Pontificia Universidad Católica del Perú

Escuela de Posgrado

Semigrupos numéricos y una descripción de semigrupos de Weierstrass

Tesis para Optar el Grado de

Magíster en Matemática

Orlando Alfredo Galarza Gerónimo

Asesor

Dr. Percy Braulio Fernández Sánchez

Jurado

Dr. Christian Holger Valqui Haase

Dr. Percy Braulio Fernández Sánchez

Dra. Nancy Edith Saravia Molina

Lima - Perú

Diciembre - 2018

SEMIGRUPOS NUMÉRICOS Y UNA DESCRIPCION DE SEMIGRUPOS DE WEIERSTRASS

Orlando Alfredo Galarza Gerónimo [1]

Tesis presentada a consideración del Cuerpo Docente de la Escuela de Posgrado, de la PUCP, como parte de los requisitos para obtener el grado académico de Magister en Matemática

Miembros de Jurado:

Dr. Percy Braulio Fernández Sánchez (Asesor)

Dr Christian Holger Valqui Haase (Presidente)

Dr. Nancy Edith Saravia Molina (Miembro)

Lima - Perú

Febrero - 2019

[1] La tesis forma parte del Proyecto DGI 2018-1-0059

A mi esposa Pilar y mi hijo Rodrigo, que son mi motor, ...mi vida.

... A mis padres Victor y Filomena, que con su esfuerzo, me enseñaron que no hay que rendirse.

RESUMEN

En este trabajo, se estudia fundamentalmente diversas relaciones aritméticas que hay en los semigrupos numéricos, como por ejemplo, obtener el conjunto de lagunas, teniendo solamente el conjunto Apery; también, dado un conjunto de elementos generadores, se asociará a cada uno de ellos, un propio semigrupo numérico.

Se finaliza, haciendo una descripción de diversos conceptos de la Geometría Algebraica, los cuales se relacionan con los semigrupos numéricos, mediante los semigrupos de Weierstrass, que tienen fundamento, en el teorema de Riemann - Roch.

ABSTRACT

In the present work, we mainly study different arithmetic relationships that exist in the numerical semigroups, such as, for example, obtain the set of gaps, having only the Apery set; also, given a set generating elements, each one of them will be associated with its own numerical semigroup.

We conclude, making a description of various concepts of Algebraic Geometry, wich are related to the numerical semigroups, through the Weierstrass semigroups, wich are based on the Riemann-Roch theorem.

1.3

AGRADECIMIENTOS

A mi asesor, el Dr. Percy Fernández, por todo los aportes y el tiempo dedicado al desarrollo de esta tesis. Gracias a su apoyo y paciencia, este trabajo pudo culminarse. Infinitamente agradecido.

Al Dr, Maynard Kong, allá en el cielo, reciba mi agradecimiento, por los diversos cursos en los que lo tuve como profesor y por iniciarme, en el estudio de los semigrupos numéricos.

A mis profesores PUCP, tanto de pregrado, como de Maestría. Gracias por compartir sus conocimientos.

Índice general

ÍNDICE DE TABLAS

LISTA DE SIMBOLOS

$\mathbb{N}$	Enteros no negativos
$\mathbb{N}^*$	Enteros positivos
S	Semigrupo numérico
S^*	$S \setminus \{0\}$
$Ap(S,n)$	Conjunto Apery
$F(S)$	Número de Frobenius del semigrupo numérico S
$c(S)$	Conductor del semigrupo numérico S
ℓ_i	Laguna i-ésima del semigrupo numérico S
$L(S)$	Conjunto de lagunas del semigrupo numérico S
$g(S)$	Género del semigrupo numérico S
S/n	Semigrupo numérico S cociente por n
$N(S)$	Conjunto de elementos esporádicos del semigrupo numérico S
$n(S)$	Cardinalidad de $N(S)$
$S[a_n]$	Semigrupo numérico asociado al elemento generador a_n
$f(S)$	Pseudo-número de Frobenius del semigrupo numérico S
$PF(S)$	Conjunto de pseudo-números de Frobenius
$t(S)$	Tipo del semigrupo numérico S
$A^n(K)$	Espacio afín de dimensión n sobre K
$P^n(K)$	Espacio proyectivo de dimensión n sobre K
χ	Curva algebraica
$H(P)$	Semigrupo de Weierstrass en P

Introducción

En el presente trabajo, se estudiará a los semigrupos numéricos. Se denomina semigrupo numérico a una estructura algebraica que consta de un subconjunto de enteros no negativos, que es cerrado bajo la operación de adición y que tiene un complemento finito en $\mathbb{N}$.

Inicialmente aparecieron en el estudio de las ecuaciones diofánticas lineales, sobre los enteros no negativos, de la forma $a_1.n_1 + a_2.n_2 + a_3.n_3 + \cdots + a_k.n_k = b$
donde $a_1, a_2, a_3, \cdots, a_k$ son enteros positivos dados, que deben ser primos entre sí.

Semigrupos numéricos aparecen cuando se coleccionan todos los valores enteros de b para los cuales existe al menos una solución con enteros no negativos para $n_1, n_2, n_3, \cdots, n_k$, de la ecuación anterior.

Por ejemplo, dada la ecuación diofántica lineal $3n_1 + 5n_2 = b$, ¿para qué valores enteros no negativos de b, la ecuación anterior, siempre tiene al menos una solución? Vemos que $3(0) + 5(0) = 0$, $3(1) + 5(0) = 3$, $3(0) + 5(1) = 5$, $3(2) + 5(0) = 6$, $3(1) + 5(1) = 8$, $3(3) + 5(0) = 9$, $3(0) + 5(2) = 10$, $3(2) + 5(1) = 11$, etc. Luego el conjunto de valores de b, determinará un semigrupo numérico:

$$S = \{0, 3, 5, 6, 8, 9, 10, 11, \cdots\}$$

y los valores enteros positivos que no están en S, serán sus *lagunas* , los cuales representan a los valores de b, para el cual la ecuación diofántica no tiene solución. En esta parte, el matemático francés Ferdinand Frobenius, se interesó en determinar: ¿Cuál es el mayor valor de b, para el cual la ecuación diofántica no tiene solución? O equivalentemente ¿Cuál sería la máxima cantidad de dinero que no se puede reunir, si se tuviera solamente monedas de valor 3 y 5 unidades monetarias?. Esto dio origen a un elemento especial denominado *número de Frobenius*, que se define como el mayor entero que no está en el semigrupo numérico.

El número de Frobenius, no determina en forma única a un semigrupo numérico, pues por ejemplo se ha encontrado que para el número 39, hay 1156012 semigrupos numéricos que lo tienen como número de Frobenius.

En este trabajo se da aportes para determinar en casos especiales semigrupos numéricos, que tienen a un entero dado como su número de Frobenius. Hasta hoy, es un problema abierto, la determinación de alguna fórmula que permita hallar el número de Frobenius, dado un semigrupo numérico cualquiera.

A continuación describimos otra forma de obtener los semigrupos numéricos, a partir de la ecuación diofántica:

$$a_1.n_1 + a_2.n_2 + a_3.n_3 + \cdots + a_k.n_k = b.$$

Colocando una base x, a cada lado de la ecuación se obtiene

$$x^{a_1.n_1+a_2.n_2+a_3.n_3+\cdots+a_k.n_k} = x^b$$

y por álgebra elemental se tiene

$$(x^{a_1})^{n_1}(x^{a_2})^{n_2}(x^{a_3})^{n_3}\cdots(x^{a_k})^{n_k} = x^b$$

de donde se tiene que una potencia con exponente entero no negativo b, se debe obtener a partir del producto de potencias de x^{a_i} con exponentes no negativos.
A partir de este enfoque, puede obtenerse resultados importantes en la teoría de semigrupos numéricos, utilizando las *Bases de Groebner*. Sin embargo, aquí no consideraremos este enfoque.

El capítulo 1 inicia dando la definición de semigrupo numérico, para luego mostrar que estos son generados a partir de una combinación lineal en los enteros no negativos, de los elementos de un conjunto finito de enteros positivos, al cual se le denomina *sistema de generadores*. Además se detallará aquí los diversos elementos notables que forman parte de la teoría de semigrupos numéricos, como por ejemplo: la multiplicidad, la dimensión inmersa y fundamentalmente el conjunto Apery, el cual permite deducir y demostrar diversos resultados. Además a manera de ejemplos, se muestran, algunos tipos de semigrupos numéricos de especial interés.

En el capítulo 2, se realizan diversos análisis al número de Frobenius y al conjunto de lagunas, encontrandose diversas relaciones entre ellos, incluido el género (g), que es el cardinal del conjunto de lagunas. También se dan casos para obtener semigrupos numéricos especiales, conociendo el número de Frobenius.

En el capítulo 3, se revisarán diversos conceptos de la geometría algebraica y en especial se dan resultados para lagunas y conductores, ya que estos participan activamente en los *semigrupos de Weierstrass.* Así como los semigrupos numéricos tienen sus aplicaciones, en la aritmética, como también en el álgebra superior, en este capítulo, se describe una aplicación a la geométria algebraica, en la cual se utiliza curvas algebraicas no singulares y se prueba que para cada punto de ella, existe un semigrupo numérico asociado, al que se denomina *semigrupo de Weierstrass.*

Capítulo 1

CONCEPTOS BÁSICOS PARA LA TEORÍA DE SEMIGRUPOS NUMÉRICOS

1.1. Definición de semigrupo numérico

Las definiciones y diversas propiedades de los semigrupos numéricos que se da en este capítulo, pueden ser revisados con mas detalle en [16], obra de Rosales y García-Sánchez.

Un *semigrupo numérico* es una estructura algebraica, definida mediante un subconjunto S no vacío, de enteros no negativos y una operación binaria, que es la suma usual, tal que cumpla las tres condiciones siguientes:

1. El número *cero* está en S. [Elemento neutro de S]

2. Si se toma dos elementos cualquiera x e y de S, entonces su suma $x + y$ necesariamente estará en S. [Propiedad de clausura en S]

3. Su complemento $\mathbb{N} \setminus S$ es finito.

Equivalentemente, puede decirse que un semigrupo numérico S, es un subsemigrupo conmutativo de $\mathbb{N}$, que tiene complemento finito, respecto a $\mathbb{N}$.

Ejemplo 1.1. Sea el conjunto $S = \{2x + 7y : x, y \in \mathbb{N}\}$. Si se desarrolla por extensión, se tiene $S = \{0, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, \ldots\}$. Dicho conjunto cumple con las dos primeras condiciones y dado que su complemento $\mathbb{N} \setminus S = \{1, 3, 5\}$ es finito, entonces puede afirmarse que es un semigrupo numérico.

Ejemplo 1.2. Sea el conjunto $S = \{6x + 8y : x, y \in \mathbb{N}\}$. Si se desarrolla por extensión, se obtiene $S = \{0, 6, 8, 12, 14, 16, 18, 20, 22, 24, 26, \ldots\}$. Este conjunto no es un semigrupo numérico, pues $\mathbb{N} \setminus S = \{1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 15, 17, 19, 21, 23, 25, \ldots\}$ no es un conjunto finito, ya que, como se aprecia, estarán contenidos todos los impares.

Ejemplo 1.3. El conjunto de los enteros $\mathbb{N}$ es un semigrupo numérico trivial, ya que cumple con las tres condiciones. En cambio $2\mathbb{N}$, $3\mathbb{N}$, $4\mathbb{N}$, $\ldots$, no son semigrupos numéricos, pues sus respectivos complementos son infinitos.

El único semigrupo numérico que posee al número 1, como un elemento suyo, es $\mathbb{N}$. Esto se prueba a continuación.

Proposición 1.4. *Si el número* 1*, pertenece a un semigrupo numérico* S*, entonces necesariamente* $S = \mathbb{N}$*.*

Demostración. Los enteros 0 y 1 están en S. Dado que el entero 1 está en S, entonces, usando la propiedad de clausura para un semigrupo numérico, se obtiene los siguientes elementos de S, que pueden ser generados: $2, 3, 4, 5, 6, \ldots, n$ y para cualquier n que se obtenga, al sumarse con 1, siempre va a generar a su elemento sucesor $n + 1$, obteniéndose así, todo $\mathbb{N}$. $\square$

La intersección de dos semigrupos numéricos, es un semigrupo numérico; esto se prueba en la proposición siguiente.

Proposición 1.5. *La intersección finita de semigrupos numéricos es también un semigrupo numérico.*

Demostración. Consideremos una colección finita de semigrupos numéricos denotados por S_i, con $i \in \{1, 2, 3, ..., n\}$. Probaremos que $\bigcap_{i=1}^{n} S_i$ es también un semigrupo numérico.

1. Dado que para todo $i \in \{1, 2, 3, ..., n\} : 0 \in S_i$, entonces $0 \in \bigcap_{i=1}^{n} S_i$.
2. Sean $x, y \in \bigcap_{i=1}^{n} S_i$, entonces para todo $i \in \{1, 2, 3, ..., n\} :\ x, y \in S_i$, luego, dado que cada S_i es un semigrupo numérico, entonces, si $i \in \{1, 2, 3, ..., n\} :\ x + y \in S_i$ y por lo tanto: $x + y \in \bigcap_{i=1}^{n} S_i$.

3. Para todo $i \in \{1,2,3,...,n\}$: $\mathbb{N} \setminus S_i$ es finito, luego $\mathbb{N} \setminus \bigcap_{i=1}^{n} S_i = \bigcup_{i=1}^{n} (\mathbb{N} \setminus S_i)$ es también finito, por ser la unión finita de conjuntos finitos.

Con esto se cumplen las 3 condiciones para ser semigrupo numérico. $\square$

Ejemplo 1.6. Sean los semigrupos numéricos:

$$S = \{2x + 7y : x, y \in \mathbb{N}\} = \{0, 2, 4, 6, 7, 8, 9, 10, 11, \ldots\}$$
$$T = \{3x + 7y : x, y \in \mathbb{N}\} = \{0, 3, 6, 7, 9, 10, 12, 13, \ldots\}$$

la intersección de ambos, es $S \cap T = \{0, 6, 7, 9, 10, 12, 13, 14, 15, ...\}$ y puede observarse que es un semigrupo numérico, el cual puede ser expresado de la forma

$$S \cap T = \{6w + 7x + 9y + 10z : w, x, y, z \in \mathbb{N}\}.$$

La proposición 1.5 no se cumple para el caso de una intersección infinita de semigrupos numéricos. Mediante un contraejemplo, mostramos que la intersección infinita de semigrupos numéricos, no es necesariamente un semigrupo numérico:
Sean los semigrupos numéricos siguientes:

$$S_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots\}$$
$$S_2 = \{0, 2, 3, 4, 5, 6, 7, 8, 9, \ldots\}$$
$$S_3 = \{0, 3, 4, 5, 6, 7, 8, 9, 10, \ldots\}$$
$$\vdots$$
$$S_i = \{0, i, i + 1, i + 2, i + 3, \ldots\}$$

entonces se tiene que $\bigcap_{i=1}^{\infty} S_i$ tendrá un complemento infinito y por ello no es un semigrupo numérico.

La unión de semigrupos numéricos, en general no es un semigrupo numérico, como se muestra a continuación:

Ejemplo 1.7. Con los semigrupos numéricos S y T, dados en el ejemplo 1.6, se obtiene

$$S \cup T = \{0, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, ...\}$$

el cual no es un semigrupo numérico, pues no se cumple la propiedad de clausura, pues $2 + 3 = 5 \notin S \cup T$ y también $4 + 7 = 11 \notin S \cup T$. Sin embargo, si consideramos los semigrupos numéricos

$$S = \{2x + 7y : x, y \in \mathbb{N}\} = \{0, 2, 4, 6, 7, 8, 9, 10, 11, \ldots\}$$
$$U = \{4x + 7y : x, y \in \mathbb{N}\} = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, 19, 20, 21, \ldots\}$$

su conjunto unión será $S \cup U = \{0, 2, 4, 6, 7, 8, 9, 10, 11, \ldots\}$, el cual si es un semigrupo numérico.

1.2. Generador de un semigrupo numérico

Sea A un subconjunto finito de los enteros positivos:

$$A = \{a_1, a_2, a_3, \ldots, a_n\}.$$

Se denotará mediante $\langle A\rangle$, al *conjunto de combinaciones lineales de los elementos de* A, con coeficientes en los enteros no negativos, es decir:

$$\langle A\rangle = \{\lambda_1\, a_1 + \lambda_2\, a_2 + \lambda_3\, a_3 + \cdots + \lambda_n\, a_n : \lambda_i \in \mathbb{N}\}. \tag{1.1}$$

El siguiente lema, (extraído de [16]) da una condición necesaria y suficiente, para que $\langle A\rangle$ sea un semigrupo numérico.

Lema 1.8. *Sea A un subconjunto finito y no vacio, de $\mathbb{N}$. Entonces $\langle A\rangle$ es un semigrupo numérico, si y solo sí $MCD(A) = 1$.*

Demostración. Se debe probar ambas implicaciones.

Sea $\langle A\rangle = \{\lambda_1\, a_1 + \lambda_2\, a_2 + \lambda_3\, a_3 + \cdots + \lambda_n\, a_n /\lambda_i \in \mathbb{N}\}$ un semigrupo numérico y $MCD(A) = d$, entonces, como el complemento de $\langle A\rangle$ es finito, tiene que haber por lo menos una pareja de números consecutivos $x, x+1 \in \langle A\rangle$. En el supuesto que no existieran los números consecutivos $x, x+1 \in \langle A\rangle$, entonces entre cada pareja de enteros que estan en $\langle A\rangle$, habría al menos un número natural que pertenece al complemento de $\langle A\rangle$ y dado que en $\langle A\rangle$, hay infinitas parejas de enteros no negativos, se obtendrán infinitos naturales que están afuera de $\langle A\rangle$; luego $\mathbb{N}\setminus\langle A\rangle$ no sería finito. Finalmente, como $d = MCD(A)$ y tanto x como $x+1$ son combinaciones lineales de los elementos de A, entonces, d tiene que dividir a x y $x+1$, lo cual se cumple únicamente cuando $d = 1$.

Recíprocamente, si $MCD(A) = 1$, probaremos que $\langle A\rangle$ es un semigrupo numérico. Sabemos por teoría de números, que existen números $e_i \in \mathbb{Z}$ tal que

$$e_1 a_1 + e_2 a_2 + \cdots + e_m a_m = 1, \tag{1.2}$$

donde $a_i \in A \subset \mathbb{N}$; además, entre los e_i hay enteros positivos y negativos. Reordenando términos si fuera necesario, puede asumirse que los positivos son λ_i, con $i \in [1, \ldots, k]$ y los negativos son $-\lambda_j$, con $j \in [k+1, \ldots, m]$; nótese que los λ_i y λ_j son no negativos.

Reemplazando en la ecuación (1,2), se obtiene:

$\lambda_1\, a_1 + \lambda_2\, a_2 + \lambda_3\, a_3 + \cdots + \lambda_k\, a_k - \lambda_{k+1}\, a_{k+1} - \lambda_{k+2}\, a_{k+2} - \lambda_{k+3}\, a_{k+3} - \cdots - \lambda_m\, a_m = 1,$

lo que equivale a

$$\lambda_1\, a_1 + \cdots + \lambda_k\, a_k + 0.a_{k+1} + \cdots + 0.a_m = 0.a_1 + \cdots + 0.a_k + \lambda_{k+1} a_{k+1} + \cdots + \lambda_m a_m + 1,$$

con excepción del número 1 que está en la derecha, se aprecia que se ha construido dos combinaciones lineales de elementos de A :

$$s = 0.a_1 + \cdots + 0.a_k + \lambda_{k+1}\, a_{k+1} + \cdots + \lambda_m a_m$$

$$s + 1 = \lambda_1\, a_1 + \cdots + \lambda_k\, a_k + 0.a_{k+1} + \cdots + 0.a_m.$$

Esto implica que existen dos naturales consecutivos s y $s+1$ que estan en $\langle A \rangle$.

Ahora se probará que estos dos elementos hallados s y $s+1$, generan todos los naturales, a partir de un n_0 y por tanto $\mathbb{N} \setminus \langle A \rangle$ es finito. Dado que s y $s+1$ pertenecen a $\langle A \rangle$, entonces puede afirmarse que:

$$\begin{aligned}(s+1)(s) + 0(s+1) &= s^2 + s \in \langle A \rangle,\\ (s)(s) + 1(s+1) &= s^2 + s + 1 \in \langle A \rangle,\\ (s-1)(s) + 2(s+1) &= s^2 + s + 2 \in \langle A \rangle,\\ (s-2)(s) + 3(s+1) &= s^2 + s + 3 \in \langle A \rangle\end{aligned}$$

y así se continúa hasta:

$$(s - (s-2))(s) + (s-1)(s+1) = s^2 + s + (s-1) \in \langle A \rangle.$$

Luego, teniendo los elementos s y $s+1$ de $\langle A \rangle$, se han generado s elementos consecutivos que también están en $\langle A \rangle$:

$$s^2 + s, s^2 + s + 1, s^2 + s + 2, s^2 + s + 3, \ldots, s^2 + s + (s-1)$$

y si se suma s a cada uno de estos, se obtendrá los s números enteros siguientes. Nuevamente adicionando s a cada uno de los números hallados, se encuentra los s números enteros siguientes. Así, puede apreciarse que se generarán todos los enteros positivos, a partir de $n_0 = s(s+1)$, los cuales estarán en $\langle A \rangle$ y por ello, $\mathbb{N} \setminus \langle A \rangle$ será un conjunto finito; así se ha probado que $\langle A \rangle$ es un semigrupo numérico.

