LA GENERACIÓN

Desde los espacios vectoriales hasta los monoides

Autor: Juan José Tébar Vizcaíno
Titulación: Grado de Matemáticas

Director: David Llena Carrasco
Fecha de defensa: 21 de Julio de 2014

A mi familia

Índice general

Introducción

En esta memoria de Trabajo de Fin de Grado, queremos estudiar un concepto, el de la **generación minimal** en los distintos campos en que, desde el punto de vista algebraico, podemos trabajar. La importancia de los sistemas de generadores radica en que son una manera cómoda y fácil de atacar los problemas que aparecen en conjuntos más grandes, normalmente infinitos, con la única información de unos pocos elementos del conjunto.

El caso más fácil y sencillo se plantea en el ambiente de espacios vectoriales, y es el que se presenta en el primer capítulo de esta memoria. El poder contar con una base en un espacio vectorial, nos permite controlar y estudiar, e incluso, clasificar los espacios vectoriales finitamente generados, que son aquellos en los que hay sistemas de generadores finitos. Conocer una base, permite definir una aplicación de forma concreta, dando o conociendo las imágenes de los elementos de una base. Y además, el número elementos de una base, en el caso de Espacios Vectoriales es siempre el mismo, y es lo que conocemos como dimensión del espacio. Como resultado principal, tenemos que dos espacios vectoriales finitamente generados son isomorfos (indistinguibles como espacios vectoriales) si y solo si tienen la misma dimensión. Así pues, un espacio vectorial real de dimensión n es "igual" a $\mathbb{R}^n$, como espacios vectoriales.

Asociados a los sistemas de generadores, estudiamos los sistemas de ecuaciones lineales homogéneos. Ya que, éstos definen espacios vectoriales dentro de un espacio vectorial general. Serán los llamados subespacios de un espacio. Un estudio exhaustivo de estos sistemas de ecuaciones, nos ayudará a la hora de afrontar el concepto de generación en los otros ambientes en que trabajaremos: los módulos y los monoides.

Una estructura típica, y así lo recogemos en el correspondiente epígrafe, para los espacios vectoriales, es la idea de espacio cociente que nos permite ver como un nuevo espacio vectorial, el conjunto formado por todos los subespacios afines paralelos a un subespacio vectorial fijo. También será útil para el estudio de módulos y monoides, apareciendo en el primer caso los módulos de torsión y en el segundo una forma sencilla para afrontar el estudio de los monoides y en particular los semigrupos afines a partir del concepto de congruencia que definiremos.

Por último, y también como la herramienta para comparar objetos de las mismas características tenemos las aplicaciones, que serán lineales si se dan entre espacios vectoriales y respetan dichas estructuras, y que se denominarán morfismos de módulos o monoides en sus respectivos casos.

En cada uno de los tres capítulos fundamentales, tratamos de seguir el hilo conductor que no es otro, que ver cómo se van trasformando los conceptos que hemos comentado anteriormente, conforme el conjunto sobre el que se hace la estructura va cambiando desde los cuerpos en el caso de espacios vectoriales, pasando por anillos en el caso de módulos, y acabando en $\mathbb{N}$ para el caso de monoides. Aunque también nos acercaremos a construcciones

nuevas que van apareciendo, por ejemplo los módulos de torsión o la clasificación de monoides cancelativos a partir de las congruencias.

Se trata, pues, de un trabajo que pretende recorrer unos conceptos concretos, y por tanto, nos centramos sólo en casos y ambientes en los que éstos se perciben más claramente, y se pueden estudiar con comodidad. Dejamos, así, de estudiar los sistemas infinitos de generadores, o también, los módulos en los que el anillo base no es especialmente "bueno", o en los monoides, acabaremos centrando nuestra atención en dos clases concretas de los mismos.

La parte de espacios vectoriales, en su totalidad está recogida en la asignatura GEOMETRÍA ELEMENTAL de primer curso de grado, aunque algunas demostraciones se han rehecho para facilitar el hilo conductor y poder compararlas en el caso de módulos o monoides. Esta labor también se ha realizado en los otros capítulos. Se podría decir, que adaptar las demostraciones para poder compararlas, ha sido la parte más compleja de este Trabajo de Fin de Grado. Las ideas desarrolladas en el capítulo de módulos aparecen diseminadas en las asignaturas: ESTRUCTURAS BÁSICAS DEL ÁLGEBRA de primero de grado, MATEMÁTICA DISCRETA de segundo, GRUPOS, ANILLOS Y CUERPOS de tercer curso, aunque no hay un estudio pormenorizado como el que aquí se presenta. Por último, el capítulo de monoides, no se contempla en el grado, siendo por tanto su estudio una parte exclusiva de este Trabajo Fin de Grado, para este tercer capítulo nos hemos ayudado de los libros de García-Sánchez y Rosales que aparecen referenciados en la bibliografía.

Al ser este, un trabajo que discurre por varias disciplinas de las matemáticas, no es un estudio en profundidad y, como hemos comentado anteriormente, nos centramos en sólo algunos aspectos de cada uno de los campos que atravesamos, con la idea de ver la trasformación que sufren los distintos conceptos que pretendemos estudiar. La principal complejidad ha sido seleccionar aquellos aspectos a tratar, entre todos los que pudimos estudiar, y luego adaptar las demostraciones para que se pudiesen comparar y sacar así con más nitidez las dificultades que sobrevienen conforme avanzamos en el camino: Espacios vectoriales, módulos, monoides...

Espacios vectoriales

DEFINICIÓN 1. *Dado un cuerpo* $\mathbb{K}$, *definimos un* $\mathbb{K}$***-espacio vectorial*** *como un conjunto* V *junto con dos operaciones: una suma* $(+)$ *de elementos de* V *y un producto* $(\cdot)$ *de elementos de* $\mathbb{K}$ *por elementos de* V, *cumpliendo las siguientes propiedades:*

1. $u + (v + w) = (u + v) + w$, *para todo* $u, v, w \in V$ *(asociativa),*
2. $u + v = v + u$, *para todo* $u, v \in V$ *(conmutativa),*
3. *Existe* $0 \in V$ *tal que* $0 + v = v + 0 = v$, *para todo* $v \in V$ *(elemento neutro),*
4. *Para cada* $v \in V$ *existe* $-v$ *tal que* $v + (-v) = (-v) + v = 0$ *(elemento opuesto),*
5. $a \cdot (b \cdot v) = (a \cdot b) \cdot v$, *para todo* $v \in V$, *para todo* $a, b \in \mathbb{K}$ *(seudo-asociativa),*
6. $a \cdot (u + v) = a \cdot u + a \cdot v$ *para todo* $u, v \in V$ *y para todo* $a \in \mathbb{K}$ *(distributiva respecto a la suma de vectores),*
7. $(a + b) \cdot v = a \cdot v + b \cdot v$, *para todo* $v \in V$ *y para todo* $a, b \in \mathbb{K}$ *(distributiva respecto a la suma de escalares),*
8. $1 \cdot v = v$, *para todo* $v \in V$ *(unimodular).*

Llamaremos vectores a los elementos de V *y escalares a los elementos de* $\mathbb{K}$.

Si no hay peligro de confusión omitiremos el punto en la multiplicación de un escalar y un vector.

1. Sistemas de generadores

DEFINICIÓN 2. *Sea* V *un* $\mathbb{K}$*-espacio vectorial. Un subconjunto* S, *posiblemente infinito, de* V *se dice* ***sistema de generadores*** *de* V *si, para todo* $v \in V$, *existen* $s_1, \ldots, s_n \in S$ *y* $a_1, \ldots, a_n \in \mathbb{K}$ *tales que* $v = a_1 s_1 + \cdots + a_n s_n$.

Mientras no haya confusión hablaremos simplemente de espacio vectorial, sin escribir el cuerpo $\mathbb{K}$.

DEFINICIÓN 3. *Decimos que un espacio vectorial* V *es* ***finitamente generado*** *si es posible encontrar un sistema de generadores finito.*

En este trabajo nos centraremos en los espacios vectoriales que sean finitamente generados.

Recordemos también la definición de independencia lineal que, unida a la anterior, nos da la noción de base, herramienta fundamental en espacios vectoriales.

DEFINICIÓN 4. *Un subconjunto* S *de* V *se dice* ***linealmente independiente*** *si para cualesquiera* $s_1, \ldots, s_n \in S$ *se tiene que:*

$$a_1 s_1 + \cdots + a_n s_n = 0 \text{ con } a_i \in \mathbb{K} \Rightarrow a_1 = a_2 = \cdots = a_n = 0.$$

La idea es que la única combinación lineal nula es aquella en la que todos los escalares son cero.

DEFINICIÓN 5. *Una **base** para un espacio vectorial es un sistema de generadores linealmente independiente.*

PROPOSICIÓN 6. *Todo elemento v de un espacio vectorial se puede escribir de forma única como combinación lineal de una base.*

DEMOSTRACIÓN. La unicidad viene asegurada por la independencia lineal. Sea $B = \{e_1, \dots, e_n\}$ una base de V, por ser sistema de generadores todo $v \in V$ se puede escribir: $v = a_1e_1 + \cdots + a_ne_n$. Si además existiese otra combinación lineal $v = b_1e_1 + \cdots + b_ne_n$ restando ambas igualdades tenemos que $0 = (a_1 - b_1)e_1 + \cdots + (a_n - b_n)e_n$. Usando la independencia lineal se tiene que $a_i - b_i = 0$ para todo $i = 1, \dots, n$. Probando que ambas escrituras del vector son la misma. □

DEFINICIÓN 7. *Llamaremos **coordenadas de** $v \in V$ **respecto de una base** $B = \{e_1, \dots, e_n\}$ a la n-upla $(a_1, \dots, a_n)_B$ si $v = a_1e_1 + \cdots + a_ne_n$.*

Vamos a probar el principal resultado sobre las bases de un espacio vectorial, que nos asegura que todas tienen el mismo número de elementos. A dicho número lo llamaremos dimensión del espacio vectorial. Antes un lema técnico.

LEMA 8. *Sea $B = \{e_1, \dots, e_n\}$ una base de un espacio vectorial V, sea $v \in V$ y $v = \sum_{i=1}^{n} \lambda_i e_i$. Si $\lambda_1 \neq 0$, entonces $B' = \{v, e_2, \dots, e_n\}$ es una base de V.*

DEMOSTRACIÓN. Veamos que B' es linealmente independiente. Sea $av + a_2e_2 + \cdots + a_ne_n = 0$. Sustituimos el valor de v y tenemos $a\left(\sum_{i=1}^{n} \lambda_i e_i\right) + a_2e_2 + \cdots + a_ne_n = 0$. Ahora, desarrollando tenemos:

$$a\lambda_1e_1 + (a\lambda_2 + a_2)e_2 + \cdots + (a\lambda_n + a_n)e_n = 0.$$

Y como B es una base, todos los escalares de la igualdad anterior son nulos. En particular $a\lambda_1 = 0$ y como $\lambda_1 \neq 0$ se tendría que $a = 0$. Y como $a\lambda_i + a_i = 0$, se deduce fácilmente que todos los a_i son nulos, puesto que $a = 0$.

Veamos ahora que B' es un sistema de generadores. Sabemos que cualquier $u \in V$ se puede escribir como $u = a_1e_1 + a_2e_2 + \cdots + a_ne_n$. Por otra parte como $\lambda_1 \neq 0$ podemos escribir $e_1 = \frac{1}{\lambda_1}v - \frac{\lambda_2}{\lambda_1}e_2 - \cdots - \frac{\lambda_n}{\lambda_1}e_n$, que sustituyendo en la igualdad anterior quedaría:

$$u = a_1\left(\frac{1}{\lambda_1}v - \frac{\lambda_2}{\lambda_1}e_2 - \cdots - \frac{\lambda_n}{\lambda_1}e_n\right) + a_2e_2 + \cdots + a_ne_n.$$

Reordenado podríamos escribir cualquier $u \in V$ como:

$$u = a_1\frac{1}{\lambda_1}v + \left(a_2 - \frac{a_1\lambda_2}{\lambda_1}\right)e_2 + \cdots + \left(a_n - \frac{a_1\lambda_n}{\lambda_1}\right)e_n.$$

Con lo que quedaría demostrado que B' es un sistema de generadores. □

NOTA 9. En el lema anterior, el vector v se puede sustituir por cualquier e_i, siempre y cuando el correspondiente $\lambda_i \neq 0$.

Utilizando este lema podemos demostrar el Teorema de la Base.

TEOREMA 10 (de la Base). *Sea V un espacio vectorial finitamente generado. Entonces todas las bases de V tienen el mismo cardinal.*

DEMOSTRACIÓN. Sean $B = \{e_1, \ldots, e_m\}$ y $B' = \{v_1, \ldots, v_n\}$ dos bases de V con $m \leq n$. Entonces podemos escribir $e_1 = a_1v_1 + \cdots + a_nv_n$ con algún $a_i \neq 0$, por comodidad supondremos que es el primero (si no, reordenamos B'). Así, $a_1 \neq 0$ y aplicando el lema anterior $\{e_1, v_2, \ldots, v_n\}$ es una base. Ahora se puede escribir $e_2 = a_1e_1 + a_2v_2 + \cdots + a_nv_n$ (estos a_i no son los de la cuenta anterior). Por el lema anterior, algún $a_i \neq 0$, y además, tiene que ser distinto del primero ya que si el único a_i no nulo fuese a_1 se tendría que $e_2 = a_1e_1$, pero esto no puede ser porque ambos forman parte de la base B. Así pues, como antes, podemos suponer que $a_2 \neq 0$ (salvo reordenamiento en B') y aplicar el lema anterior para tener que $\{e_1, e_2, v_3, \ldots, v_n\}$ es base de V. De forma análoga se iría razonando hasta llegar a meter todos los elementos de B y obtener que $\{e_1, \ldots, e_m, v_{m+1}, \ldots, v_n\}$ es una base. Pero todos los v_i que quedan se pueden poner como combinación de $e_1, \ldots, e_m$ que son la base B, pero esto es imposible en una base. Por tanto, no es cierto que existan tales $\{v_{m+1}, \ldots, v_n\}$, a no ser que $n = m$. □

COROLARIO 11. *Si $\{e_1, \ldots, e_m\}$ es un conjunto linealmente independiente y $\{v_1, \ldots, v_n\}$ es un sistema de generadores de un espacio vectorial V, entonces $m \leq n$.*

DEMOSTRACIÓN. Es repetir el argumento de la demostración del teorema anterior, ya que el Lema 8 también es cierto si cambiamos base por sistema de generadores, y de $B = \{e_1, \ldots, e_m\}$, realmente solo se utiliza que sean linealmente independientes. □

DEFINICIÓN 12. *Se define la **dimensión** de un espacio vectorial V como el cardinal de una cualquiera de sus bases.*

COROLARIO 13. *Si V es un espacio vectorial de dimensión n y $B = \{v_1, \ldots, v_n\}$ es un conjunto de vectores linealmente independiente (respectivamente sistema de generadores) entonces B es una base. Es decir, si sabemos que n es la dimensión del espacio vectorial, sólo es necesario probar una de las dos condiciones para asegurar que un conjunto de n vectores es una base.*

DEMOSTRACIÓN. En ambos casos el razonamiento es análogo. Si B es linealmente independiente pero no es sistema de generadores, es porque algún elemento $v \in V$ no es combinación lineal de $\{v_1, \ldots, v_n\}$ por tanto $\{v, v_1, \ldots, v_n\}$ sería un conjunto linealmente independiente con $n + 1$ elementos, pero B es un sistema de generadores con n elementos, contradiciendo el Corolario 11. Por otra parte, si B es sistema de generadores pero no linealmente independiente, con un argumento similar al desarrollado en el Lema 8, podríamos quitar un elemento y tendríamos un sistema de generadores con menos elementos que B, que es linealmente independiente, en contradicción de nuevo con el Corolario 11. □

Con los resultados obtenidos hasta ahora es fácil deducir los dos siguientes teoremas.

TEOREMA 14 (Teorema de Extensión de la Base). *Sea V un espacio vectorial finitamente generado. Entonces cualquier conjunto linealmente independiente de V se puede completar hasta una base de V.*

TEOREMA 15 (Teorema de Extracción de una Base). *Sea V un espacio vectorial finitamente generado. Entonces de cualquier sistema de generadores de V se puede extraer una base para V.*

Obsérvese que la condición para añadir un elemento, es que sea linealmente independiente del resto. Mientras que la condición para quitar un elemento es que sea generado por el resto.

2. Subespacios

DEFINICIÓN 16. *Un subconjunto U de un $\mathbb{K}$-espacio vectorial V, es un* ***$\mathbb{K}$-subespacio vectorial****, si U es espacio vectorial con las mismas operaciones suma y producto por escalares que V.*

Otras definiciones equivalentes son las siguientes:

DEFINICIÓN 17. *Sea V un $\mathbb{K}$-espacio vectorial y sea U un subconjunto no vacío de V. Diremos que U es* ***$\mathbb{K}$-subespacio vectorial*** *de V si:*

1. *U es cerrado para la suma: $\forall u, v \in U, u + v \in U$.*
2. *U es cerrado para el producto por escalares: $\forall u \in U, \forall a \in \mathbb{K}, au \in U$.*

Ambas propiedades se pueden probar a la vez como recogemos en la tercera definición.

DEFINICIÓN 18. *Un subconjunto U no vacío de un $\mathbb{K}$-espacio vectorial V, es un* ***$\mathbb{K}$-subespacio vectorial*** *de V si:*

$$\forall u, v \in U \text{ y } \forall a, b \in \mathbb{K}, \text{ se tiene que } au + bv \in U.$$

DEFINICIÓN 19. *Dado $S = \{x_1, \ldots, x_n\}$ un conjunto de vectores de un espacio vectorial V, se define el* ***subespacio generado por*** *S, como el menor subespacio de V que contiene a S. Lo denotaremos $L(S)$. De forma práctica este subespacio se puede obtener como:*

$$L(S) = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}, r_i \in \mathbb{K}, x_i \in S \right\}.$$

Todo subespacio vectorial se puede definir, esencialmente, de dos formas distintas:

1. Dando un sistema de generadores del mismo, o equivalentemente una base.
2. Dando unas ecuaciones lineales homogéneas que sólo cumplan los elementos del subespacio.

EJEMPLO 20. En $\mathbb{R}^3$ el subespacio generado por $\{(1,0,0),(0,1,0)\}$ es el mismo que el descrito por la ecuación $z = 0$. Es decir:

$$L(\{(1,0,0),(0,1,0)\}) = \{(x,y,z) \in \mathbb{R}^3 \colon z = 0\}.$$

DEFINICIÓN 21. *Si ninguna de dichas ecuaciones es redundante, se dice que son unas* ***ecuaciones cartesianas*** *de dicho subespacio.*

Hay una fórmula muy conocida que nos relacionan las dimensiones de U, V y el número de ecuaciones cartesianas que definen a U:

$$dim(U) = dim(V) - \text{número de ecuaciones cartesianas.}$$

La demostración la obtendremos al final del siguiente epígrafe, como una consecuencia elemental.

