Subsemigrupos de monoides conmutativos finitamente generados

Tesis Doctoral

Juan Ignacio García García

Departamento de Álgebra
Universidad de Granada
Granada (España)

Diciembre del 2000

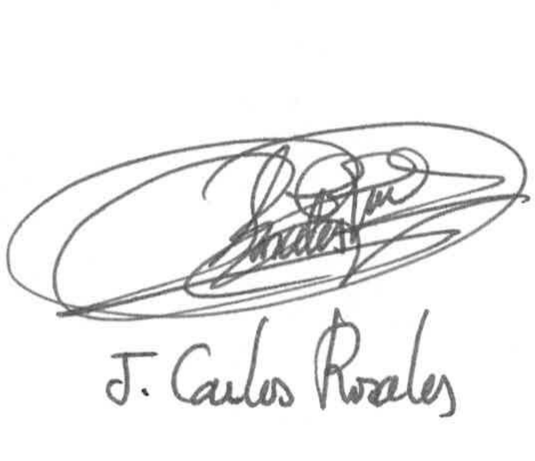
Subsemigrupos de monoides conmutativos finitamente generados

Memoria realizada por

D. Juan Ignacio García García

en el Departamento de Álgebra de la Universidad de Granada bajo la dirección de los Profesores Dr. José Carlos Rosales González y Dr. Pedro A. García Sánchez, profesores titulares de dicho departamento, para obtener el grado de Doctor en Ciencias Matemáticas por la Universidad de Granada.

V.B. Directores



Aspirante

Quisiera agradecer a mis directores, José Carlos Rosales y Pedro A. García Sánchez, por toda la ayuda recibida, el interés que más que de sobra han mostrado en que todo salga bien y todo lo que he aprendido de ellos.

Deseo también agradecer a mi familia todo el apoyo y ayuda que he recibido por su parte.

En especial, me gustaría darle las gracias a Marián, a quien dedico esta memoria, por haberme aguantado y haber estado siempre ahí para escucharme.

A Marián

Índice General

Introducción

El objeto de estudio de esta memoria son los subsemigrupos de monoides conmutativos finitamente generados. Todos los monoides y semigrupos que aparecerán en la misma serán conmutativos, por lo que en adelante omitiremos este adjectivo.

Los monoides finitamente generados han sido y siguen siendo objeto de gran cantidad de estudio. Entre otros podemos destacar los trabajos [**19**], [**30**] , [**33**], [**34**], [**53**] y [**56**]. Una de las razones que motivan dicho estudio es que dado un semigrupo se puede definir su anillo de semigrupo asociado. Resulta que las propiedades del anillo pueden determinarse vía las propiedades del semigrupo que lo define (véase por ejemplo [**30**]). Así, tomando como punto de partida los resultados proporcionados en esta memoria, podrían estudiarse anillos de semigrupos asociados a semigrupos no finitamente generados. De entre los trabajos que dan métodos para determinar propiedades de monoides destacamos [**65**] por ser éste un trabajo que sigue una línea similar a la seguida en esta memoria. Inspirados en él, hemos tenido siempre como objetivo el proporcionar algoritmos que solucionen todos los problemas que nos han ido surgiendo.

Gran parte del estudio de monoides finitamente generados se realiza en base a un resultado de Rédei. Ese resultado, cuya demostración puede encontrarse en [**56**], prueba que todo monoide finitamente generado tiene una presentación finita o equivalentemente, toda congruencia sobre $\mathbb{N}^p$ es finitamente generada (demostraciones más sencillas del mismo pueden encontrarse en [**40**] ó [**65**]). Así, al ser todo monoide finitamente generado isomorfo a un cociente de la forma $\mathbb{N}^p/\sigma$ y tener que la congruencia σ puede reconstruirse a partir de un subconjunto finito de $\mathbb{N}^p \times \mathbb{N}^p$, tenemos que todo monoide puede ser descrito a partir de un número finito de datos. Pero ocurre que en general no todo subsemigrupo de un monoide finitamente generado es necesariamente finitamente generado, por lo que esta forma de describir monoides finitamente generados no es válida para describir sus subsemigrupos (un ejemplo sencillo se tiene tomando en el monoide $(\mathbb{N}^2,+)$ el subconjunto $A = \{(x,y) \mid x \geq 1, y \in \mathbb{N}\}$; es fácil ver que $(A,+)$ es un subsemigrupo no finitamente generado de $(\mathbb{N}^2,+)$ y que en cambio éste último sí lo es). Así, las técnicas usadas para determinar propiedades de monoides finitamente generados no pueden usarse para estudiar propiedades de subsemigrupos de monoides finitamente generados.

De todo lo expuesto surge la primera pregunta: ¿cuándo un monoide finitamente generado tiene todos sus submonoides finitamente generados? De cumplirse esa condición, todos sus submonoides tendrían una presentación finita que podría ser usada

para determinar sus propiedades. Una reformulación del problema consiste en lo siguiente: dada una presentación de un monoide, ¿cómo podemos determinar si todos sus submonoides son finitamente generados? A los monoides que cumplan esa condición los llamaremos HFG-monoides (*hereditarily finitely generated monoides*) y la solución al problema se encuentra [**62**] y constituye el contenido del Capítulo 2. En él caracterizaremos las congruencias σ tales que su cociente $\mathbb{N}^p/\sigma$ sea un HFG-monoide y usando esa caracterización, obtendremos un algoritmo para decidir a partir de una presentación de un monoide finitamente generado si éste es o no un HFG-monoide.

