Universidad Nacional Autónoma de México

Facultad de Ciencias

Soluciones de Sistemas de ecuaciones lineales diofantinas

T E S I S

que para obtener el título de:

Matemático

presenta:

Alan Bonilla Nava

Tutora:

Dra. Diana Avella Alaminos

Ciudad Universitaria, CD. MX., 2024

Dedicado a mis padres y mi hermana.

Agradecimientos

A mi tía Maru y mi tío Omar por permitirme vivir con ellos durante mis tres años de preparatoria y por el continuo apoyo que me han brindado desde que comencé a vivir solo iniciando la carrera.

A mi prima Xalli por todo el apoyo, por escucharme y aconsejarme durante los últimos 8 años de manera constante.

A mis abuelitos Vaudelio y Vicenta por todas las enseñanzas tanto directas como indirectas que me han brindado durante estos 23 años de vida, las cuales me han ayudado a ser lo que soy hoy en día.

A mi tía Raquel Bonilla y mi tía Xóchitl Nava porque aunque no las vea tan seguido sé que cuando requiera de su ayuda o ser escuchado, estarán cuando lo necesite.

A mis amigos y amigas de la preparatoria, Abraham Hernández, Alfredo Gallardo, Ángel García, Arturo García, Daniel Chávez, Fernando Bruno, Gerardo Sandoval, Giseel Franco, Jonathan Torres y Natasha Zavala por todos las salidas, risas, toda la diversión y demás que hemos pasado hasta la fecha y la amistad que espero siga perdurando por mucho tiempo más. Especialmente quiero agradecer a Fernando Bruno, quien vivió conmigo durante los primeros años de la universidad, y me ayudó a no sentirme solo durante todo ese tiempo. Además me gustaría agradecer a mi amiga Fernanda Ordónez (Q.E.P.D.); donde quiera que estés sé que estarías orgullosa de ver hasta donde he llegado.

A mis amigos de la universidad, Alberto Estrella, Eduardo Ramos, Emmanuel Delgadillo, Francisco Alvarado, Gerardo Carmona, Lorenzo Alvarado, Miguel Sánchez, Ninive Atenea y Pedro Astudillo por hacer más ameno el ambiente en las clases y durante los 4 años de carrera, además de todo el apoyo que me brindaron y por esta unión que hemos tenido gracias a las matemáticas.

Al profesor Benjamín Juárez (Q.E.P.D.) por haberme dado la oportunidad de comenzar a ser ayudante con él y así comenzar a adquirir experiencia enseñando.

A mi profesora y asesora Diana Avella por todo el apoyo y toda la paciencia que ha tenido a lo largo de la elaboración de este trabajo.

A Randy (Q.E.P.D) por acompañarme durante 10 años de mi vida y a Marley que ahora me acompaña.

A Aranza por estos 4 años llenos de felicidad, emoción y aventuras, por escucharme, apoyarme y ser un fuerte pilar en mi vida, además por ayudarme en varias ocasiones a salir de mi zona de confort, espero sigamos compartiendo más experiencias juntos.

A mi hermana Briseida por llegar a darle color a mi vida, por ayudarme a ser mejor en varios aspectos de mi vida y por tenerme mucha confianza y quererme mucho.

A mamá Eu por absolutamente todo, darme de comer cada vez que voy a visitarte, jugar conmigo, reir conmigo, platicar conmigo, verme crecer y demostrarme siempre el amor y cariño que me tienes. No es mentira cuando digo que tú eres la razón más importante por la cual he mejorado en varias cosas desde que tengo 16 años.

A mis padres, Omar y Maritza por todo su apoyo incondicional, por apoyarme en las decisiones que he tomado a lo largo de mi vida, por aconsejarme en varias situaciones ya que gracias a ello soy quien soy y por siempre protegerme animarme y amarme por sobre todo.

Introducción

Una ecuación diofantina es una ecuación de la forma $P(x_1, \ldots, x_n) = 0$, donde $P(x_1, \ldots, x_n)$ es un polinomio no nulo de grado mayor o igual a 1 con coeficientes enteros, en la que además se busca que las soluciones también sean números enteros. Cuando el grado del polinomio es uno, les llamaremos **ecuaciones lineales diofantinas** y son éstas el objeto de estudio del presente trabajo.

El nombre de ecuación **diofantina** se debe al matemático griego Diofanto de Alejandría (se desconoce su fecha de nacimiento, pero se presume que nació en el siglo III y falleció a la edad de 84 años[1]), quien es considerado como *el padre del Álgebra*. Fue autor de una compilación de 13 libros titulados *Arithmetica*, de los cuales desafortunadamente se conservan sólo los primeros seis. En ellos, Diofanto estudió y coleccionó una serie de problemas relacionados con ecuaciones algebraicas. Además de los griegos, otras culturas de la antigüedad como la china y la india resolvieron problemas referentes a ecuaciones diofantinas. Desde ese entonces el estudio de dichas ecuaciones ha continuado, siendo el teorema de Fermat y el décimo problema de Hilbert dos de los ejemplos más significativos en la historia de las matemáticas. El análisis de las ecuaciones diofantinas se presenta, como muchos problemas en la teoría de los números, con una formulación muy sencilla. Pero su entendimiento puede ser sumamente complejo y requerir de resultados de otras áreas de las matemáticas. Existen numerosos resultados teóricos referentes a las ecuaciones lineales diofantinas como por ejemplo el análisis para simplificar la matriz de coeficientes de un sistema de ecuaciones lineales diofantinas y la descripción de condiciones equivalentes a que el sistema tenga soluciones enteras. Sin embargo resolver en la práctica ecuaciones lineales diofantinas no es un problema trivial y se han buscado algoritmos eficientes con este fin, por lo que en épocas recientes el estudio de este problema se ha desarrollado en gran medida en el ámbito computacional en el área de la programación lineal entera. En este trabajo los resultados que se presentan son de tipo teórico, pero el lector interesado puede encontrar información sobre algoritmos computacionales relacionados con ecuaciones lineales diofantinas en las referencias [Go71] y [Cho79].

La presente tesis comenzó teniendo como objetivo desarrollar toda la teoría necesaria para entender y probar el teorema principal del artículo [Ch06], el cual afirma que el conjunto de soluciones de un sistema de ecuaciones lineales diofantinas tiene estructura de grupo abeliano con una operación binaria definida por el mismo autor, más aún, dicho conjunto puede ser expresado como una suma directa externa de grupos cíclicos. Durante el

[1] Fernández, Tomás y Tamaro, Elena. «Biografia de Diofanto de Alejandría». En Biografías y Vidas. La enciclopedia biográfica en línea [Internet]. Barcelona, España, 2004. Disponible en `https://www.biografiasyvidas.com/biografia/d/diofanto.htm` [fecha de acceso: 16 de enero de 2024].

desarrollo del trabajo se descubrieron inconsistencias en ciertas afirmaciones presentes en dicho artículo, por lo que esta tesis no sólo se enfocó en la teoría detrás del teorema en [Ch06], sino que también consistió en analizar qué se podía rescatar del resultado mencionado y en refutar con un sencillo contraejemplo la parte del material que no es cierta, además de brindar una correción a tal afirmación y demostrarla. Adicionalmente, se reflexionó acerca del motivo por el cual el autor del artículo, Ajai Choudhry, definió la operación binaria como lo hizo, observando que se trataba de una construcción más general para dar estructura de grupo a las clases laterales de un grupo con respecto a un subgrupo.

La tesis está constituida por cuatro capítulos, con el material distribuido como se detalla a continuación.

El Capítulo 1 consiste de resultados preliminares de la teoría de los números. En él se definen conceptos fundamentales como la divisibilidad y el máximo común divisor. También se prueban propiedades relacionadas con estos conceptos y resultados importantes como el algoritmo de Euclides, que nos permite calcular el máximo común divisor de dos números. Al final del capítulo se introducen las ecuaciones lineales diofantinas con dos variables, determinando las condiciones para que tengan soluciones y recordando el método clásico para resolverlas.

El Capítulo 2 está dedicado a estudiar conceptos básicos de la teoría de grupos, tales como grupo, grupo abeliano, grupos cíclicos y suma directa de grupos, entre otros, necesarios para comprender más a fondo el material de la parte final de la tesis.

El Capítulo 3 profundiza en el estudio de las ecuaciones lineales diofantinas, comenzando por generalizar resultados referentes al máximo común divisor, considerando ahora ecuaciones diofantinas de más de dos incógnitas y presentando un método para resolverlas. Posteriormente, se amplía el estudio de ecuaciones a sistemas con más de una ecuación, buscando entender cuándo existe solución a dichos sistemas y cómo encontrarlas en el caso en que existan. Para ello se retoman conceptos y resultados relacionados a la resolución de sistemas de ecuaciones lineales vistos en Álgebra Lineal adaptándolos al contexto de sistemas de ecuaciones diofantinas. En la tercera sección se dan dos maneras de resolver un sistema de ecuaciones lineales diofantinas usando el escalonamiento por renglones de una matriz y también la reducción por columnas. Para finalizar el capítulo, se utiliza el escalonamiento por renglones y por columnas para transformar una matriz en una matriz con ciertas características llamada su forma normal de Smith; se prueba la existencia de dicha matriz diagonal en el caso de matrices con entradas enteras (aunque el resultado se puede generalizar al contexto de matrices con entradas en un dominio euclidiano o bien en un dominio de ideales principales). Finalmente se usa la forma normal de Smith para dar una condición necesaria y suficiente para que un sistema de ecuaciones lineales diofantinas tenga solución, reformulando un resultado presente en el artículo [La96] y obteniendo así un análogo más completo del último teorema de la Sección 3.3. Cabe señalar que a lo largo del capítulo se desarrollan diversos ejemplos

en los que se busca reflexionar acerca de las distintas maneras de encontrar las soluciones de un sistema de ecuaciones lineales diofantinas.

Finalmente, en el Capítulo 4 se desglosa todo el material del artículo [Ch06] utilizando la teoría de grupos necesaria. Como se mencionó anteriormente, se brinda un contraejemplo a la segunda afirmación del teorema que se encuentra en el artículo, además se brinda una prueba sobre el isomorfismo de grupos entre el conjunto de soluciones de un sistema de ELD y $\mathbb{Z}^t$, donde t corresponde al número de parámetros libres en las soluciones del sistema y se explica cómo la operación binaria definida por el autor es una construcción más general que otorga estructura de grupo a las clases laterales de un grupo con respecto a un subgrupo.

Índice general

Capítulo 1

Conceptos fundamentales de teoría de números

El objetivo de este capítulo es introducir y desarrollar los conceptos básicos de la teoría de los números, tales como divisibilidad, máximo común divisor, etc. De esta manera, introduciremos las ecuaciones lineales diofantinas que son el objeto de estudio principal de la presente tesis. En este capítulo nos enfocaremos en las ecuaciones lineales diofantinas de dos variables, *i.e.* las ecuaciones de la forma $ax + by = c$ con a, b y c enteros, analizando qué condiciones tienen que cumplir los números a, b y c para que existan soluciones enteras. Además, estudiaremos algunos conceptos y resultados que serán de ayuda para los próximos capítulos.

1.1. Algoritmo de la división

Teorema 1.1.1. ***(Algoritmo de la división)***

Sean $a \in \mathbb{Z}$ y $b \in \mathbb{Z} \setminus \{0\}$. Entonces, existen $q, r \in \mathbb{Z}$ únicos tales que

$$a = bq + r,$$

donde $0 \leq r < |b|$.

Demostración. La prueba se dividirá en 2 pasos: la existencia y la unicidad. Empezaremos con el primer caso: $b > 0$.

(Existencia)

1. **(Caso 1)** $b > 0$. Sea S el siguiente conjunto

$$S = \{a - bn \,|\, n \in \mathbb{Z}, a - bn \geq 0\}.$$

Notemos que $S \subseteq \mathbb{N} \cup \{0\}$. Veamos que S es no vacío.

Supongamos que $a \geq 0$, entonces $a = a - b \cdot 0 \in S$. Si $a < 0$ entonces $-a > 0$ y como $b \in \mathbb{Z}^+$ entonces $b \geq 1$. Multiplicando la desigualdad $b \geq 1$ por $-a$ tenemos que $-ab \geq -a$, lo que implica que

$$a - ab \geq 0,$$

por lo tanto $a - ab \in S$. Luego $S \neq \emptyset$. Entonces, por el **Principio del Buen Orden**, tenemos que S tiene un elemento mínimo, llámese r. Dado que $r \in S$, existe $q \in \mathbb{Z}$ tal que $r = a - bq$, con $r \geq 0$.

Probemos que $r < b$. En efecto, supongamos por contradicción que $r \geq b$. Entonces $r - b \geq 0$. Como $r = a - bq$ se tiene que $(a - bq) - b \geq 0$, y

$$(a - bq) - b \geq 0 \implies a - b(q + 1) \geq 0.$$

Dado que $a - b(q + 1)$ es de la forma $a - bn \geq 0$ con $n = q + 1 \in \mathbb{Z}$, concluimos que $r - b \in S$. Por otra parte, como $b \in \mathbb{Z}^+$ tenemos que $b > 0$, así $b + r > r$, por lo que $r - b < r$, lo cual contradice que r sea el elemento mínimo de S. Luego $0 \leq r < b$.

2. **(Caso 2)** $b < 0$. Como $-b > 0$, por el caso 1 se sigue que existen $q, r \in \mathbb{Z}$ tales que

$$a = (-b)q + r, \qquad \text{donde } 0 \leq r < |b| = -b,$$

así, tenemos que

$$a = b(-q) + r,$$

con $-q, r \in \mathbb{Z}$ y $0 \leq r < |b| = -b$.

(Unicidad) Supongamos que existen $r, r', q, q' \in \mathbb{Z}$ tales que

$$\begin{aligned} a &= bq + r, \qquad 0 \leq r < |b| \\ a &= bq' + r', \qquad 0 \leq r' < |b|. \end{aligned}$$

Supongamos sin pérdida de generalidad que $r' \geq r$. Así

$$\begin{aligned} bq + r = bq' + r' &\implies bq - bq' = r' - r \\ &\implies b(q - q') = r' - r \\ &\implies |b||q - q'| = |r' - r| = r' - r. \end{aligned}$$

Demostraremos que $q = q'$. Por reducción al absurdo, si $q \neq q'$ tendríamos que $0 < |q - q'|$, y en consecuencia $1 \leq |q - q'|$. Así, $|b| \leq |b||q - q'| = r' - r$. Pero por otro lado $r' - r < r' < |b|$, lo cual es una contradicción. Concluimos entonces que $q = q'$, y en consecuencia $r' - r = b(0) = 0$, por lo cual $r' = r$. □

En la práctica, estos dos enteros q y r mencionados en el teorema anterior se les conoce como **cociente** y

residuo. A partir de ahora, prestaremos especial atención al residuo, ya que si este es igual a cero entonces tendremos un concepto de suma importancia en la teoría de números: la **divisibilidad**.

Definición 1.1.1. *Sean $a, b \in \mathbb{Z}$. Decimos que b **divide** al entero a, a es **divisible** por b, a es **múltiplo** de b o b es un **divisor** de a, si existe $q \in \mathbb{Z}$ tal que $a = bq$. Si b divide al entero a entonces escribimos $b|a$.*

Ejemplo 1.1.2. *De la definición, si consideramos $b = 2$ y $a = 8$, fácilmente podemos observar que 2 divide a 8 pues $8 = 2 \cdot 4$. Sin embargo, si $b = 3$ entonces 3 no divide a 8 pues no existe un entero q tal que $8 = 3q$, ya que el único valor que puede tomar q para satisfacer la igualdad anterior es $q = \frac{8}{3}$, sin embargo $\frac{8}{3}$ no es un número entero.*

A continuación, probaremos un resultado importante que posteriormente nos ayudará.

Proposición 1.1.3. *Sean a y b números enteros con b distinto de cero, tales que $a|b$, entonces $|a| \leq |b|$.*

Demostración. Sean a, b enteros, con $b \neq 0$, tales que $a \mid b$. Entonces existe $m \in \mathbb{Z}$ tal que $b = am$, por lo cual $|b| = |am| = |a||m|$. Luego,

$$|b| - |a| = |a||m| - |a| = |a|(|m| - 1).$$

Notemos que si $m = 0$ tendríamos que $b = a(0) = 0$ y eso contradice nuestra hipótesis. Entonces m debe ser también distinto de cero. Así, $|m|$ es un número positivo, entonces $|m| \geq 1$, lo que significa que $|m| - 1 \geq 0$. Por lo tanto, como $a > 0$ se sigue que $|b| - |a| = |a|(|m| - 1) \geq 0$. Luego $|b| \geq |a|$.

□

Enunciaremos algunas de las propiedades básicas sobre divisibilidad, las cuales son sencillas de demostrar; por ello únicamente probaremos los incisos 2) y 4).

Teorema 1.1.4. *Sean a, b, c, α y β números enteros.*

1. *Si $a|b$ y $b|a$, entonces $|a| = |b|$.*
2. *Si $a|b$ y $b|c$, entonces $a|c$.*
3. *Si $a|b$ y $a|c$, entonces $a|b + c$.*
4. *Si $a|b$, entonces $a|bc$.*
5. *Si $a|b$ y $a|c$, entonces $a|\alpha b + \beta c$.*

Demostración. Sean $a, b, c \in \mathbb{Z}$ números enteros:

2. Supongamos que $a|b$ y $b|c$, entonces tenemos que existen $t, s \in \mathbb{Z}$ tales que $b = at$ y $c = bs$ respectivamente. De esta manera, obtenemos que $c = (at)s$, teniendo así que $c = a(ts)$ con ts entero. Luego $a|c$.
4. Supongamos que $a|b$, entonces existe $t \in \mathbb{Z}$ tal que $b = at$. Multiplicando esta última igualdad por $c \in \mathbb{Z}$, tenemos que $bc = (at)c =$, por lo que $bc = a(tc)$ con tc entero. Luego $a|bc$.

□

1.2. Máximo común divisor y algoritmo de Euclides

Un número entero puede ser un divisor de dos números distintos (inclusive de más números). Por ejemplo, 24 tiene como divisores positivos a 1, 2, 3, 4, 6, 8, 12 y 24, y 18 tiene como divisores positivos a 1, 2, 3, 6, 9 y 18; notemos que los divisores positivos que tienen en común 18 y 24 son 1, 2, 3 y 6. A los números que son divisores a la vez de dos o más números se les conoce como ***divisores comunes***. Claramente el 1 es un divisor positivo de todos los números enteros, por lo que resulta ser el divisor común positivo más pequeño de cualquier par de números; sin embargo esto no tiene mucha relevancia, puesto que siempre sabremos que el divisor común positivo más pequeño es el 1. Por el contrario, el que resulta ser más significativo es el divisor común más grande, el cual definiremos a continuación.

Sea $a \in \mathbb{Z}$ un número entero y el conjunto $\mathcal{D}(a)$ de todos los divisores positivos de a. Notemos que este conjunto es no vacío y es un subconjunto de los números naturales, dado que $1 \in \mathcal{D}(a)$, de hecho el elemento mínimo de este conjunto es 1 y si a es distinto de cero, el elemento máximo es $|a|$, pues si d es un divisor positivo de a, por la Proposición 1.1.3 tenemos que $d \leq |a|$. Dados a, b enteros y $\mathcal{D}(a)$ y $\mathcal{D}(b)$ los conjuntos de divisores positivos de a y b respectivamente, consideremos el conjunto $\mathcal{D}(a) \cap \mathcal{D}(b)$. Notemos que es no vacío, pues $1 \in \mathcal{D}(a) \cap \mathcal{D}(b)$ y además es un subconjunto de los naturales; más aún si a es distinto de cero o b es distinto de cero $\mathcal{D}(a)$ o $\mathcal{D}(b)$ es finito por lo tanto $\mathcal{D}(a) \cap \mathcal{D}(b)$ también es finito. Así, dados a y b enteros no ambos nulos, $\mathcal{D}(a) \cap \mathcal{D}(b)$ es finito. Entonces el conjunto de los divisores comunes de a y b tiene elemento máximo[1]. A este elemento se le conocerá como el **máximo común divisor**.

Definición 1.2.1. *(**Máximo común divisor**) Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Decimos que d es el **máximo común divisor** de a y b si:*

1. *$d|a$ y $d|b$,*

2. *dado $d' \in \mathbb{Z}$, si $d'|a$ y $d'|b$, entonces $d' \leq d$,*

y lo denotamos como $d = (a, b)$.

El primer punto de la definición anterior quiere decir que d (el mcd, por sus siglas) es un divisor común de a y b, mientras que el segundo punto nos dice que cualquier otro divisor común d', de a y b debe ser menor o igual a d. Siempre que usemos la notación (a, b) vamos a suponer que a y b no son ambos ceros.
A continuación, veremos un resultado, el cual nos va a permitir trabajar sólo con los naturales:

Lema 1.2.1. *Sean $a, b \in \mathbb{Z}$ entonces $(a, b) = (-a, -b) = (a, -b) = (-a, b)$.*

Demostración. Únicamente probaremos la primera igualdad, debido a que las otras se prueban de manera análoga. Sea $d = (a, b)$ entonces $d|a$ y $d|b$, por lo que existen enteros n y m tales que $a = nd$ y $b = md$. Si multiplicamos ambos lados de la igualdad por -1 tendremos que d es un divisor común de $-a$ y $-b$, teniendo así que $(a, b) \leq (-a, -b)$. De manera análoga se tiene que $(-a, -b) \leq (a, b)$. Luego $(a, b) = (-a, -b)$ □

[1] Se puede probar que dado $A \subseteq \mathbb{N}$ finito y no vacío, entonces A tiene elemento máximo y elemento mínimo.

Como mencionamos, el lema anterior nos va a permitir trabajar con enteros no negativos. Además sabemos que si a es no nulo $(a, 0) = |a|$, así que a partir de ahora trabajaremos sólo con el máximo común divisor de enteros positivos.

Ejemplo 1.2.2. *Anteriormente consideramos a los números* 18 *y* 24*, los cuales tenían como divisores comunes positivos a 1, 2, 3 y 6, entonces* $(18, 24) = 6$*. Además, por lema anterior* $(-18, 24) = (-18, -24) = (18, -24) = 6$.

Previo a la Definición 1.2.1 mencionamos que el 1 siempre es el divisor común positivo más pequeño, sin embargo, también puede ser el único divisor común positivo de dos números (o más) y de esta manera convertirse en el máximo común divisor entre ellos. Esto nos da la siguiente definición.

Definición 1.2.2. *Sean a y b enteros positivos. Decimos que a y b son* ***primos relativos*** *si* $(a, b) = 1$.

Ejemplo 1.2.3. *Consideremos los números 6 y 35. Los divisores positivos de 6 son 1, 2, 3 y 6; los divisores positivos de 35 son 1, 5, 7, 35. De esta manera, el único divisor común positivo de 6 y 35 es el 1, por lo tanto* $(6, 35) = 1$ *y así 6 y 35 son primos relativos.*

Ahora que ya conocemos quien es el máximo común divisor de dos números, estudiaremos algunas propiedades de este.

Teorema 1.2.4. *Sea $d = (a, b)$ el máximo común divisor de a y b, entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Demostración. Sea $d' = \left(\frac{a}{d}, \frac{b}{d}\right)$.
Veamos que $d' = 1$.
Dado que d' es el máximo común divisor de $\frac{a}{d}$ y $\frac{b}{d}$ por hipótesis, entonces $\frac{a}{d} = nd'$ y $\frac{b}{d} = md'$, para algunas $m, n \in \mathbb{Z}$. Entonces $a = nd'd$ y $b = md'd$ teniendo así que $d'd$ es un divisor común de a y b. Como $d = (a, b)$ entonces por definición $d'd \leq d$, por lo que $d' \leq 1$. Como $d' \in \mathbb{Z}^+$ entonces $d' = 1$. □

Otra manera de expresar al máximo común divisor entre dos números enteros positivos a y b es como la suma de ciertos múltiplos de éstos; dicho de otra manera, como una **combinación lineal entera** de a y b, esto es, una expresión de la forma $\alpha a + \beta b$, donde $\alpha, \beta \in \mathbb{Z}$. Formalicemos lo anterior en el siguiente teorema.

Teorema 1.2.5. *El máximo común divisor de los enteros positivos a y b es una combinación lineal entera de a y b.*

Demostración. Consideremos el conjunto de todas las combinaciones lineales enteras positivas de a y b

$$S = \{x \in \mathbb{Z} | x = \alpha a + \beta b > 0 \text{ y } \alpha, \beta \in \mathbb{Z}\},$$

el cual es no vacío, ya que por hipótesis $a > 0$ y podemos escribirlo de la siguiente manera $a = 1 \cdot a + 0 \cdot b \in S$. Así, por el **Principio del Buen Orden**, S tiene elemento mínimo. Llamemos a este elemento mínimo d y demostremos que justamente es el máximo común divisor entre a y b.

Como d es un elemento de S entonces $d = \alpha a + \beta b$ para algunos enteros α, β. De la Definición 1.2.1, queremos probar que d divide tanto a a como a b y que además cualquier divisor común d' de a y b es menor o igual que d.

1. Veamos que $d|a$ y $d|b$. Por el algoritmo de la división existen enteros q y r tales que $a = dq + r$ con $0 \leq r < d$. Supongamos que d no divide a a, es decir que $0 < r$. Como $d = \alpha a + \beta b$, entonces:

$$\begin{aligned} r &= a - dq \\ &= a - (\alpha a + \beta b)q \\ &= a - \alpha aq - \beta bq \\ &= (1 - \alpha q)a + (-\beta q)b. \end{aligned}$$

   De esta manera pudimos expresar a r como una combinación lineal de a y b. Pero como supusimos $r > 0$ y además el algoritmo de la división nos dice que $r < d$ entonces r sería un elemento en S más pequeño que d, lo cual es una contradicción. Por lo tanto $r = 0$ y así $a = dq$. Luego $d|a$.
   De manera análoga se prueba que $d|b$.

2. Veamos ahora que si $d'|a$ y $d'|b$, entonces $d' \leq d$. Por hipótesis $d'|a$ y $d'|b$, entonces por inciso 3 del Teorema 1.1.4 se tiene que $d'|\alpha a + \beta b$. Como $d = \alpha a + \beta b$, se sigue que $d'|d$. Luego por la Proposición 1.1.3 se sigue que $|d'| \leq |d|$, y como $d' \leq |d'|$ y $|d| = d$ tenemos que $d' \leq d$.

Dado que se cumplen las condiciones de la Definición 1.2.1 entonces $d = (a, b)$. □

Corolario 1.2.6. *Sean a y b enteros positivos. Entonces a y b son primos relativos si y sólo si existen enteros α y β tales que $\alpha a + \beta b = 1$.*

Demostración. $\Longrightarrow$ Dado que a y b son primos relativos, entonces $(a, b) = 1$. Así, por el Teorema anterior, existen enteros α y β tales que $\alpha a + \beta b = 1$.

$\Longleftarrow$ Supongamos que existen enteros α y β tales que $\alpha a + \beta b = 1$. Sea $d = (a, b)$. Entonces, $d|a$ y $d|b$. Por el Teorema 1.1.4, $d|\alpha a + \beta b$, por lo que $d|1$. Además, $1|d$. Entonces, de nuevo por el Teorema 1.1.4, $|d| = |1|$. Por lo tanto, $d = 1$. Luego, a y b son primos relativos.

□

Corolario 1.2.7. *Sean $a, b, c \in \mathbb{Z}^+$.*

1. *Si $(a, b) = 1 = (a, c)$, entonces $(a, bc) = 1$.*
2. *Si $a|c$, $b|c$ y $(a, b) = 1$, entonces $ab|c$.*
3. *Si $(a, b) = 1$ y $a|bc$, entonces $a|c$.*
4. *$(ac, bc) = c(a, b)$.*

Demostración. Sean $a, b, c \in \mathbb{Z}^+$.

1. Por el Corolario 1.2.6 se tiene que existen enteros α y β tales que $\alpha a + \beta b = 1$, y enteros γ y δ tales que $\gamma a + \delta c = 1$. Multiplicando ambas combinaciones lineales tenemos que $(\alpha a + \beta b)(\gamma a + \delta c) = 1$, entonces $\alpha\gamma a^2 + \alpha\delta ac + \beta\gamma ba + \beta\delta bc = 1$, o bien $(\alpha\gamma a + \alpha\delta c + \beta\gamma b)a + \beta\delta(bc) = 1$. Hemos expresado al uno como combinación lineal entera de a y bc. Dado que uno es el menor entero positivo, no puede existir otra combinación lineal entera positiva más pequeña, por lo que $(a, bc) = 1$.

2. Por el Corolario 1.2.6 se tiene que existen enteros α y β tales que $\alpha a + \beta b = 1$, entonces si multiplicamos por c en ambos lados de la igualdad, obtenemos

$$\alpha ac + \beta bc = c.$$

Como $a|c$ y $b|c$, entonces existen enteros t y s tales que $c = at$ y $c = bs$ respectivamente, por lo que

$$\begin{aligned} \alpha ac + \beta bc &= c \\ \alpha a(bs) + \beta b(at) &= c \\ ab(\alpha s + \beta t) &= c. \end{aligned}$$

Luego, $ab|c$.

3. De igual manera, por el Corolario 1.2.6 se tiene que existen enteros α y β tales que $\alpha a + \beta b = 1$. Multiplicando por c a ambos lados

$$\alpha ac + \beta bc = c.$$

Además, como $a|bc$ por hipótesis, existe algún $t \in \mathbb{Z}$ entero tal que $bc = at$, entonces

$$\begin{aligned} \alpha ac + \beta bc &= c \\ \alpha ac + \beta at &= c \\ a(\alpha a + \beta t) &= c. \end{aligned}$$

Luego, $a|c$.