2.1. Las trasformaciones elementales de matrices: Una herramienta. Asociadas al algoritmo de Gauss para la resolución de sistemas de ecuaciones lineales, aparecen las trasformaciones elementales por filas de matrices, que se clasifican en tres tipos.

1. Intercambiar dos filas. Denotaremos A_{ij} a la matriz que se obtiene de A intercambiando las filas i y j.
2. Multiplicar una fila por un número distinto de cero. Denotaremos $A_i(k)$ a la matriz que se obtiene de A multiplicando la fila i por $k \in \mathbb{K} \setminus \{0\}$.
3. Sumar a una fila otra multiplicada por un número. Denotaremos $A_{ij}(k)$ a la matriz que se obtiene de A al sumar a la fila j la fila i multiplicada por $k \in \mathbb{K}$.

DEFINICIÓN 22. *Dos matrices del mismo tamaño se dicen* ***equivalentes por filas*** *si se puede obtener una de otra por trasformaciones elementales.*

Es fácil ver que estas operaciones se trasladan a los sistemas de generadores como nos dice la siguiente proposición.

PROPOSICIÓN 23. *Si $S = \{u_1, u_2, \ldots, u_n\}$ es un sistema de generadores del subespacio vectorial U, entonces también son sistemas de generadores de U los siguientes conjuntos:*

1. *El conjunto $\{u_1, \ldots, u_j, \ldots, u_i, \ldots, u_n\}$, que se obtiene de S intercambiando la posición del vector u_i por la posición del vector u_j.*
2. *El conjunto $\{u_1, \ldots, ku_i, \ldots, u_n\}$, que se obtiene de S multiplicando el vector u_i por un escalar $k \in \mathbb{K}$ no nulo.*
3. *El conjunto $\{u_1, \ldots, u_i, \ldots, u_j + ku_i, \ldots, u_n\}$, que se obtiene de S sumando al vector u_j el vector u_i multiplicado por $k \in \mathbb{K}$.*

DEMOSTRACIÓN. La demostración es bastante elemental y se puede encontrar en [**3**]. □

PROPOSICIÓN 24. *Sea $B = \{(a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})\}$ un sistema de generadores de un subespacio U de $\mathbb{K}^n$. Consideramos la matriz:*

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

Sea $A' = (a'_{ij})$ una matriz equivalente por filas a A, entonces el conjunto formado por las filas de A':

$$B' = \{(a'_{11}, a'_{12}, \ldots, a'_{1n}), (a'_{21}, a'_{22}, \ldots, a'_{2n}), \ldots, (a'_{m1}, a'_{m2}, \ldots, a'_{mn})\},$$

también es un sistema de generadores de U.

DEMOSTRACIÓN. Es la proposición anterior para el caso en que trabajemos en $\mathbb{K}^n$. □

Si aplicamos las trasformaciones elementales a la matriz identidad obtenemos las llamadas matrices elementales que denotaremos E_{ij}, $E_i(k)$ y $E_{ij}(k)$ respectivamente.

Es fácil comprobar las siguientes afirmaciones:

1. Las matrices elementales son invertibles ya que: $det(E_{ij}) = -1$, $det(E_i(k)) = k$, y $det(E_{ij}(k)) = 1$.

2. Las trasformaciones elementales por filas en una matriz A se pueden obtener multiplicando por la izquierda por las matrices elementales: $A_{ij} = E_{ij}A$, $A_i(k) = E_i(k)A$ y $A_{ij}(k) = E_{ij}(k)A$.
3. Si hacemos las trasformaciones elementales a la matriz A por columnas y las denominamos A'_{ij}, $A'_i(k)$ y $A'_{ij}(k)$, se tiene que: $A'_{ij} = AE_{ij}$, $A'_i(k) = AE_i(k)$ y $A'_{ij}(k) = AE_{ji}(k)$.

Como resultado de lo anterior se tiene el siguiente teorema.

TEOREMA 25. *Dada A una matriz de tamaño $m \times n$, se pueden encontrar dos matrices invertibles P y Q de tamaños $m \times m$ y $n \times n$ respectivamente, tales que $QAP^{-1} = D_r$. Donde D_r es la matriz con r unos consecutivos en la diagonal principal y el resto de las entradas nulas.*

DEMOSTRACIÓN. Las matrices P y Q serán el producto de matrices elementales, que recogen las trasformaciones por filas, en Q, y por columnas, en P^{-1}, que se hacen a la matriz A para obtener la matriz D_r. Ambas matrices P y Q son invertibles por el resultado anterior y debido a que $det(AB) = det(A)det(B)$.

En el algoritmo siguiente explicitaremos el método para construir D_r. □

Para más detalles del desarrollo de estos resultados, remitimos al lector a la monografía [**3**].

DEFINICIÓN 26. *Al número r del teorema anterior se le denomina **rango** de la matriz A.*

Damos a continuación el algoritmo para obtener dichas matrices. Definimos, previamente, lo que será el pivote de una fila.

DEFINICIÓN 27. *El pivote de una fila de una matriz será el primer elemento empezando por la izquierda no nulo, tras dividir por él la fila entera, obteniendo así un 1 en ese lugar.*

ALGORITMO 28. *Para obtener la matriz D_r.*

1. *Buscar una fila con el elemento de la primera columna no nulo, llamémosle a. Si no existe, ir al paso 5.*
2. *Llevar esta fila al principio.*
3. *Dividir la fila por el elemento no nulo a para obtener un pivote en dicha fila.*
4. *Usar ese pivote para eliminar todos los elementos de la columna por debajo del mismo. Para ello hay que sumar a cada fila inferior, la fila del pivote, multiplicada por el opuesto del elemento que se quiera eliminar.*
5. *Repetir el paso 1 con la siguiente columna y en el paso 2, llevar la fila en cuestión a la primera fila sin pivote.*

Una vez acabado el bucle anterior se tiene una matriz escalonada por filas, pero por encima de los pivotes puede haber elementos no nulos que hay que eliminar (no es reducida). Las filas por debajo de los pivotes son nulas.

6 *Buscar el último pivote y eliminar todos los elementos no nulos de su columna que quedan por encima de él, multiplicando dicho pivote por el opuesto del elemento a eliminar.*

7 *Repetir el paso 6 con el pivote anterior.*

Al acabar este segundo bucle tendremos una matriz escalonada reducida por filas. Ahora, trabajando por columnas llegaremos a la matriz D_r.

8 Con el primer pivote y haciendo trasformaciones por columnas eliminamos todos los elementos no nulos a la derecha del pivote.

9 Hacemos el paso 8 con el siguiente pivote.

10 Si el pivote de una fila i no está en la diagonal principal se intercambian las columnas i y la que tiene el pivote para colocarlo en la diagonal principal.

Al acabar obtenemos la matriz D_r.

Ahora, todas las trasformaciones hechas en los pasos del 1 al 7 son trasformaciones por filas, con ellas se obtendrá la matriz Q. Mientras que las trasformaciones realizadas en los pasos del 8 al 10 son trasformaciones por columnas, que darán lugar a la matriz P^{-1}.

Veamos un ejemplo y luego recogemos el resultado en forma de proposición.

Ejemplo 29. A la hora de hacer trasformaciones por filas, es práctico colocar a la derecha la matriz identidad, y hacer las trasformaciones a toda la matriz. De esta forma, en esta segunda matriz se recogen los cambios por filas, y al acabar se obtendrá la matriz Q.

$$(A|Id) = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 3 & 5 & 0 & 1 & 0 \\ 3 & 4 & 7 & 0 & 0 & 1 \end{array}\right) \sim_f \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & -1 & 0 \\ 0 & -2 & -2 & -3 & 0 & 1 \end{array}\right) \sim_f$$

$$\sim_f \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right) \sim_f \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & -3 & 2 & 0 \\ 0 & 1 & 1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right) = (QA|Q).$$

Y ahora hacemos trasformaciones elementales por columnas a la matriz resultante, de forma análoga, colocamos la matriz identidad debajo, para recoger los cambios por columnas y así obtener la matriz P^{-1}.

$$\left(\frac{QA}{Id}\right) = \left(\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \sim_c \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ \hline 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{array}\right) = \left(\frac{D_r}{P^{-1}}\right).$$

Una vez hecho esto tendría $QAP^{-1} = D_r$ con la siguiente escritura:

$$\begin{pmatrix} -3 & 2 & 0 \\ 2 & -1 & 0 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 5 \\ 3 & 4 & 7 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Como $r = 2$, por la Proposición 24, sabemos que las dos primeras filas de QA forman una base de U: $\{(1, 0, 1), (0, 1, 1)\}$. Fácilmente se observa que al multiplicar estas dos filas por la última columna de P^{-1} se anulan. Por tanto esta última columna son los coeficientes de una ecuación cartesiana de U, que sería: $-x - y + z = 0$.

El algoritmo reflejado en el ejemplo anterior,busca una matriz QA escalonada reducida por filas, i.e, una matriz tal que:

1. El pivote de cada fila (el primer elemento no nulo de cada fila) sea 1.
2. Por encima y por debajo de cada pivote solo hay ceros.
3. Cada pivote esté situado a la derecha del pivote de la fila anterior.
4. Las filas nulas están situadas en la parte inferior de la matriz.

NOTA 30. El número de pivotes coincidirá con el rango de A.

Una vez obtenida QA, usaremos el pivote de cada fila para ir anulando los elementos que aparezcan en su fila. Y por último, intercambiaremos las columnas para poner los unos en la diagonal principal.

PROPOSICIÓN 31. *Sea U el subespacio y A matriz de la Proposición 24. Sean P y Q como en el Teorema 25. Entonces las r primeras filas de QA son una base de U, y por tanto, $dim(U) = r$. Además las $(n-r)$ últimas columnas de P^{-1} nos dan unas ecuaciones cartesianas de U. Con lo que se demuestra que $dim(U) = dim(\mathbb{K}^n) -$ número de ecuaciones cartesianas.*

DEMOSTRACIÓN. Siguiendo la notación de la Proposición 24, sabemos que QA es un sistema de generadores, pero es fácil ver que también es linealmente independiente, por tanto es una base de U. Con lo que r también es la dimensión de U. Ahora, como al multiplicar todos estos elementos por las $n-r$ últimas columnas de P^{-1} se anulan, ya que dan las $n-r$ últimas columnas de D_r que son nulas, y estas $n-r$ columnas son linealmente independientes, podemos deducir que: las $n-r$ últimas columnas de P^{-1} son los coeficientes de unas ecuaciones cartesianas que definen al subespacio U. Y así, tendríamos una prueba de la fórmula:

$$dim(U) = dim(\mathbb{K}^n) - \text{número de ecuaciones cartesianas.}$$

□

3. Aplicaciones Lineales

DEFINICIÓN 32. *Una aplicación, $f\colon V \to V'$, entre dos $\mathbb{K}$-espacios vectoriales, se dice* ***aplicación lineal****, si respeta la suma y el producto por escalares, es decir si:*

1. *$f(u+v) = f(u) + f(v)$ para todo $u, v \in V$.*
2. *$f(av) = af(v)$ para todo $a \in \mathbb{K}$ y todo $v \in V$.*

Como sucede en el caso de los subespacios, ambas propiedades se pueden resumir en una y obtenemos una definición alternativa.

DEFINICIÓN 33. *Una aplicación, $f : V \to V'$, entre dos $\mathbb{K}$-espacios vectoriales, es lineal si*

$$f(au + bv) = af(u) + bf(v),\ \forall a, b \in \mathbb{K},\ \forall u, v \in V.$$

PROPOSICIÓN 34. *Sea $f : V \to V'$ una aplicación lineal, entonces se verifica:*

1. *$f(0) = 0$.*
2. *$f(-v) = -f(v)$.*
3. *$f(a_1v_1 + \cdots + a_nv_n) = a_1f(v_1) + \cdots + a_nf(v_n)$, para cualesquiera $a_1, \ldots, a_n \in \mathbb{K}$, $v_1, \ldots, v_n \in V$.*

La demostración es muy sencilla y se puede encontrar en [**3**].

NOTA 35. La tercera propiedad, se vuelve muy útil en el ambiente de espacios vectoriales, ya que nos permite definir completamente una aplicación lineal dando únicamente las imágenes de los elementos de una base.

DEFINICIÓN 36. *Sea $f : V \to V'$ una aplicación lineal, se definen su* ***núcleo*** *y su* ***imagen*** *como:*

$$\mathrm{Ker}(f) = \{v \in V \mid f(v) = 0\}$$
$$\mathrm{Im}(f) = \{f(v) \mid v \in V\}$$

LEMA 37. *Dada una aplicación lineal $f : V \to V'$, se tiene que* $\mathrm{Ker}(f)$ *es un subespacio de V y que* $\mathrm{Im}(f)$ *es un subespacio de V'.*

DEMOSTRACIÓN. Probemos primero que $\mathrm{Ker}(f)$ es un subespacio de V. Para ello, sean $a, b \in \mathbb{K}, u, v \in \mathrm{Ker}(f)$, entonces: $f(au + bv) = af(u) + bf(v) = a0 + b0 = 0$ luego $au + bv \in \mathrm{Ker}(f)$.

Probemos, ahora, que $\mathrm{Im}(f)$ es un subespacio de V'. Tomemos $a, b \in \mathbb{K}, u', v' \in \mathrm{Im}(f)$. Por la definición de $\mathrm{Im}(f)$, existen $u, v \in V$ de forma que $f(u) = u'$ y $f(v) = v'$, pero entonces tenemos que $f(au+bv) = af(u)+bf(v) = au'+bv'$. Con lo que, también $au'+bv' \in \mathrm{Im}(f)$. □

El siguiente lema es un resultado muy natural, en el sentido de que podremos extenderlo hasta el ambiente de monoides. Sin embargo, otros resultados que veremos posteriormente serán más difíciles de extender o incluso imposible.

LEMA 38. *Dada una aplicación $f : V \to V'$, si $\{v_1, \ldots, v_n\}$ es un sistema de generadores de V, entonces $\{f(v_1), \ldots, f(v_n)\}$ es un sistema de generadores de* $\mathrm{Im}(f)$.

DEMOSTRACIÓN. Dado $v' \in \mathrm{Im}(f)$, existe $v \in V$ de forma que $f(v) = v'$ y, puesto que $\{v_1, \ldots, v_n\}$ es un sistema de generadores de V, el vector $v \in V$ se podrá escribir como combinación lineal de ellos: $v = a_1v_1 + \cdots + a_nv_n$, entonces:

$$v' = f(v) = f(a_1v_1 + \cdots + a_nv_n) = a_1f(v_1) + \cdots + a_nf(v_n).$$

Luego cualquier $v' \in \mathrm{Im}(f)$ se escribe como combinación lineal de $\{f(v_1), \ldots, f(v_n)\}$, y por tanto es un sistema de generadores de $\mathrm{Im}(f)$. □

PROPOSICIÓN 39. *Dada una aplicación lineal $f : V \to V'$, se verifica que:*

1. *f es inyectiva $\Leftrightarrow$ para todo conjunto lineal independiente, $\{v_1, \ldots, v_r\}$, el conjunto $\{f(v_1), \ldots, f(v_r)\}$ es linealmente independiente.*
2. *f es sobreyectiva $\Leftrightarrow$ para cada sistema de generadores de V, $\{v_1, \ldots, v_s\}$, el conjunto $\{f(v_1), \ldots, f(v_s)\}$ es un sistema de generadores de V'.*

DEMOSTRACIÓN.

1. Supongamos que f es inyectiva y que el conjunto $\{v_1, \ldots, v_r\}$ es linealmente independiente, y veamos que también el conjunto $\{f(v_1), \ldots, f(v_r)\}$ es linealmente independiente. Consideremos una combinación lineal igualada a cero:

   $$a_1f(v_1) + \cdots + a_rf(v_r) = 0.$$

   Entonces $f(a_1v_1 + \cdots + a_rv_r) = 0$ y $a_1v_1 + \cdots + a_rv_r \in \mathrm{Ker}(f) = 0$. Por tanto $a_1v_1 + \cdots + a_rv_r = 0$, y como $\{v_1, \ldots, v_r\}$ es linealmente independiente se tiene $a_1 = \ldots = a_r = 0$. Con lo que $\{f(v_1), \ldots, f(v_r)\}$ es linealmente independiente.

Para la otra implicación, veamos que $\mathrm{Ker}(f) = 0$. Sea pues $v \in \mathrm{Ker}(f)$. Como el conjunto $\{f(v)\} = \{0\}$ es linealmente dependiente, por hipótesis, también el conjunto $\{v\}$ ha de ser linealmente dependiente y esto fuerza $v = 0$.

2. Si $\{v_1, \ldots, v_s\}$ es un sistema de generadores de V, entonces $\{f(v_1), \ldots, f(v_s)\}$ es un sistema de generadores de $\mathrm{Im}(f)$, y en consecuencia $\{f(v_1), \ldots, f(v_s)\}$ es sistema de generadores de V' si, y sólo si, $\mathrm{Im}(f) = V'$ o equivalentemente si, y sólo si, f es sobreyectiva.

□

TEOREMA 40. *Dada $f\colon V \to V'$ una aplicación lineal, siempre se tiene que $dim(\mathrm{Im}(f)) = dim(V) - dim(\mathrm{Ker}(f))$.*

DEMOSTRACIÓN. Consideremos $B_k = \{u_1, \ldots, u_r\}$ una base de $\mathrm{Ker}(f)$, y por el Teorema de Extensión de la Base, la ampliamos hasta una base de V, digamos $B = \{u_1, \ldots, u_r, v_{r+1}, \ldots, v_n\}$. Veamos que $\{f(v_{r+1}), \ldots, f(v_n)\}$ son una base de $\mathrm{Im}(f)$.

Probemos, primero, que es un sistema de generadores de $\mathrm{Im}(f)$. Para ello dado $v' \in \mathrm{Im}(f)$, sabemos que existe $v \in V$, tal que $f(v) = v'$. Dicho v, se puede escribir como $v = a_1u_1 + \cdots + a_ru_r + a_{r+1}v_{r+1} + \cdots + a_nv_n$ y, por ser f lineal, se tiene que:

$$v' = f(v) = a_1f(u_1) + \cdots + a_rf(u_r) + a_{r+1}f(v_{r+1}) + \cdots + a_nf(v_n) = a_{r+1}f(v_{r+1}) + \cdots + a_nf(v_n),$$

ya que $f(u_i) = 0$. Obteniendo que $\{f(v_{r+1}), \ldots, f(v_n)\}$ es un sistema de generadores de $\mathrm{Im}(f)$.