Tener en cuenta que este número n_0 no necesariamente es el menor entero, a partir del cual se generan los enteros consecutivos. $\square$

De acuerdo al lema 1.8, que se acaba de probar, cuando A es subconjunto de los enteros positivos, tal que $MCD(A) = 1$, entonces el conjunto de combinaciones lineales $\langle A \rangle$ es un semigrupo numérico S y se le denotará

$$S = \langle A \rangle = \{\lambda_1\, a_1 + \lambda_2\, a_2 + \lambda_3\, a_3 + \cdots + \lambda_n\, a_n \,/ \lambda_i \in \mathbb{N}\}. \tag{1.3}$$

En adelante se dirá que S *es generado por el conjunto* A o también *el conjunto* A *es un sistema de generadores de* S.

Ejemplo 1.9. Dado el conjunto $A = \{6, 8, 9\}$, se tiene que $MCD(6, 8, 9) = 1$ y haciendo uso del lema 1.8, puede afirmarse que $\langle A \rangle$ es un semigrupo numérico. Por extensión será

$$S = \langle A \rangle = \{0, 6, 8, 9, 12, 14, 15, 16, 18, 20, 21, 22, 23, 24, 25, \ldots\}.$$

El conjunto A es un sistema de generadores de S y puede escribirse lo siguiente:

$$S = \langle A \rangle = \{6\lambda_1 + 8\lambda_2 + 9\lambda_3 : \lambda_i \in \mathbb{N}\}.$$

Nótese que a partir de 20, ya se generan todos los enteros siguientes. Puede usarse también la siguiente representación:

$$A = \{0, 6, 8, 9, 12, 14, 15, 16, 18, 20, \rightarrow\},$$

indicando la flecha dentro del conjunto, que a partir de 20 ya se generan todos los enteros siguientes. Para asegurar que a partir de 20, ya se generan todos los naturales siguientes, ha sido necesario generar 6 enteros consecutivos 20, 21, 22, 23, 24, 25, luego, adicionando a cada uno de ellos, múltiplos de 6, se obtendrán todos los enteros siguientes. Así: $26 = 20 + 6, 27 = 21 + 6, 28 = 22 + 6, 29 = 23 + 6,$ *etc.*
También $\mathbb{N} \setminus S = \{1, 2, 3, 4, 5, 7, 10, 11, 13, 17, 19\}$ es el complemento finito de S.

A continuación se define la *suma de dos semigrupos numéricos*, de la forma usual. Sean los semigrupos numéricos S y T, entonces

$$S + T = \{s + t \in \mathbb{N} : s \in S,\ t \in T\}.$$

Proposición 1.10. *Si S y T son dos semigrupos numéricos, entonces $S + T$ es un semigrupo numérico.*

Demostración. Se debe probar que $S + T$ satisface las tres condiciones que caracterizan a un semigrupo numérico:

1. $0 \in S + T$ pues $0 \in S$ y $0 \in T$, además $0 = 0 + 0$.

2. Sean $x, y \in S + T$, entonces $x = s_1 + t_1$, siendo $s_1 \in S$ y $t_1 \in T$. De manera similar, $y = s_2 + t_2$ siendo $s_2 \in S$ y $t_2 \in T$. Si sumamos estas igualdades: $x + y = (s_1 + s_2) + (t_1 + t_2)$, siendo $s_1, s_2 \in S$ y $t_1, t_2 \in T$. De esto se concluye que $x + y \in S + T$.

3. Por ser S y T semigrupos numéricos: $\mathbb{N} \setminus S$ y $\mathbb{N} \setminus T$ son finitos; con ello se prueba ahora, que también $\mathbb{N} \setminus (S+T)$ es finito:
   En S existe un elemento $a \in S$, tal que, para todo $x \geqslant a :\ x \in S$.
   En T existe un elemento $b \in T$, tal que, para todo $y \geqslant b :\ y \in T$.
   Luego, podemos afirmar que, existe el entero $c = a + b \ \in\ S + T$, para el cual se cumple que, si $x + y \geq c$ entonces $x + y \in S + T$; lo que implicará que el complemento de $S + T$ es finito.

Así, se ha probado que $S + T$ es un semigrupo numérico. □

Proposición 1.11. *Si S y T son dos semigrupos numéricos, entonces $S + T$ es el menor semigrupo numérico que contiene a $S \cup T$.*

Demostración. Ya está probado que $S + T$ es semigrupo numérico, ahora debe probarse que es el menor semigrupo numérico que contiene a la unión de S y T. Primero probamos que $S \cup T \subset S + T$: Sea $n \in S \cup T$ entonces $n \in S$ ó $n \in T$, teniéndose las posibilidades siguientes:

a. $n \in S$, entonces $n \in S$ y $0 \in T$, por tanto $n = n + 0 \in S + T$.

b. $n \in T$, entonces $n \in T$ y $0 \in S$, por tanto $n = 0 + n \in S + T$.

Para ambos casos $n \in S + T$. Luego $S \cup T \subset S + T$.

Probamos a continuación que $S+T$ es el menor semigrupo numérico que contiene a $S \cup T$. Sea M otro semigrupo numérico, tal que $S \cup T \subset M$ y consideremos que $n \in S + T$, entonces $n = x + y$, siendo $x \in S$, $y \in T$. Como $x \in S \subset S \cup T \subset M$, $y \in T \subset S \cup T \subset M$ y dado que M es otro semigrupo numérico, entonces $n = x + y \in M$. Luego $S + T \subset M$ y por ello $S + T$ es el menor conjunto que contiene a S $\cup T$. □

Proposición 1.12. *Sean S y T dos semigrupos numéricos. Si A y B son sistemas de generadores de S y T, respectivamente, entonces $A \cup B$ es un sistema de generadores de $S + T$.*

Demostración. Sean $S = \langle A \rangle$ y $T = \langle B \rangle$, donde

$$A = \{a_1, a_2, \ldots, a_n\} \text{ con } MCD(a_1, a_2, \ldots, a_n) = 1 \text{ y}$$

$$B = \{b_1, b_2, \ldots, b_m\} \text{ con } MCD(b_1, b_2, \ldots, b_m) = 1.$$

Debe probarse que $\langle A \cup B \rangle = S + T$. Al ser una igualdad de conjuntos, se debe probar las dos inclusiones.

Probamos primero que $\langle A \cup B \rangle$ está incluido en $S + T$. Para ello, consideremos $x \in \langle A \cup B \rangle$. Puede suceder que A y B tengan intersección no vacía, entonces, su unión puede ser expresada, como la union de dos disjuntos, así $A \cup B = A \cup (B \setminus A)$. En el caso que A y B no tengan intersección, también se cumple la igualdad anterior. De aquí se tiene que el elemento x se ha generado con elementos de los conjunto A y $B \setminus A$. Luego, se obtiene que x puede ser representado, mediante suma de algún elemento de A y otro de $B \setminus A$. Así podemos afirmar que $x = p + q$, es tal que $p \in \langle A \rangle$ y $q \in \langle B \setminus A \rangle$; pero como $B \setminus A \subset B$, entonces se ha probado que: $x \in S + T$.

Probemos ahora que $S + T \subset A \cup B$. Para ello, consideremos $x \in S + T$, entonces se tiene que $x = s + t$, tal que $s \in S$ y $t \in T$. Estos elementos s y t, deben ser generados, por los elementos de A y B respectivamente; luego se pueden expresar, de la forma siguiente $s = \alpha_1 a_1 + \cdots + \alpha_n a_n$ y $t = \beta_1 b_1 + \cdots + \beta_m b_m$. El elemento x, se obtiene al sumar estas igualdades:

$$x = \alpha_1 a_1 + \cdots + \alpha_n a_n + \beta_1 b_1 + \cdots + \beta_m b_m,$$

apreciándose que x está siendo generado por elementos de $A \cup B$. Además, como los elementos de A tienen MCD igual a 1 y forman un subconjunto de $A \cup B$, entonces los elementos de $A \cup B$, tienen también MCD igual a 1 y por tanto, es un sistema de generadores de $S + T$. $\square$

Notación:

- S^* denotará a un semigrupo numérico sin el elemento nulo, es decir

$$S^* = S \setminus \{0\}.$$

- $S^* + S^*$ denota al conjunto de los elementos de S, que se expresan como la suma de 2 elementos no nulos de S.

Teorema 1.13. *Sea S un semigrupo numérico. Entonces*

a) Un sistema de generadores de S está dado por $S^* \smallsetminus (S^* + S^*)$.

b) $S^* \smallsetminus (S^* + S^*)$ está contenido en todo sistema de generadores de S.

c) $S^* \smallsetminus (S^* + S^*)$ es un sistema minimal de generadores de S.

Demostración. En este teorema se está dando una forma general, para obtener un sistema de generadores, dado S. Iniciamos la prueba:

a) Sea $s \in S^*$. Se tiene dos casos para s.
CASO 1: Si $s \in S^* \smallsetminus (S^* + S^*)$, entonces el elemento s no se puede expresar como la suma de dos elementos no nulos de S , lo que significa, que s es perteneciente al generador de S y por ello, $S^* \smallsetminus (S^* + S^*)$ contiene solo a elementos de S, que no pueden ser generados por otros.
CASO 2: Si $s \notin S^* \smallsetminus (S^* + S^*)$, entonces al ser s un elemento de S^*, implicará que $s \in (S^* + S^*)$ y por tanto existen elementos no nulos $x, y \in S^*$ tal que $s = x + y$; es decir s ha quedado expresado como la suma de x e y, que ahora son menores que s. Pero, como el conjunto de enteros positivos, menores que s, es finito, entonces, para cada uno de los x e y que se hallan, puede aplicarse nuevamente, el caso 1 o caso 2, hasta que, luego de una cantidad finita de pasos, se obtenga solamente números que ya no se podrán expresar como la suma de 2 elementos no nulos de S^*; lo que implica que esta última colección de enteros positivos, estará en $S^* \smallsetminus (S^* + S^*)$ y se ha probado que sus elementos generan a aquellos elementos que no están en $S^* \smallsetminus (S^* + S^*)$.
Así, se ha probado que $S^* \smallsetminus (S^* + S^*)$ es un sistema generador de S.

b) Ahora se prueba que , cualquier otro sistema de generadores de S, contiene a $S^* \smallsetminus (S^* + S^*)$. Sea A un sistema cualquiera, de generadores de S. Si se toma $x \in S^* \smallsetminus (S^* + S^*)$, entonces x es un entero no nulo de S, que no se puede expresar como la suma de 2 enteros no nulos de S; pero también, $x = \lambda_1\ a_1 + \lambda_2\ a_2 + \lambda_3\ a_3 + ... + \lambda_n\ a_n$ tal que $\lambda_i \in \mathbb{N}$ y $a_i \in A$. Sin embargo, dado que x no debe expresarse como una suma de elementos no nulos de S, entonces, la única posibilidad es que x debe ser alguno de los a_i y como $a_i \in A$, entonces $x \in A$. Así, se ha probado que $S^* \smallsetminus (S^* + S^*) \subset A$.

c) Es evidente combinando lo que se probó en (a) y (b).

□

1.3. El conjunto Apery

Este conjunto es muy utilizado y necesario, para los diversos tópicos de la teoría y aplicaciones de semigrupos numéricos. A continuación se da su definición:
Sean S un semigrupo numérico y $n \in S^*$, entonces, el *conjunto Apery de* n en S, viene dado por:

$$Ap(S;n) = \{s \in S : s - n \notin S\}. \tag{1.4}$$

El conjunto Apery de n en S, es el conjunto de todos los elementos que están en S, tales que, al ser disminuidos en n, estén fuera de S. El nombre de este conjunto se debe al matemático francés Roger Apery, que hizo grandes aportaciones en la teoría de números y en el álgebra, que aquí no se tratan. Como referencia, puede revisarse la obra de Roger Apery *Sur les Branches Superlineaires des courbes algébriques - R. Acad Sci. Paris 222 (1946).*
Hoy en día, hay diversos trabajos para la obtención del conjunto Apery; entre ellos, usando la teoría de Bases de Groebner, puede ser obtenido, mediante algoritmos especiales. Un ejemplo de ello se menciona y demuestra en [11], trabajo presentado por Guadalupe Marquez Campos, para la obtención de su Tesis Doctoral en la Universidad de Sevilla, en enero del 2014.

A continuación se presentan algunos lemas extraidos de [16].

Lema 1.14. *Sean S un semigrupo numérico y $n \in S^*$. Considerando que $w(0) = 0$ y $w(i) \in S^*$ representan a los menores elementos tales que $w(i) = nk + i$, para todo $i \in \{1, 2, 3, ..., n-1\}$ y $k \in \mathbb{N}$, entonces:*

$$Ap(S,n) = \{w(0), w(1), w(2), \ldots, w(n-1)\}, \tag{1.5}$$

donde $Card[Ap(S,n)] = n$.

Demostración. Dado que (1.5) es una igualdad de conjuntos, se demostrará que se cumple la doble inclusión , entre tales conjuntos.

Probamos que $Ap(S,n) \subset \{w(0), w(1), w(2), \ldots, w(n-1)\}$. Sea $s \in Ap(S,n)$, entonces $s \in S$ y $s - n = e$ es un elemento que no está en S. Aquí se tiene 3 casos:
CASO 1: Sea $e < 0$. Entonces puede escribirse $e = -m$, con m positivo y menor que n, se tendrá así que $s = 0n + (n - m)$ del cual se deduce $s = w(n-m)$ y $n - m \in \{0, 1, 2, 3, ..., n-1\}$.
CASO 2: Sea $0 < e < n$. Entonces $s = n + e$ y así, $s = w(e)$ y $e \in \{1, 2, 3, ..., n-1\}$.

CASO 3: Sea $e > n$. Entonces se puede dividir e entre n y se obtiene $e = nq + r$ siendo $r \in \{1, 2, 3, ..., n-1\}$ y q el menor entero. Así $s = w(r)$.
Luego, de todo lo anterior $Ap(S, n) \subset \{w(0), w(1), w(2), ..., w(n-1)\}$.

Ahora se prueba que $\{w(0), w(1), w(2), \ldots, w(n-1)\} \subset Ap(S, n)$. Consideremos que $w(i) \in \{w(0), w(1), w(2), ..., w(n-1)\}$, entonces $w(i)$ es el menor entero de S, tal que $w(i) - i = nk$. Luego, $w(i) = nk + i \in S$ es el menor posible y restando n, se tiene que $w(i) - n = (k-1)n + i \notin S$, pues si perteneciera a S, entonces $w(i) - n$ sería menor que $w(i)$, lo que contradice al hecho de que $w(i)$ es el menor de S que es congruente con $i(mod\, n)$. Así se ha probado que $w(i) \in Ap(S, n)$. □

Proposición 1.15. *Sean S un semigrupo numérico y $n \in S^*$. Para cualquier elemento s que está en S, existe un único entero no negativo k y un único w que está en $Ap(S, n)$, tal que, $s = nk + w$.*

Demostración. Por el algoritmo de la división se tiene que $s = n.q + i$ siendo $i \in \{0, 1, 2, 3, ..., n-1\}$. Pero también $w(i)$ es el menor elemento de S que es congruente con i módulo n, es decir $w(i) = n.p + i$. Si ahora restamos ambas igualdades se obtiene: $s - w(i) = n(q-p)$, es decir $s = n(q-p) + w(i)$ y de aquí, se obtiene que $s = nk + w(i)$. □

De esta proposición se deduce que los elementos $w(i) \in Ap(S, n)$ y $n \in S^*$ generan a S, es decir, *un generador de S* está dado por:

$$S = \langle Ap(S, n) \cup \{n\} \rangle. \tag{1.6}$$

Sin embargo, por el teorema 1.3, se debe tener en cuenta que *el generador minimal* es

$$S = S^* \setminus (S^* + S^*). \tag{1.7}$$

Proposición 1.16. *Sea $A = \{a_1, a_2, \ldots, a_n\}$ tal que $a_1 < a_2 < \cdots < a_n$ y a_1 no es 0. Si $S = \langle A \rangle$, entonces, $\langle A \rangle$ es el sistema minimal de generadores de S si y solo si $a_{i+1} \notin \langle a_1, a_2, \ldots, a_i \rangle$; siendo i un entero desde 1 hasta $n-1$.*

Demostración. Probaremos primero que: *si $\langle A \rangle$ es el sistema minimal de generadores del semigrupo numérico S, entonces $a_{i+1} \notin \langle a_1, a_2, \ldots, a_i \rangle$*. Si suponemos que $a_{i+1} \in \langle a_1, a_2, \ldots, a_i \rangle$, se tendría que, A no sería un generador minimal, pues al menos hay un elemento que se está generando, a partir de los anteriores; por tal motivo, se tiene que $a_{i+1} \notin \langle a_1, a_2, \ldots, a_i \rangle$.

Recíprocamente, probamos ahora que: *si $a_{i+1} \notin \langle a_1, a_2, \dots, a_i \rangle$, con i entero desde 1 hasta $n-1$, entonces $\langle A \rangle$ es el sistema minimal de generadores de S.* Dado que $a_{i+1} \notin \langle a_1, a_2, \dots, a_i \rangle$, entonces cada elemento de A no se puede generar por los anteriores, pero como $\langle A \rangle$ es un generador de S, solo queda que, debe ser el generador minimal de S. □

La diferencia de semigrupos numéricos no es un semigrupo numérico, pues se obtendría un conjunto finito. La diferencia de un semigrupo numérico y un conjunto arbitrario, no necesariamente resultará ser otro semigrupo numérico. La siguiente proposición da una condición necesaria y suficiente para que la diferencia entre un semigrupo numérico y un conjunto unitario, resulte otro semigrupo numérico.

Proposición 1.17. *Si A es un conjunto que genera minimalmente al semigrupo numérico S y C es un subconjunto unitario de S, entonces $S \setminus C$ es un semigrupo numérico si y solo sí C es un subconjunto de A.*

Demostración. Sea $A = \{a_1, a_2, ..., a_n\}$. Probaremos que: *si $S \setminus C$ es un semigrupo numérico, entonces C es un subconjunto de A.* Sea c el único elemento del conjunto C y supongamos que c no pertenece al generador minimal A, entonces este elemento puede ser expresado como

$$c = x_1 a_1 + \dots + x_n a_n,$$

Ahora $S \setminus C$ es un nuevo semigrupo numérico, el cual tendrá un nuevo generador minimal $B = \{b_1, b_2, \dots, b_m\}$. Por ello se puede expresar a cada a_i como combinación lineal de los b_i, luego el elemento c también estaría expresado como combinación lineal de los b_i lo que implica que $c \in S \setminus C$, que es absurdo y por ello $C \subset A$.

Ahora se prueba el recíproco:
Si $C = \{c\} \subset A$, entonces $S \setminus C$ es un semigrupo numérico.
Dado que $\{c\} \subset A$ entonces c debe de ser, alguno de los elementos de A. Sin pérdida de generalidad, podemos asumir que $c = a_n$ (es alguno de los a_i). Ahora probaremos con ello que $S \setminus C$ es un semigrupo numérico.

1. Como $c = a_n$ es un elemento del generador minimal de S, entonces $c \neq 0$, por lo tanto $0 \in S \setminus \{c\}$.

2. Ahora se prueba que, dados $u \in S \setminus \{c\}$ y $v \in S \setminus \{c\}$, su suma $u + v$ estará en $S \setminus \{c\}$. Dado que $u \in S \setminus \{c\}$ entonces $u = x_1 a_1 + x_2 a_2 + \dots + x_{n-1} a_{n-1}$, y además

$u \neq c$. De manera similar, $v \in S \setminus \{c\}$ entonces $v = y_1a_1 + y_2a_2 + \cdots + y_{n-1}a_{n-1}$ y además $v \neq c$.

Si ahora sumamos estas ecuaciones, se obtiene una combinación lineal de los elementos de $A \setminus \{c\}$, pero tambien $u + v \neq c$, pues si fuera $u + v = c$, entonces c no sería un generador minimal en S.

