1^2 + hy_1z_1}{m_1^2} - 2x_1 \qquad (*)$$

donde

$$m_1 = \frac{x_1^3 - bx_1 - 2c}{3x_1^2 + b} - x_1 = -2\frac{x_1^3 + bx_1 + c}{3x_1^2 + b} = -2\frac{rz_1^2 + sy_1^2 + hy_1z_1}{3x_1^2 + b}$$

sustituyendo en $*$ obtenemos

$$x_3 = \frac{rz_1^2 + sy_1^2 + hy_1z_1}{\left(\frac{-2(rz_1^2+sy_1^2+hy_1z_1)}{3x_1^2+b}\right)^2} - 2x_1 = \frac{(3x_1^2 + b)^2}{4(rz_1^2 + sy_1^2 + hy_1z_1)} - 2x_1$$

para las otras componentes definimos

$$\lambda = \frac{x_3 - x_1}{m_1} = (x_3 - x_1)\left(\frac{3x_1^2 + b}{-2(rz_1^2 + sy_1^2 + hy_1z_1)}\right)$$

de donde obtenemos

$$x_3 = \frac{(3x_1^2 + b)^2}{4(rz_1^2 + sy_1^2 + hy_1z_1)} - 2x_1 \qquad (1)$$

$$y_3 = \frac{y_1}{2}\left(\frac{3x_1^2 + b}{rz_1^2 + sy_1^2 + hy_1z_1}\right)(x_1 - x_3) - y_1 \qquad (2)$$

$$z_3 = \frac{z_1}{2}\left(\frac{3x_1^2 + b}{rz_1^2 + sy_1^2 + hy_1z_1}\right)(x_1 - x_3) - z_1 \qquad (3)$$

Es evidente que la duplicación no está definida cuando $rz_1^2 + hy_1z_1 + sy_1^2 = 0$. Sin embargo, debemos notar que no es tan grande el lugar geométrico de esta discontinuidad, debido al hecho de que estamos operando puntos sobre $\mathcal{S}$. Por tanto, $rz_1^2 + hy_1z_1 + sy_1^2 = x^3 + bx + c$. Entonces tenemos a lo más 3 discontinuidades. No discutimos más esto ya que esta misma ecuación es objeto del siguiente desarrollo.

Si tuviéramos que $h^2 - 4rs = 0$. Entonces $\mathcal{S}$ se reduce a

$$(\alpha x + \beta y)^2 = x^3 + bx + c$$

Algo similar a fig. 3.3. Es decir, la parte cuadrática de nuestra superficie se *degenera* a una recta. En el caso de cuando se tiene un *residuo cuadrático* se obtiene una degeneración a dos rectas. Esto puede generar casos donde $P \neq Q$ en $\mathcal{S}$ y $Q \in T_P\mathcal{S}$. Esto entorpece el desarrollo en la *ley de composición*. Pero ya lo hemos identificado por lo que podemos restringirlo, una cosa que sin embargo falta restringir es una *multiplicidad triple*. Es decir, *Bézout* nos asegura que tenemos siempre 3 puntos de intersección. Pero eso no evita que todos sean el mismo. Por tanto, procedemos a determinar cuando esto ocurre considerando el siguiente razonamiento.

Sea $\ell(t) = P + Mt$ una recta cuya intersección con $\mathcal{S}$ es no vacía. Entonces $\mathcal{S}(\ell(t)) = \mathcal{S}(t) = \mathcal{S}(P + Mt)$, este es un polinomio de grado 3. Por tanto, puede tener a lo más 3 raíces. Observamos que esto sucede cuando

$$\mathcal{S}(\ell(t)) = \mathcal{S}(P+Mt) = 0\ ,\ S'(\ell(t)) = \nabla\mathcal{S}(P+Mt)\cdot M = 0\ ,\ M^T H_{\mathcal{S}}(P+Mt)M = 0\ ,\ t = 0$$

de donde obtenemos

$$\mathcal{S}(P) = 0\ ,\ \nabla\mathcal{S}(P)\cdot M = 0\ ,\ M^T\cdot H_{\mathcal{S}}(P)M = 0$$

Notemos que aquí M actúa como una *tangente*.

Observación 3.8. Este tipo de problema ya está estudiado en *curvas elípticas* y en general no supone una dificultad en sus procedimientos.

Buscamos una *condición* que nos diga cuales puntos o parámetros evitar. No definimos el *Hessiano* $H_{\mathcal{S}}$. Ya hemos hablado antes del *gradiente*. Por lo que hacemos una digresión breve para introducir el *Hessiano*.

Definición 3.9. Sea $f : \mathbb{R}^n \to \mathbb{R}$. una *función escalar* cuyas derivadas parciales de segundo orden existen. Entonces llamamos *matriz Hessiana* a

$$H_f \begin{pmatrix} \frac{\partial^2 f}{\partial^2 x_1} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 f}{\partial^2 x_n} \end{pmatrix}$$

Entonces, dado $P_0 \in \mathcal{S}$ y v asociado con la recta tangente usada en la duplicación, es decir $v = P_0 - \left(\frac{x_0^3 - bx_0 - 2c}{3x_0^2 + b}, 0, 0\right)$, nuestro sistema es

$$rz_0^2 + hy_0z_0 + sy_0^2 = x_0^3 + bx_0 + c = 0 \tag{1}$$

$$(-3x_0^2 - b, 2sy_0 + hz_0, 2rz_0 + hy_0) \cdot \left(x_0 - \frac{x_0^3 - bx_0 - 2c}{3x_0^2 + b}, y_0, z_0\right) = 0 \tag{2}$$

$$v^T \begin{pmatrix} -3x_0 & 0 & 0 \\ 0 & 2s & h \\ 0 & h & 2r \end{pmatrix} v = 0 \tag{3}$$

Simplificando y recordando como desarrollamos expresiones explicitas para la dupli-

cación obtenemos

$$rz_0^2 + hy_0z_0 + sy_0^2 = x_0^3 + bx_0 + c = 0 \tag{1}$$

$$-2(rz_0^2 + hy_0z_0 + sy_0^2) + 2(sy_0^2 + hz_0y_0 + rz_0^2) = 0 \tag{2}$$

$$-24x_0\left(\frac{rz_0^2 + hy_0z_0 + sy_0^2}{3x_0^2 + b}\right) + 2(sy_0^2 + hy_0z_0 + rz_0^2) = 0 \tag{3}$$

Las primeras dos ecuaciones son *triviales*. De (3) obtenemos

$$-12x_0\frac{rz_0^2 + hy_0z_0 + sy_0^2}{(3x_0^2 + b)^2} + 1 = 0$$

En caso de que $3x_0^2 + b \neq 0$. Esto es lo mismo que

$$-12x_0(rz_0^2 + hy_0z_0 + sy_0^2) + (3x_0^2 + b)^2$$

Recordando que $P \in \mathcal{S}$ esto se reduce a

$$D = 3x^4 + 6x^2b + 12xc + b^2 = 0$$

Por tanto, las raíces de esta ecuación condicionan la superficie, dado que estas producen problemas con nuestra operación en secciones de la forma

$$rz^2 + hyz + sy^2 = r^3 + br + c$$

donde $D(r) = 0$. Mas aun, dado todo el desarrollo para llegar a esto, podemos deducir que también se tiene problemas cuando r es una raíz de $x^3 + bx + c$. Por tanto, tenemos que limitar nuestra operación. Es decir

$$\oplus : \mathcal{J} \times \mathcal{J} \to \mathcal{J} \quad , \quad \mathcal{J} = \mathcal{V}(\mathcal{S}) \backslash (\mathcal{V}(x^3 + bx + c) \cup \mathcal{V}(D))$$

por tanto, nuestra operación se dice *racional* (esto desde una perspectiva de la geometría algebraica).