Veamos, ahora, que son linealmente independientes. Si $a_{r+1}f(v_{r+1}) + \cdots + a_nf(v_n) = 0$, se tiene que $f(a_{r+1}v_{r+1} + \cdots + a_nv_n) = 0$ y por tanto $a_{r+1}v_{r+1} + \cdots + a_nv_n \in \mathrm{Ker}(f)$. Pero como B_k es una base de $\mathrm{Ker}(f)$ tenemos que existen $b_1, \ldots, b_r$ tales que $a_{r+1}v_{r+1} + \cdots + a_nv_n = b_1u_1 + \cdots b_ru_r$ de donde:

$$b_1u_1 + \cdots b_ru_r - a_{r+1}v_{r+1} - \cdots - a_nv_n = 0.$$

Pero esto es una combinación lineal nula de elementos de la base B y, por tanto, todos los a_i y los b_j son cero. Probamos así, la independencia lineal de $\{f(v_{r+1}), \ldots, f(v_n)\}$. □

TEOREMA 41 (Fundamental de los Espacios Vectoriales). *Dos espacios vectoriales de la misma dimensión son isomorfos. Es decir, se puede establecer entre ellos una aplicación lineal y biyectiva.*

DEMOSTRACIÓN. La demostración se deduce fácilmente de la Proposición 39. □

COROLARIO 42. *Todo $\mathbb{K}$-espacio vectorial V de dimensión n, es isomorfo a $\mathbb{K}^n$.*

El resultado anterior se traduce básicamente en que, para trabajar en un espacio vectorial de dimensión finita, podemos fijar una base e identificar los vectores con sus coordenadas en dicha base. Y de esta forma todo el desarrollo hecho para $\mathbb{K}^n$ en la Proposición 24 es válido para cualquier espacio vectorial V de dimensión n. Basta considerar una base de V y trabajar con sus coordenadas.

4. Cocientes: una construcción típica de los espacios vectoriales

DEFINICIÓN 43. *Dados V un espacio vectorial y U un subespacio suyo, definimos el **espacio vectorial cociente** como $V/U = \{v+U\colon v \in V\}$. Donde $v+U = \{v' \in V\colon v-v' \in U\}$. Al conjunto $v+U$ se le llama clase de v.*

Iremos precisando esta definición, conforme vayamos avanzando a módulos y monoides.

DEFINICIÓN 44. *La suma y el producto por escalares en V/U están definidos por:*

$$(v+U)+(v'+U)=(v+v')+U$$
$$a\cdot(v+U)=(av)+U$$

PROPOSICIÓN 45. *$dim(V/U)=dim(V)-dim(U)$.*

DEMOSTRACIÓN. La demostración es análoga a la del Teorema 40.

Consideramos una base de U, $\{u_1,\dots,u_m\}$ y la ampliamos hasta una base de V, $B=\{u_1,\dots,u_m,v_{m+1},\dots,v_n\}$. Vamos a probar que los elementos de V/U, $\{v_{m+1}+U,\dots,v_n+U\}$ son una base del cociente.

En primer lugar, veamos que son sistema de generadores. Para ello, partimos de un elemento $v+U\in V/U$ y consideramos $v=a_1u_1+\cdots a_mu_m+a_{m+1}v_{m+1}+\cdots+a_nv_n$ puesto que B es base de V. Ahora si pasamos al cociente, tenemos que:

$$\begin{aligned} v+U &= (a_1u_1+\cdots+a_mu_m+a_{m+1}v_{m+1}+\cdots+a_nv_n)+U \\ &= (a_1u_1+\cdots+a_mu_m)+U+a_{m+1}(v_{m+1}+U)+\cdots+a_n(v_n+U) \\ &= a_{m+1}(v_{m+1}+U)+\cdots+a_n(v_n+U), \end{aligned}$$

ya $a_1u_1+\cdots+a_mu_m\in U$ y por tanto $a_1u_1+\cdots+a_mu_m\in 0+U$. Con lo que queda probado que es sistema de generadores.

Para ver que son linealmente independientes, hagamos: $a_{m+1}(v_{m+1}+U)+\cdots+a_n(v_n+U)=0+U$, o dicho de otra forma $(a_{m+1}v_{m+1}+\cdots+a_nv_n)+U=0+U$, que significa que $a_{m+1}v_{m+1}+\cdots+a_nv_n\in U$. Como tenemos una base de U, podemos escribir que $a_{m+1}v_{m+1}+\cdots+a_nv_n=b_1u_1+\cdots+b_mu_m$ para ciertos $b_1,\dots,b_m\in\mathbb{K}$ y, pasando todo a un lado, llegaríamos a que $b_1u_1+\cdots+b_mu_m-a_{m+1}v_{m+1}-\cdots-a_nv_n=0$. Pero esto es una combinación lineal de vectores de la base B igualada a cero, por tanto, todos los coeficientes son nulos. En particular $a_{m+1}=\cdots=a_n=0$. □

Módulos

Definición 46. *Dado A un anillo conmutativo unitario, definimos un A-**módulo** como un conjunto M junto con dos operaciones: una suma $(+)$ y un producto $(\cdot)$ de elementos de A por elementos de M, cumpliendo las siguientes propiedades :*

1. $m_1 + (m_2 + m_3) = (m_1 + m_2) + m_3$ *para todo* $m_1, m_2, m_3 \in M$,
2. $m_1 + m_2 = m_2 + m_1$ *para todo* $m_1, m_2 \in M$,
3. *Existe un elemento* $0 \in M$ *tal que* $m + 0 = 0 + m = m$ *para todo* $m \in M$,
4. *Para todo* $m \in M$ *existe un elemento* $-m \in M$ *tal que* $m + (-m) = (-m) + m = 0$,
5. $(a + b)m = am + bm$ *para todo* $a, b \in A$ *y todo* $m \in M$,
6. $a(m + m') = am + am'$ *para todo* $a \in A$ *y todo* $m, m' \in M$,
7. $a(bm) = (ab)m$ *para todo* $a, b \in A$ *y todo* $m \in M$,
8. $1m = m$ *para todo* $m \in M$.

El punto de la multiplicación será omitido si no hay confusión.
Cuando A es un cuerpo obtenemos la definición de espacio vectorial.

Ejemplo 47.

1. El propio A, es un A-módulo con su suma y su producto.
2. Todo grupo abeliano G se puede ver como $\mathbb{Z}$-módulo definiendo:
   - $n \cdot x = x + \cdots + x$ si $n > 0$ para todo $x \in G$,
   - $0 \cdot x = 0$ para todo $x \in G$ y,
   - $n \cdot x = (-x) + \cdots + (-x)$ si $n < 0$ para todo $x \in G$.
3. Todo $\mathbb{R}$-espacio vectorial o $\mathbb{Q}$-espacio vectorial se puede ver como $\mathbb{Z}$-módulo restringiendo el producto por escalares a los elementos de $\mathbb{Z}$.

5. Sistemas de generadores, submódulos y morfismos

Vamos a dar primeramente las definiciones que se pueden trasladar directamente desde los espacios vectoriales. Luego volveremos a estudiar estos conceptos con más detalle, en aquellos aspectos que no se puedan trasladar tan fácilmente.

Definición 48. *Sea M un A-módulo. Un subconjunto S, posiblemente infinito, de M se dice **sistema de generadores** de M si, para todo $m \in M$, existen $x_1, \ldots, x_n \in S$ y $r_1, \ldots, r_n \in A$ tales que $m = r_1x_1 + \cdots + r_nx_n$.*

Definición 49. *Si M tiene un sistema de generadores finito, se dirá que M es **finitamente generado**.*

Definición 50. *Un conjunto de generadores S de M se dice **conjunto minimal de generadores** si, ningún subconjunto propio de S genera a M. Si M es finitamente generado, entonces todo conjunto de generadores contiene un sistema minimal de generadores finito.*

Hay módulos que no contienen conjuntos de generadores minimales finitos.

Ejemplo 51. Un sistema minimal de generadores para el $\mathbb{Z}$-módulo $\mathbb{Q}$ sería, por ejemplo, el intervalo unidad semiabierto $[0, 1)$.

Definición 52. *Sea M un A-módulo, diremos que $N \subset M$, $N \neq \emptyset$; es un* ***submódulo*** *de M si, con las mismas operaciones de M, N es un A-módulo.*

Como en el caso de espacios vectoriales aparecen dos definiciones análogas:

Definición 53. *Sea M un A-módulo. Un subconjunto N de M, $N \neq \emptyset$; es un* ***submódulo*** *si, para cualesquiera $x, y \in N$ se tiene que $x + y \in N$ y para cualesquiera $r \in A$ y $x \in N$; se tiene que que $rx \in N$.*

Como siempre, las condiciones anteriormente exigidas para ser submódulo pueden resumirse en una sola:

Definición 54. *Sea M un A-módulo. Un subconjunto N de M, $N \neq \emptyset$; es un* ***submódulo*** *de M, si para todo $r, s \in A$ y todo $x, y \in N$ se cumple que $rx + sy \in N$.*

Definición 55. *Dado S subconjunto de M. Se define $G(S)$ el* ***submódulo de generado*** *por S, mediante:*

$$G(S) = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}, r_i \in A, x_i \in M \right\}.$$

Es claro que, S es un sistema de generadores de M si, y sólo si, $G(S) = M$.

Ejemplo 56. Los submódulos de un anillo A, visto como A-módulo, son los ideales de A. Recordemos que $I \subseteq A$ es ideal de A, si para cualesquiera $i \in I$ y $a \in A$, se tiene que $ia \in I$.

Ejemplo 57. Si U es un subespacio vectorial de $\mathbb{R}^n$, entonces $U \cap \mathbb{Z}^n$ es un submódulo de $\mathbb{Z}^n$. Ya que si $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in U$ tienen coordenadas enteras y $r, s \in \mathbb{Z}$ entonces $r(x_1, \ldots, x_n) + s(y_1, \ldots, y_n) \in U$ y con coordenadas enteras.

Definición 58. *Una aplicación $f\colon M \to M'$ entre dos A-módulos se dice* ***morfismo de módulos*** *si $f(rm + sn) = rf(m) + sf(n)$ para cualesquiera $r, s \in A$ y $m, n \in M$.*

Proposición 59. *El núcleo* $\mathrm{Ker}(f) = \{m \in M \mid f(m) = 0\}$ *es un submódulo de M y la imagen* $\mathrm{Im}(f) = \{f(m) \in M' \mid m \in M\}$ *es un subespacio de M'.*

La demostración es análoga a la hecha para espacios vectoriales: Lema 37.

Proposición 60. *Si M es un A-módulo finitamente generado y $\{m_1, \ldots, m_r\}$ un sistema minimal de generadores, entonces existe un epimorfismo $p\colon A^r \to M$ dado por $(a_1, \ldots, a_r) \mapsto a_1 m_1 + \cdots + a_r m_r$.*

Demostración. Basta calcular,

$$\begin{aligned} p(a(a_1, \ldots, a_r) + b(b_1, \ldots, b_r)) &= p(aa_1 + bb_1, \ldots, aa_n + bb_n) \\ &= (aa_1 + bb_1)m_1 + \cdots + (aa_n + bb_n)m_r \\ &= a(a_1 m_1 + \cdots + a_r m_r) + b(b_1 m_1 + \cdots + b_r m_r) \\ &= ap(a_1, \ldots, a_r) + bp(b_1, \ldots, b_r), \end{aligned}$$

comprobándose que es morfismo de módulos. La sobreyectividad es clara. □

La proposición y su demostración se puede trasladar también a los espacios vectoriales.

En el caso de espacios vectoriales, la inyectividad del morfismo anterior está relacionada con la independencia lineal del sistema de generadores. Esta independencia no siempre se podrá tener, incluso a veces ni se podrá definir, pero cuando sí sea posible, la inyectividad también se tendrá para morfismos de módulos.

6. Base y rango de un subgrupo de $\mathbb{Z}^n$

Vamos a centrarnos en el caso de $\mathbb{Z}$-módulos para encontrar las primeras diferencias entre los espacios vectoriales y los módulos. Entre otras cosas veremos que hay que imponer algunas condiciones al anillo para que podamos realizar las cuentas sin muchos problemas.

A continuación daremos dos definiciones análogas al caso de espacios vectoriales, de la noción de base para un subgrupo de $\mathbb{Z}^n$. La primera atendiendo a la idea de generación única, y la segunda introduciendo la idea de independencia lineal.

DEFINICIÓN 61. *Sea M un subgrupo de $\mathbb{Z}^n$, decimos que $\{m_1, \dots, m_r\} \subset M$ es una **base** de M, si todo elemento de M se puede escribir de forma única como $m = \sum_{i=1}^{r} z_i m_i$ con $z_1, \dots, z_r \in \mathbb{Z}$.*

DEFINICIÓN 62. *Tenemos que $\{m_1, \dots, m_r\}$ es una **base** de M si y solo si*

1. *Todo elemento $m \in M$ admite una expresión de la forma $m = \sum_{i=1}^{r} z_i m_i$ con $z_1, \dots, z_r \in \mathbb{Z}$.*
2. *Si $\sum_{i=1}^{r} z_i m_i = 0$ para ciertos $z_1, \dots, z_r \in \mathbb{Z}$, entonces $z_i = 0$ para todo i.*

Veamos que en $\mathbb{Z}$, donde $\{1\}$ es una base, tienen cabida multitud de subgrupos. Serían, por tanto, submódulos de $\mathbb{Z}$ y, veremos que todos tienen una base formada, también, por un solo elemento. Tenemos, pues, submódulos de la misma "dimensión"que el módulo que lo contiene de forma estricta, cosa que no sucedía en espacios vectoriales.

PROPOSICIÓN 63. *Sea $M \neq \{0\}$ un subgrupo de $\mathbb{Z}$. Entonces existe $g \in M$ tal que $\{g\}$ es una base de M.*

DEMOSTRACIÓN. Como $M \neq \{0\}$, claramente, el conjunto $\{m \in M \mid m > 0\}$ es no vacío y por tanto tiene un mínimo. Sea g ese mínimo. Probemos que $\{g\}$ es la base que andamos buscando. La inclusión $G(g) \subseteq M$ es trivial. Para la otra inclusión tomamos $m \in M$. Por el algoritmo de la división en $\mathbb{Z}$, existen $q, r \in \mathbb{Z}$ con $0 \leq r < g$ tales que $m = qg + r$. Como $0 \leq r = m - qg < g$ y g es el menor elemento de M mayor que cero, se tiene que $r = 0$ y por tanto $m = qg \in G(g)$. □

NOTA 64. Llamaremos $g\mathbb{Z}$ al submódulo de $\mathbb{Z}$ generado por g.

PROPOSICIÓN 65. *Existen cadenas "descendentes" infinitas de submódulos de $\mathbb{Z}$.*

DEMOSTRACIÓN. Basta considerar, por ejemplo:

$$\cdots \subset 2^n\mathbb{Z} \subset 2^{n-1}\mathbb{Z} \subset \cdots \subset 4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$$

□

Como vemos, es una gran diferencia entre los módulos y los espacios vectoriales, ya que estos, no tienen subespacios propios de la misma dimensión como puede verse en la Proposición 161.

PROPOSICIÓN 66. *Sea M un subgrupo de $\mathbb{Z}^n$. Entonces M tiene una base con, como mucho, n elementos.*

DEMOSTRACIÓN. Para cada $j \in \{1, \ldots, n\}$, definimos $M_j = M \cap G(\{e_1, \ldots, e_j\})$. Podemos observar que $M_n = M$. Veamos por inducción, que M_i tiene una base con, como mucho, i elementos. Si $M_i = \{0\}$, entonces una base para M_i es el conjunto vacío.

Si $M_1 \neq \{0\}$, consideramos $H = \{k \in \mathbb{Z} \mid ke_i \in M_1\}$. Claramente, H es un subgrupo de $\mathbb{Z}$ y por la Proposición 63, es igual a $G(\{z\})$ para algún $z \in \mathbb{Z} \setminus \{0\}$. Es sencillo ver que $M_1 = G(\{ze_1\})$ y como consecuencia $\{ze_1\}$ es una base de M_1. Esto nos muestra que se cumple para $i = 1$.

Supongamos que M_k tiene una base $\{m_1, \ldots, m_r\}$ con $r \leq k$. Nótese que si $M_{k+1} = \{0\}$, entonces también lo es M_k, y por tanto $r = 0$, y una base de M_{k+1} sería el conjunto vacío. Asumimos pues, que $M_{k+1} \neq \{0\}$ y definimos

$$H = \{z \in \mathbb{Z} \mid y + ze_{k+1} \in M \text{ para algún } y \in G(\{e_1, \ldots, e_k\})\}.$$

De nuevo, H es un subgrupo de $\mathbb{Z}$ y por tanto $H = G(\{z\})$ para algún $z \in \mathbb{Z}$. Si $z = 0$, entonces $M_{k+1} = M_k$, con lo que M_{k+1} tiene una base con r elementos y $r \leq k < k + 1$. Si $z \neq 0$, entonces existe un elemento $y \in G(\{e_1, \ldots, e_k\})$ tal que $w = y + ze_{k+1} \in M_{k+1}$. Veamos que $\{m_1, \ldots, m_r, w\}$ es una base para M_{k+1}.

- Sea $m \in M_{k+1}$. Por tanto, $m \in G(\{e_1, \ldots, e_{k+1}\})$ lo cual significa que $m = \sum_{i=1}^{k+1} z_i e_i$ para ciertos $z_1, \ldots, z_{k+1} \in \mathbb{Z}$. Entonces, $z_{k+1} \in H$ lo que implica que $z_{k+1} = zt$ para algún $t \in \mathbb{Z}$. Así, $m = \sum_{i=1}^{k} z_i e_i - ty + tw$ y en consecuencia

  $$m - tw \in M \cap G(\{e_1, \ldots, e_k\}) = M_k.$$

  Tenemos que $\{m_1, \ldots, m_r\}$ es una base de M_k, entonces existen $t_1, \ldots, t_r \in \mathbb{Z}$ tal que $m - tw = \sum_{i=1}^{r} t_i m_i$, lo cual nos lleva a que $m = \sum_{i=1}^{r} t_i m_i + tw$. Y así, probamos que es sistema de generadores.
- Supongamos ahora que existen $s_1, \ldots, s_{r+1} \in \mathbb{Z}$ tal que $\sum_{i=1}^{r} s_i m_i + s_{r+1} w = 0$. Si $s_{r+1} = 0$, como $G(\{e_1, \ldots, e_k\})$ es base se tendría que $s_i = 0$ para todo $i = 1, \ldots, r+1$. Mientras que si $s_{r+1} \neq 0$, tendríamos que $0 \neq s_{r+1} w = -\sum_{i=1}^{r} s_i m_i \in G(\{e_1, \ldots, e_k\})$ y $w = y + ze_{k+1}$. Con lo que $s_{r+1} z e_{k+1} = -s_{r+1} y - \sum_{i=1}^{r} s_i m_i \in G(\{e_1, \ldots, e_k\})$ que sería una contradicción.