En [**61**] el problema de estudiar subsemigrupos de monoides se aborda basándonse en los resultados dados por Tamura en [**79**] para la construcción de $\mathcal{N}$-semigrupos. Ese trabajo obtiene clases de monoides que se embeben en otra estructura parecida, pero con más propiedades, como son los grupos. Se consigue de esa forma una nueva clase de semigrupos llamados $\mathcal{N}$-semigrupos generalizados y cuya clase coincide con los semigrupos cancelativos, con al menos un elemento arquimediano que no son grupos. Además, a través de esa construcción clasificaremos y obtendremos importantes familias de semigrupos, donde una de ellas la forman los $\mathcal{N}$-semigrupos, semigrupos éstos muy estudiados (véase por ejemplo [**53**], [**79**], [**81**], [**82**]). Ejemplos de clases de semigrupos que clasificaremos son los monoides que no son grupos que se embeben en un grupo finitamente generado, los submonoides reducidos de grupos finitamente generados, los submonoides de $\mathbb{Z}^n$ y los submonoides finitamente generados de $\mathbb{N}^n$. Utilizando los resultados de [**61**], en [**60**] se estudian las extensiones racionales de $(\mathbb{Z},+)$ como una generalización de cuando este grupo se embebe en $\mathbb{R}$ ó $\mathbb{Q}$. Dicho estudio, que veremos en el Capítulo 4, se interesa especialmente en las extensiones racionales que son aquellas en las que el grupo de los enteros es isomorfo a un subgrupo de $(\mathbb{Q},+)$.

Las extensiones ideales fueron introducidas por Clifford en [**19**] y desde entonces han sido ampliamente estudiadas (véase por ejemplo [**53**] ó [**33**]). Al igual que en [**69**], en el Capítulo 5 caracterizaremos las extensiones ideales de grupos abelianos. Esas caracterizaciones nos darán un algoritmo para decidir si un monoide finitamente generado es o no una extensión ideal de un grupo abeliano. Como consecuencia de ese estudio obtendremos también un algoritmo para calcular, a partir de una presentación de un monoide, su conjunto de elementos idempotentes. Otro problema relacionado con el de las extensiones ideales, y en el que también juegan un papel fundamental los ideales, es el problema de determinar si un monoide es débilmente reductivo. En numerosas ocasiones estos monoides han sido objeto de estudio debido a que su envolvente de traslaciones forma una extensión ideal suya (véase por ejemplo [**42**], [**53**], [**55**], [**80**]). En el Capítulo 6 daremos un algoritmo para determinar, a partir de una presentación de un semigrupo, si éste es o no débilmente reductivo. Además, relacionaremos este tipo de semigrupos con los semigrupos arquimedianos y cancelativos. Esos resultados y el concepto de $\mathcal{N}$-semigrupo será fundamental para dar teoremas de estructura para semigrupos finitamente generados, arquimedianos y débilmente reductivos.

En [**68**] se prueba que todo submonoide de un monoide finitamente generado puede describirse a partir de un semigrupo afín y una congruencia de $\mathbb{N}^p$. Tomando como base ese trabajo en [**63**] se introduce un nuevo tipo de presentación para ideales principales de monoides finitamente generados y se dan métodos para probar propiedades de tales subsemigrupos usando ese nuevo tipo de presentación. En general, los ideales de semigrupos destacan por la sencilla forma con la que pueden ser descritos además de darnos numerosos ejemplos de semigrupos no finitamente generados. Existe gran cantidad de trabajos referentes a este tipo de semigrupos como son [**7**], [**8**], [**21**], [**35**]. Siguiendo las ideas antes mencionadas de [**63**] y [**68**], veremos como el concepto de presentación dado por Rédei puede extenderse de manera sencilla a los ideales de monoides finitamente generados. Es más, usaremos ese nuevo tipo de presentación de ideales para dar una serie de métodos que nos determinen las propiedades de un ideal a partir de una de sus presentaciones. Entre otros, daremos algoritmos para determinar cuando un ideal es cancelativo, grupo, separativo, etc. De esta forma tenemos que no sólo esa presentación nos servirá para obtener un ideal isomorfo al de partida, sino que además puede usarse para determinar sus propiedades tal y como se hace en [**65**] para monoides finitamente generados y en [**63**] para ideales principales.

No solamente está en nuestros objetivos el dar propiedades de un ideal dado, sino también el clasificarlos. Existen muchas similitudes entre la teoría de ideales de semigrupos y la teoría de ideales de anillos. Muchas definiciones y teoremas de la teoría de semigrupos tienen sus análogos en la teoría de anillos. Usando ese paralelismo y el concepto de topología de Zariski del espectro de un anillo, introduciremos el concepto de topología de Zariski del espectro de un semigrupo. Haciendo uso de esa topología y del retículo de componentes arquimedianas de un monoide, veremos como obtener los ideales radicales de un monoide y caracterizaremos los ideales primos de un monoide. Más recientemente, los problemas de factorización están siendo trasladados a un contexto más general como el de los semigrupos (véase [**14**], [**26**], [**35**] y [**49**]). Por este motivo nuevos e interesantes conceptos están apareciendo, entre ellos está el de elemento primario de un monoide y, relacionados con él, el de ideal primario e ideal irreducible. Normalmente, la existencia de descomposiciones de ideales en ideales irreducibles ha sido usada para probar la existencia de descomposiciones en ideales primarios (véase [**7**] y [**9**]). Parece que hasta [**39**] el estudio de los ideales irreducibles y la descomposición en estos ideales había sido casi olvidada. En el Capítulo 9 expondremos los resultados y métodos de [**71**] para obtener la descomposición de un ideal en irreducibles. Usando esos resultados generalizaremos los resultados de [**64**] y resolveremos el problema de determinar cuándo un ideal es primario, del que como consecuencia obtendremos un algoritmo para determinar cuándo un elemento es primario (todo ello siempre en monoides finitamente generados).