Observación 3.10. Aun cuando tenemos esta restricción, en lo que sigue continuaremos con $\mathcal{S}$, esto dado que $\mathcal{S}$ sigue siendo la superficie que nos da propiedades para trabajar. Después se discutirá que sucede cuando nos restrinjamos a $\mathcal{J}$

Ya hemos obtenido expresiones para la suma y duplicación de puntos, estos nos servirán para realizar cálculos computacionales y algunas pruebas.

Observación 3.11. Supongamos por un momento que se buscará desarrollar un *loop* en lugar de un *quasigrupo*. Falta un *neutro* en ese caso. considerando la *homogeneización* de $\mathcal{S}$. Entonces obtenemos

$$rZ^2W + hYZW + sY^2W = X^3 + bXW^2 + cW^3$$

considerando los puntos en el *espacio proyectivo* (W = 0). Tenemos

$$X^3 = 0$$

de donde nuestros *puntos al infinito* están dados por

$$[0 : Y : Z : 0] \simeq \mathbb{P}^1$$

Por tanto, tenemos infinitos puntos en el infinito a diferencia de *curvas elípticas* donde solo se tenía uno. El problema de esto es que no parece haber ningún tipo de punto especial, elegir uno de forma arbitraria podría parecer una opción, pero luego está el problema de las intersecciones con rectas normales al eje X. Ya que, desde luego, estas pueden tener infinitas direcciones. Intentar proponer y fundamentar un neutro sale del alcance de este trabajo

Proposición 3.12. Sea $(\mathcal{S}, \oplus)$ con $\oplus$ como se definió anteriormente. Entonces este forma un *quasigrupo* conmutativo.

Demostración. Sean $P, Q \in \mathcal{S}$ no nulos

- (*bien definida*) Lo que esto quiere decir es que $P \oplus Q$ exista y sea único. La existencia está garantizada dado que por definición $P \oplus Q$ define una recta PQ la cual tiene una tercera intersección R por *Bézout* teorema 2.169. Es decir $P \oplus Q = \phi(R)$ y es única por *Bézout* (incluso si $P = Q$).

- (*conmutatividad*) Probamos primero esta propiedad dado que es bastante útil. considerando $P \oplus Q$ con $P = (x_1, y_1, z_1), Q = (x_2, y_2, z_2)$, usando las *coordenadas explicitas*, se tiene

$$x_3 = \frac{rm_3^2 + sm_2^2 + hm_2m_3}{m_1^2} - x_1 - x_2 \tag{1}$$
$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \tag{2}$$
$$z_3 = \left(\frac{z_2 - z_1}{x_2 - x_1}\right)(x_1 - x_3) - z_1 \tag{3}$$

  por otro lado $Q \oplus P$

$$x_3 = \frac{rm_3^2 + sm_2^2 + hm_2m_3}{m_1^2} - x_2 - x_1 \tag{4}$$
$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_2 - x_3) - y_2 \tag{5}$$
$$z_3 = \left(\frac{z_2 - z_1}{x_2 - x_1}\right)(x_2 - x_3) - z_2 \tag{6}$$

  trivialmente las rectas PQ y QP son las mismas por lo que dan el tercer punto de intersección R y por tanto las componentes deberían ser iguales, esto es

obvio para x_3, para las demás puede no serlo, pero igualando (2) y (5) tenemos

$$\begin{aligned}
&\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_2-x_3)-y_2\\
\Rightarrow&\left(\frac{y_2-y_1}{x_2-x_1}\right)[x_1-x_3-(x_2-x_3)]=-(y_2-y_1)\\
\Rightarrow&\left(\frac{y_2-y_1}{x_2-x_1}\right)\frac{x_2-x_1}{y_2-y_1}=1
\end{aligned}$$

por tanto, tenemos una igualdad, este proceso es análogo para z_3

- (*divisibilidad*) Dado que ya hemos probado la *conmutatividad*, solo hace falta probar, que dados P y R no nulos, existe $X \in \mathcal{S}$ tal que $P \oplus X = R$. Sin embargo, no tenemos que meternos con este problema algebraico sino solo notar que $R = \phi(Q)$ y, dado que ϕ es una involución, se tiene $\phi(R) = Q$. Por tanto, tenemos la recta PQ, por *Bézout* esta tiene una *tercera intersección única* con $\mathcal{S}$.

□

Debemos recordar que la computación de inversos en $\mathbb{Z}_p$ es costosa. Por este mismo hecho se suelen hacer operaciones sobre coordenadas proyectivas o Jacobianas en curvas elípticas. Por ello, procedemos a obtener expresiones en coordenadas proyectivas para nuestras operaciones.

Consideramos ahora el *espacio proyectivo ponderado* $\mathbb{P}(\alpha)$ con $\alpha = (2, 3, 3, 1)$. dados $P = [X_1, Y_1, Z_1, W_1]$, $W \neq 0$ y $Q = (x_2, y_2, z_2)$ pertenecientes a nuestra variedad proyectiva. Entonces P es tal que

$$[X_1 : Y_1 : Z_1 : W_1] = \{(\lambda^2 X_1, \lambda^3 Y_1, \lambda^3 Z_1, \lambda W_1)\}$$

Identificando P con su correspondiente punto en el *afín* tomando $\lambda W_1 = 1$, se tiene $\lambda = 1/W_1$. Con lo que obtenemos expresiones $P = [X_1/W_1^2 : Y_1/W_1^3 : Z_1/W_1^3 : 1]$. Q

se identifica como $Q = [X_2, Y_2, Z_2, 1]$. Sustituyendo en las ecuaciones explicitas de la suma en *coordenadas afines* tenemos.

$$X_3' = \frac{r\left(Z_2 - \frac{Z_1}{W_1^3}\right)^2 + s\left(Y_2 - \frac{Y_1}{W_1^3}\right)^2 + h\left(Y_2 - \frac{Y_1}{W_1^3}\right)\left(Z^2 - \frac{Z_1}{W_1^3}\right)}{\left(X_2 - \frac{X_1}{W_1^2}\right)^2} - \left(\frac{X_1}{W_1^2}\right) - X_2 \quad (1)$$

$$Y_3' = \left(\frac{Y_2 - \frac{Y_1}{W_1^3}}{X_2 - \frac{X_1}{W_1^2}}\right)\left(\frac{X_1}{W_1^2} - X_3\right) - \frac{Y_1}{W_1^3} \quad (2)$$

$$Z_3' = \left(\frac{Z_2 - \frac{Z_1}{W_1^3}}{X_2 - \frac{X_1}{W_1^2}}\right)\left(\frac{X_1}{W_1^2} - X_3\right) - \frac{Z_1}{W_1^3} \quad (3)$$

Simplificando obtenemos

$$X_3' = \frac{rM_3^2 + sM_2^2 + hM_2M_3}{W_1^2M_1^2} - \frac{X_1 + X_2W_1^2}{W_1^2} \quad (1)$$

$$Y_3' = \left(\frac{M_2}{W_1M_1}\right)\left(\frac{X_1}{W_1^2} - X_3'\right) - \frac{Y_1}{W_1^3} \quad (2)$$

$$Z_3' = \left(\frac{M_3}{W_1M_1}\right)\left(\frac{X_1}{W_1^2} - X_3'\right) - \frac{Z_1}{W_1^3} \quad (3)$$

donde $M_3 = (Z_2W_1^3 - Z_1), M_2 = (Y_2W_1^3 - Y_1), M_1 = (X_2W_1^2 - X_1)$. Considerando estas expresiones en *coordenadas proyectivas* podemos limpiar denominadores con $W_3 = M_1W_1$, reescribiendo tenemos $X_3 = X_3'W_3^2, Y_3 = Y_3'W_3^3, Z_3 = Z_3'W_3^3$. Finalmente obtenemos las expresiones

$$X_3 = rM_3^2 + sM_2^2 + hM_2M_3 - (X_1 + X_2W_1^2)(X_2W_1^2 - X_1)^2 \quad (1)$$

$$Y_3 = (Y_2W_1^3 - Y_1)(X_1(X_2W_1^2 - X_1)^2 - X_3) - Y_1(X_2W_1^2 - X_1)^3 \quad (2)$$

$$Z_3 = (Z_2W_1^3 - Z_1)(X_1(X_2W_1^2 - X_1)^2 - X_3) - Z_1(X_2W_1^2 - X_1)^3 \quad (3)$$

$$W_3 = (X_2W_1^2 - X_1)W_1 \quad (4)$$

Haremos un procedimiento *análogo* para la *duplicación de puntos*. Sea P como en el procedimiento anterior. Consideramos $P = [X_1/W_1^2 : Y_1/W_1^3 : Z_1/W_1^3 : 1]$.