3. Dado que S es semigrupo numérico, entonces $\mathbb{N} \setminus S$ es un conjunto finito. Además, el conjunto $S \setminus \{c\}$ tendrá tambien un complemento finito, ya que $\mathbb{N} \setminus (S \setminus \{c\}) = (\mathbb{N} \setminus S) \cup \{c\}$ como se observa, será también finito.

Se ha probado así que $S \setminus \{c\}$ es un semigrupo numérico.

□

1.4. Multiplicidad y dimensión inmersa

Dado un semigrupo numérico S, se define:

Multiplicidad de S : es el menor elemento del sistema generador minimal de S o también se dice que es el mínimo de S^*. En adelante se le denotará por $m(S)$.

Dimensión inmersa de S : es el cardinal del sistema minimal generador y será denotado mediante $e(S)$.

Sea $m(S) = m$. Usando el lema 1.14, el cardinal de $Ap(S, m)$ es m; si ahora se le quita el 0, entonces el cardinal de $Ap(S, m) \setminus \{0\}$ será $m - 1$ y si se aumenta ahora el número m, el cardinal de $[Ap(S, m) \setminus \{0\}] \cup \{m\}$, será $m = m(S)$.
Por la proposición 1.15 , cualquier elemento de S, se puede generar mediante algún elemento de $Ap(S, m)$ y el número m. Esto implica que $[Ap(S, m) \setminus \{0\}] \cup \{m\}$ es un sistema de generadores de S, pero no es necesariamente el minimal, el cual tendría por cardinal $e(S)$. así se ha probado que

$$e(S) \leq m(S). \tag{1.8}$$

De esta última desigualdad, se tiene que, el número de elementos del sistema minimal generador de S, no debe exceder al mínimo de S^*.

Ejemplo 1.18. Considérese el semigrupo numérico $S = \{0, s, s+1, s+2, \rightarrow\}$. Aquí $m(S) = s$ y dado que el conjunto $\{s, s+1, s+2, \ldots, s+(s-1)\}$ es su sistema generador minimal, entonces su dimensión inmersa es $e(S) = s$. Asi, se ha mostrado un ejemplo en el cual se cumple la igualdad $e(S) = m(S)$.

Si en el semigrupo numérico S anterior, se considera $s = 1$, entonces $S = \mathbb{N}$ y por tanto se cumplira también la igualdad $e(S) = m(S) = 1$. Tener presente que, $e(S) = 1$ se cumple únicamente, cuando $S = \mathbb{N}$, pues como la dimensión inmersa es 1, su sistema generador minimal debe tener un único elemento s y de aquí, $S = \langle\{s\}\rangle$, por tanto $S = \{x.s : x \in \mathbb{N}\}$, generandose así un conjunto formado por todos los múltiplos de s, el cual no sería un semigrupo numérico pues su complemento es infinito; para que lo sea, debe cumplirse que $s = 1$ y así se obtiene que $S = \mathbb{N}$.

La prueba de la siguiente proposición es simple, pero será bastante útil para obtener un número especial llamado número de Frobenius, que se estudiará en la siguiente sección.

Proposición 1.19. *Sea S un semigrupo numérico, con multiplicidad $m(S) = m$. Si se tiene que los m números consecutivos $s_0, s_0 + 1, s_0 + 2, \ldots, s_0 + m - 1$, pertenecen a S, entonces todos los enteros siguientes, también pertenecerán a S.*

Demostración. Lo que se quiere demostrar aquí, es equivalente a probar que, si los enteros $s_0, s_0 + 1, s_0 + 2, \ldots, s_0 + m - 1$ están en S entonces, para todo $x \geq s_0 + m :$ $x \in S$. Sea $x = s_0 + m + n$. Se probará por inducción que, con la condición dada, para todo n entero no negativo, se cumple que $x \in S$.

Si $n = 0$ se cumple, pues como $s_0 \in S$ y $m(S) = m \in S$, entonces $x = s_0 + m \in S$.

Si es válido para $n = k$, ahora se probará que también se cumple para $n = k + 1$. Se divide k entre $m(S) = m$ y se obtiene, por el algoritmo de la división, que deben existir, enteros q, i tal que $k = q.m + i$, siendo $0 \leq i \leq m - 1$. Luego $x = s_o + m + (q.m + i) \in S$ y reordenando términos $x = (1 + q)m + (s_0 + i) \in S$. Ahora se le suma 1, para obtener su sucesor $x + 1 = (1 + q)m + (s_0 + i + 1)$ y como $s_0 + i + 1$ tambien pertenece a S, entonces se tendrá que $x + 1$ se logra generar con $m \in S$ y $(s_0 + i + 1) \in S$. Luego, para $n = k + 1$ se obtendrá que $x + 1 \in S$. $\square$

1.5. Semigrupos numéricos especiales

Existen diversos tipos de semigrupos numéricos; aquí describimos a continuación, algunos que son de especial interés.

1.5.1. Semigrupo numérico cociente por n

Considérese el semigrupo numérico

$$S = \langle\{5,7\}\rangle = \{0,5,7,10,12,14,15,17,19,20,21,22,24,\rightarrow\}.$$

Se procederá a obtener otros semigrupos numéricos, realizando una operacion de división exacta por un entero n. Para ello, si se desea obtener S/n se realizará la división de cada elemento de S por n y solo se coleccionará a aquellos cocientes exactos, es decir con residuo cero. La colección de tales números formará el semigrupo numérico S/n.
Mencionamos algunos:

$$\begin{aligned}
S/2 &= \{0,5,6,7,10,11,12,13,14,\rightarrow\} = \langle\{5,6,7\}\rangle\\
S/3 &= \{0,4,5,7,8,9,10,\rightarrow\} = \langle\{4,5,7\}\rangle\\
S/4 &= \{0,3,5,6,7,\rightarrow\} = \langle\{3,5,7\}\rangle\\
S/5 &= \{0,1,2,3,4\rightarrow\} = \mathbb{N}\\
S/6 &= \{0,2,4,7,8,9,10,11,12,\rightarrow\} = \langle\{2,7\}\rangle\\
S/7 &= \{0,1,2,3,4,\rightarrow\} = \mathbb{N}\\
S/10 &= \{0,1,2,3,4,\rightarrow\} = \mathbb{N}\\
S/100 &= \{0,1,2,3,4,\rightarrow\} = \mathbb{N}\\
&\text{etc.}
\end{aligned}$$

Puede notarse que los conjuntos S/n son semigrupos numéricos, lo cual se probará, lineas abajo.

Podemos definir lo siguiente: Sean S un semigrupo numérico y n un entero positivo. El *semigrupo numérico cociente por* n se denota mediante S/n y se obtiene mediante el siguiente conjunto:

$$S/n = \left\{\tfrac{p}{n} \in \mathbb{N} :\ p \in S\right\},$$

o equivalentemente:

$$S/n = \{s \in \mathbb{N} :\ ns \in S\}.$$

A continuación, se prueba que el conjunto S/n es también un semigrupo numérico:

1. Dado que se está considerando que $0 \in \mathbb{N}$ y $n0 \in S$, entonces $0 \in S/n$.

2. Sea $a \in S/n$, entonces $a \in \mathbb{N}$ y $n.a \in S$; también sea $b \in S/n$, entonces $b \in \mathbb{N}$ y $n.b \in S$. Entonces, $a + b \in \mathbb{N}$ y $n(a + b) \in S$, por lo tanto $a + b \in S/n$.

3. El complemento $\mathbb{N} \smallsetminus S$ es finito, entonces existe un entero F, tal que todo entero x que excede a F, estará en S. Luego, puede encontrarse un primer entero nk que sea múltiplo de n y que sea superior a F; pero entonces, a partir de ahí se puede hallar los siguientes múltiplos de n y así se tendrían enteros tales que $F < nk < nk + n < nk + 2n < nk + 3n < nk + 4n < \cdots$ y por ello, los enteros $k, k + 1, k + 2, k + 3, k + 4, \ldots$ estarán en S/n; lo que significa que si hay enteros que estan afuera de S/n, la cantidad de ellos, será finita, pues a partir de k, hay seguridad de que todos estén contenidos en S/n. Esto no significa que $k-1$ esté fuera de S/n, ya que tal entero, puede o no, estar en S/n.

De todo lo anterior, S/n es un semigrupo numérico.

Mediante un razonamiento sencillo, puede probarse el siguiente resultado:
Sea S un semigrupo numérico y sea F un entero que no está en S, con la condición de que todo entero n que supere a F, si está en S. Entonces, si $n > F$ se tendrá que, $S/n = \mathbb{N}$.

1.5.2. Semigrupo numérico Arf

Este tipo de semigrupo numérico es de suma importancia, debido a que tiene una característica propia de ellos; todos estos, poseen dimensión inmersa máxima. Como ya se vió en (1.8), la dimensión inmersa $e(S)$ no puede exceder a la multiplicidad $m(S)$, pero para algunos semigrupos numéricos, llega a obtenerse la igualdad

$$e(S) = m(S),$$

entonces, aquí se dirá que tal semigrupo numérico, tiene dimensión inmersa máxima.

Es sabido que un semigrupo numérico S se origina, mediante una colección de enteros positivos que tengan MCD igual a 1 y mediante un proceso de sumas entre estos elementos, se obtendrá todos los elementos de S.

Para obtener este tipo de semigrupos numéricos, se va a imponer una condición adicional: cualquier elemento de S, que se descompone como la suma de 2 elementos x e y de S, mayores que un elemento no nulo z de S, debe generarse mediante dicho elemento z y algún otro, de S. Si se cumple tal condición , se obtendrá un semigrupo numérico Arf.

Ejemplo 1.20. Sea $S = \langle\{3,7\}\rangle$ con dimensión inmersa 2, el cual origina al siguiente semigrupo numérico $S = \{0,3,6,7,9,10,12,13,14,\rightarrow\}$; éste no es un semigrupo numérico Arf, pues:

$$14 = 7 + 7 = 3 + n \rightarrow n = 11 \notin S.$$

Ejemplo 1.21. Si ahora se considera el nuevo semigrupo numérico $S' = \langle\{3,7,11\}\rangle$ con dimensión inmersa 3, se obtendrá que $S' = \{0,3,6,7,9,10,11,\rightarrow\}$ y este si será un semigrupo numérico Arf, pues se cumplirá que:

$$\begin{gathered}12 = 6 + 6 = 3 + n \rightarrow n = 9 \in S',\\ 13 = 6 + 7 = 3 + n \rightarrow n = 10 \in S',\\ 14 = 7 + 7 = 3 + n \rightarrow n = 11 \in S',\\ 15 = 6 + 9 = 3 + n \rightarrow n = 12 \in S'.\end{gathered}$$

y seguirá cumpliéndose para el resto de elementos de S'. Nótese que S' tiene dimensión inmersa máxima, pues $e(S') = m(S') = 3$.

Ejemplo 1.22. Sea $S = \langle\{4,7\}\rangle$ con dimensión inmersa 2, que origina al siguiente semigrupo numérico $S = \{0,4,7,8,11,12,14,15,16,18,19,20,21,\rightarrow\}$. Este no es un semigrupo numérico Arf, pues:

$$14 = 7 + 7 = 4 + n \rightarrow n = 10 \notin S.$$

Ejemplo 1.23. Si ahora se considera el nuevo semigrupo numérico $S' = \langle\{4,7,10\}\rangle$ con dimensión inmersa 3, se obtendrá que:

$$S' = \{0,4,7,8,10,11,12,14,15,16,17,\rightarrow\},$$

aún no es Arf, pues:

$$17 = 7 + 10 = 4 + n \rightarrow n = 13 \notin S'.$$

Ejemplo 1.24. Considérese ahora $S'' = \langle\{4,7,10,13\}\rangle$ con dimensión inmersa 4, el cual origina $S'' = \{0,4,7,8,10,11,12,13,14,15,16,17,\rightarrow\}$, pero aún no es Arf, pues:

$$16 = 8 + 8 = 7 + n \to n = 9 \notin S''.$$

Pero ahora 9 y 4 generan a 13, entonces ya no debe colocarse a 13 como generador y se obtiene $S''' = \langle\{4,7,9,10\}\rangle$ con dimensión inmersa 4 y por extensión será

$$S''' = \{0,4,7,8,9,10,11,12,13,14,15,16,17,\to\},$$

el cual ya es Arf y se aprecia, que también tendrá dimensión inmersa máxima, pues $e(S''') = m(S''') = 4$.

Todo semigrupo numérico Arf, tendrá dimensión inmersa máxima, pero lo contrario no es cierto. Pues por ejemplo el semigrupo numérico S'' dado lineas arriba, tiene dimensión inmersa máxima, pero no es Arf.

El concepto de semigrupo numérico Arf, que se está usando equivale a lo siguiente: *Un semigrupo numérico, será Arf, si al tomar 2 elementos x e y de S, mayores que un tercer elemento z de S, existe un elemento n de S, tal que $x+y = z+n$.*

Puede extenderse la definicion de Arf, si se tiene en cuenta que:
Si $z = 0$, evidentemente existirá n.
Si $z = y$, también sería evidente la existencia de n.
Así, se obtiene la siguiente definición, que puede encontrarse en diversos textos, por ejemplo en [16]: *Un semigrupo numérico será Arf, si al tomar 3 elementos x, y, z pertenecientes a S, tales que $x \geq y \geq z$, entonces $x + y - z \in S$.*

Ejemplo 1.25. El semigrupo numérico

$$S = \{0, k, k+1, k+2, \to\}$$

es Arf y puede verificarse ello, tomando elementos $x, y, z \in S$, que cumplan con $x \geq y \geq z$, obteniéndose así, los siguientes casos:
Si $z = 0$ entonces $x + y - z = x + y \in S$.
Si $y = z \geq k$, entonces $x + y - z = x \in S$.
Si $x \geq y > z > 0$, entonces $y - z \geq 1 \wedge x \geq k$, luego $x + y - z \geq k + 1 \to x + y - z \in S$.
Así se ha probado que, con $x \geq y \geq z$, se tiene $x + y - z \in S$ y por lo tanto S es Arf.

1.5.3. Semigrupo numérico simétrico

Dado un semigrupo numérico S, siempre existirá un entero $F(S)$ que no está en S, tal que, si n supera a $F(S)$, entonces $n \in S$. Al número $F(S)$ se le denomina

número de Frobenius.
Consideremos un semigrupo numérico S con número de Frobenius $F(S)$.
Si s es un elemento de S, entonces $F(S)-s$ con seguridad, no pertenece a S.
Esto es válido, pues si se supone que $F(S)-s\in S$, entonces por la clausura en S, se debe tener que $(F(S)-s)+s\in S$, es decir $F(S)\in S$, lo cual es absurdo y por ello debe cumplirse que $F(S)-s\notin S$. Pero, el caso contrario, no es necesariamente cierto. Es decir: Si $F(S)-x\notin S$, entonces ¿$x\in S$? Esto no siempre ocurre.

Ejemplo 1.26. Sea el semigrupo numérico $S=\{0,5,6,7,8,9,\ldots\}$. Se observa que todos los enteros que exceden a 4 están en S, entonces $F(S)=4$. Luego:

$$
\begin{gathered}
4-0\notin S \text{ y } 0\in S,\\
4-1\notin S \text{ y } 1\notin S,\\
4-2\notin S \text{ y } 2\notin S,\\
4-3\notin S \text{ y } 3\notin S.
\end{gathered}
$$

Aquí notamos que, si $F(S)-x\notin S$, entonces no puede afirmarse que $x\in S$.

Los semigrupos numéricos en los cuales, el entero $x\in S$, reciben el nombre de *Simétricos* y su definición precisa es la siguiente:
Un semigrupo numérico S con número de Frobenius $F(S)$ es Simétrico, si se cumple que $F(S)-s\notin S$ si y solo sí $s\in S$.
Equivalentemente:
Un semigrupo numérico S con número de Frobenius $F(S)$ es llamado Simétrico, si se cumple que $s\notin S$ si y solo sì $F(S)-s\in S$.

Ejemplo 1.27. Consideremos los siguientes semigrupos:

1. El conjunto de los enteros no negativos $\mathbb{N}$, es un semigrupo numérico simétrico.

2. El generado por $A=\{2,3\}$, que origina a $S=\{0,2,3,\rightarrow\}$ es un semigrupo numérico simétrico, pues $F(S)=1$ y se cumple que:

$$
\begin{gathered}
1\notin S\rightarrow F(S)-1=0\in S\\
-1\notin S\rightarrow F(S)-(-1)=2\in S\\
-2\notin S\rightarrow F(S)-(-2)=3\in S\\
\text{etc.}
\end{gathered}
$$

3. El generado por $B=\{3,4,5\}$, que origina a $S=\{0,3,4,5,\rightarrow\}$ no es un semigrupo numérico simétrico, pues $F(S)=2$ y si se considera $s=1\notin S$, entonces $F(S)-s=1\notin S$.

Notar que, cuando $F(S)$ es número par, entonces para n entero positivo, $F(S) = 2n$ y llevará a la siguiente conclusión $F(S) - n = n$, lo que implica que, si $n \notin S$ entonces $F(S) - n$ no pertenecerá a S; luego puede afirmarse lo siguiente: *Cuando el número de Frobenius* $F(S)$ *es par, entonces el semigrupo numérico* S*, no será simétrico.*

Capítulo 2

NÚMERO DE FROBENIUS, GÉNERO Y LAGUNAS

2.1. Definiciones y proposiciones básicas

El mayor número entero que no pertenece al semigrupo numérico S, es denominado *número de Frobenius* y representa al menor entero x tal que sumado con cualquier entero positivo, siempre generará un elemento de S; es decir para todo $n \in \mathbb{N}$ se tendrá que $x + n + 1 \in S$. Este número puede ser incluso -1, como lo es para el caso en que el semigrupo numérico es todo $\mathbb{N}$. Asimismo, se denominará *conductor* al menor elemento de S tal que, al ser sumado con cualquier entero no negativo, siempre da un elemento de S. A continuación se dan algunas definiciones:

1. El *número de Frobenius* será denotado por $F(S)$ y no pertenece a S, pero para todo $n \in \mathbb{N}$ debe cumplir que $F(S) + n + 1 \in S$.

2. El *conductor de S* se denotará por $c(S)$ y es el sucesor de $F(S)$, es decir $c(S) = F(S) + 1$.

3. El conjunto de enteros $L(S) = \mathbb{N} \setminus S$ que representa al complemento del semigrupo númerico S, se le conoce como el *conjunto de lagunas* de S y contiene a todos los enteros positivos que no pertenecen a S. Cada uno de sus elementos pueden denotarse mediante ℓ_i y se le denominará *laguna i-ésima.*

4. La cardinalidad de $L(S)$ será denominada *género* y será denotada por $g(S)$, a la que tambien se le conoce como el *grado de singularidad de S*.

5. El *conjunto de elementos esporádicos de S*, denotado por $N(S)$, está conformado por todos los elementos del semigrupo numérico, que son menores

que el número de Frobenius; es decir $N(S) = \{s \in S : s < F(S)\}$.

6. La cantidad de elementos esporádicos se denota por $n(S)$.

Ejemplo 2.1. Sea $S = \{3x + 7y : x, y \in \mathbb{N}\} = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\} = \langle\{3, 7\}\rangle$ Entonces $m(S) = 3$, $e(S) = 2$, $L(S) = \{1, 2, 4, 5, 8, 11\}$, $g(S) = 6$, $F(S) = 11$, $c(S) = 12$, $N(S) = \{0, 3, 6, 7, 9, 10\}$, $n(S) = 6$.

A continuación se establece una relación bastante evidente entre el género $g(S)$, la cantidad de elementos esporádicos $n(S)$ y el conductor $c(S)$.

Lema 2.2. *Dado un semigrupo numérico S, se cumple que*

$$c(S) = g(S) + n(S). \tag{2.1}$$

Demostración. Notar que $L(S)$ y $N(S)$ son conjuntos disjuntos. La unión de $L(S)$ y $N(S)$, es el conjunto de enteros no negativos menores que el conductor de S, esto es:

$$\{0, 1, 2, 3, \ldots, F(S)\} = L(S) \cup N(S).$$

Luego, tomando cardinal a cada lado de la igualdad, se obtiene:

$$c(S) = g(S) + n(S).$$

□

Lema 2.3. *Si $n \in S^*$, siendo S un semigrupo numérico y x un entero tal que $x > max[Ap(S, n)]$, entonces $x \in S$.*

Demostración. Suponiendo que éste entero x no está en S, entonces debe existir el menor k entero no nulo tal que $x + kn \in S$, lo que implica que al calcular $x + kn - n$ no estaría en S, luego se ha obtenido un elemento $x + kn$ que estará en $Ap(S, n)$, pero que excederá al $max[Ap(S, n)]$, lo cual es absurdo. Luego $x \in S$. □

El lema 2.3 asegura que excediendo al máximo de $Ap(S, n)$, se tendrá elementos del semigrupo numérico, pero no dice que este máximo de $Ap(S, n)$ sea el conductor de S. Sin embargo, si a cualquier elemento w del Apery $Ap(S, n)$, se le resta n, entonces por definición se obtendrá un elemento que no está en S; es decir

$$\text{si } w \in Ap(S, n) \text{ entonces } w - n \notin S.$$

Esto significa que, si $w \in Ap(S, n)$ entonces $w - n$ es una laguna de S. Luego, en particular para el $w_m = max[Ap(S, n)]$ se cumple que $max[Ap(S, n)] - n \in L(S)$. Pero ¿será este elemento, el máximo del conjunto $L(S)$? A continuación se prueba, que la respuesta es afirmativa.