Por lo tanto, llegamos a que $\{m_1, \ldots, m_r, w\}$ es una base de M_{k+1} con $r + 1$ elementos y $r + 1 \leq k + 1$. □

TEOREMA 67. *Sea M un subgrupo de $\mathbb{Z}^n$. Entonces toda base de M tiene el mismo cardinal.*

DEMOSTRACIÓN. Sean $B = \{m_i \mid i \in I\}$ y $B' = \{n_i \mid i \in I'\}$ son dos bases diferentes de M. Los elementos de B son linealmente independientes como vectores de $\mathbb{Q}^n$, sabemos que puede haber, como mucho, n elementos en B. Lo mismo ocurre con B'. Obsérvese también que B es una base del espacio vectorial $V = L_{\mathbb{Q}}(B)$ y $B' \subset M = G(\{m_1, \ldots, m_r\}) \subset L_{\mathbb{Q}}(B)$ es un conjunto linealmente independiente de vectores de V el cardinal de B' debe ser menor o igual al cardinal de B. Análogamente, se puede hacer la otra desigualdad. □

También es fácil la consecución del siguiente resultado:

PROPOSICIÓN 68. *Sea M un subgrupo de $\mathbb{Z}^n$ de rango k. Entonces M es isomorfo a $\mathbb{Z}^k$.*

DEMOSTRACIÓN. Sea $B = \{m_1, \ldots, m_k\}$ una base de M. Todo elemento en M tiene coordenadas únicas con respecto a B, lo que implica que la aplicación

$$p\colon \mathbb{Z}^k \to M, \text{ dada por } (z_1, \ldots, z_k) \mapsto \sum_{i=1}^{k} z_i m_i$$

es un isomorfismo de grupos. Este morfismo p es el definido en la Proposición 60. □

Este resultado nos muestra lo anunciado anteriormente: cuando se puede hablar de independencia lineal de un sistema de generadores, podemos considerar una base en M, y con ella, la aplicación p es un isomorfismo. Esta aplicación tendrá un papel fundamental en el caso de monoides, y será muy útil para una cierta clasificación de los mismos.

Vamos ahora a trasladar algunas proposiciones que ya se daban en espacios vectoriales, para señalar, la dificultad que se tiene cuando el cuerpo pasa a ser un anillo, aunque se tengan bases en los A-módulos.

PROPOSICIÓN 69. *Sea M un subgrupo de $\mathbb{Z}^n$. Si $\{x_1, \ldots, x_n\}$ es una base de M y $m_1 = x_1 + a_2x_2 + \cdots + a_nx_n$ entonces $\{m_1, x_2, \ldots, x_n\}$ es base de M.*

DEMOSTRACIÓN. Veamos que es sistema de generadores. Sea $m = r_1x_1 + r_2x_2 + \cdots + r_nx_n$ entonces, despejando x_1 en la igualdad del enunciado y sustituyendo en la anterior, tenemos: $m = r_1(m_1 - a_2x_2 - \cdots - a_nx_n) + r_2x_2 + \cdots + r_nx_n = r_1m_1 + (r_2 - r_1a_2)x_2 + \cdots + (r_n - r_1a_n)x_n$. Por tanto es sistema de generadores.

Ahora, si tomamos $r_1m_1 + r_2x_2 + \cdots + r_nx_n = 0$ tendríamos: $r_1(x_1 + a_2x_2 + \cdots + a_nx_n) + r_2x_2 + \cdots + r_nx_n = 0$, de donde $r_1x_1 + (r_1a_2 + r_2)x_2 + \cdots + (r_1a_n + r_n)x_n = 0$. Ahora como $\{x_1, \ldots, x_n\}$ son una base, tenemos que $r_1 = 0$ y $r_1a_i + r_i = 0$, deduciendo fácilmente que todos los $r_i = 0$. □

De forma análoga también podemos probar la siguiente proposición.

COROLARIO 70. *Sea $\{x_1, \ldots, x_n\}$, un sistema de generadores de M un A-módulo. Si $x_1 = a_2x_2 + \cdots + a_nx_n$ entonces $\{x_2, \ldots, x_n\}$ también es un sistema de generadores.*

Nos hemos centrado en el caso particular en el que el coeficiente de x_1 es igual a uno, para señalar el problema de pasar esta proposición al ambiente de módulos. Más adelante veremos que la proposición también es cierta aunque dicho coeficiente sea distinto de uno.

7. Cocientes, módulos de torsión y módulos libres

En este apartado, nos vamos a acercar a los $g\mathbb{Z}$, subgrupos de $\mathbb{Z}$, con la misma "dimensión" que $\mathbb{Z}$. Estos subgrupos, mediante la herramienta del cociente, nos descubrirán nuevos grupos y módulos que no aparecen en el caso de espacios vectoriales. Se puede decir, que son objetos típicos del ambiente de módulos. También se tendrán en monoides, aunque su sitio natural, como veremos, son los módulos.

Empecemos, pues, por trasladar, desde los espacios vectoriales, la idea de cociente.

DEFINICIÓN 71. *Sea M un A-módulo y N un submódulo de M. Definimos la clase de $m \in M$ como: $m + N = \{m' \in M \mid m - m' \in N\}$. Y denotamos M/N el conjunto de*

dichas clases. Existe, entonces, una estructura de ***módulo en cociente*** *en M/N dada por las operaciones: $(x+N)+(y+N)=(x+y)+N$ y $r(x+N)=rx+N$.*

TEOREMA 72 (Primer Teorema de Isomorfía). *Sea $f\colon M\to N$ un morfismo de módulos entonces $M/\mathrm{Ker}(f)\simeq \mathrm{Im}(f)$.*

DEMOSTRACIÓN. Definimos $b\colon M/\mathrm{Ker}(f)\to \mathrm{Im}(f)$ mediante: $m+\mathrm{Ker}(f)\mapsto f(m)$. Veamos que esta aplicación está bien definida, i.e. no depende del representante, y además es un morfismo de módulos biyectivo.

Para ver que está bien definida, consideramos $m'\in M$ con $m'+\mathrm{Ker}(f)=m+\mathrm{Ker}(f)$, esto quiere decir que $m'-m\in\mathrm{Ker}(f)$, o equivalentemente que $f(m'-m)=0$ y por tanto $f(m)=f(m')$ y la aplicación está bien definida.

Para ver que es un morfismo de módulos basta hacer $b(r(m+\mathrm{Ker}f)+s(m'+\mathrm{Ker}f))=b(rm+sm'+\mathrm{Ker}f)=f(rm+sm')=rf(m)+sf(m')=rb(m+\mathrm{Ker}f)+sb(m'+\mathrm{Ker}f)$.

Para ver que es inyectivo, sean $b(m+\mathrm{Ker}f)=b(m'+\mathrm{Ker}f)$, se tiene que $f(m)=f(m')$, o equivalentemente $f(m-m')=0$, es decir $m-m'\in\mathrm{Ker}f$, y esto no es más que decir que $m+\mathrm{Ker}f=m'+\mathrm{Ker}f$.

Por último veamos que es sobreyectivo. Pero esto es sencillo, ya que cualquier elemento de $\mathrm{Im}(f)$ es de la forma $f(m)$ y por tanto dicho m cumple que $b(m+\mathrm{Ker}f)=f(m)$, obteniendo así que el morfismo b es sobreyectivo. □

NOTA 73. En el ambiente de espacios vectoriales hay una demostración más sencilla usando la idea de dimensión mediante la Proposición 40 y el Teorema Fundamental de los Espacios Vectoriales 41.

EJEMPLO 74. Sea $2\mathbb{Z}$ submódulo de $\mathbb{Z}$ formado por todos los números pares. Al hacer el cociente $\mathbb{Z}/2\mathbb{Z}$, obtenemos $\mathbb{Z}_2=\{0+2\mathbb{Z},1+2\mathbb{Z}\}$, es decir el cociente tiene dos elementos. Encontramos un $\mathbb{Z}$-módulo finito, que obviamente no es submódulo de $\mathbb{Z}$, pues sus elementos son clases de equivalencia y no son elementos de $\mathbb{Z}$, ni se puede establecer un morfismo de módulos desde $\mathbb{Z}_2$ a $\mathbb{Z}$. Es claro que $\{1+2\mathbb{Z}\}$ es un sistema de generadores de $\mathbb{Z}_2$, pues $1\cdot 1+2\mathbb{Z}=1+2\mathbb{Z}$ y $0\cdot 1+1\mathbb{Z}=0+2\mathbb{Z}$, pero sin embargo no cumple la condición de independencia lineal, ya que $2\cdot 1+2\mathbb{Z}=0+2\mathbb{Z}$ y $2\neq 0\in\mathbb{Z}$, y tampoco la idea de unicidad puesto que $3\cdot 1+2\mathbb{Z}=1\cdot 1+2\mathbb{Z}$. Por tanto, **existen $\mathbb{Z}$-módulos que no tienen bases**.

Vamos a determinar cuales son estos $\mathbb{Z}$-módulos, pero dando la definición de forma más general:

DEFINICIÓN 75. *Un A-módulo se dice de* ***torsión*** *si para cualquier $m\in M$ existe $a\in A$, $a\neq 0$, tal que $a\cdot m=0$.*

DEFINICIÓN 76. *Diremos también que un A-módulo M es* ***libre de torsión*** *si no existe ningún elemento $m\neq 0$ tal que $a\cdot m=0$ con $a\in A$, $a\neq 0$.*

DEFINICIÓN 77. *Sea M un A-módulo, se define:*

$$t(M)=\{m\in M\mid \exists r\in A\setminus\{0\} \text{ con } rm=0\},$$

como el conjunto de los elementos de torsión. Además, es fácil ver que $t(M)$ es un submódulo de M, al que llamaremos ***submódulo torsión de*** *M.*

NOTA 78.

- Si $M = t(M)$ se dice que M es un A-módulo torsión.
- Si $t(M) = 0$ tenemos que M es un A-módulo libre de torsión.

Es claro que para el submódulo $t(M)$, no es posible encontrar una base ya que si $\{m_1, \ldots, m_r\}$ es un sistema de generadores, existen $a_1, \ldots, a_r \in A \setminus \{0\}$ tales que $a_1 m_1 = 0, \ldots, a_r m_r = 0$, y por tanto, $a_1 m_1 + \cdots + a_m r_m = 0$.

LEMA 79. *El módulo cociente $M/t(M)$ es libre de torsión.*

DEMOSTRACIÓN. Si $x + t(M)$ es un elemento de torsión en $M/t(M)$, entonces existe $\lambda \neq 0$ tal que $\lambda(x + t(M)) = (0 + t(M))$ con lo que $\lambda x \in t(M)$, por tanto debe existir $\mu \neq 0$ con $\mu(\lambda x) = 0$ pero entonces $x \in t(M)$, ya que $\mu\lambda \neq 0$, de donde se deduce que $x + t(M) = 0 + t(M)$. Probando así que el único elemento de torsión en $M/t(M)$ es el $0 + t(M)$. □

DEFINICIÓN 80. *Diremos que M es un A-módulo **libre** si es posible encontrar una base X, para M. También se dirá que M es libre sobre X.*

PROPOSICIÓN 81. *Sea M un $\mathbb{Z}$-módulo libre de torsión y sea $a_1 m_1 + \cdots + a_r m_r = 0$ con $a_i \in \mathbb{Z}$ y $m_i \in M$, entonces existen $m'_1, \ldots, m'_{r-1}$ tales que: $G(m_1, \ldots, m_r) = G(m'_1, \ldots, m'_{r-1})$.*

DEMOSTRACIÓN. Si algún $a_i = \pm 1$, despejamos el correspondiente m_i, y por el Corolario 70, tenemos que todos los demás son un sistema de generadores de M.

Supongamos, pues, que todos los $a_i \neq \pm 1$. Si $gcd(a_1, \ldots, a_r) = d$ entonces podemos escribir $d(a'_1 m_1 + \cdots + a'_r m_r) = 0$ y como es libre de torsión se tiene que $a'_1 m_1 + \cdots + a'_r m_r = 0$. Así pues, podemos supone que todos los a_i son primos relativos.

Supongamos ahora que existe $\alpha \in \mathbb{Z}$ tal que $a_1 + \alpha a_2 = \pm 1$. En este caso podemos escribir: $(a_1 + \alpha a_2)m_1 + a_2(m_2 - \alpha m_1) + a_3 m_3 + \cdots + a_r m_r = 0$ donde $\{m_1, m_2 - \alpha m_1, m_3, \ldots, m_r\}$ sigue siendo sistema de generadores, pues cualquier $m = b_1 m_1 + b_2 m_2 + \cdots + b_r m_r$ también se puede escribir como $m = (b_1 + \alpha b_2)m_1 + b_2(m_2 - \alpha m_1) + \cdots + b_r m_r$. Y como $a_1 + \alpha a_2 = \pm 1$, se puede concluir como antes, usando el Corolario 70.

Por último, como $gcd(a_1, \ldots, a_m) = 1$, la cuenta anterior se podrá hacer tantas veces como sea necesario para obtener un m'_i que vaya multiplicado por ± 1, y entonces, lo despejaríamos usando de nuevo el Corolario 70. □

PROPOSICIÓN 82. *Un $\mathbb{Z}$-módulo M, finitamente generado, es libre si y solo si es libre de torsión.*

DEMOSTRACIÓN. Si M es libre, podemos considerar $B = \{m_1, \ldots, m_r\}$ una base. Si $0 \neq m \in M$ es de torsión, se tendría que $xm = 0$ para algún $x \neq 0$. Por otra parte, $m = a_1 m_1 + \cdots + a_r m_r$. Entonces $0 = xm = xa_1 m_1 + \cdots + xa_r m_r$, y como B es base, podemos deducir que $xa_i = 0$ para todo $i = 1, \ldots, r$. Ahora bien, como $x \neq 0$, se tendría que todos los $a_i = 0$ y por tanto $m = 0$, lo que sería una contradicción.

Para la otra implicación consideramos que $\{m_1, \ldots, m_r\}$ es un sistema de generadores de elementos libres de torsión y usaremos la inducción sobre r. Si $r = 1$ el resultado es inmediato.

Mientras que, en general, si tenemos que $a_1 m_1 + \cdots + a_r m_r = 0$; por la Proposición 81, obtenemos un sistema de generadores con $r - 1$ elementos libres de torsión y por inducción tendríamos el resultado. □

DEFINICIÓN 83. *Dados M un A-módulo y N_1, N_2 dos submódulos suyos. se dice que M es* ***suma directa*** *de N_1 y N_2, y se denota $M = N_1 \oplus N_2$, si para cualquier $m \in M$, existen $n_1 \in N_1$ y $n_2 \in N_2$ con $m = n_1 + n_2$ y además $N_1 \cap N_2 = \{0\}$.*

TEOREMA 84. *Sea M un módulo finitamente generado entonces existe un submódulo $f(M)$ de M que es isomorfo a $M/t(M)$ tal que $M = f(M) \oplus t(M)$.*

DEMOSTRACIÓN. En primer lugar por los resultados anteriores tenemos que $M/t(M)$ es libre, y por tanto podemos considerar $\{x_1 + t(M), \ldots, x_r + t(M)\}$ una base del mismo. Es fácil ver que $\{x_1, \ldots, x_r\}$ son linealmente independientes en M, ya que lo son en $M/t(M)$. Denotamos $f(M) = G(\{x_1, \ldots, x_r\})$, que es un submódulo libre de M por ser libre de torsión. Es fácil ver que $f(M) \cap t(M) = \{0\}$, ya que si $x \in t(M)$, existe $\lambda \neq 0$ con $\lambda x = 0$; pero si esto ocurre en $f(M)$ es porque $x = 0$.

Por último si $m \in M$, consideramos $f\colon M \to M/t(M)$ la proyección canónica dada por $m \mapsto m + t(M)$, y consideramos $m + t(M) = a_1(x_1 + t(M)) + \cdots + a_r(x_r + t(M)) = (a_1x_1 + \cdots + a_rx_r) + t(M)$ ya que $\{x_1 + t(M), \ldots x_r + t(M)\}$ es una base de $M/t(M)$. Pero entonces tenemos que $m - (a_1x_1 + \cdots + a_rx_r) \in t(M)$. Llamando $t(m)$ a esta diferencia que está en $t(M)$, tenemos que

$$m = (a_1x_1 + \cdots + a_rx_r) + t(m) \in f(M) \oplus t(M)$$

□

Vamos a centrarnos en los $\mathbb{Z}$-módulos libres, que son, básicamente, los subgrupos de $\mathbb{Z}^n$ y seguir trasladando proposiciones del ambiente de los espacios vectoriales.

TEOREMA 85. *Sea M un $\mathbb{Z}$-módulo libre, sea $L = \{x_1, \ldots, x_s\}$ un conjunto linealmente independiente y sea $S = \{m_1, \ldots, m_r\}$ un sistema de generadores. Entonces $s \leq r$.*

DEMOSTRACIÓN. La idea de la demostración es análoga al caso de espacios vectoriales (Teorema 10), ir substituyendo los m_i por los x_i, y luego probar que los elementos de L no se pueden acabar antes que los S.

Vamos a utilizar las ideas de la demostración de la Proposición 81. Como S es un sistema de generadores tenemos que $x_1 = a_1m_1 + \cdots + a_rm_r$. Consideramos $\{m_1, x_1, m_2, \ldots m_r\}$ que también es un sistema de generadores de S. Si algún $a_i = \pm 1$, supongamos $i = 1$, podríamos escribir $m_1 = x_1 - a_2m_2 \cdots - a_rm_r$ y por el Corolario 70 tendríamos el resultado.

Si ningún $a_i = \pm 1$, y $d = gcd(a_1, \ldots, a_r)$ y consideramos $x_1' = x_1/d = a_1'm_1 + \cdots + a_r'm_r \in G(\{m_1, \ldots, m_r\}) = M$ donde $da_i' = a_i$. Es fácil ver que $\{x_1', x_2, \ldots, x_s\}$ sigue siendo linealmente independiente.

Por tanto, podemos suponer que $x_1 = a_1m_1 + a_2m_2 + \cdots + a_rm_r$ con todos los $a_i \neq \pm 1$ y primos relativos. Usamos la idea de escribir $a_1' = a_1 + \alpha a_2$ que se describe en la demostración de la Proposición 81, para buscar un elemento m_i' que esté multiplicado por ± 1, despejarlo y sustituirlo por x_1, y así obtener que $\{x_1, m_2 \ldots, m_r\}$ es un sistema de generadores de M.

A continuación procederíamos con x_2. Tendríamos que $x_2 = a_1x_1 + a_2m_2 + \cdots + a_rm_r$, es claro que si $a_2 = a_3 = \cdots = a_r = 0$ entonces $x_2 = a_1x_1$ con lo que $x_2 - a_1x_1 = 0$ pero esto es imposible. Ahora, si alguno de los $a_i = \pm 1$ con $i \geq 2$, se despejaría dicho m_i y se aplica, de nuevo, el Corolario 70 quedaría sustituido por x_2.

Si ningún $a_i = \pm 1$ y $d = gcd(a_2, \ldots, a_r)$, entonces haciendo $x_2' = (x_2 - a_1x_1)/d$, se tendría que $\{x_1, x_2', x_3, \ldots, x_s\}$ son linealmente independientes. Ya que, si $b_1x_1 + b_2x_2' + b_3x_3 + \cdots +$

$b_s x_s = 0$, entonces $b_1 x_1 + b_2(x_2 - a_1 x_1)/d + b_3 x_3 + \cdots + b_s x_s = 0 \Rightarrow (db_1 - b_2 a_1)x_1 + b_2 x_2 + db_3 x_3 + \cdots + db_s x_s = 0$. De donde, $db_1 - b_2 a_1 = 0$, $b_2 = 0$ y $db_i = 0$, y se concluye fácilmente que el conjunto de partida es linealmente independiente.

Así pues, podemos suponer, de nuevo, que $gcd(a_2, a_3 \ldots, a_r) = 1$. Y volviendo a usar el truco de escribir $a_2' = a_2 + \alpha a_3$, tendríamos el camino para poder intercambiar x_2 por un cierto m_i'.