Relacionado tanto con los ideales como con los problemas de teoría de números en monoides presentamos a los monoides de ideales principales (MIP para abreviar). De nuevo, debido a las analogías entre la teoría de monoides y la de anillos (véase [**7**] ó [**78**]), el problema de caracterizar a este tipo de monoides no es la primera vez que se intenta abordar, por ejemplo en [**77**] se dan aproximaciones al mismo. Entre las

propiedades de estos monoides está la sencillez de los ideales que lo forman, pudiendose realizar a partir de [**63**] un estudio de sus propiedades, y el que en ellos podemos definir de manera natural el concepto de máximo común divisor. En [**70**] se da una caracterización de los monoides finitamente generados que cumple esa condición y además se proporciona un algoritmo para determinar, a partir de una presentación de un monoide, si éste es o no un MIP. En el Capítulo 11 veremos los métodos expuestos en ese trabajo e ilustraremos con algunos ejemplos el algoritmo que allí aparece.

Inspirados en los trabajos [**12**] y [**56**], Zaks introduce el concepto de dominio semifactorial. Con el objeto de medir la desviación de un dominio atómico de ser semifactorial, Valenza introduce en [**84**] el concepto de elasticidad. Desde entonces numerosos trabajos han aparecido en los cuales la elasticidad de un dominio es estudiada, véase por ejemplo [**1**], [**2**] y [**5**]. Como antes hemos mencionado, el concepto de factorización está siendo trasladado al contexto más general de los monoides. Estas ideas han dado lugar a una gran cantidad de trabajos donde, aparte de los anteriormente citados, tenemos [**3**], [**17**], [**27**], [**47**]. El uso del lenguaje de los monoides no sólo se debe a un intento de generalización sino además a un intento de simplificación y utilización de resultados tal y como se explica en [**3**]. Así, en los Capítulos 12 y 13 hacemos un estudio relativo a las descomposiciones de elementos en monoides. En el primero de ellos, resolveremos el problema del cálculo de los elementos irreducibles de un monoide y daremos un método para comprobar si un monoide es atómico. Por último, particularizamos los resultados de este capítulo a monoides cancelativos finitamente generados resolviendo para ese caso el cálculo de sus elementos irreducibles, determinación de si un monoide cancelativo es factorial y/o semifactorial y el cálculo de las descomposiciones de un elemento. El Capítulo 13 lo dedicaremos a dar un método para el cálculo de la elasticidad de un monoide. Además del algoritmo que presentamos, daremos métodos para comprobar si un monoide tiene elasticidad aceptable, para el cálculo los elementos irreducibles de un monoide atómico, cálculo de las factorizaciones de elementos de elasticidad finita y para comprobar si un monoide de elasticidad finita es factorial o semifactorial. Por último, como consecuencia del método expuesto para el cálculo de la elasticidad de un monoide mostraremos un método para el cálculo de la elasticidad de un monoide de Krull del que además, de manera inmediata, se puede deducir que la elasticidad de ese tipo de monoides es racional. Este último hecho era conocido y fue probado en [**2**] y [**29**], aunque la demostración que aquí damos usa técnicas totalmente diferentes y más asequibles. Lo que en general no se conocía era un método para el cálculo de la elasticidad de tal tipo de monoides, sólo se tenían aproximaciones como la que por ejemplo se tiene en [**4**] que resuelve el problema para tipos muy especiales de monoides de Krull. Estos resultados son los expuestos en el Capítulos 14.

CAPÍTULO 1

Preliminares

En este capítulo daremos una pequeña introducción sobre monoides conmutativos finitamente generados, con el objeto de que al lector le resulte más fácil y cómoda la lectura del resto de la memoria.

La mayor parte de las explicaciones, definiciones y resultados que damos en este capítulo se encuentran en [**65**].

1. Monoides y congruencias

Un **semigrupo** es un par $(S,+)$ con S un conjunto no vacío y $+$ una operación binaria sobre él verificando la propiedad asociativa y la conmutativa. Cuando en el conjunto S existe además un elemento 0 tal que $0+s=s$ para todo $s\in S$, decimos que $(S,+)$ es un **monoide**. Al elemento 0 se le llama el **elemento neutro** de S.

Denotemos por $\mathbb{N}$ y $\mathbb{Z}$ el conjunto de los naturales y el de los enteros, respectivamente. Dado un semigrupo S y B un subconjunto suyo, podemos definir el conjunto

$$\{\lambda_1 s_1+\cdots+\lambda_p s_p \mid p\neq 0,\ \lambda_i\in\mathbb{N}\setminus\{0\},\ s_i\in B \text{ para todo } i\in\{1,\ldots,p\}\}.$$

Claramente este conjunto es un subconjunto de S que además verifica ser junto con la operación de S un semigrupo, al que llamaremos el **subsemigrupo** de S generado por B, que denotaremos por $\langle B\rangle$. Si además S es un monoide, considerando todas las expresiones de la forma $0s$ con $s\in S$ iguales al elemento neutro de S, podemos definir el conjunto

$$\{\lambda_1 s_1+\cdots+\lambda_p s_p \mid p\neq 0,\ \lambda_i\in\mathbb{N},\ s_i\in B \text{ para todo } i\in\{1,\ldots,p\}\},$$

el cual verifica ser un submonoide de S y al que llamaremos el **submonoide** de S generado B. A este conjunto lo denotaremos también por $\langle B\rangle$.