Sea $w_m = max(Ap(S,n))$ entonces w_m está en S, además $w_m - n \notin S$ y cualquier otro $s > w_m$ obliga a que $s \in S$, por el lema 2.3 y se obtiene que $s - n \in S$, pues si $s - n \notin S$ entonces s pertenecería a $Ap(S,n)$ y así w_m no sería $max(Ap(S,n))$.

Se prueba ahora que $max(Ap(S,n)) - n = w_m - n$ es el mayor entero que no pertenece a S, es decir cualquier otro entero y, que excede a $w_m - n$, tiene que estar en S. Sea y un entero cualquiera, tal que y excede a $w_m - n$ entonces $y + n > w_m$, luego como w_m es el máximo de $Ap(S,n)$, entonces por el lema 2.3, se tiene que $y + n \in S$ y además al restarle n tiene que estar en S. Así $(y+n) - n \in S$, de donde se obtiene $y \in S$. Por lo tanto, cualquier entero que exceda a $w_m - n$ estará en S y así

$$F(S) = w_m - n = max(Ap(S,n)) - n.$$

Así se ha probado lo siguiente:

Proposición 2.4. *Sea S un semigrupo numérico y $n \in S^*$. Entonces*

$$F(S) = max(Ap(S,n)) - n.$$

Ahora nótese que para cada $w \in Ap(S,n)$, se tiene que w será congruente módulo n, con algún $i \in \{0,1,2,\dots,n-1\}$ y por tanto $w = i + k_i n$, para algún entero no negativo k_i. Así $Ap(S,n) = \{w(0), w(1), w(2), \dots, w(n-1)\}$ donde $w(0) = 0$ y $w(i) = i + k_i n$. Analizamos los valores de k_i:

- Si $k_i = 0$ entonces $w(i) = i$, el cual tiene que pertenecer a S, pues los $w(i) \in S$.
- Si $k_i = 1$ entonces $w(i) = i+n \in S$, entonces $w(i)-n = i \notin S$ y por tanto $i \in L(S)$. De esta manera hemos hallado un elemento de $L(S)$.
- Si $k_i = 2$ entonces $w(i) = i+2n \in S$, luego se tiene que $\begin{cases} w(i) - n &= i + n \notin S \\ w(i) - 2n &= i \notin S \end{cases}$
  Se halló así, dos elementos más de $L(S)$.

Por lo tanto el número de elementos de $L(S)$ viene dado por:

$$g(S) = k_1 + k_2 + \cdots + k_{n-1}$$

$$g(S) = \tfrac{1}{n}(nk_1 + nk_2 + \cdots + nk_{n-1})$$

$$g(S) = \tfrac{1}{n}((nk_1 + 1) + (nk_2 + 2) + \cdots + (nk_{n-1} + n - 1) - (1 + 2 + \cdots + n - 1))$$

$g(S) = \frac{1}{n}(w_1 + w_2 + \cdots + w_{n-1} - \frac{(n-1)n}{2})$

$g(S) = \frac{1}{n}(\sum_{w_i \in Ap(S.n)} w_i) - \frac{n-1}{2}$

Con ello se ha probado la proposición siguiente:

Proposición 2.5. *Si n es un elemento no nulo del semigrupo numérico S, entonces la cantidad total de lagunas, queda determinado por la igualdad siguiente:*

$$g(S) = \frac{1}{n}(\sum_{w \in Ap(S,n)} w) - \frac{n-1}{2}.$$

Ejemplo 2.6. Consideremos el siguiente semigrupo numérico

$$S = \langle\{4,9,11\}\rangle = \{0,4,8,9,11,12,13,15,16,17,18,\rightarrow\}.$$

Verifiquemos que se cumplen las proposiciónes 2.4 y 2.5:

i) S tiene multiplicidad $m(S) = 4$, dimensión inmersa $e(S) = 3$, número de Frobenius $F(S) = 14$, conjunto de lagunas $L(S) = \{1,2,3,5,6,7,10,14\}$ y género $g(S) = 8$.

ii) Algunos conjuntos Apery son:

- $Ap(S,4) = \{0,9,11,18\}$.
- $Ap(S,8) = \{0,4,9,11,13,15,18,22\}$.

iii) Ahora se comprueba la proposición 2.5:

- Con $Ap(S,4)$, tenemos $F(S) = max(Ap(S,4)) - 4 = 18 - 4 = 14$,

$$g(S) = \frac{1}{4}(0+9+11+18) - \frac{4-1}{2} = 8.$$

- Con $Ap(S,8)$, se tiene $F(S) = max(Ap(S,8)) - 8 = 22 - 8 = 14$,

$$g(S) = \frac{1}{8}(0+4+9+11+13+15+18+22) - \frac{8-1}{2} = 8.$$

Ejemplo 2.7. Sea el semigrupo numérico

$$S = \langle\{5,7,9\}\rangle = \{0,5,7,9,10,12,14,15,16,17,18,\rightarrow\}.$$

i) S tiene multiplicidad $m(S) = 5$, dimensión inmersa $e(S) = 3$, número de Frobenius $F(S) = 13$, conjunto de lagunas $L(S) = \{1,2,3,4,6,8,11,13\}$ y género $g(S) = 8$.

ii) De aquí se hallan algunos $Ap(S, n)$

- $Ap(S, 5) = \{0, 7, 9, 16, 18\}$
- $Ap(S, 7) = \{0, 5, 9, 10, 15, 18, 20\}$
- $Ap(S, 9) = \{0, 5, 7, 10, 12, 15, 17, 20, 22\}$

iii) Se verifican las proposiciónes 2.4 y 2.5 para cada $Ap(S, n)$, que se halló:

- Con $Ap(S, 5)$: $F(S) = max(Ap(S, 5)) - 5 = 18 - 5 = 13$,
$$g(S) = \frac{1}{5}(0 + 7 + 9 + 16 + 18) - \frac{5-1}{2} = 8.$$
- Con $Ap(S, 7)$: $F(S) = max(Ap(S, 7)) - 7 = 20 - 7 = 13$,
$$g(S) = \frac{1}{7}(0 + 5 + 9 + 10 + 15 + 18 + 20) - \frac{7-1}{2} = 8.$$
- Con $Ap(S, 9)$: $F(S) = max(Ap(S, 9)) - 9 = 22 - 9 = 13$,
$$g(S) = \frac{1}{9}(0 + 5 + 7 + 10 + 12 + 15 + 17 + 20 + 22) - \frac{9-1}{2} = 8.$$

Una tabla de doble entrada, como la que se muestra abajo, es util para generar a un semigrupo numérico que se genera con 2 enteros a y b, tales que $MCD(a, b) = 1$.

0	a	2a	3a	4a	$\cdots$
b	a+b	2a+b	3a+b	4a+b	$\cdots$
2b	a+2b	2a+2b	3a+2b	4a+2b	$\cdots$
3b	a+3b	2a+3b	3a+3b	4a+3b	$\cdots$
4b	a+4b	2a+4b	3a+4b	4a+4b	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tabla 1

De aquí, se tiene que

$$S = \langle\{a, b\}\rangle = \{0, a, 2a, 3a, \ldots, b, 2b, 3b, \ldots, a + b, 2a + b, a + 2b, 3a + b, a + 3b, \ldots\}.$$

También de la tabla 1 se halla fácilmente $Ap(S, a)$, cuyos elementos están ubicados en la primera columna de la tabla, pero solamente hasta la fila *a-ésima*, esto es hasta el elemento $(a - 1)b$, ya que son los únicos que al restarle a, generan elementos que no pertenecen a S, puesto que con el siguiente elemento ab, al restarle a se obtendrá $(b - 1)a$ que si está en S, ubicándose en la primera fila de la tabla. Si se quisiera $Ap(S, 2a)$, todos sus elementos están en las dos primeras columnas, pero solo hasta la fila *a-ésima*. Luego, para un semigrupo numérico S, generado por dos enteros positivos diferentes, tal que $MCD(a,b) = 1$, su conjunto Apery viene dado por

$$Ap(S,a) = \{0, b, 2b, 3b, \dots, (a-1)b\}. \tag{2.2}$$

Proposición 2.8. *Sean a y b enteros positivos con $MCD(a,b) = 1$ y sea S el semigrupo numérico generado por a y b, entonces*

1. *Su número de Fobenius está dado por $F(S) = (a-1)(b-1) - 1$.*

2. *El genero está dado por $g(S) = \frac{(a-1)(b-1)}{2}$.*

Demostración. Utilizando la proposición 2.4, se prueba el primer item. Se tiene que $F(S) = max[Ap(S,a)] - a$, pero de (2.2) se tendrá que $F(S) = [(a-1)b] - a$, que al efectuar resulta $F(S) = ab - b - a = (a-1)(b-1) - 1$.

El segundo item, se sigue de la proposición 2.5. Además, usando el conjunto Apery, que se ha deducido de la tabla 1, en (2.2) se obtiene

$$g(S) = \tfrac{1}{a}(0 + b + 2b + 3b + \dots + (a-1)b) - \tfrac{n-1}{2}$$
$$g(S) = \tfrac{1}{a}\tfrac{(a-1)ab}{2} = \tfrac{ab-a-b-1}{2},$$
$$\text{luego: } g(S) = \tfrac{(a-1)(b-1)}{2}.$$

□

La proposición 2.8 nos asegura que, en semigrupos numéricos de dimensión inmersa $e(S) = 2$, siempre se cumplirá que $g(S) = \frac{F(S)-1}{2}$.

2.2. Conjunto de lagunas a partir del $Ap(S,n)$

El conjunto Apery tiene también otra utilidad. A partir del conjunto $Ap(S,n)$ puede obtenerse el conjunto de lagunas $L(S)$. De la proposición 2.5 se conoce que el género o cardinal del conjunto de lagunas, está dado por

$$g(S) = \frac{1}{n}(\sum_{w \in Ap(S.n)} w) - \frac{n-1}{2},$$

pero ¿como se hallan los elementos de $L(S)$, a partir del $Ap(S,n)$?

Mediante la siguiente proposición podemos identificar a los elementos de $L(S)$. Para ello, previamente se define el siguiente conjunto:

$$H_n = \{w - kn : w \in Ap(S,n), k \in \mathbb{N}, w - kn > 0\}.$$

Proposición 2.9. *Sean S un semigrupo numérico, $n \in S^*$ y su conjunto Apery en n, $Ap(S,n) = \{w_0, w_1, w_2, \ldots, w_{n-1}\}$. Entonces $H_n(S) = L(S)$.*

Demostración. Primero probemos que: $H_n(S) \subset L(S)$. Sea $h \in H_n(S)$, entonces $h = w - kn$. Dado que en el conjunto Apery están todos los elemento de S que disminuidos en n son elementos de $\mathbb{N} \setminus S$, para cada $w \in Ap(S,n)$ se tendrá que $w - n \notin S$ entonces $w - n \in L(S)$, siempre que $w - n > 0$. Pero también $w - 2n \notin S$ entonces $w - 2n \in L(S)$, siempre que $w - 2n > 0$, pues si suponemos que $w - 2n \in S$, entonces $(w - 2n) + n = w - n \in S$, lo cual es una contradicción. También $w - 3n \notin S$ entonces $w - 3n \in L(S)$, siempre que $w - 3n > 0$. Luego, en general $w - kn \in L(S)$, siempre que $w - kn > 0$. Así $h \in L(S)$.

Ahora probaremos que $L(S) \subset H_n(S)$. Sea $h \in L(S)$, entonces $h \in \mathbb{N} \setminus S$. Además, dado que los elementos que no están en S, son una cantidad finita, entonces necesariamente existe un entero mínimo k', tal que $h + k'n \in S$, ya que si no existiera tal k', habría un número ilimitado de lagunas y sabemos que el género de S es finito. Luego, si a este elemento $h + k'n \in S$, le restáramos n entonces $(h + nk') - n$ ya no estaría en S, pues $h + k'n \in S$ con un mínimo valor de k', entonces $h + k'n = w \in Ap(S,n)$ de donde se tiene que $h = w - k'n$ y entonces si $w - k'n > 0$, se tendrá que $h \in H_n(S)$. Con lo cual se concluye la prueba. ☐

De lo anterior se deduce que todas las lagunas de S, son obtenidas a partir del $Ap(S,n)$ restando múltiplos de n a sus elementos, mientras esta resta sea positiva.

Ejemplo 2.10. Sea $Ap(S,8) = \{0, 4, 9, 13, 15, 18, 19, 22\}$, de algún semigrupo numérico S. Se puede hallar $L(S)$ usando el procedimiento anterior. Dado que $n = 8$, entonces los elementos de $L(S)$ serán:

22-8=14, 14-8=6,

19-8=11, 11-8=3,

18-8=10, 10-8=2,

15-8=7,

13-8=5,

9-8=1.

Coleccionando todos estos enteros se obtiene

$$L(S) = \{1, 2, 3, 5, 6, 7, 10, 11, 14\},$$

del cual se tiene que $g(S) = 9$. Esto puede comprobarse haciendo uso de la fórmula dada en la proposición 2.5, así:

$$g(S) = \frac{1}{8}(0 + 4 + 9 + 13 + 15 + 18 + 19 + 22) - \frac{8-1}{2} = 9.$$

Además, el número de Frobenius es 14 y se obtiene directamente del conjunto $L(S)$. Pero también usando la fórmula de la proposición 2.4, se comprueba que es $F(S) = 22 - 8 = 14$. Como $L(S) = \mathbb{N} \setminus S$ entonces $S = \mathbb{N} \setminus L(S)$, luego se puede hallar el semigrupo numérico, mediante el complemento de $L(S)$:

$$S = \{0, 4, 8, 9, 12, 13, 15, 16, 17, 18, \rightarrow\}.$$

Como conclusión, mencionamos que, teniendo un conjunto Apery, puede determinarse $L(S)$ y luego el semigrupo numérico S.

Acabamos de ver como se obtiene un semigrupo numérico, si se tiene un conjunto de n números que forman un $Ap(S, n)$. Pero ahora, si se tiene una colección de n números enteros diferentes y no negativos $x_0, x_1, \cdots, x_{n-1}$, ¿formarán estos un $Ap(S, n)$? Pues no necesariamente. Cada uno de los n números x_i deben ser congruentes con i módulo n. Así $x_i = k_i n + i$, donde $i = 0, 1, 2, \cdots, n-1$ y $x_0 = 0$. Pero esta condición no es suficiente. Veamos el caso siguiente.

Ejemplo 2.11. Sea el conjunto $X = \{0, 5, 11, 22\}$. Notemos que $n = 4$ y además

$$0=4(0)+0, \qquad 5=4(1)+1, \qquad 22=4(5)+2, \qquad 11=4(2)+3,$$

y a pesar que cada elemento x_i es congruente a i, módulo n, no puede ser el $Ap(S, 4)$ de un semigrupo numérico S, ya que, si lo fuera, entonces

$$\begin{array}{cccc} 22\text{-}4=18, & 18\text{-}4=14, & 14\text{-}4=10, & 10\text{-}4=6, \\ 6\text{-}4=2, & 11\text{-}4=7, & 7\text{-}4=3, & 5\text{-}4=1 \end{array}$$

se habría formado $L(S) = \{1, 2, 3, 6, 7, 10, 14, 18\}$, el cuál sería el conjunto de lagunas y por ello $S = \mathbb{N} \setminus L(S) = \{0, 4, 5, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 22, \cdots\}$, sería su semigrupo numérico, lo cuál no es cierto pues se aprecia que algunos elementos de $L(S)$, como 10, 14 y 18, pueden ser generados por elementos de S, así:

$$10 = 5 + 5, \ 14 = 9 + 5, \ 18 = 9 + 9.$$

Luego, el conjunto X no puede ser $Ap(S,4)$ de un semigrupo numérico S.

Ejemplo 2.12. Sea el conjunto $X = \{0, 7, 13, 22\}$. Aquí $n = 4$ y además

$$0{=}4(0){+}0, \qquad 13{=}4(3){+}1, \qquad 22{=}4(5){+}2, \qquad 7{=}4(1){+}3.$$

Este conjunto X, tampoco puede ser un conjunto Apery. Si fuera $Ap(S,4)$ de algún semigrupo numérico S, entonces se tendría $L(S) = \{1, 2, 3, 5, 6, 9, 10, 14, 18\}$ y entonces $S = \mathbb{N} \setminus L(S) = \{0, 4, 7, 8, 11, 12, 13, 15, 16, 17, 19, 20, 21, 22, \ldots\}$, el cuál no puede ser semigrupo numérico, pues hay elementos de $L(S)$, que son generados por elementos de S.

2.3. Test de comprobación de un conjunto Apery

Como ya se vió en los ejemplos 2.11 y 2.12, no todos los conjuntos X de n enteros diferentes y no negativos, formarán un conjunto Apery. En esta sección, se da un test que permite detectar si este conjunto X, es o no, un conjunto Apery $Ap(S,n)$ de algún semigrupo numérico. Es decir, sin tener el semigrupo numérico y solo teniendo a un conjunto de n enteros (no negativos y diferentes), se determinará si forman o no, algún $Ap(S,n)$.
Sean n enteros no negativos y diferentes, tales que

$$x_0 < x_1 < x_2 < \cdots < x_{n-1}$$

siendo $x_0 = 0$ y cada $x_i = kn + j_i$ donde $j_i \in \{1, 2, 3, \cdots, n-1\}$, para i entero de 1 a $n-1$, con la condición de que todos los j_i adopten valores diferentes.
Sea, además la siguiente *ecuación diofántica*

$$x_i - n = \alpha n + \alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_{i-1} x_{i-1}.$$

Iniciar con $i = 1$.

1. Se remplaza en la ecuación diofántica

2. Se resuelve la ecuación diofántica.

   - Si existen valores no negativos de los α_i se concluirá que el conjunto $X = \{x_0, x_1, x_2, \ldots, x_{n-1}\}$ no puede ser un Apery $Ap(S,n)$ de algún semigrupo numérico S.
     FIN.

- Si no existen los valores no negativos, de todos los α_i, entonces: CONTINUAR CON EL PASO 3.

3. Se analiza con $i := i + 1$

   - Si $i \leq n - 1$ ir al paso 1.
   - Si $i = n$ se concluye que, $X = \{x_0, x_1, x_2, \ldots, x_{n-1}\}$ si es un conjunto Apery $Ap(S, n)$, de algún semigrupo numérico S.
   FIN.

Ejemplo 2.13. Sea la colección de enteros siguiente

$$X = \{0, 4, 9, 13, 15, 18, 19, 22\}.$$

¿Será este conjunto, el Apery de algún semigrupo numérico S ?
Aquí $n = 8$ y además:
$x_0 = 0 = 0(8) + 0 \to j_0 = 0$
$x_1 = 4 = 0(8) + 4 \to j_1 = 4$
$x_2 = 9 = 1(8) + 1 \to j_2 = 1$
$x_3 = 13 = 1(8) + 5 \to j_3 = 5$
$x_4 = 15 = 1(8) + 7 \to j_4 = 7$
$x_5 = 18 = 2(8) + 2 \to j_5 = 2$
$x_6 = 19 = 2(8) + 3 \to j_6 = 3$
$x_7 = 22 = 2(8) + 6 \to j_7 = 6$
Aplicamos el Test
Sea $i = 1$:
$x_1 - 8 = 8\alpha + 0 \to 4 - 8 = 8\ \alpha \to$ no existe α entero.
Sea $i = 2$:
$x_2 - 8 = 8\alpha + 0 + 4\alpha_1 \to 9 - 8 = 8\alpha + 4\alpha_1 \to$ no existe α, ni α_1 enteros.
Sea $i = 3$:
$x_3 - 8 = 8\alpha + 0 + 4\alpha_1 + 9\alpha_2 \to 13 - 8 = 8\alpha + 4\alpha_1 + 9\alpha_2 \to$ no existe α, ni α_1, ni α_2 enteros.
Sea $i = 4$:
$x_4 - 8 = 8\alpha + 0 + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 \to 15 - 8 = 8\alpha + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 \to$ no existen valores enteros no negativos de α y de los α_i.
Sea $i = 5$:
$x_5 - 8 = 8\alpha + 0 + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 + 15\alpha_4 \to 18 - 8 = 8\alpha + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 + 15\alpha_4 \to$ no existen valores enteros no negativos de α y de los α_i.
Sea $i = 6$:

$x_6 - 8 = 8\alpha + 0 + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 + 15\alpha_4 + 18\alpha_5 \rightarrow 19 - 8 = 8\alpha + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 + 15\alpha_4 + 18\alpha_5 \rightarrow$ no existen valores enteros no negativos de α y de los α_i.
Sea $i = 7$:
$x_7 - 8 = 8\alpha + 0 + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 + 15\alpha_4 + 18\alpha_5 + 19\alpha_6 \rightarrow 22 - 8 = 8\alpha + 4\alpha_1 + 9\alpha_2 + 13\alpha_3 + 15\alpha_4 + 18\alpha_5 + 19\alpha_6 \rightarrow$ no existen valores enteros no negativos de α, ni de los α_i.
Y se llega a $i = 8$. Según el test presentado, el conjunto

$$X = \{0, 4, 9, 13, 15, 18, 19, 22\},$$

si es un conjunto Apery de algún semigrupo numérico S. Luego, no se tiene aún el semigrupo numérico S, pero ya se tiene su conjunto Apery, denotado $Ap(S, 8) = X$. Utilizando el procedimiento dado en la sección anterior, podrá hallarse el semigrupo numérico correspondiente.