Finalmente, argumentaríamos, como en el caso de espacios vectoriales (ver Teorema 10), que si $r < s$, una vez cambiados los r primeros elementos del sistema linealmente independiente $\{x_1, \ldots, x_r\}$ sería un sistema de generadores, pero en ese caso $x_{r+1} = c_1 x_1 + \cdots + c_r x_r$ obteniendo que no serían entonces linealmente independientes. □

Como se está viendo en las demostraciones, al no poder multiplicar por el inverso como en espacios vectoriales, se recurre a la división entera, es decir, si $a, b \in \mathbb{Z}$ con $|a| \geq |b|$ entonces existen $q, r \in \mathbb{Z}$ con $|r| < |a|$ tales que $a = qb + r$. Dichos q y r son el cociente y el resto de dividir a entre b. Vamos a explotar de un modo importante esta herramienta.

Por tanto, nos vamos a centrar en los anillos conmutativos en los que vamos a poder usar la división entera, dentro de los cuales está $\mathbb{Z}$. Estos anillos son los llamados **dominios euclídeos**. La definición la daremos un poco más adelante.

Antes de pasar al epígrafe siguiente donde aplicaremos la división entera para encontrar bases y ecuaciones cartesianas para $\mathbb{Z}$-módulos. Daremos un resultado interesante a la hora de decidir si una base con n elementos es base de $\mathbb{Z}^n$ o sólo de un subgrupo suyo de rango n.

PROPOSICIÓN 86. *Un conjunto $S = \{(a_{11}, \ldots, a_{1n}), \ldots, (a_{n1}, \ldots, a_{nn})\}$ linealmente independiente de elementos de $\mathbb{Z}^n$, son una base de $\mathbb{Z}^n$, si y solo si el determinante de*

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

es igual ± 1.

DEMOSTRACIÓN. Si $det(A) = \pm 1$ sabemos que A es invertible y que su inversa se calcula como $A^{-1} = (AdjA)^t/det(A)$ (la traspuesta de la adjunta partido por el determinante). Tanto las operaciones de adjunción como transposición de matrices de elementos enteros, dan salidas enteras y si el determinante es ± 1, tenemos que la inversa de A tiene entradas enteras. Por tanto, si $x_{i1}, \ldots, x_{in}$ son las entradas enteras de la fila i-ésima de A^{-1}, como $A^{-1}A = I$, se tiene que $x_{i1}(a_{11}, \ldots, a_{1n}) + \cdots + x_{in}(a_{n1}, \ldots, a_{nn}) = e_i$. Demostrando que todos los e_i están generados por los elementos de S.

Para el recíproco, consideramos que S es una base y por tanto cada e_i se escribirá como $e_i = x_{i1}(a_{11}, \ldots, a_{1n}) + \cdots + x_{in}(a_{n1}, \ldots, a_{nn})$ con los $x_{ij} \in \mathbb{Z}$. Dicho de otra forma, la matriz A tiene como inversa la formada por los x_{ij} correspondientes. Ambos determinantes, $det(A), \det(A^{-1})$ son enteros y su producto es igual a 1. Por tanto la única posibilidad es que $\det(A) = \det(A^{-1}) = \pm 1$. □

8. Sistemas de ecuaciones y Matrices

El objetivo de este epígrafe es probar la siguiente proposición y extraer consecuencias de ella.

PROPOSICIÓN 87. *Si M es el subgrupo de $\mathbb{Z}^n$ formado por las soluciones de un sistema de ecuaciones homogéneas*

$$\left.\begin{array}{rcl} a_{11}x_1 + \cdots + a_{1n}x_n & = & 0 \\ \cdots & \cdots & \cdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n & = & 0 \end{array}\right\}$$

con rango $n - r$, entonces existe una base de M con r elementos.

El camino a seguir, a la hora de calcular las ecuaciones que definen un $\mathbb{Z}$-módulo, será el mismo que en el Ejemplo 29. Usar trasformaciones elementales que habrá que adecuar al ambiente de $\mathbb{Z}$-módulos, aunque trabajaremos en otros anillos un poco más generales.

Es el momento de definir esas condiciones que vamos a exigir al anillo para que podamos hacer las cuentas de un modo "agradable".

DEFINICIÓN 88. *Un **dominio de integridad** A, es un anillo donde para cualesquiera $a, b \in A$ tal que $a \cdot b = 0$ se tiene que $a = 0$ o $b = 0$.*

EJEMPLO 89. $\mathbb{Z}$ es un dominio de integridad, cualquier cuerpo es un dominio de integridad. $\mathbb{Z}_8$ no es dominio de integridad ya que $2 \cdot [4]_8 = 0$.

DEFINICIÓN 90. *Un elemento $u \in A$ se denomina **unidad** si existe u' tal que $uu' = 1$.*

EJEMPLO 91. Elemento $[5]_8$ de $\mathbb{Z}_8$ es una unidad ya que $5 \cdot [5]_8 = 1 \in \mathbb{Z}_8$.

Y también vamos a exigirle la posibilidad de hacer la división entera como apuntamos más arriba.

DEFINICIÓN 92. *Un **dominio euclídeo** R es un dominio de integridad junto con una aplicación $\phi\colon R \to \mathbb{N}$, llamada norma euclídea, cumpliendo:*

1. *$\phi(0) = 0$.*
2. *Si a, b son elementos de R no nulos, entonces $\phi(a) \leq \phi(ab)$.*
3. *Si a, b con $a \neq 0$ entonces existen q y r tales que $b = qa + r$ con $r = 0$ o $\phi(r) < \phi(a)$*

Veamos que para estos anillos podemos trascribir sin mucho problema los cálculos que hemos hecho antes en $\mathbb{Z}$-módulos.

De las tres trasformaciones elementales que se hacían a una matriz para obtener otra equivalente, solo hay que preocuparse de la segunda de ellas. Ahora, no podemos multiplicar las filas o columnas por elementos distintos de 1 o -1, si queremos asegurar entradas enteras y/o no variar el submódulo que generan. Sin embargo, la primera y tercera no sufren restricciones. Este inconveniente nos impide obtener el pivote igual a 1 dividiendo toda la fila por el valor de ese pivote.

NOTA 93. Más precisamente, para poder hacer la segunda trasformación el elemento k por el que se multiplique la fila ha de ser una unidad.

Lo recogemos en el siguiente teorema:

PROPOSICIÓN 94. *Sea M un R-módulo libre con R dominio euclídeo, generado por un conjunto. El sistema de generadores (base) no se modifica si aplicamos a sus elementos una o varias de las transformaciones siguientes:*

1. *Cambiar el orden inicial de los generadores.*
2. *Multiplicar un generador por una unidad.*
3. *Sumarle a un elemento un múltiplo de otro.*

La demostración es seguir la que se hace en espacios vectoriales.

Ahora, para determinar bases y sistemas de ecuaciones lineales que definan a un R-módulo libre, la idea será, a partir de una base, obtener matrices similares a las P y Q del caso de espacios vectoriales. Recuérdese que estas matrices eran el producto de matrices elementales que recogían los cambios que se realizaban sobre la matriz A. De las trasformaciones de espacios vectoriales, valen todas salvo multiplicar o dividir por elementos distintos de ± 1. Y, como hemos hecho ya en varias demostraciones, la herramienta que vamos a usar es la división entera.

Vamos a ver que toda matriz A, de tamaño $s \times t$, con entradas enteras, se puede escribir como $PAQ^{-1} = D_r$ donde P y Q son matrices invertibles y la matriz D_r es diagonal de rango r. Pero no siempre tendremos unos en la diagonal principal. Lo que se conseguirá, en este caso, es que cada d_{ii} divida a d_{jj} con $1 \leq i < j \leq r$.

La matriz D_r se obtiene con el siguiente algoritmo.

ALGORITMO 95. *de reducción de matrices sobre un dominio euclídeo.*

El primer paso del algoritmo será encontrar d_{11} y luego se repetirán los pasos para las siguientes submatrices. La idea es dada $M \in M_{s\times t}(R)$ con R dominio euclídeo, encontrar una matriz C de la siguiente forma:

$$C = \left(\begin{array}{c|ccc} d_1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & C^* & \\ 0 & & & \end{array}\right)$$

donde $d_1 \neq 0$ y divide a cada entrada de C^*.

Para encontrar dicho d_1 haremos lo siguiente:

1. *Se busca un elemento $a_{ij} \neq 0$ de A tal que $\phi(a_{ij}) = \min\{\phi(a_{hk}) \mid h, k = 1, \dots, n\}$ e intercambiando las filas y columnas correspondientes, se lleva a la primera posición. Si existe más de uno, se elige uno cualquiera. Encontramos así $a_{11} \neq 0$, con $\phi(a_{11})$ menor o igual que cualquier otro de la matriz.*
2. *Si a_{11} divide a todos los elementos de la primera fila, multiplicando por el elemento adecuado podremos ir haciendo cero todos los elementos de la primera fila y entonces vamos al paso 4.*
3. *Si $\exists a_{1j}$ tal que a_{11} no divide a a_{1j}. Entonces haciendo $a_{1j} = a_{11}q + r$ con $\phi(r) < \phi(a_{11})$ podemos hacer el siguiente cambio: $F_j - qF_1$ y $C_1 \leftrightarrow C_j$, encontrando un elemento r con $\phi(r)$ menor que todos los A. Una vez llevado al principio, volvemos al paso 2. Al obtenerse cada vez un elemento con norma menor estricta, y ser este conjunto de enteros positivos, acotado inferiormente, el algoritmo acaba, obteniendo un a_{11} en las condiciones para aplicar el paso 2.*
4. *Si a_{11} divide a todos los elementos de la primera columna, multiplicando por el elemento adecuado podremos ir haciendo cero todos los elementos de la primera columna y entonces vamos al paso 6.*

5. *Si $\exists a_{j1}$ tal que a_{11} no divide a a_{j1}. Se actúa como en el Paso 3, pero esta vez por columnas. Una vez que a_{11} divide a los elementos de la primera columna, aplicamos el paso 4.*

   Llegamos a

$$D = \left(\begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & D^* & \\ 0 & & & \end{array}\right)$$

6. *Si a_{11} divide a cualquier entrada de D^*, repetimos el algoritmo con D^*.*
7. *En otro caso, $\exists d_{ij}$ con a_{11} no dividiendo a d_{ij}. Hacemos $F_1 + F_i$ y vamos en el Paso 3. Como se argumentó antes, se van obteniendo elementos con norma euclídea cada vez más pequeña, lo que nos asegura que el algoritmo acaba en un número finito de pasos.*

EJEMPLO 96. Forma reducida de $A = \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix} \in M_3(\mathbb{Z})$.

$$\left(\begin{array}{c|c} A & Id \\ \hline Id & \end{array}\right) = \left(\begin{array}{ccc|ccc} -4 & -6 & 7 & 1 & 0 & 0 \\ 2 & 2 & 4 & 0 & 1 & 0 \\ 6 & 6 & 15 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \xrightarrow{F_1 \leftrightarrow F_2} \left(\begin{array}{ccc|ccc} 2 & 2 & 4 & 0 & 1 & 0 \\ -4 & -6 & 7 & 1 & 0 & 0 \\ 6 & 6 & 15 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \xrightarrow[F_3-3F_1]{F_2+2F_1}$$

$$\left(\begin{array}{ccc|ccc} 2 & 2 & 4 & 0 & 1 & 0 \\ 0 & -2 & 15 & 1 & 2 & 0 \\ 0 & 0 & 3 & 0 & -3 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \xrightarrow[C_3-2C_1]{C_2-C_1} \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & -2 & 15 & 1 & 2 & 0 \\ 0 & 0 & 3 & 0 & -3 & 1 \\ \hline 1 & -1 & -2 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right)$$

Ahora, 2 no divide a todas las entradas de $\begin{pmatrix} -2 & 15 \\ 0 & 3 \end{pmatrix}$ ya que 2 no divide a $3 = C_{33}$ Por tanto sumaremos la fila que tiene dicho número a la primera.

$$\xrightarrow{F_1+F_3} \left(\begin{array}{ccc|ccc} 2 & 0 & 3 & 0 & -2 & 1 \\ 0 & -2 & 15 & 1 & 2 & 0 \\ 0 & 0 & 3 & 0 & -3 & 1 \\ \hline 1 & -1 & -2 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \text{ como 2 no divide a 3 } \xrightarrow{C_3-C_1} \left(\begin{array}{ccc|ccc} 2 & 0 & 1 & 0 & -2 & 1 \\ 0 & -2 & 15 & 1 & 2 & 0 \\ 0 & 0 & 3 & 0 & -3 & 1 \\ \hline 1 & -1 & -3 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right)$$

$$\xrightarrow{C_1 \leftrightarrow C_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 0 & -2 & 1 \\ 15 & -2 & 0 & 1 & 2 & 0 \\ 3 & 0 & 0 & 0 & -3 & 1 \\ \hline -3 & -1 & 1 & & & \\ 0 & 1 & 0 & & & \\ 1 & 0 & 0 & & & \end{array}\right) \xrightarrow[F_3-3F_1]{F_2-15F_1} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 0 & -2 & 1 \\ 0 & -2 & -30 & 1 & 32 & -15 \\ 0 & 0 & -6 & 0 & 3 & -2 \\ \hline -3 & -1 & 1 & & & \\ 0 & 1 & 0 & & & \\ 1 & 0 & 0 & & & \end{array}\right) \xrightarrow{C_3-2C_1}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -2 & 1 \\ 0 & -2 & -30 & 1 & 32 & -15 \\ 0 & 0 & -6 & 0 & 3 & -2 \\ \hline -3 & -1 & 7 & & & \\ 0 & 1 & 0 & & & \\ 1 & 0 & -2 & & & \end{array}\right) \xrightarrow{-C_2;-F_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -2 & 1 \\ 0 & 2 & -30 & 1 & 32 & -15 \\ 0 & 0 & 6 & 0 & -3 & 2 \\ \hline -3 & 1 & 7 & & & \\ 0 & -1 & 0 & & & \\ 1 & 0 & -2 & & & \end{array}\right) \xrightarrow{C_3+15C_2}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -2 & 1 \\ 0 & 2 & 0 & 1 & 32 & -15 \\ 0 & 0 & 6 & 0 & -3 & 2 \\ \hline -3 & 1 & 22 & & & \\ 0 & -1 & -15 & & & \\ 1 & 0 & -2 & & & \end{array}\right) = \left(\begin{array}{c|c} D_r & Q \\ \hline P^{-1} & \end{array}\right)$$

Por tanto:

$$QAP^{-1} = \begin{pmatrix} 0 & -2 & 1 \\ 1 & 32 & -15 \\ 0 & -3 & 2 \end{pmatrix} \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix} \begin{pmatrix} -3 & 1 & 22 \\ 0 & -1 & -15 \\ 1 & 0 & -2 \end{pmatrix} = D_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

Lo recogemos todo en la siguiente proposición.

PROPOSICIÓN 97. *Sea A una matriz con s filas y t columnas y con entradas enteras. Entonces A es equivalente a una matriz de la forma*

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

donde $r \leq min\{s,t\}$,$\{d_1,\dots,d_r\} \subset \mathbb{N} \setminus \{0\}$ y d_i divide a d_{i+1} para todo i.

Los elementos $d_1,\dots,d_r$ se llaman factores invariantes de A. Y a la matriz anterior se le denomina forma normal de Smith.

DEFINICIÓN 98. *Un k-**menor** de una matriz A es el determinante de una submatriz de A de orden k. Denotamos $D_k(A)$ al máximo común divisor de todos los k-menores de A.*

PROPOSICIÓN 99. *Dada A una matriz de entradas enteras se tiene que:*

1. $D_k(E_{ij}A) = D_k(A) = D_k(AE_{ij})$.
2. $D_k(E_i(-1)A) = D_k(A) = D_k(AE_i(-1))$.
3. $D_k(E_{ij}(z)A) = D_k(A) = D_k(AE_{ij}(z))$.

donde las matrices E son las matrices elementales que se definen en el ambiente de espacios vectoriales.

La demostración es inmediata. Como consecuencia, si A y B son equivalentes entonces $D_k(A) = D_k(B)$ para todo k.

PROPOSICIÓN 100. *Sean A y B dos matrices con entradas enteras. Entonces A es equivalente a B si, y solo si, las dos matrices tienen los mismos factores invariantes.*

DEMOSTRACIÓN. Supongamos que $\{d_1, \ldots, d_r\}$ y $\{d'_1, \ldots, d'_s\}$ son los factores invariantes de A y B, respectivamente y sean H y H' las formas normales de Smith de A y B, entonces $D_k(H) = d_1 \cdots d_k$ y $D_k(H') = d'_1 \cdots d'_k$ y como A y B son equivalentes, $D_k(H) = D_k(H')$ para todo k, se tiene que $d_i = d'_i$ y también $r = s$. El recíproco es inmediato. □

Vamos, ahora, a recuperar las matrices P y Q, con el objetivo de encontrar unas ecuaciones cartesianas que definan el Z-módulo M. Recuérdese que estas matrices recogen los cambios que se le hacen a A, por filas en Q y por columnas en P.

TEOREMA 101. *Sea M un subgrupo de $\mathbb{Z}^n$ de rango r. Entonces podemos encontrar una base $\{f_1, \ldots, f_r, \ldots, f_n\}$ de $\mathbb{Z}^n$ y $\{d_1, \ldots, d_r\} \in \mathbb{N} \setminus \{0\}$, con d_i dividiendo a d_{i+1} para todo i, tales que $\{d_1 f_1, \ldots, d_r f_r\}$ es una base de M.*

DEMOSTRACIÓN. Consideramos $\{(x_{11}, \ldots, x_{1n}), (x_{21}, \ldots, x_{2n}), \ldots, (x_{r1}, \ldots, x_{rn})\}$ una base de M, y S la forma normal de Smith de la matriz A, cuya filas son los elementos de la base de M. Como ambas matrices son equivalentes sabemos que existen P y Q invertibles tales que $QAP^{-1} = S$, de donde $QA = SP$. Como S solo tiene las r primeras filas no nulas, el producto SP tendrá las últimas $n - r$ filas nulas. Es decir, la matriz QA tiene solo r filas no nulas, que nos darán una base del subgrupo M. Y si las columnas de P son $B = \{f_1 = (f_{11}, \ldots, f_{1n}), \ldots, f_n = (f_{n1}, \ldots, f_{nn})\}$, entonces esos primeros elementos de QA son $\{d_1 f_1, \ldots, d_r f_r\}$ que forman una base para M. □

Volvamos ahora a la igualdad $QAP^{-1} = S$, y razonemos como en el caso de los espacios vectoriales (véase la Proposición 31). Tendremos que las $n - r$ últimas columnas de P^{-1} nos dan unas ecuaciones homogéneas de M. Pero además, también se tiene que al multiplicar las r primeras filas de QA por las r primeras columnas de P^{-1}, se obtienen los factores invariantes $d_1, \ldots d_r$. Es decir, una fila cualquiera de las r primeras de QA cumple las siguientes condiciones:

$$\left.\begin{array}{rcll} p_{11}x_1 + \cdots + p_{n1}x_n & \equiv & 0 & \text{mód } d_1 \\ & \vdots & & \\ p_{1r}x_1 + \cdots + p_{nr}x_n & \equiv & 0 & \text{mód } d_r \\ p_{1(r+1)}x_1 + \cdots + p_{n(r+1)}x_n & = & 0 & \\ & \vdots & & \\ p_{1n}x_1 + \cdots + p_{nn}x_n & = & 0 & \end{array}\right\}$$

donde $(p_{11}, \ldots, p_{n1}), \ldots, (p_{1n}, \ldots, p_{nn})$ son las columnas de la matriz P^{-1}.