Si un conjunto finito B es tal que el subsemigrupo que genera coincide con S, decimos que el semigrupo S es **finitamente generado** y que B es un **sistema de generadores** suyo. Si al prescindir de alguno de sus elementos ya no obtenemos el semigrupo S, o lo que es lo mismo, ningún elemento s_i de B puede ser expresado en función de los otros, decimos que B es un **sistema minimal de generadores** de S. Estos conceptos se trasladan a monoides, obteniendo las definiciones de **monoide finitamente generado** y **sistema minimal de generadores**.

Dados S_1, S_2 dos semigrupos diremos que una aplicación $f:S_1\to S_2$ es un **homomorfismo de semigrupos** si $f(a+b)=f(a)+f(b)$ para todo $a,b\in S_1$. Si además S_1 y S_2 son también monoides y $f(0)=0$, entonces la aplicación f es un **homomorfismo de monoides**.

Un ejemplo de homomorfismo de monoides, que nos va a ser de gran utilidad, lo describimos a continuación. El conjunto $\mathbb{N}^p$ junto con la suma coordenada a coordenada es un monoide. Dado S un monoide finitamente generado por $\{s_1, \ldots, s_p\}$, podemos definir la aplicación

$$\varphi : \mathbb{N}^p \to S,$$

$$\varphi(n_1, \ldots, n_p) = n_1 s_1 + \cdots + n_p s_p,$$

la cual es claramente sobreyectiva. A partir de esta aplicación definimos el siguiente conjunto

$$\sigma = \{(a, b) \in \mathbb{N}^p \times \mathbb{N}^p \mid \varphi(a) = \varphi(b)\}.$$

La relación binaria σ es una relación de equivalencia. Ahora bien, utilizando que φ es un homomorfismo de monoides, lo cual puede probarse fácilmente, se llega a que σ es una **congruencia**, esto es, siempre que $a\sigma b$ tenemos que $a + c\sigma a + c$ para todo $c \in \mathbb{N}^p$. Además dada σ una congruencia sobre $\mathbb{N}^p$, el cociente $\mathbb{N}^p/\sigma$ resulta ser un monoide con la operación que hereda de $\mathbb{N}^p$ (sus elementos son de la forma $[(a_1, \ldots, a_p)]_\sigma$ con $(a_1, \ldots, a_p) \in \mathbb{N}^p$). Así, podemos definir la aplicación

$$\overline{\varphi} : \mathbb{N}^p/\sigma \to S,$$

$$\overline{\varphi}([(a_1, \ldots, a_p)]_\sigma) = a_1 s_1 + \cdots + a_p s_p,$$

la cual resulta ser un isomorfismo de monoides. Podemos así enunciar el siguiente resultado.

PROPOSICIÓN 1.1. *Sea S un monoide finitamente generado. Entonces existen $p \in \mathbb{N}$ y σ un congruencia sobre $\mathbb{N}^p$ tales que S es isomorfo al monoide $\mathbb{N}^p/\sigma$.*

Además, si denotamos por e_i al elemento de $\mathbb{N}^p$ cuyas sus coordenadas son todas cero salvo la i-ésima que es igual a uno, un sistema de generadores del monoide $\mathbb{N}^p/\sigma$ es $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$.

2. Presentaciones finitas, problemas de palabras y eliminación de coordenadas en congruencias

Ya sabemos que todo monoide finitamente generado es isomorfo a uno de la forma $\mathbb{N}^p/\sigma$. Ahora bien, surge con este tipo de monoides un problema: ¿es posible manejar congruencias sobre $\mathbb{N}^p$ usando sólo un número finito de datos? La respuesta a esto es afirmativa, tal y como puede verse en [**56**] ó [**65**]. En ellos se prueba que para toda congruencia sobre $\mathbb{N}^p$ existen un número finito de elementos de $\mathbb{N}^p \times \mathbb{N}^p$ que la describen totalmente y a partir de los cuales se puede decidir si dos elementos $a, b \in \mathbb{N}^p$ están o no σ relacionados. Lo que se tiene es el siguiente resultado.

PROPOSICIÓN 1.2. *Sea σ una congruencia sobre $\mathbb{N}^p$. Entonces existe un subconjuto finito $\rho = \{(a_1, b_1), \ldots, (a_t, b_t)\}$ de $\mathbb{N}^p \times \mathbb{N}^p$ de forma que la menor congruencia que contiene a ρ coincide con σ.*

Démonos cuenta que todo subconjunto de $\mathbb{N}^p \times \mathbb{N}^p$ está contenido en la congruencia en la que todos los elementos están relacionados. Además es fácil probar que la intersección de dos congruencias es de nuevo una congruencia, por lo que siempre existirá la menor congruencia que contenga a un subconjunto ρ de $\mathbb{N}^p \times \mathbb{N}^p$. A esa congruencia la llamaremos la **congruencia generada** por ρ y la denotamos por $\langle\rho\rangle$. Además al conjunto ρ lo llamaremos una **presentación** del monoide $\mathbb{N}^p/\sigma$ (y de cualquiera isomorfo a él).

También dado ρ podemos preguntarnos cómo puede reconstruirse σ, o de otro modo, cómo se puede describir el conjunto σ a partir de ρ. Una forma de hacerlo nos la da la siguiente Proposición (ver [**56**] para más detalles).