Ejemplo 2.14. El conjunto $X = \{0, 7, 13, 22\}$ ¿Será un conjunto Apery de algún semigrupo numérico?
Aquí $n = 4$ y además:
$x_0 = 0 = 0(4) + 0 \rightarrow j_0 = 0$
$x_1 = 7 = 1(4) + 3 \rightarrow j_1 = 3$
$x_2 = 13 = 3(4) + 1 \rightarrow j_2 = 1$
$x_3 = 22 = 5(4) + 2 \rightarrow j_3 = 2$
Sea $i = 1$:
$x_1 - 4 = 4\alpha + 0 \rightarrow 7 - 4 = 4\alpha \rightarrow$ no existe α entero.
Sea $i = 2$:
$x_2 - 4 = 4\alpha + 0 + 7\alpha_1 \rightarrow 13 - 4 = 4\alpha + 7\alpha_1 \rightarrow$ no existe α, ni α_1 enteros no negativos.
Sea $i = 3$:
$x_3 - 4 = 4\alpha + 0 + 7\alpha_1 + 13\alpha_2 \rightarrow 22 - 4 = 4\alpha + 7\alpha_1 + 13\alpha_2 \rightarrow$ Aquí si existen valores de los α y α_i enteros no negativos, que satisfacen la ecuación Diofántica:
$18 = 4\alpha + 7\alpha_1 + 13\alpha_2$ se satisface con $\alpha = 1$, $\alpha_1 = 2$ y $\alpha_2 = 0$, por lo tanto, de acuerdo al test dado, el conjunto $X = \{0, 7, 13, 22\}$ no puede ser un conjunto Apery, de algún semigrupo numérico S.

2.4. Semigrupo numérico asociado a un elemento generador

Se sabe que, si $\{a_1, a_2, \ldots, a_n\}$ es un conjunto generador de un semigrupo numérico S, entonces $MCD(a_1, a_2, \ldots, a_n) = 1$; pero puede ocurrir que sin contar al entero a_n, los otros $n-1$ enteros de tal generador, tengan un máximo común divisor d, entonces dividiendo a cada uno de estos números entre d, se hallará otro conjunto $\left\{\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{n-1}}{d}\right\}$ cuyo MCD es 1. Pero dado que el entero a_n no tenía divisor común con los otros $n-1$ enteros, entonces, puede ser añadido a este último conjunto y se hallará otro conjunto con MCD igual a 1, que puede funcionar como un nuevo conjunto generador de otro semigrupo numérico, al que se denominará: *semigrupo numérico asociado al elemento generador* a_n. Nótese además, que si los $n-1$ enteros restantes tienen MCD igual a 1, entonces el semigrupo numérico asociado al elemento generador a_n sería el mismo semigrupo numérico S. A continuación se da su definición.
Sea $S = \langle\{a_1, a_2, \ldots, a_n\}\rangle$ tal que $MCD(a_1, a_2, \ldots, a_{n-1}) = d$, entonces el *semigrupo numérico asociado al elemento generador* a_n *de* S, se denotará mediante $S[a_n]$ y queda determinado mediante

$$S[a_n] = \langle\left\{\tfrac{a_1}{d}, \tfrac{a_2}{d}, \ldots, \tfrac{a_{n-1}}{d}, a_n\right\}\rangle.$$

Ejemplo 2.15. Sea $S = \langle\{6, 8, 9\}\rangle$, como $MCD(6, 8) = 2$, entonces el semigrupo numérico asociado al elemento generador a_3, será

$$S[a_3] = \langle\{3, 4, 9\}\rangle = \langle\{3, 4\}\rangle.$$

Un caso particular, es el siguiente: Si $MCD(a_1, a_2, \ldots, a_{n-1}) = 1$, entonces $S[a_n] = S$.

Seguidamente, se presenta algunos resultados dados en [16].

Lema 2.16. *Sea* S *un semigrupo numérico generado por* $\{a_1, a_2, \ldots, a_n\}$*, donde* $MCD(a_1, a_2, \ldots, a_{n-1}) = d$*, entonces*

$$Ap(S, a_n) = d(Ap(S[a_n], a_n)).$$

Demostración. Probamos primero que $Ap(S, a_n) \subseteq d.(Ap(S[a_n], a_n))$. Para ello, considérese que $w \in Ap(S, a_n)$, entonces por definición de Apery, $w \in S$ y además $w - a_n \notin S$, luego $w \in \langle a_1, a_2, \ldots, a_{n-1}\rangle$. En el caso que $w = \sum\limits_{1}^{n} \alpha_i a_i$ con α_n entero

positivo, entonces $w - a_n \in S$, lo cual sería una contradicción.
Dado que por condición, $d = MCD(a_1, a_2, \ldots, a_{n-1})$, entonces $w \in d.\langle \frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{n-1}}{d} \rangle$.
Luego, $\frac{w}{d} \in \langle \frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{n-1}}{d} \rangle \subseteq S[a_n]$ y así, $\frac{w}{d} \in S[a_n]$; faltando probar únicamente que $\frac{w}{d} - a_n \notin S[a_n]$, para afirmar que $\frac{w}{d} \in Ap(S[a_n], a_n)$. Supongamos que $\frac{w}{d} - a_n$ está en $S[a_n]$, entonces se tendrá $\frac{w}{d} - a_n = \sum_{1}^{n-1} (\alpha_i \frac{a_i}{d}) + \beta.a_n$ y de aquí, se despeja $\frac{w}{d}$, obteniéndose $\frac{w}{d} = \sum_1^{n-1} (\alpha_i \frac{a_i}{d}) + (\beta + 1).a_n$; luego $w = \sum_1^{n-1} (\alpha_i a_i) + (\beta d + d) a_n$.
Aquí restamos a_n en ambos lados y se tendrá:
$w - a_n = \sum_1^{n-1} (\alpha_i a_i) + \underbrace{(\beta d + d - 1)}_{(+)}.a_n \in S$, lo cual es una contradicción.
Por lo tanto $\frac{w}{d} - a_n \notin S[a_n]$. Así se ha probado que $\frac{w}{d}$ es un elemento del conjunto $Ap(S[a_n], a_n)$ y de aquí $w \in d.Ap(S[a_n], a_n)$.

Ahora se prueba lo recíproco, es decir $d.Ap(S[a_n], a_n) \subseteq Ap(S, a_n)$. Consideremos que $w \in Ap(S[a_n], a_n)$, entonces por definición $w \in S[a_n]$ y $w - a_n \notin S[a_n]$, luego $w \in \langle \frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{n-1}}{d} \rangle$. Debe notarse que w no puede generarse con a_n, pues esto llevaría a que $w - a_n \in S[a_n]$, lo que sería una contradición. Ahora, multiplicando todo por d se tendrá: $wd \in \langle a_1, a_2, \ldots, a_{n-1} \rangle \subseteq S$ y de aquí $wd \in S$.
Faltaría probar que $wd - a_n \notin S$, para afirmar que $wd \in Ap(S, a_n)$. Supóngase que $wd - a_n \in S$, entonces $wd - a_n = \sum_1^{n} \alpha_i a_i$, luego $wd = \sum_1^{n-1} (\alpha_i a_i) + (\alpha_n + 1) a_n$.
Pero $MCD(a_1, a_2, \ldots, a_n) = 1$ y $MCD(a_1, a_2, \ldots, a_{n-1}) = d$, luego, $MCD(d, a_n) = 1$, por lo tanto, como $wd = \sum_1^{n-1} (\alpha_i a_i) + (\alpha_n + 1) a_n$, al dividir entre d, se tiene que en $w = \sum_1^{n-1} (\alpha_i . \frac{a_i}{d}) + (\frac{\alpha_n + 1}{d}).a_n$, necesariamente d divide a $(\alpha_n + 1)$ y se obtiene que w no es generado por $\langle \frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{n-1}}{d} \rangle$, lo cual se contradice con el hecho de que w es generado por $\langle \frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{n-1}}{d} \rangle$. Así, $wd - a_n$ no debe estar en S, entonces $wd \in Ap(S, a_n)$ y por ello $w \in \frac{1}{d} Ap(S, a_n)$.
Es decir $Ap(S[a_n], a_n) \subseteq \frac{1}{d} Ap(S, a_n)$ o también $d.Ap(S[a_n], a_n) \subseteq Ap(S, a_n)$.

Luego, está probado que $Ap(S, a_n) = d.(Ap(S[a_n], a_n)$. □

Proposición 2.17. *Dado un semigrupo numérico S, cuyo sistema minimal de generadores está dado por $\{a_1, a_2, \cdots, a_n\}$ y $MCD\{a_1, a_2, \cdots, a_{n-1}\} = d$, entonces*

1. $F(S) = d.F(S[a_n]) + (d - 1).a_n$.

2. $g(S) = d.g(S[a_n]) + \frac{(d-1)(a_n - 1)}{2}$.

Demostración. Sea $F(S)$ el número de Frobenius de S y $g(S)$ el género, correspondiente al conjunto de lagunas de S.

1. Se sabe que
   $F(S) = max(Ap(S, a_n)) - a_n$
   $F(S) = max(d.(Ap(S[a_n], a_n))) - a_n$
   $F(S) = d.max(Ap(S[a_n], a_n)) - a_n$
   $F(S) = d.(max(Ap(S[a_n], a_n)) - a_n + a_n) - a_n$
   $F(S) = d.(F(S[a_n]) + a_n) - a_n$
   $F(S) = d.F(S[a_n]) + (d-1).a_n.$

2. $g(S) = \frac{1}{a_n}(\sum_{w_i \in Ap(S,a_n)} w_i) - \dfrac{a_n - 1}{2}$
   $g(S) = \frac{1}{a_n}(w_0 + w_1 + \cdots + w_{a_n-1}) - \frac{a_n-1}{2}$
   $g(S) = \frac{1}{a_n}(d\frac{w_0}{d} + d\frac{w_1}{d} + \cdots + d\frac{w_{a_n-1}}{d}) - \frac{a_n-1}{2}$
   $g(S) = \frac{1}{a_n}.d(\frac{w_0}{d} + \frac{w_1}{d} + \cdots + \frac{w_{a_n-1}}{d}) - \frac{a_n-1}{2}$
   la expresión entre parentesis, es la expansión de la sumatoria que inteviene, en la fórmula de la proposición 2.5 y así se tiene

   $$g(S[a_n]) = \frac{1}{a_n}(\sum_{w_i \in Ap(S[a_n],a_n)} w) - \frac{a_n - 1}{2},$$

   de aqui se despeja la sumatoria y se reemplaza, en la expresión anterior de $g(S)$, obteniéndose

   $$g(S) = \frac{d}{a_n}.(g(S[a_n]) + \frac{a_n-1}{2}).a_n - \frac{a_n-1}{2}.$$

   Simplificando y efectuando operaciones:

   $$g(S) = d.g(S[a_n]) + \frac{(d-1)(a_n-1)}{2}.$$

□

Ejemplo 2.18. Aplicamos la proposición 2.17 al siguiente semigrupo numérico

$$S = \langle 4, 6, 9\rangle = \{0, 4, 6, 8, 9, 10, 12, \rightarrow\}.$$

De aquí $F(S) = 11$, $L(S) = \{1, 2, 3, 5, 7, 11\}$, $g(S) = 6$, además $d = MCD(4, 6) = 2$ y $a_3 = 9$, luego construimos el semigrupo numérico asociado al elemento a_3 :

$$S[9] = \langle \frac{4}{2}, \frac{6}{2}, 9\rangle = \langle 2, 3, 9\rangle = \langle 2, 3\rangle = \{0, 2, 3, 4, 5, \ldots\} = \{0, 2, 3, \rightarrow\}$$

y se obtiene los siguientes elementos $F(S[9]) = 1$, $L(S[9]) = \{1\}$, $g(S[9]) = 1$, con los cuales se puede comprobar la proposición 2.17.

- $F(S) = d.F(S[9]) + (d-1).a_n$
  $11 = 2(1) + 1 \times 9.$

- $g(S) = d.g(S[9]) + \frac{(d-1)(a_n-1)}{2}$
  $6 = 2(1) + \frac{1\times 8}{2}.$

2.5. Pseudo números de Frobenius

Sea un semigrupo numérico S y sea el entero $F(S)$ su correspondiente número de Frobenius, del cual ya se conoce que $F(S) \notin S$ y para cualquier m entero positivo, se tendrá que $F(S) + m \in S$.

Ahora se hará un cambio en tal definición para obtener un nuevo elemento de los semigrupos numéricos. En lugar de que se cumpla para todo entero positivo, se va a restringir a todo entero positivo de S, obteniéndose así un nuevo elemento que se denominará *pseudo-número de Frobenius* y que ahora se denotará mediante $f(S)$ o tambien simplemente, mediante f, si es que el semigrupo numérico, ya es sobreentendido como S.
Se da a continuación su definición: Si el entero $f(S)$ es tal que $f(S) \notin S$ y $f(S)+s \in S$ para todo $s \in S^*$, entonces $f(S)$ será un *pseudo-número de Frobenius.*

A diferencia del número de Frobenius que es único, para cada semigrupo numérico, ahora puede tenerse varios pseudo-números de Frobenius y de darse este caso, en su notación se agregará un sub-índice, como se aprecia en el siguiente:

Ejemplo 2.19. Sea el semigrupo numérico $S = \langle\{3, 5, 7\}\rangle = \{0, 3, 5, 6, 7, 8, \rightarrow\}$.
Hay 2 enteros que cumplen la definición de pseudo-número de Frobenius:
$f_1(S) = 2$ y $f_2(S) = 4$. Además $F(S) = 4 = f_2(S)$.

Algunas definiciones adicionales:
$PF(S)$ es el *conjunto de los pseudo-números de Frobenius.*
$t(S) = card(PF(S))$ será denominado *tipo* del semigrupo numérico S.

En el ejemplo 2.19, $PF(S) = \{2, 4\}$ y $t(S) = 2$.

Ejemplo 2.20. El conjunto de los enteros no negativos, es también un semigrupo numérico y para este caso: $F(S) = -1$. Aquí, el único pseudo-número de Frobenius es $f = -1$. Además, $PF(S) = \{-1\}$ y $t(S) = 1$.

El único caso en el cual $F(S)$ es negativo y además $PF(S)$ contiene a un negativo, sucede cuando se considera que $S = \mathbb{N}$.

Nótese que $PF(S)$ es un conjunto no vacío, ya que, como se aprecia en el ejemplo 2.19, el número de Frobenius $F(S)$, es también un pseudo-número de Frobenius, ya que $F(S) \notin S$ y cumple con la definición de pseudo-número de Frobenius, pues para todo $s \in S^*$, se verifica que $F(S) + s \in S$.

También se cumple que $F(S) = max(PF(S))$.

En el caso que se tenga varios pseudo- números de Frobenius, cada uno de estos, serán elementos maximales de una cadena de números, que se enlazan entre si, mediante la siguiente relación de orden, que se determina para enteros:

$$x \leq_S y \quad \leftrightarrow \quad y - x \in S.$$

En efecto, para enteros positivos, negativos o nulo y considerando al semigrupo numérico S:

- La relación $\leq_S$ es reflexiva: Pues para todo entero $x : x - x = 0 \in S$ y por tanto $x \leq_S x$.
- La relación $\leq_S$ es transitiva: Sean los enteros x, y, z, tales que $x \leq_S y \wedge y \leq_S z$ entonces $y - x \in S \wedge z - y \in S$ y al sumar ambas desigualdades
$$(y - x) + (z - y) = z - x \in S \rightarrow x \leq_S z.$$
- La relación $\leq_S$ es anti-simétrica:
Sean los enteros x, y tales que $x \leq_S y \wedge y \leq_S x$ entonces $y - x \in S \wedge x - y \in S$
Si $x \neq y \rightarrow$ una de las diferencias $x - y$ ó $y - x$ será negativa, lo cual no puede ser en S, entonces, debe tenerse que $x = y$.

Con la relación de orden $\leq_S$ que se ha definido, para enteros, se puede obtener el conjunto $Maximales_{\leq_S}(L(S))$, que contiene a todos los elementos maximales del conjunto finito $L(S)$, es decir contiene a elementos de $L(S)$ que no son excedidos, por los elementos de alguna cadena de números, bajo la relación de orden definida.

Ahora se comprobará que efectivamente la colección de todos los maximales de $L(S)$, bajo la relación de orden $\leq_S$, dará todo el conjunto de pseudo-números de Frobenius.

(1) Primero se prueba que $PF(S) \subseteq Maximales_{\leq_S}(L(S))$: tomemos $f \in PF(S)$, entonces por su definición $f \notin S$ y también para todo elemento no nulo de S: $f+s$ debe

estar en S. Supóngase que existe una laguna y tal que $f \leq_S y$ es decir, $y - f = s \in S$. Entonces, como $f \in PF(S) : f + s = f + (y - f) = y \in S$, lo cual se contradice con la suposición de que y es una laguna. Esto implica que no existe un elemento fuera de S, que supere a f, según la relación $\leq_S$ y por ello, f es un maximal de $L(S)$ bajo la relación $\leq_S$.

(2) Ahora se prueba que $PF(S) \supseteq Maximales_{\leq_S}(L(S))$:
Sea $x \in Maximales_{\leq_S}(L(S))$, entonces no puede existir elemento de $L(S)$ que supere a x, bajo la relación de orden $\leq_S$. Si se supone que para algún $s \in S$ existe $y \notin S$ tal que $x + s = y$, entonces $y - x = s \in S$, lo que implica que $x \leq_S y$, contradiciéndose al hecho de que x es maximal de $L(S)$ bajo la relación de orden definida.
Luego, para todo s de S, $x + s = y$ con $y \in S$. De donde se concluye que $x \in PF(S)$

Así, se ha demostrado lo siguiente:

Proposición 2.21. *En todo semigrupo numérico S, con pseudo-números de Frobenius positivos, se cumple que:*

$$PF(S) = Maximales_{\leq_S}(L(S)).$$

De esta proposición puede notarse que el conjunto de lagunas $L(S)$ y el conjunto de pseudo-números de Frobenius $PF(S)$ están relacionados y por lo tanto sus elementos también.

La siguiente proposición, será denominada, *caracterización de las lagunas de un semigrupo numérico.*

Proposición 2.22. *El entero l es una laguna de un semigrupo numérico S, si y solo si, para algún pseudo número de Frobenius de S: $f - l \in S$.*

Demostración. Sea l una laguna de S, entonces bajo la relación de orden $\leq_S$ restringida ahora a $L(S)$, debe suceder que l debe pertenecer a alguna cadena de números y por lo tanto existirá un elemento $f \in L(S)$ tal que $l \leq_S f$, es decir $f - l \in S$. Como $L(S)$ es finito, se puede elegir como f al mayor de todos aquellos que satisfacen la relación $l \leq_S f$ y así, $f \in Maximales_{\leq_S}(L(S))$. Luego por la proposición 2.21, $f \in PF(S)$ y $f - l \in S$.