Usando entonces las expresiones para un punto doble de coordenadas afines tenemos.

$$X_3' = \frac{\left(3\left(\frac{X_1}{W_1^2}\right)^2 + b\right)^2}{4\left(r\left(\frac{Z_1}{W_1^3}\right)^2 + s\left(\frac{Y_1}{W_1^3}\right)^2 + h\left(\frac{Y_1}{W_1^3}\right)\left(\frac{Z_1}{W_1^3}\right)\right)} - 2\left(\frac{X_1}{W_1^2}\right) \quad (1)$$

$$Y_3' = \left(\frac{Y_1}{2W_1^3}\right)\left(\frac{3\left(\frac{X_1}{W_1^2}\right)^2 + b}{r\left(\frac{Z_1}{W_1^3}\right)^2 + s\left(\frac{Y_1}{W_1^3}\right)^2 + h\left(\frac{Y_1}{W_1^3}\right)\left(\frac{Z_1}{W_1^3}\right)}\right)\left(\left(\frac{X_1}{W_1^2}\right) - X_3'\right) - \left(\frac{Y_1}{W_1^3}\right) \quad (2)$$

$$Z_3' = \left(\frac{Y_1}{2W_1^3}\right)\left(\frac{3\left(\frac{X_1}{W_1^2}\right)^2 + b}{r\left(\frac{Z_1}{W_1^3}\right)^2 + s\left(\frac{Y_1}{W_1^3}\right)^2 + h\left(\frac{Y_1}{W_1^3}\right)\left(\frac{Z_1}{W_1^3}\right)}\right)\left(\left(\frac{X_1}{W_1^2}\right) - X_3'\right) - \left(\frac{Z_1}{W_1^3}\right) \quad (3)$$

simplificando obtenemos

$$X_3' = \frac{(3X_1^2 + bW_1^4)^2}{4W^2(rZ_1^2 + SY_1^2 + hY_1Z_1)} - 2\left(\frac{X_1}{W_1^2}\right) \quad (1)$$

$$Y_3' = \left(\frac{Y_1}{2W_1}\right)\left(\frac{3X_1^2 + bW_1^4}{rZ_1^2 + SY_1^2 + hY_1Z_1}\right)\left(\left(\frac{X_1}{W_1^2}\right) - X_3'\right) - \left(\frac{Y_1}{W_1^3}\right) \quad (2)$$

$$Z_3' = \left(\frac{Y_1}{2W_1}\right)\left(\frac{3X_1^2 + bW_1^4}{rZ_1^2 + SY_1^2 + hY_1Z_1}\right)\left(\left(\frac{X_1}{W_1^2}\right) - X_3'\right) - \left(\frac{Z_1}{W_1^3}\right) \quad (3)$$

Considerando estas expresiones en *coordenadas proyectivas* podemos limpiar denominadores con $W_3 = 2(rZ_1^2 + SY_1^2 + hY_1Z_1)W_1$, reescribiendo tenemos $X_3 = X_3'W_3^2, Y_3 = Y_3'W_3^3, Z_3 = Z_3'W_3^3$. Finalmente obtenemos las expresiones

$$X_3 = (3X_1^2 + bW_1^4)^2(rZ_1^2 + SY_1^2 + hY_1Z_1) - 8X_1(rZ_1^2 + SY_1^2 + hY_1Z_1)^2 \quad (1)$$

$$Y_3 = 4Y_1(3X_1^2 + bW_1^4)(X_1(rZ_1^2 + SY_1^2 + hY_1Z_1)^2 - X_3) - 8Y_1(rZ_1^2 + SY_1^2 + hY_1Z_1)^3 \quad (2)$$

$$Z_3 = 4Z_1(3X_1^2 + bW_1^4)(X_1(rZ_1^2 + SY_1^2 + hY_1Z_1)^2 - X_3) - 8Z_1(rZ_1^2 + SY_1^2 + hY_1Z_1)^3 \quad (3)$$

$$W_3 = 2(rZ_1^2 + SY_1^2 + hY_1Z_1)W_1 \quad (4)$$

3.3 Propiedades Algebraicas

En está sección mencionamos algunas propiedades favorables de nuestra operación desde la teoría criptográfica y de *loops*.

Una cosa de relevancia cuando se suele trabajar con *curvas elípticas* es la cantidad de instancias disponibles, es decir, bajo ciertos *parámetros globales* como la *característica* del *campo* bajo el cual se trabaja, cuantas curvas tengo a disponibilidad para trabajar sin considerar aquellas con *singularidades* o que presenten una estructura particular que resulte vulnerable bajo ataques criptográficos. Esto es algo que puede suceder por ejemplo cuando se tiene una curva elíptica

$$y^2 = x^3 + bx + c$$

y $b = -3$. Esto puede parecer una trivialidad, pero en este caso se obtiene una celeridad en el cálculo [27].

Entonces procedemos a calcular la probabilidad de que al tomar parámetros aleatorios $r, h, s, b, c \in \mathbb{F}_p$. Se obtenga una estructura permitida según las condiciones que hemos hallado. Sean

$$\begin{aligned} F =& \{(b,c) \in \mathbb{F}_p^2 \mid 4b^3 + 27c^2 = 0\} \cup \\ & \left\{(r,h,s) \in \mathbb{F}_p^3 \mid h^2 - 4rs = 0 \vee \left(h^2 - 4rs = c \wedge \left(\frac{c}{p}\right) = 1\right)\right\} \end{aligned}$$

entonces la probabilidad de F no es difícil de obtener observando que este es una unión de disjuntos. Además, aproximadamente la mitad de los elementos en $\mathbb{F}_p$ (sin considerar el 0) son *residuos cuadráticos*. Esto debido a que al considerar $g \in (\mathbb{F}_p^*, \cdot)$ siendo g un generador, entonces

$$\mathbb{F}_p^* = \{[1], [g], [g^2], [g^3], [g^4], \dots\}$$

Considerando además

$$b^3 = 27c^2/4 \quad , \quad h^2 = 4rs$$

ambas fungen como ecuaciones cuadráticas que tienen a lo más 2 raíces. Si nos enfocamos en la prima ecuación c puede tomar p valores y para cada uno de estos tenemos una probabilidad $1/2$ de un *residuo cuadrático*. Entonces obtenemos $(p/2) * 2$ tuplas (b, c) que satisfacen la ecuación y hay p^2 en total, es decir, la probabilidad de obtener una solución es p/p^2. Análogamente (r, h, s) definen p^3 ternas. $h^2 = 4rs$ implica buscar pares r, s que formen un *residuo cuadrático*. Entonces tenemos $\frac{p^2}{2} \cdot 2$ soluciones. Por tanto, la probabilidad es $p^2/p^3 = 1/p$.

Observación 3.13. Esto pareciera ser casi como lanzamientos de una moneda independientes, incluso la probabilidad de que un elemento sea *residuo cuadrático*. No analizaremos esto ya que sale del contexto, pero resulta interesante.

$$P(\neg F) = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{p}\right)^2$$

Continuamos ahora con resultados algebraicos.

Proposición 3.14. Sean $P, Q \in (\mathcal{S}, \oplus)$ puntos cualesquiera. Entonces estos satisfacen

$$(Q \oplus P) \oplus Q = Q \oplus (P \oplus Q)$$

y, por tanto $(\mathcal{S}, \oplus)$ es *flexible*.