4. Sean $d = (ac, bc)$ y $d' = c(a, b)$. Entonces por el Teorema 1.2.5 tenemos que $d = ac\alpha + bc\beta$. Así

$$d = (ac\alpha + bc\beta)\frac{d'}{d'} = \left(\frac{ac}{c(a,b)}\alpha + \frac{bc}{c(a,b)}\beta\right)d' = \left(\frac{a}{(a,b)}\alpha + \frac{b}{(a,b)}\beta\right)d'.$$

Notemos que $\frac{a}{(a,b)}, \frac{b}{(a,b)} \in \mathbb{Z}$, por definición de máximo común divisor. Por lo tanto, $d'|d$.

Por otra parte, como $d' = c(a, b)$, entonces, por el Teorema 1.2.5 se tiene que $d' = c(as + bt) = acs + bct$, para alguna $s, t \in \mathbb{Z}$. Dado que $d|ac$ y $d|bc$, entonces por el Teorema 1.1.4, $d|acs + bct = d'$. De esta forma, obtuvimos que $d|d'$ y $d'|d$. Entonces, una vez más por el Teorema 1.1.4, se tiene que $|d| = |d'|$. Pero ambos son positivos, por lo tanto $d = d'$.

□

Antes de ver uno de los métodos más eficientes para calcular el máximo común divisor probaremos un lema, el cual nos ayudará para el resultado más importante de la sección.

Lema 1.2.8. *Sean a y b enteros positivos, r el residuo que se obtiene al dividir a entre b. Entonces $(a, b) = (b, r)$.*

Demostración. Por el algoritmo de la división sabemos que existe un único $q \in \mathbb{Z}$ tal que $a = bq + r$. Como a y b son enteros positivos y $0 \leq r < b$ entonces q es positivo. Sean $d = (a, b)$ y $d' = (b, r)$, probemos que $d|d'$ y $d'|d$.

1. Veamos que $d|d'$. Como $d = (a, b)$ entonces $d|a$ y $d|b$, entonces por el inciso 4 del Teorema 1.1.4 se tiene que $d|bq$, luego por el inciso 5 del Teorema 1.1.4 tenemos que $d|a - bq$. Por lo tanto $d|r$ y además $d|b$. Debido a que $(b, r) = \alpha b + \beta r$ para algunos enteros α y β, entonces $d|\alpha b + \beta r = (b, r)$, concluyendo que $d|d'$.

2. Veamos ahora que $d'|d$. Como $d'|b$ y $d'|r$, entonces por el inciso 4 del Teorema 1.1.4 se tiene que $d'|bq$, luego por el inciso 5 del Teorema 1.1.4 tenemos que $d'|bq + r$. Por lo tanto $d'|a$ y además $d'|b$. Dado que $(a, b) = as + bt$ para algunos enteros s y t, entonces $d'|as + bt = d$, teniendo así que $d'|d$.

Por lo tanto tenemos que $d|d'$ y $d'|d$. Así por inciso 1 del Teorema 1.1.4 tenemos que $|d| = |d'|$, pero ambos son positivos, por lo tanto $d = d'$. Luego $(a, b) = (b, r)$. □

Hallar el máximo común divisor de dos números pequeños puede ser muy sencillo; en cambio, si los números son relativamente grandes, puede ser muy laborioso calcular los divisores de cada uno y después ver cuáles tienen en común para luego determinar el más grande de ellos. Para solucionar este problema usaremos un algoritmo muy importante para el cálculo del máximo común divisor.

Teorema 1.2.9. ***(Algoritmo de Euclides)***

Sean $a, b \in \mathbb{Z}^+$ con $b > 0$.

Si $b|a$ entonces $(a, b) = b$. En caso contrario, consideremos la siguiente secuencia del algoritmo de la división:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0.
\end{aligned}$$

Entonces $r_n = (a, b)$. Además, r_n se podrá escribir como combinación lineal de a y b.

Demostración. La prueba será por inducción sobre n.

- **Caso base** $n = 1$**:** En este caso tenemos la siguiente secuencia:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b \\ b &= r_1 q_1 \end{aligned}$$

  Como $r_1|b$ entonces $(b, r_1) = r_1$, así por el Lema 1.2.8 se tiene que $(a, b) = (b, r_1) = r_1$.

- **H.I.** Supongamos que si obtenemos $n - 1$ residuos distintos de cero se cumple el resultado, es decir el máximo común divisor de los números es el último residuo distinto de cero.

- **P.I.** Mostremos que se da el resultado para n. Consideremos lo siguiente:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b \\ b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

  si omitimos la primera línea, obtendríamos por hipótesis de inducción que $r_n = (b, r_1)$ entonces por el lema 1.2.8 se tiene que $(a, b) = (b, r_1) = r_n$.

  Más aún, como $r_n = (a, b)$, entonces por el Teorema 1.2.5, r_n lo podemos escribir como combinación lineal de a y b, concluyendo la demostración.

□

Notemos entonces del **algoritmo de Euclides** que el proceso para calcular el máximo común divisor entre dos números a y b consiste en aplicar el algoritmo de la división, primero entre a y b y posteriormente entre b y el residuo que se obtuvo de dividir a entre b; seguido eso, una vez más aplicar el algoritmo de la división entre el primer residuo y el residuo que se obtuvo al dividir b entre el primer residuo... y así sucesivamente hasta que al aplicar el algoritmo de la división obtengamos residuo cero. Notemos que por el Lema 1.2.1, si queremos calcular el máximo común divisor entre dos números negativos o, uno positivo y uno negativo usando el **algoritmo de Euclides**, basta aplicarlo a sus valores absolutos. A continuación haremos un ejemplo para entender cómo aplicar el **algoritmo de Euclides**.

Ejemplo 1.2.10. *Veamos cuál es el máximo común divisor entre 286 y 398 aplicando el* ***algoritmo de Eu-***

clides.

$$\begin{aligned} 398 &= 286 \cdot 1 + 112 \\ 286 &= 112 \cdot 2 + 62 \\ 112 &= 62 \cdot 1 + 50 \\ 62 &= 50 \cdot 1 + 12 \\ 50 &= 12 \cdot 4 + 2 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

concluyendo que $(286, 398) = 2$ *ya que* 2 *es el último residuo no nulo. Ahora escribamos a* 2 *como combinación lineal de* 286 *y* 398*. Para ello vamos despejando los residuos a partir de la penúltima línea de las igualdades anteriores:*

$$\begin{aligned} 2 &= 50 - 12 \cdot 4 \\ &= 50 - (62 - 50 \cdot 1)4 \\ &= 50 \cdot 5 - 62 \cdot 4 \\ &= (112 - 62 \cdot 1) \cdot 5 - 62 \cdot 4 \\ &= 112 \cdot 5 - 62 \cdot 9 \\ &= 112 \cdot 5 - (286 - 112 \cdot 2) \cdot 9 \\ &= 112 \cdot 23 - 286 \cdot 9 \\ &= (398 - 286 \cdot 1) \cdot 23 - 286 \cdot 9 \\ &= 398 \cdot 23 + 286 \cdot (-32) \end{aligned}$$

Observación 1.2.11. *La forma de expresar al máximo común divisor* $d = (a, b)$ *como combinación lineal de* a *y* b *no es única. Del ejemplo anterior obtuvimos que* $2 = 398 \cdot 23 + 286 \cdot (-32)$*, pero igual tenemos que* $2 = 398 \cdot 166 + 286 \cdot (-231)$.

1.3. Ecuaciones lineales diofantinas

Ahora trabajaremos con el personaje principal de la presente tesis: las **ecuaciones lineales diofantinas**. En particular en este capítulo nos interesaremos en las ecuaciones lineales en dos variables. Estas son de la siguiente forma:

$$ax + by = c, \tag{1.1}$$

donde a, b, c son elementos de $\mathbb{R}$ y x, y son incógnitas. Sabemos que en $\mathbb{R}$ hay una infinidad de soluciones y además no importa qué valores tomen a, b y c, salvo en el caso en que $a = b = 0$ y $c \neq 0$ no hay solución. Entonces ¿cuál es el motivo de trabajar con ellas? Bueno, sabemos que la teoría de los números es una rama de las matemáticas encargada del estudio de propiedades de los números enteros, entonces es bueno preguntarnos, para el caso en que a, b y c sean números enteros, cuándo la ecuación (1.1) tiene como soluciones a números enteros x y y. Estas ecuaciones se conocen como **ecuaciones lineales diofantinas**. A partir de este momento las llamaremos por sus siglas: **ELD**.
Con esto podemos preguntarnos algo muy sencillo, ¿todas las ELD tienen solución entera? La respuesta a esta pregunta la veremos con el siguiente ejemplo.

Ejemplo 1.3.1. *Consideremos la siguiente ELD:*

$$2x + 8y = 11.$$

Notemos que del lado izquierdo de la igualdad tenemos a los coeficientes 2 y 8, los cuales son números pares. De esta manera, sin importar qué valores tomen x y y, la expresión $2x + 8y$ siempre va a ser un número par; sin embargo 11 es impar así que no es posible que $2x + 8y = 11$. Por lo tanto, la ELD $2x + 8y = 11$ no tiene ninguna solución entera.

Gracias al Ejemplo 1.3.1 nos podemos dar cuenta que **NO** toda ELD tiene soluciones, y que además los números a, b y c están jugando un papel importante para determinar la solubilidad de una ELD. Entonces, ¿qué condiciones tienen que satisfacer a, b y c de la ELD (1.1) para que existan soluciones enteras?

Ejemplo 1.3.2. *Consideremos la ELD*

$$ax + by = c$$

donde $a, b, c \in \mathbb{Z}$. Supongamos que $b = 0$ y a, c son distintos de cero. Entonces la ecuación anterior se transforma en $ax = c$. Recordemos que estamos trabajando en $\mathbb{Z}$ entonces no podemos "despejar" a x con total confianza, de hecho, la ecuación tiene solución en los enteros si y sólo si $a|c$. Teniendo así que existe una única $t \in \mathbb{Z}$ tal que $at = c$, por lo que las soluciones a la ecuación $ax + 0y = c$ son todos los pares (t, y) con $y \in \mathbb{Z}$.

El ejemplo anterior nos da una ligera idea de las condiciones necesarias y suficientes para que una ELD tenga soluciones. El siguiente teorema nos brinda una respuesta ante ello.

Teorema 1.3.3. *Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. Entonces para la **ecuación lineal diofantina** $ax + by = c$ existen soluciones enteras si y sólo si $d|c$, donde $d = (a, b)$.*

Demostración. Sean a, b, c números enteros distintos de cero y consideremos la ecuación $ax + by = c$.

$\Longrightarrow$) Supongamos que existen soluciones para la ELD $ax + by = c$. Sean $x = x_0$ y $y = y_0$ dichas soluciones. Entonces tenemos que

$$ax_0 + by_0 = c.$$

Sea $d = (a, b)$ el máximo común divisor de a y b. Por la Definición 1.2.1 sabemos que $d|a$ y $d|b$, además como x_0 y y_0 son números enteros por el Teorema 1.1.4 se tiene que $d|ax_0 + by_0 = c$. Luego $d|c$.

$\Longleftarrow$) Sea $d = (a, b)$ el máximo común divisor de a y b. Supongamos que $d|c$, entonces existe $t \in \mathbb{Z}$ tal que $dt = c$. Además, por el Teorema 1.2.5 existen enteros α y β tales que

$$a\alpha + b\beta = d.$$

Entonces, multiplicando por t en ambos lados tenemos que:

$$a\alpha t + b\beta t = dt \implies a(\alpha t) + b(\beta t) = c,$$

donde el par (x, y) con $x = \alpha t$ y $y = \beta t$ es solución de la ELD.

□

Una vez teniendo las condiciones para saber cuándo una ELD tiene soluciones, podemos hacernos la siguiente pregunta ¿cómo son estas soluciones? El siguiente teorema nos brinda una respuesta.

Teorema 1.3.4. *Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$ y $d = (a, b)$, con $d|c$. Si existen soluciones para la* ***ecuación lineal diofantina****, $ax + by = c$, entonces hay una infinidad de soluciones y son de la forma*

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t,$$

donde t es un número entero y el par (x_0, y_0) es una solución particular de la ELD.

Demostración. Tenemos que probar que efectivamente que todos los pares de la forma:

$$x = x_0 + \frac{b}{d}t$$
$$y = y_0 - \frac{a}{d}t$$

son soluciones de la ELD y además que cada par $(\hat{x}, \hat{y})$ que sea solución se puede expresar de esta forma. En efecto:

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

Notemos que la última igualdad se da pues (x_0, y_0) es una solución particular de la ELD. Ahora supongamos que (x_0, y_0) es una solución particular de la ELD y que el par $(\hat{x}, \hat{y})$ es una solución arbitraria. Entonces tenemos

las dos igualdades siguientes

$$ax_0 + by_0 = c, \qquad a\hat{x} + b\hat{y} = c.$$

Si las igualamos tenemos que

$$\begin{aligned} a\hat{x} + b\hat{y} &= ax_0 + by_0 \\ a\hat{x} - ax_0 &= by_0 - b\hat{y} \\ a(\hat{x} - x_0) &= b(y_0 - \hat{y}). \end{aligned}$$

Dividiendo a cada lado de la igualdad anterior por $d = (a, b)$ obtenemos

$$\frac{a}{d}(\hat{x} - x_0) = \frac{b}{d}(y_0 - \hat{y}). \tag{1.2}$$

De esta última igualdad obtenemos que $\frac{b}{d} | \frac{a}{d}(\hat{x} - x_0)$, y además como $(a, b) = d$, por el Teorema 1.2.4 inciso 1) se tiene que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Usando el Corolario 1.2.7 inciso 3), tenemos entonces que $\frac{b}{d} | \hat{x} - x_0$, lo que significa que existe $t \in \mathbb{Z}$ tal que

$$\hat{x} - x_0 = \frac{b}{d}t,$$

luego $\hat{x} = x_0 + \frac{b}{d}t$. Ahora, si sustituimos $\hat{x} - x_0$ en (1.2) tenemos que

$$\frac{a}{d}\left(\frac{b}{d}t\right) = \frac{b}{d}(y_0 - \hat{y})$$

.

Como $b \neq 0$ podemos cancelar dicho factor, y multiplicando por d obtenemos

$$\begin{aligned} \frac{a}{d}t &= y_0 - \hat{y} \\ \hat{y} &= y_0 - \frac{a}{d}t \end{aligned}$$

Luego, cada solución de la ELD es de la forma deseada, concluyendo la demostración. □

Viendo la prueba nos podemos preguntar cómo encontrar una solución particular. En muchas ocasiones se puede hacer a prueba y error. Sin embargo para encontrarla podemos utilizar el **algoritmo de Euclides**. Lo aclararemos con el siguiente ejemplo.

Ejemplo 1.3.5. *Comprobar si la siguiente ELD tiene soluciones y en caso afirmativo encontrar todas sus soluciones:*

$$286x + 398y = 112.$$

Del Ejemplo 1.2.10 tenemos que $(286, 398) = 2$ *y* $2|112$*, ya que* $112 = 2 \cdot 56$*, por lo tanto, por el Teorema 1.3.3*

existen soluciones enteras y además por el Teorema 1.3.4 son de la forma

$$x = x_0 + \frac{398}{2}t = x_0 + 199t, \qquad y = y_0 - \frac{286}{2}t = y_0 - 143t$$

donde el par (x_0, y_0) *es una solución particular. Para calcularla utilicemos la combinación lineal obtenida en el Ejemplo 1.2.10*

$$2 = 398 \cdot 23 + 286 \cdot (-32).$$

Ahora multipliquemos ambos lados por 56

$$\begin{aligned} 2 &= 398 \cdot 23 + 286 \cdot (-32) \\ 2 \cdot 56 &= 398 \cdot 23 \cdot 56 + 286 \cdot (-32) \cdot 56 \\ 112 &= 398 \cdot 1288 + 286 \cdot (-1792). \end{aligned}$$

Teniendo así que una solución particular es el par $(-1792, 1288)$*, por lo tanto las soluciones a la ecuación* $286x + 398y = 112$ *son*

$$x = -1792 + 199t, \qquad y = 1288 - 143t, \quad t \in \mathbb{Z}.$$

Capítulo 2

Teoría de grupos

El objetivo principal de este capítulo es dar una introducción a la teoría de grupos, la cual nos ayudará a probar los resultados desarrollados en el Capítulo 4.

2.1. Conceptos fundamentales

Definición 2.1.1. *Sea G un conjunto no vacío. Una operación binaria en G es una función*

$$* : G \times G \to G.$$

Definición 2.1.2. *Sea G un conjunto no vacío y $* : G \times G \to G$ una operación binaria, decimos que el par $(G, *)$ es un* ***grupo*** *si:*

1. ***Asociatividad****: Para todo $a, b, c \in G$ se cumple que $a * (b * c) = (a * b) * c$.*
2. *Existe $e \in G$ tal que $a * e = a = e * a$, para todo $a \in G$.*
3. *Para cada $a \in G$, existe un elemento $b \in G$ tal que $a * b = e = b * a$.*

Al elemento $e \in G$ en (2) se le conoce como un ***elemento neutro de*** G y al elemento $b \in G$ de (3) se le conoce como un ***inverso de*** a.

Ejemplo 2.1.1. *Definiendo la operación binaria: $a * b = a + b$ (la cual es la suma usual) con a y b elementos de los conjuntos enseguida escritos, tenemos que $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ y $(\mathbb{C}, +)$ forman una estructura de grupo. Si ahora consideramos la operación: $a * b = a \cdot b$ (la multiplicación usual), de manera sencilla podemos comprobar que $(\mathbb{Z}, \cdot)$ ya no forma una estructura de grupo; cumple la cerradura, esto es que para cada elemento $a, b \in \mathbb{Z}$ tenemos que $a \cdot b \in \mathbb{Z}$; también la cumple la asociatividad y además $1 \in \mathbb{Z}$ desempeña el papel del neutro bajo esta operación. Sin embargo la propiedad (3) no se cumple, pues no para toda $a \in \mathbb{Z}$ existe un elemento $b \in \mathbb{Z}$ tal que $a \cdot b = 1 = b \cdot a$, por ejemplo, no existe $b \in \mathbb{Z}$ tal que $5 \cdot b = 1 = b \cdot 5$ (en ese caso tendríamos que $b = \frac{1}{5} \notin \mathbb{Z}$). Para los conjuntos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ basta quitarles al 0 para que formen una estructura de grupo con la multiplicación.*

Volviendo al ejemplo de $(\mathbb{Z}, +)$, fácilmente podemos verificar que $0 \in \mathbb{Z}$ es el elemento neutro bajo la suma; además, el inverso de cada entero a con respecto a la suma es $-a$. Es natural preguntarnos si estos elementos (el neutro y los inversos) son únicos. El siguiente teorema responderá esa pregunta.
Cuando no exista confusión, para simplificar la notación al grupo $(G, *)$ lo denotaremos simplemente como G.

Teorema 2.1.2. *Sea G un grupo, entonces el elemento neutro de G es único. Además, para cada $a \in G$, el inverso de a es único.*

Demostración. Supongamos que $e \in G$ es un neutro de G y que $e' \in G$ también lo es. Queremos probar que $e = e'$. Notemos que como $e' \in G$ es un elemento neutro entonces $e = e' * e$ y además $e' = e' * e$, pues $e \in G$ es neutro. Por lo tanto, de las dos igualdades concluimos que $e = e'$.

Por otra parte, sea $a \in G$ y $b \in G$ un inverso de a. Supongamos que también $b' \in G$ es un inverso de a. Como $b \in G$ es un inverso de a se tiene que $a * b = e = b * a$, y como $b' \in G$ es un inverso de a se tiene que $a * b' = e = b' * a$. Entonces

$$\begin{aligned} b' = b' * e = b' * (a * b) &= (b' * a) * b \\ &= e * b \\ &= b, \end{aligned}$$

teniendo así que $b' = b$. □

Si b es el inverso de a, entonces lo denotaremos como a^{-1}.

Además de estas propiedades, nos van a interesar también los grupos en donde se cumpla la *conmutatividad* de la operación. A estos grupos les llamaremos ***grupos abelianos***.

Definición 2.1.3. *Un grupo $(G, *)$ se dice que es* **abeliano**, *si para cada $a, b \in G$, se tiene que $a * b = b * a$.*

Notación 2.1.1. *Cuando hablamos de un grupo abeliano, la operación binaria se suele escribir con la notación aditiva, esto es, $a * b = a + b$, para cada $a, b \in G$. Además, el neutro se denota por 0 y el inverso del elemento a en notación aditiva se escribe como $-a$.*

Ejemplo 2.1.3. *Retomando los ejemplos anteriores, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ y $(\mathbb{C}, +)$ tienen estructura de grupo abeliano.*

Ejemplo 2.1.4. *Consideremos al conjunto de las matrices cuadradas de $n \times n$ con entradas en $\mathbb{R}$ e invertibles, denotado por $GL_n(\mathbb{R})$ y $\cdot$ la multiplicación usual de matrices; $(GL_n(\mathbb{R}), \cdot)$ forma un grupo, sin embargo no es abeliano para $n \geq 2$, ya que en general la multiplicación de matrices no es conmutativa.*

Ejemplo 2.1.5. *Recordemos que $(\mathbb{R}, +, \cdot)$ es un campo y para simplificar la notación escribamos $x \cdot y = xy$. Sea $G = \mathbb{R} \setminus \{1\}$ y $a, b \in G$, definamos la operación $* : G \times G \to G$ como $a * b := a + b - ab$. Demostremos que $(G, *)$ tiene estructura de grupo.*

Notemos que la operación es cerrada, pues $(\mathbb{R}, +, \cdot)$ *es un campo y la suma y producto usual son operaciones cerradas. Veamos que la operación es asociativa*

$$\begin{aligned} a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= (a * b) + c - (a * b)c \\ &= (a * b) * c. \end{aligned}$$

Veamos que la operación tiene un elemento neutro, para esto notemos que en caso de que exista un neutro $e \in G$*, requerimos que* $a * e = e * a = a$*, para todo* $a \in G$ *pero*

$$\begin{aligned} a * e = a &\implies a + e - ae = a \\ &\implies e - ae = 0. \end{aligned}$$

Como esto debe ocurrir para toda $a \in G$*, en particular se debe cumplir para* $a = 0$*, de donde concluimos que* $e = 0$*. Entonces, en caso de que exista* $e \in G$ *un neutro, éste debe ser el cero. Veamos que efectivamente* 0 *es un neutro en* G*:*

$$a * 0 = a + 0 - a \cdot 0 = a = 0 + a - 0 \cdot a = 0 * a.$$

Así, $e = 0$ *es un neutro en* G*, y por el Teorema 2.1.2 éste es único.*
Para verificar la existencia de inversos para cada elemento $a \in G$ *haremos un razonamiento similar. Sea* $a \in G$*, en caso de que exista* $b \in G$ *un inverso de* a *se requeriría que* $a * b = b * a = 0$*, pero:*

$$\begin{aligned} a * b = 0 &\implies a + b - ab = 0 \\ &\implies b(1 - a) = -a \\ &\implies b = \frac{a}{a - 1}. \end{aligned}$$

Notemos que $b = \frac{a}{a-1}$ *está bien definido pues* $a \neq 1$*. Así, si* a *tiene un inverso éste debe ser* $b = \frac{a}{a-1} \in G$*.*

Veamos que efectivamente es un inverso de a:

$$\begin{aligned} a * b = a * \left(\frac{a}{a-1}\right) &= a + \frac{a}{a-1} - a \cdot \frac{a}{a-1} \\ &= \frac{a(a-1)+a}{a-1} - \frac{a^2}{a-1} \\ &= \frac{a^2 - a + a}{a-1} - \frac{a^2}{a-1} \\ &= \frac{a^2}{a-1} - \frac{a^2}{a-1} \\ &= 0. \end{aligned}$$

Análogamente se puede verificar que $b * a = 0$, por lo tanto cada elemento en G tiene un inverso.

Concluimos que $(\mathbb{R} \setminus \{1\}, *)$ es un grupo; más aún, es un grupo abeliano ya que para todos $a, b \in G$ se tiene que

$$a * b = a + b - ab = b + a - ba = b * a.$$

Notemos del Ejemplo 2.1.5 que si tomamos a $G = \mathbb{R}$ y la misma operación $*$, $(\mathbb{R}, *)$ no tendría estructura de grupo, ya que por definición de grupo se requiere que cada elemento $a \in \mathbb{R}$ tenga un inverso, sin embargo, $a = 1$ no tendría inverso bajo esta operación.

A continuación daremos una definición importante, la cual nos ayudará a comprender de qué manera se comparan algunos grupos con otros, preservando la operación binaria de éstos.

Definición 2.1.4. *Sean $(G, *)$ y $(H, \circ)$ dos grupos. La función $f : G \to H$ es un **homomorfismo** de grupos si*

$$f(a * b) = f(a) \circ f(b)$$

*para todo $a, b \in G$. Si f es inyectiva, lo llamaremos **monomorfismo**. Si f es suprayectiva, lo llamaremos **epimorfismo**. Además, si f es una biyección, entonces decimos que f es un **isomorfismo** de grupos. Dos grupos G y H se dicen isomorfos si existe un isomorfismo $f : G \to H$ entre ellos y se denota como $G \cong H$.*

Ejemplo 2.1.6. *Consideremos a $(\mathbb{R}, +)$ y $(\mathbb{R}^+, *)$ el grupo aditivo de los números reales y el grupo multiplicativo de los números reales distintos de cero respectivamente y sea la función $g : (\mathbb{R}, +) \to (\mathbb{R}^+, *)$ dada por*

$$g(x) = e^x.$$

Por las propiedades que ya conocemos de la exponencial se sigue que

$$g(x + y) = e^{x+y} = e^x e^y = g(x) * g(y),$$

teniendo así que g es un homomorfismo de grupos. Más aún, como $h : (\mathbb{R}^+, *) \to (\mathbb{R}, +)$ dada por

$$h(x) = ln(x)$$

es la función inversa de g, entonces g es un isomorfismo de grupos.

El siguiente resultado nos será útil más adelante:

Teorema 2.1.7. *Sean $(G,\cdot),(H,*)$ y $(K,\star)$ tres grupos y sean $\phi: G \to H$ y $\psi: H \to K$ isomorfismos. Entonces $\psi \circ \phi: G \to K$ es también un isomorfismo.*

Demostración. Veamos que $\phi \circ \psi$ es un homomorfismo de grupos. Sean $x, y \in G$ arbitrarios. Entonces

$$\begin{aligned}(\psi \circ \phi)(x \cdot y) &= \psi(\phi(x \cdot y)) \\ &= \psi(\phi(x) * \phi(y)) \\ &= \psi(\phi(x)) \star \psi(\phi(y)) \\ &= (\psi \circ \phi)(x) \star (\psi \circ \phi)(y).\end{aligned}$$

Por lo tanto $\psi \circ \phi$ es un homomorfismo de grupos. Además, como ψ y ϕ son biyecciones, entonces $\psi \circ \phi$ es una biyección. Luego $\psi \circ \phi: G \to K$ es un isomorfismo de grupos. □

Definición 2.1.5. *Sea G un grupo. G es un **grupo finito** si y sólo si el conjunto G es finito, en caso contrario, se dice que G es un **grupo infinito**.*
*El **orden de** G es n si y sólo si el cardinal de G es n, esto es*

$$|G| = n.$$

Definición 2.1.6. *Sea G un grupo y $a \in G$. Definimos las **potencias** de a como: $a^0 = e$ y para $n \geq 1$, definimos $a^{n+1} = a^n * a$, y además $a^{-n} = (a^{-1})^n$.*

Observación 2.1.8. *Se puede probar por inducción que*

$$a^n = \underbrace{a * a * \cdots * a}_{n-veces}$$

y si $n = 0$ entenderemos que el producto de a cero veces da como resultado el neutro del grupo.

Con la definición y observación anteriores damos paso a un resultado que nos servirá más adelante.

Teorema 2.1.9. *Sea G un grupo, $a \in G$ y $m, n \in \mathbb{Z}$ entonces*

1. $a^m * a^n = a^{m+n} = a^n * a^m$.

2. $(a^m)^n = a^{mn} = (a^n)^m$.

Demostración. 1. Consideremos los siguientes casos:

(i) Si $m, n \in \mathbb{N}$.

$$\begin{aligned} a^m * a^n &= \underbrace{a * a * \cdots * a}_{m-\text{veces}} * \underbrace{a * a * \cdots * a}_{n-\text{veces}} \\ &= \underbrace{a * a * \cdots * a}_{m+n-\text{veces}} \\ &= a^{m+n} \\ &= a^{n+m} \\ &= \underbrace{a * a * \cdots * a}_{n+m-\text{veces}} \\ &= \underbrace{a * a * \cdots * a}_{n-\text{veces}} * \underbrace{a * a * \cdots * a}_{m-\text{veces}} \\ &= a^n * a^m. \end{aligned}$$

(ii) Si $m < 0$ y $n < 0$, entonces se tiene que

$$a^m * a^n = (a^{-1})^{-m} * (a^{-1})^{-n} = (a^{-1})^{-m-n} = (a^{-1})^{-(m+n)} = a^{n+m}.$$

(iii) Si $m < 0$ y $n > 0$, entonces tenemos que

$$a^m * a^n = (a^{-1})^{-m} * a^n = \underbrace{a^{-1} * \cdots * a^{-1}}_{-m-\text{veces}} * \underbrace{a * \cdots * a}_{n-\text{veces}}.$$

Supongamos que $n > -m$, entonces asociando de tal manera que obtengamos todos los productos $a^{-1}a = e$ posibles llegamos a

$$\underbrace{a^{-1} * \cdots * a^{-1}}_{-m-\text{veces}} * \underbrace{a * \cdots * a}_{n-\text{veces}} = \underbrace{a * \cdots * a}_{n-(-m)-\text{veces}} = a^{n-(-m)} = a^{n+m} = a^{m+n}.$$

Ahora supongamos que $n < -m$, entonces asociando de tal manera que obtengamos todos los productos $a^{-1}a = e$ posibles llegamos a

$$\underbrace{a^{-1} * \cdots * a^{-1}}_{-m-\text{veces}} * \underbrace{a * \cdots * a}_{n-\text{veces}} = \underbrace{a^{-1} * \cdots * a^{-1}}_{-m-n-\text{veces}} = (a^{-1})^{-m-n} = (a^{-1})^{-(m+n)} = a^{m+n}.$$

(iv) El caso en que $m > 0$ y $n < 0$ es analógo al anterior.