Se obtendrían, así, unas ecuaciones cartesianas de M. Veremos, en el siguiente capítulo, que la parte en congruencias y la parte homogénea responden a los submódulos de torsión y libre de torsión de M, respectivamente. Pero estos resultados tendrán, además, otras consecuencias en el ambiente de monoides. Es por esta razón que lo ubicamos en el siguiente capítulo.

Monoides y semigrupos

DEFINICIÓN 102. *Un* ***semigrupo*** *es un par* $(S, +)$*, donde* S *es un conjunto no vacío y* $+$ *es una operación binaria y cumpliendo la propiedad asociativa, es decir,* $a+(b+c) = (a+b)+c$ *para todo* $a, b, c \in S$*.*

Si, además, existe elemento neutro, que denotaremos por 0*, cumpliendo* $a+0 = 0+a = a$ *para todo* $a \in S$*, se dirá que* S *es un* ***monoide****.*

Si la operación binaria de un monoide es conmutativa, se dirá que el monoide es conmutativo.

EJEMPLO 103. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, son monoides conmutativos. También lo son $(\mathbb{Z}, \cdot)$ y $(\mathbb{Q}, \cdot)$, donde aquí el elemento neutro es el 1.

Sin embargo, $(\mathbb{N}, -)$ no es un monoide porque la sustracción no es ley de composición interna en $\mathbb{N}$. $(\mathbb{N}, \star)$ donde $\star$ está definido como $a \star b = max\{a, b\}$ es un monoide.

DEFINICIÓN 104. *Un* ***submonoide*** *de un monoide* S *es un conjunto* $H \subseteq S$ *tal que* $0 \in H$ *y para cualquier* $a, b \in H$ *el elemento* $a + b \in H$*.*

NOTA 105. Un submonoide de un monoide es en sí mismo un monoide, y la intersección de una familia de submonoides de un monoide S es un submonoide de S.

9. Sistemas de generadores y morfismos

DEFINICIÓN 106. *Sea* A *un subconjunto de un monoide* S*, el* ***monoide generado por*** A*, denotado por* $\langle A \rangle$*, es el menor submonoide de* S *que contiene a* A*. Viene dado por*

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}, r_i \in \mathbb{N}, x_i \in A \right\}.$$

DEFINICIÓN 107. *Cuando existe un subconjunto finito* A *de* S *tal que* $S = \langle A \rangle$ *se dice que el monoide* $(S, +)$ *es* ***finitamente generado*** *por* A*.*

EJEMPLO 108. $(\mathbb{N}, +)$ está generado por $\{1\}$ y por consiguiente es un monoide finitamente generado. El monoide $(\mathbb{Z}, +)$ está generado por el subconjunto $\{-1, 1\}$. El monoide $(\mathbb{N}^*, \cdot)$ no es finitamente generado. El monoide $(\mathbb{N}^*, \cdot)$ está generado por el subconjunto formado por $\{1\} \cup \{p \in \mathbb{N}^* \mid p \text{ primo}\}$.

DEFINICIÓN 109. *Decimos que* S *está* ***minimalmente generado*** *por* A *si* $\langle A \rangle = S$ *y no existe un subconjunto propio de* A *que genere a* S*.*

DEFINICIÓN 110. *Una aplicación* $f \colon S \to S'$ *entre dos monoides es un morfismo de monoides si*

1. $f(0) = 0$

2. $f(a+b) = f(a) + f(b)$ *para todo* $a, b \in S$.

Obsérvese que si $n \in \mathbb{N}$ entonces y $f\colon S \to S'$ un **morfismo de monoides** con $S \subset \mathbb{N}^k$ y $S' \subset \mathbb{N}^r$ entonces $f(ns) = f(s + \cdots + s) = f(s) + \cdots + f(s) = nf(s)$.

Definición 111. *Sea* $f\colon S \to S'$ *un morfismo de monoides, se definen su* ***núcleo*** *y su* ***imagen*** *como*

$$\mathrm{Ker}(f) = \{(a, b) \in S \times S \mid f(a) = f(b)\}$$
$$\mathrm{Im}(f) = \{f(a) \mid a \in S\}.$$

Obsérvese que $\mathrm{Ker}(f)$ no es un subconjunto de S. Sin embargo, sí que se puede utilizar para decir que: el morfismo de monoides f es inyectivo si y sólo si $\mathrm{Ker}(f) = \{(x, x) \in S \times S \mid x \in S\}$.

Con esta definición de núcleo se tienen las propiedades necesarias para construir un monoide cociente. A saber una relación de equivalencia que respeta la suma.

Definición 112. *Una* ***congruencia*** σ *para un monoide* S *es una relación de equivalencia en* S *que respeta la suma de* S.

Ejemplo 113. Sea $f\colon S \to S'$ un morfismo de monoides, entonces $\mathrm{Ker}(f)$ es una congruencia en S. Ya que es:

1. Reflexiva: $(x, x) \in \mathrm{Ker}(f)$ para todo $x \in S$.
2. Simétrica: Si $(x, y) \in \mathrm{Ker}(f)$ entonces $(y, x) \in \mathrm{Ker}(f)$.
3. Transitiva: Si $(x, y) \in \mathrm{Ker}(f)$ e $(y, z) \in \mathrm{Ker}(f)$ entonces $(x, z) \in \mathrm{Ker}(f)$.
4. Respeta la suma: Si $(x, y) \in \mathrm{Ker}(f)$ y $s \in S$ entonce $(x + s, y + s) \in \mathrm{Ker}(f)$.

Con la noción de congruencia, podemos contar, en el ambiente de monoides, con la herramienta del cociente.

Definición 114. *Si* S *es un monoide y* σ *una congruencia, podemos definir* $[a]_\sigma = \{b \in S \mid (a, b) \in \sigma\}$. *Y así obtener, en el conjunto cociente* S/σ, *una estructura de monoide mediante* $[a]_\sigma + [b]_\sigma = [a + b]_\sigma$. *Denotaremos* S/σ *al* ***monoide cociente****.*

Si no hay peligro de confusión escribiremos $[s]$ en lugar de $[s]_\sigma$.

Teorema 115. *Sea* $f\colon S \to S'$ *un morfismo de monoides. Entonces existe un isomorfismo de monoides*

$$\overline{f}\colon S/\mathrm{Ker}(f) \to \mathrm{Im}(f),$$

dado por $\overline{f}([a]) = f(a)$.

La demostración es análoga al caso de módulos (véase el Teorema 72).

Como consecuencia de este teorema tenemos el siguiente resultado.

Teorema 116. *Sea* S *un monoide generado por* $\{s_1, \ldots, s_n\}$ *entonces existe una congruencia* σ *en* $\mathbb{N}^n$ *tal que* S *es isomorfo a* $\mathbb{N}^n/\sigma$.

Demostración. Basta considerar el morfismo de monoides sobreyectivo:

$$f\colon \mathbb{N}^n \to S \tag{1}$$

dado por $f(a_1, \ldots, a_n) = a_1 s_1 + \cdots + a_n s_n$, y usando el teorema anterior $\mathbb{N}^n/\mathrm{Ker}(f)$ es isomorfo a S. □

10. Monoides cancelativos

Por tanto el estudio de los monoides se puede realizar desde el estudio de congruencias y, aunque parece algo más artificial, hay, sin embargo, un detalle importante que nos permitirá utilizar gran parte de lo que hemos estudiado hasta ahora. Demos algunos pasos explorando este camino.

DEFINICIÓN 117. *Dada una congruencia σ en $\mathbb{N}^n$, podemos definir:*

$$M_\sigma = \{a - b \in \mathbb{Z}^n \mid (a, b) \in \sigma\}.$$

PROPOSICIÓN 118. *M_σ es un subgrupo de $\mathbb{Z}^n$.*

DEMOSTRACIÓN. La propiedad reflexiva de σ nos asegura la existencia del elemento neutro en M_σ. La propiedad simétrica de σ nos permite contar en M_σ con el opuesto de cada elemento de M_σ. Y como σ respeta la suma podemos hacer la siguiente cuenta:

$$\begin{array}{rcl}(a, b) \in \sigma & \Rightarrow & (a + c, b + c) \in \sigma, \\ (c, d) \in \sigma & \Rightarrow & (c + b, d + b) \in \sigma.\end{array}$$

Ahora, por la transitividad de σ, tenemos que $(a+c, b+d) \in \sigma$. Con lo que M_σ es un subgrupo de $\mathbb{Z}^n$. □

La construcción recíproca también se puede llevar a cabo, pero con alguna restricción. Cuando lo tengamos, podremos aplicar todo lo que sabemos sobre subgrupos de $\mathbb{Z}^n$ para el estudio de los monoides finitamente generados, que son todos isomorfos a $\mathbb{N}^n/\sigma$.

DEFINICIÓN 119. *Dado M subgrupo de $\mathbb{Z}^n$ definimos*

$$\sim_M = \{(a, b) \in \mathbb{N}^n \times \mathbb{N}^n \mid a - b \in M\}.$$

PROPOSICIÓN 120. *$\sim_M$ es una congruencia.*

DEMOSTRACIÓN. Como antes, la existencia del cero en M nos permite obtener la propiedad reflexiva para $\sim_M$, mientras que la existencia de opuesto de un elemento en M, nos da la propiedad simétrica para $\sim_M$. Para la propiedad transitiva si $(a, b) \in \sim_M$ y $(b, c) \in \sim_M$ entonces $a - b, b - c \in M$ con lo que $a - b + b - c = a - c \in M$ nos asegura la transitividad. Y por último, para comprobar que respeta la suma, es claro que si $(a, b) \in \sim_M$ y $x \in \mathbb{N}^n$ entonces $a - b \in M$ y por tanto también $a + x - (b + x) \in M$ y por tanto $(a + x, b + x) \in \sim_M$. □

Obsérvese que si $(a + x, b + x) \in \sigma$, entonces $a + x - (b + x) \in M_\sigma$ y por tanto $a - b \in M_\sigma$ y tenemos que $(a, b) \in \sim_{M_\sigma}$. Luego, si partimos de σ y construimos $\sim_{M_\sigma}$, pueden aparecer nuevos elementos; salvo que se exija a σ alguna condición adicional.

DEFINICIÓN 121. *Un monoide se dice **cancelativo** si para cualesquiera $a, b, c \in S$, con $a + c = b + c$ se tiene que $a = b$.*

PROPOSICIÓN 122. *Si $\mathbb{N}^n/\sigma$ es cancelativo entonces $\sigma = \sim_{M_\sigma}$.*

A partir de ahora, salvo mención contraria, supondremos que todos los monoides son cancelativos.

PROPOSICIÓN 123. *Sea M un subgrupo de $\mathbb{Z}^n$ tal que $(x_1, \dots, x_n) \in M$ si y solo si*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &\equiv 0 \mod d_1, \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &\equiv 0 \mod d_r, \\ a_{(r+1)1}x_1 + \cdots + a_{(r+1)n}x_n &= 0, \\ &\vdots \\ a_{(r+k)1}x_1 + \cdots + a_{(r+k)n}x_n &= 0. \end{aligned}$$

Entonces $\mathbb{N}^n/\sim_M$ es isomorfo a un submonoide de $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ generado por:
$\{([a_{11}]_{d_1}, \dots, [a_{r1}]_{d_r}, a_{(r+1)1}, \dots, a_{(r+k)1}), \dots, ([a_{1n}]_{d_1}, \dots, [a_{rn}]_{d_r}, a_{(r+1)n}, \dots, a_{(r+k)n})\}$

DEMOSTRACIÓN. Basta trasladar la demostración que se hizo sobre espacios vectoriales (Lema 38), que nos aseguraba que las imágenes por una aplicación lineal f, de un sistema de generadores, eran un sistema de generadores de la imagen $\mathrm{Im}(f)$. Tenemos que $\{e_1, \dots, e_n\}$ es un sistema de generadores de $\mathbb{N}^n$ y la aplicación $f\colon \mathbb{N}^n \to \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ dada por:

$$f(e_i) = ([a_{1i}]_{d_1}, \dots, [a_{ri}]_{d_r}, a_{(r+1)i}, \dots, a_{(r+k)i})$$

□

DEFINICIÓN 124. *Un monoide S se dice **libre de torsión** si para cualesquiera $a, b \in S$ y para cualquier $k \in \mathbb{N} \setminus \{0\}$, se tiene que $ka = kb$ implica que $a = b$.*

PROPOSICIÓN 125. *Sea M un subgrupo de $\mathbb{Z}^n$. Entonces son equivalentes:*

1. *M es homogéneo. Es decir, en las ecuaciones de la Proposición 123, no aparece ninguna congruencia.*
2. *El monoide cancelativo $\mathbb{N}^n/\sim_M$ es isomorfo a un submonoide de $\mathbb{Z}^k$ para algún $k \in \mathbb{N}$.*
3. *El monoide cancelativo $\mathbb{N}^n/\sim_M$ es libre de torsión.*

DEMOSTRACIÓN. Haremos la demostración de 3. $\Rightarrow$ 1, las otras son inmediatas. Para ello, probaremos que los factores invariantes (que dan las congruencias) son todos iguales a 1. Sean $d_1, \dots, d_r$ los factores invariantes, por el Teorema 101, sabemos que existe una base $\{f_1, \dots, f_r, \dots, f_n\}$ base de $\mathbb{Z}^n$, tal que $\{d_1 f_1, \dots, d_r f_r\}$ son una base de M. Si $d_1 > 1$ y $f_1 = (a_1, \dots, a_n)$, definimos: $f_1^+ = (\max\{a_1, 0\}, \dots, \max\{a_n, 0\})$ y $f_1^- = (\max\{-a_1, 0\}, \dots, \max\{-a_n, 0\})$ (esto no es más que separar los elementos positivos y negativos de f_1, tomando estos últimos con signo positivo). Ahora bien $f_1^+, f_1^- \in \mathbb{N}^n$, y como $d_1 f_1 \in M$ y $d_1 > 0$ tenemos que $f_1 = f_1^+ - f_1^- \notin M$, y por tanto $[f_1^+]_{\sim_M} \neq [f_1^-]_{\sim_M}$. Sin embargo, como $d_1 f_1 \in M$, tenemos que $d_1[f_1^+]_{\sim_M} = d_1[f_1^-]_{\sim_M}$, pero esto no es posible si $\mathbb{N}^n/\sim_M$ es libre de torsión. □

La conclusión de los siguientes resultados será que la parte de torsión, en el caso cancelativo, será un subgrupo dentro del monoide. Por tanto esta parte se estudiará con las técnicas de $\mathbb{Z}$-módulos.

PROPOSICIÓN 126. *Sea S un monoide finito. Entonces S es un grupo, si y solo si es cancelativo.*

DEMOSTRACIÓN. Todo grupo es cancelativo. Veamos por tanto la otra implicación. Sea $s \in S \setminus \{0\}$, como S es finito, también lo es $\{ns \mid n \in \mathbb{N}\}$, por tanto existen $m, n \in \mathbb{N}$ con

$m < n$, tales que $ms = ns$ y como $ms = ns = (n-m)s+ms$ al ser S cancelativo tenemos que $(n-m)s = 0$ con $n-m > 1$. Por tanto, tenemos que $(n-m-1)s+s = 0$ y $n-m-1 \geq 0$, y así, s tiene un elemento opuesto, con lo que llegamos a que S es un grupo. □

Podemos hacer una proposición similar al caso libre de torsión. En este caso diría lo siguiente:

PROPOSICIÓN 127. *Sea M un subgrupo de $\mathbb{Z}^n$. Entonces son equivalentes.*

1. *El monoide cancelativo $\mathbb{N}^n/\sim_M$ es finito.*
2. *El monoide cancelativo $\mathbb{N}^n/\sim_M$ es isomorfo a $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$.*
3. *Las ecuaciones que definen a M son todas congruencias.*

La segunda afirmación es la que adelantábamos antes. La parte de torsión de un monoide, es un grupo finito. Así pues, nos centraremos en estudiar los monoides libres de torsión.

Hay monoides, no cancelativos, finitos que no son grupos.

EJEMPLO 128. Consideremos el conjunto $\{0, 3, 6, 9, 12, 15, 18\}$ con tabla de suma:

$+$	3	6	9	12	15	18
3	6	9	12	15	18	9
6	9	12	15	18	9	12
9	12	15	18	9	12	15
12	15	18	9	12	15	18
15	18	9	12	15	18	9
18	9	12	15	18	9	12

Puede comprobarse que es un monoide, pero claramente no es cancelativo. Este monoide es isomorfo al cociente de $3\mathbb{N}/\sigma$, donde σ es la congruencia generada por $(21, 9)$.

Vamos a ver ahora, varios ejemplos sobre los resultados anteriores, para motivar el estudio de los sistemas de generadores en un tipo particular de monoides.

EJEMPLO 129. Consideramos M el subgrupo dado por $M = G(\{(2,0,0),(0,1,-1)\})$. Calculemos los factores invariantes y un sistema de generadores de $\mathbb{N}^3/\sim_M$.

$$\left(\begin{array}{ccc|cc} 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \xrightarrow{F_1 \leftrightarrow F_2} \left(\begin{array}{ccc|cc} 0 & 1 & -1 & 0 & 1 \\ 2 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \xrightarrow{C_1 \leftrightarrow C_2} \left(\begin{array}{ccc|cc} 1 & 0 & -1 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & & \\ 1 & 0 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \xrightarrow{C_3 = C_3 + C_1}$$

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & & \\ 1 & 0 & 1 & & \\ 0 & 0 & 1 & & \end{array}\right) = \left(\begin{array}{c|c} D & Q \\ \hline P^{-1} & \end{array}\right).$$

Por tanto:

$$QAP^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -1 \end{pmatrix} \left(\begin{array}{c|cc} 0 & 1 & 0 \\ \hline 1 & 0 & 1 \\ \hline 0 & 0 & 1 \end{array}\right) = D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

Ahora, usando la Proposición 123, tenemos que $\mathbb{N}^3/\sim_M$ es isomorfo al submonoide de $\mathbb{Z}_2\times\mathbb{Z}$ generado por $\{([1]_2,0),([0]_2,1),([0]_2,1)\}$. Claramente un sistema minimal de generadores es: $\{([1]_2,0),([0]_2,1)\}$.