Demostración. La demostración es trivial utilizando la propiedad de *conmutatividad*.

□

Proposición 3.15. Sea $(S, \oplus)$. Entonces este tiene *potencias asociativas*.

Demostración. Sea $P \in \mathcal{S}$. Primero notemos que no tenemos problemas con definir

una potencia debido a la flexibilidad. Observemos que

$$2P = P \oplus P \ , \ 3P = P \oplus (P \oplus P) = (P \oplus P) \oplus P \ , \ \ldots$$

El problema está en la composición de potencias. Es decir, mostrar que $nP \oplus mP = (n+m)P$. Sin embargo, debido a la geometría detrás del proceso para la *duplicación de puntos*. El punto P y $2P$ viven sobre un mismo plano L donde $X \subseteq L$ siendo X el eje X. Esto es cierto al observar que para obtener $2P$ consideramos el plano tangente a P y tomamos un punto de orientación situado sobre el eje X. Por tanto, tenemos una recta de P hacia el eje X. La cual está contenida trivialmente en el plano L y asimismo $\phi(2P)$. Y observando que

$$L : z - my = 0 \Rightarrow \phi(L) : (-z) - m(-y) = 0 = z - my \Rightarrow \phi(L) = L$$

Es obvio que $P, 2P \in L$, además, tomando $P \oplus 2P = 3P$. Aun en este caso $3P \in L$ dado que la recta de P a $2P$ está contenida en L dado que P y $2P$ lo están, esto mismo sucede para $\phi(3P)$ y el procedimiento para ver que $3P \in L$ es análogo al proceso de ver que $2P \in L$. Entonces $nP \in L \, , \, \forall n \in \mathbb{N}$. Y debido a que la intersección del plano L con $\mathcal{S}$ forma una *curva elíptica* (3.7). La orbita entera de P está sobre una curva elíptica, más aun, la órbita forma un *subgrupo* con una *ley de grupo* dada por la sustitución de $z = my$ en las ecuaciones de suma (1) y duplicación (1). Por tanto, la asociatividad se obtiene sobre la órbita de P. □

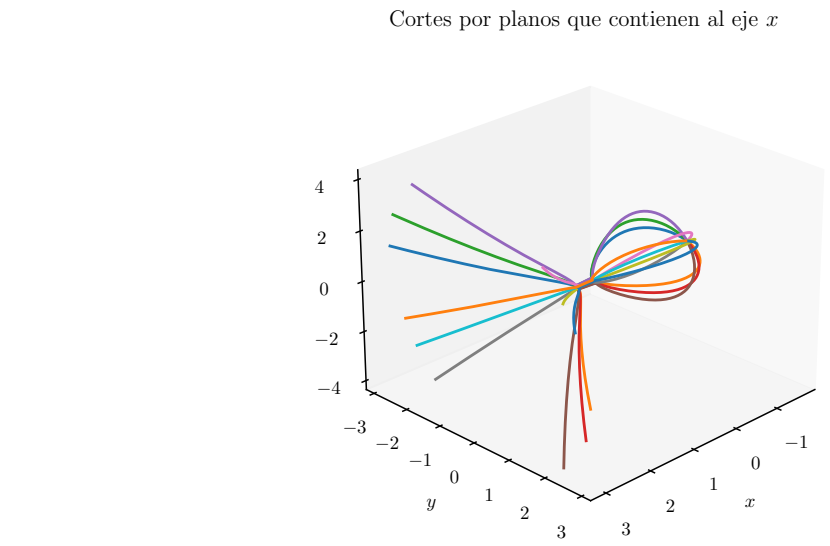


Figura 3.4: Familia de orbitas

Observación 3.16. Si se tiene duda respecto al argumento del plano y su intersección con la *superficie* solo notemos que L debe estar definido por $L : z - my = 0$. Sustituyendo esto en $\mathcal{S}$ obtenemos.

$$rm^2y^2 + hmy^2 + sy^2 = x^3 + bx + c \Rightarrow (rm^2 + hm + s)y^2 = x^3 + bx + c \qquad (3.7)$$

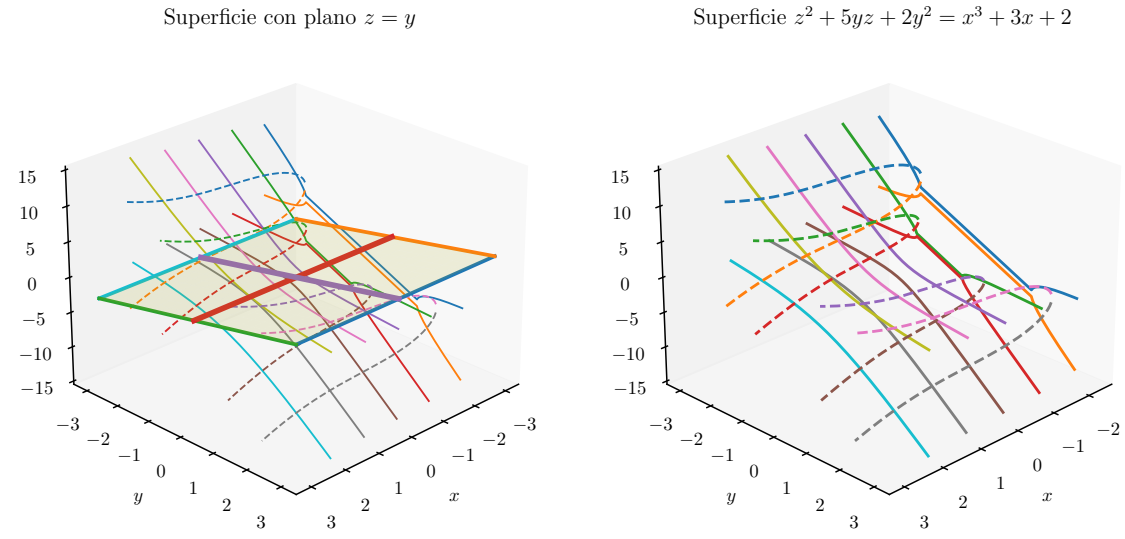


Figura 3.5: Grafica con y sin $X \subseteq L$

Teorema 3.17. Sea $(\mathcal{S}, \oplus)$. Entonces se tiene la *propiedad del inverso*.

Demostración. Sean $P, Q \in \mathcal{S}$. Por definición $P \oplus Q = R$. Notemos entonces que podemos considerar la recta definida por $R\phi(Q)$ y por *Bézout*. Tenemos $R\phi(Q) \cap \mathcal{S} = \{R, \phi(Q), T\}$. Por definición, debemos tener que $R \oplus T = \phi(\phi(Q)) = Q$. Es decir

$$T \oplus (P \oplus Q) = T \oplus R = Q$$

Esto sería perfecto sin embargo T no debe depender de R, esto debido a que R depende a su vez de Q y T debe ser independiente de Q. Es decir, Q debe ser cualquiera y T seguir funcionando para la propiedad del inverso. Entonces probamos que la recta $R\phi(Q)$ es la misma que pasa por $\phi(P)\phi(Q)$. Notemos entonces que

$$PQ = \{P + (Q - P)t \mid t \in \mathbb{Q}\} \Rightarrow \phi(PQ) = \{\phi(P + (Q - P)t) \mid t \in \mathbb{Q}\}$$

observando que

$$\{\phi(P+(Q-P)t) \mid t \in \mathbb{Q}\} = \{(x_1+(x_2-x_1)t, -y_1+(-y_2+y_1)t, -z_1+(-z_2+z_1)t)\}$$

esto es lo mismo que $\phi(P)\phi(Q)$. Dado que $\phi(R) \in PQ$, entonces $\phi(\phi(R)) \in \phi(P)\phi(Q)$. Es decir, $R \in \phi(P), \phi(Q)$. De donde $\phi(P)\phi(Q) \cap \mathcal{S}\{\phi(P), \phi(Q), R\}$, y recordando que por hipótesis $R\phi(Q) \cap \mathcal{S} = \{R, \phi(Q), T\}$. Por *Bézout* tenemos que $T = \phi(P)$. El cual es un punto independiente al operar con Q. Por tanto, tenemos una biyeccion

$$J : \mathcal{S} \to \mathcal{S}$$

$$P \mapsto \phi(P)$$

que satisface

$$J(P) \oplus (P \oplus Q) = \phi(P) \oplus (P \oplus Q) = Q \ , \ \forall Q \in \mathcal{S}$$

□

Observación 3.18. Por el procedimiento realizado en la prueba anterior seria incluso posible demostrar que $(\mathcal{S}, \oplus)$ tiene *inversos automórficos*. Es decir, dados $P, Q \in \mathcal{S}$

$$\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$$

De todos estos procedimientos podemos enunciar el *resultado principal*.