2. Se omitirá la demostración ya que es similar a la del inciso previo analizando los diferentes casos que existen de acuerdo a los signos de n y m.

□

Observación 2.1.10. *Si usamos la notación aditiva, a^n se escribe como na.*

Ahora veremos otro concepto importante. Es natural pensar que un grupo tenga subconjuntos, ya que en sí, un grupo es un conjunto, pero ¿todos los subconjuntos de un grupo seguirán manteniendo la misma estructura que el grupo? Aquí es donde surge el concepto de **subgrupo**.

Definición 2.1.7. *Sea G es un grupo y $H \subseteq G$, no vacío. Decimos que H es un **subgrupo** de G si cumple lo siguiente:*

1. *El neutro $e \in G$ está en H, es decir, $e \in H$.*
2. *H es cerrado con la operación de G, esto es, si $a, b \in H$, entonces $a * b \in H$.*
3. *Si $a \in H$ entonces $a^{-1} \in H$.*

En este caso, lo denotamos por $H \leq G$.

Proposición 2.1.11. *Sean G un grupo y $H \subseteq G$, no vacío. Entonces H es un subgrupo de G si y sólo si para todo $a, b \in H$ se tiene que $a * b^{-1} \in H$.*

Demostración. $\implies$) Supongamos que $H \leq G$, por lo tanto si $b \in H$, entonces $b^{-1} \in H$, así, como la operación de G es cerrada en H entonces para $a, b^{-1} \in H$ tenemos que $a * b^{-1} \in H$.

$\impliedby$) Supongamos que $c \in H$, pues H es no vacío, entonces $e = a * a^{-1} \in H$. Ahora, sean $a, b \in H$. Como $e \in H$, entonces $b^{-1} = e * b^{-1} \in H$. Con esto, ya tenemos que $a, b^{-1} \in H$, por lo que $a * b = a * (b^{-1})^{-1} \in H$. Por lo tanto H cumple las tres propiedades de la definición, así, H es un subgrupo de G. □

Por conveniencia, escribamos a partir de ahora ab en lugar de $a * b$. Además, como observación, dado que H es cerrado bajo la operación, si $a \in H$ entonces $a^n \in H$ para todo entero positivo n.

Ejemplo 2.1.12. *Sea $\mathbb{Q}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Q}\}$. Demostremos que $\mathbb{Q}[i]$ es un subgrupo de $\mathbb{C}$ con la suma usual.*
En efecto. Notemos que $\mathbb{Q}[i]$ es no vacío, dado que $0 = 0 + 0i \in \mathbb{Q}[i]$ y por definición del conjunto $\mathbb{Q}[i] \subseteq \mathbb{C}$. Ahora, sean $x = a + bi, y = c + di \in \mathbb{Q}[i]$. Por la proposición anterior, basta mostrar que $x - y \in \mathbb{Q}[i]$. Notemos que

$$x - y = a + bi - (c + di) = (a - c) + (b - d)i,$$

como $a - c$ y $b - d$ son elementos de $\mathbb{Q}$, ya que $(\mathbb{Q}, +)$ es un grupo, concluímos que $x - y \in \mathbb{Q}[i]$. Luego $\mathbb{Q}[i] \leq \mathbb{C}$.

Teorema 2.1.13. *Sean G un grupo y $H, K \leq G$ subgrupos de G. Entonces $H \cap K$ es un subgrupo de G.*

Demostración. Sean H y K subgrupos de G. Sabemos que la intersección de estos subgrupos está contenida en H y K. Podemos notar que $H \cap K$ es un subconjunto de G, ya que H y K lo son, luego $H \cap K \neq \emptyset$, pues el elemento neutro está en H y K por ser ambos subgrupos de G. Ahora, sean $a, b \in H \cap K$, entonces $a, b \in H$ y $a, b \in K$, y al ser ambos subgrupos, por la Proposición 2.1.11 tenemos que $ab^{-1} \in H$ y $ab^{-1} \in K$. Luego $ab^{-1} \in H \cap K$. □

Este hecho se puede generalizar ya que para $\{H_i\}_{i\in I}$ una familia no vacía de subgrupos de G, se tiene que $\bigcap_{i\in I} H_i$ es un subgrupo de G.
Naturalmente uno se podría preguntar si dados dos subgrupos H y K de G, se tendrá que $H \cup K$ es un subgrupo; desafortunadamente no siempre se cumple esto. Es más, rara vez es cierto; consideremos a $G = \mathbb{Z}$ con la operación suma y los subgrupos $H = 3\mathbb{Z}$ y $K = 5\mathbb{Z}$. Notemos que $3, 5 \in H \cup K$ pero $3 + 5 = 8 \notin H \cup K$.
Con esto podemos formularnos varias preguntas, pero hay una que nos interesa en particular y que será respondida en la próxima sección, ¿se podrá construir un subgrupo más pequeño que contenga a H y K también? La respuesta es que sí.

2.2. Generado y grupos cíclicos

Definición 2.2.1. *Sea $S \subseteq G$. El **grupo generado** por S, denotado por $\langle S\rangle$, se define como la intersección de todos los subgrupos de G que contienen a S.*

Por la generalización del Teorema 2.1.13, se sigue que $\langle S\rangle$ es un subgrupo de G y por construcción S está contenido en $\langle S\rangle$.

Notación 2.2.1. *Si $n \in \mathbb{N}^+$ y S es un subconjunto finito de G con n elementos, podemos escribir $S = \{x_1, \ldots, x_n\}$. Denotaremos a su generado como*

$$\langle S\rangle = \langle\{x_1, \ldots, x_n\}\rangle = \langle x_1, \ldots, x_n\rangle.$$

El siguiente resultado nos dice que $\langle S\rangle$ es el subgrupo más pequeño de G que contiene a S.

Teorema 2.2.1. *Sea $S \subseteq G$. Si H es un subgrupo de G tal que $S \subseteq H$, entonces $\langle S\rangle \subseteq H$.*

Demostración. Como $\langle S\rangle$ es la intersección de todos los subgrupos de G que contienen a S y H es un subgrupo de G que contiene a S, entonces $\langle S\rangle \subseteq H$. □

En particular, si tenemos dos subgrupos H, K de G, entonces el subgrupo más pequeño que contiene a H y K es $\langle H \cup K\rangle$.

A continuación veremos cuál es el generado por un elemento de un grupo G.

Proposición 2.2.2. *Sean G un grupo y $a \in G$. Entonces*

$$\{a^n | n \in \mathbb{Z}\}$$

es un subgrupo de G. Además $\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$.

Demostración. Notemos que $e = a^0 \in \{a^n | n \in \mathbb{Z}\}$.
Si $x, y \in \{a^n | n \in \mathbb{Z}\}$ entonces $x = a^k$ y $y = a^m$ con $k, m \in \mathbb{Z}$, así,

$$xy^{-1} = a^k a^{-m} = a^{k-m} \in \{a^n | n \in \mathbb{Z}\}.$$

Luego, $\{a^n | n \in \mathbb{Z}\}$ es un subgrupo de G.

Ahora veamos que $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

$\subseteq$) Dado que $\{a^n | n \in \mathbb{Z}\}$ es un subgrupo de G que contiene a $\{a\}$ por el teorema anterior $\langle a \rangle \subseteq \{a^n | n \in \mathbb{Z}\}$.

$\supseteq$) Sea $x \in \{a^n | n \in \mathbb{Z}\}$ entonces $x = a^n$ para algún $n \in \mathbb{Z}$. Como $a \in \langle a \rangle$ y el generado es un subgrupo de G, luego $x = a^n \in \langle a \rangle$. □

El subgrupo anterior se conoce como el subgrupo cíclico de G generado por a. Esto da pie a una definición que será muy útil para este trabajo, la cual es la definición de *grupo cíclico*.

Definición 2.2.2. *Sea G un grupo. Decimos que G es un **grupo cíclico** si $G = \langle g \rangle$ para algún $g \in G$. A g le llamaremos un **generador** de G.*

Ejemplo 2.2.3. *Sea $G = \mathbb{Z}$ el grupo de los números enteros con la suma usual y $a \in G$, entonces el conjunto $\langle a \rangle$ lo podemos escribir como $\{na | n \in \mathbb{Z}\} = n\mathbb{Z}$, recordando la notación aditiva. Notemos de manera sencilla que $\mathbb{Z} = \langle 1 \rangle$, ya que cada entero $n = n \cdot 1$ es múltiplo de 1, por lo que $(\mathbb{Z}, +)$ es un grupo cíclico. Además, también $\mathbb{Z} = \langle -1 \rangle$, pues $n = (-n)(-1)$, para cada $n \in \mathbb{Z}$. Con esto observamos que un grupo cíclico puede tener más de un generador.*

Ejemplo 2.2.4. *Consideremos a $G = \{1, -1, i, -i\} \subseteq \mathbb{C}$ un grupo con la operación multiplicación de los números complejos. Notemos que G es un grupo cíclico, ya que i es un generador de G*

$$\langle i \rangle = \{i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i\} = G.$$

Para concluir con la sección probaremos que un subgrupo de un grupo cíclico es un subgrupo cíclico.

Teorema 2.2.5. *Sea G un grupo cíclico y $H \leq G$ un subgrupo de G. Entonces H es un subgrupo cíclico.*

Demostración. Sea G un grupo cíclico. Entonces existe $a \in G$ tal que $\langle a \rangle = G$. Sea $H \leq G$ un subgrupo de G. Si $H = \{e\}$ es el subgrupo trivial se sigue que $\langle e \rangle = H$. Sea $H \leq G$ un subgrupo de G no trivial. Entonces existe un $a^m \in H$ tal que $m \neq 0$. Si m es un entero positivo, entonces $m \in \{n \in \mathbb{N}^+ | a^n \in H\}$ y si m es un entero negativo, dado que $a^{-m} = (a^m)^{-1}$ y $a^m \in H$, entonces $a^{-m} \in H$ y así $-m \in \{n \in \mathbb{N}^+ | a^n \in H\}$. En cualquier caso, $\{n \in \mathbb{N}^+ | a^n \in H\} \neq \emptyset$. Luego, por el principio del buen orden existe $k \neq 0$ elemento mínimo de $\{n \in \mathbb{N}^+ | a^n \in H\}$ entero positivo más pequeño tal que $a^k \in H$. Demostraremos que $\langle a^k \rangle = H$.

Como $a^k \in H$ y H es un subgrupo, entonces $(a^k)^m \in H$ para toda $m \in H$, probando así que $\langle a^k \rangle \subseteq H$.

A la inversa, dado que H es un subgrupo de $G = \langle a \rangle$ se tiene que los elementos de H son potencias de a. Sea $a^m \in H$ un elemento de H. Por el algoritmo de la división, existen enteros q, r tales que

$$m = qk + r, \qquad 0 \leq r < k,$$

por lo tanto $r = m + qk$. Supongamos por reducción al absurdo que $r \neq 0$, así

$$a^r = a^{m-qk} = a^m a^{-qk} = a^m (a^k)^{-q} \in H$$

ya que H es un subgrupo es cerrado bajo la multiplicación y para cada elemento del subgrupo, el inverso también está en el subgrupo. Notemos que por el algoritmo de la división $r < k$, entonces encontramos un entero r distinto de cero más pequeño que k tal que $a^r \in H$, lo cual es una contradicción por la elección de k. Así, $r = 0$. Dado esto tenemos que

$$a^m = a^{qk} = (a^k)^q \in H$$

lo que nos dice que a^k es generador de H.

Por lo tanto $\langle a^k \rangle = H$ y en consecuencia H es un subgrupo cíclico. □

2.3. Suma directa de grupos

En esta última sección veremos tres conceptos importantes, de los cuales uno de ellos nos ayudará en la demostración de un lema en el Capítulo 4.

Notación 2.3.1. *Dado que trabajaremos a partir de ahora con grupos abelianos, usaremos la notación aditiva en todo momento, por lo que el neutro e lo denotaremos con el* 0.

Definición 2.3.1. *Sea $(G, +)$ un grupo abeliano. La **suma interna** de una familia finita $\{H_i\}_{i=1}^n$ de subgrupos de G es el conjunto*

$$\sum_{i=1}^{n} H_i := \{x = h_1 + h_2 + \ldots + h_n \in G : h_i \in H_i \ \forall i\}$$

Para cada $i = 1, 2, \ldots, n$ consideramos la suma de subgrupos

$$\sum_{j \neq i} H_j = H_1 + H_2 + \ldots + H_{i-1} + \overline{H}_i + H_{i+1} + \ldots + H_n$$

donde $\overline{H}_i = \{0\}$ es el subgrupo trivial abeliano.

Veamos que este conjunto es un subgrupo.

Proposición 2.3.1. *Sea $(G, +)$ un grupo abeliano y consideremos $\{H_i\}_{i=1}^n$ una familia finita de subgrupos de G, entonces*

$$H = \sum_{i=1}^{n} H_i$$

es un subgrupo de G. Además

$$H = \langle H_1 \cup H_2 \cup \ldots \cup H_n \rangle$$

Demostración. Notemos que H es no vacío, ya que al ser cada H_i subgrupos de G para toda $1 \leq i \leq n$ se tiene que $0 \in H_i$ para todo $1 \leq i \leq n$, por lo tanto $0 = \underbrace{0 + \ldots + 0}_{n-\text{veces}} \in H$.

Veamos que H es cerrado bajo la operación de G, esto es, probemos que si $h, k \in H$, entonces $h + k \in H$.

En efecto. Sean $h, k \in H$, dados por

$$h = h_1 + h_2 + \ldots + h_n, \qquad k = k_1 + k_2 + \ldots + k_n$$

donde $h_i, k_i \in H_i$ para todo $1 \leq i \leq n$. Entonces por conmutatividad y asociatividad

$$h + k = (h_1 + k_1) + (h_2 + k_2) + \ldots + (h_n + k_n).$$

Como para cada $1 \leq i \leq n$, H_i es subgrupo de G, y $h_i, k_i \in H_i$, se sigue que cada $h_i + k_i \in H_i$. Por lo tanto $h + k \in H$.

Por último, veamos que si $h \in H$ entonces $-h \in H$. Como $h \in H$ tenemos que

$$h = h_1 + h_2 + \ldots + h_n$$

dado que cada $h_i \in H_i$ para todo $1 \leq i \leq n$ así $-h_i \in H_i$, pues $\{H_i\}_{i=1}^n$ es una familia de subgrupos de G. Por lo tanto $-h = (-h_1) + (-h_2) + \ldots + (-h_n) \in H$. Luego,

$$H = \sum_{i=1}^{n} H_i$$

es un subgrupo de G.

Por último probemos que

$$H = \langle H_1 \cup H_2 \cup \ldots \cup H_n \rangle.$$

$\supseteq$) Veamos primero que $H_1 \cup H_2 \cup \ldots \cup H_n$ es subconjunto de H. Sea $h \in H_1 \cup H_2 \cup \ldots \cup H_n$. Supongamos sin pérdida de generalidad que $h \in H_1$, entonces h lo podemos escribir como

$$h = h + 0 + \ldots + 0$$

donde $0 \in H_i$ es el neutro para toda $2 \leq i \leq n$. Por lo tanto $h \in H$. Así, $H_1 \cup H_2 \cup \ldots \cup H_n \subseteq H$, y por el Teorema 2.2.1, concluimos que

$$\langle H_1 \cup H_2 \cup \ldots \cup H_n \rangle \subseteq H$$

.

$\subseteq$) Sea $h \in H$, entonces

$$h = h_1 + h_2 + \ldots + h_n$$

donde $h_i \in H_i$ para todo $1 \leq i \leq n$ y en consecuencia $h_i \in H_1 \cup H_2 \cup \ldots \cup H_n$ para todo $1 \leq i \leq n$. Además,

$$H_1 \cup H_2 \cup \ldots \cup H_n \subseteq \langle H_1 \cup H_2 \cup \ldots \cup H_n \rangle$$

teniendo así que $h_i \in \langle H_1 \cup H_2 \cup \ldots \cup H_n \rangle$ para todo $1 \leq i \leq n$. Luego $h = h_1 + h_2 + \ldots + h_n \in \langle H_1 \cup H_2 \cup \ldots \cup H_n \rangle$.

□

Definición 2.3.2. *Sea $(G,+)$ un grupo abeliano y $\{H_i\}_{i=1}^n$ una familia finita de subgrupos de G. Decimos que G es la* ***suma directa interna*** *de $\{H_i\}_{i=1}^n$ si*

$$G = \sum_{i=1}^{n} H_i \qquad y \qquad H_i \cap \left(\sum_{j \neq i} H_j \right) = \{0\}, \qquad \forall i \in \{1, \ldots, n\}$$

y la denotamos como

$$G = \bigoplus_{i=1}^{n} H_i.$$

A continuación, damos una caracterización de la suma directa interna.

Proposición 2.3.2. *Sea $(G,+)$ un grupo abeliano y $\{H_i\}_{i=1}^n$ una familia finita de subgrupos de G. La suma $H_1 + H_2 + \ldots + H_n$ es directa si y sólo si para todos $x_1 \in H_1, \ldots, x_n \in H_n$*

$$x_1 + x_2 + \ldots + x_n = 0 \implies x_1 = x_2 = \ldots = x_n = 0.$$

Demostración. $\implies$) Supongamos que la suma $H_1 + \ldots + H_n$ es directa. Sean $x_i \in H_i$ con $1 \leq i \leq n$ tales que $x_1 + \ldots + x_i + \ldots + x_n = 0$. Entonces tenemos que para $1 \leq i \leq n$

$$x_i = -x_1 - \ldots - \overline{x_i} - \ldots - x_n,$$

donde $\overline{x_i} = 0$. Así, dado que $x_i \in H_i$ y $x_i = -x_1 - \ldots - \overline{x_i} - \ldots - x_n \in \sum_{j \neq i} H_j$, se sigue que $x_i \in H_i \cap \left(\sum_{j \neq i} H_j \right)$ pero como la suma $H_1 + \ldots + H_n$ es directa, tenemos que $H_i \cap \left(\sum_{j \neq i} H_j \right) = \{0\}$, por lo que $x_i = 0$ para todo $1 \leq i \leq n$.

$\impliedby$) Supongamos que para todos $x_1 \in H_1, \ldots, x_n \in H_n$

$$x_1 + x_2 + \ldots + x_n = 0 \implies x_1 = x_2 = \ldots = x_n = 0.$$

Consideremos $1 \leq i \leq n$ arbitraria y $x_i \in H_i \cap \left(\sum_{j=i} H_j \right)$, entonces podemos escribir $x_i = y_1 + \cdots + y_{i-1} + y_{i+1} + \cdots + y_n$ con $y_j \in H_j$ para toda $j \in \{1, \ldots, i-1, i+1, n\}$. Así,

$$x_i - y_1 - \cdots - y_{i-1} - y_{i+1} - \cdots - y_n = 0$$

lo que por hipótesis implica que $x_i = -y_1 = \cdots = -y_{i-1} = -y_{i+1} = \cdots = -y_n = 0$, en particular $x_i = 0$. Luego $H_i \cap \left(\sum_{j=i} H_j \right) = \{0\}$. □

Veamos un ejemplo sencillo.

Ejemplo 2.3.3. *Sea $\mathbb{R}^3 = \{(x,y,z) | x,y,z \in \mathbb{R}\}$. Notemos que $(\mathbb{R}^3,+)$ es un grupo abeliano con la suma*

coordenada a coordenada. Consideremos los planos coordenados

$$XY = \{(x, y, 0) \in \mathbb{R}^3 | x, y \in \mathbb{R}\}, \quad YZ = \{(0, y, z) \in \mathbb{R}^3 | y, z \in \mathbb{R}\}$$

Notemos que XY y YZ son subgrupos de $\mathbb{R}^3$. Además, $\mathbb{R}^3$ lo podemos ver como una suma interna de XY y YZ; esto es,

$$\mathbb{R}^3 = XY + YZ$$

pues cada $(x, y, z) \in \mathbb{R}^3$ lo podemos escribir como

$$(x, y, z) = \left(x, \frac{y}{2}, 0\right) + \left(0, \frac{y}{2}, z\right).$$

Sin embargo, no es suma directa interna ya que $XY \cap YZ = \{(0, y, 0) | y \in \mathbb{R}\}$.

Ejemplo 2.3.4. *Sea $\mathbb{R}^2 = \{(x, y) | x, y \in \mathbb{R}\}$. Notemos que $(\mathbb{R}^2, +)$ es un grupo abeliano con la suma coordenada a coordenada. Consideremos a $V_1 = \{(x, 2x) | x \in \mathbb{R}\}$ y $V_2 = \{(x, 3x) | x \in \mathbb{R}\}$. Notemos que $\mathbb{R}^2 = V_1 + V_2$ pues cada $(x, y) \in \mathbb{R}^2$ lo podemos escribir como*

$$(x, y) = (3x - y, 2(3x - y)) + (y - 2x, 3(y - 2x))$$

Además si $(x, 2x) + (y, 3y) = (0, 0)$ entonces tendríamos que $x = y = 0$, y por la Proposición 2.3.2 tenemos entonces que $\mathbb{R}^2 = V_1 \oplus V_2$.

Para concluir la sección, veremos otra definición, un tanto parecida a la de suma directa interna. Este concepto será fundamental en el último capítulo.

Definición 2.3.3. *Sea $\{(G_i, +)\}_i^n$ una familia finita de grupos abelianos. Definimos la **suma directa externa** como el par $(G, +)$, donde*

$$G = G_1 \times G_2 \times \ldots \times G_n$$

y la operación está definida como

$$(g_1, g_2, \ldots, g_n) + (h_1, h_2, \ldots, h_n) = (g_1 + h_1, g_2 + h_2, \ldots, g_n + h_n)$$

donde $g_i, h_i \in G_i$, con $1 \leq i \leq n$.

Por simplicidad, en vez de escribir a la familia de grupos abelianos como $\{(G_i, +)\}_i^n$ solamente la escribiremos como $\{G_i\}_i^n$. Veamos que la suma directa externa de grupos abelianos es un grupo abeliano.

Proposición 2.3.5. *Sea $\{G_i\}_i^n$ una familia finita de grupos abelianos, entonces la **suma directa externa**, definida como G, es un grupo abeliano.*

Demostración. Sea $\{G_i\}_i^n$ una familia de grupos abelianos y G la suma directa externa de dicha familia. Notemos que la suma en G se definió como la suma entrada a entrada. Dado esto, como cada G_i es un grupo abeliano,

entonces + en cada G_i es asociativa para toda $1 \leq i \leq n$, entonces la suma en G es asociativa. En efecto, sean $g, h, k \in G$ tales que

$$g = (g_1, g_2, \ldots, g_n), \quad h = (h_1, h_2, \ldots, h_n), \quad k = (k_1, k_2, \ldots, k_n)$$

donde $g_i, h_i, k_i \in G_i$, para toda $1 \leq i \leq n$, entonces

$$\begin{aligned} g + (h + k) &= (g_1, g_2, \ldots, g_n) + [(h_1, h_2, \ldots, h_n) + (k_1, k_2, \ldots, k_n)] \\ &= (g_1, g_2, \ldots, g_n) + (h_1 + k_1, h_2 + k_2, \ldots, h_n + k_n) \\ &= (g_1 + (h_1 + k_1), g_2 + (h_2 + k_2), \ldots, g_n + (h_n + k_n)) \\ &= ((g_1 + h_1) + k_1, (g_2 + h_2) + k_2, \ldots, (g_n + h_n) + k_n) \\ &= (g_1 + h_1, g_2 + h_2, \ldots, g_n + h_n) + (k_1, k_2, \ldots, k_n) \\ &= [(g_1, g_2, \ldots, g_n) + (h_1, h_2, \ldots, h_n)] + (k_1, k_2, \ldots, k_n) \\ &= (g + h) + k, \end{aligned}$$

por lo tanto, la suma en G es asociativa. Notemos que $0 = (0, 0, \ldots, 0)$ es el neutro aditivo en G. En efecto, sea $g \in G$, entonces

$$\begin{aligned} g + 0 &= (g_1, g_2, \ldots, g_n) + (0, 0, \ldots, 0) \\ &= (g_1 + 0, g_2 + 0, \ldots, g_n + 0) \\ &= (g_1, g_2, \ldots, g_n) = g. \end{aligned}$$

Análogamente $0 + g = g$. Notemos que al ser G_i un grupo abeliano, para toda $1 \leq i \leq n$, entonces cada $g_i \in G_i$ tiene inverso y es $-g_i \in G_i$, para toda $1 \leq i \leq n$. Veamos que $-g = (-g_1, -g_2, \ldots, -g_n)$ es el inverso de $g \in G$. En efecto

$$\begin{aligned} g + (-g) &= (g_1, g_2, \ldots, g_n) + (-g_1, -g_2, \ldots, -g_n) \\ &= (g_1 + (-g_1), g_2 + (-g_2), \ldots, g_n + (-g_n)) \\ &= (0, 0, \ldots, 0) = 0. \end{aligned}$$

Por último, sean $g, h \in G$, entonces

$$\begin{aligned} g + h &= (g_1, g_2, \ldots, g_n) + (h_1, h_2, \ldots, h_n) \\ &= (g_1 + h_1, g_2 + h_2, \ldots, g_n + h_n) \\ &= (h_1 + g_1, h_2 + g_2, \ldots, h_n + g_n) \\ &= (h_1, h_2, \ldots, h_n) + (g_1, g_2, \ldots, g_n) = h + g. \end{aligned}$$

Luego, G es un grupo abeliano. □

Ejemplo 2.3.6. *A lo largo de este trabajo consideraremos frecuentemente el grupo $\mathbb{Z}^n$ que es una suma directa externa formada por n copias del grupo abeliano $\mathbb{Z}$. Esto es*

$$\mathbb{Z}^n = \mathbb{Z} \times \ldots \times \mathbb{Z}.$$

Por último, hagamos una sencilla obervación, en la cual veremos cómo se relacionan la suma directa externa y la suma directa interna de grupos. Sea $G = G_1 \times \ldots \times G_n$ una suma directa externa, donde $\{G_i\}_{i=1}^n$ es una familia de grupos abelianos. Si consideramos los grupos $G_i^* = \{(0, 0, \ldots, x_i, \ldots, 0, 0) \mid x_i \in G_i, \forall 1 \leq i \leq n\}$, los cuales son subgrupos de G, se puede ver claramente que $G = G_1^* \oplus \ldots \oplus G_n^*$, teniendo así que

$$G_1 \times G_2 \times \ldots \times G_n = G_1^* \oplus G_2^* \oplus \ldots \oplus G_n^*.$$

Ahora, si G es un grupo abeliano, $H_1, \ldots, H_n$ son subgrupos de G y $G = H_1 \oplus H_2 \oplus \ldots \oplus H_n$, consideremos la suma directa externa $H_1 \times H_2 \times \ldots \times H_n$ y definamos la función

$$\phi : H_1 \times H_2 \times \ldots \times H_n \to G$$

con $\phi(x_1, \ldots, x_n) = x_1 + \cdots + x_n$. Entonces ϕ resulta ser un isomorfismo de grupos teniendo así que

$$H_1 \times H_2 \times \ldots \times H_n \cong H_1 \oplus H_2 \oplus \ldots \oplus H_n = G.$$

De esta manera, toda suma directa externa es una suma directa interna, y toda suma directa interna es isomorfa a una suma directa externa. Es por ello que, haciendo un abuso de notación, podemos escribir una suma directa externa usando la misma notación que para una suma directa interna, es decir $G = G_1 \oplus \ldots \oplus G_n$ para referirnos a la suma directa externa de $G_1, \ldots, G_n$.

Capítulo 3

Sistemas de ecuaciones lineales diofantinas

Este capítulo se enfocará en hacer una generalización al material de ecuaciones lineales diofantinas desarrollado en el primer capítulo. Iniciaremos analizando cuáles son las condiciones para que la ecuación

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c, \tag{3.1}$$

donde $a_1, \ldots, a_n, c \in \mathbb{Z}$, tenga soluciones enteras. Además, generalizaremos esto aún más viendo cuáles son las condiciones para que el **sistema de ecuaciones lineales diofantinas**

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \quad \cdots \quad + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \quad \cdots \quad + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \quad \cdots \quad + a_{mn}x_n = b_m, \end{cases} \tag{3.2}$$

donde $a_{ij} \in \mathbb{Z}$ para toda $1 \leq i \leq m$ y para toda $1 \leq j \leq j$ y $b_1, \ldots b_m \in \mathbb{Z}$, tenga soluciones enteras. Veremos también un método particular para resolver las ecuaciones del tipo 3.1 y estudiaremos dos métodos para resolver sistemas del tipo 4 en términos de reducción modular de renglones o de columnas de la matriz de coeficientes del sistema, lo que nos llevará a otra manera de resolver una ecuación lineal diofantina de n incógnitas.
En la última sección de este capítulo estudiaremos la forma normal de Smith de una matriz y cómo ésta nos permite dar condiciones equivalentes para que un sistema de ecuaciones lineales diofantinas tenga solución y en caso de que existan encontrarlas.

3.1. Ecuaciones lineales diofantinas de n incógnitas

En el Capítulo 1 vimos las condiciones para que la ecuación

$$ax + by = c$$

con $a, b, c \in \mathbb{Z}$ distintos de cero, tuviera solución en los enteros. Ahora, en esta sección nos enfocaremos en saber cuáles son las condiciones para que una ecuación lineal diofantina de n incógnitas tenga soluciones enteras; esto quiere decir que si consideramos $n \geq 3$ y $a_1, \ldots, a_n, b \in \mathbb{Z}$ números enteros distintos de cero, veremos qué condiciones deben satisfacer estos números para que la ecuación

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

tenga soluciones enteras. Además, si tiene soluciones ¿cuántas tiene y cuáles son? Para ello, introduciremos una manera de calcular el máximo común divisor de n enteros de forma recursiva, pero antes daremos la definición de **combinación lineal de n números enteros positivos** y veremos una generalización del Teorema 1.2.5.