Recíprocamente, considérese ahora que, para algún $f \in PF(S)$, se verifica que $f - l \in S$, entonces, si se supone que $l \in S$, puede deducirse que $(f - l) + l = f \in S$, lo que sería una contradicción al hecho de que $f \in PF(S)$. Luego $l \notin S$, es decir $l \in L(S)$. □

Ahora la relación de orden $\leq_S$, será restringida a un conjunto Apery de S y la proposición siguiente, sera denominada, *caracterización de los pseudo-números de Frobenius.*

Proposición 2.23. *El entero f es un pseudo-número de Frobenius de un semigrupo numérico S, si y solo si, para algún $w \in Maximales_{\leq_S}(Ap(S,s))$ con $s \in S^*$ se cumple que $f = w - s$.*

Demostración. Sea s un elemento de S^*, siendo S un semigrupo numérico.
Considérese el pseudo-número de Frobenius f, entonces por definición $f \notin S$ y $f + s \in S$. Entonces $f + s \in Ap(S,s)$ pues $(f+s) - s = f \notin S$. Ahora se considera un $w \in Ap(S,s)$, tal que $f + s \leq_S w$, mas aún, se le elegirá como el mayor entero del $Ap(S,s)$, que supere a $f + s$ bajo la relación $\leq_S$, entonces w es un maximal de $Ap(S,s)$ bajo la relación $\leq_S$ y esto implica que $w - (f+s) = m \in S$.
De aquí $w - s = f + m$ y como $w \in Ap(S,s)$ entonces $w - s \notin S$, es decir $f + m \notin S$.
Además, como $m \in S$, se tiene dos posibilidades: $m = 0$ o $m \neq 0$.
Si se considera que $m \neq 0$ entonces por definición de pseudo-número de Frobenius, $f + m \in S$; lo que genera una contradicción y por ello, necesariamente $m = 0$ y así $w - (f+s) = 0$, implicando que $f = w - s$ y $w \in Maximales_{\leq_S}(Ap(S,s))$.

Sea $x = w - s$, siendo w un elemento maximal en $Ap(S,s)$, bajo la relación de orden $\leq_S$, entonces, $x \notin S$. Supóngase ahora, que para algún $y \in S^*$, se cumple que $x + y \notin S$, entonces $(w - s) + y \notin S$. Luego $(w + y) - s \notin S$, de lo cual se deduce que $w + y \in Ap(S,s)$ y dado que también $w \in Ap(S,s)$ entonces $w \leq_S w + y$ lo que implicaría que w no sería un maximal de $Ap(S,n)$, llevando a una contradicción y por ello, necesariamente debe cumplirse que, para todo $y \in S^*$, se tiene que $x + y \in S$.
Así $x \in PF(S)$. □

Ejemplo 2.24. Retomamos el ejemplo 2.19, en el cual $S = \langle\{3,5,7\}\rangle$. Luego, se tiene $S = \{0,3,5,6,7,8,9,10,\ldots\}$, $L(S) = \{1,2,4\}$, $g(S) = 3$ y $F(S) = 4$. Se obtendrá el conjunto $PF(S)$, hallando un conjunto Apery y luego usando la proposición 2.23.
Sea $Ap(S,9) = \{0,3,5,6,7,8,10,11,13\}$ en el cual se forman las siguientes cadenas de orden:

$$0 \leq_S 3 \leq_S 6 \leq_S 11$$
$$0 \leq_S 5 \leq_S 8 \leq_S 11$$

$$0 \leq_S 13.$$

Estas comparaciones se dan pues:

$$3 - 0 = 3 \in S,\ 6 - 3 = 3 \in S,\ 11 - 6 = 5 \in S.$$
$$5 - 0 = 5 \in S,\ 8 - 5 = 3 \in S,\ 11 - 8 = 3 \in S.$$
$$13 - 0 = 13 \in S.$$

Luego: $Maximales_{\leq_S} Ap(S,9) = \{11, 13\}$ y usando la caracterización de los pesudo-números de Frobenius, dado en la proposición 2.23, los elementos de $PF(S)$, se hallarán restando 9, a cada elemento de $Maximales_{\leq_S} Ap(S,9)$.
Así: $PF(S) = \{2, 4\}$.

Proposición 2.25. *Si S es semigrupo numérico con dimensión inmersa igual a dos, entonces $t(S) = 1$.*

Demostración. Como ya se vió antes, para semigrupos numéricos $S = \langle\{a, b\}\rangle$, siendo $MCD(a, b) = 1$, es útil considerar nuevamente la tabla 1.

0	a	2a	3a	4a	$\cdots$
b	a+b	2a+b	3a+b	4a+b	$\cdots$
2b	a+2b	2a+2b	3a+2b	4a+2b	$\cdots$
3b	a+3b	2a+3b	3a+3b	4a+3b	$\cdots$
4b	a+4b	2a+4b	3a+4b	4a+4b	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tabla 1

Aquí todos los elementos que forman parte de la tabla, pertenecen a S.
Para determinar un conjunto Apery, por ejemplo $Ap(S, b)$, basta con tomar todos los elementos de la primera fila, pero hasta la columna $b - \acute{e}sima$; es decir

$$Ap(S, b) = \{0, a, 2a, 3a, \dots, (b-1)a\}.$$

Aquí se establece la siguiente relación de orden:

$$0 \leq_S a \leq_S 2a \leq_S 3a \leq_S \cdots \leq_S (b-1)a.$$

Luego, solo existe un elemento maximal que es $(b-1)a$ y por ello, usando la proposición 2.23, se obtiene $PF(S) = \{(b-1)a - b\}$ y entonces $t(S) = 1$. $\square$

Proposición 2.26. *Sea S un semigrupo numérico. Si $t(S) = 1$ entonces*

- $g(S) = n(S)$.
- $F(S) = 2g(S) - 1$.

Demostración. Sea S el semigrupo numérico, en el cual $L(S) = \{l_1, l_2, \dots, l_g\}$, $N(S) = \{s_1, s_2, \dots, s_n\}$, $PF(S) = \{F(S)\}$.
Debido a la caracterizacion para lagunas: $l_x \in L(S)$ si y solo sí, existe $f \in PF(S)$ tal que $f - l_x = s_x \in S$.
Como aquí solo hay un pseudo-número de Frobenius, entonces, la f que se menciona es $F(S)$. Luego, $L(S)$, $N(S)$ y $PF(S)$ se pueden relacionar mediante una función biyectiva, definida por la siguiente tabla:

$L(S)$	$\Leftrightarrow$	$PF(S)$	$N(S)$
l_1	$\leftrightarrow$	$F(S)$	s_n
l_2	$\leftrightarrow$	$F(S)$	s_{n-1}
$\vdots$		$\vdots$	$\vdots$
l_g	$\leftrightarrow$	$F(S)$	s_1

Tabla 2

La biyección entre los conjuntos $L(S)$ y $PF(S) \times N(S)$ está justificada por la caracterización de lagunas, dada en la proposición 2.22. Por lo tanto, tendrán la misma cantidad de elementos: $card(L(S)) = card(PF(S) \times N(S))$, de donde $g(S) = (1)(n(S))$ y entonces $g(S) = n(S)$.
Además, como siempre se debe cumplir que $c(S) = g(S) + n(S)$, entonces de aquí se obtiene $F(S) + 1 = g(S) + g(S)$, de donde $F(S) = 2g(S) - 1$. □

Proposición 2.27. *Para todo semigrupo numérico S, se cumple la siguiente desigualdad*

$$g(S) \leq t(S).n(S).$$

Demostración. Similar a demostración de la proposición 2.26, pero ahora se tiene $PF(S) = \{f_1, f_2, \dots, f_t\}$ y debido a ello, ahora no necesariamente se cumple que $card(L(S)) = card(PF(S) \times N(S))$. Usamos nuevamente la proposición 2.22, de la cual se tiene que $l_x \in L(S)$ si y solo si, existe $f \in PF(S)$ tal que $f - l_x \in S$. Pero ahora, puede haber mas de una f, por ello, se considera para cada $l_x \in L(S)$, el pseudo número f_x, definido como

$$f_x = min\{f \in PF(S) : f - l_x = s_x \in S\}.$$

Esta f_x que se ha definido para cada l_x, es la que se colocará en la tabla siguiente:

$L(S)$	$\Rightarrow$	$PF(S)$	$N(S)$
l_1	$\rightarrow$	f_{x1}	s_{x1}
l_2	$\rightarrow$	f_{x2}	s_{x2}
$\vdots$		$\vdots$	$\vdots$
l_g	$\rightarrow$	f_{xg}	s_{xg}

Tabla 3

De esta tabla se genera una inyección de $L(S)$ a $PF(S) \times N(S)$, ya que, se deduce una función h que va de $L(S)$ a $PF(S) \times N(S)$ y que se define como

$$h(x) = (f_x; s_x) \text{ siendo } s_x = f_x - x.$$

Comprobamos la inyectividad: sea $h(x) = h(y)$ entonces $(f_x; s_x) = (f_y; s_y)$ e igualando las respectivas componentes: $f_x = f_y$ y $s_x = s_y$ entonces $f_x - x = f_y - y$, de donde se tiene $x = y$.

Dado que ya se probó que es inyectiva, debe cumplirse que

$$card(L(S)) \leq card(PF(S) \times N(S)),$$

luego $g(S) \leq t(S).n(S)$. □

Proposición 2.28. *Dado un semigrupo numérico S (distinto de $\mathbb{N}$), la cantidad de pseudo-números de Frobenius debe ser menor al primer elemento positivo de S; es decir:*

$$t(S) < m(S).$$

Demostración. Sea $PF(S)$ el conjunto de pseudo-números de Frobenius de S. De la proposición 2.23 se tiene que $PF(S) = \{w - n : w \in Maximales_{\leq_S}(Ap(S, n))\}$, entonces, $card(PF(S)) = card\{w - n : w \in Maximales_{\leq_S}(Ap(S, n))\}$. Luego $t(S) = card[Maximales_{\leq_S}(Ap(S, n))] \leq card(Ap(S, n)) - 1$. Esto se cumple, pues $0 \in Ap(S, n)$, pero 0 no puede ser un maximal de $Ap(S, n)$, por lo tanto debe cumplirse $t(S) \leq e(S) - 1$. Pero $e(S) \leq m(S)$ y así se obtiene $t(S) \leq m(S) - 1$.

Con lo que se concluye que $t(S) < m(S)$. □

De las proposiciones 2.27 y 2.28 se deduce que, la cantidad de pseudo-números de Frobenius, satisface lo siguiente

$$\tfrac{g(S)}{n(S)} \leq t(S) < m(S).$$

2.6. Generación de semigrupos numéricos, conociendo el número de Frobenius

Cada semigrupo numérico define a un número de Frobenius, sin embargo lo recíproco no se cumple, es decir, conociendo el número de Frobenius no queda definido un único semigrupo numérico; pueden haber varios, que tengan por número de Frobenius a un entero F dado.

En esta sección, lo que se dárá son casos especiales que permiten obtener semigrupos numéricos conociéndose su número de Frobenius. De hecho, puede haber otros semigrupos numéricos.

CASO 1

Todo entero positivo F, puede ser considerado como el número de Frobenius de algún semigrupo numérico.

Para comprobarlo basta con construir un semigrupo numérico que tenga a F como su número de Frobenius:
Sea F el entero positivo, entonces se tiene que con el semigrupo numérico

$$S = \langle\{F+1, F+2, F+3, \cdots, F+(F+1)\}\rangle,$$

se tendrá $F(S) = F$, ya que S tiene multiplicidad $F+1$ y con la colección

$$F+1, F+2, F+3, \cdots, F+(F+1),$$

puede generarse todos los enteros siguientes, debido a la proposición 1.19.

Ejemplo 2.29. Se dan 2 semigrupos numéricos que cumplen con lo anterior.

- El número 5 es un número de Frobenius, de por lo menos el semigrupo numérico

$$S = \langle\{6, 7, 8, 9, 10, 11\}\rangle.$$

- El número 9 es un número de Frobenius, de por lo menos el semigrupo numérico

$$S = \langle\{10, 11, 12, 13, 14, 15, 16, 17, 18, 19\rangle\}.$$

CASO 2

Dado un número impar positivo F, el semigrupo numérico $S = \langle\{2, F+2\}\rangle$, tendrá como número de Frobenius $F(S) = F$.

Si F es impar, entonces $F \notin \langle 2, F+2 \rangle$ pues si perteneciera, se tendría que

$$2\alpha + (F+2)\beta = F.$$

Entonces necesariamente $\beta = 0$, pues de lo contrario, en la izquierda habría un número mayor que F; pero entonces $2\alpha = F$, lo que sería una contradicción.
Además $F+1$ es un número par y por ello se puede generar, con el 2. También $F+2 \in \langle 2, F+2 \rangle$. Luego, por la proposición 1.19, dado que la multiplicidad de S es 2, basta obtener dos números consecutivos que están en S, para afirmar que todos los enteros siguientes también pertenecen a S.
Además, por la definición de número de Frobenius, se tiene que $F(S) = F$.

Ejemplo 2.30. Se dan 2 semigrupos numéricos.

- El número 17 es número de Frobenius de $S = \langle \{2, 19\} \rangle$.
- El número 35 es número de Frobenius de $S = \langle \{2, 37\} \rangle$.

CASO 3

Si F es múltiplo de 2 pero no múltiplo de 3, puede obtenerse un semigrupo numérico $S = \langle \{3, \frac{F}{2}+3, F+3\} \rangle$, que tendrá como número de Frobenius a $F(S) = F$.
En este caso, F no es múltiplo de 6, es decir, dado que F debe ser par, solo quedan dos posibilidades $F = 6k+2$ o $F = 6k+4$
a) Si $F = 6k+2$ entonces $S = \langle \{3, 3k+4, 6k+5\} \rangle$.

- $6k+2 \notin \langle \{3, 3k+4, 6k+5\} \rangle$, pues no existen enteros no negativos α, β, λ tal que $3\alpha + (3k+4)\beta + (6k+5)\lambda = 6k+2$.
- Además:
  $F+1 = 6k+3 \in \langle \{3\} \rangle$
  $F+2 = 6k+4 \in \langle \{3, 3k+4\} \rangle$, pues $3.k + (3k+4),1 = 6k+4$.
  $F+3 = 6k+5 \in \langle \{6k+5\} \rangle$ y por la proposición 1.19, todos los siguientes enteros estarán en S.
  Así $F = 6k+2 = F(S)$.

b) Si $F = 6k+4$ entonces $S = \langle \{3, 3k+5, 6k+7\} \rangle$

- $6k+4 \notin \langle \{3, 3k+5, 6k+7\} \rangle$, pues no existen enteros no negativos α, β, λ tal que $3\alpha + (3k+5)\beta + (6k+7)\lambda = 6k+4$.

- Además:

  $F + 1 = 6k + 5 \in \langle\{3, 3k + 5\}\rangle$, pues $3.k + (3k + 5)$,$1 = 6k + 5$

  $F + 2 = 6k + 6 \in \langle\{3\}\rangle$

  $F + 3 = 6k + 7 \in \langle\{6k + 7\}\rangle$ y por la proposición 1.19, todos los siguientes enteros estarán en S.

  Así $F = 6k + 4 = F(S)$.

Ejemplo 2.31. Generamos dos semigrupos.

- El número 20, es número de Frobenius de $S = \langle\{3, 13, 23\}\rangle$.
- El número 100, es número de Frobenius de $S = \langle\{3, 53, 103\}\rangle$.

CASO 4

Si F es múltiplo de 2 y 3, pero no múltiplo de 4, puede obtenerse un semigrupo numérico $S = \langle\{4, \frac{F}{2} + 2, \frac{F}{2} + 4\}\rangle$, que tendrá como número de Frobenius a $F(S) = F$.
Hay dos posibilidades $F = 6(4k + 1)$ o $F = 6(4k + 3)$.

a) Si $F = 24k + 6$ entonces $S = \langle\{4, 12k + 5, 12k + 7\}\rangle$.
Sea $P = 4\alpha + (12k + 5)\beta + (12k + 7)\lambda$,:

P	α	β	λ	conclusión
F=24k+6	-	-	-	F$\notin S$
F+1=24k+7	3k	0	1	F+1$\in S$
F+2=24k+8	6k+2	0	0	F+2$\in S$
F+3=24k+9	3k+1	1	0	F+3$\in S$
F+4=24k+10	0	2	0	F+4$\in S$

Tabla 4

Luego $F(S) = F$.

b) Si $F = 24k + 18$ entonces $S = \langle\{4, 12k + 11, 12k + 13\}\rangle$.
Sea $P = 4\alpha + (12k + 11)\beta + (12k + 13)\lambda$:

P	α	β	λ	conclusión
F=24k+18	-	-	-	F$\notin S$
F+1=24k+19	3k+2	1	0	F+1$\in S$
F+2=24k+20	6k+5	0	0	F+2$\in S$
F+3=24k+21	3k+2	0	1	F+3$\in S$
F+4=24k+22	0	2	0	F+4$\in S$

Tabla 5

Luego $F(S) = F$.

CASO 5

Si F es múltiplo de 2, de 3 y de 4, pero no múltilplo de 5, puede obtenerse un semigrupo numérico $S = \langle\{5, \frac{F}{4} + 5, \frac{3F}{4}\}\rangle$, que tendrá como número de Frobenius a $F(S) = F$.

Hay 4 posibilidades:
$F = 12(5k + 1)$, $F = 12(5k + 2)$, $F = 12(5k + 3)$ o $F = 12(5k + 4)$.

a) Si $F = 60k + 12$ entonces $S = \langle\{5, 15k + 8, 45k + 9\}\rangle$.
Sea $P = 5\alpha + (15k + 8)\beta + (45k + 9)\lambda$:

P	α	β	λ	conclusión
F=60k+12	-	-	-	F$\notin S$
F+1=60k+13	9k+1	1	0	F+1$\in S$
F+2=60k+14	3k+1	0	1	F+2$\in S$
F+3=60k+15	12k+3	0	0	F+3$\in S$
F+4=60k+16	6k	2	0	F+4$\in S$
F+5=60k+17	0	1	1	F+5$\in S$

Tabla 6

Luego $F(S) = F$.

b) Si $F = 60k + 24$ entonces $S = \langle\{5, 15k + 11, 45k + 18\}\rangle$.
Sea $P = 5\alpha + (15k + 11)\beta + (45k + 18)\lambda$:

P	α	β	λ	conclusión
F=60k+24	-	-	-	F$\notin S$
F+1=60k+25	12k+5	0	0	F+1$\in S$
F+2=60k+26	9k+3	1	0	F+2$\in S$
F+3=60k+27	9k+1	2	0	F+3$\in S$
F+4=60k+28	3k+2	0	1	F+4$\in S$
F+5=60k+29	0	1	1	F+5$\in S$

Tabla 7

Luego $F(S) = F$.

c) Si $F = 60k + 36$ entonces $S = \langle\{5, 15k + 14, 45k + 27\}\rangle$.
Sea $P = 5\alpha + (15k + 14)\beta + (45k + 27)\lambda$:

P	α	β	λ	conclusión
F=60k+36	-	-	-	F$\notin S$
F+1=60k+37	3k+2	0	1	F+1$\in S$
F+2=60k+38	6k+2	2	0	F+2$\in S$
F+3=60k+39	9k+5	1	0	F+3$\in S$
F+4=60k+40	12k+8	0	0	F+4$\in S$
F+5=60k+41	0	1	1	F+5$\in S$

Tabla 8

Luego $F(S) = F$.

d) Si $F = 60k + 48$, entonces $S = \langle\{5, 15k + 17, 45k + 36\}\rangle$.
Sea $P = 5\alpha + (15k + 17)\beta + (45k + 36)\lambda$:

P	α	β	λ	conclusión
F=60k+48	-	-	-	F$\notin S$
F+1=60k+49	6k+3	2	0	F+1$\in S$
F+2=60k+50	12k+10	0	0	F+2$\in S$
F+3=60k+51	3k	3	0	F+3$\in S$
F+4=60k+52	9k+7	1	0	F+4$\in S$
F+5=60k+53	0	1	1	F+5$\in S$

Tabla 9

Luego $F(S) = F$.

Capítulo 3

SEMIGRUPOS NUMERICOS DE WEIERSTRASS

3.1. Conceptos básicos

Se comienza esta sección, definiendo algunos conceptos que estan inmersos en el desarrollo de la geometría algebraica y en particular en los semigrupos numéricos de Weierstrass.
Existen diversos textos, de donde se puede hallar mas detalles sobre los conceptos que aquí se exponen, entre ellos, puede revisarse [23].

1. *Anillo:* Un anillo, denotado por $(R, +, .)$, es un conjunto no vacío, dotado de dos operaciones, que son la adición y la multiplicación, tal que
   i) El par $(R, +)$ es un grupo abeliano y que tiene como elemento neutro, al *cero*.
   ii) El par $(R, .)$ es un semigrupo y por tanto cumple con la asociatividad.
   iii) La multiplicación debe cumplir con las leyes distributivas respecto de la adición.
   Se denominará *anillo conmutativo con unidad*, cuando la multiplicación es conmutativa y existe el elemento neutro para la multiplicación.
   Puede denotarse al anillo, mediante R, si se considera la adición y multiplicación usuales.

2. *Dominio entero:* Un anillo $(R, +, .)$ es un dominio entero si el *cero* no tiene divisores, es decir, si $a, b \in R$ son tales que $a \neq 0$ y $b \neq 0$ entonces, $a.b \neq 0$.