Teorema 3.19. Sea $\mathcal{S}$ nuestra superficie (3.1). Entonces $\oplus$ induce una estructura de *quasigrupo conmutativo* en la que cada orbita de $P \in \mathcal{S}$ genera un *subgrupo* de una *curva elíptica* con una *ley de grupo*.

Demostración. No se hará uso de una demostración formal dado que este resultado es producto directo de los resultados anteriormente enunciados. Los argumentos por revisar son teorema 3.12, teorema 3.15. □

Observación 3.20. El anterior resultado básicamente nos dice que nuestra superficie se asemeja a una familia de *curvas elípticas*.

CAPÍTULO 4

CONCLUSION

Ya hemos obtenido algunos resultados de una construcción que *generaliza* o *extiende* de cierta forma los procedimientos de *curvas elípticas*. Lo que haremos ahora es discutir las acepciones que pueden tomar estos resultados y, lo que podemos concluir acerca del trabajo realizado así como futuros trabajos.

4.1 Discusión

Comenzamos hablando de la *curva elíptica* que elegimos como base.

$$y^2 = x^3 + bx + c$$

Dado que la idea desarrollada para este trabajo era nueva desde nuestra perspectiva, decidimos empezar con una curva ciertamente *restringida*, por tanto, con una *operación* y *estructura* ideal para una primera exploración. Es decir, este trabajo aún no se ha tratado de extender a otras *curvas elípticas* conocidas. Por lo que realizar estos procedimientos con otras curvas puede ser interesante por las distintas propiedades se tienen y como pueden interactuar con estructuras no asociativas.

Pasar de curva a superficie requirió tiempo debido a las distintas particularidades que se tienen en superficies cubicas. Uno de ellos el *teorema de Cayley Salmon*, este establece que en toda *superficie cubica suave* se tienen exactamente 27 rectas proyectivas. Es decir, nuestra superficie podía contener en su estructura

rectas. Al principio no sabíamos cómo lidiar con esto, pero luego de observar que la complejidad de verificar si un punto pertenece a alguna de estas es *constante* no hubo mucho problema, también algunas de las condiciones que establecimos restringen la existencia de ciertas rectas. Al definir una instancia se podía hacer una verificación que al operar puntos, la recta que definen estuviera en la curva. Esto tampoco es complicado observando que al sustituir un valor aleatorio en la recta parametrizada, sí este está en la superficie entonces debe estarlo la recta también. Esto debido a que *Bézout* asegura 3 intersecciones. Obtener más implicaría una contención. Con esto claro podría parecer que el proceso es largo, pero a lo mucho hay 27 rectas por lo que el proceso de identificarlas es finito. También, no necesariamente se encuentran las 27 en toda superficie. Dado que trabajamos sobre $\mathbb{Q}$, sabemos por Ludwig Schläfli que podrían haber solo $15, 7, 3$ o quizá ninguna y que todas se encuentren en el *espacio proyectivo* (este resultado esta enunciado actualmente sobre $\mathbb{R}$). Si se quiere optimizar este proceso, es necesario profundizar en la *clasificación constructiva de superficies cúbicas* sobre $\mathbb{F}_q$, la cual actualmente es objeto de estudio, como se muestra en [41].

Hablando ahora sobre *suavidad*. El hecho de que el *discriminante* obtenido para $\mathcal{S}$ fuera el mismo que se tiene en curvas elípticas podría hacer parecer que no tenemos nada distinto, pero hay que considerar las otras restricciones que obtuvimos y el hecho de que la estructura definida globalmente es no asociativa a diferencia de *curvas elípticas*. Observando que esta estructura se asemeja a una familia de *curvas elípticas*, que las *restricciones* coincidan implica que este discriminante es global (recuerde teorema 3.15). Por tanto no tenemos que preocuparnos por la suavidad de las curvas elípticas que contienen nuestras orbitas.

Considerar una *involución* no fue un detalle trivial o solamente algo inspirado por *curvas elípticas* sino que es algo *crucial* para definir la *operación*. Esto es obvio debido a su constante uso en los procedimientos realizados y es que si no se tuviera la propiedad *característica* de una *involución* es decir, $\phi^2 = i$ (donde i es el mapeo

identidad), asegurar muchas de las propiedades algebraicas que actualmente se tienen sería imposible (bajo nuestros supuestos actuales). Uno puede pensar que al pasar de curva a superficie aparecerían más *simetrías*. Y esto es cierto, pero tenemos una restricción importante y es que el eje X sea *invariante* ante estas. Esto debido a la *expresión* en términos de x en la ecuación (3.1), tal resulta gozar de poca simetría. Afortunadamente al buscar alguna *rotación* respecto al eje X. Hallamos que solo existe una y que de hecho viene a ser una *extensión* de la *simetría* usada en *curvas elípticas*. Se busco otras alternativas y se halló una *simetría* sin embargo, esta dependía totalmente de los residuos cuadráticos y de los *parámetros* seleccionados para la *superficie*. Debido a los pocos casos donde era utilizable se descartó. Aunque esta se podría usar perfectamente sobre campos de *característica* 2. Por lo que puede ser una *opción* para estos procedimientos realizados usando una *curva elíptica* que permita $car(K) = 2$. Los resultados en este caso son inciertos e interesantes debido a que tal *simetría* es una *inversión* y a su vez una *involución*.

La suavidad ya estaba asegurada por *Jacobi* sin embargo, cosas como una *tangencia múltiple* pueden suceder y que como consecuencia, no se tengan operaciones bien definidas para ciertos elementos. Esto fue algo que notamos cuando comprendimos que *Bézout* solo nos asegura 3 puntos, pero no necesariamente distintos. Es decir, en *curvas elípticas* uno tiene que $P \oplus P = P$ implica que $P = \mathcal{O}$. Esto es una consecuencia de la *asociatividad* y más que eso, de la geometría. Entonces en la ausencia de un *neutro* global. Tuvimos que restringir esto utilizando el *Hessiano*. Así identificamos bajo qué condiciones tenemos *idempotencia* para ciertos puntos. Hay un problema sobre esto, para entenderlo mejor entendamos que nuestra *superficie* no solo se puede ver como una *familia* de *curvas elípticas* sino también como una de *cónicas*, tomando *intersecciones* de planos normales al eje X. Por tanto, para cada x se tiene una *cónica*. Trabajando con el *Hessiano* hallamos (3.2) (3.2) que hay a lo mucho 7 valores de x para los cuales tenemos *familias de cónicas* con *idempotencia* en la

operación. Esto no supone un gran problema dado que podemos evitarlo simplemente restringiendo el *dominio de la operación* o los *parámetros que adopta la parte cubica* en la ecuación de nuestra *superficie*. Esto último para reducir la cantidad de raíces en las ecuaciones antes mencionadas. El *que se debería de restringir* aún es algo por investigarse dado que aún no se conoce bien en que puede afectar el no tener *raíces* y su costo computacional. Asimismo, tampoco si la *restricción* del dominio pueda afectar a las *orbitas*. Respecto a lo que controla $h^2 - 4rs \neq 0$, esta asegura que las *familias de cónicas* no se degeneran, la ausencia de *puntos dobles* y rectas. Con esto nos referimos a un caso donde $P \neq Q$ y sin embargo $Q \in T_P\mathcal{S}$. Puntos dobles quiere decir, el caso cuando P y Q están lo suficientemente cerca para que uno este contenido en el plano tangente del otro. Esto generalmente sucede cuando se tienen *direcciones diferenciadas*. Como en el caso $h^2 - 4rs = 0$, dado que entonces se tiene que $rz^2 + hyz + sy^2$ se reduce a $(\alpha z + \beta y)^2 = 0$. Asimismo, cuando se tiene no 0 sino un *residuo cuadrático*. Tenemos una degeneración a un par de rectas.