Definición 3.1.1. *Sea $n \in \mathbb{N}$ con $n \geq 2$. Una **combinación lineal de n números enteros positivos** $a_1, a_2, \ldots, a_n$ es una suma de la forma*

$$\alpha_1a_1 + \alpha_2a_2 + \ldots + \alpha_na_n$$

con $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}$.

Ejemplo 3.1.1. *Notemos que a 12 lo podemos ver como combinación lineal de $6, 4, 12$ y 8, pues*

$$2 \cdot 6 + (-1) \cdot 4 + 3 \cdot 12 + (-4) \cdot 8 = 12.$$

Generalicemos la definición de máximo común divisor para más de dos números:

Definición 3.1.2. *(**Máximo Común Divisor Generalizado**) Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ no todos nulos. Decimos que d es el **máximo común divisor** de $a_1, a_2, \ldots, a_n$ si:*

1. *$d|a_i$ para toda $1 \leq i \leq n$,*
2. *dado $d' \in \mathbb{Z}$, si $d'|a_i$ para toda $1 \leq i \leq n$, entonces $d' \leq d$,*

y lo denotamos como $d = (a_1, a_2, \ldots, a_n)$.

Recordemos que $(a, 0) = |a|$, para todo a no nulo. Entonces de manera más general, si consideramos $a_1, \ldots, a_i, \ldots, a_n \in \mathbb{Z}$ de tal forma que para alguna $1 \leq i \leq n$, $a_i = 0$, entonces

$$(a_1, \ldots, a_i, \ldots, a_n) = (a_1, \ldots, a_{i-1}, a_{i+1}, a_n).$$

Así, basta calcular el máximo común divisor de los enteros no nulos. Además, dado que $a \mid b$ si y sólo si $ua \mid vb$ con $u, v \in \{1, -1\}$, consideraremos a partir de ahora $a_1, a_2, \ldots, a_n \in \mathbb{Z}^+$.

Teorema 3.1.2. *El máximo común divisor de $a_1, a_2, \ldots, a_n \in \mathbb{Z}^+$ enteros positivos es el menor entero positivo que es una combinación lineal de $a_1, a_2, \ldots, a_n$.*

Demostración. Consideremos el conjunto de todas las combinaciones lineales enteras positivas de $a_1, \ldots, a_n$

$$S = \{x \in \mathbb{Z}^+ | x = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n \text{ y } \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}$$

Notemos que es no vacío, pues por hipótesis $a_1 > 0$ y se puede escribir de la siguiente manera

$$a_1 = 1 \cdot a_1 + 0 \cdot a_2 + \ldots + 0 \cdot a_n \in S.$$

Así, por el principio del buen orden, S tiene un elemento mínimo. Llamemos a este elemento mínimo d y demostremos que justamente es el máximo común divisor de $a_1, \ldots, a_n$.

Como d es un elemento de S entonces $d \in \mathbb{Z}^+$ y

$$d = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n$$

para algunos enteros $\alpha_1, \ldots, \alpha_n$. De la Definición 3.1.2, queremos probar que $d|a_i$, para toda $1 \leq i \leq n$ y que además cualquier divisor común d' de $a_1, \ldots, a_n$, es menor o igual que d.

1. Veamos que $d|a_i$ para toda $1 \leq i \leq n$. Primero veamos que $d|a_1$. Por el algoritmo de la división existen enteros $q, r \in \mathbb{Z}$ tales que $a_1 = qd + r$ con $0 \leq r < d$. Por otra parte tenemos que

   $$d = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n.$$

   Supongamos por contradicción que $d \nmid a_1$, es decir que $r > 0$. Tenemos que

   $$\begin{aligned} r &= a_1 - qd \\ &= a_1 - q(\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n) \\ &= (1 - q\alpha_1)a_1 + (-q\alpha_2)a_2 + \ldots + (-q\alpha_n)a_n \end{aligned}$$

   así, escribimos a r como combinación lineal de $a_1, \ldots, a_n$. Pero ya que supusimos que $r > 0$ y por el algoritmo de la división $r < d$, entonces r sería un elemento de S más pequeño que d, lo cual es una contradicción. Por tanto $r = 0$ y así $a_1 = dq$. Luego $d|a_1$.
   Análogamente $d|a_i$ para cada $2 \leq i \leq n$.

2. Veamos ahora que si $d'|a_i$, para cada $1 \leq i \leq n$ entonces $d' \leq d$. Supongamos que $d'|a_i$, para cada $1 \leq i \leq n$, entonces por el Teorema 1.1.4 se tiene que

   $$d'|\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n$$

   con $d = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n$, entonces $d'|d$. Luego por Proposición 1.1.3 se sigue que $|d'| \leq |d|$, y como $d' \leq |d'|$ y $|d| = d$ tenemos que $d' \leq d$.

Dado que se cumplen las condiciones de la Definición 3.1.2 entonces $d = (a_1, a_2, \ldots, a_n)$. □

Corolario 3.1.3. *Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ números enteros. Sea $d = (a_1, a_2, \ldots, a_n)$ y d' un divisor común de $a_1, a_2, \ldots, a_n$, entonces $d'|d$.*

Demostración. Como $d = (a_1, a_2, \ldots, a_n)$ entonces por el teorema anterior a d lo podemos escribir como combinación lineal de $a_1, a_2, \ldots, a_n$, esto es, existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}$ números enteros tales que

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = d$$

Como d' es un divisor común de $a_1, a_2, \ldots, a_n$ entonces existen $t_1, t_2, \ldots, t_n \in \mathbb{Z}$ tales que

$$a_1 = d't_1, \quad a_2 = d't_2, \quad \ldots, a_n = d't_n$$

por lo tanto, tenemos que

$$\begin{aligned} a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n &= d \\ d't_1\alpha_1 + d't_2\alpha_2 + \ldots + d't_n\alpha_n &= d \\ d'(t_1\alpha_1 + t_2\alpha_2 + \ldots + t_n\alpha_n) &= d \end{aligned}$$

Luego, $d'|d$. □

A continuación, veremos cómo calcular el máximo común divisor de n números enteros positivos de manera recursiva (recordemos que si queremos calcular el máximo común divisor de enteros negativos, basta calcular el máximo común divisor para sus valores absolutos).

Teorema 3.1.4. *Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}^+$. Entonces*

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

Demostración. Sea $d = (a_1, a_2, \ldots, a_n)$, $d' = (a_1, a_2, \ldots, a_{n-1})$ y $d'' = (d', a_n)$. Veamos que $d = d''$.
Como $d = (a_1, a_2, \ldots, a_n)$ entonces $d|a_i$, para todo $1 \leq i \leq n$. En particular $d|a_i$, para todo $1 \leq i \leq n-1$ y dado que $d' = (a_1, a_2, \ldots, a_{n-1})$ entonces por el Corolario anterior $d|d'$. Además $d|a_n$, se sigue que $d|d'$ y $d|a_n$ por lo que $d|(d', a_n) = d''$. Luego $d|d''$.
Dado que $d'' = (d', a_n)$ entonces $d''|d'$ y $d''|a_n$. Además como $d''|d'$ y $d' = (a_1, a_2, \ldots, a_{n-1}) \mid a_i$, para toda $1 \leq i \leq n-1$, por transitividad $d''|a_i$, para toda $1 \leq i \leq n-1$. Por lo tanto $d''|a_i$, para cada $1 \leq i \leq n$. Luego, $d''|d$.
Así por el Teorema 1.1.4 se tiene que $|d| = |d''|$. Pero como $d, d'' \geq 0$, concluimos que $d = d''$. □

Ejemplo 3.1.5. *Usemos el teorema anterior para calcular el máximo común divisor de* $18, 24, 36$ *y* 63.

$$\begin{aligned}(18, 24, 36, 63) &= ((18, 24, 36), 63)\\ &= (((18, 24), 36), 63)\\ &= ((6, 36), 63)\\ &= (6, 63)\\ &= 3.\end{aligned}$$

Con lo anterior podemos responder la primera pregunta que habíamos planteado: ¿cuáles son las condiciones para que la ELD

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

tenga soluciones? Claro, podemos hacer uso de nuestra intuición y recordar que para una ELD de dos variables $ax+by = c$, con $a, b, c \in \mathbb{Z}\setminus\{0\}$, existen soluciones enteras si y sólo si el máximo común divisor de los coeficientes a, b divide a c. Basándonos en ello, la respuesta podría ser justamente una generalización de eso; de hecho, el siguiente teorema le da la razón total a nuestra intuición.

Teorema 3.1.6. *Sean* $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. *Consideremos la ELD* $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, *entonces existen soluciones enteras para la ELD si y sólo si* $(a_1, a_2, \ldots, a_n)|b$.

Demostración. Observemos que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ tiene soluciones enteras si y sólo si $|a_1|x_1 + |a_2|x_2 + \ldots + |a_n|x_n = b$ tiene soluciones enteras, y $(a_1, a_2, \ldots, a_n) = (|a_1|, |a_2|, \ldots, |a_n|)$ por lo que basta probar el resultado para $a_1, \ldots, a_n \in \mathbb{Z}^+$.

$\Longrightarrow$) Supongamos que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ tiene soluciones enteras. Consideremos $(s_1, \ldots, s_n)$ una solución. Entonces

$$a_1s_1 + a_2s_2 + \ldots + a_ns_n = b.$$

Como $(a_1, a_2, \ldots, a_n) \mid a_i$ para toda $1 \leq i \leq n$, por el Teorema 1.1.4 tenemos que

$$(a_1, a_2, \ldots, a_n) \mid a_1s_1 + a_2s_2 + \ldots + a_ns_n = b.$$

$\Longleftarrow$) Supongamos que $d|b$, donde $d = (a_1, \ldots, a_n)$. Por el Teorema 3.1.2 existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}$ números enteros tales que

$$d = \alpha_1a_1 + \alpha_2a_2 + \ldots + \alpha_na_n, \tag{3.3}$$

como $d|b$ entonces existe $t \in \mathbb{Z}$ tal que $b = dt$. Multiplicando 3.3 por t tenemos

$$b = dt = (\alpha_1a_1 + \alpha_2a_2 + \ldots + \alpha_na_n)t \;=\; \alpha_1(a_1t) + \alpha_2(a_2t) + \ldots + \alpha_n(a_nt)$$

y así $(\alpha_1t, \ldots \alpha_nt)$ es una solución de $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$. □

Ejemplo 3.1.7. *Veamos si la ecuación*

$$18x + 24y + 36z + 63w = 12$$

tiene soluciones enteras. Por el Ejemplo 3.1.5 tenemos que $(18, 24, 36, 63) = 3$ *y* $3|12$. *Entonces por el Teorema anterior, la ecuación dada tiene soluciones enteras.*

Ya tenemos las condiciones para que una ELD de n variables tenga soluciones, pero ¿son finitas dichas soluciones? o ¿al igual que el caso de dos variables, tiene soluciones infinitas siempre y cuando existan estas soluciones? Una vez más, nuestra intuición nos indica que la respuesta sería que tendría infinitas soluciones siempre y cuando la ELD tenga soluciones.

Teorema 3.1.8. *Sean* $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. *Si existen soluciones para la ELD*

$$a_1x_1 + \ldots + a_nx_n = b,$$

entonces estas son infinitas.

Demostración. Sean $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. Supongamos que existen soluciones para la ELD

$$a_1x_1 + \ldots + a_nx_n = b.$$

Sea $(s_1, \ldots, s_n) \in \mathbb{Z}^n$ una solución de dicha ecuación. Dado $t \in \mathbb{Z}$ tenemos que

$$\begin{aligned} &a_1(s_1 - a_2t) + a_2(s_2 + a_1t) + a_3s_3 + \ldots + a_ns_n \\ &= (a_1s_1 + a_2s_2 + a_3s_3 + \ldots + a_ns_n) + (-a_1a_2t + a_2a_1t) \\ &= b + 0 = b. \end{aligned}$$

Entonces el conjunto

$$\{(s_1 - a_2t, s_2 + a_1t, s_3, \ldots, s_n) \mid t \in \mathbb{Z}\}$$

es un conjunto infinito formado por soluciones de $a_1x_1 + \ldots + a_nx_n = b$, por lo que existen una infinidad de soluciones a dicha ecuación.

□

Notemos también que el conjunto

$$\{(s_1, s_2 - a_3t, s_3 + a_2t, s_4, \ldots . s_n) | t \in \mathbb{Z}\}$$

también es un conjunto infinito formado por soluciones de $a_1x_1 + \ldots + a_nx_n = b$, por lo que el conjunto dado en el teorema anterior no cuenta con todas las soluciones a la ELD.

3.2. Método para resolver una ecuación lineal diofantina de n incógnitas

Ahora que hemos entendido las condiciones para que una ecuación lineal diofantina de n incógnitas tenga solución, y en su caso cuántas soluciones existen, buscamos describir el proceso para encontrar dichas soluciones. Este proceso se realizará de forma recursiva y con el fin de entender mejor cómo se realiza, desarollemos primero un ejemplo concreto para después describir el método general a seguir.

Ejemplo 3.2.1. *Recordemos la ELD del Ejemplo 3.1.7*

$$18x + 24y + 36z + 63w = 12. \tag{3.4}$$

Ya vimos que sí existen soluciones, ahora tenemos que encontrarlas. Para ello intentaremos ir reduciendo la ELD a una de dos incógnitas.
Notemos que $(24, 36, 63) = 3$*, entonces* $24y + 36z + 63w = 3(8y + 12z + 21w)$*, denotando a* $8y + 12z + 21w$ *por* u *tenemos así una nueva ELD*

$$18x + 3u = 12 \tag{3.5}$$

notemos que $(18, 3) = 3$ *y* $3|12$ *entonces la Ecuación 3.5 tiene solución. Vemos que* $x_0 = 1$ *y* $u_0 = -2$ *es una solución a esta última ecuación, entonces por el Teorema 1.3.4 las soluciones de la Ecuación 3.5 son de la forma*

$$\begin{aligned} x &= 1 + t_0 \\ u &= -2 - 6t_0, \end{aligned}$$

con $t_0 \in \mathbb{Z}$*. Sustituyendo* u *en* $24y + 36z + 63w = 3u$*, tenemos que* $24y + 36z + 63w = 3(-2 - 6t_0)$*. Como* $(36, 63) = 9$ *entonces* $36z + 63w = 9(4z + 7w)$*, y denotando por* v *a* $4z + 7w$ *obtenemos que* $36z + 63w = 9v$*. Por lo tanto tenemos la ELD*

$$24y + 9v = 3(-2 - 6t_0). \tag{3.6}$$

Como $(24, 9) = 3$ *y* $3 \mid 3(-2-6t_0)$ *la Ecuación 3.6 tiene solución. Observemos que* $24(2)+9(-5) = 3$*, entonces, multiplicando por* $-2 - 6t_0$ *tenemos que*

$$24(2(-2 - 6t_0)) + 9(-5(-2 - 6t_0)) = 3(-2 - 6t_0),$$

obteniendo así una solución particular de la Ecuación 3.6. La solución general viene dada por

$$\begin{aligned} y &= -4 - 12t_0 + 3t_1 \\ v &= 10 + 30t_0 - 8t_1 \end{aligned}$$

con $t_1 \in \mathbb{Z}$. *Sustituyendo* v *en* $36z + 63w = 9v$ *obtenemos una nueva ELD*

$$36z + 63w = 9(10 + 30t_0 - 8t_1). \tag{3.7}$$

Como $(36, 63) = 9$ *y* $9 \mid 9(10 + 30t_0 - 8t_1)$ *entonces la ecuación anterior tiene solución. Además notamos que* $36(2) + 63(-1) = 9$. *De esta manera, multiplicando por* $10 + 30t_0 - 8t_1$, *obtenemos que*

$$36(20 + 60t_0 - 16t_1) + 63(-10 - 30t_0 + 8t_1) = 9(10 + 30t_0 - 8t_1),$$

hallando así una solución particular de la Ecuación 3.7. Por lo tanto, la solución general de la ELD 3.7 viene dada por

$$\begin{aligned} z &= 20 + 60t_0 - 16t_1 + 7t_2 \\ w &= -10 - 30t_0 + 8t_1 - 4t_2 \end{aligned}$$

con $t_2 \in \mathbb{Z}$. *Concluimos entonces que la solución general para la ELD,* $18x + 24y + 36z + 63w = 12$, *es*

$$\begin{aligned} x &= 1 + t_0 \\ y &= -4 - 12t_0 + 3t_1 \\ z &= 20 + 60t_0 - 16t_1 + 7t_2 \\ w &= -10 - 30t_0 + 8t_1 - 4t_2 \end{aligned}$$

con $t_i \in \mathbb{Z}$, *para* $i = 0, 1, 2$.

Este ejemplo nos da una idea de cómo podemos ir construyendo las soluciones de la ELD de n variables

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \tag{3.8}$$

de manera general.

Para el caso $n = 2$ tenemos que, si tiene solución, las soluciones a $a_1x_1 + a_2x_2 = b$ están dadas por

$$\begin{aligned} x_1 &= x_1' + \frac{a_2}{d_1}t_1 \\ x_2 &= x_2' - \frac{a_1}{d_1}t_1 \end{aligned}$$

donde $d_1 = (a_1, a_2)$, $t_1 \in \mathbb{Z}$ y (x_1', x_2') es una solución particular.

Para el caso $n = 3$

$$a_1x_1 + a_2x_2 + a_3x_3 = b$$

sean $d_1 = (a_1, a_2, a_3)$ con $d_1 \mid b$, y $d_2 = (a_2, a_3)$, entonces $d_2 \mid a_2x_2 + a_3x_3$ y así

$$a_2x_2 + a_3x_3 = d_2y_2 \tag{3.9}$$

por lo tanto nos queda una nueva ELD

$$a_1x_1 + d_2y_2 = b \tag{3.10}$$

Notemos que tiene solución, ya que

$$\begin{aligned}(a_1, d_2) &= (a_1, (a_2, a_3)) \\ &= (a_1, a_2, a_3) \\ &= d_1|b.\end{aligned}$$

Entonces si (x_1', y_2') es una solución particular de 3.10, tenemos que la solución general de dicha ecuación, dada por el Teorema 1.3.4, es

$$\begin{aligned}x_1 &= x_1' + \frac{d_2}{d_1}t_1 \\ y_2 &= y_2' - \frac{a_1}{d_1}t_1\end{aligned}$$

con $t_1 \in \mathbb{Z}$. Sustituyendo el valor de y_2 en 3.9 tenemos la nueva ELD

$$a_2x_2 + a_3x_3 = d_2\left(y_2' - \frac{a_1}{d_1}t_1\right). \tag{3.11}$$

Sabemos que d_2 lo podemos expresar como combinación lineal de a_2 y a_3, entonces existen enteros α_1 y β_1 tales que

$$a_2\alpha_1 + a_3\beta_1 = d_2.$$

Multiplicando ambos lados por y_2 tenemos que

$$a_2\alpha_1\left(y_2' - \frac{a_1}{d_1}t_1\right) + a_3\beta_1\left(y_2' - \frac{a_1}{d_1}t_1\right) = d_2\left(y_2' - \frac{a_1}{d_1}t_1\right)$$

obteniendo así una solución particular a la Ecuación 3.9 que es

$$x_2' = \alpha_1\left(y_2' - \frac{a_1}{d_1}t_1\right), \qquad x_3' = \beta_1\left(y_2' - \frac{a_1}{d_1}t_1\right),$$

teniendo así que las soluciones generales de la Ecuación 3.9 son

$$x_2 = x_2' + \frac{a_3}{d_2}t_2$$
$$x_3 = x_3' - \frac{a_2}{d_2}t_2$$

donde $t_2 \in \mathbb{Z}$, concluyendo que las soluciones para el caso $n = 3$ son

$$x_1 = x_1' + \frac{d_2}{d_1}t_1$$
$$x_2 = x_2' + \frac{a_3}{d_2}t_2$$
$$x_3 = x_3' - \frac{a_2}{d_2}t_2$$

donde $t_1, t_2 \in \mathbb{Z}$ son números enteros, $d_1 = (a_1, a_2, a_3)$ y $d_2 = (a_2, a_3)$. Nótese que en dichas soluciones aparecen dos parámetros, t_1 y t_2, pero t_2 depende de t_1.

Podemos usar un procedimiento similar para más variables, pero aparecerán más parámetros, unos dependientes de otros, debido a lo cual el proceso se volverá todavía más laborioso para n mayor que tres. Intentemos sin embargo dar una descripción recursiva del método general para obtener las soluciones:

1. Consideremos la ELD
$$a_1x_1 + \ldots + a_{n-1}x_{n-1} + a_nx_n = b \tag{3.12}$$
y supongamos que $d_n|b$, donde $d_n = (a_1, \ldots, a_n)$. Debido a dicha condición, sabemos que sí tiene soluciones y además hay una infinidad de ellas.

2. Tomaremos los primeros $n-1$ sumandos que aparecen en el lado izquierdo de la Ecuación 3.12
$$a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1}.$$
Sea $d_{n-1} = (a_1, a_2, \ldots, a_{n-1})$. Como $a_1x_1+a_2x_2+\ldots+a_{n-1}x_{n-1}$ es una combinación lineal de $a_1, a_2, \ldots, a_{n-1}$, entonces debe ser igual a un múltiplo de d_{n-1}, teniendo así que
$$a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} = d_{n-1}y_1 \tag{3.13}$$
para alguna $y_1 \in \mathbb{Z}$.

3. Reescribimos la Ecuación 3.12 como
$$d_{n-1}y_1 + a_nx_n = b.$$
Esta ecuación tiene solución ya que
$$d_n = (a_1, \ldots, a_{n-1}, a_n) = ((a_1, \ldots, a_{n-1}), a_n) = (d_{n-1}, a_n)$$

divide a b. Además, por el Teorema 1.3.4 sabemos cómo son las soluciones y podemos describir con ello a y_1 y a x_n.

4. Para describir ahora a x_{n-1} sustituimos en la ecuación 3.13 el valor de y_1 previamente encontrado y repetimos el mismo proceso pero ahora tomando los primeros $(n-1)-1 = n-2$ sumandos; en esa nueva ecuación lograremos obtener la descripción de x_{n-1}.

5. Seguimos así hasta que nos quede una última ecuación con 2 sumandos, la cual será de la forma

$$a_1x_1 + a_2x_2 = d_2y_{n-1},$$

con $d_2 = (a_1, a_2)$. A partir de ella podremos encontrar cómo deben ser x_1 y x_2.

En la siguiente sección desmostraremos un teorema que nos permitirá, además de saber de otra forma cuándo una ELD de n variables tiene solución, también conocer una forma más explícita de las soluciones a la ELD de n variables.

3.3. Sistemas de ecuaciones lineales diofantinas de $m \times n$

Ahora hagamos la siguiente pregunta, ¿podremos encontrar soluciones a un sistema de m ecuaciones lineales diofantinas de n incógnitas? Es decir ¿podemos encontrar las soluciones enteras del siguiente sistema?

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \quad \cdots \quad + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \quad \cdots \quad + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \quad \cdots \quad + a_{mn}x_n = b_m. \end{cases}$$

La respuesta es que sí. Para ello consideraremos la forma matricial del sistema de ELD, $AX = B$, donde A es una matriz de $m \times n$ y B es una matriz de $m \times 1$, ambas con entradas enteras y no nulas, dadas a continuación:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}, \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Antes de adentrarnos a las soluciones de dicho sistema tenemos que recordar algunos resultados referentes a matrices para adaptarlos posteriormente a matrices con entradas enteras.

Consideremos primero un campo F. Al conjunto de las matrices de $m \times n$ con coeficientes en F lo denotaremos como $M_{m\times n}(F)$.

Definición 3.3.1. *Sea $A \in M_{m\times n}(F)$ una matriz. Decimos que A es una* ***matriz escalonada por filas*** *si es la matriz nula o cumple que:*

1. *Todas las filas con ceros están debajo de las filas no nulas de la matriz.*
2. *La primera entrada distinta de cero de cada fila no nula, llamada la* ***entrada principal de la fila****, está a la derecha de todas las entradas principales de los renglones previos.*

Ejemplo 3.3.1. *Las siguientes matrices son matrices escalonadas por filas:*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 4 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

La siguiente matriz no es escalonada por filas:

$$C = \begin{pmatrix} 0 & 3 & 2 & 1 & 8 \\ 1 & 2 & 9 & 0 & 1 \\ 0 & 0 & 1 & 1 & 2 \\ 1 & 0 & 6 & 0 & 0 \end{pmatrix}$$

En este punto es natural preguntarnos si toda matriz se puede transfromar en una escalonada reducida por filas y si es así, cuál sería la manera de poder llegar a ella. La respuesta es sencilla: mediante las llamadas **operaciones elementales por filas**. Éstas son intercambiar filas, multiplicar una fila por un escalar distinto de 0 y sumar a una fila un múltiplo de otra. De manera más precisa tenemos que:

Definición 3.3.2. *Las operaciones elementales por filas de matrices son:*

1. *Intercambiar las filas R_i y R_j, con $i \neq j$, que denotaremos por $R_i \leftrightarrow R_j$.*
2. *Multiplicar una fila R_i por un escalar λ no nulo, que denotaremos por $R_i \to \lambda R_i$.*
3. *Dado λ un escalar reemplazar la fila R_i por $R_i + \lambda R_j$, con $i \neq j$, que denotaremos por $R_i \to R_i + \lambda R_j$.*

De forma análoga, podemos definir las operaciones elementales por columnas de matrices.

En el siguiente resultado se enuncia el hecho de que dichas operaciones permiten llevar una matriz a una en forma escalonada, omitiremos su demostración ya que probaremos un resultado análogo pero en el caso que nos interesa en el cual las entradas de la matriz son números enteros y se usan operaciones elementales modificadas para trabajar sólo con enteros como veremos más adelante.

Teorema 3.3.2. *Toda matriz se puede transformar en una matriz escalonada por filas mediante operaciones elementales por filas.*

Demostración. Ver la demostración en [GL14, p. 494]. □

Justamente la acción de realizar una operación elemental por filas (en este caso, ya que también se puede hacer por columnas) de alguna matriz A es simplemente el multiplicar esa matriz A por la izquierda o por la derecha con otro tipo de matrices, llamadas **matrices elementales**, las cuales se definen de la siguiente forma.

Definición 3.3.3. *Una matriz $E \in M_{n\times n}(F)$ es elemental, si resulta de la matriz identidad $I_{n\times n}$ al realizar una operación elemental sobre las filas (o columnas).*

A continuación enunciaremos un teorema. La demostración es directa analizando los distintos posibles casos y realizando los productos correspondientes.

Teorema 3.3.3. *Sea $A \in M_{m\times n}(F)$. Si B se obtiene de A al realizar una operación elemental sobre los renglones (columnas), y E es la matriz elemental que resulta de $I_{m\times m}$ ($I_{n\times n}$) al realizar la misma operación elemental que se hizo en A, entonces $EA = B$ ($AE = B$).*

Demostración. Ver la demostración en [GL14, p. 546]. □

En consecuencia tenemos lo siguiente.

Observación 3.3.4. *Toda matriz elemental es invertible, y si E es la matriz elemental que se obtiene de aplicar a la identidad la operación elemental e, su matriz inversa es la matriz elemental que se obtiene de aplicar a la identidad la operación elemental inversa de e.*

Del Teorema 3.3.2 y el Teorema 3.3.3 podemos deducir algo muy importante, que será de utilidad en la prueba del resultado principal de esta sección. Digamos que el proceso para escalonar una matriz A por filas mediante operaciones elementales consta de l pasos, obteniendo al final una matriz escalonada B. Entonces tendremos l matrices elementales $E_1, E_2, \ldots, E_l$ correspondientes a cada operación elemental realizada y por el Teorema 3.3.3 se cumplirá la siguiente igualdad:

$$B = E_l \cdots E_2 E_1 A.$$

Del mismo modo, si el proceso para escalonar una matriz A por columnas mediante operaciones elementales consta de m pasos, obteniendo al final una matriz escalonada C, entonces tendremos m matrices elementales $E_1, E_2, \ldots, E_m$ correspondientes a cada operación elemental realizada y de nuevo, por el Teorema 3.3.3 se cumplirá la siguiente igualdad

$$C = AE_1E_2 \cdots E_m.$$

Antes de comenzar con lo importante de la sección, es crucial dar otra definición importante, ya que más adelante nos será de ayuda.

Definición 3.3.4. *El rango de una matriz A es la dimensión del espacio generado por las filas de A y se denota como* $\operatorname{rg}(A)$.

La definición anterior tiene conceptos que no se tratan en este trabajo, por lo que calcular el rango de una matriz basándonos en ella está fuera de nuestro alcance, sin embargo es posible calcularlo usando las operaciones elementales.

Proposición 3.3.5. *Sean $A, B \in M_{m\times n}(F)$ tales que A es equivalente a B mediantes operaciones elementales por filas. Entonces* $\operatorname{rg}(A) = \operatorname{rg}(B)$.

Demostración. Ver en [GL14, p. 574]. □

El resultado anterior también se puede valer cuando hacemos una transformación con operaciones elementales por columnas y además haciendo operaciones elementales, ya sea por columnas o renglones, no lo afecta en absoluto. Gracias a esta proposición podemos enunciar el teorema que nos ayudará a saber el rango de una matriz usando herramientas que tenemos a la mano.