PROPOSICIÓN 1.3. *Sea* ρ *un subconjunto de* $\mathbb{N}^p \times \mathbb{N}^p$. *Definimos*

$$\rho_0 = \rho \cup \{(b,a) \mid (a,b) \in \rho\} \cup \{(a,a) \mid a \in \mathbb{N}^p\},$$
$$\rho_1 = \{(v+u, w+u) \mid (v,w) \in \rho_0, u \in \mathbb{N}^p\}.$$

Entonces $\langle\rho\rangle$ *es el conjunto de pares* $(v,w) \in \mathbb{N}^p \times \mathbb{N}^p$ *tales que existe* $k \in \mathbb{N}$ *y* $v_1, \ldots, v_k \in \mathbb{N}^p$ *con* $v_1 = v, v_k = w$ *y* $(v_i, v_{i+1}) \in \rho_1$ *para todo* $1 \leq i \leq k-1$.

Nótese que en la proposición anterior ρ_0 es el cierre reflexivo-simétrico de ρ, ρ_1 hace que ρ_0 sea compatible con la suma y finalmente, el último paso es el cierre transitivo.

Ya sabemos cómo la congruencia σ, la cual determina en última instancia al monoide $\mathbb{N}^p/\sigma$, puede describirse de forma finita. El problema ahora es el siguiente: ¿cómo podemos saber cuando dos elementos $[(a_1, \ldots, a_p)]_\sigma, [(b_1, \ldots, b_p)]_\sigma \in \mathbb{N}^p/\sigma$ son el mismo elemento?, o lo que es lo mismo, ¿cómo ver si $a \sigma b$? Para ello haremos uso de los sistemas canónicos de generadores, los cuales decribimos a continuación.

Un **orden lineal admisible** sobre $\mathbb{N}^p$ es una relación de **orden** $\preceq$ (verifica las propiedades reflexiva, simétrica y transitiva) sobre $\mathbb{N}^p$ que cumple las siguientes condiciones:

(1) para todo $a \in \mathbb{N}^p$, $0 \preceq a$,
(2) para todo $a, b, c \in \mathbb{N}^p$, si $a \preceq b$, entonces $a + c \preceq b + c$,
(3) para todo $a, b \in \mathbb{N}^p$, $a \preceq b$ ó $b \preceq a$.

Obsérvese que esto es equivalente a que $\preceq$ sea un buen orden que contiene al orden usual de $\mathbb{N}^p$. Un ejemplo de orden lineal admisible es el orden lexicográfico, el cual se define como $a \preceq_{lex} b$ si y sólo si la menor coordenada no nula de $a - b$ es negativa; o el orden lexicográfico inverso definido por $a \preceq_{rlex} b$ si y sólo si la mayor coordenada no nula de $a - b$ es negativa.

Sea $\preceq$ un orden lineal admisible sobre $\mathbb{N}^p$. El conjunto

$$\rho = \{(a_1, b_1), \ldots, (a_k, b_k)\} \subseteq \mathbb{N}^p \times \mathbb{N}^p$$

es **reducido** con respecto a $\preceq$ si satisface las siguientes condiciones:

(1) $b_i \prec a_i$ para todo $i \in \{1, \ldots, k\}$,
(2) si $a_i - a_j \in \mathbb{N}^p$, entonces $i = j$,
(3) $b_j - a_i \notin \mathbb{N}^p$ para todo $i, j \in \{1, \ldots, k\}$.

Si $\rho = \{(a_1, b_1), \ldots, (a_k, b_k)\}$ es un subconjunto reducido de $\mathbb{N}^p \times \mathbb{N}^p$, podemos definir la aplicación $\mathrm{NF}_\rho : \mathbb{N}^p \to \mathbb{N}^p$ como sigue.

(1) Si $x - a_i \notin \mathbb{N}^p$ para todo $i \in \{1, \ldots, k\}$, entonces $\mathrm{NF}_\rho(x) = x$.
(2) Si $x - a_1 \notin \mathbb{N}^p, \ldots, x - a_i \notin \mathbb{N}^p$ y $x - a_{i+1} \in \mathbb{N}^p$, entonces $\mathrm{NF}_\rho(x) = \mathrm{NF}_\rho(x - a_{i+1} + b_{i+1})$.

Dada una congruencia σ sobre $\mathbb{N}^p$, definimos la aplicación μ asociada a σ con respecto a $\preceq$ como

$$\mu : \mathbb{N}^p \to \mathbb{N}^p,\ \mu(x) = \text{mínimo}_{\preceq}([x]_\sigma).$$

Un subconjunto reducido ρ de $\mathbb{N}^p \times \mathbb{N}^p$ es un **sistema canónico de generadores** de σ respecto de $\preceq$ si verifica que $\mathrm{NF}_\rho(x) = \mu(x)$ para todo $x \in \mathbb{N}^p$. Obsérvese que en ese caso tenemos que $x \sigma y$ si y sólo si $\mathrm{NF}_\rho(x) = \mathrm{NF}_\rho(y)$.

En [**65**, §6] aparece un método que calcula a partir de un sistema de generadores de una congruencia un sistema canónico de generadores para la misma con respecto a un orden lineal admisible dado.