3. *Ideal:* Sea $(R, +, .)$ un anillo e I un subconjunto de R, entonces I será un *Ideal del anillo* $(R, +, .)$, si $(I, +, .)$ es un subanillo de $(R, +, .)$ y además, para todo

$a \in R$ y para todo $b \in I$, se cumple que $ab \in I$. De aquí se tiene tambien que, si $u, v \in I$ entonces $u - v \in I$.

Un ideal I será *primo* si además cumple que: $a.b \in I$ implica que $a \in I$ o $b \in I$.

Un ideal I será *principal* si está generado por un elemento.

4. *Cuerpo:* Se denomina *cuerpo* a un anillo conmutativo con unidad, en el cual, todo elemento que es distinto de *cero*, es invertible respecto del producto. Se le denotara $(K, +; .)$ o símplemente K, si se considera la adición y multiplicación usuales. Se denotará por $K^* = K \setminus \{0\}$ al grupo multiplicativo del cuerpo K.

5. *Cuerpo algebraicamente cerrado:* denominado así, cuando todo polinomio que tiene coeficientes en K, tiene por lo menos una raíz que está en K. De aquí, se tendrá que, todo polinomio con coeficientes en K, se podrá descomponer en factores lineales.

3.2. Espacio Afín y Espacio Proyectivo

Considerando que K, es un campo algebraicamente cerrado, se define al *espacio afín de dimensión* n sobre K, mediante el producto cartesiano siguiente:

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

En este espacio afín $\mathbb{A}^n(K)$, los conjuntos cerrados serán los conjuntos de ceros de ideales I de $K[X_1, X_2, \ldots, X_n]$; es decir, I será generado por un subconjunto F del anillo de polinomios $K[X_1, X_2, \ldots, K_n]$, y los ceros comunes, en $\mathbb{A}^n(K)$, de los polinomios en F, quedarán contenidos en

$$V(I) = V(\langle F \rangle) = \{(x_1, x_2, \ldots, x_n) \in A^n(K) : f(x_1, x_2, \ldots, x_n) = 0, \text{ para todo } f \in I\}.$$

A este conjunto se le denomina *conjunto algebraico afín*. De esa forma quedará definida una *topología de Zariski* y los conjuntos cerrados de esta topología, son los conjuntos algebraicos afines.

Todos los conjuntos algebraicos afines, son los ceros comunes que se obtienen a partir de un conjunto finito de polinomios, este es el Teorema de la Base de Hilbert [22].

Enunciamos dos propiedades de estos conjuntos algebraicos afines:
i) Dada una colección finita de conjuntos algebraicos afines, su unión también será un conjunto algebraico afín.
ii) Dada una colecćíon arbitraria de conjuntos afines, su intersección también será un conjunto algebraico afín.

Considerese ahora, un ideal primo I_p de $K[X_1, X_2, \ldots, K_n]$, se da a continuación, algunas definiciones:

1. Se denominará *variedad afín*, al conjunto χ que contiene a los ceros del ideal I_p.

2. El anillo $K[\chi] = K[X_1, X_2, \cdots, X_n]/I_P$ será denominado *anillo de coordenadas* de la variedad afín χ. Además $K[\chi]$ es un dominio. Como ejemplo, mencionamos a las coordenadas x_i, las cuales pertenecen a $K[\chi]$ y se les puede ver como funciones $x_i : \chi \to K$, que asignan a cada punto $P = (a_1, \ldots, a_n) \in \chi$, su i-ésima coordenada $x_i(P) = a_i$.

3. Se denotará mediante $K(\chi)$ al cuerpo cociente de $K[\chi]$ y se le denomina, *cuerpo de funciones racionales de la variedad* χ.

4. Se denomina *curva algebraica* a una variedad χ del plano afín $\mathbb{A}^2$, dado por los ceros de un polinomio $f(X,Y) = 0$.

5. Para curvas en $\mathbb{A}^2$, definidas por $f(X,Y) = 0$, se dirá que un punto $P = (a,b)$ de la curva, es no singular, si por lo menos, una de las derivadas parciales f_x o f_y no se anula en P. Si todos los puntos de la curva son no singulares, se le llama curva suave o curva no singular.

En el espacio $\mathbb{A}^{n+1} \setminus \{0\}$, se definirá una relación de equivalencia:

$$(y_0; \ldots ; y_n) \sim (x_0; \ldots ; x_n) \leftrightarrow \lambda \in K^* \text{ tal que, } y_i = \lambda x_i,\ i \in \{0, 1, \ldots, n\}.$$

El espacio proyectivo n-dimensional sobre K, es el cociente

$$\mathbb{P}^n_K = (\mathbb{A}^{n+1}(K) \setminus \{0\})/ \sim.$$

Si el campo K es sobreentendido, puede denotarse este espacio como $\mathbb{P}^n$.

Se considera a los puntos P de $\mathbb{P}^n$, con coordenadas proyectivas $(x_0 : \ldots : x_n)$

$$P = (x_0 : \ldots : x_n) = \{(y_0; \ldots ; y_n) : (y_0; \ldots ; y_n) \sim (x_0; \ldots ; x_n)\}.$$

Puede interpretarse a los puntos de $\mathbb{P}^n$, como el conjunto de rectas que pasan por el origen de $\mathbb{A}^{n+1}$. Dado que la unión de $\{(x_0 : \ldots : x_{n-1} : 1)/(x_0, \ldots, x_{n-1}) \in \mathbb{A}^n\}$ y $\{(x_0 : \ldots : x_{n-1} : 0)/(x_0, \ldots, x_{n-1}) \in \mathbb{A}^n \setminus \{0\}\}$, es el espacio proyectivo $\mathbb{P}^n$, entonces

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{\,n-1}.$$

En particular, se obtiene $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{P}^0$. Puede entenderse que $\mathbb{P}^0$ representa al conjunto $\{(0:1)\}$, que será llamado *punto en el infinito* y se le denotará mediante P_∞.

Aquí se considerarán solo polinomios homogéneos, es decir, polinomios en los cuales todos sus términos tienen igual grado algebraico.
Debe recordarse también que:

si $P = (x_0 : \ldots : x_n) \in V(f)$ entonces $f(\lambda x_0, \ldots, \lambda x_n) = 0$, para todo $\lambda \in K^*$.

Una forma de homogenizar a un polinomio f que es no homogéneo, de grado m, con respecto a una nueva variable X_{n+1}, es

$$f_{homogenizado} = f^*(X_1, \ldots, X_n, X_{n+1}) = (X_{n+1})^m . f(\tfrac{X_1}{X_{n+1}}, \ldots, \tfrac{X_n}{X_{n+1}}),$$

donde $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$.
A f^* se le denominará *el polinomio homogeneo asociado a f*.

En el espacio proyectivo $\mathbb{P}^n$ se trabajará solamente con coordenadas homogéneas, es decir, se usará solo funciones racionales, en las cuales, el numerador y el denominador, sean polinomios homogéneos del mismo grado.

Considérese un punto P que pertenece a una variedad proyectiva χ; entonces, $h = \frac{f}{g}$ será *regular en P*, si siendo f y g polinomios homogéneos del mismo grado, se tiene que $g(P) \neq 0$.

Ahora, para extender una variedad afin χ en $\mathbb{A}^n$, definida sobre un ideal primo I, a una variedad proyectiva χ^*, se considerará el ideal primo I^*, que está generado por el conjunto $\{f^* : f \in I\}$.

Si se define $\chi^*_{x_0} = \{(x_0 : \ldots : x_n) \in \chi^* : x_0 \neq 0\}$, puede construirse un isomorfismo entre χ y $\chi^*_{x_0}$, mediante la aplicación

$$\chi \Rightarrow \chi^*_{x_0}$$

$$(x_1,\ldots,x_n) \to (1:x_1:\ldots:x_n)$$

Análogamente, puede definirse $\chi^*_{x_i}$:

$$\chi^*_{x_i} = \{(x_0:\ldots:x_i:\ldots:x_n) \in \chi^* : \ x_i \neq 0\}.$$

Se denominará *puntos en el infinito de la variedad afin* χ, a los puntos $(x_0:\cdots:x_n)$ de χ^* que tengan $x_0 = 0$.

También los cuerpos de funciones $K(\chi)$ y $K^*(\chi)$ son isomorfos mediante la aplicación:

$$\tfrac{f}{g} \to \tfrac{f^* x_0^m}{g^*}$$

siendo $m = grado(g) - grado(f)$.

3.3. Divisores

En lo que sigue, se considera que χ es una curva algebraica en la que todos sus puntos son no singulares y además es proyectiva sobre K.

Recordemos que un polinomio $f \in K[X]$ está bien determinado, (salvo por una constante que lo puede multiplicar) por sus raíces y sus respectivas multiplicidades. Luego, si se tiene una función racional $f(X) = \frac{h(X)}{g(X)}$, con h y g en $K[X]$, entonces ahora $f(X)$ está determinada, por los ceros de h y g, llamándose a estos últimos, los *polos* de f. Se asignará multiplicidad positiva a los ceros de h y multiplicidad negativa a los ceros de g.

En general, para una curva χ regular y considerando el punto P perteneciente a la curva χ, se define al *anillo local de* χ *en* P

$$\mathcal{O}_P(\chi) = \{f \in K(\chi)/\ f = \tfrac{h}{g}\ ,\ g(P) \neq 0\}.$$

Se tiene que, el único ideal máximal de $\mathcal{O}_P(\chi)$ está dado por

$$m = \{f \in \mathcal{O}_P(\chi)/f(P) = 0\}.$$

Cuando χ es regular entonces m es un ideal principal, es decir $m = \langle t \rangle$ (para mas detalles, puede revisarse [22]). Luego, si $f \in \mathcal{O}_P(\chi)$ entonces f puede expresarse de la forma $f = t^n u$, siendo u una unidad, definiéndose con ello la *valoración de f en P* mediante $v_P(f) = n$.

Damos las siguientes definiciones:

1. Se denomina *divisor de χ*, a una suma formal de la forma

$$D = \sum_{P \in \chi} n_P P,$$

   siendo n_P un entero, el cual es cero, salvo en un número finito de puntos P. El conjunto de todos los divisores sobre χ se denota por $Div(\chi)$ y se denomina *grupo divisor de χ*. Este conjunto tiene estructura de grupo abeliano respecto a la suma formal de estos divisores. Un divisor de la forma $D = P$ con $P \in \chi$, es llamado *divisor primo*.

2. Si en la definición anterior de *divisor*, se considera solo valores enteros no negativos, para n_P, entonces el divisor D pasará a llamarse *divisor efectivo* y se le denotará por $D \geq 0$.

3. Dado un divisor $D = \sum_{P \in \chi} n_P P$, se define al *grado de un divisor D*, a la suma de coeficientes n_P, es decir;

$$\textit{grado de un divisor } D = \sum_{P \in \chi} n_P$$

4. El *soporte de un divisor D* se define por $supp(D) = \{P \in \chi : n_P \neq 0\}$.

5. Un divisor $D = \sum_{P \in \chi} n_P P$ es mayor o igual que otro divisor $D' = \sum_{P \in \chi} n'_P P$, si $D - D'$ es efectivo, es decir, en $D - D' = \sum_{P \in \chi} (n_P - n'_P) P$, los coeficientes $n_P - n'_P \geq 0$ y se denotará $D \geq D'$.

6. El *divisor de una función racional* f se define por $(f) = \sum_{P \in \chi} v_P(f) P$. Siendo $v_P(f)$ la valoración de f en P y además, f no debe ser identicamente nula en χ. Puede revisarse [18] para mas detalles.

7. El *divisor de ceros* se define por $(f)_0 = \sum_{v_P(f) > 0} v_P(f) P$.
   Si $v_P(f) = t > 0$, se dice que P es *cero de f, de orden t*.

8. El *divisor de polos* se define por $(f)_\infty = \sum_{v_P(f) < 0} -v_P(f) P$.
   Si $v_P(f) = -t < 0$, se dice que P es un *polo de f, de orden t*.

9. El *divisor principal de* f se define por $(f)= (f)_0 - (f)_\infty$.

Ejemplo 3.1. Mostramos aquí como se realiza el cálculo del divisor de una función racional en el espacio proyectivo $\mathbb{P}^1$. Sea $h \in K(\chi)$ y $h = \frac{f}{g}$, siendo f y g polinomios homogéneos, del mismo grado y ambos en $K[X_0, X_1]$. Dado que K es algebraicamente cerrado y asumiendo aquí, que f y g no tienen factores comúnes, entonces puede escribirse lo siguiente:

$$f(X_0, X_1) = X_0^m.X_1^n[(X_0 - \alpha_1 X_1)^{a_1}(X_0 - \alpha_2 X_1)^{a_2} \dots (X_0 - \alpha_i X_1)^{a_i}],$$

$$g(X_0, X_1) \ = X_0^p.X_1^q\ [(X_0 - \beta_1 X_1)^{b_1}(X_0 - \beta_2 X_1)^{b_2} \dots (X_0 - \beta_j X_1)^{b_j}],$$

donde todos los exponentes son enteros no negativos, tales que, $mp = 0$ y $nq = 0$, para no tener factores comunes, pero también todos los coeficientes α y β deben ser diferentes. Además, para ser del mismo grado, debe cumplirse que

$$m + n + a_1 + \dots + a_i = p + q + b_1 + \dots + b_j.$$

Luego, para la función racional h, ya puede calcularse

$$(h) = (m - p)(0:1) + (n - q)(1:0) + [a_1(\alpha_1 : 1) + \dots + a_i(\alpha_i : 1)] - [b_1(\beta_1 : 1) + \dots + b_j(\beta_j : 1)].$$

3.4. El espacio vectorial de Riemann - Roch

Considerando un divisor D de una curva χ:

$$Ł(D) = \{f \in K(\chi)^* : (f) + D \geq 0\} \cup \{0\}$$

es un espacio vectorial, llamado espacio vectorial de Riemann-Roch. Además, su dimension se denota mediante:

$$\ell(D) = dim_K Ł(D).$$

¿Cómo son los elementos de $Ł(D)$? Consideremos el divisor

$$D = \sum_{i=1}^{\alpha} n_i P_i - \sum_{j=1}^{\beta} m_j Q_j.$$

El espacio $Ł(D)$ contiene a 0 y además a las funciones f tales que:

$$(f) = \sum_{j=1}^{\beta} m'_j Q_j - \sum_{i=1}^{\alpha} n'_i P_i,$$

con la condición de que $(f) + D$ sea efectivo, lo que equivale a tener *ceros* en Q_j, con $m'_j \geq m_j$ y *polos* en P_i, con $n'_i \leq n_i$.

¿En que casos, $\text{Ł}(D) = \{0\}$? Esto ocurrirá si y solo sí, el grado del divisor D es negativo. Si denotamos $D' = (f) + D$, con $f \in K(\chi)^*$, entonces $D \equiv D'$, lo cual asegura que $\text{Ł}(D)$ y $\text{Ł}(D')$ son isomorfos. Luego, como $grado(D) < 0$, también será $grado((f) + D) < 0$, para toda $f \in K(\chi)^*$. Esto asegura que, $f \notin \text{Ł}(D)$ y por ello, se tendrá: $\text{Ł}(D) = \{0\}$.

A continuación damos dos definiciones, útiles para el teorema de Riemann - Roch.

- *Divisor de un diferencial racional ω en una curva suave y proyectiva χ*: $(\omega) = \sum_{P \in \chi} v_P(f_P)P$; siendo $\omega = f_P dt_P$ una representación local de ω. Además $W = (\omega)$ se denomina *divisor canónico*. Esta definición puede revisarse en [19].

- *Género de una curva algebraica proyectiva*: Considerando que χ es una curva algebraica y proyectiva sobre K, se define al *género de la curva χ* como

$$g = max\{grado(D) - \ell(D) + 1 : D \text{ es divisor de } \chi\}.$$

A continuación se enuncia, sin demostración, un teorema que es muy importante en el estudio de la geometría algebraica y que aquí sirve para llegar al teorema de Weierstrass. Para tener mas información sobre la prueba de este teorema, puede revisarse el texto dado en [22].

Teorema 3.2 (Riemann-Roch). *Sea χ una curva algebraica proyectiva, no singular, de género g. Si D es un divisor en la curva χ, entonces para cualquier divisor canónico W_0, se cumple*

$$\ell(D) = gr(D) + 1 - g + \ell(W_0 - D).$$

Haciendo $D = 0$ en el teorema de Riemann-Roch, $\ell(0) = gr(0) + 1 - g + \ell(W_0 - 0)$, entonces $1 = 0 + 1 - g + \ell(W_0)$, de donde se obtiene que $\ell(W_0) = g$.

Si en el teorema hacemos $D = W_0$, se obtendrá $\ell(W_0) = gr(W_0) + 1 - g + \ell(W_0 - W_0)$ lo que lleva a $\ell(W_0) = gr(W_0) + 1 - g + \ell(0)$. De aquí se obtiene $gr(W_0) = 2g - 2$.

Ejemplo 3.3. Verificamos que se cumple este teorema, en la línea proyectiva $\mathbb{P}^1$. Si D es un divisor en $\mathbb{P}^1$, puede escribirse $D = D_1 - D_2$, siendo

$$D_1 = \sum_{i=1}^{\alpha} n_i P_i \quad \text{y} \quad D_2 = \sum_{j=1}^{\beta} m_j Q_j \text{ con } n_i \text{ y } m_j \text{ no negativos.}$$

Consideremos $h(X) = a - bX$, la cual al homogenizarse es $h^*(X,Y) = aY - bX$. La denotaremos $h_P(X,Y) = aY - bX$, en el punto $P = (a : b)$.

Determinamos ahora $Ł(D)$. Sea $f \in K(\chi)^*$: $f \in Ł(D)$ si y solo sí $(f) + D \geq 0$. Reemplazando aquí $D = D_1 - D_2$, se obtendrá:

$$f \in Ł(D) \text{ si y solo sí } (f) \geq \sum_{j=1}^{\beta} m_j Q_j - \sum_{i=1}^{\alpha} n_i P_i,$$

lo que implica que $f \in Ł(D)$, si y solo sí tiene *cero* de orden $\geq m_j$ en Q_j, para todo j entero de 1 a β y f tiene *polo* de orden $\leq n_i$ en P_i, para todo i entero de 1 a α. Luego, f debe ser de la forma

$$f = \frac{F h_{Q_1}^{m_1} \ldots h_{Q_\beta}^{m_\beta}}{h_{P_1}^{n_1} \ldots h_{P_\alpha}^{n_\alpha}},$$

siendo F un polinomio homogéneo, tal que el numerador y denominador de f, sean de igual grado. Con ello se obtiene que

$$gr(F) + \sum_{j=1}^{\beta} m_j Q_j = \sum_{i=1}^{\alpha} n_i P_i,$$

luego

$$gr(F) = gr(D_1) - gr(D_2) = gr(D).$$

Luego, el espacio vectorial de Riemann-Roch $Ł(D)$ es isomorfo al espacio de polinomios homogéneos, en dos variables, cuyo grado es $gr(D)$. Luego, se obtiene la dimensión de $Ł(D)$, como sigue:

$$\text{Si } gr(D) \geq 0 : \ell(D) = gr(D) + 1,$$
$$\text{Si } gr(D) < 0 : \ell(D) = 0.$$

Ahora consideramos $dt = d(X/Y) = \frac{YdX - XdY}{Y^2}$, el cual es una 1-forma en $\mathbb{P}^1$, que no tiene ceros, pero si tiene un único polo con orden 2 en $(1:0)$, por ello, se tiene que $(dt) = -2(1:0)$. Luego, $gr(W_0) = gr(dt) = -2$, además como $gr(W_0) = 2g - 2$, se tendrá que $g = 0$.

Dado que $gr(W_0 - D) = -2 - gr(D)$, se puede obtener $\ell(W_0 - D)$. Para ello, según lo comentado en 3.4, se tiene que $\ell(W_0 - D) = 0$, si $gr(W_0 - D) < 0$, es decir, cuando

$gr(D) > -2$. En el caso que $gr(W_0 - D) \geq 0$, se tendrá $\ell(W_0 - D) = gr(W_0 - D) + 1$. Luego, se ha hallado la dimensión de $Ł(W_0 - D)$:

$$\text{Si } gr(D) \leq -2 : \ell(W_0 - D) = -1 - gr(D),$$
$$\text{Si } gr(D) > -2 : \ell(W_0 - D) = 0.$$

Ahora comprobamos el teorema de Riemann-Roch, evaluando la expresión $\ell(D) - \ell(W_0 - D) - gr(D) + g - 1$ y se debe obtener cero, en todos los casos:

- CASO 1: Si $gr(D) \leq -2$:
  $\ell(D) - \ell(W_0 - D) - gr(D) + g - 1 = 0 - (-1 - gr(D)) - gr(D) - 1 = 0.$

- CASO 2: Si $-2 < gr(D) < 0$, es decir $gr(D) = -1$:
  $\ell(D) - \ell(W_0 - D) - gr(D) + g - 1 = 0 - 0 - (-1) + 0 - 1 = 0.$

- CASO 3: Si $gr(D) \geq 0$:
  $\ell(D) - \ell(W_0 - D) - gr(D) + g - 1 = (gr(D) + 1) - 0 - gr(D) + 0 - 1 = 0.$

Con lo cual se ha verificado el teorema de Riemann-Roch.