Teorema 3.3.6. *Sea $A \in M_{m\times n}(F)$ una matriz escalonada reducida. Entonces el rango de A es igual al número de renglones distintos de cero en A.*

Demostración. Ver en [GL14, p. 574-575]. □

Notemos que por el momento mencionamos matrices con coeficientes en un campo F. Sin embargo, a partir de ahora buscamos trabajar únicamente con el conjunto de los números enteros, $\mathbb{Z}$, que claramente no es un campo, así que tendremos que definir una nueva forma de llevar una matriz no nula a una forma escalonada por filas. Entonces, si trabajaremos con entradas en $\mathbb{Z}$ ¿cómo podemos llegar a esta forma? Bueno, podremos hacerlo mediante la **reducción modular de filas**, la cual se define como sigue:

Definición 3.3.5. *Las operaciones modulares por filas de matrices son:*

1. *Intercambiar las filas R_i y R_j, que denotaremos por $R_i \leftrightarrow R_j$.*
2. *Multiplicar una fila R_i por -1, que denotaremos por $R_i \to (-1)R_i$.*
3. *Dado $k \in \mathbb{Z}$ reemplazar la fila R_i por $R_i + kR_j$, con $i \neq j$, que denotaremos por $R_i \to R_i + kR_j$.*

A la aplicación de estas operaciones modulares por filas a una matriz con entradas enteras para llevarla a una matriz escalonada, se le conoce como **reducción modular de filas.**

De forma análoga, podemos definir las operaciones modulares por columnas de matrices, las cuales las representaremos con la letra C.

Ejemplo 3.3.7. *Hagamos la reducción modular por filas de la siguiente matriz:*

$$\begin{pmatrix} 2 & 3 & 5 \\ 4 & 1 & 6 \\ 5 & 8 & 12 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 5 \\ 5 & 8 & 12 \\ 0 & 5 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 5 \\ 1 & 1 & 3 \\ 0 & 5 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & -1 \\ 0 & 5 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & 9 \end{pmatrix}.$$

En el proceso anterior hicimos los siguientes cambios de izquierda a derecha:

1) Intercambiamos $R_2 \leftrightarrow R_3$ para posteriormente hacer $R_3 \to R_3 + (-2)R_1$ y finalmente $R_3 \to -R_3$.

2) $R_2 \to R_2 + (-3)R_1$ y después $R_2 \to -R_2$.

3) Intercambiamos $R_2 \leftrightarrow R_1$ y seguido eso $R_2 \to R_2 + (-2)R_1$.

4) Por último hicimos $R_3 \to R_3 + (-5)R_2$.

Además, notemos que la matriz tiene rango 3.

A continuación probaremos un resultado que nos muestra una relación entre el máximo común divisor y la reducción modular por filas de una matriz columna, que generalizaremos después a una matriz $m \times n$.

Lema 3.3.8. *Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ no todos nulos. Si $d = (a_1, a_2, \ldots, a_n)$ es el máximo común divisor de estos enteros, entonces la matriz columna* $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ *puede ser reducida a la matriz* $\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ *por reducción modular por filas.*

Demostración. Hagamos la prueba por inducción matemática sobre n.

1. **Caso base** $n = 2$**:** Hagamos la reducción por filas de la matriz columna $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$. Sea $d = (a_1, a_2)$. Consideremos las siguientes operaciones por filas

$$R_1 \to -R_1 \text{ si } a_1 < 0$$
$$R_2 \to -R_2 \text{ si } a_2 < 0,$$

por lo que podemos suponer que a_1 y a_2 son positivos. Además, haciendo después el siguiente intercambio de filas

$$R_2 \leftrightarrow R_1 \text{ si } a_2 > a_1,$$

podemos suponer que $a_1 > a_2$. Supongamos entonces sin pérdida de generalidad que $a_1 > a_2 > 0$.

Dado esto, por el **algoritmo de la división** existen enteros k_1 y r_1 tales que $a_1 = a_2k_1 + r_1$ con $0 \leq r_1 < a_2$. Entonces, si hacemos la operación modular $R_1 \to R_1 + (-k_1)R_2$ tenemos la matriz columna $\begin{pmatrix} r_1 \\ a_2 \end{pmatrix}$. Como $r_1 < a_2$, intercambiamos los renglones, obteniendo la matriz $\begin{pmatrix} a_2 \\ r_1 \end{pmatrix}$. Si $r_1 > 0$, aplicando una vez más el algoritmo de la división tenemos que $a_2 = r_1k_2 + r_2$ con $k_2, r_2 \in \mathbb{Z}$ enteros y $0 \leq r_2 < r_1$. Haciendo la operación modular $R_1 \to R_1 + (-k_2)R_2$, tenemos la matriz $\begin{pmatrix} r_2 \\ r_1 \end{pmatrix}$.

Claramente el procedimiento que estamos realizando es el mismo que se realiza en la prueba del **algoritmo de Euclides**, por lo que al continuar con este procedimiento al final habremos calculado el máximo común divisor entre a_1 y a_2, el cual es d, y por lo tanto obtenemos la matriz columna $\begin{pmatrix} d \\ 0 \end{pmatrix}$.

Sea $n \in \mathbb{N}$ con $n > 2$.

2. **H.I.**: El resultado es válido para una matriz columna con $n - 1$ renglones.

3. **P.I.**: La reducción modular por filas se hará de abajo hacia arriba y de la misma manera que en el caso base. Recordemos que el Teorema 3.1.4 nos permite hacer lo siguiente:

$$d = (a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, (a_{n-1}, a_n)) = (a_1, a_2, \ldots, d_{n-1}) \tag{3.14}$$

donde $d_{n-1} = (a_{n-1}, a_n)$. Ahora consideremos la matriz columna $\begin{pmatrix} a_1 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix}$. Podemos suponer que a_{n-1} y a_n son positivos ya que en caso contrario podemos realizar las siguientes operaciones por fila

$$R_{n-1} \to -R_{n-1} \text{ si } a_{n-1} < 0$$
$$R_n \to -R_n \text{ si } a_n < 0.$$

Más aún, haciendo

$$R_n \leftrightarrow R_{n-1} \text{ si } a_n > a_{n-1}$$

podemos suponer que $a_{n-1} > a_n$.

Supongamos así, sin pérdida de generalidad, que $a_{n-1} > a_n > 0$, entonces por el caso base sabemos que podemos usar reducción modular para transformar la matriz $\begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix}$ en $\begin{pmatrix} d_{n-1} \\ 0 \end{pmatrix}$, con $d_{n-1} = (a_{n-1}, a_n)$.

Realizando estas mismas operaciones elementales, la matriz columna original quedará de la siguiente manera $\begin{pmatrix} a_1 \\ \vdots \\ a_{n-2} \\ d_{n-1} \\ 0 \end{pmatrix}$. Ahora, por la hipótesis de inducción se tiene que podemos hacer la siguiente reducción modular

$$\begin{pmatrix} a_1 \\ \vdots \\ a_{n-2} \\ d_{n-1} \\ 0 \end{pmatrix} \to \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

donde $d' = (a_1, a_2, \ldots, d_{n-1})$. Pero por la igualdad 3.14, $d = (a_1, a_2, \ldots, d_{n-1})$. Por lo tanto $d' = d$,

teniendo así la reducción buscada

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \to \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

□

El anterior lema también es válido para una matriz renglón y haciendo operaciones modulares por columnas. A continuación probaremos un lema que nos ayudará a comprender cómo el máximo común divisor de las entradas de una columna no se verá afectado al hacer las operaciones modulares por filas; del mismo modo, no se verá afectado el máximo común divisor de las entradas de un renglón al hacer operaciones modulares por columnas.

Lema 3.3.9. *Sean $a_1, \ldots, a_n \in \mathbb{Z}$ números enteros no todos nulos, $i, j \in \{1, 2, \ldots, n\}$ con $i \neq j$ y λ un entero. Entonces*

$$(a_1, \ldots, a_j, \ldots, a_n) = (a_1, \ldots, a_i + \lambda a_j, \ldots, a_j, \ldots, a_n).$$

Demostración. Sean $a_1, \ldots, a_n \in \mathbb{Z}$ números enteros no todos nulos, $i, j \in \{1, 2, \ldots, n\}$ con $i \neq j$ y λ un entero. Consideremos $d = (a_1, \ldots, a_j, \ldots, a_n)$ y $d' = (a_1, \ldots, a_i + \lambda a_j, \ldots, a_j, \ldots, a_n)$.
Como $d = (a_1, \ldots, a_j, \ldots, a_n)$, entonces $d|a_t$ para toda $1 \leq t \leq n$, en particular se tiene que $d|a_i$ y $d|a_j$. Por inciso 4 del Teorema 1.1.4 tenemos que $d|\lambda a_j$, por consiguiente por el inciso 3 de dicho teorema sabemos que $d|a_i + \lambda a_j$. Así, d es un divisor común de $a_1, \ldots, a_i + \lambda a_j, \ldots, a_j, \ldots, a_n$. Como d' es el máximo común divisor de $a_1, \ldots, a_i + \lambda a_j, \ldots, a_j, \ldots, a_n$ por el Corolario 3.1.3 concluimos que $d|d'$.

Ahora como $d' = (a_1, \ldots, a_i + \lambda a_j, \ldots, a_j, \ldots, a_n)$, entonces $d|a_t$ para toda $1 \leq t \leq n$ con $t \neq i$ y $d'|a_i + \lambda a_j$, en particular se tiene que $d|a_i + \lambda a_j$ y $d'|a_j$. Por inciso 4 del Teorema 1.1.4 tenemos que $d'| - \lambda a_j$, entonces por el inciso 3 de dicho teorema sabemos que $d|a_i + \lambda a_j + (-\lambda a_j) = a_i$. Así, d' es un divisor común de $a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n$. Como d es el máximo común divisor de $a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n$ por el Corolario 3.1.3 concluimos que $d'|d$.

Por inciso 1 del Teorema 1.1.4 concluimos que $|d'| = |d|$. Pero el máximo común divisor es siempre positivo, por lo tanto $d = d'$. □

Estos dos lemas nos ayudarán a probar el siguiente teorema que es un análogo al Teorema 3.3.2 para el caso de la reducción modular:

Teorema 3.3.10. *Toda matriz $A = (a_{ij}) \in M_{m\times n}(\mathbb{Z})$ se puede transformar en una matriz escalonada por filas $R \in M_{m\times n}(\mathbb{Z})$ mediante operaciones modulares por filas. Además, si R es no nula con r renglones no nulos y $a'_{1k_1}, \ldots, a'_{rk_r}$ son sus entradas principales y $d_{k_i} = (a_{1k_i}, a_{2k_i}, \ldots, a_{mk_i})$ para $i = 1, 2, \ldots, r$, se tiene que $a'_{1k_1} = d'_{k_1}$, $a'_{ik_i} = \alpha_i d_{k_i}$ y $\alpha_i \in \mathbb{Z}^+$ para $i = 2, \ldots, r$, es decir su primera entrada principal es el máximo común divisor de las entradas de la primera columna de A, y el resto de sus entradas principales son múltiplos positivos del máximo común divisor de las entradas de la columna correspondiente de A.*

Demostración. Si A es la matriz nula, es ya escalonada reducida. Supongamos entonces que A es una matriz no nula.

Haremos la prueba por inducción sobre el número de columnas, *i.e.* sobre n.

1. **Caso base** $n = 1$**:** Se sigue del Lema 3.3.8.

   Sea $n > 1$.

2. **H.I.**: Supongamos que el resultado es válido para matrices de $n-1$ columnas.

3. **P.I.**: Sea $A \in M_{m\times n}(\mathbb{Z})$ no nula dada por:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

   Consideremos la matriz $\tilde{A} \in M_{m\times n-1}(\mathbb{Z})$ que se obtiene de A quitando la columna n. Por la hipótesis de inducción podemos aplicar operaciones modulares a $\tilde{A}$ para obtener una matriz $\tilde{R} \in M_{m\times n-1}(\mathbb{Z})$ escalonada reducida. Si $\tilde{R}$ es nula, el resultado se sigue del Lema 3.3.8. Si $\tilde{R}$ es no nula y tiene $\tilde{r}$ renglones no nulos, sus entradas principales son de la forma $\alpha_1 d_{k_1}, \dots, \alpha_{\tilde{r}} d_{k_{\tilde{r}}}$ con $\alpha_i \in \mathbb{Z}^+$, y $d_{k_i} = (a_{1k_i}, a_{2k_i}, \dots, a_{mk_i})$, para $i = 1, 2, \dots, \tilde{r}$.

   Caso 1. $\tilde{r} = m$.

   Aplicando las mismas operaciones modulares a A tendríamos una matriz de la forma:

$$\begin{pmatrix} 0 & \dots 0 & d_{k_1} & \cdots & & \cdots & & a'_{1(n-1)} & a'_{1n} \\ 0 & \dots 0 & \cdots & \alpha_2 d_{k_2} & & \dots & \dots & a'_{2(n-1)} & a'_{1n} \\ 0 & \dots 0 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots 0 & 0 & 0 & \dots & \alpha_{\tilde{r}} d_{k_{\tilde{r}}} & \dots & a'_{\tilde{r}(n-1)} & a'_{\tilde{r}n} \end{pmatrix}$$

   que ya es una matriz escalonada de la forma buscada.

   Caso 2. $\tilde{r} < m$.

   Aplicando las mismas operaciones a A tendríamos una matriz de la forma:

$$\begin{pmatrix} 0 & \dots 0 & d_{k_1} & \cdots & & \cdots & & a'_{1(n-1)} & a'_{1n} \\ 0 & \dots 0 & \cdots & \alpha_2 d_{k_2} & & \dots & \dots & a'_{2(n-1)} & a'_{1n} \\ 0 & \dots 0 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots 0 & 0 & 0 & \dots & \alpha_{\tilde{r}} d_{k_{\tilde{r}}} & \dots & a'_{\tilde{r}(n-1)} & a'_{\tilde{r}n} \\ 0 & \dots 0 & 0 & 0 & & & \dots & 0 & a'_{(\tilde{r}+1)n} \\ 0 & \dots 0 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots 0 & 0 & 0 & & & \dots & 0 & a'_{mn} \end{pmatrix}. \tag{3.15}$$

Si $a'_{(\tilde{r}+1)n} = \cdots = a'_{mn} = 0$, ésta es una matriz escalonada de la forma buscada. Supongamos entonces que $a'_{(\tilde{r}+1)n}, \ldots, a'_{mn}$ no son todos nulos. Ahora, usando el Lema 3.3.8 podemos transformar la matriz columna $\begin{pmatrix} a'_{(\tilde{r}+1)n} \\ a'_{(\tilde{r}+2)n} \\ \vdots \\ a'_{mn} \end{pmatrix}$ en $\begin{pmatrix} D \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, con $D = (a'_{(\tilde{r}+1)n}, \ldots, a'_{mn})$ y aplicando las mismas operaciones modulares a la matriz 3.15 obtenemos

$$\begin{pmatrix} 0 & \ldots 0 & d_{k_1} & \cdots & & \cdots & & a'_{1(n-1)} & a'_{1n} \\ 0 & \ldots 0 & \cdots & 0 & \alpha_2 d_{k_2} & \ldots & \ldots & a'_{2(n-1)} & a'_{1n} \\ 0 & \ldots 0 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots 0 & 0 & 0 & \ldots & \alpha_{\tilde{r}} d_{k_{\tilde{r}}} & \ldots & a'_{\tilde{r}(n-1)} & a'_{\tilde{r}n} \\ 0 & \ldots 0 & 0 & 0 & & & \ldots & 0 & D \\ 0 & \ldots 0 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots 0 & 0 & 0 & & & \ldots & 0 & 0 \end{pmatrix}. \tag{3.16}$$

Por el lema previo, $d_n = (a_{1n}, \ldots, a_{mn}) = (a'_{1n}, \ldots a'_{\tilde{r}n}, D, 0 \ldots, 0)$ y así $d_n \mid D$, por lo que $D = \alpha_n d_n$ para alguna $\alpha_n \in \mathbb{Z}$. Además como D y d_n son positivos por ser máximos comunes divisores, se tiene que α_n también debe ser positiva. Así, la matriz 3.16 es de la forma buscada.

□

Este último resultado nos permite darnos una idea de cómo tiene que verse la "diagonal principal"de la matriz escalonada al momento de hacer la reducción modular.

En álgebra lineal regularmente se utiliza el **método de eliminación de Gauss-Jordan** para resolver un sistema de ecuaciones lineales, el cual consiste en transformar una matriz en una escalonada. Mediante este proceso se busca reducir el sistema a otro equivalente pero más sencillo de resolver, donde en cada ecuación aparezcan menos incógnitas que en la ecuación anterior; de esta forma al final podemos, en caso de que exista la solución, resolver el sistema, ya sea hallando una única solución, o varias en el caso en que aparezcan parámetros. Antes de justificar lo mencionado anteriormente, daremos la notación de la matriz aumentada.

Notación 3.3.1. *Sean $A \in M_{m\times n}(\mathbb{Z})$ y $B \in M_{m\times k}(\mathbb{Z})$. La matriz aumentada de A y B es*

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \ldots & a_{1n} & b_{11} & b_{12} & \ldots & b_{1k} \\ a_{21} & a_{22} & \ldots & a_{2n} & b_{21} & b_{22} & \ldots & b_{2k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_{m1} & b_{m2} & \ldots & b_{mk} \end{array}\right)$$

y la denotamos por $(A|B)$.

Teorema 3.3.11. *Sean $A, R \in M_{m\times n}(\mathbb{R})$, $B, B' \in M_{m\times 1}(\mathbb{R})$. Si $(A|B)$ es equivalente por renglones a $(R|B')$, entonces los sistemas de ecuaciones lineales $AX = B$ y $RX = B'$ tienen las mismas soluciones.*

Demostración. Ver en el libro [GL14, p. 486]. □

En particular, si $A, R \in M_{m\times n}(\mathbb{Z})$, $B, B' \in M_{m\times 1}(\mathbb{Z})$ y $(R|B')$ se obtiene de $(A|B)$ mediante operaciones modulares, tenemos que $(A|B)$ es equivalente por renglones a $(R|B')$, y por el teorema anterior $AX = B$ y $RX = B'$ tienen las mismas soluciones, de modo que las soluciones enteras de $AX = B$ serán las mismas que las soluciones enteras de $RX = B'$. Basados en este resultado, podríamos usar el método de Gauss-Jordan para buscar las soluciones en los sistemas de ecuaciones diofantinas, sin embargo el resultado no es tan satisfactorio como lo es en el caso de sistemas de ecuaciones con coeficientes en un campo. A continuación ejemplificaremos lo mencionado anteriormente.

Ejemplo 3.3.12. *Consideremos el siguiente sistema de ecuaciones lineales diofantinas:*

$$\begin{pmatrix} 2 & 4 & 5 \\ 3 & 1 & 8 \\ 5 & 8 & 12 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix} \tag{3.17}$$

Usando el método de Gauss-Jordan con operaciones modulares llegamos a lo siguiente:

$$\left(\begin{array}{ccc|c} 2 & 4 & 5 & 2 \\ 3 & 1 & 8 & 5 \\ 5 & 8 & 12 & 3 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & -3 & 3 & 3 \\ 0 & 1 & 2 & 8 \\ 0 & 0 & 7 & 28 \end{array}\right)$$

teniendo así las siguientes ecuaciones:

$$\begin{cases} x - 3y + 3z = 3 \\ \quad y + 2z = 8 \\ \quad\quad 7z = 28. \end{cases}$$

De la última ecuación se deduce que $z = 4$, sustituyendo este valor en la ecuación previa y despejando tenemos que $y = 8 - 2z = 8 - 2(4) = 0$, finalmente de la ecuación anterior se tiene que $x = 3 + 3y - 3z = 3 + 3(0) - 3(4) = -9$. Así, la única solución del sistema es $(-9, 0, 4)$.

Ahora consideremos el siguiente sistema de ecuaciones lineales diofantinas.

$$\begin{pmatrix} 3 & 1 & 4 \\ 7 & 2 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix} \tag{3.18}$$

Una vez más, usando el método de Gauss-Jordan llegamos a lo siguiente:

$$\left(\begin{array}{ccc|c} 3 & 1 & 4 & 2 \\ 7 & 2 & 9 & 5 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{array}\right)$$

donde obtenemos las siguiente ecuaciones:

$$\begin{cases} x + z = 1 \\ y + z = -1 \end{cases}$$

Si damos a z el valor entero que elijamos, i.e. hacemos $z = t_1 \in \mathbb{Z}$ entonces las soluciones al sistema 3.18 están descritas por $x = 1 - t_1$, $y = -1 - t_1$ y $z = -t_1$, donde $t_1 \in \mathbb{Z}$ está fijo. Notemos que x, y y z son números enteros, por lo que logramos conseguir soluciones en los números enteros.
Consideremos ahora el siguiente sistema, similar al anterior, seguido de la reducción obtenida por el método de Gauss-Jordan usando operaciones modulares:

$$\begin{pmatrix} 2 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 17 \\ -13 \end{pmatrix}, \qquad \left(\begin{array}{ccc|c} 2 & 1 & 4 & 17 \\ -5 & 2 & 6 & -13 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & -4 & -14 & -21 \\ 0 & 9 & 32 & 59 \end{array}\right).$$

Así, conseguimos las siguientes ecuaciones:

$$\begin{aligned} x - 4y - 14z &= -21 \\ 9y + 32z &= 59 \end{aligned}$$

Si elegimos $z = t_1 \in \mathbb{Z}$ entonces la segunda ecuación nos quedaría como $9y + 32t_1 = 59$, la cual a final de cuentas es una ecuación lineal diofantina a resolver de dos incógnitas. Sabemos cómo resolverla, pero una vez resuelta habría que analizar cuáles de las soluciones nos sirven para dar solución también a la ecuación diofantina $x - 4y - 14z = -21$. Notamos entonces que el proceso podría volverse tedioso para más ecuaciones o más incógnitas, ya que al hacer la reducción de las matrices quizás obtengamos diversas ecuaciones diofantinas con más incógnitas y de acuerdo a lo que estudiamos en la sección anterior simplemente encontrar la solución de una de ellas, sin pensar aún en la solución común a todas, puede ser muy laborioso.

El ejemplo anterior nos permite percatarnos que intentar resolver un sistema de ecuaciones lineales diofantinas por el método de Gauss-Jordan no siempre resolverá por completo el problema, pues podremos obtener ecuaciones diofantinas con una buena cantidad de incógnitas y el capítulo anterior nos hizo ver que no es trivial encontrar soluciones a ecuaciones de más de dos incógnitas. Debido a lo anterior, necesitamos encontrar condiciones para que un sistema de ELD tenga soluciones enteras y además un método que nos permita resolverlos sin toparnos con más ecuaciones a resolver.

A continuación enunciaremos una condición equivalente para que un sistema de ELD $AX = B$ tenga soluciones enteras y a su vez exhibiremos cómo se ven, en caso de que existan, todas sus soluciones. Después de ello, veremos algunos ejemplos aplicando el resultado.

Teorema 3.3.13. *Sea $A \in M_{m\times n}(\mathbb{Z})$ una matriz con coeficientes enteros. El sistema $AX = B$ tiene soluciones enteras si y sólo si el sistema $R^tK = B$ tiene soluciones enteras, donde $R \in M_{n\times m}(\mathbb{Z})$ es una matriz escalonada por filas obtenida mediante la reducción modular por filas de A^t. Más aún si $(A^t|I_{n\times n})$ se reduce mediante operaciones modulares a $(R|T)$, entonces todas las soluciones de $AX = B$ son de la forma $X = T^tK$, con K*

una solución entera del sistema $R^tK = B$.

Demostración. Sea $A \in M_{m\times n}(\mathbb{Z})$ una matriz con coeficientes en los enteros. Por el Teorema 3.3.10 sabemos que podemos hacer una reducción modular por filas de $(A^t|I_{n\times n})$ para obtener $(R|T)$, realizando ciertas operaciones elementales por filas $e_1, e_2, \ldots, e_l$, donde R es una matriz escalonada por filas de $n \times m$. Notemos que dado el procedimiento, T es la matriz $n \times n$ que se obtiene de $I_{n\times n}$ al realizar $e_1, e_2, \ldots, e_l$, y por el Teorema 3.3.3 si $E_1, E_2, \ldots, E_l$ son las matrices elementales correspondientes a $e_1, e_2, \ldots, e_l$ respectivamente, tenemos las igualdades de matrices

$$R = E_l \cdots E_2 E_1 A^t, \quad T = E_l \cdots E_2 E_1 I_{n\times n} = E_l \cdots E_2 E_1,$$

teniendo así que $R = TA^t$. Entonces por propiedades de la matriz transpuesta tenemos que $R^t = AT^t$.
Notemos entonces que la ecuación $R^tK = B$ se puede reescribir como $AT^tK = B$.

Así, si $X_1 = T^tK$ con K una solución entera del sistema $R^tK = B$, tenemos que $A(T^tK) = (AT^t)K = R^tK = B$, por lo que X_1 resulta ser una solución entera del sistema $AX = B$.

A la inversa, si X_1 es una solución entera del sistema $AX = B$, tenemos que $AX_1 = B$. Por otro lado, dado que T es un producto de matrices invertibles, por la observación 3.3.4, T es invertible y en consecuencia T^t también lo es, entonces podemos expresar a X_1 como $X_1 = T^t(T^t)^{-1}X_1$. Además $R^t((T^t)^{-1}X_1) = (R^t(T^t)^{-1})X_1 = AX_1 = B$ por lo que al hacer $K_1 = (T^t)^{-1}X_1$ se tiene que $X_1 = T^tK_1$ con K_1 una solución entera del sistema $R^tK = B$. □

Observación 3.3.14. *Notemos que en el Teorema 3.3.13 se obtienen las soluciones de un sistema $AX = B$, a partir de las soluciones del sistema $R^tX = B$, donde R es una matriz escalonada por filas obtenida mediante la reducción modular de A^t. Pero aplicar operaciones modulares por renglones en A^t es lo mismo que aplicar dichas operaciones modulares por columnas en A, entonces el método descrito en el Teorema 3.3.13 usa la reducción por columnas de la matriz de coeficientes, en lugar de la reducción por renglones que ocupamos en el método de Gauss-Jordan.*

Veamos algunos ejemplos:

Ejemplo 3.3.15. *Consideremos el primer sistema trabajado en el Ejemplo 3.3.12:*

$$\begin{cases} 2x_1 + 4x_2 + 5x_3 = 2 \\ 3x_1 + x_2 + 8x_3 = 5 \\ 5x_1 + 8x_2 + 12x_3 = 3 \end{cases}$$

entonces siguiendo los mismos pasos que en el Ejemplo 3.3.7 para escalonar la matriz obtenemos lo siguiente

$$\left(\begin{array}{ccc|ccc} 2 & 3 & 5 & 1 & 0 & 0 \\ 4 & 1 & 8 & 0 & 1 & 0 \\ 5 & 8 & 12 & 0 & 0 & 1 \end{array}\right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 3 & 0 & -1 \\ 0 & 1 & -1 & -5 & 0 & 2 \\ 0 & 0 & 9 & 27 & -1 & -10 \end{array}\right)$$

donde

$$R = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & 9 \end{pmatrix}, \qquad T = \begin{pmatrix} 3 & 0 & -1 \\ -5 & 0 & 2 \\ 27 & -1 & -10 \end{pmatrix}.$$

Siguiendo el resultado del Teorema 3.3.13 veamos si el sistema $R^tK = B$ tiene soluciones enteras. Escribiendo el sistema de forma matricial tenemos

$$R^tK = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 3 & -1 & 9 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} k_1 \\ k_1 + k_2 \\ 3k_1 - k_2 + 9k_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix} = B.$$

Teniendo de esta forma que $k_1 = 2$, $k_2 = 3$ y $k_3 = 0$. Como $R^tK = B$ tiene una solución entera, entonces por el Teorema 3.3.13 el sistema $AX = B$ también tiene una solución entera y está dada de la siguiente manera

$$X = T^tK = \begin{pmatrix} 3 & -5 & 27 \\ 0 & 0 & -1 \\ -1 & 2 & -10 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix} = \begin{pmatrix} -9 \\ 0 \\ 4 \end{pmatrix},$$

por lo que la terna $x_1 = -9$, $x_2 = 0$ y $x_3 = 4$ es una solución entera al sistema de ecuaciones inicial tal y como lo vimos en el Ejemplo 3.3.12.

Revisemos en seguida la última ecuación vista en el Ejemplo 3.3.12

$$\begin{cases} 2x_1 + x_2 + 4x_3 = 17 \\ -5x_1 + 2x_2 + 6x_3 = -13 \end{cases}$$

Al hacer la reducción modular por filas de la matriz A^t obtenemos lo siguiente

$$\left(\begin{array}{cc|ccc} 2 & -5 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 4 & 6 & 0 & 0 & 1 \end{array}\right) \rightarrow \left(\begin{array}{cc|ccc} 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & -14 & 4 \\ 0 & 0 & 2 & 32 & -9 \end{array}\right)$$

donde

$$R = \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & 1 & 0 \\ -1 & -14 & 4 \\ 2 & 32 & -9 \end{pmatrix}.$$

Ahora tenemos que comprobar si el sistema $R^tK = B$ tiene soluciones enteras, entonces

$$R^tK = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} k_1 \\ 2k_1 + k_2 \end{pmatrix} = \begin{pmatrix} 17 \\ -13 \end{pmatrix} = B.$$

con lo que tenemos que $k_1 = 17$, $k_2 = -47$ y $k_3 \in \mathbb{Z}$. Así, entonces el sistema $AX = B$ tiene soluciones enteras y vienen dadas por la ecuación $X = T^t K$, por lo tanto:

$$X = T^t K = \begin{pmatrix} 0 & -1 & 2 \\ 1 & -14 & 32 \\ 0 & 4 & -9 \end{pmatrix} \begin{pmatrix} 17 \\ -47 \\ k_3 \end{pmatrix} = \begin{pmatrix} 47 + 2k_3 \\ 675 + 32k_3 \\ -188 - 9k_3 \end{pmatrix}$$

Gracias a estos ejemplos podemos observar lo siguiente: el primer sistema pudo resolverse completamente usando el Teorema 3.3.13, aunque usando el método de Gauss-Jordan en el Ejemplo 3.3.12 resultó un poco más sencillo llegar a las soluciones. Observemos que en este caso la matriz A, tiene rango 3, que es igual al número de incógnitas; por otra parte en el segundo ejemplo, hacerlo por el método de Gauss-Jordan resultaría más complicado, ya que tendríamos que resolver más ecuaciones diofantinas para calcular la solución general del sistema, lo cual evitamos al utilizar el Teorema 3.3.13. En este caso notamos que el rango de A es 2, mientras que el número de incógnitas es 3.
Analicemos entonces que cuando el rango de la matriz asociada a un sistema de ecuaciones lineales diofantinas es menor al número de incógnitas resulta más viable resolver el sistema utilizando el Teorema 3.3.13.