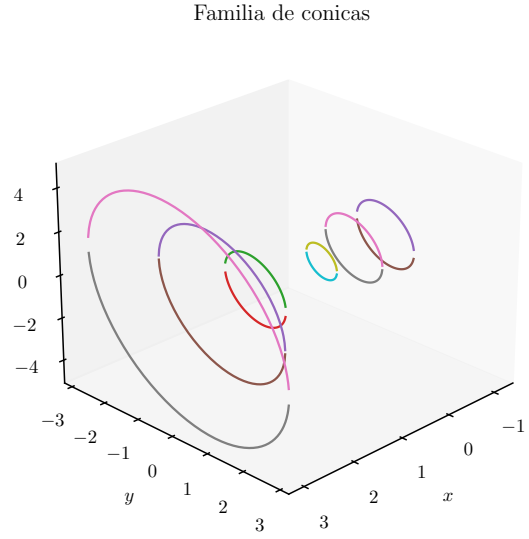


Figura 4.1: Familia de cónicas no degeneradas

El tema del *infinito* como neutro aún está en discusión dado que *geométricamente* y en *curvas elípticas* este satisface una propiedad global. Sin embargo, en

quasigrupos aún si no se exige un *neutro*. Puede existir uno *localmente*. Y eso es algo que de hecho sucede con cada *orbita* de un punto $P \in \mathcal{S}$. En cualquier caso si se desea hacer de este algo *global*, se tendría que hacer una diferenciación de algún punto en la *recta proyectiva* lo cual no es trivial. Por tanto, decidimos restringir nuestra estructura a un *quasigrupo*. Si se hallara alguna propuesta seria malo. Esto puede parecer contra intuitivo, pero considerando que tenemos una estructura no asociativa la cual aún no está del todo adaptada a ataques criptográficos tradicionales y cuánticos. El estar cerca de un grupo al obtener *neutro* puede debilitar la estructura. Esto ya es un tema profundamente relacionado con la *teoría de loops* que entra en conceptos de *homotopía* e *isotopía*. Tal teoría nos dice que tener un *loop* nos acerca más a un *grupo* e incluso por *isotopía* podríamos tener un *grupo*. Aunque actualmente se podría hallar un loop isotopico al quasigrupo definido. No mencionamos mucho estos conceptos dado que el estudio de tales posibilidades puede considerarse un trabajo más profundo sobre la estructura presentada. Se puede hallar más sobre esto en [11] y [42].

Una cosa que se puede observar es que definimos las operaciones también en el *espacio proyectivo* y además con *coordenadas mixtas*. El primer hecho fue debido a que se deseaban realizar algunos cálculos de interés como el *grado de asociatividad*, es decir, cual es la probabilidad de que al tomar puntos aleatorios, estos satisfagan *asociatividad*. Para entender que tan pesado es esto. Una *estimación trivial* sobre la cardinalidad de $|\mathcal{S}(\mathbb{F}_p)|$ fue de $2p^2$ elementos. Por tanto, para un primo como $p = 7$ se tienen aproximadamente 98 puntos, realmente no son muchos. pero la propiedad de asociatividad usualmente usa 3 puntos distintos. Por lo que se tienen $98 * 97 * 96$ ternas que equivalen a $912,576$ comprobaciones. Esto solo para un numero *primo* de un solo dígito. Evidentemente la capacidad de cálculo no fue suficiente para primos que considerábamos relevantes (de al menos tres dígitos) por lo que se trató de optimizar las operaciones pasando al *espacio proyectivo*. Esto debido a que generalmente se tiene una reducción de *inversiones* que a veces suelen ser hasta 8 veces más pesadas

que un *producto*. Aun con esto no se logró el cometido tras largas horas de cálculo en las cuales se terminó por desistir. El tema de la optimización mediante *concurrencia*, *heurísticas* o *paralelizar operaciones* es algo que investigar para obtener resultados acerca de estas estructuras. Respecto al segundo punto que se mencionaba al principio de esta discusión, es bueno definir la operación en *coordenadas mixtas* para poder operar en diferentes sistemas de coordenados.

Las propiedades que se probaron fueron principalmente seleccionadas por un enfoque al uso *criptográfico*. Esto es evidente ya que si se quisiera considerar algún *problema análogo* al del *logaritmo* discreto. Se necesitan *potencias asociativas*. Claro que podría considerarse tal problema como similar e incluso equivalente al de *curvas elípticas* debido a que nuestras *orbitas* forman *subgrupos* de tales estructuras. Pero hay que considerar una cosa y es que la dinámica es distinta dado que se puede cambiar de una órbita a otra y lo que se tiene es una *curva elíptica* distinta. Si se insistiera con descartar esta idea y se mencionara entonces la similitud con una *familia indexada de curvas elípticas* no hay ningún problema dado que a diferencia de ello, nosotros tenemos una operación no asociativa sobre una familia que, también es *continua* en cierto aspecto. Algo que no necesariamente sucede con una *familia indexada*. Por tanto, es posible idear un problema de *logaritmo discreto* que a su vez utilice la dinámica no asociativa de nuestra operación. Pero de hecho esto puede investigarse, más en concreto, el problema de la interacción entre *orbita* y *operación*. Hay entonces varios planteamientos sobre cómo se puede relacionar $P \oplus Q$ y $\langle P \rangle, \langle Q \rangle$. Sera que

$$(P \oplus Q) \oplus Q \stackrel{?}{=} P \oplus 2Q$$

Tener la *propiedad del inverso* también nos permite resolver ecuaciones con una *solución explicita*. Esto debido a que usualmente sin la propiedad del inverso ecuaciones

como $P \oplus X = R$ tienen una solución que se debe buscar. Con esta propiedad tenemos

$$J(P) \oplus (P \oplus X) = J(P) \oplus R \Rightarrow X = \phi(P) \oplus R$$

Esto nos permite seguir tomando supuestos que usan un inverso para *problemas difíciles* o usualmente para *descifrados*.

Por ultimo, trabajar sobre $\mathcal{J}$ o $\mathcal{S}$ no es muy diferente bajo ciertos parámetros para $\mathcal{S}$. Sabemos cuando la operación no esta definida, lo que la hace parcial. Y las operaciones por componente son funciones racionales lo que hace a la operación completa racional. El único problema respecto a esto que aun se tiene que solucionar es la cerradura bajo el abierto $\mathcal{J}$. Más esto no supone un obstáculo para futuros procedimientos porque como expreso antes, sabemos cuando no operar.

4.2 Conclusión

La asociación de conocimientos y las distintas ideas y discusiones que se llegaron a tener nos llevaron a esta estructura que podemos llamar, *quasigrupo racional definido parcialmente, con comportamiento elíptico local*. Es decir, tenemos una *estructura no asociativa* en donde cada *orbita* se comporta como un *subgrupo de una curva elíptica*. Además tenemos condiciones que aseguran

$$4b^3 + 27c^2 \qquad \textit{Suavidad}$$

$$h^2 - 4rs \neq 0\,, x\,, \left(\frac{x}{p}\right) = 1 \quad \textit{Operación regular}$$

$$D \neq 0\,,\ x^3 + bx + c \neq 0 \quad \textit{Geometría regular}$$

Por tanto, de cierta forma tenemos la *extensión* de una *curva elíptica* que era nuestro objetivo inicial. Mas aun, con las propiedades que se hallaron es posible extender

algunas de las *primitivas criptográficas* utilizadas en *curvas elípticas* a esta estructura, analizar complejidad contra eficiencia. Aún hay mucho trabajo posible por hacer. La teoría de las estructuras no asociativas en criptografía se encuentra en una edad temprana y creemos que esta propuesta será de utilidad como referencia.