Enunciamos a continuación, dos relaciones que permiten diferenciar al orden o número de un polo y al orden o número, de una laguna:
Sea $n \in \mathbb{N}$

- n es un número de polo de P, si y solo sí, $dim(nP) > dim((n-1)P)$.

- n es un número de laguna de P, si y solo sí $Ł(nP) = Ł((n-1)P)$.

Proposición 3.4. *Sea χ una curva algebraica de género g, en la que todos sus puntos son no singulares y además es proyectiva sobre K. Si $P \in \chi$, entonces para cualquier $n > 2g$, existe $f \in K(\chi)*$ tal que P será un polo de orden n, es decir existe $f \in K(\chi)* \ / \quad (f)_\infty = nP$.*

Proposición 3.5. *Sea χ una curva algebraica de género g, en la que todos sus puntos son no singulares y además es proyectiva sobre K. Si D es un divisor en la curva χ, tal que $gr(D) > 2g - 2$, entonces se cumple*
$\ell(D) = gr(D) + 1 - g$.

Puede encontrarse las pruebas de tales proposiciones en [21].

3.5. Propiedades de lagunas en un semigrupo numérico

Recordemos la notación que se usaba en los dos primeros capítulos:

1. $L(S) = \{\ell_1, \ell_2, \cdots, \ell_g\}$ es el conjunto de lagunas.

2. $N(S) = \{s \in S : s < F(S)\}$ es el conjunto de elementos esporádicos de S.

3. $n(S)$ es el cardinal de $N(S)$.

4. $F(S)$ es el número de Frobenius.

5. $c(S)$ es el conductor.

Del lema 2.2, se obtiene

$$c(S) = g(S) + n(S).$$

De aquí se tiene que, la cantidad de elementos esporádicos o *no lagunas menores que el conductor* está dada por $n(S) = c(S) - g(S)$, o mas abreviadamente:

Cantidad de no lagunas menores que el conductor $= n = c - g = F(S) + 1 - g$.

Tener en cuenta que, no es lo mismo *elemento esporádico* que *no laguna*, ya que, los elementos esporádicos, son los elementos del semigrupo numérico, que no exceden a $F(S)$, en tanto que, no laguna, es cualquier elemento de S.

Ejemplo 3.6. El conjunto de lagunas y conjunto de esporádicos, del semigrupo numérico $S = \{0, 4, 5, 8, 9, 10, 12, 13, 14, \ldots\}$, son los siguientes:

$$L(S) = \{1, 2, 3, 6, 7, 11\},\ N(S) = \{0, 4, 5, 8, 9, 10\},$$

luego $g(S) = 6$ y $n(S) = 6$, además $F(S) = 11$, $c(S) = 12$. Se observa que se cumple $c(S) = g(S) + n(S)$ y también se verifica aquí, que el conjunto de no lagunas, es lo mismo que S, el cual no es igual al conjunto de elementos esporádicos $N(S)$.

Proposición 3.7. *Si s_i es un elemento esporádico, entonces su complemento respecto del número de Frobenius F(S), será una laguna.*

Demostración. Si s_i es un elemento esporádico, entonces, su complemento respecto de $F(S)$ es $F(S) - s_i$. Si ahora se supone que $F(S) - s_i \in S$, entonces por la propiedad de clausura, se tiene que $(F(S) - s_i) + s_i \in S$; es decir $F(S) \in S$, lo cual es una contradición y por ello, necesariamente debe ocurrir que $F(S) - s_i \notin S$. $\square$

Nótese que lo contrario, no necesariamente se cumple. Es decir, si ℓ_i es una laguna, entonces su complemento respecto de $F(S)$, no necesariamente será un elemento esporádico. Una consecuencia de la proposición 3.6 es lo siguiente.

Proposición 3.8. *La cantidad de elementos esporádicos, no excede a la cantidad de lagunas, es decir* $n(S) \leq g$.

Proposición 3.9. *Si* ℓ *es una laguna y* k *es un entero positivo tal que* $d = \frac{\ell}{k}$ *es también un entero, entonces* d *es una laguna.*

Demostración. Si $d = \frac{\ell}{k}$ fuera un elemento esporádico, entonces al calcular

$$\frac{\ell}{k} + \frac{\ell}{k} + \cdots \text{ (k veces)},$$

se obtendría que $\ell \in S$. Esto implica que el entero $d = \frac{\ell}{k}$ es una laguna. □

Como algo particular de la proposición 3.8, *cualquier divisor aritmético del número de Frobenius, es necesariamente una laguna del semigrupo numérico.*

Al conjunto $S = \mathbb{N}$, se le denomina *semigrupo numérico trivial*, el cual no tendrá lagunas y por ello $g = 0$. En lo que sigue se excluye este caso.

Si $g > 0$ *entonces es seguro que* $\ell_1 = 1$.

Para casos generales de semigrupos numéricos, se considera que las lagunas son ℓ_i, tales que $0 < \ell_1 < \ell_2 < \ell_3 < \cdots < \ell_g = F(S)$.

Proposición 3.10. *Dado un semigrupo numérico S, tal que su género sea* $g(S) = g$, *entonces toda laguna* ℓ_i *debe ser menor que* $2g$. *Además* $F(S) < 2g$.

Demostración. De acuerdo a la proposición 3.7, la cantidad de elementos esporádicos n, no debe exceder a la cantidad de lagunas g, es decir $n \leq g$, pero también se sabe del lema 2.2, que $c(S) = n(S) + g(S)$, entonces $n = F(S) + 1 - g$, que se reemplaza en la desigualdad anterior, obteniéndose que $F(S) + 1 - g \leq g$ y de aquí $F(S) \leq 2g - 1$, luego $\ell_i < 2g$. □

Proposición 3.11. *En el conjunto* $\{0, 1, \ldots, 2g\}$ *la cantidad de no lagunas, excede a la cantidad de lagunas, en 1. Además, dado que el 0 está en todo semigrupo numérico, entonces en el conjunto* $\{1, 2, \ldots, 2g\}$ *se encuentra la misma cantidad de lagunas, que de no lagunas.*

Demostración. Dado que en el intervalo de enteros $[0, 2g]$, hay $2g + 1$ elementos y la cantidad de lagunas es g, entonces, necesariamente debe haber $g + 1$ no lagunas, en dicho intervalo. Quitando el cero, que es no laguna, habría la misma cantidad de lagunas y no lagunas. □

Proposición 3.12. *Para que un semigrupo numérico tenga g lagunas, debe ocurrir que, en cada conjunto de enteros de la forma* $C_k = \{1, 2, 3, \ldots, 2k - 1\}$ *debe de haber por lo menos k lagunas, para cada k entero positivo que no exceda a g.*

Demostración. Aquí S debe tener g lagunas. Para tener un camino de demostración, nótese que:

Si $k = 1$ entonces $C_1 = \{1\}$ y por ello, necesariamente $\ell_1 = 1$ es una laguna, de lo contrario, $S = \mathbb{N}$ y no habría g lagunas.

Si $k = 2$ entonces $C_2 = \{1, 2, 3\}$ y si se supone que hay menos de 2 lagunas en C_2, necesariamente $S = \langle\{2, 3\}\rangle$,luego no habrían más lagunas. Por ello, en C_2 debe haber por lo menos 2 lagunas.

Si $k = 3$ entonces $C_3 = \{1, 2, 3, 4, 5\}$, luego si se supone que hay menos de 3 lagunas en C_3, necesariamente $S =< 3, 4, 5 >$ o $S =< 2, 5 >$ o $S =< 2, 3 >$ y en estos casos, ya no habrían mas lagunas. Luego, en C_3 debe haber por lo menos 3 lagunas.

Continuándose de forma similar, hasta llegar a $k = g$ y obteniéndose el conjunto $C_g = \{1, 2, \ldots, 2g-1\}$, en el cual, usando la proposición 3.7, debe haber g lagunas. □

3.6. Semigrupos numéricos de Weierstrass

En esta sección, se mostrará, algunos resultados de suma importancia en la geometría algebraica, que lo relacionan con los semigrupos numéricos. Mediante los semigrupos de Weierstrass, quedan relacionados propiedades geométricas de una curva algebraica, con propiedades aritméticas.

Considérese que χ es una curva algebraica, con género $g \geq 1$, no singular, proyectiva y ademas irreducible, que está definida sobre un cuerpo K algebraicamente cerrado. Si P es un punto que pertenece a χ, entonces el conjunto

$$H(P) = \{n \in \mathbb{N} : \exists f \in K(\chi); \textit{ que es regular en } \chi \setminus P \text{ y } (f)_\infty = nP\},$$

es un semigrupo numérico que se denomina *semigrupo numérico de Weierstrass en* P. La función f que está en $H(P)$, es racional y tiene en P un polo de orden n. Además, el género del semigrupo numérico es g, es decir, el número de lagunas del semigrupo numérico coincide con el género de la curva algebraica.

Antes de probar que $H(P)$ es un semigrupo numérico, daremos un ejemplo de ello. Para esto, enunciamos sin demostración, dos proposiciones extraidas de [20] que serán necesarias.

Proposición 3.13. *Sea F una curva irreducible no singular. Si existen $P \neq Q$ en F racionalmente equivalentes, entonces F es racional.*

Proposición 3.14. *Si F es una cúbica no singular, entonces F no es racional.*

Ejemplo 3.15. Consideremos la curva algebraica χ, en el espacio proyectivo $\mathbb{P}^2$

$$ZY^2 = X(X-Z)(X-2Z).$$

Probemos, que esta curva es no singular en todos sus puntos.
Sea $F = ZY^2 - X(X-Z)(X-2Z)$, entonces:

$$F_X = -3X^2 + 6XZ - 2Z^2, \qquad F_Y = 2YZ, \qquad F_Z = Y^2 + 3X^2 - 4XZ.$$

Partiendo de $F_Y = 2YZ \neq 0$, se tiene $Y \neq 0$ y $Z \neq 0$.
La recta $Y = 0$ interseca a $F = 0$, en los puntos $(0:0:1)$, $(1:0:1)$ y $(2:0:1)$. Luego, se evalúa cada uno de estos puntos en F_X, obteniendose

$$F_X(0:0:1) = -2 \neq 0, \qquad F_X(1:0:1) = 1 \neq 0, \qquad F_X(2:0:1) = -2 \neq 0,$$

La recta $Z = 0$ interseca a F=0, en el único punto $(0;1,0)$, luego se evalúa este punto en F_Z y se obtiene

$$F_Z(0;1;0) = 1 \neq 0.$$

Luego, F es no singular en todos sus puntos.

Sea $P = (0:1:0)$, el punto que es la única intersección entre $Z = 0$ y $F = 0$. Determinaremos aquí, su respectivo semigrupo de Weierstrass $H(P)$. Para ello, comprobemos que $1 \notin H(P)$. Si se supone que $1 \in H(P)$, entonces existe $f \in K(\chi)$ tal que $(f)_\infty = 1.P$, pero como f es racional, debe cumplirse que $(f) = 1.Q - 1.P$, lo que implica que Q es racionalmente equivalente a P. Si Q es diferente de P, entonces la cúbica $F = 0$ sería racional (proposición 3.13). Lo cual se contradice con el hecho de que toda cúbica no singular, no es racional (proposición 3.14). Esto implica que $Q = P$, pero entonces, se obtiene tambien un absurdo, puesto que ya se tenía que $(f) = 1.Q - 1.P$. Luego, $1 \notin H(P)$.

Sin embargo para $n \geq 2$: $n \in H(P)$. En efecto, basta con considerar la siguiente función racional

$$f = \frac{(X-Z)^n}{Z^n},$$

la cual tiene, polo de orden n: $(f)_\infty = n.P$. Por lo tanto, hemos encontrado el semigrupo de Weierstrass de la curva, en el punto $P = (0:1:0)$

$$H(P) = \{0, 2, 3, 4, \rightarrow\}.$$

Hemos dado arriba los cálculos para construir un semigrupo de Weierstrass, dado la función y un punto. Ahora comprobemos en general, que $H(P)$ es un semigrupo numérico.

Proposición 3.16 (Semigrupo de Weierstrass). *Sea χ una curva algebraica, con género $g \geq 1$, no singular, proyectiva y ademas irreducible, definida sobre un cuerpo K algebraicamente cerrado. Si $P \in \chi$, entonces*

$$H(P) = \{n \in \mathbb{N} : \exists f \in K(\chi);\ \text{que es regular en } \chi \setminus P \ \text{y}\ (f)_\infty = nP\},$$

es un semigrupo numérico, con género g.

Demostración. Probaremos que $H(P)$ cumple con las tres condiciones dadas en 1.1. En efecto, $0 \in H(P)$, pues basta con considerar $f = 1$ y así se tiene $(1)_\infty = 0P$. Pasemos a verificar que cumple la clausura para la adición: Sean los enteros n y m que están en $H(P)$, entonces existen $f, g \in K(\chi)$ regulares en $\chi \setminus P$, tales que $(f)_\infty = nP$ y $(g)_\infty = mP$. Luego, $f.g \in K(\chi)$ es regular en $\chi \setminus P$, tal que $(f)_\infty + (g)_\infty = nP + mP$, además dado que se cumple $(f.g) = (f) + (g)$, entonces $(f.g)_\infty = (n+m)P$, es decir $n + m \in H(P)$. Hasta aquí se ha probado que $H(P)$ es un semigrupo aditivo.

La prueba de que el complemento de $H(P)$ es finito, se debe a que en $H(P)$ habrá exactamente g lagunas, siendo g el género de la curva algebraica. Esto quedará comprobado con el *teorema de lagunas de Weierstrass* que seguidamente se enuncia y se prueba. □

Teorema 3.17 (De las lagunas de Weierstrass). *Sea χ una curva algebraica de género $g \geq 1$, en la que todos sus puntos son no singulares y además es proyectiva sobre K. Si $P \in \chi$ entonces, existe exactamente g lagunas de P (en $H(P)$), que se denotan por ℓ_i, las cuales estan en el conjunto $\{0, 1, 2, \ldots, 2g-1\}$, siendo la primera laguna $\ell_1 = 1$.*

Demostración. Se sabe de la proposición 3.10, que todas las lagunas son menores que $2g$. También es evidente que 0 es un polo. Luego, podemos considerar las inclusiones siguientes:

$$Ł(0) \subseteq Ł(P) \subseteq Ł(2P) \subseteq Ł(3) \subseteq \cdots \subseteq Ł((2g-1)P).$$

Pero se conoce que $dim(Ł(0)) = 1$, ya que $Ł(0) = K$, además mediante la proposición 3.4 se tiene que $dim(Ł(2g-1)P) = g$ y dado que $dim(Ł(iP)) \leq dim(Ł(i-1)P) + 1$, para todo i (ver [18]), entonces, necesariamente hay $g-1$ enteros entre 1 y $2g-1$ tales que $Ł((i-1)P) \subsetneq Ł(iP)$. Luego los g enteros sobrantes, tendrían que ser las lagunas de P.

Falta probar que $\ell_1 = 1$. Para ello, supongamos que $\ell_1 \neq 1$, entonces 1 sería una no laguna y se sabe que en este caso, se habría generado todo $\mathbb{N}$ y no habrá lagunas, generándose así,una contradición. Luego $\ell_1 = 1$. □

Si una curva χ tiene género g y $P \in \chi$, entonces, existe exactamente g enteros no negativos, $\ell_1, \ell_2, \ldots, \ell_g$, para los cuales, no se podrá encontrar la función racional $f \in K(\chi)$ y que tenga polo de orden ℓ_i en P.

En el ejemplo anterior, hemos considerado la curva:

$$ZY^2 = X(X-Z)(X-2Z),$$

y se ha determinado, su semigrupo de Weierstrass en $P = (0:1:0)$, obteniendo que

$$H(P) = \{0, 2, 3, 4, \rightarrow\},$$

el cual posee solo una laguna. Pero de acuerdo al teorema 3.13, si la curva que hemos tomado, tiene género g, entonces debe tener g lagunas, luego necesariamente la cúbica que se tomó, debe tener género 1, para satisfacer al teorema. Esto coincide con el hecho, de que las cúbicas, al ser elípticas, deben tener género 1.

Finalmente, se ha probado que al tomar un punto P sobre una curva algebraica, con género $g \geq 1$, no singular, proyectiva e irreducible sobre un campo K, existe un semigrupo numérico, al que se denomina *semigrupo de* $Weierstrass$ *en* P. Sin embargo, el caso contrario, no ocurre. Es decir, no todo semigrupo numérico, admite una curva χ, con las características anteriores y que sea un semigrupo de Weierstrass. Fué Hurwitz quien en 1893, cuestionó el hecho de que todo semigrupo numérico, pueda ser considerado como un semigrupo de Weierstrass. Pero recién en 1980, el matemático alemán, Ragnar Olaf Buchweitz, construyó un semigrupo numérico que no es de Weierstrass (ver [2]). Sin embargo, las condiciones que dio Buchweitz, para afirmar que un semigrupo numérico es de Weierstrass, (ver [19]), fueron refutados posteriormente y hasta hoy, no se ha logrado obtener, condiciones suficientes que permitan detectar, que semigrupo numérico, es de Weierstrass.

.

Bibliografía

[1] Assi, Abdallah and García-Sanchez, Pedro A : Numerical semigroups and applications. Springer, 2016.

[2] Buchweitz, Ragnar Olaf: On Zariski's criterion for equisingularity and non-smoothable monomial curves, 1981.

[3] Chacón, M. : El problema diofántico de Frobenius. Universidad de Sevilla. Facultad de Matemáticas, 2016.

[4] Da Silva,T.F. : Semigrupos numéricos e corpos de funcoes algebricas. www.ufac.br/elementos/edicoes/edicao-no-01-2011/semigrupos-numericos-e-corpos-de-funcoes-algebricas.pdf. 50-56

[5] Dornelas S.:Semigrupos de valores de anéis Gorenstein, Kunz e Arf e a árvore de semigrupos numericos. Universidade Federal de Vicosa – Minas Gerais, 2015.

[6] Faria de Paiva, N. y Alves García R. : Semigrupos numéricos e curvas algébricas. https://www.researchgate.net/publication/268185597_Semigrupos_Numericos_e_Curvas_Algebricas.

[7] García-Sanchez, P. A. : Tres sesiones con semigrupos numéricos. Minicurso Jarandilla. www.ugr.es/ pedro/minicurso-jarandilla.pdf

[8] Hefez, A. : Irreducibles plane singularities.The sixth workshop at Sao Carlos,2003.

[9] Kaplan, N. : Counting numerical semigroups by genus and some cases of a question of Wilf. Department of Mathematics Harvard University, Cambridge, MA 02138, 2011. https://www.math.uci.edu/ñckaplan/research_files/kaplancountingsemigroups.pdf

[10] Macedo, A. : Crescimento do numero de semigrupos numéricos em funcao do genero. Universidade estadual de Maringá, 2015.

[11] Marquez Campos, G.: Cálculo de invariantes combinatorios de semigrupos numéricos y aplicaciones. Tesis Doctoral. Universidad de Sevilla, España, 2014.

[12] Monteiro, S.: Semigrupos numéricos nao associados a curvas algébricas. Tese de mestrado. Universidade Federal de Vicosa - Minas Gerais, 2017.

[13] Oliveira,G. : Weierstrass semigroups and the canonical ideal of non trigonal curves. Manuscripta mathematica. 71 (1), 431-450.

[14] Rosales, J and Branco, M. : Irreducible numerical semigroups. Pacific Journal of Mathematics. Vol. 209. No 1. 2003.

[15] Rosales, J. and Branco, M.: Numerical semigroups that can be expressed as an intersection of symmetric numerical semigroups. Journal of Pure and Applied Algebra 171 (2002). 303–314.

[16] Rosales, J. and García-Sanchez, Pedro A.: Numerical semigroups. Springer, 2009.

[17] Rosales, J. and Robles-Perez, A.: The frobenius problem for some numerical semigroups with embedding dimension equal to three. Hacettepe Journal of Mathematics and Statistics Volume 44(4) (2015), 901–908

[18] Stichtenoth,Henning: Algebraic function fields and codes. Springer, 1993.

[19] Torres, F. : Semigrupos de Weierstrass. Pro Mathematica: Vol. X, 1996.

[20] Vainsencher, Israel: Introducao as Curvas Algébricas Planas (1979).

[21] Wagner Dias, A. : Semigrupo de Weierstrass e Códigos AG Bipontuais.Tese de mestrado. Universidade federal de Uberlandia, 2017.

[22] William Fulton : Algebraic Curves (2008). https://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[23] Zaldívar, Felipe : Notas de Geometría Algebraica.