Ejemplo 130. Consideremos ahora $M = G(\{(4,1,-3),(1,-2,1)\})$. Si calculamos sus factores invariantes y sus matrices P y Q, tenemos:

$$QAP^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} 4 & 1 & -3 \\ 1 & -2 & 1 \end{pmatrix}\left(\begin{array}{ccc|c} 1 & -2 & 5 \\ 0 & -3 & 7 \\ 0 & -4 & 9 \end{array}\right) = D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Con lo que M está definido por una sola ecuación $5x+7y+9z=0$ y un sistema de generadores del submonoide de $\mathbb{Z}$ isomorfo a $\mathbb{N}^3/\sim_M$ está dado por $\{5,7,9\}$. Obsérvese que este submonoide está contenido en $\mathbb{N}$ y que ninguno de los tres generadores es superfluo. Es decir, dentro de $\mathbb{N}$ hay un submonoide con un sistema minimal de generadores formado por tres elementos. La idea de dimensión empieza a fallar cuando un submonoide tiene "mayor dimensión" que el monoide en el que está incluido. De ahí que hablemos de sistema minimal de generadores en vez de bases.

Obsérvese también, que el hecho de que todos los coeficientes de las ecuaciones de M sean positivos, nos permite encontrar submonoides de $\mathbb{N}^k$.

Veamos un último ejemplo para motivar, algo más, el caso de monoides dentro de $\mathbb{N}^k$ para un cierto k.

Ejemplo 131. Consideremos esta vez el subgrupo $M = G\{(1,-2,2,-1),(-3,1,1,1)\} \subset \mathbb{Z}^4$. Tenemos como factores invariantes y matrices P y Q:

$$QAP^{-1} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & -2 & 2 & -1 \\ -3 & 1 & 1 & 1 \end{pmatrix}\left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & -1 & 1 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 5 \end{array}\right) = D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Por tanto, las ecuaciones de M son dos y vienen dadas por:

$$\begin{aligned} x_1+x_2+x_3+x_4 &= 0, \\ x_1-2x_2+5x_4 &= 0. \end{aligned}$$

Así pues, M es homogéneo y el monoide $S = \mathbb{N}^4/\sim_M$ es libre de torsión isomorfo a un submonoide de $\mathbb{Z}^2$. Además, un sistema de generadores de dicho monoide podría ser: $\{(1,1),(1,-2),(1,0),(1,5)\}$. Ahora mismo, no podemos asegurar S sea isomorfo a un submonoide de $\mathbb{N}^2$, pues $(1,-2)$ no está en $\mathbb{N}^2$. Sin embargo, sí será posible hacerlo.

Para conseguirlo, podemos aprovechar el hecho de tener una ecuación con todas las entradas positivas para, multiplicándola por 2 y sumándola a la otra, obtener un nuevo sistema de ecuaciones para M:

$$\begin{aligned} x_1+x_2+x_3+x_4 &= 0, \\ 3x_1+2x_3+7x_4 &= 0. \end{aligned}$$

Y ahora, se tendría el sistema de generadores $\{(1,3),(1,0),(1,2),(1,7)\}$, que nos asegura que S sí es isomorfo a un submonoide de $\mathbb{N}^2$.

Así pues, parece que teniendo un sistema homogéneo con, al menos, una ecuación con todos los coeficientes positivos, podremos deducir que, el submonoide asociado $\mathbb{N}^n/\sim_M$, es isomorfo a un submonoide de $\mathbb{N}^k$ para un cierto k.

DEFINICIÓN 132. *Un monoide S se dice* ***reducido*** *si el único elemento que tiene opuesto es el cero.*

Con esta condición, enunciaremos el teorema de Grillet, cuya demostración requiere algunos otros resultados y que puede verse en [**4**].

TEOREMA 133 (Teorema de Grillet). *Sea S un monoide finitamente generado. S es cancelativo, libre de torsión y reducido si y sólo si es isomorfo a un submonoide de $\mathbb{N}^k$, para algún entero positivo k.*

Al ser cancelativo, S es de la forma $\mathbb{N}^n/\sim_M$ y al ser libre de torsión M es homogéneo. La hipótesis de reducción nos servirá para demostrar la existencia de un elemento fuertemente positivo (con todas las coordenadas positivas), que serán los coeficientes de una ecuación de M.

Como se observa por todo lo dicho hasta ahora, el estudio de los monoides cancelativos, se puede hacer desde el punto de vista de los subgrupos M de $\mathbb{N}^n$, que básicamente pasa por estudiar los coeficientes de un sistema de ecuaciones. Dicho más correctamente, del estudio de presentaciones (generadores y relatores) o, equivalentemente, de congruencias en $\mathbb{N}^n$. Nosotros no vamos a seguir ese camino y vamos a estudiar los sistemas de generadores para los monoides que sean isomorfos a submonoides de $\mathbb{N}^n$. En la literatura estos monoides reciben el nombre de semigrupos afines.

11. Sistemas minimales de generadores en semigrupos afines

Vamos, pues, a centrar el estudio de sistemas minimales de generadores a monoides cancelativos dentro de $\mathbb{N}^n$, es decir, los semigrupos afines; y dentro de esta clase, nos vamos a fijar en dos tipos. Por un lado, aquellos que se obtienen considerando los elementos positivos de subgrupos de $\mathbb{Z}^n$, son los llamados semigrupos afines completos. Por ejemplo, el conjunto de soluciones enteras no negativas de sistemas homogéneos de ecuaciones lineales diofánticas, (diofántica significa con coeficientes enteros). Y, por otro lado, los semigrupos numéricos, que son aquellos semigrupos afines de $\mathbb{N}$. En ambos casos tendremos condiciones adicionales para poder especificar un sistema minimal de generadores.

DEFINICIÓN 134. *Un semigrupo afín $S \subseteq \mathbb{N}^n$ se dice* ***completo*** *si existe un subgrupo M de $\mathbb{Z}^n$ tal que $S = M \cap \mathbb{N}^n$.*

NOTA 135.

1. Como $G(S)$ es el menor subgrupo que contiene a S, se tiene que $S = G(S) \cap \mathbb{N}^n$. Por tanto, se puede tomar esta última propiedad como una caracterización de estos semigrupos completos.
2. Sea $S = \{x \in \mathbb{N}^n \mid Ax = 0\}$, es claro que S es un monoide incluido en $\mathbb{N}^n$. Además, si $x, y \in S$ con $x - y \in \mathbb{N}^n$, entonces $x - y \in S$. Por tanto S es un semigrupo afín completo.

En el Ejemplo 130, pudimos ver como un submonoide de $\mathbb{N}$ está generado minimalmente por 3 elementos. Diremos que $S = \langle 5, 7, 9\rangle$. Este semigrupo afín no es completo ya que $2 = 7 - 5 \in G(S) \cap \mathbb{N}$ y $2 \notin \langle 5, 7, 9\rangle$.

Definición 136. *Un* ***semigrupo numérico*** *es un submonoide de* $\mathbb{N}$ *con complemento finito.*

Proposición 137. *El único semigrupo numérico completo es* $\mathbb{N}$.

Demostración. Es claro por la Proposición 63, que los subgrupos de $\mathbb{Z}$ son de la forma $g\mathbb{Z}$ para algún $g \in \mathbb{Z}$. Por tanto, si S es completo $S = g\mathbb{N} = \langle g\rangle$, pero estos conjuntos no tienen complemento finito salvo cuando $g = 1$. □

Probaremos que, para estas dos clases de monoides, los sistemas minimales de generadores son únicos.

Veamos alguna idea más del semigrupo numérico.

Ejemplo 138. El monoide $S = \langle 5, 7, 9\rangle$ está formado por los siguientes elementos:

$$\{0, 5, 7, 9, 10, 12, 14, 15, \to\}.$$

Donde $\to$ significa que a partir de este número están todos los elementos de $\mathbb{N}$.

En cuanto al otro tipo de monoides, consideramos el siguiente ejemplo.

Ejemplo 139. Sea el sistema:

$$\left.\begin{array}{rcl} x_1 - 2x_2 + x_3 + 3x_4 & = & 0 \\ -2x_1 - x_2 - x_3 + 2x_4 & = & 0 \end{array}\right\}.$$

En $\mathbb{Z}^4$ cualquier solución es de la forma $a(-3, 1, 5, 0)+b(4, 0, -6, 1)$ con $a, b \in \mathbb{Z}$. Sin embargo, si trabajamos en $\mathbb{N}^4$ las soluciones son de la forma $a(0, 4, 2, 3)+b(1, 5, 1, 4)+c(2, 6, 0, 5)$, como podíamos intuir, el cardinal del sistema minimal de generadores no depende del número de ecuaciones como sucede en $\mathbb{R}$ o en $\mathbb{Z}$.

Nota 140. Obsérvese que, ahora, estamos estudiando las soluciones "no negativas" de sistema de ecuaciones con coeficientes enteros. Mientras que en los desarrollos anteriores, lo que se buscaba era que los coeficientes de las ecuaciones que definen a M, fuesen positivos para encontrar, mediante el cociente $\mathbb{N}^n/\sim_M$, sistemas de generadores de ciertos submonoides de $\mathbb{N}^k$. Ahora estudiamos soluciones de sistemas lineales homogéneos con coeficientes enteros, pero los coeficientes no tienen por qué ser positivos.

11.1. Semigrupos afines. Para proseguir el estudio de los sistemas de generadores en semigrupos afines, vamos a considerar las siguientes definiciones.

Definición 141. *Sean* $x = (x_1, \ldots, x_n)$ *e* $y = (y_1, \ldots, y_n) \in \mathbb{N}^n$, *se dice que* $x \leq y$ *si* $x_i \leq y_i$. *Claramente este orden es un orden parcial, salvo para* $n = 1$ *que es un orden total. Se notará* $<$ *si en alguna coordenada la desigualdad es estricta.*

Definición 142. *Sea* X *un subconjunto de* $\mathbb{N}^n$ *y sea* $x \in X$. *Se dice que* x *es* ***minimal*** *en* X *si no existe otro elemento* $x' \in X$, *tal que* $x' < x$.

El siguiente teorema nos asegura que el conjunto de los minimales de un subconjunto de $\mathbb{N}^n$ es finito. Es un primer paso a la hora de calcular un sistema minimal de generadores para estos semigrupos afines.

TEOREMA 143 (Lema de Dickson). *Sea $X \subseteq \mathbb{N}^n$ no vacío. Entonces $M = Minimales(X)$ tiene un número finito de elementos.*

DEMOSTRACIÓN. La demostración de este resultado se hace por inducción, siendo el caso $n = 1$ inmediato, ya que en este caso sólo hay un elemento mínimo. Supongamos cierto para $n-1$ y comprobémoslo para n. Sea $m = (a_1, \ldots, a_n) \in M$ y, para aplicar inducción, consideramos los siguientes conjuntos: para cada $1 \leq i \leq n$ y para cada $0 \leq j \leq a_i$ denotamos:

$$M_{ij} = \{(x_1, \ldots, x_n) \in M \mid x_i = j\} \text{ y}$$
$$B_{ij} = \{(x_1, \ldots, x_{n-1}) \in \mathbb{N}^{n-1} \mid (x_1, \ldots, x_{i-1}, j, x_i, \ldots, x_{n-1}) \in M_{ij}\}.$$

Es claro que $Minimales(M) = M$ y también $Minimales(B_{ij}) = B_{ij}$, que por hipótesis de inducción son finitos y por tanto también lo son los M_{ij}, y su unión $\bigcup M_{ij}$. Probemos que $M \subseteq \bigcup M_{ij}$. Tomemos un elemento $x = (x_1, \ldots, x_n) \in M$, si existe alguna coordenada de m menor que la correspondiente de x, pongamos $a_i \leq x_i$, entonces tenemos que $x \in M_{ix_i}$, y por tanto está en la unión. Si para todas las coordenadas de m se tiene que $a_i > x_i$, tendríamos que $m > x$ pero esto es una contradicción ya que m era minimal. □

A continuación daremos una serie de resultados de fácil comprobación.

COROLARIO 144. *Sea $x \in \mathbb{N}^n$, entonces el conjunto $A = \{y \in \mathbb{N}^n \mid y < x\}$ es finito.*

COROLARIO 145. *Toda cadena ordenada descendente de elementos de $\mathbb{N}^n$ es finita.*

COROLARIO 146. *Sea X un subconjunto no vacío de $\mathbb{N}^n$ y sea $M = Minimales(X)$. Entonces para cada $x \in X$ existe $m \in M$ con $m \leq x$.*

Vamos a ver que el conjunto de elementos minimales son un sistema de generadores para los semigrupos afines completos, entre los que están los conjuntos de soluciones no negativas de sistemas homogéneos de ecuaciones diofánticas.

PROPOSICIÓN 147. *Sea S un semigrupo afín completo, y consideremos $M = \{x_1, \ldots, x_n\}$ el conjunto de elementos minimales, entonces $S = \langle x_1, \ldots, x_n \rangle$.*

DEMOSTRACIÓN. Sea $s \in S \setminus \{0\}$, entonces por el corolario anterior existe $x_{i_1} \in M$ tal que $x_{i_1} < s$. Consideramos ahora $s - x_{i_1} \in G(S) \cap \mathbb{N}^n = S$ y repetimos: si $s - x_{i_1} \in M$ paramos, si no, existe $x_{i_2} \in M$ con $x_{i_2} < s - x_{i_1}$, por el Corolario 145, esta cadena termina y al final tendremos que $x_{i_t} = s - \sum_{j=1}^{t-1} x_{i_j}$. Con lo que $s = \sum_{j=1}^{t} x_{i_j}$. □

Además, este conjunto sería minimal, ya que si algún elemento de M, digamos x_1, se pudiese escribir como $x_1 = a_2x_2 + \cdots + a_nx_n$ con algún $a_i > 0$ se tendría que $x_1 - a_ix_i \geq 0$ con lo que $x_1 \geq a_ix_i$ pero esto es imposible pues x_1 es minimal y distinto de x_i.

Esta idea de ir restando elementos del semigrupo para encontrar los elementos minimales, se puede extender a semigrupos afines, incluso de dimensión infinita.

Sistemas de generadores en semigrupos afines completos

Vamos a centrarnos en el cálculo efectivo de dicho conjunto que es un sistema minimal de generadores. Lo haremos dando un par de algoritmos interesantes en su filosofía.

ALGORITMO 148 (Fortenbacher). *Sea $a_1x_1 + \cdots + a_qx_q = 0$ una ecuación diofántica homogénea. La idea de este algoritmo es comenzar por los elementos de la base canónica $\{(1, 0, \ldots, 0), \ldots, (0, \ldots, 1)\}$ y realizar la siguiente acción:*

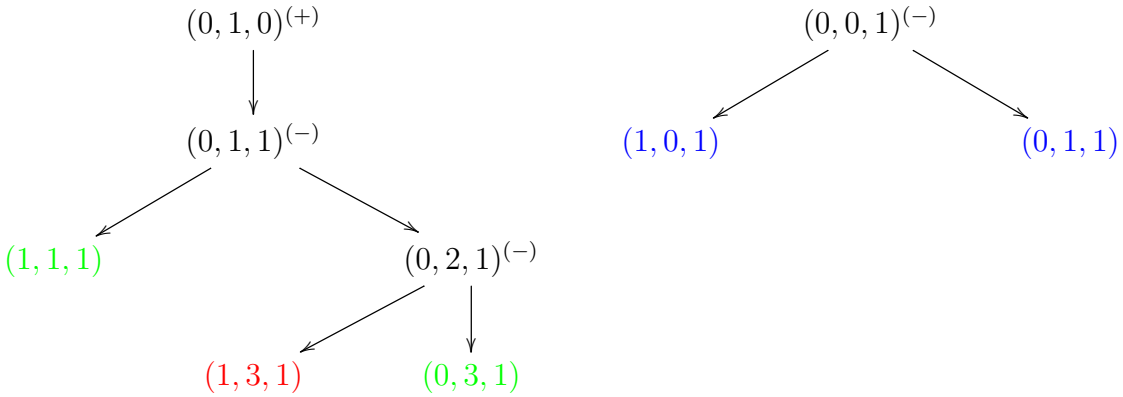
Si $(x_1, \ldots, x_q)$ no es aún una solución de la ecuación hacemos lo siguiente:

- *Si $a_1x_1 + \cdots + a_qx_q < 0$ entonces incrementamos en uno el valor de x_j si $a_j > 0$. Apareciendo un elemento nuevo, por cada j que cumpla la condición.*
- *Si $a_1x_1 + \cdots + a_qx_q > 0$ entonces incrementamos en uno el valor de x_j si $a_j < 0$.*

Es claro que si aumentamos en los otros casos que no contempla el algoritmo, obtenemos valores más altos que los de partida. Es decir, las condiciones nos marcan unas direcciones que no debemos seguir.

EJEMPLO 149. Sea la ecuación diofántica homogénea $2x_1 + x_2 - 3x_3 = 0$. Y evaluamos en los tres elementos de la base canónica: En $(1, 0, 0)$ es positivo $(= 2)$. Por tanto, solo nos interesa seguir por $(1, 0, 1)$ que, al evaluar, nos da negativo (-1). Ahora aparecen dos caminos: $(2, 0, 1)$ que sale positivo $(= 1)$ y $(1, 1, 1)$ que es una solución. Si continuamos por $(2, 0, 1)$, sólo podemos añadir en la última coordenada $(2, 0, 2)$, que sale negativo (-2). Aparecen, de nuevo, dos nuevos caminos: $(3, 0, 2)$ que es otra solución y $(2, 1, 2)$ que podemos descartar ya que es mayor que la solución $(1, 1, 1)$ (el objetivo es encontrar las soluciones minimales).

Escribimos de forma más esquemática y clara los resultados para los otros dos elementos de la base canónica.



El elemento en rojo se descarta por ser mayor que la solución $(1, 1, 1)$, los elementos en azul se pueden descartar porque ya han sido estudiados antes, y los elementos en verde son las soluciones.