Para finalizar esta sección sólo nos queda comentar otro problema que aparecera a menudo cuando manejemos sistemas de generadores de congruencias. Supongamos que ρ es un sistema de generadores de una congruencia σ sobre $\mathbb{N}^p$. Tomemos $A = \{i_1, \ldots, i_r\} \subsetneq \{1, \ldots, p\}$ y definamos σ_A por

$$(a_{i_1}, \ldots, a_{i_r}) \sigma_A (b_{i_1}, \ldots, b_{i_r}) \text{ si y sólo si } a_{i_1} e_{i_1} + \cdots + a_{i_1} e_{i_1} \sigma b_{i_1} e_{i_1} + \cdots + b_{i_r} e_{i_r}.$$

Es fácil probar que σ_A es una congruencia sobre $\mathbb{N}^r$. El problema es cómo a partir de ρ podemos calcular un sistema de generadores de σ_A. A este problema se le conoce como el problema de **eliminación de coordenadas** (en este caso las coordenadas a eliminar son $\{1, \ldots, p\} \setminus A$). Para simplificar supongamos que $A = \{r+1, \ldots, p\}$ (en caso contrario podemos reordenar las variables). Supongamos que

$$\rho = \{(a_1, b_1), \ldots, (a_t, b_t)\}$$

es un sistema canónico de generadores de σ con respecto al orden $\preceq_{rlex}$ (si no lo es lo podemos calcular a partir de ρ) y que

$$(a_i, b_i) = ((a_{i1}, \ldots, a_{ip}), (b_{i1}, \ldots, b_{ip})).$$

Definimos

$$\rho' = \{((a_{i1}, \ldots, a_{ir}), (b_{i1}, \ldots, b_{ir})) \mid ((a_{i1}, \ldots, a_{ir}, 0, \ldots, 0), (b_{i1}, \ldots, b_{ir}, 0, \ldots, 0)) \in \rho\}.$$

En [**65**, §14], se prueba que el conjunto ρ' es un sistema de generadores de la congruencia σ_A.

3. Monoides cancelativos

Prestamos ahora atención a un tipo especial de monoides: los llamados monoides cancelativos. Un monoide S es **cancelativo** si siempre que $a + c = b + c$ con $a, b, c \in S$, se tiene que $a = b$. Un ejemplo de monoide cancelativo es $(\mathbb{N}^p, +)$.

Si $\mathbb{N}^p/\sigma$ es un monoide con $\rho = \{(a_1,b_1),\ldots,(a_r,b_r)\}$ un sistema de generadores de σ, podemos definir

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

Puede probarse que el conjunto M_σ es un subgrupo de $\mathbb{Z}^p$ y que $\{a_1-b_1,\ldots,a_p-b_p\}$ es un sistema de generadores suyo. Recíprocamente, si M es un subgrupo de $\mathbb{Z}^p$ definimos $\sim_M$ la congruencia dada por

$$a \sim_M b \text{ si y sólo si } a-b \in M.$$

A partir de σ podemos definir la congruencia $\sim_{M_\sigma}$. El siguiente resultado nos dice como se relacionan estas dos congruencias.

PROPOSICIÓN 1.4. *Sea σ una congruencia sobre $\mathbb{N}^p$.*

- *Si $a\sigma b$, entonces $a \sim_{M_\sigma} b$, o lo que es lo mismo, $\sigma \subseteq \sim_{M_\sigma}$.*
- *El monoide $\mathbb{N}^p/\sigma$ es cancelativo si y sólo si $\sigma = \sim_{M_\sigma}$.*
- *Para todo $a,b \in \mathbb{N}^p$ tales que $a \sim_{M_\sigma} b$, existe $c \in \mathbb{N}^p$ tal que $a+c\sigma b+c$.*

En [**65**, §8] se dan métodos para comprobar a partir de una presentación de un monoide si éste es o no cancelativo. Nótese por tanto que todo monoide finitamente generado y cancelativo es de la forma $\mathbb{N}^p/\sim_M$ para algún $p \in \mathbb{N}$ y M subgrupo de $\mathbb{Z}^p$.

Otra de las propiedades que cumplen estos monoides es que todos ellos son siempre isomorfos a algún submonoide de un grupo abeliano. En el caso de los finitamente generados todos se pueden embeber dentro de un grupo abeliano finitamente generado, es decir, un grupo de la forma $\mathbb{Z}^t \times \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$ con $d_1,\ldots,d_s \in \mathbb{N}\setminus\{0\}$ (véase [**65**, §3]; $\mathbb{N}^p/\sim_M \hookrightarrow \mathbb{Z}^p/M$, $d_1,\ldots,d_s$ son los factores invariantes de M). Esto nos permite, siempre que S sea un monoide cancelativo, definir el **grupo de cocientes de** S como el menor grupo, salvo isomorfismos, con respecto a la inclusión que lo contiene. De esta forma podremos hacer de expresiones tales como $x-y$, $0x=0$, $x+0$, $x-0$, etc.

4. Unidades, elementos arquimedianos e idempotentes

Dentro de un monoide, podemos encontrar elementos que verifican propiedades especiales. Para el desarrollo de esta memoria nos interesan destacar los siguientes: unidades, elementos arquimedianos y elementos idempotentes.

Dado un monoide S, un elemento $u \in S$ diremos que es una **unidad** si existe otro elemento $u' \in S$ tal que $u+u'=0$. Al elemento u' se le llama el **inverso** del elemento u y es fácil probar que caso de que exista es único. Si consideramos el conjunto

$$\mathcal{U}(S) = \{u \in S \mid u \text{ es una unidad de } S\},$$

resulta que este conjunto es un submonoide de S y que $(\mathcal{U}(S),+)$ es un grupo. A este grupo se le conoce como el **grupo de unidades** de S. Cuando en un monoide S tenemos que $\mathcal{U}(S)=\{0\}$, decimos que S es **reducido**.

Surge ahora el problema de determinar si un determinado monoide es o no reducido y caso de no serlo, cómo calcular su grupo de unidades.