4.3 Trabajos Futuros

Lo que hicimos tenía como finalidad proponer y fundamentar una estructura alternativa y se cumplió el cometido. Como ya vimos en los *Preliminares*, esto es solo la base para comenzar a hacer criptografía por lo que todavía queda mucho trabajo como

- Hallar *problemas difíciles* únicos sobre esta estructura.
- Analizar la adaptabilidad de *problemas dificiles* ya conocidos en *teoría de grupos y quasigrupos* en la estructura propuesta.
- Clasificar esta estructura por isotopía u isomorfía, el primero por un sentido algebraico y el segundo geométrico. Incluso hallar alguna forma de clasificación particular.
- Extender este procedimiento a curvas elípticas de característica 2. Mas en concreto, sobre $\mathbb{F}_q$ siendo $q = 2^n$
- Buscar propiedades de interés en *teoría de quasigrupos*. Esto debido a que la falta de asociatividad hace que muchas cosas *naturales*, sean propiedades con distintos usos, como *criptográficos* y *criptoanalíticos*.
- Obtener una mejor estimación para la cardinalidad de $\mathcal{S}$, quizá utilizando la familia de cónicas asociada y analizando la cardinalidad de sus elementos.
- Analizar las *parastrofes* de la estructura. Esto con un sentido más algebraico

debido a que tales conceptos rompen con la geometría, pero su análisis puede traer propiedades interesantes y quizá de utilidad.

BIBLIOGRAFÍA

[1] Richard Bruck. *A Survey of Binary Systems*. Vol. 20. Ergebnisse der Mathematik und ihrer Grenzgebiete. Berlin: Springer, 1958.

[2] Reinhold Baer. *LINEAR ALGEBRA AND PROJECTIVE GEOMETRY*. Pure and applied mathematics. Second printing. New York: Academic Press Inc., 1966.

[3] Saunders Mac Lane y Garrett Birkhoff. *Algebra*. Third printing. New York: Macmillan, 1968.

[4] Yu Manin. *Cubic Forms : Algebra, Geometry, Arithmetic*. Vol. 4. North-Holland Mathematical Library. Amsterdam: North-Holland Publishing Company, 1974. ISBN: 0-7204-2450-X.

[5] Diffie Whitfield y Martin E. Hellman. «New Directions in Cryptography». En: *IEEE TRANSACTIONS ON INFORMATION THEORY* 22.6 (1976). URL: https://ee.stanford.edu/~hellman/publications/24.pdf.

[6] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. New York: Springer-Verlag, 1977. ISBN: 978-0-387-90244-9.

[7] H. W. Lenstra Jr. «Factoring Integers with Elliptic Curves». En: *Annals of Mathematics* 126.3 (1987), págs. 649-673. URL: http://www.jstor.org/stable/1971363?origin=JSTOR-pdf.

[8] Neal Koblitz. «Elliptic Curve Cryptosystems». En: *MATHEMATICS OF COMPUTATION* 48.177 (1987), págs. 203-209. URL: https://ec.kparc.io/ref/Koblitz1987_EllipticCurveCryptosystems.pdf.

[9] Peter Shor. «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer». En: *SIAM Journal on Computing* 26.5 (1987). ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

[10] Miles Reid. *Undergraduate Algebraic Geometry*. Vol. 12. LMS Student Texts. Also available as lecture notes (2007 TeX edition). Cambridge University Press, 1988.

[11] Hala Pflugfelder. *Quasigroups and Loops: Introduction*. Vol. 7. Sigma Series in Pure Mathematics. Berlin: Heldermann Verlag, 1990.

[12] Joe Jarris. *Algebraic Geometry: A First Course*. Vol. 133. Graduate Texts in Mathematics. Newy York: Springer-Verlag, 1992. ISBN: 978-1-4419-3099-6.

[13] Neal Koblitz. *A Course in Number Theory and Cryptography*. Vol. 114. Graduate Texts in Mathematics. Second printing. Springer-Verlag, 1994. ISBN: 978-1-4612-6442-2. DOI: 10.1007/978-1-4419-8592-7.

[14] Miles Reid. *Undergraduate Commutative Algebra*. Vol. 29. London Mathematical Society Student Text. Cambridge University Press, 1995. ISBN: 0-521-45255-4.

[15] Joseph Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Fourth printing. Springer-Verlag, 1995. ISBN: 0-387-94285-8.

[16] Alfred Menezes, Paul van Oorschot y Scott A. Vanstone. *Handbook of Applied Cryptography*. First printing. CRC Press, 1996. ISBN: 9780849385230.

[17] Czelaw Koscienly y Gary L. Mullen. «A Quasigroup-Based Public-Key Cryptosystem». En: *International Journal of Applied Mathematics and Computer Science* 9.4 (1999), págs. 955-963. URL: https://uz.zgora.pl.

[18] Neal Koblitz, Alfred Menezes y Scott Vanstone. «The State of Elliptic Curve Cryptography». En: *Designs, Codes and Cryptography* 19 (2000). DOI: https://doi.org/10.1023/A:1008354106356.

[19] Vladimir Shcherbacov. *Quasigroups based crypto-algorithms*. Inf. téc. Chisinau, Moldova: Academy of Sciences of Moldova, 2003.

[20] Darrel Hankerson, Alfred Menezes y Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004. ISBN: 0-387-95273-X.

[21] Steve Roman. *Field Theory*. Vol. 158. Graduate Texts in Mathematics. Second printing. Springer New York, 2006. ISBN: 978-1-4419-2095-9. DOI: https://doi.org/10.1007/0-387-27678-5.

[22] Jonathan Smith. *An Introduction to Quasigroups and Their Representations*. CRC Press, 2006. ISBN: 9780429137983. DOI: 10.1201/9781420010633.

[23] Felipe Zaldivar. *Introducción a la Teoría de Grupos*. Vol. 30. Aportaciones Matemáticas : Textos. Reverte, 2007. ISBN: 9686708669.

[24] Alexei Myasnikov, Vladimir Shpilrain y Alexander Ushakov. *Group-based Cryptography*. Advanced Courses in Mathematics CRM Barcelona. Basel: Birkhäuser-Verlag, 2008. ISBN: 978-3-7643-8826-3.

[25] Harald Niederreiter y Chaoping Xing. *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, 2009. ISBN: 9781400831302. URL: https://books.google.com.mx/books?id=utDJWUVogZ4C.

[26] Vladimir Shcherbacov. «Quasigroups in cryptology». En: *Computer Science Journal of Moldova* 17.2 (2009).

[27] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[28] Jean-Charles Faugere y Pierre-Jean Spaenlehauer. «Algebraic Cryptanalysis of the PKC'2009 Algebraic Surface Cryptosystem». En: *Public Key Cryptography - PKC 2010*. Springer Berlin Heidelberg, 2010, págs. 35-52. ISBN: 978-3-642-13013-7.

[29] Aleksandra Mileva. «Cryptographic Primitives with Quasigroup Transformations». En: *Mathematica Balkanica* 24 (2010).

[30] Felipe Zaldívar. *Introducción a la teoría de Galois*. Mexico: Alfaomega, 2010.

[31] A.A. Bruen, J.W.P Hirschfeld y D.L. Wehlau. «Cubic Curves, Finite Geometry and Cryptography». En: *Acta Applicandae Mathematicae* 115 (2011), págs. 265-278. DOI: https://doi.org/10.1007/s10440-011-9620-z.

[32] Ann Hibner Koblitz, Neal Koblitz y Alfred Menezes. «Elliptic curve cryptography: The serpentine course of a paradigm shift». En: *Journal of Number Theory* 131.5 (2011). Elliptic Curve Cryptography, págs. 781-814. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2009.01.006. URL: https://www.sciencedirect.com/science/article/pii/S0022314X09000481.