Si consideramos un sistema de m ecuaciones con n incógnitas en el que al menos una ecuación no cumple las condiciones para que existan soluciones, entonces el sistema no tendrá soluciones. Sin embargo, el hecho de que cada una de las ecuaciones del sistema tenga soluciones al analizarlas por separado, no implica automáticamente que el sistema tenga soluciones. A continuación ejemplificaremos lo dicho anteriormente.

Ejemplo 3.3.16. *Consideremos el siguiente sistema*

$$\begin{cases} 5x + 6y = 2 \\ 9x + 4y = 3 \end{cases}$$

Notemos que la ecuación $5x+6y = 2$ tiene soluciones, pues el máximo común divisor de los coeficientes $(5, 6) = 1$ divide a 2. De manera análoga la segunda ecuación $9x + 4y = 3$ tiene solución ya que $(9, 4) = 1$ divide a 3.
Para resolver el sistema, escalonemos la matriz $\left(\begin{array}{cc|cc} 5 & 9 & 1 & 0 \\ 6 & 4 & 0 & 1 \end{array}\right)$*:*

$$\left(\begin{array}{cc|cc} 5 & 9 & 1 & 0 \\ 6 & 4 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & -5 & -1 & 1 \\ 0 & 34 & 6 & -5 \end{array}\right)$$

por lo tanto tenemos que R es la matriz

$$R = \begin{pmatrix} 1 & -5 \\ 0 & 34 \end{pmatrix}.$$

Veamos si el sistema $R^t K = B$ tiene solución.

$$R^tK = \begin{pmatrix} 1 & 0 \\ -5 & 34 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \begin{pmatrix} k_1 \\ -5k_1 + 34k_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

Teniendo así que $k_1 = 2$ *y* $-5k_1 + 34k_2 = 3$*, lo que significa que* $34k_2 = 13$*. Pero no existe* $k_2 \in \mathbb{Z}$ *un entero tal que* $34k_2 = 13$*, de esta forma por el Teorema 3.3.13 el sistema*

$$\begin{cases} 5x + 6y = 2 \\ 9x + 4y = 3 \end{cases}$$

no tiene soluciones enteras.

Consideremos ahora el sistema

$$\begin{cases} 5x + 6y = b_1 \\ 9x + 4y = b_2 \end{cases}$$

con $b_1, b_2 \in \mathbb{Z}$ *números enteros arbitrarios. Sería natural preguntarnos lo siguiente: ¿cuándo este sistema tiene soluciones? es decir ¿para qué valores de* $b_1, b_2 \in \mathbb{Z}$ *el sistema anterior tiene solución?*

Dado que ya calculamos R*, por el Teorema 3.3.13 tenemos que ver cuándo* $R^tK = B$ *tiene soluciones enteras. Entonces tenemos lo siguiente*

$$R^tK = \begin{pmatrix} 1 & 0 \\ -5 & 34 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \begin{pmatrix} k_1 \\ -5k_1 + 34k_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}.$$

Por lo tanto si el sistema anterior tiene solución entera $k_1 = b_1$ *y* $-5k_1 + 34k_2 = b_2$*. Notemos entonces que en principio* $k_1 = b_1$ *podría ser cualquier número entero, luego como* $34k_2 = b_2 + 5b_1$*,* k_2 *sería un número entero si y sólo si* 34 *dividiera a* $b_2 + 5b_1$*.*

Notemos que el par $b_2 = 4k_2$ *y* $b_1 = 6k_2$ *es una solución particular, pues* $4k_2 + 5(6k_2) = 34k_2$*. Así, por el Teorema 1.3.4 las soluciones van a estar dadas de la siguiente forma*

$$\begin{aligned} b_2 &= 4k_2 + 5s \\ b_1 &= 6k_2 - s \end{aligned}$$

donde $k_2, s \in \mathbb{Z}$ *son número enteros arbitrarios. Por lo tanto el sistema*

$$\begin{cases} 5x + 6y = b_1 \\ 9x + 4y = b_2 \end{cases}$$

tiene soluciones enteras si y sólo si $b_1 = 6k_2 - s$ *y* $b_2 = 4k_2 + 5s$*, para* $k_2, s \in \mathbb{Z}$*. De esta manera, regresando al sistema* $R^tK = B$ *obtenemos entonces que* $k_1 = b_1 = 6k_2 - s$ *y* $b_2 = 4k_2 + 5s$*. Notemos que* $k_1 \in \mathbb{Z}$ *y además*

$k_2, s \in \mathbb{Z}$ también son enteros arbitrarios, por lo que el sistema

$$\begin{cases} 5x + 6y = 6k_2 - s \\ 9x + 4y = 4k_2 + 5s \end{cases}$$

tiene soluciones enteras con $k_2, s \in \mathbb{Z}$ arbitrarios y son de la forma $X = T^t K$, esto es

$$X = T^t K = \begin{pmatrix} -1 & 6 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 6k_2 - s \\ k_2 \end{pmatrix} = \begin{pmatrix} s \\ k_2 - s \end{pmatrix}.$$

Si sustituimos en el sistema tendremos que se satisface que sean soluciones:

$$5s + 6(k_2 - s) = 5s + 6k_2 - 6s = 6k_2 - s$$
$$9s + 4(k_2 - s) = 9s + 4k_2 - 4s = 4k_2 + 5s.$$

Hagamos un ejemplo más concreto; consideremos $k_2 = 7$ y $s = -3$, entonces el sistema a resolver es el siguiente

$$\begin{cases} 5x + 6y = 45 \\ 9x + 4y = 13, \end{cases}$$

entonces por el resultado anterior las soluciones deben ser $x = -3$ y $y = 10$, en efecto, pues $5(-3) + 6(10) = 45$ y $9(-3) + 4(10) = 13$.

El ejemplo anterior nos ayuda a darnos cuenta de dos puntos importantes: el primero es que el hecho de que cada ecuación por sí sola tenga soluciones enteras, no necesariamente implica que el sistema va a tener soluciones enteras; y el segundo punto es la importancia de los elementos constantes $b_i \in \mathbb{Z}$, ya que de ellos depende si el sistema tiene o no soluciones.

Al finalizar la sección anterior prometimos que el resultado de ésta también nos podría servir para encontrar soluciones de ecuaciones lineales diofantinas de n incógnitas. Apliquemos entonces el procedimiento anterior a un sistema con una sola ecuación diofantina, la ecuación del Ejemplo 3.2.1.

Ejemplo 3.3.17. *Consideremos la siguiente ELD:*

$$18x + 24y + 36z + 63w = 12$$

Notemos que tenemos la matriz $A = \begin{pmatrix} 18 & 24 & 36 & 63 \end{pmatrix}$, entonces el sistema a escalonar es el siguiente

$$\left(\begin{array}{c|cccc} 18 & 1 & 0 & 0 & 0 \\ 24 & 0 & 1 & 0 & 0 \\ 36 & 0 & 0 & 1 & 0 \\ 63 & 0 & 0 & 0 & 1 \end{array}\right)$$

En la sección anterior calculamos el máximo común divisor entre $18, 24, 36$ *y* 63 *que es igual a 3 o dicho de otro modo* $(18, 24, 36, 63) = 3$*, entonces por el Lema 3.3.8 tenemos que* R *es la matriz columna* $R = \begin{pmatrix} 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}$*, por lo tanto para comprobar la existencia de las soluciones enteras, tenemos que ver qué sucede con la ecuación* $R^t K = B$*, entonces*

$$R^t K = \begin{pmatrix} 3 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{pmatrix} = (3k_1) = (12) = B$$

teniendo así que $k_1 = 4$ *y* k_2, k_3 *y* k_4 *pueden tomar cualquier valor en los enteros. Por lo que la ecuación tiene soluciones enteras (ya lo habíamos visto anteriormente) y vienen dadas de la forma* $X = T^t K$*. Falta calcular* T*, así que para ello es necesario escalonar el sistema antes mencionado. Realizando la reducción modular por filas tendremos lo siguiente:*

$$\left(\begin{array}{c|cccc} 18 & 1 & 0 & 0 & 0 \\ 24 & 0 & 1 & 0 & 0 \\ 36 & 0 & 0 & 1 & 0 \\ 63 & 0 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{c|cccc} 3 & 4 & -4 & -1 & 1 \\ 0 & -9 & 9 & 2 & -2 \\ 0 & 4 & -3 & 0 & 0 \\ 0 & -2 & 0 & 1 & 0 \end{array}\right).$$

Entonces las soluciones vienen dadas por:

$$X = T^t K = \begin{pmatrix} 4 & -9 & 4 & -2 \\ -4 & 9 & -3 & 0 \\ -1 & 2 & 0 & 1 \\ 1 & -2 & 0 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ k_2 \\ k_3 \\ k_4 \end{pmatrix} = \begin{pmatrix} 16 - 9k_2 + 4k_3 - 2k_4 \\ -16 + 9k_2 - 3k_3 \\ -4 + 2k_2 + k_4 \\ 4 - 2k_2 \end{pmatrix}$$

donde

$$\begin{aligned} x &= 16 - 9k_2 + 4k_3 - 2k_4 \\ y &= -16 + 9k_2 - 3k_3 \\ z &= -4 + 2k_2 + k_4 \\ w &= 4 - 2k_2 \end{aligned}$$

son las soluciones a la ELD dada, con $k_2, k_3, k_4 \in \mathbb{Z}$*.*

3.4. Forma normal de Smith en $\mathbb{Z}$

En los ejemplos de la sección anterior, ver que el sistema $R^tK = B$ tiene soluciones enteras fue sumamente sencillo ya que todo se redujo a resolver ecuaciones de una sola incógnita en $\mathbb{Z}$ viendo si un número es divisible por otro o no. Además notamos que por el método tradicional visto en álgebra lineal escalonamos por renglones para conocer las soluciones de nuestro sistema y en el Teorema 3.3.13 escalonamos por columnas para saber cuándo un sistema tiene soluciones enteras obteniendo también una fórmula explícita de ellas. Dicho esto, sería una buena idea trabajar con operaciones modulares por filas y por columnas al mismo tiempo. Para ello consideremos el siguiente ejemplo, donde además de escalonar por filas, también escalonaremos por columnas.

Ejemplo 3.4.1. *Consideremos a $A \in M_{2\times 3}(\mathbb{Z})$ una matriz de 2×3 con coeficientes en $\mathbb{Z}$ de la siguiente forma.*

$$A = \begin{pmatrix} 3 & 1 & 4 \\ 7 & 2 & 9 \end{pmatrix}$$

Hagamos la reducción modular por filas y por columnas.

$$\begin{pmatrix} 3 & 1 & 4 \\ 7 & 2 & 9 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

De izquierda a derecha hicimos las siguientes operaciones:

1) Primero $C_1 - 3C_2$ y $C_3 - 4C_2$.

2) Luego un intercambio de columnas $C_2 \leftrightarrow C_1$.

3) Luego $R_2 - 2R_1$.

4) Por último hicimos $C_3 - C_2$.

Además, siguiendo la idea del Teorema 3.3.3, al aplicar las mismas operaciones modulares por filas que aplicamos a A pero ahora a la matriz identidad $I \in M_2(\mathbb{Z})$, obtenemos una matriz invertible $L \in M_2(\mathbb{Z})$. Análogamente, al aplicar las mismas operaciones modulares por columnas que aplicamos a A pero ahora a la matriz identidad $I \in M_3(\mathbb{Z})$, obtenemos una matriz invertible $R \in M_3(\mathbb{Z})$. En este caso R y L están dadas de la siguiente forma:

$$L = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \qquad R = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -3 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Asimismo, por el Teorema 3.3.3 podemos escribir a la matriz D de la siguiente forma

$$D = LAR.$$

*A esta matriz D se le conoce como la **forma normal de Smith de** A.*

Generalizando lo escrito en el anterior ejemplo, lo que buscamos probar en esta sección es que dada una matriz A con coeficientes en $\mathbb{Z}$, mediante operaciones modulares por columnas y filas podemos obtener una

matriz D tal que $d_{ij} \neq 0$ cuando $1 \leq i = j \leq r$, donde r es el rango de la matriz A, y $d_{ij} = 0$ en cualquier otro caso. Además, al aplicar estas operaciones modulares vamos a obtener matrices invertibles tales que D podemos escribirla como un producto de la matriz original con ellas. Dicho de manera más formal, si tenemos una matriz $A \in M_{m\times n}(\mathbb{Z})$, entonces van a existir matrices invertibles $L \in M_m(\mathbb{Z})$ y $R \in M_n(\mathbb{Z})$ tales que[1]

$$LAR = D = \begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}.$$

donde $r = \text{rg}(A)$, $d_i > 0$, para toda $1 \leq i \leq r$ y $d_i | d_{i+1}$ para toda $1 \leq i < r$. Esta última condición es importante al probar el resultado, porque al hacer operaciones modulares por filas y columnas podemos llegar a una matriz como la antes descrita donde cada entrada d_{ii} sea distinta de cero pero donde quizás no se cumpla esta condición de divisibilidad. Por ello debemos ser cuidadosos al hacer la reducción modular con el fin de lograr que se cumpla esta condición.

La idea de la prueba es la siguiente: primero, mediante operaciones modulares por filas y columnas de nuestra matriz, conseguir que el máximo común divisor de todas las entradas de la matriz A aparezca en una entrada de la matriz; posteriormente, mediante intercambios de filas y columnas, llevarlo a la posición 11; luego, realizando operaciones modulares, llegar a una matriz donde toda la fila 1 y columna 1 sean 0 salvo el coeficiente de la posición 11. De esta manera, obtendremos una matriz en la que el elemento 11 dividirá a cada entrada de la matriz. Continuando con este proceso lograremos obtener la matriz D buscada.

Pero antes de dar la prueba formal sobre la forma normal de Smith en $\mathbb{Z}$ necesitaremos algunas herramientas que nos permitan simplificar la prueba; para ello comencemos dando la siguiente notación.

Notación 3.4.1. *Sea $A \in M_{m\times n}(\mathbb{Z})$ no nula. Denotaremos al máximo común divisor de todas las entradas de A como*

$$d(A) = \text{mcd}\{a_{ij} | 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Observación 3.4.2. *Sea $A \in M_{m\times n}(\mathbb{Z})$ una matriz no nula y $d(A)$ el máximo común divisor de todos los coeficientes en A. Entonces al aplicar operaciones modulares por renglones y/o columnas obtendremos una matriz B tal que $d(B) = d(A)$.*

Demostración. El hacer intercambio de filas o de columnas no altera a $d(A)$ ya que no cambia la colección de entradas de la matriz, sólo el orden en que aparecen; multiplicar por -1 a alguna columna o alguna fila tampoco lo altera gracias a la generalización del Lema 1.2.1. Finalmente sumar a una fila el múltiplo de otra o sumar una

[1]La matriz describe el caso general, sin embargo notemos que, dado que n y m no necesariamente son iguales, puede ser que no aparezcan los renglones de ceros, o bien las columnas de ceros.

columna el múltiplo de otra columna no cambia el máximo común divisor de las entradas de la matriz debido al Lema 3.3.9. □

El siguiente resultado nos permite transformar una matriz $A \in M_{m\times n}(\mathbb{Z})$ a una matriz $B \in M_{m\times n}(\mathbb{Z})$ por medio de operaciones modulares por filas y columnas de tal manera que la entrada de valor absoluto mínimo de B, el cual llamaremos $t(B)$, es $d(A)$. Este resultado será fundamental al probar el teorema relacionado con la forma normal de Smith. Una prueba similar puede ser encontrada en [SM].

Lema 3.4.3. *Sea $A \in M_{m\times n}(\mathbb{Z})$ una matriz no cero con coeficientes enteros y $d(A)$ el máximo común divisor de todos los coeficientes de A. Usando operaciones modulares por filas y/o columnas podemos transformar a la matriz A en una matriz $B = (b_{ij}) \in M_{m\times n}(\mathbb{Z})$ de tal forma que $t(B) = d(A)$, donde $t(B)$ es el elemento de mínimo del conjunto $\{|b_{ij}| : b_{ij} \neq 0, 1 \leq i \leq m, 1 \leq j \leq n\}$.*

Demostración. Sea $A \in M_{m\times n}(\mathbb{Z})$ la matriz no nula

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Consideremos el conjunto $S = \{|a_{ij}| : a_{ij} \neq 0, 1 \leq i \leq m, 1 \leq j \leq n\}$. Notemos que $S \subseteq \mathbb{N}$, así por el Principio del Buen Orden S tiene un elemento mínimo. Llamemos a ese elemento $t(A)$. Claramente $t(A) \geq d(A)$, entonces usemos inducción sobre $t(A)$.

1. **Caso base** $t(A) = d(A)$**:** En este caso basta dejar la matriz A como está, es decir considerar $B = A$.

   Consideremos $t(A) > d(A)$.

2. **H.I.:** Supongamos que el resultado es válido para una matriz $C \in M_{m\times n}(\mathbb{Z})$ tal que $d(C) = d(A)$ y $t(C) < t(A)$, es decir que si $C \in M_{m\times n}(\mathbb{Z})$ tal que $d(C) = d(A)$ y $t(C) < t(A)$, usando operaciones modulares por filas y/o columnas podemos transformar a la matriz C en una matriz $B = (b_{ij}) \in M_{m\times n}(\mathbb{Z})$ de tal forma que $t(B) = d(A)$.

3. **P.I.:** Sea $t(A) = |a_{su}|$. Si $a_{su} > 0$ entonces $|a_{su}| = a_{su}$, de otra manera podemos hacer la siguiente operación $R_s \to (-1)R_s$. Por lo tanto supongamos que $t(A) = a_{su}$.

   Observemos que si $t(A) \mid a_{ij}$ para todas $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$, entonces $t(A)$ sería un divisor común de las entradas de A, y así $t(A) \mid d(A)$, lo que es una contradicción ya que $t(A) > d(A) > 0$. En consecuencia existe una entrada de A que no es dividida por $t(A) = a_{su}$.

   Consideremos ahora dos casos, uno donde existe una entrada de A que no es dividida por $t(A) = a_{su}$ y que se encuentra en la misma fila o columna que a_{su} y el otro donde existe una entrada de A que no es dividida por $t(A) = a_{su}$ pero todas las entradas de la fila s de A y todas las entradas de la columna u de A son divididas por $t(A) = a_{su}$.

a) **Caso 1:** Supongamos que existe una entrada a_{kl} de A, con $1 \leq k \leq m$ y $1 \leq l \leq n$, tal que $a_{su} \nmid a_{kl}$, con $k = s$ o $l = u$. Sin pérdida de generalidad supongamos que $l = u$.

Por el algoritmo de Euclides existen enteros q y r tales que $a_{ku} = qa_{su} + r$ con $0 < r < a_{su}$. Haciendo la operación modular por filas $R_k \to R_k - qR_s$ restaremos a a_{ku} q veces a_{su}, obteniendo así como resultado una matriz C con entrada ku igual a $qa_{su} + r - qa_{su} = r$. De esta forma, conseguimos una matriz C tal que $d(C) = d(A)$ (por la Observación 3.4.2) y además como $r < a_{su}$ tenemos que $t(C) \leq r < a_{su} = t(A)$, entonces por la hipótesis de inducción, podemos transformar la matriz C a una matriz B tal que $t(B) = d(A)$.

b) **Caso 2:** Supongamos que existe una entrada a_{kl} de A, con $1 \leq k \leq m$ y $1 \leq l \leq n$, tal que $a_{su} \nmid a_{kl}$ pero de modo que todas las entradas de la fila s de A y todas las entradas de la columna u de A son divididas por a_{su}.

Veamos primero que mediante operaciones modulares podemos hacer cero el resto de las entradas en la columna y la fila donde se encuentra a_{su}.

Para ello consideremos primero una entrada a_{iu} con $i \neq s$, como por hipótesis a_{su} divide a a_{iu} entonces existe $\alpha \in \mathbb{Z}$ tal que $a_{iu} = \alpha a_{su}$ luego la operación por filas $R_i \to R_i - \alpha R_s$ transforma la entrada iu en cero; realizando esto para toda $i \neq s$ obtenemos una matriz donde la columna u es cero salvo por el elemento a_{su}, notemos que estas operaciones no modifican el renglón s de la matriz, por lo que en la nueva matriz todas las entradas de la fila s de A son divididas por a_{su}.

De igual forma, consideremos ahora una entrada de la matriz obtenida a_{sj}, con $j \neq u$, como por hipótesis a_{su} divide a a_{sj} entonces existe $\beta \in \mathbb{Z}$ tal que $a_{sj} = \beta a_{su}$ y realizando la operación por columnas $C_j \to C_j - \beta C_u$ hacemos cero la entrada sj. Así, realizando esto para toda $j \neq u$ obtenemos una matriz B cuya fila s y cuya columna u es cero, salvo por a_{su}.

Además, la matriz B obtenida es tal que $d(B) = d(A)$ por la Observación 3.4.2 y además $t(B) \leq t(A)$, dado que $b_{su} = a_{su} = t(A)$.

Por otro lado sabemos que $d(B) \leq t(B)$, y como $d(B) = d(A)$ esto es equivalente a que $d(A) \leq t(B)$. Si $t(B) = d(A)$ entonces acabamos la prueba. Si $d(A) < t(B)$ no es posible que b_{su} divida a toda entrada de B pues si lo hiciera sería un divisor común de las entradas de B y tendríamos que $b_{su} \leq d(B)$ y en consecuencia $t(A) = a_{su} = b_{su} \leq d(B) = d(A)$, lo que contradice nuestra hipótesis de que $t(A) > d(A)$. Existe entonces una entrada b_{tv} tal que $b_{su} \nmid b_{tv}$, con $t \neq s$ y $v \neq u$ ya que la fila s y la columna u de B es cero, salvo por la entrada su. Haciendo la operación por filas en B $R_s \to R_s + R_t$ tendremos una nueva matriz C, en la que $c_{su} = b_{su} + b_{tu}$. Dado que $b_{tu} = 0$ por construcción tenemos que $c_{su} = b_{su}$, entonces $t(C) \leq c_{su} = b_{su} = t(A)$. No obstante, la entrada $c_{sv} = b_{sv} + b_{tv} = b_{tv}$, ya que $b_{sv} = 0$ por construcción. Entonces se tiene que $c_{su} = b_{su}$ y que $c_{sv} = b_{tv}$ con $b_{su} \nmid b_{tv}$, es decir $c_{su} \nmid c_{sv}$. Así, como en el caso 1, podemos hacer operaciones modulares para transformar C en una matriz D de tal forma que $t(D) < t(C) \leq t(A)$, con $d(D) = d(A)$. Finalmente, por hipótesis de inducción, podemos transformar D en una matriz B' tal que $t(B') = d(A)$.

□

Ahora que ya tenemos lo necesario veamos el último teorema del capítulo, que enuncia la forma normal de Smith en $\mathbb{Z}$. Cabe mencionar que el resultado se puede generalizar a matrices sobre un dominio de ideales principales[2], el lector interesado puede revisar la prueba para dominios euclidianos, que es similar a la que se dará en este trabajo, en [Ja85, p. 181-183].

Teorema 3.4.4. *Sea $A \in M_{m\times n}(\mathbb{Z})$. Existen matrices invertibles $L \in M_m(\mathbb{Z})$ y $R \in M_n(\mathbb{Z})$ tales que*

$$LAR = D = \begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}$$

con $d_1 = d(A)$, $r = \mathrm{rg}(A)$, $d_i > 0$, para toda $1 \leq i \leq r$ y $d_i | d_{i+1}$ para toda $1 \leq i < r$. A D se le llama la ***forma normal de Smith de*** *A.*

Demostración. Si A es la matriz nula, entonces el resultado es evidente, supongamos entonces que A es una matriz no nula.

Haremos la prueba por inducción sobre el número de columnas, *i.e.* sobre n.

1. **Caso base** $n = 1$**:** Se sigue del Lema 3.3.8.

   Sea $n \geq 2$.

2. **H.I.**: Supongamos que el resultado es válido para matrices de $n - 1$ columnas.

3. **P.I.**: Sea $A \in M_{m\times n}(\mathbb{Z})$ no nula dada por:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

   Por el Lema 3.4.3 podemos transformar la matriz A en una matriz A', por medio de operaciones modulares

[2]Un dominio de ideales principales es un dominio entero donde todos sus ideales son principales (*i.e.* están generados por un elemento).

por filas y columnas, dada de la siguiente forma

$$A' = \begin{pmatrix} a'_{11} & a'_{12} & \dots & a'_{1n} \\ a'_{21} & a'_{22} & \dots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{m1} & a'_{m2} & \dots & a'_{mn} \end{pmatrix}$$

de tal manera que alguna entrada a'_{ij} de A' cumpla que $a'_{ij} = d(A)$ con $1 \leq i \leq m$ y $1 \leq j \leq n$. Por medio de las siguientes operaciones $R_i \leftrightarrow R_1$ y $C_j \leftrightarrow C_1$ podemos mandar al coeficiente $a'_{ij} = d(A)$ a la posición 11, para obtener la nueva matriz

$$B = \begin{pmatrix} d(A) & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

Notemos que gracias a que B se obtuvo de A mediante operaciones modulares, cada entrada de B es combinación lineal de ciertas entradas de A, por lo que $d(A)$ divide también a cada entrada de B. En particular se tiene que $d(A)$ divide a todas las demás entradas del primer renglón y a todas las demás entradas de la primera columna, entonces sumando a las columnas $2, \dots, n$ múltiplos adecuados de la primera columna y sumando a los renglones $2, \dots, m$ múltiplos adecuados del primer renglón (de modo análogo a lo que se hizo en el caso 2 del Lema 3.4.3) tenemos la siguiente transformación:

$$\begin{pmatrix} d(A) & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} \to \begin{pmatrix} d(A) & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & \dots & c_{mn}. \end{pmatrix}$$

Llamemos T a la matriz formada por las entradas c_{kl}, es decir a la matriz que se obtiene quitando el primer renglón y la primera columna de la última matriz descrita. Notemos que cada c_{kl} es una combinación lineal de las entradas de B y es por tanto dividida por $d(A)$. Por hipótesis de inducción tenemos la siguiente

transformación:

$$\begin{pmatrix} d(A) & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & \dots & c_{mn} \end{pmatrix} \to \begin{pmatrix} d(A) & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix} = D$$

con $d_2 = d(T)$, $r - 1 = \text{rg}(T)$, $d_i > 0$, para toda $2 \leq i \leq r$ y $d_i | d_{i+1}$ para toda $2 \leq i < r$. Llamemos $d(A) = d_1$. Dado que d_2 es el máximo común divisor de las entradas c_{kl}, como $d_1 = d(A)$ divide a cada c_{kl}, entonces $d_1 \mid d_2$ y por hipótesis de inducción $d_i \mid d_{i+1}$ para cada $2 \leq i \leq r - 1$. Además

$$rg(A) = rg \begin{pmatrix} d(A) & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{m2} & \dots & c_{mn} \end{pmatrix} = 1 + rg \begin{pmatrix} c_{22} & \dots & c_{2n} \\ \vdots & \ddots & \vdots \\ c_{m2} & \dots & c_{mn} \end{pmatrix} = 1 + rg(T) = 1 + (r-1) = r.$$

Sean $e_1, e_2, \dots, e_t$ las operaciones modulares por renglones y $e'_1, e'_2, \dots, e'_q$ las operaciones modulares por columnas que aplicamos a A para obtener la matriz D. Consideremos $E_1, E_2, \dots, E_t$ y $E'_1, E'_2, \dots, E'_q$ las matrices elementales correspondientes. Definamos $L = E_t \dots E_2 E_1$ y $R = E'_1 E'_2 \cdots E'_q$. Por construcción tenemos que L y R son matrices invertibles pues son productos de matrices elementales, que son invertibles por la Observación 3.3.4.

Finalmente, por el Teorema 3.3.3 se cumple que

$$D = E_t \cdots E_2 E_1 A E'_1 E'_2 \cdots E'_q = LAR.$$

es decir

$$LAR = D = \begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}$$

□

Usando la forma normal de Smith escribamos un resultado similar al Teorema 3.3.13.

Teorema 3.4.5. *Sea $A \in M_{m\times n}(\mathbb{Z})$ una matriz con coeficientes enteros. Entonces el sistema $AX = B$ tiene soluciones enteras si y sólo si el sistema $DK = LB$ tiene soluciones enteras, donde $D \in M_{m\times n}(\mathbb{Z})$ es la forma normal de Smith de A y $L \in M_m(\mathbb{Z})$ es una matriz invertible obtenida al realizar operaciones modulares por renglones en A. Más aún, todas las soluciones de $AX = B$ son de la forma $X = RK$, con K una solución del sistema $DK = LB$ y $R \in M_n(\mathbb{Z})$ es una matriz invertible obtenida al realizar operaciones modulares por columnas en A.*

Demostración. Sea $A \in M_{m\times n}(\mathbb{Z})$ una matriz con coeficientes en los enteros. Por el Teorema 3.4.4 sabemos que existen matrices invertibles $L \in M_m(\mathbb{Z})$ y $R \in M_n(\mathbb{Z})$ tales que $D = LAR$, donde D es la forma normal de Smith de A.
Consideremos $X_1 = RK$ con K una solución entera del sistema $DK = LB$. Veamos que X_1 es una solución entera de $AX = B$. Sabemos que $AX_1 = A(RK) = (AR)K$, además $D = LAR$ y como L es invertible $L^{-1}D = AR$. Entonces

$$AX_1 = A(RK) = (AR)K = (L^{-1}D)K = L^{-1}(DK).$$

Pero por hipótesis $DK = LB$, entonces

$$AX_1 = L^{-1}(DK) = L^{-1}(LB) = (L^{-1}L)B = B,$$

por lo que X_1 resulta ser una solución entera del sistema $AX = B$.