PROPOSICIÓN 1.5. *Dado un monoide S con sistema de generadores $\{s_1,\dots,s_p\}$. Entonces*

$$\mathcal{U}(S) = \langle \{s_i \mid s_i \text{ es unidad de } S\} \rangle.$$

Por tanto en el monoide $\mathbb{N}^p/\sigma$ sólo hemos de determinar las unidades que hay en $\{[e_1]_\sigma,\dots,[e_p]_\sigma\}$ para tener un sistema de generadores de su grupo de unidades. Un algoritmo para hacer este cálculo usando sistemas canónicos de generadores se puede encontrar en [**65**, §6].

El siguiente tipo de elemento notable de un monoide es el de elemento arquimediano. En todo semigrupo S (no necesariamente finitamente generado) podemos definir la relación $\leq$ de la siguiente forma, dados dos elemento $a,b \in S$, diremos que $a \leq b$ si y sólo si $b = a+c$ para algún $c \in S$. Un elemento $a \in S$ es **arquimediano** si para todo elemento $b \in S$ existe $k \in \mathbb{N}$ tal que $ka \geq b$. Definimos la relación $\mathcal{N}$ de la siguiente forma

$$a\mathcal{N}b \text{ si existen } k,l \in \mathbb{N}\setminus\{0\} \text{ tales que } ka \geq b \text{ y } lb \geq a.$$

Es fácil comprobar que $\mathcal{N}$ es una congruencia, por lo que podemos definir el conjunto $S/\mathcal{N}$, el cual junto con la operación que hereda de S es un monoide. Esto hace que en $S/\mathcal{N}$ podamos definir una relación $\leq$ como la definida para S. Resulta que en general el conjunto $S/\mathcal{N}$ junto con $\leq$ es un **semirretículo**, en este caso superior, pues para todo par de elementos existe un supremo que es precisamente la suma de ambos (esto equivale a que el conjunto $S/\mathcal{N}$ junto con la operación que hereda de S sea un semigrupo donde todos sus elementos son idempotentes). Cuando el semigrupo S es un monoide finitamente generado el par $(S/\mathcal{N},\leq)$ es un **retículo**, esto es, $\leq$ es un orden tal que para todo par de elementos $a,b \in S/\mathcal{N}$ existen tanto su supremo como su ínfimo. En general nos referiremos a $S/\mathcal{N}$ como al **semirretículo asociado** a S. Además, tal y como se ve en [**65**, §13], si S tiene un sistema de generadores con p elementos (por ejemplo si $S \cong \mathbb{N}^p/\sigma$), entonces $S/\mathcal{N}$ tiene a lo sumo 2^p elementos. A los elementos de $S/\mathcal{N}$ los llamamos **componentes arquimedianas** de S. Cuando S es un monoide cabe destacar de entre éstas a $[0]_\mathcal{N}$, que coincide con el conjunto $\mathcal{U}(S)$. Si el conjunto $S/\mathcal{N}$ lo forma un solo elemento el semigrupo S se dice que es un **semigrupo arquimediano**.

Dado $a = (a_1,\dots,a_p) \in \mathbb{N}^p$, definimos su **soporte** como

$$\operatorname{Supp}(a) = \{i \in \{1,\dots,p\} \mid a_i \neq 0\}.$$

Considerando σ una congruencia sobre $\mathbb{N}^p$ y $\mathbb{N}^p/\sigma$ un monoide finitamente generado, es fácil probar que si $a,b \in \mathbb{N}^p$ y $\operatorname{Supp}(a) = \operatorname{Supp}(b)$, entonces $[a]_\sigma \mathcal{N} [b]_\sigma$. Además, cada componente arquimediana se puede determinar de la siguiente forma (véase [**65**, §13]).

PROPOSICIÓN 1.6. *Sea C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces existen $A_1^C,\dots,A_s^C,A^C \subseteq \{1,\dots,p\}$ tales que $A^C = \bigcup_{i=1}^p A_i^C$ y*

$$C = \{[x]_\sigma \mid x \in \mathbb{N}^p \text{ y existe } i \in \{1,\dots,s\} \text{ tal que } A_i^c \subseteq \operatorname{Supp}(x) \subseteq A^C\}.$$

En [**65**, §13] se da un método algorítmico que determina de esta forma cada una de las componentes arquimedianas de un monoide a partir de cualquiera de sus presentaciones (lo que devuelve ese algoritmo es para cada una de las componentes arquimedianas son los conjuntos A_i^C y el A^C). Otra cosa que podemos deducir del anterior resultado es que la suma de dos elementos de una misma componente arquimediana nunca será de soporte mayor que el correspodiente conjunto A^C, es por ello que las componentes arquimedianas de un monoide son subsemigrupos suyos. Al conjunto A^C lo llamaremos $\mathrm{Supp}(C)$.

El último tipo de elemento del que hacemos mención es el de elemento idempotente. Decimos que $s \in S$ es **idempotente** si $s+s=s$. Basta observar la definición para darse cuenta que en un monoide cancelativo sólo hay un elemento idempotente, su elemento neutro. Otra de las propiedades que usaremos de este tipo de elementos es que en toda componente arquimediana hay a lo sumo un elemento idempotente (véase [**33**]).

Para finalizar con esta sección damos la definición de un tipo de semigrupo que aparecerá con frecuencia, y en el cual se ven reflejados parte de los conceptos vistos hasta ahora. Decimos que un semigrupo S es un **$\mathcal{N}$-semigrupo** si es cancelativo, arquimediano y no tiene elementos idempotentes.