[33] Vladimir Shcherbacov. «Quasigroups based crypto-algorithms». En: (2012). arXiv: 1201.3016 [math.GR]. URL: https://arxiv.org/abs/1201.3016.

[34] Dima Grigoriev y Vladimir Shpilrain. «Tropical Cryptography». En: *Communications in Algebra* 42.6 (2014), págs. 2624-2632. DOI: 10.1080/00927872.2013.766827.

[35] Jeffrey Hoffstein, Jill Pipher y Joseph Silverman. *An Introduction to Mathematical Cryptography*. Undergraduate Texts in Mathematics. Second printing. Springer Science+Business, 2014. ISBN: 978-1-4939-1710-5. DOI: 10.1007/978-1-4939-1711-2.

[36] Smile Markovskim. «Design of crypto primitives based on quasigroups». En: *Quasigroups and Related Systems* 23.1 (2015), págs. 41-90.

[37] Alberto Sonnino y Giorgio Sonnino. «Elliptic-Curves Cryptography on High-Dimensional Surfaces». En: (2016). arXiv: 1610.01518 [cs.CR]. URL: https://arxiv.org/abs/1610.01518.

[38] Fanggui Wang y Hwankoo Kim. *Foundations of Commutative Rings and Their Modules*. Vol. 22. Algebra and Applications. Springer Nature, 2016. ISBN: 978-981-10-3336-0. DOI: 10.1007/978-981-10-3337-7.

[39] Timothy Hosgood. «An introduction to varieties in weighted projective space». En: (2017). eprint: arXiv:1708.05956.

[40] Douglas Stinson y Maura Paterson. *Cryptography : Theory and practice*. second printing. CRC Press, 2018. ISBN: 9781138197015. DOI: 10.1201/9781315282497.

[41] Anton Betten y Fatma Karaoglu. «Cubic Surfaces over small finite fields». En: *Designs, Codes and Cryptography* 87 (2019), págs. 931-953. DOI: https://doi.org/10.1007/s10623-018-0590-2.

[42] George Olufemi, Adeniran Olusola y Jhonson Olaleru. «LWPC Quasigroups». En: *International Journal of Mathematics and Computer Science* 14.3 (2019), págs. 591-599.

[43] Emily Clader y Dustin Ross. *Beginning in Algebraic Geometry*. Undergraduate Texts in Mathematics. Open Acces. Springer, 2020. DOI: https://doi.org/10.1007/978-3-031-88819-9.

[44] Mariya Bessonov, Dima Grigoriev y Vladimir Shpilrain. «A framework for unconditionally secure public-key encryption (with possible decryption errors)». En: *International Journal of Computer Mathematics: Computer Systems Theory* 6.4 (2021), págs. 285-290. DOI: 10.1080/23799927.2020.1853238.

[45] Felipe Cano et al. *Curso breve de geometría proyectiva*. Colección Papirhos. Textos 11. Primera edición. Ciudad de Mexico: Universidad Nacional Autónoma de Mexico, 2021. ISBN: 978-607-30-3686-3.

[46] Felipe Zaldivar. *Introducción a la teoría de números*. Primera Edición. Fondo de Cultura Económica, 2022. ISBN: 978-6071684110.

[47] Delaram Kahrobaei, Ramón Flores y Marialaura Noce. «Group-based Cryptography in the Quantum Era». En: *NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY* 70.5 (2023). DOI: https://doi.org/10.1090/noti2684.

[48] D. Kanevsky. *An example of a non-associative Moufang loop of point classes on a cubic surface*. arXiv:2104.05118. 2023. arXiv: 2104.05118 [math.NT].

[49] Dinesh Khattar y Neha Agrawal. *Group Theory*. Springer Cham, 2023. ISBN: 978-3-031-21309-0. DOI: https://doi.org/10.1007/978-3-031-21307-6.

[50] Delaram Kahrobaei et al. *Applications of Group Theory in Cryptography : Post-quantum Group-based Cryptography*. Vol. 278. Mathematical Surveys and Monographs. Providence, Rhode Island: American Mathematical Society, 2024. ISBN: 9781470474690.

[51] Stephan Rosebrock. *Visual Group Theory*. Undergraduate Mathematics Series. 2024. ISBN: 978-3-662-69364-3. DOI: https://doi.org/10.1007/978-3-662-69365-0.

[52] Peter Shiu. *Number Theory with Computations*. Springer Undergraduate Mathematics. First printing. Springer Charm, 2024. ISBN: 978-3-031-63813-8.

[53] Albrecht Beutelspacher, Jörg Schwenk y Klaus-Dieter Wolfenstetter. *Modern Cryptography*. Mathematics Study Resources. First printing. Springer Berlin, Heidelberg, 2026. ISBN: 978-3-662-67442-0.

RESUMEN

Abraham Alejandro Puente Rodríguez

Fecha de Obtención del Grado: Agosto, 2026

Institución: UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

Facultad de adscripción: Facultad de Ciencias Físico Matemáticas

Localización: San Nicolás de los Garza, Nuevo León, México

Título del Estudio: GENERALIZACIÓN DEL GRUPO DE PUNTOS EN UNA CURVA ELÍPTICA CON BASE EN QUASIGRUPOS PARA CRIPTOGRAFÍA

Número de Páginas: 112

Candidato para el Grado de Maestría en Ciencias con Orientación en Matemáticas

Área de Estudio: Matemáticas

Propósito y Método del Estudio:

Generalizar la estructura de *grupo* definida sobre una curva elíptica, esto con el fin de plantear una estructura base alternativa para criptografía, por medio de una rotación generalizada a una curva elíptica reducida. Después se tuvo que fundamentar la superficie y su estructura operacional, utilizando herramientas de la geometría algebraica y teoría de quasigrupos. Pero dado que esto desea aplicarse a criptografía se eligieron probar propiedades algebraicas especificas, con el fin de determinar si funciona como estructura base para su aplicación en primitivas criptográficas.

Contribuciones y Conclusiones:

Se obtuvo un *quasigrupo racional conmutativo* definido parcialmente con propiedades ideales para su aplicación en criptografía como *potencias asociativas*, *propiedad del inverso* y *flexibilidad*. Asimismo expresiones en *coordenadas proyectivas* para la operación de elementos, dado que gozan de una menor complejidad computacional en comparación con *coordenadas afines*. Es por tanto que esta es una alternativa con la suficiente estructura para trabajar.

Firma del Asesor

Dr. Pablo Cesar Rodríguez Ramírez

RESUMEN AUTOBIOGRÁFICO

Abraham Alejandro Puente Rodríguez

Candidato para el Grado de

Maestría en Ciencias con Orientación en Matemáticas

Título de la tesis: GENERALIZACIÓN DEL GRUPO DE PUNTOS EN UNA CURVA ELÍPTICA CON BASE EN QUASIGRUPOS PARA CRIPTOGRAFÍA

Campo o rama profesional: Matemáticas Aplicadas.

Biografía: Nacido en Nuevo León, el 24 de Julio del 2000. Hijo de Ana María Puente Rodríguez y Juan Antonio Santos Piña.

Educación: Licenciado en Matemáticas por la UANL.

Experiencia profesional: Asistente en las escuelas *Escuela de Álgebra y Geometría Algebraica 2023*, *Métodos Algebraicos para Resolver Ecuaciones Diferenciales 2025* respectivamente en el Centro de Investigación en Matemáticas unidad Guanajuato. Asistente en la *Escuela de Verano en Modelación y Herramientas para el Análisis de Datos 2023* llevada a cabo en la UANL. Auxiliar en organización para la *Escuela de Verano en Modelación y Herramientas para el Análisis de Datos 2025* asimismo en la UANL. Auxiliar en el *51 Congreso Nacional de la Sociedad Matemática Mexicana* en el 2018, edición celebrada en el estado de Nuevo León.