A la inversa, si X_1 es una solución entera del sistema $AX = B$, tenemos que $AX_1 = B$. Por otro lado dado que R es invertible entonces podemos expresar a X_1 como $X_1 = (RR^{-1})X_1 = R(R^{-1}X_1)$. Notemos que R^{-1} es al igual que R un producto de matrices elementales obtenidas por operaciones modulares, por lo que sus entradas son enteras. Veamos ahora que $K_1 = R^{-1}X_1$ es una solución entera de $DK = LB$. Tenemos que

$$DK_1 = D(R^{-1}X_1) = (DR^{-1})X_1$$

y como $D = LAR$ y R es invertible sabemos que $DR^{-1} = LA$, así

$$DK_1 = (DR^{-1})X_1 = (LA)X_1 = L(AX_1).$$

Finalmente, como por hipótesis $AX_1 = B$, concluimos que

$$DK_1 = L(AX_1) = LB$$

probando que $K_1 = R^{-1}X_1$ es una solución entera de $DK_1 = LB$.

□

Notemos que el teorema anterior tiene una estructura similar a la del Teorema 3.3.13, pero en esta ocasión

además de trabajar con operaciones modulares por renglones también consideramos las operaciones modulares por columnas, mismas que quedan codificadas en la matriz R que se menciona en el enunciado. Por otra parte, en el Teorema 3.3.13 las soluciones enteras del sistema $AX = B$ se relacionan con las soluciones enteras del sistema $R^tK = B$, mientras que en el resultado anterior se relacionan con las del sistema $DK = LB$. Cabe mencionar que el Teorema 3.4.5 puede ser encontrado en el artículo [La96], aunque con una redacción distinta. El cambio en dicha redacción se realizó para que fuera análogo al Teorema 3.3.13 y se lograra una mayor consistencia en el presente trabajo.

Hagamos un ejemplo para ilustrar el Teorema 3.4.5.

Ejemplo 3.4.6. *Consideremos el siguiente sistema de ELD*

$$\begin{pmatrix} 3 & 1 & 4 \\ 7 & 2 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -3 \\ 3 \end{pmatrix}.$$

Por lo tanto la matriz de coeficientes del sistema es la matriz del Ejemplo 3.4.1

$$A = \begin{pmatrix} 3 & 1 & 4 \\ 7 & 2 & 9 \end{pmatrix}$$

y como vimos en ese ejemplo previo, al realizar operaciones modulares por filas y columnas en A obtenemos las matrices D, R y L que se escriben a continuación

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad R = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -3 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad L = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

De acuerdo al Teorema 3.4.5 tenemos que ver que el sistema $DK = LB$ tiene soluciones enteras, para así asegurar la existencia de soluciones enteras del sistema $AX = B$ Calculando tenemos

$$DK = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}, \qquad LB = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} -3 \\ 3 \end{pmatrix} = \begin{pmatrix} -3 \\ 9 \end{pmatrix}.$$

Así, $k_1 = -3$, $k_2 = 9$ y podemos elegir a k_3 como cualquier entero. Por el Teorema 3.4.5, el sistema $AX = B$ tiene soluciones enteras y son de la forma

$$X = RK = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -3 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -3 \\ 9 \\ k_3 \end{pmatrix} = \begin{pmatrix} 9 - k_3 \\ -30 - k_3 \\ k_3 \end{pmatrix}$$

con $k_3 \in \mathbb{Z}$.

Capítulo 4

El grupo $(\mathcal{D}, \oplus_k)$.

Ahora que ya sabemos cuándo el sistema de ecuaciones lineales diofantinas

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \quad \cdots \quad + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \quad \cdots \quad + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \quad \cdots \quad + a_{mn}x_n = b_m, \end{cases}$$

tiene soluciones y además cómo calcularlas, nos podemos preguntar si se puede dotar al conjunto de las soluciones de un sistema de ecuaciones lineales diofantinas de una operación adecuada con la cual éste tenga estructura de grupo. Por comodidad, el sistema anterior lo escribiremos de la siguiente forma

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1, \ldots, m.$$

En este capítulo desarrollaremos el material del artículo [Ch06] definiendo una operación binaria en el conjunto de las soluciones de un sistema de ELD y viendo que con ella se tiene una estructura de grupo abeliano. Además, haremos una generalización de dicho resultado y brindaremos un contraejemplo de una afirmación del teorema en [Ch06], así como también la correción de esa afirmación y por supuesto, probarla.

4.1. Operación binaria en el conjunto de soluciones de un sistema de ELD

Primero definamos, para cada $k \in \mathbb{Z}$, una operación binaria en $\mathbb{Z}$ que se construye en términos de la suma y resta usual.

Definición 4.1.1. *Sean $a, b \in \mathbb{Z}$ y $k \in \mathbb{Z}$ un entero fijo, definimos la operación binaria $\oplus_k$ como*

$$a \oplus_k b = a + b - k,$$

donde $+$ y $-$ son la suma y la resta usual en $\mathbb{Z}$.

Dicho esto, tenemos el siguiente resultado.

Proposición 4.1.1. *Sea $k \in \mathbb{Z}$ un número entero fijo, entonces $(\mathbb{Z}, \oplus_k)$ es un grupo abeliano.*

Demostración. Sean $a, b \in \mathbb{Z}$, notemos que la operación binaria está bien definida ya que está dada en términos de la suma y resta usual; además como $k \in \mathbb{Z}$ entonces $a \oplus_k b = a+b-k \in \mathbb{Z}$ lo que se traduce a que la operación es cerrada. Veamos que se cumplen las demás propiedades. Sean $a, b, c \in \mathbb{Z}$ y k un entero fijo, entonces

1. (Asociatividad)

$$a \oplus_k (b \oplus_k c) = a \oplus_k (b+c-k) = a + (b+c-k) - k = (a+b-k) + c - k = (a \oplus_k b) + c - k = (a \oplus_k b) \oplus_k c.$$

2. (Conmutatividad)

$$a \oplus_k b = a + b - k = b + a - k = b \oplus_k a.$$

3. (Existencia de neutro aditivo) Buscamos un $a' \in \mathbb{Z}$ tal que $a \oplus_k a' = a$ para toda $a \in \mathbb{Z}$, entonces requerimos que $a \oplus_k a' = a$ para toda $a \in \mathbb{Z}$, pero

$$\begin{aligned} a \oplus_k a' = a \quad \forall a \in \mathbb{Z} &\implies a + a' - k = a \quad \forall a \in \mathbb{Z} \\ &\implies a' = k, \end{aligned}$$

   por lo que en caso de que exista un neutro éste debe ser $a' = k$. En efecto k es el elemento neutro, pues $a \oplus_k k = a + k - k = a$ para toda $a \in \mathbb{Z}$.

4. (Existencia de inverso aditivo) Dado $a \in \mathbb{Z}$, buscamos un $a' \in \mathbb{Z}$ tal que $a \oplus_k a' = k$, entonces requerimos que $a \oplus_k a' = k$, pero

$$\begin{aligned} a \oplus_k a' = k &\implies a + a' - k = k \\ &\implies a' = 2k - a, \end{aligned}$$

   por lo que si a tiene inverso, éste debería ser $a' = 2k - a$. En efecto, $a \oplus_k (2k - a) = a + (2k - a) - k = k$. Así, cada $a \in \mathbb{Z}$ tiene un inverso, a saber $a' = 2k - a$.

Luego, $(\mathbb{Z}, \oplus_k)$ es un grupo abeliano. □

A partir de este momento consideraremos k un número entero fijo.
Veamos ahora que $\mathbb{Z}$ con esta nueva operación resulta ser isomorfo al conjunto de los enteros con la suma usual.

Teorema 4.1.2. $(\mathbb{Z}, \oplus_k)$ *es un grupo isomorfo a* $(\mathbb{Z}, +)$.

Demostración. Consideremos la siguiente función $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, \oplus_k)$, donde para cada $a \in \mathbb{Z}$

$$\phi(a) = a + k.$$

ϕ está dada en términos de la suma usual y por lo tanto está bien definida.

Veamos que es un homomorfismo de grupos. Sean $a, b \in \mathbb{Z}$, entonces

$$\begin{aligned}\phi(a+b) &= a + b + k \\ &= a + k + b + k - k \\ &= \phi(a) + \phi(b) - k \\ &= \phi(a) \oplus_k \phi(b).\end{aligned}$$

Claramente la función $\psi : (\mathbb{Z}, \oplus_k) \to (\mathbb{Z}, +)$, donde para cada $a \in \mathbb{Z}$ se tiene que $\psi(a) = a - k$, es la función inversa de ϕ, por lo que ϕ es una función biyectiva.

Por lo tanto, ϕ es un isomorfismo de grupos entre $(\mathbb{Z}, +)$ y $(\mathbb{Z}, \oplus_k)$. □

Recordemos que $(\mathbb{Z}, +)$ es un grupo cíclico, por lo que al tener este isomorfismo de grupos concluimos que $(\mathbb{Z}, \oplus_k)$ es también un grupo cíclico y como los generadores de $(\mathbb{Z}, +)$ son 1 y -1, entonces los generadores de $(\mathbb{Z}, \oplus_k)$ son sus imágenes bajo ϕ, es decir $1 + k$ y $-1 + k$.

Más aún, por el Teorema 2.2.5 tenemos que los subgrupos de $(\mathbb{Z}, \oplus_k)$ son cíclicos y corresponden a los generados por alguna $a \in \mathbb{Z}$, pero con la operación $\oplus_k$. Para describir entonces a dichos subgrupos será necesario entender cómo son las potencias de cada $a \in \mathbb{Z}$ con dicha operación, que en notación aditiva son los elementos de la forma $\underbrace{a \oplus_k \ldots \oplus_k a}_{m-\text{veces}}$.

Definamos para ello lo que significa ser "m-ésimo múltiplo" de un elemento $a \in \mathbb{Z}$ con la operación $\oplus_k$ de forma recursiva.

Definición 4.1.2. *Sea* $a \in (\mathbb{Z}, \oplus_k)$ *y* m *un entero no negativo, definimos el* m*-ésimo múltiplo de* a *de manera recursiva, denotado por* $m *_k a$*, como*

$$\begin{aligned}0 *_k a &= k \\ m *_k a &= ((m-1) *_k a) \oplus_k a, \qquad \textit{si } m > 0.\end{aligned}$$

Observación 4.1.3. *Se puede probar por inducción que para* $m > 0$*, se tiene que* $m *_k a = \underbrace{a \oplus_k \ldots \oplus_k a}_{m-\textit{veces}}$.

Notemos que $2 *_k a = 2a - k$ y $3 *_k a = 3a - 2k$, lo cual nos da una idea de cómo se ve el m-ésimo múltiplo de a.

Proposición 4.1.4. *Sea $a \in (\mathbb{Z}, \oplus_k)$ y m un entero no negativo, entonces $m *_k a = ma - (m-1)k$.*

Demostración. Probemos el resultado por inducción sobre m.

1. **Base:** $m = 0$. De acuerdo a la definición, se tiene que $0 *_k a = k = 0a - (0-1)k$.

   Sea m un entero tal que $m \geq 1$.

2. **H.I.** Supongamos que el resultado se cumple para $m-1$, entonces tenemos la igualdad

$$(m-1) *_k a = (m-1)a - (m-2)k.$$

3. **P.I.** Por cómo definimos el m-ésimo múltiplo de a, tenemos lo siguiente:

$$\begin{aligned} m *_k a &= ((m-1) *_k a) \oplus_k a \\ &= ((m-1)a - (m-2)k) \oplus_k a \\ &= (m-1)a - (m-2)k + a - k \\ &= ma - (m-1)k. \end{aligned}$$

□

Ahora, en el caso que m sea negativa, tenemos que $-m$ es positiva y recordando que el inverso de $a \in \mathbb{Z}$ bajo $\oplus_k$ es $2k - a$ entonces podemos definir el m-ésimo múltiplo de a como

$$m *_k a = (-m) *_k (2k - a).$$

Notemos que al desarrollar la operación $(-m) *_k (2k-a)$ nos queda lo siguiente:

$$\begin{aligned} (-m) *_k (2k-a) &= (-m)(2k-a) - (-m-1)k \\ &= -2km + ma + km + k \\ &= ma - km + k \\ &= ma - (m-1)k. \end{aligned}$$

Con esto notamos que tanto para m positiva como para m negativa, se tiene que $m *_k a = ma - (m-1)k$ para toda a entera. Por lo tanto, hemos logrado describir al m-ésimo mútliplo de $a \in \mathbb{Z}$ bajo $\oplus_k$ para cualquier $m \in \mathbb{Z}$. Ahora, recordemos que los subgrupos de $\mathbb{Z}$ bajo la suma usual son los conjuntos $a\mathbb{Z} = \{ma \mid m \in \mathbb{Z}\}$ para alguna a entera, es decir los generados por algún entero a, esto es $\langle a \rangle$ con $a \in \mathbb{Z}$. Entonces ahora los subgrupos de $(\mathbb{Z}, \oplus_k)$ son de la forma

$$S_a := \{m *_k a \mid m \in \mathbb{Z}\} = \{ma - (m-1)k \mid m \in \mathbb{Z}\}.$$

La colección de todos los subgrupos de $(\mathbb{Z}, \oplus_k)$ es entonces

$$\{S_a \mid a \in \mathbb{Z}\}.$$

Para tener una descripción más sencilla de dichos subgrupos notemos que

$$\{S_a \mid a \in \mathbb{Z}\} = \{S_{a+k} \mid a \in \mathbb{Z}\}$$

y como

$$S_{a+k} := \{m *_k (a+k) \mid m \in \mathbb{Z}\} = \{m(a+k) - (m-1)k \mid m \in \mathbb{Z}\} = \{ma + k \mid m \in \mathbb{Z}\},$$

concluimos que los subgrupos de $(\mathbb{Z}, \oplus_k)$ son grupos cíclicos de la forma $S_{a+k} = \{ma + k \mid m \in \mathbb{Z}\}$, donde S_{a+k} es generado por $a + k$ para alguna $a \in \mathbb{Z}$. De hecho éste era el resultado esperado ya que $S_{a+k} = \{ma + k \mid m \in \mathbb{Z}\} = \phi[\langle a \rangle]$, es decir los subgrupos de $(\mathbb{Z}, \oplus_k)$ son las imágenes directas de los subgrupos de $(\mathbb{Z}, +)$ bajo el isomorfismo ϕ.

Recordemos que $\mathbb{Z}^n$ es la suma directa externa de n copias de $\mathbb{Z}$ y $(\mathbb{Z}^n, +)$, donde $+$ es la suma entrada-entrada, es un grupo abeliano. Usando las operaciones $\oplus_k$ definidas para enteros k ¿podremos dotar ahora a $\mathbb{Z}^n$ de una operación bajo la cual resulte ser un grupo abeliano? Lo más natural sería usar las operaciones en cada entrada.

Definición 4.1.3. *Sea $k = (k_1, k_2, \ldots, k_n)$ una n-ada de números enteros. Definimos la operación $\oplus_k$ en $\mathbb{Z}^n$ dada por*

$$(a_1, a_2, \ldots, a_n) \oplus_k (b_1, b_2, \ldots, b_n) = (a_1 + b_1 - k_1, a_2 + b_2 - k_2, \ldots, a_n + b_n - k_n)$$

para todos $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{Z}^n$, es decir operamos los elementos de $\mathbb{Z}^n$ usando en cada entrada j la operación $\oplus_{k_j}$.

A continuación probaremos un lema que, en términos generales, es una extensión de lo que hemos hecho en esta sección con $(\mathbb{Z}, \oplus_k)$, pero ahora con $(\mathbb{Z}^n, \oplus_k)$.

Lema 4.1.5. *$(\mathbb{Z}^n, \oplus_k)$ es un grupo abeliano. Además, $(\mathbb{Z}^n, +)$ es isomorfo a $(\mathbb{Z}^n, \oplus_k)$.*

Demostración. Sea $k = (k_1, k_2, \ldots, k_n) \in \mathbb{Z}^n$, con $k_j \in \mathbb{Z}$ para cada $1 \leq j \leq n$. Consideremos los grupos $(\mathbb{Z}, \oplus_{k_j})$, los cuales son de la forma vista en la Proposición 4.1.1. Notemos que $(\mathbb{Z}^n, \oplus_k)$ lo podemos ver como una suma directa externa de estos grupos, esto es

$$(\mathbb{Z}^n, \oplus_k) = (\mathbb{Z}, \oplus_{k_1}) \oplus \ldots \oplus (\mathbb{Z}, \oplus_{k_n}).$$

Así, por la Proposición 2.3.5 tenemos que $(\mathbb{Z}^n, \oplus_k)$ es un grupo abeliano. Notemos que $(k_1, k_2, \ldots, k_n)$ es el

elemento neutro en $(\mathbb{Z}^n, \oplus_k)$; en efecto, sea $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ entonces

$$\begin{aligned}(a_1, a_2, \ldots, a_n) \oplus_k (k_1, k_2, \ldots, k_n) &= (a_1 + k_1 - k_1, a_2 + k_2 - k_2, \ldots, a_n + k_n - k_n) \\ &= (a_1, a_2, \ldots, a_n).\end{aligned}$$

Más aún, para cada $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ el inverso es $(2k_1 - a_1, \ldots, 2k_n - a_n)$; en efecto

$$\begin{aligned}(a_1, \ldots, a_n) \oplus_k (2k_1 - a_1, \ldots, 2k_n - a_n) &= (a_1 + 2k_1 - a_1 - k_1, \ldots, a_n + 2k_n - a_n - k_n) \\ &= (k_1, \ldots, k_n).\end{aligned}$$

Con esto concluimos la primera parte de la prueba.

Para la segunda parte, consideremos $\phi : (\mathbb{Z}^n, +) \to (\mathbb{Z}^n, \oplus_k)$ la función definida como sigue

$$\phi(a_1, \ldots, a_n) = (a_1 + k_1, \ldots, a_n + k_n).$$

Veamos que es un homomorfismo de grupos; en efecto

$$\begin{aligned}\phi((a_1, \ldots, a_n) + (b_1, \ldots, b_n)) &= \phi(a_1 + b_1, \ldots, a_n + b_n) \\ &= (a_1 + b_1 + k_1, \ldots, a_n + b_n + k_n) \\ &= (a_1 + b_1 + 2k_1 - k_1, \ldots, a_n + b_n + 2k_n - k_n) \\ &= ((a_1 + k_1) + (b_1 + k_1) - k_1, \ldots, (a_n + k_n) + (b_n + k_n) - k_n) \\ &= (a_1 + k_1, \ldots, a_n + k_n) \oplus_k (b_1 + k_1, \ldots, b_n + k_n) \\ &= \phi(a_1, \ldots, a_n) \oplus_k \phi(b_1, \ldots, b_n).\end{aligned}$$

Claramente la función $\psi : (\mathbb{Z}^n, \oplus_k) \to (\mathbb{Z}^n, +)$ dada por $\psi(a_1, \ldots, a_n) = (a_1 - k_1, \ldots, a_n - k_n)$ es la inversa de ϕ, por lo que ϕ es biyectiva, concluyendo que ϕ es un isomorfismo de grupos.

□

4.2. El conjunto de soluciones de un sistema de ELD tiene estructura de grupo

Teniendo ya las herramientas necesarias, podemos probar el teorema principal de esta sección y que motivó este trabajo.

Teorema 4.2.1. *Sea*

$$\sum_{j=1}^{n} a_{ij} x_j = b_i, \qquad i = 1 \ldots, m. \tag{4.1}$$

un sistema de ELD con $\mathcal{D} \neq \emptyset$ su conjunto de soluciones enteras y $k = (k_1, k_2, \ldots, k_n) \in \mathcal{D}$. Entonces $(\mathcal{D}, \oplus_k)$

es un subgrupo de $(\mathbb{Z}^n, \oplus_k)$ *y por lo tanto* $(\mathcal{D}, \oplus_k)$ *tiene estructura de grupo abeliano.*

Demostración. Sea $\mathcal{D}$ el conjunto de soluciones enteras de (3.13) y consideremos a $k = (k_1, k_2, \ldots, k_n) \in \mathcal{D}$ una solución arbitraria de (3.13), teniendo así que

$$\sum_{j=1}^{n} a_{ij} k_j = b_i, \qquad i = 1 \ldots, m$$

Notemos que $\mathcal{D} \subseteq \mathbb{Z}^n$, veamos que $\oplus_k$ es cerrada en $\mathcal{D}$. En efecto, sean $X = (X_1, \ldots, X_n)$ y $Y = (Y_1, \ldots, Y_n)$ soluciones de (3.13), por lo que

$$\sum_{j=1}^{n} a_{ij} X_j = b_i, \qquad \sum_{j=1}^{n} a_{ij} Y_j = b_i, \qquad i = 1 \ldots, m$$

Notemos que

$$X \oplus_k Y = (X_1 + Y_1 - k_1, \ldots, X_n + Y_n - k_n)$$

entonces para cada $j = 1, \ldots, n$ tenemos que

$$\begin{aligned} \sum_{j=1}^{n} a_{ij}(X_j + Y_j - k_j) &= \sum_{j=1}^{n} a_{ij} X_j + \sum_{j=1}^{n} a_{ij} Y_j - \sum_{j=1}^{n} a_{ij} k_j \\ &= b_i + b_i - b_i \\ &= b_i, \end{aligned}$$

teniendo así que $X \oplus_k Y \in \mathcal{D}$. Además hemos elegido $k = (k_1, k_2, \ldots, k_n) \in \mathcal{D}$, pero como habíamos notado $k = (k_1, k_2, \ldots, k_n)$ es precisamente el neutro de $(\mathbb{Z}^n, \oplus_k)$, entonces el neutro de $(\mathbb{Z}^n, \oplus_k)$ está en $\mathcal{D}$. Finalmente probemos que si $X \in \mathcal{D}$ entonces su inverso está en $\mathcal{D}$. Sea $X = (X_1, \ldots, X_n) \in \mathcal{D}$, recordemos que el inverso de X bajo $\oplus_k$ está dado de la siguiente manera

$$(2k_1 - X_1, \ldots, 2k_n - X_n)$$

entonces

$$\begin{aligned} \sum_{j=1}^{n} a_{ij}(2k_j - X_j) &= \sum_{j=1}^{n} a_{ij} 2k_j - \sum_{j=1}^{n} a_{ij} X_j \\ &= 2 \sum_{j=1}^{n} a_{ij} k_j - b_i \\ &= 2b_i - b_i \\ &= b_i. \end{aligned}$$

Por lo tanto $(2k_1 - X_1, \ldots, 2k_n - X_n) \in \mathcal{D}$. Concluimos que $(\mathcal{D}, \oplus_k)$ es un subgrupo de $(\mathbb{Z}^n, \oplus_k)$. Al ser $(\mathcal{D}, \oplus_k)$ un subgrupo de un grupo abeliano, $(\mathcal{D}, \oplus_k)$ resulta ser también un grupo abeliano.

□

Notemos que la prueba anterior funciona aún cuando un sistema de ELD tiene una única solución (como en el Ejemplo 3.3.15). En efecto. Consideremos el siguiente sistema de ELD

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1, \ldots, m,$$

con $\mathcal{D} = \{X\}$ su conjunto de soluciones, donde $X = (X_1, \ldots, X_n)$. En este caso k debe ser la única solución posible, es decir $k = X$ y podemos ver de forma trivial que la operación es cerrada, ya que

$$X \oplus_k X = (X_1 + X_1 - X_1, \ldots, X_n + X_n - X_n) = (X_1, \ldots, X_n) = X$$

y además el inverso de X es $(2X_1 - X_1, \ldots, 2X_n - X_n) = X \in \mathcal{D}$, teniendo así que $(\mathcal{D}, \oplus_k)$ es en este caso un grupo trivial.

Antes de concluir el capítulo haremos dos reflexiones importantes referentes tanto al Lema 4.1.5 y al Teorema 4.2.1: la primera será sobre las versiones originales del lema y el teorema mencionados previamente que se encuentran en el artículo [Ch06]; la segunda será cuestionarnos de dónde surge la asignación de dicha operación para atribuirle al conjunto de soluciones de sistemas de ecuaciones lineales diofantinas estructura de grupo abeliano.

En la versión del Lema 4.1.5 que se encuentra en el artículo [Ch06], se menciona que cada subgrupo de $(\mathbb{Z}^n, \oplus_k)$ es la suma directa externa de n grupos cíclicos y que el j-ésimo grupo cíclico de esta suma directa es un subgrupo de $(\mathbb{Z}, \oplus_{k_j})$ de la forma $\{ma + k_j \mid m \in \mathbb{Z}\}$ para algún $a \in \mathbb{Z}$ y utiliza este hecho para demostrar la versión del Teorema 4.2.1 en la que afirma que el grupo formado por las soluciones de un sistema de ecuaciones lineales diofantinas dotado de la operación $\oplus_k$ es la suma directa externa de n grupos cíclicos con esta forma. Sin embargo, esto no es del todo correcto; para ello consideremos el sistema de ecuaciones diofantinas dado por una sola ecuación

$$x - y = 0$$

que tiene como conjunto solución $H = \{(a, a) \mid a \in \mathbb{Z}\}$. En este caso utilizaremos a $k = (k_1, k_2) = (0, 0)$, la cual es la solución trivial de la ecuación, por lo que si (a, a) y (b, b) son soluciones de la ecuación entonces

$$(a, a) \oplus_k (b, b) = (a + b - k_1, a + b - k_2) = (a + b - 0, a + b - 0) = (a, a) + (b, b),$$

donde $+$ es la suma usual en $\mathbb{Z}^2$. Veamos que $(H, \oplus_k)$ es un subgrupo de $(\mathbb{Z}^2, \oplus_k)$, en efecto, $(0, 0) \in H$, además si $(a, a), (b, b) \in H$ entonces $(a, a) + (b, b) = (a + b, a + b) \in H$, pues $(a + b) - (a + b) = 0$, por lo que $a + b$ también es solución de la ecuación $x - y = 0$. Finalmente, dado $(a, a) \in H$ entonces $(-a, -a) \in H$, pues $(-a) - (-a) = 0$ lo que implica que $(-a, -a)$ también es solución de la ecuación dada. Por lo tanto $(H, \oplus_k)$ es un subgrupo de $(\mathbb{Z}^2, \oplus_k)$.

De acuerdo al artículo [Ch06], H sería la suma directa externa de grupos cíclicos; para $k_1 = 0$ tenemos que

un subgrupo del grupo cíclico $(\mathbb{Z}, \oplus_0)$ es de la forma $\{ma_1 \mid m \in \mathbb{Z}\}$ para algún $a_1 \in \mathbb{Z}$; para $k_2 = 0$ tenemos que un subgrupo del grupo cíclico $(\mathbb{Z}, \oplus_0)$ es de la forma $\{ma_2 \mid m \in \mathbb{Z}\}$, para algún $a_2 \in \mathbb{Z}$. Notemos que el sistema tiene más soluciones además de la trivial por lo que $a_1 \neq 0$ o $a_2 \neq 0$. Entonces H sería de la forma

$$H = \{ma_1 \mid m \in \mathbb{Z}\} \oplus \{ma_2 \mid m \in \mathbb{Z}\}.$$

Si $a_1 \neq a_2$ tendríamos en particular que $(a_1, a_2) \in \{ma_1 \mid m \in \mathbb{Z}\} \oplus \{ma_2 \mid m \in \mathbb{Z}\} = H$ es decir (a_1, a_2) sería solución de $x - y = 0$, lo que no es posible ya que $a_1 \neq a_2$. Por otro lado si $a_1 = a_2 \neq 0$ tendríamos que $(2a_1, a_2) \in \{ma_1 \mid m \in \mathbb{Z}\} \oplus \{ma_2 \mid m \in \mathbb{Z}\} = H$ es decir $(2a_1, a_2)$ sería solución de $x - y = 0$, lo que no es posible ya que $2a_1 - a_2 = a_1 \neq 0$.

Veamos ahora de dónde surge la operación que se define en el artículo [Ch06] para atribuirle al conjunto de soluciones de un sistema de ecuaciones lineales diofantinas estructura de grupo abeliano. Para ello veamos dos resultados referentes a las soluciones de un sistema de ecuaciones diofantinas. Primero consideremos un sistema arbitrario de ecuaciones lineales diofantinas homogéneo y luego el caso general:

Teorema 4.2.2. *Sea*

$$\sum_{j=1}^{n} a_{ij}x_j = 0, \qquad i = 1 \ldots, m. \tag{4.2}$$

un sistema de ELD homogéneo y H el conjunto de sus soluciones. Entonces $(H, +)$ es un subgrupo de $(\mathbb{Z}^n, +)$.

Demostración. Claramente $H \subseteq \mathbb{Z}^n$. Notemos primero que $\sum_{j=1}^{n} a_{ij}(0) = 0$ para toda $i = 1 \ldots, m$ por lo que $(0, \ldots, 0)$ es solución del sistema, es decir $(0, \ldots, 0) \in H$. Ahora, sean $(h_1, \ldots, h_n), (k_1, \ldots, k_n) \in H$ entonces

$$\sum_{j=1}^{n} a_{ij}(h_j + k_j) = \sum_{j=1}^{n} a_{ij}h_j + \sum_{j=1}^{n} a_{ij}k_j = 0 + 0 = 0$$

por lo que $(h_1, \ldots, h_n) + (k_1, \ldots, k_n) = (h_1 + k_1, \ldots, h_n + k_n) \in H$.

Notemos que el inverso de $(h_1, \ldots, h_n) \in H$ respecto a la operación $+$ es $(-h_1, \ldots, -h_n)$, por lo que

$$\sum_{j=1}^{n} a_{ij}(-h_j) = -\sum_{j=1}^{n} a_{ij}h_j = -0 = 0$$

por lo que $(-h_1, \ldots, -h_n) \in H$. Luego $(H, +)$ es un subgrupo de $(\mathbb{Z}^n, +)$.