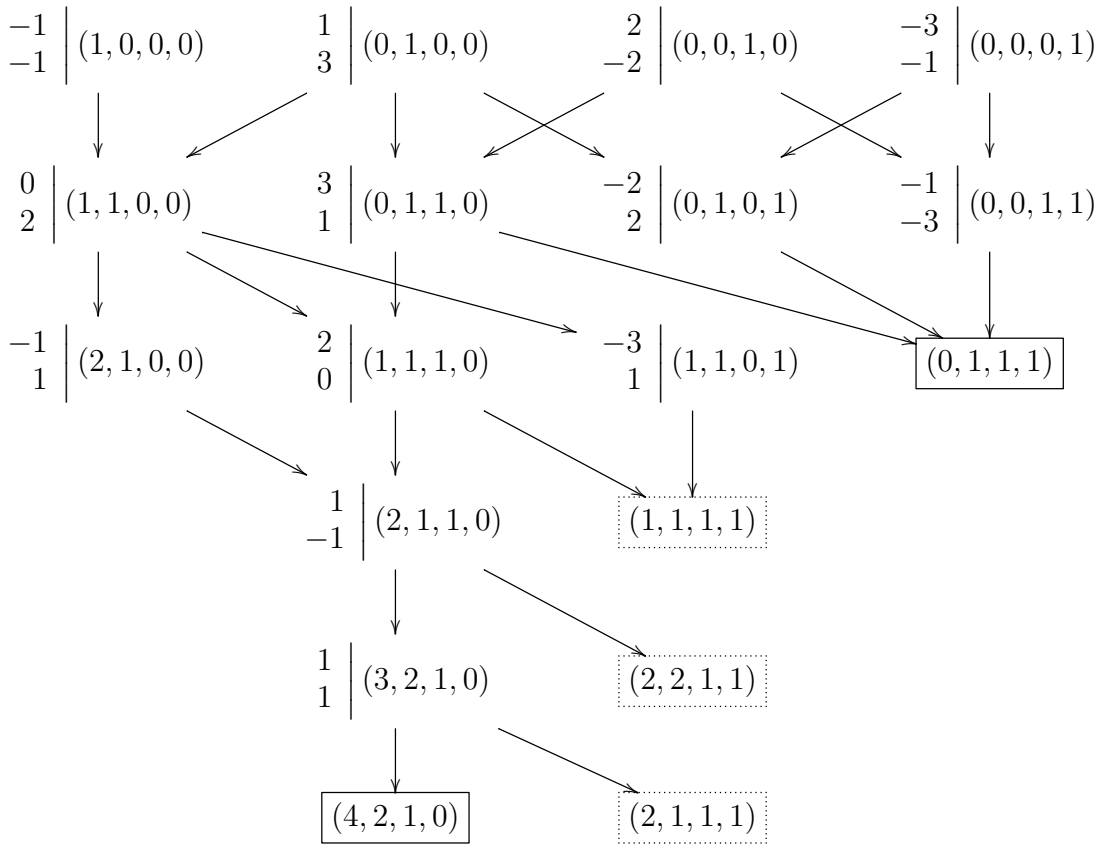
ALGORITMO 150 (Contejean & Devie). *Este algoritmo es una extensión del anterior a un número arbitrario de ecuaciones. Lo único que hay que hacer es concretar que entendemos por una "dirección correcta" a la hora de continuar el algoritmo. Obsérvese que las dos condiciones del algoritmo anterior se pueden resumir en una mediante:* ***incrementamos en uno el valor de*** *x_j* ***si*** *$(a_1x_1 + \cdots + a_qx_q)(a_j) < 0$. Así pues, si $Ax = 0$ es un sistema homogéneo de ecuaciones lineales diofánticas, consideramos la siguiente condición:*

Si $(x_1, \ldots, x_q)$ no es todavía solución, aumentamos en uno el valor de x_j si $Ax \cdot Ae_j < 0$ donde el producto, es el producto escalar usual.

Ejemplo 151. Consideremos el sistema de ecuaciones:

$$\left.\begin{array}{rcl} -x_1 + x_2 + 2x_3 - 3x_4 & = & 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 & = & 0 \end{array}\right\}.$$

Partimos de $\{e_1, e_2, e_3, e_4\}$ y con flechas indicamos los pasos que se pueden dar desde cada solución, obviamente cada elemento se podrá obtener desde varias soluciones anteriores. Denotaremos $Ax|x$ para controlar los elementos (x) y el valor a comparar (Ax).



Obteniéndose que las soluciones minimales del sistema son $(0, 1, 1, 1)$ y $(4, 2, 1, 0)$. Hemos recuadrado las soluciones, y aquellas cuaternas que son comparables con alguna solución ya encontrada.

Para más detalles puede consultarse [**2**].

Sistemas minimales de generadores en semigrupos numéricos

En esta última sección, vamos a estudiar un tipo particular de monoides, entre los que se encuentra el del Ejemplo 130. Y vamos a dar una manera práctica para encontrar dicho sistema minimal de generadores, que ya sabemos que existe, a partir del Lema de Dickson y los resultados posteriores.

Recordemos que un semigrupo numérico S era un submonoide de $\mathbb{N}$ cuyo complemento es finito.

Lema 152. *Sea A un subconjunto no vacío de $\mathbb{N}$. Entonces $\langle A\rangle$ es un semigrupo numérico si y solo si* $\gcd(A) = 1$.

Demostración. Sea $d = \gcd(A.)$ Entonces d divide a todos los elementos de $\langle A\rangle$, y si es un semigrupo numérico, entonces el complemento es finito, por tanto deben existir $x, x+1 \in \langle A\rangle$. Pero si d divide a x y a $x+1$ es porque $d = 1$.

Si $\gcd(A) = 1$ entonces existen $a_1, \ldots, a_n \in A$ y $x_1 \ldots, x_n \in \mathbb{Z}$ tales que $x_1a_1 + \ldots + x_na_n = 1$, podemos suponer que todos los coeficientes positivos están al principio, y que son los i primeros, entonces tenemos que $x_1n_1 + \ldots + x_ia_i = 1 - x_{i+1}a_{i+1} - \ldots - x_na_n$, tenemos que $s = -(x_{i+1}a_{i+1} + \ldots + x_na_n) \in \langle A\rangle$ y que $s + 1 = x_1n_1 + \ldots + x_ia_i \in \langle A\rangle$. Veamos ahora que si $n \geq (s-1)s + (s-1)$ entonces $n \in \langle A\rangle$. Consideremos $n = rs + q$ con $0 \leq r < s$ o, equivalentemente, $r \leq s - 1$. Como $qs + r = n \geq (s_1)s + (s-1)$ tenemos que $q \geq s - 1 \geq r$ y por tanto $n = (rs + r) + (q - r)s = r(s + 1) + (q - r)s$ y por tanto $n \in \langle A\rangle$. □

Obsérvese que si H es un monoide en $\mathbb{N}$ con $d = \gcd(H)$ entonces podemos considerar $H/d = \{m/d \mid m \in H\}$ y tenemos que H y H/d son isomorfos. Por tanto, todo monoide no trivial de $\mathbb{N}$ es isomorfo a un semigrupo numérico.

Vamos a dar un primer resultado que nos indica el camino a seguir a la hora de buscar un sistema de generadores para los semigrupos numéricos.

Lema 153. *Sea S un submonoide de $\mathbb{N}^n$. Entonces $S \setminus (S^* + S^*)$ es un sistema de generadores de S y además cualquier otro lo contiene. Denotamos $S^* = S \setminus \{0\}$.*

Demostración. El conjunto $S \setminus (S^* + S^*)$ es el conjunto de elementos de S que no se pueden poner como suma de dos elementos no nulos de S. Así pues, si $s \notin S \setminus (S^* + S^*)$, es porque existen $x, y \in S \setminus \{0\}$ tal que $s = x + y$ y por tanto $x, y < s$. Si repetimos el proceso con cada sumando obtendremos en un número finito de pasos que $s = s_1 + \cdots + s_n$ con $s_i \in S \setminus (S^* + S^*)$, lo que prueba que este conjunto es un sistema de generadores.

Mientras que, si A es otro sistema de generadores y tomamos $x \in S \setminus (S^* + S^*)$, tenemos que $x = r_1a_1 + \cdots + r_ta_t$, con $a_i \in A$ y $r_i \in \mathbb{N}$, pero como $x \in S \setminus (S^* + S^*)$, se tiene que $x = a_i$ para algún $i = 1, \ldots, t$. □

En particular, para todo semigrupo numérico S, existe un único sistema minimal de generadores, a saber $S \setminus (S^* + S^*)$. El objetivo ahora es probar que siempre será finito.

Para ello, vamos a introducir un concepto que es muy útil en el ambiente de los semigrupos numéricos sobretodo en la parte computacional. Los conjuntos de Apéry.

Definición 154. *Dado S un semigrupo numérico y $n \in S$ definimos el **conjunto de Apéry** de n en S como:*

$$Ap(S, n) = \{s \in S \mid s - n \notin S\}.$$

Lema 155. *$Ap(S, n) = \{0 = w(0), w(1), \ldots, w(n-1)\}$ donde $w(i) = min\{s \in S \mid s \equiv i$ mód $n\}$.*

Demostración. Basta considerar cualquier elemento $s \in S$ y escribirlo como $s = qn + r$, y entonces tomar $j = \max\{i \in \mathbb{N} \mid s - in \in S\}$, dicho $s - jn = w(r)$, como $\mathbb{N} \setminus S$ es finito, se pueden encontrar n elementos seguidos a los que aplicar el razonamiento anterior, obteniendo así todos los elementos de $Ap(S, n)$. □

Ejemplo 156. Sea $S = \langle 5, 7, 9\rangle$. Vimos que $S = \{0, 5, 7, 9, 10, 12, 14, \rightarrow\}$. De aquí, es fácil calcular $Ap(s, 5) = \{0, 7, 9, 16, 18\}$. Para ello podemos tomar los 5 elementos que hay tras el 14 que son los 5 primeros consecutivos en S, $\{14, 15, 16, 17, 18\}$, y a partir de ellos calculamos el mayor a tal que $14 - a * 5 \in S$, obteniendo el 9, y haciéndolo para todos se tiene que :

14 →	14-5=9
15 →	15-3*5=0
16 →	16
17 →	17-2*5=7
18 →	18

La aplicación inmediata es que si S es un semigrupo numérico y $n = \text{mín}\{s \in S \mid s \neq 0\}$, entonces $S \setminus S^* + S^* \subseteq Ap(S,n)^* \cup \{n\}$. También es claro que la igualdad no siempre se da como sucede en el ejemplo anterior.

COROLARIO 157. *Dado S un semigrupo numérico, el conjunto $S \setminus S^* + S^*$ es un sistema minimal de generadores y su cardinal es menor o igual que* $\text{mín}\{s \in S \mid s \neq 0\}$.

DEFINICIÓN 158. *Sea $S = \langle a_1, \ldots, a_n \rangle$ y supongamos el conjunto ordenado $\{a_1 < a_2 \cdots < a_n\}$ es su sistema minimal de generadores entonces a a_1 se le denomina* ***multiplicidad*** *de S y se denota por $m(S)$ y a n se le dice* ***dimensión de inmersión*** *de S y la notaremos $e(S)$.*

Por los resultados anteriores es claro que $e(S) \leq m(S)$. Cuando se da la igualdad se dice que S es un semigrupo con máxima dimensión de embebimiento o MED (maximal embedding dimension).

EJEMPLO 159. Dado $n \in \mathbb{N}$ el semigrupo $\{0, m, \rightarrow\}$ es un MED.

PROPOSICIÓN 160. *Sea S un MED, y sea $n = e(S) = m(S)$. Entonces $Ap(S,n)$ es su sistema minimal de generadores.*

DEMOSTRACIÓN. Es una consecuencia inmediata del Corolario 157. □

Conclusión: como hemos visto en este par de familias de semigrupos afines, los elementos que forman un sistema minimal de generadores, son aquellos minimales en un cierto sentido, que se ve más claramente en el caso de semigrupos numéricos con la introducción de los conjuntos de Apery. Los generadores estarán entre aquellos elementos del semigrupo que no se puedan escribir como suma de dos elementos del semigrupo no nulos. En el caso de los semigrupos afines completos, bastaba exigir la minimalidad puesto que esta condición de no escribirse como suma de otros dos viene implícita en la naturaleza de esta familia de semigrupos.

Esta condición de "no escribirse como suma de otros dos elementos no nulos" puede verse como una especie de "independencia lineal individual". Aquí, las soluciones de ecuaciones homogéneas con coeficientes en $\mathbb{N}$, no tienen cabida. Nunca $x_1a_1 + \cdots + a_nx_n = 0$ con todos los $a_i \in \mathbb{N}$ y también los $x_i \in \mathbb{N}$, salvo que todos los $x_i = 0$. Claramente esto no quiere decir, que cualquier elemento en S tiene una única escritura como combinación de los elementos del sistema minimal de generadores ya que por ejemplo en $S = \langle 5, 7, 9 \rangle$, se tiene que $14 = 2 \cdot 7 = 1 \cdot 5 + 1 \cdot 9$. Recordemos que este semigrupo era isomorfo a $\mathbb{Z}^3/\sim M$; donde M era el subgrupo de $\mathbb{Z}^3$ dado por $M = G(\{(4, 1, -3), (1, -2, 1)\})$.

Apéndice

12. Resultados interesantes

PROPOSICIÓN 161. *Sea U un subespacio de V, si $dim(U) = dim(V)$ entonces $U = V$.*

DEMOSTRACIÓN. Es claro que $U \subseteq V$ probemos el contrario. Sea $B_U = \{u_1, \ldots, u_n\}$ una base de U y sea $v \in V$ tal que $v \notin U$ por el teorema de ampliación de la base podríamos añadir v a B_U y tendríamos un conjunto linealmente independiente de $n+1$ vectores en un espacio de dimensión n lo que es una contradicción. Por tanto, $v \in U$. □

Obsérvese la importancia de que en el teorema de ampliación de la base para añadir un vector, la única condición es que sea linealmente independiente del resto.

COROLARIO 162. *Si v es un vector no nulo de un espacio vectorial V, v pertenece a una base de V.*

DEMOSTRACIÓN. Es consecuencia inmediata del teorema de extensión de una base. □

COROLARIO 163. *En todo sistema de generadores de un espacio vectorial V, existe un subconjunto suyo que es base.*

DEMOSTRACIÓN. Es otra escritura del teorema de extracción de una base. □

COROLARIO 164. *Sea V un espacio vectorial de dimensión n. Sea $X = \{e_1, \ldots, e_m\}$ un conjunto de vectores linealmente independiente (resp. sistema de generadores). Entonces $m \leq n$ (resp. $m \geq n$). Ademas se tiene la igualdad si y solamente si X es base de V.*

DEMOSTRACIÓN. Es consecuencia directa del Corolario 11. □

Consideramos $\mathbb{Z}$ que es un anillo, en lugar de $\mathbb{K}$ que es un cuerpo. ¿Cómo afecta esto a las proposiciones y definiciones anteriores?

13. Diferencias de los módulos con respecto a espacio vectorial

La Proposición 161 deja de cumplirse, veamos un ejemplo:

EJEMPLO 165. $(2\mathbb{Z})^2 \subseteq \mathbb{Z}^2$.
La dimensión de $2\mathbb{Z} \times 2\mathbb{Z}$ es dos y la dimensión de $\mathbb{Z} \times \mathbb{Z}$ también es dos. $2\mathbb{Z} \times 2\mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$ y no son el mismo espacio.

En el caso de monoides, consideremos $\langle 5, 7, 9\rangle \subset \mathbb{N}$ que tiene como sistema minimal de generadores a $\{5, 7, 9\}$ con tres elementos y contenido en $\mathbb{N}$ cuyo sistema minimal de generadores tiene un solo elemento: $\{1\}$.

El Corolario 162 deja de cumplirse, veamos un ejemplo:

Ejemplo 166. El $2 \in \mathbb{Z}$ y no pertenece a la base de $\mathbb{Z}$ que sería $\{1\}$ o $\{-1\}$.

En el caso de monoides, solo unos elementos concretos de cada monoide pueden ser los elementos del único sistema minimal de generadores.

El Corolario 163 deja de cumplirse, veamos un ejemplo:

Ejemplo 167. El conjunto $\{(1,2),(2,1),(1,-2)\}$ es sistema de generadores de $\mathbb{Z}\times\mathbb{Z}$ y si le quito algún vector deja de ser sistema de generadores. Sin embargo la cardinalidad de un conjunto linealmente independiente, sigue siendo menor que la cardinalidad de un sistema de generadores en el caso de $\mathbb{Z}$-módulos.

En el caso de monoides, no tiene mucho sentido hablar de independencia lineal, como se argumentó al final de capítulo anterior.

El Corolario 164 deja de cumplirse, veamos un ejemplo:

Ejemplo 168. El conjunto $\{(1,2),(2,1)\}$ es linealmente independiente en $\mathbb{Z}\times\mathbb{Z}$ pero no es base.

La Proposición 45 deja de cumplirse, veamos un ejemplo:

Ejemplo 169. Como $\mathbb{Z}_2 \times \mathbb{Z} \simeq \dfrac{\mathbb{Z}\times\mathbb{Z}}{2\mathbb{Z}\times\{0\}}$, si aplicamos la Proposición 45, tendríamos que $dim(\mathbb{Z}_2\times\mathbb{Z}) = dim(\mathbb{Z}\times\mathbb{Z}) - dim(2\mathbb{Z}\times\{0\}) = 2-1 = 1$, pero esto es imposible ya que entonces $\mathbb{Z}_2\times\mathbb{Z}$ tendría una base con un solo elemento y esto es imposible. Un sistema de generadores para $\mathbb{Z}_2\times\mathbb{Z}$ es $\{([1]_2,0),([0]_2,1)\}$ como ya sabemos. Fallaría la condición de independencia lineal ya que $2([1]_2,0) = ([0]_2,0)$.

Claramente, el resultado no se da en monoide, ni incluso cuando $S = \mathbb{N}^r/\sim_M$, considerando $rg(M)$ como $\mathbb{Z}$-módulo. Véase el Ejemplo 139.

Veamos un cuadro comparativo para $\mathbb{R}$ como $\mathbb{R}$-espacio vectorial, $\mathbb{Z}$ como $\mathbb{Z}$-módulo y $\mathbb{N}$ como monoide.

	$\mathbb{R}$	$\mathbb{Z}$	$\mathbb{N}$
Sistemas minimales de generadores	Infinitos $\{v\}$ con $v\neq 0$	Dos $\{1\}$ y $\{-1\}$	Uno $\{1\}$
Subespacios, submódulos y submonoides	Solamente hay dos llamados triviales $\{0\}$ y $\mathbb{R}$	Hay infinitos tantos como naturales $g\mathbb{Z}$ con $g\in\mathbb{N}$	Infinitos $g\mathbb{N}$ con $g\in\mathbb{N}$ numéricos etc.
Sistemas minimales de generadores en subesp.	No hay subespacios propios	Dos para cada $g\mathbb{Z}$, $\{g\}$ y $\{-g\}$	$\{g\}$ $\{a_1,\ldots,a_n\}$ etc
Bases	Cualquier conjunto sistemas de generadores linealm.independientes	Sólo en módulos libres sist.generadores y l.independiente	No tiene sentido. Hay sist.minimales de generadores
dimensiones de subespacios propios para $\mathbb{R}^n$,$\mathbb{Z}^n$ y $\mathbb{N}^n$	Siempre menores estrictas que n	Siempre menores que n vale $(=)$	Hay sistemas minimales de generadores con "muchos" elementos
cocientes en $\mathbb{R}^n$,$\mathbb{Z}^n$ y $\mathbb{N}^n$	Sobre subespacios y son esp. vectoriales	Sobre submódulos. Libres y torsión	Sobre congruencias

En la fila "sistemas minimales de generadores en subespacios", entiéndase subespacios, submódulos, submonoides.

Bibliografía

[1] P.M. Cohn, "Classic Algebra" *Wiley* (2000).

[2] E. Contejean, H. Devie, "An Eficient Incremental Algorithm for Solving Systems of Linear Diophantine Equations" *Information and Computation* 113(1) pag 143-172. (1994).

[3] L. Merino, E. Santos, "Álgebra lineal con metodos elementales" *Paraninfo.* (2006).

[4] J. C. Rosales, P. A. García-Sánchez, ''Finitely Generated Commutative Monoids" *Nova Science Publisher.* New York, (1999)

[5] J. C. Rosales, P. A. García-Sánchez. "Numerical Semigroups " *Developments in Mathematics* 20. Springer, New York, (2009).