□

Teorema 4.2.3. *Sea*

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1 \ldots, m. \tag{4.3}$$

un sistema de ELD, $\mathcal{D}$ el conjunto de soluciones del sistema 4.7, H el conjunto de soluciones del sistema homogéneo asociado al sistema 4.7 y $k = (k_1, \ldots, k_n) \in \mathcal{D}$. Entonces

$$\mathcal{D} = \{k + h \mid h \in H\}.$$

Demostración. Sea $d = (d_1, \ldots, d_n) \in \mathcal{D}$. Tenemos que $d = k + (d - k)$. Veamos que $d - k$ es un elemento en H. En efecto

$$\sum_{j=1}^{n} a_{ij}(d_i - k_i) = \sum_{j=1}^{n} a_{ij}d_i - \sum_{j=1}^{n} a_{ij}k_i = b_i - b_i = 0, \qquad i = 1 \ldots, m$$

probando que $d - k$ es una solución del sistema homogéneo asociado al sistema 4.7, es decir $d - k \in H$. Así, $d = k + (d - k) \in \{k + h \mid h \in H\}$.

A la inversa, sea $x \in \{k + h \mid h \in H\}$, es decir $x = k + \tilde{h}$ para algún $\tilde{h} = (\tilde{h_1}, \ldots, \tilde{h_n}) \in H$. Tenemos que

$$\sum_{j=1}^{n} a_{ij}(k_i + \tilde{h_i}) = \sum_{j=1}^{n} a_{ij}k_i + \sum_{j=1}^{n} a_{ij}\tilde{h_i} = b_i + 0 = b_i, \qquad i = 1 \ldots, m,$$

es decir x es una solución del sistema 4.7. Así, $x = k + \tilde{h} \in \mathcal{D}$. □

Hemos probado entonces que las soluciones de un sistema son las soluciones del sistema homogéneo más alguna solución particular del sistema orginal. Esto nos motiva a recordar la definición de **clase lateral izquierda y derecha** con respecto a un subgrupo. Debido a que los grupos utilizados en este trabajo son abelianos, daremos la definición con notación aditiva.

Definición 4.2.1. *Sea $(G, +)$ un grupo abeliano. Sea H un subgrupo de G. Para cada $t \in G$, se definen la **clase lateral derecha** de H en G con representante t como*

$$H + t = \{h + t \in G \mid h \in H\}$$

*y la **clase lateral izquierda** de H en G con representante t como*

$$t + H = \{t + h \in G \mid h \in H\}.$$

Notación 4.2.1. *Sea $(G, +)$ un grupo abeliano y H un subgrupo de G. El conjunto de las clases laterales izquierdas de H en G se escribirá como*

$$_{\text{izq}}(G/H) := \{t + H \mid t \in G\}$$

Análogamente, el conjunto de las clases laterales derechas de H en G se escribirá como

$$(G/H)_{\text{der}} := \{H + t \mid t \in G\}.$$

Observación 4.2.4. *Dado que G es un grupo abeliano, para H un subgrupo de G y $t \in G$, se tiene que $t + H = H + t$ (es decir cada clase lateral derecha de H en G con representante t coincide con la clase lateral derecha de H en G con representante t). Debido a ello tenemos que $_{\text{izq}}(G/H) = (G/H)_{\text{der}}$ y escribiremos a este conjunto simplemente como G/H.*

De acuerdo a lo anterior, podemos enunciar nuevamente el Teorema 4.2.3 de la siguiente forma:

Teorema 4.2.5. *Sea*

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1\ldots, m. \tag{4.4}$$

un sistema de ELD, $\mathcal{D}$ el conjunto de soluciones del sistema 4.4, H el conjunto de soluciones del sistema homogéneo asociado al sistema 4.4 y $k = (k_1, \ldots, k_n) \in \mathcal{D}$. Entonces $\mathcal{D}$ es la clase lateral de H en $\mathbb{Z}^n$ con representante k.

Con esta notación, el artículo [Ch06] logra darle estructura de grupo a una clase lateral, en este caso a

$$(k_1, \ldots, k_n) + H$$

donde $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ es una solución particular del sistema $\sum_{j=1}^{n} a_{ij}x_j = b_i$ con $i = 1, \ldots, m$ y H es el conjunto de soluciones del sistema homógeneo $\sum_{j=1}^{n} a_{ij}x_j = 0$ con $i = 1, \ldots, m$.

Dada esta información podemos preguntarnos si $\mathcal{D}$ puede ser escrito de maneras diferentes como una clase lateral, con distinto representante respecto a un subgrupo diferente. De hecho, el representante si puede ser diferente, pero el subgrupo siempre será el conjunto de soluciones del sistema homógeneo asociado, aún cuando esté descrito de manera diferente. El siguiente resultado demuestra lo anterior.

Proposición 4.2.6. *Sea G un grupo abeliano y $g_1, g_2 \in G$. Si H y Q son sugbrupos de G tales que $g_1 + H = g_2 + Q$, entonces $H = Q$.*

Demostración. Sea G un grupo abeliano y $g_1, g_2 \in G$. Sean H y Q sugbrupos de G. Supongamos que $g_1 + H = g_2 + Q$. Probemos que $H = Q$.

$\subseteq$) Sea $h \in H$, entonces $g_1 + h \in g_1 + H = g_2 + Q$ por lo que $g_1 + h = g_2 + q$ para algún $q \in Q$ y despejando h tenemos que

$$h = g_2 - g_1 + q. \tag{4.5}$$

Por otro lado, como H es un subgrupo de G entonces en particular $0 \in H$ y en consecuencia $g_1 = g_1 + 0 \in g_1 + H = g_2 + Q$. Así, $g_1 = g_2 + \tilde{q}$ para algún $\tilde{q} \in Q$ y despejando $\tilde{q}$ tenemos que $g_1 - g_2 = \tilde{q} \in Q$. Sustituyendo en la ecuación 4.5 tenemos que

$$h = (g_2 - g_1) + q = -(g_1 - g_2) + q = -\tilde{q} + q.$$

Como Q es un subgrupo de G tenemos que el inverso $-\tilde{q} \in Q$ y además $-\tilde{q} + q \in Q$, por lo que $h \in Q$.

$\supseteq$) Se prueba de manera análoga que $Q \subseteq H$.

□

Veamos con ello que si expresamos al conjunto de soluciones de un sistema de ELD como una clase lateral, entonces el representante de la clase lateral es una solución particular del sistema y el subgrupo con respecto al cual se construye la clase lateral es el subgrupo de soluciones del sistema homogéneo asociado:

Corolario 4.2.7. *Sea*

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1\ldots, m. \tag{4.6}$$

un sistema de ELD, $\mathcal{D}$ el conjunto de soluciones del sistema 4.6, H el conjunto de soluciones del sistema homogéneo asociado al sistema 4.6 y $k = (k_1, \ldots, k_n) \in \mathcal{D}$. Si $\mathcal{D} = t + Q$ con $t \in \mathbb{Z}^n$ y Q un subgrupo de $\mathbb{Z}^n$ entonces $t \in \mathcal{D}$ y $Q = H$.

Demostración. Consideremos el sistema de ELD 4.6, $\mathcal{D}$ su conjunto de soluciones, H el conjunto de soluciones del sistema homogéneo asociado y $k = (k_1, \ldots, k_n) \in \mathcal{D}$. Supongamos que $\mathcal{D} = t + Q$ con $t \in \mathbb{Z}^n$ y Q un subgrupo de $\mathbb{Z}^n$. Por el Teorema 4.2.5 sabemos que también $\mathcal{D} = k + H$, entonces

$$t + Q = k + H$$

y por la Proposición 4.2.6 concluimos que $Q = H$. Finalmente $t \in t + Q = \mathcal{D}$.

□

Ejemplo 4.2.8. *Recordemos la ELD del Ejemplo 3.3.17*

$$18x + 24y + 36z + 63w = 12.$$

Entonces el conjunto de soluciones $\mathcal{D}$ viene dado de la siguiente forma:

$$\begin{aligned}
\mathcal{D} &= \{(16 - 9k_2 + 4k_3 - 2k_4, -16 + 9k_2 - 3k_3, -4 + 2k_2 + k_4, 4 - 2k_2) \in \mathbb{Z}^4 \mid k_2.k_3, k_4 \in \mathbb{Z}\} \\
&= \{(16, -16, -4, 4) + (-9k_2 + 4k_3 - 2k_4, 9k_2 - 3k_3, 2k_2 + k_4, -2k_2) \in \mathbb{Z}^4 \mid k_2.k_3, k_4 \in \mathbb{Z}\} \\
&= (16, -16, -4, 4) + \{(-9k_2 + 4k_3 - 2k_4, 9k_2 - 3k_3, 2k_2 + k_4, -2k_2) \in \mathbb{Z}^4 \mid k_2.k_3, k_4 \in \mathbb{Z}\}.
\end{aligned}$$

Además esta misma ecuación fue resuelta en la Sección 3.2 y el conjunto solución en este caso fue expresado como

$$\begin{aligned}
\mathcal{D} &= \{(1 + t_0, -4 - 12t_0 + 3t_1, 20 + 60t_0 - 16t_1 + 7t_2, -10 - 30t_0 + 8t_1 - 4t_2) \in \mathbb{Z}^4 \mid t_0, t_1, t_2 \in \mathbb{Z}\} \\
&= \{(1, -4, 20, -10) + (t_0, -12t_0 + 3t_1, 60t_0 - 16t_1 + 7t_2, -30t_0 + 8t_1 - 4t_2) \in \mathbb{Z}^4 \mid t_0, t_1, t_2 \in \mathbb{Z}\} \\
&= (1, -4, 20, -10) + \{(t_0, -12t_0 + 3t_1, 60t_0 - 16t_1 + 7t_2, -30t_0 + 8t_1 - 4t_2) \in \mathbb{Z}^4 \mid t_0, t_1, t_2 \in \mathbb{Z}\}.
\end{aligned}$$

Sean $H = \{(-9k_2 + 4k_3 - 2k_4, 9k_2 - 3k_3, 2k_2 + k_4, -2k_2) \in \mathbb{Z}^4 \mid k_2.k_3, k_4 \in \mathbb{Z}\}$ y $Q = \{(t_0, -12t_0 + 3t_1, 60t_0 - 16t_1 + 7t_2, -30t_0 + 8t_1 - 4t_2) \in \mathbb{Z}^4 \mid t_0, t_1, t_2 \in \mathbb{Z}\}$. Notemos que $H = \langle(-9, 9, 2, -2), (4, -3, 0, 0), (-2, 0, 1, 0)\rangle$ pues

$$(-9k_2 + 4k_3 - 2k_4, 9k_2 - 3k_3, 2k_2 + k_4, -2k_2) = k_2(-9, 9, 2, -2) + k_3(4, -3, 0, 0) + k_4(-2, 0, 1, 0)$$

y $Q = \langle (1,-12,60,-30),(0,3,-16,8),(0,0,7,-4)\rangle$ *ya que*

$$(t_0,-12t_0+3t_1,60t_0-16t_1+7t_2,-30t_0+8t_1-4t_2) = t_0(1,-12,60,-30)+t_1(0,3,-16,8)+t_2(0,0,7,-4).$$

De acuerdo al Corolario 4.2.7 tenemos que tanto $(16,-16,-4,4)$ *como* $(1,-4,20,-10)$ *son soluciones de la ELD* $18x+24y+36z+63w=12$ *y tanto* H *como* Q *son el conjunto de soluciones de* $18x+24y+36z+63w=0$.

Para terminar este trabajo buscaremos generalizar la operación binaria dada en el artículo [Ch06] para dotar a una clase lateral $t+H$ de estructura de grupo a través de la estructura de grupo que tiene H. La idea es sencilla y natural, consiste de considerar cualesquiera $a,b \in t+H$, luego restar t a ambos elementos para obtener $a-t$ y $b-t$ que están en H y así poder sumarlos como se suman en H obteniendo $(a-t)+(b-t)$. Finalmente trasladamos este resultado sumando t para transformarlo en un elemento en la clase lateral $t+H$, a saber

$$(a-t)+(b-t)+t = a+b-t.$$

Veamos que esto da una estructura de grupo a $t+H$ a partir de la estructura de grupo que tiene H.

Proposición 4.2.9. *Sea* $(G,+)$ *un grupo abeliano. Para algún* $t \in G$*, definamos la operación binaria* $\oplus_t : G \to G$ *tal que para cada* $a,b \in G$

$$a \oplus_t b = a+b-t$$

entonces $(G,\oplus_t)$ *es un grupo abeliano.*

Demostración. Notemos que la operación está bien definida.

1. **Asociatividad:** Sean $a,b,c \in G$ entonces

   $$(a \oplus_t b) \oplus_t c = (a+b-t) \oplus_t c = (a+b-t)+c-t = a+(b+c-t)-t = a \oplus_t (b+c-t) = a \oplus_t (b \oplus_t c).$$

2. **Conmutatividad:** Sean $a,b \in G$ entonces

   $$a \oplus_t b = a+b-t = b+a-t = b \oplus_t a.$$

3. **Neutro aditivo:** Queremos probar que existe $e \in G$ tal que $e \oplus_t a = a \oplus_t e = a$ para toda $a \in G$, entonces requerimos que

   $$a \oplus_t e = a+e-t$$

   para toda $a \in G$, lo que implica que $e = t$. Veamos que efectivamente t es un neutro aditivo. Sea $a \in G$

   $$t \oplus_t a = a \oplus_t t = a+t-t = a$$

   por lo que $t \in G$ es el neutro con respecto a $\oplus_t$.

4. **Inverso aditivo:** Queremos probar que para cada $a \in G$ existe un $c \in G$ tal que $c \oplus_t a = a \oplus c = t$, entonces necesitamos que

$$a \oplus_t c = a + c - t = t$$

lo que implica que $c = 2t - a$. Constatemos que $2t - a \in G$ es el inverso aditivo de $a \in G$, en efecto

$$(2t - a) \oplus_t a = a \oplus_t (2t - a) = a + 2t - a - t = t.$$

□

Con este resultado podemos dar una estructura de grupo a las clases laterales.

Proposición 4.2.10. *Sea $(G, +)$ un grupo abeliano, $t \in G$ y $(H, +)$ un subgrupo de $(G, +)$. Entonces, $(t+H, \oplus_t)$ es un subgrupo de $(G, \oplus_t)$.*

Demostración. Notemos primero que t, el neutro de $(G, \oplus_t)$, es un elemento de $t + H$. Esto es claro ya que $t = t + 0$ con $0 \in H$ debido a que $(H, +)$ es un subgrupo de $(G, +)$. Ahora veamos que $\oplus_t$ es cerrada en $t + H$. Sean $t + h, t + k \in t + H$ con $h, k \in H$. Tenemos que

$$(t + h) \oplus_t (t + k) = (t + h) + (t + k) - t = t + (h + k)$$

con $h + k \in H$ ya que $+$ es cerrada en H debido a que $(H, +)$ es un subgrupo de $(G, +)$, entonces

$$(t + h) \oplus_t (t + k) = t + (h + k) \in t + H.$$

Ahora sea $t + h \in t + H$. Observamos que:

$$(t + h) \oplus_t (t - h) = (t + h) + (t - h) - t = t,$$

por lo que se tiene que $t - h \in G$ es el inverso de $t + h$ respecto a $\oplus_t$ y claramente $t - h \in t + H$ pues $-h \in H$ por ser H cerrado bajo inversos.

Concluimos así que $(t + H, \oplus_t)$ es un subgrupo de $(G, \oplus_t)$. □

En el contexto particular en el que hemos estado trabajando nuestros elementos pertenecen al conjunto de soluciones de un sistema de ecuaciones lineales diofantinas de $m \times n$, denotado como $\mathcal{D}$, que a su vez son elementos del grupo abeliano $G = \mathbb{Z}^n$. De acuerdo a nuestro análisis $\mathcal{D}$ es justamente una clase lateral (izquierda o derecha) del subgrupo H formado por las soluciones del sistema homógeneo asociado con representante $k \in \mathbb{Z}^n$ una solución particular del sistema original. Entonces el Teorema 4.2.5 junto con la Proposición 4.2.10 aplicados a este contexto particular, nos dan como consecuencia otra prueba del Teorema 4.2.1. Para finalizar este trabajo escribamos con una redacción diferente el Teorema 4.2.1 acorde con este análisis en términos de clases laterales y retomemos el Ejemplo 4.2.8 para entender qué grupo es el que se tiene en ese caso:

Teorema 4.2.11. *Sea*

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1\ldots, m. \tag{4.7}$$

un sistema de ELD, $\mathcal{D}$ el conjunto de soluciones del sistema 4.7, H el conjunto de soluciones del sistema homogéneo asociado al sistema 4.7 y $k = (k_1, \ldots, k_n) \in \mathcal{D}$. Entonces $\mathcal{D}$ es la clase lateral de H en $\mathbb{Z}^n$ con representante k. Más aún, si definimos la operación $\oplus_k : \mathbb{Z}^n \to \mathbb{Z}^n$ tal que para cada $a, b \in \mathbb{Z}^n$

$$a \oplus_k b = a + b - k,$$

entonces $(\mathcal{D}, \oplus_k)$ es un subgrupo de $(\mathbb{Z}^n, \oplus_k)$.

Ejemplo 4.2.12. *Por último, una vez más consideremos la ELD del Ejemplo 3.3.17*

$$18x + 24y + 36z + 63w = 12.$$

Entonces por el Ejemplo 4.2.8, el conjunto de soluciones $\mathcal{D}$ es de la siguiente forma:

$$\mathcal{D} = (16, -16, -4, 4) + H$$

con $k = (16, -16, -4, 4) \in \mathcal{D}$ una solución particular, y H el conjunto de soluciones del sistema homógeneo. Podemos definir una función $\phi| : H \to k + H$ tal que $\phi|(x) = k + x$. Notemos que $\phi|$ es la restricción del isomorfismo $\phi : (\mathbb{Z}^4, +) \to (\mathbb{Z}^4, \oplus_k)$ dado en la demostración del Lema 4.1.5, por lo que $\phi|_H$ nos da un isomorfismo entre $(H, +)$ y $(k + H, \oplus_k)$.

Además recordemos que $H = \langle(-9, 9, 2, -2), (4, -3, 0, 0), (-2, 0, 1, 0)\rangle$, por lo que podemos definir una función $\psi : (\mathbb{Z}^3, +) \to (H, +)$ tal que

$$\psi(x, y, z) = x(-9, 9, 2, -2) + y(4, -3, 0, 0) + z(-2, 0, 1, 0)$$

la cual claramente es una biyección. Más aún

$$\begin{aligned}
&\psi((x, y, z) + (a, b, c)) = \psi(x + a, y + b, z + c)\\
&= (x + a)(9, 2, -2) + (y + b)(4, -3, 0, 0) + (z + c)(-2, 0, 1, 0)\\
&= x(-9, 9, 2, -2) + y(4, -3, 0, 0) + z(-2, 0, 1, 0) + a(-9, 9, 2, -2) + b(4, -3, 0, 0) + c(-2, 0, 1, 0)\\
&= \psi(x, y, z) + \psi(a, b, c)
\end{aligned}$$

por lo cual $\psi : (\mathbb{Z}^3, +) \to (H, +)$ es un isomorfismo teniendo así que $(\mathbb{Z}^3, +) \cong (H, +)$. De esta forma por el Teorema 2.1.7 se tiene que $\phi \circ \psi : (\mathbb{Z}^3, +) \to (k + H, \oplus_k)$ es un isomorfismo y por tanto $(\mathbb{Z}^3, +) \cong (k + H, \oplus_k)$.

El ejemplo previo nos invita a conjeturar que podemos encontrar un isomorfismo de grupos de un conjunto de soluciones de un sistema de ecuaciones lineales diofantinas con el grupo $(\mathbb{Z}^t, +)$ para algún $t \in \mathbb{N}$, donde

t correspondería al número de variables libres que tengamos al resolver el sistema. Para concluir este trabajo enunciemos y demostremos la conjetura.

Teorema 4.2.13. *Sea $AX = B$ un sistema de ELD, con $A \in M_{m\times n}(\mathbb{Z})$ y $\mathcal{D} \subseteq \mathbb{Z}^n$ el conjunto de soluciones de este sistema. Entonces*

$$(\mathcal{D}, \oplus_k) \cong (\mathbb{Z}^{n-r}, +),$$

donde $k \in \mathcal{D}$ es una solución particular de la ELD y r es el rango de A.

Demostración. Dado que $AX = B$ tiene soluciones enteras, entonces por el Teorema 3.4.5 sabemos que el sistema $DK = LB$ tiene soluciones enteras, donde D es la forma normal de Smith de A. Por lo tanto, $DK = LB$ lo podemos escribir como

$$DK = \begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix} \begin{pmatrix} k_{11} \\ \vdots \\ k_{r1} \\ k_{(r+1)1} \\ \vdots \\ k_{n1} \end{pmatrix} = \begin{pmatrix} d_1 k_{11} \\ \vdots \\ d_r k_{r1} \end{pmatrix} = LB = \begin{pmatrix} \beta_{11} \\ \vdots \\ \beta_{m1} \end{pmatrix}$$

donde $LB = (\beta_{ij}) \in M_{m\times 1}(\mathbb{Z})$. Dado que el sistema tiene soluciones enteras, entonces

$$k_1 = \frac{\beta_{11}}{d_1}, k_2 = \frac{\beta_{21}}{d_1}, \dots, k_r = \frac{\beta_{m1}}{d_1}$$

son números enteros y $k_{r+1}, \dots, k_n \in \mathbb{Z}$ son $n - r$ enteros arbitrarios. Así, las soluciones del sistema $AX = B$, están dadas por $X = RK$, lo cual es:

$$X = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1} & s_{n2} & \dots & s_{nn} \end{pmatrix} \begin{pmatrix} k_1 \\ \vdots \\ k_r \\ k_{r+1} \\ \vdots \\ k_n \end{pmatrix} = k_1 \begin{pmatrix} s_{11} \\ s_{21} \\ \vdots \\ s_{n1} \end{pmatrix} + \dots + k_r \begin{pmatrix} s_{1r} \\ s_{2r} \\ \vdots \\ s_{nr} \end{pmatrix} + k_{r+1} \begin{pmatrix} s_{1(r+1)} \\ s_{2(r+1)} \\ \vdots \\ s_{n(r+1)} \end{pmatrix} + \dots + k_n \begin{pmatrix} s_{1n} \\ s_{2n} \\ \vdots \\ s_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} s_{11}k_1 + \dots + s_{1r}k_r \\ s_{21}k_1 + \dots + s_{2r}k_r \\ \vdots \\ s_{n1}k_1 + \dots + s_{nr}k_r \end{pmatrix} + k_{r+1} \begin{pmatrix} s_{1(r+1)} \\ s_{2(r+1)} \\ \vdots \\ s_{n(r+1)} \end{pmatrix} + \dots + k_n \begin{pmatrix} s_{1n} \\ s_{2n} \\ \vdots \\ s_{nn} \end{pmatrix}.$$

Sean $u \in \mathbb{Z}^n$ el vector

$$u = \begin{pmatrix} s_{11}k_1 + \ldots + s_{1r}k_r \\ s_{21}k_1 + \ldots + s_{2r}k_r \\ \vdots \\ s_{n1}k_1 + \ldots + s_{nr}k_r \end{pmatrix}$$

con $k_1 = \frac{\beta_{11}}{d_1}, k_2 = \frac{\beta_{21}}{d_1}, \ldots, k_r = \frac{\beta_{m1}}{d_1} \in \mathbb{Z}$ y $v_1, \ldots, v_{n-r} \in \mathbb{Z}^n$ los vectores

$$v_1 = \begin{pmatrix} s_{1(r+1)} \\ s_{2(r+1)} \\ \vdots \\ s_{n(r+1)} \end{pmatrix}, \ldots, v_{n-r} = \begin{pmatrix} s_{1n} \\ s_{2n} \\ \vdots \\ s_{nn} \end{pmatrix},$$

entonces las soluciones del sistema son el conjunto de todos los $X \in \mathbb{Z}^n$ de la forma

$$X = u + k_{r+1}v_1 + \cdots + k_n v_{n-r}$$

con $k_{r+1}, \ldots, k_n \in \mathbb{Z}$ $n - r$ enteros arbitrarios. Concluimos que el conjunto $\mathcal{D}$ de soluciones del sistema de ELD está dado de la siguiente forma

$$\mathcal{D} = \{\, u + k_{r+1}v_1 + \ldots + k_n v_{n-r} \mid \ k_{r+1}, \ldots, k_n \in \mathbb{Z}\}\,.$$

Notemos que u es una solución particular del sistema que se obtiene de considerar todos los parámetros iguales a cero.

Sea $(\mathcal{D}, \oplus_u)$ el grupo formado por las soluciones del sistema $AX = B$ y $\oplus_u$ la operación definida anteriormente. Consideremos la función $\phi : (\mathbb{Z}^{n-r}, +) \to (\mathcal{D}, \oplus_u)$ dada de la siguiente manera

$$\phi(a_1, \ldots, a_{n-r}) = u + a_1v_1 + \ldots + a_{n-r}v_{n-m}.$$

Veamos que es un homomorfismo de grupos. Sean $(a_1, \ldots, a_{n-r}), (b_1, \ldots, b_{n-m}) \in \mathbb{Z}^{n-r}$. Entonces,

$$\begin{aligned} \phi((a_1, \ldots, a_{n-r}) + (b_1, \ldots, b_{n-r})) &= \phi(a_1 + b_1, \ldots, a_{n-r} + b_{n-r}) \\ &= u + (a_1 + b_1)v_1 + \ldots + (a_{n-r} + b_{n-r})v_{n-r} \\ &= (u + a_1v_1 + \ldots + a_{n-r}v_{n-r}) + (u + b_1v_1 + \ldots + b_{n-r}v_{n-r}) - u \\ &= \phi(a_1, \ldots.a_{n-r}) + \phi(b_1, \ldots.b_{n-r}) - u \\ &= \phi(a_1, \ldots.a_{n-r}) \oplus_u \phi(b_1, \ldots.b_{n-r}). \end{aligned}$$

Luego, ϕ es un homomorfismo de grupos.

Veamos ahora que ϕ es un homomorfismo inyectivo. Sean $(a_1, \ldots, a_{n-r}), (b_1, \ldots, b_{n-r}) \in \mathbb{Z}^{n-r}$ tales que

$\phi(a_1, \ldots, a_{n-r}) = \phi(b_1, \ldots, b_{n-r})$. Entonces,

$$\begin{aligned}\phi(a_1, \ldots, a_{n-r}) = \phi(b_1, \ldots, b_{n-r}) &\implies u + a_1v_1 + \ldots + a_{n-r}v_{n-r} = u + b_1v_1 + \ldots + b_{n-r}v_{n-r} \\ &\implies a_1v_1 + \ldots + a_{n-r}v_{n-r} = b_1v_1 + \ldots + b_{n-r}v_{n-r} \\ &\implies (a_1 - b_1)v_1 + \ldots + (a_{n-m} - b_{n-m})v_{n-r} = 0.\end{aligned}$$

Recordemos que $v_1, \ldots, v_{n-r}$ son las últimas $n - r$ columnas de la matriz R, que como se vio al estudiar la forma normal de Smith es invertible, por lo cual $\{v_1, \ldots, v_{n-r}\}$ es un conjunto linealmente independiente. Así,

$$\begin{aligned}(a_1 - b_1)v_1 + \ldots + (a_{n-m} - b_{n-m})v_{n-r} = 0 &\implies a_1 - b_1 = 0, \ldots, a_{n-r} - b_{n-r} = 0 \\ &\implies a_1 = b_1, \ldots, a_{n-r} = b_{n-r} \\ &\implies (a_1, \ldots, a_{n-r}) = (b_1, \ldots, b_{n-r}).\end{aligned}$$

Luego, ϕ es inyectiva. Claramente ϕ es suprayectiva, por lo que ϕ es una función biyectiva. Luego, $(\mathcal{D}, \oplus_u)$ es isomorfo a $(\mathbb{Z}^{n-r}, +)$. □

Bibliografía

[AMSS14] Avella, D., Mendoza, O., Sáenz, E. C. y Souto, M. J. (2014). *Grupos I*, Colección Papirhos IMUNAM, México, 192 pp.

[Cho79] Chou, T. W. (1979). *Ph.D. Thesis, Algorithms for the solution of systems of linear Diophantine equations*, Computer Science Dept., Univ. of Wisconsin, Madison. 123 pp.

[Ch06] Choudhry, A. (2006). *Integer Solutions of Linear Diophantine Equations Form a Group*, Missouri Journal of Mathematical Sciences, 18(2), 135-141.

[SM] Evens, Sam (s.f.). *Smith Normal Form over the Integers* .`https://www3.nd.edu/~sevens/smithform.pdf`

[Gi90] Gilbert, W. J. y Pathria, A. (1990). *Linear Diophantine Equations.* `https://www.math.uwaterloo.ca/~wgilbert/Research/GilbertPathria.pdf`

[GL14] Gómez, C. (2014). *Álgebra superior curso completo*, Ed. UNAM, México. 618 pp.

[Go71] Gordon, H. (1971). *Algorithms for Hermite and Smith normal matrices and linear Diophantine equations*, Math. Comp., 25, pp. 897–907.

[Ja85] Jacobson, N. (1985). *Basic Algebra I*, W.H. Freeman and Co., San Francisco. 499 pp.

[Ko07] Koshy, T. (2007). *Elementary Number Theory with Applications.* (2nd edition), San Diego: Harcourt/Academic Press. 800 pp.

[La96] Lazebnik, F. (1996). *On Systems of Linear Diophantine Equations*, Mathemathics Magazine, 69 (4), pp. 261-266.

[NZ91] Niven, I., Zuckerman, H. y Montgomery, H. (1991). *An Introduction to the Theory of Numbers*, New York: J. Wiley. 529 pp.

[Ro00] Rotman, J. (2000). *A first course in abstract algebra*, New Jersey, Prentice Hall, 531 pp.

[Ro99] Rotman, J. (1999). *An introduction to the theory of groups*, New York, Springer. 517 pp.