5. Ideales

Un subconjunto I de un monoide S es un **ideal** si para todo $a \in I$ y para todo $s \in S$ se tiene que $a+s \in I$. Ya que la suma de dos elementos cualesquiera de I de nuevo pertenece a I, todo ideal de S es un subsemigrupo suyo. Otra característica importante que cumplen los ideales nos la da el siguiente resultado (ver [**30**] para más detalles).

PROPOSICIÓN 1.7. *Sea S un monoide finitamente generado e I un ideal suyo. Entonces existen $a_1,\ldots,a_t \in I$ tales que $I=\{a_i+s \mid i \in \{1,\ldots,t\},\ s \in S\}$.*

El anterior resultado nos dice así que todo ideal de un monoide finitamente generado está definido a partir de un número finito de elementos. Diremos en este caso que el ideal I está generado por el conjunto $\{m_1,\ldots,m_t\}$ (esto no implica que I sea finitamente generado como semigrupo). Recíprocamente, dado un subconjunto finito de elementos $A=\{m_1,\ldots,m_t\}$ de un monoide S podemos definir $I=\{m_i+s \mid i \in \{1,\ldots,t\},\ s \in S\}$. Como cabía esperar este conjunto I es un ideal de S y el conjunto A es un sistema de generadores suyo. En general, al ideal generado por subconjunto de elementos A de un monoide S lo denotaremos por $A+S$.

Asociado a un ideal I de un monoide $S \cong \mathbb{N}^p/\sigma$ con ρ un sistema de generadores de σ, podemos definir la siguiente relación

$$a\mathcal{R}_I b \text{ si y sólo si } a,b \in I \text{ ó } a=b,$$

conocida como la **congruencia de Rees** asociada al ideal I (véase [**30**] más información). Obtenemos de esta forma el monoide $S/\mathcal{R}_I$. Supongamos que I está generado como ideal por $\{[m_1]_\sigma,\ldots,[m_t]_\sigma\}$ y tomemos

$$\rho_{\mathcal{R}_I}=\{(m_1,m_2),\ldots,(m_1,m_t),(m_1+e_1,m_1),\ldots,(m_1+e_p,m_1)\}\cup\rho.$$

Puede probarse que el conjunto $\rho_{\mathcal{R}_I}$ es una presentación de $S/\mathcal{R}_I$. A la congruencia generada por $\rho_{\mathcal{R}_I}$ la denotaremos por $\sigma_{\mathcal{R}_I}$.

Por último, nos gustaría señalar que los ideales de monoides pueden clasificarse en diferentes tipos (éstos están inspirados, al igual que la definición de ideal, en las definiciones de Teoría de Anillos). Un primer tipo que estudiaremos serán los ideales **primos**. Estos ideales son los que cumplen que dados $a, b \in S$ tales que $a+b \in I$ y $a \notin I$, entonces $b \in I$. Tras éstos veremos los radicales. Un ideal I es **radical** si siempre que existe $k \in \mathbb{N}$ y $s \in S$ tales que $ks \in I$, entonces $s \in I$. Parecida condición es la que ha de cumplir un ideal para ser **primario**; esta dice que si $x+y \in I$ y $x \notin I$, entonces existe $k \in \mathbb{N}\setminus\{0\}$ tal que $ky \in I$. A los ideales primarios les dedicaremos todo un capítulo, al igual que a los ideales **irreducibles** que son aquellos ideales I para los que no existen ideales J, K de S que lo contengan propiamente y verifique además que $I = J \cap K$.

CAPÍTULO 2

Monoides Commutativos Hereditariamente Finitamente Generados

Diremos que un monoide S es un **HFG-monoide** (*hereditarily finitely generated monoid*) si todo submonoide H de S es finitamente generado. Por ejemplo, todo monoide con un número finito de elementos es un HFG-monoide. Además, existen monoides con un número no finito de elementos que son HFG-monoides, es el caso de $\mathbb{N}$. Claramente, todo HFG-monoide es finitamente generado, pero no es verdad que todo monoide finitamente generado sea un HFG-monoide, así $\mathbb{N}\times\mathbb{N}$ es finitamente generado y $H=\{(x,y)\in\mathbb{N}\times\mathbb{N}\mid x\geq 1\}$ no lo es. El principal objetivo de este capítulo es caracterizar las congruencia σ sobre $\mathbb{N}^p$ tales que $\mathbb{N}^p/\sigma$ es un HFG-monoide. Esta caracterización se establece en el Teorema 2.7 de la Sección 1, la cual está dedicada a probar este resultado. En la siguiente sección, veremos cómo puede determinarse algorítmicamente, a partir de una presentación de σ, si $\mathbb{N}^p/\sigma$ es o no un HFG-monoide. Finalmente, en la Sección 3 aplicamos los resultados de las secciones anteriores al caso cancelativo.

Los contenidos de este capítulo pueden ser encontrados en [**62**].

1. Teorema Principal

Sea σ una congruencia sobre $\mathbb{N}^p$. La siguiente proposición da una condición necesaria para que $\mathbb{N}^p/\sigma$ sea un HFG-monoide.

Decimos que $(a_1,\ldots,a_p)\sigma(b_1,\ldots,b_p)$ es una relación no trivial si y sólo si $(a_1,\ldots,a_p)\neq(b_1,\ldots,b_p)$.

PROPOSICIÓN 2.1. *Sea $\mathbb{N}^p/\sigma$ un HFG-monoide. Entonces para todo $(i,j)\in\{1,2,\ldots,n\}\times\{1,2,\ldots,n\}$ con $i\neq j$, existe una relación no trivial de la forma $(a_{(i,j)}e_i+(b_{(i,j)}+1)e_j)\sigma(c_{(i,j)}e_i+e_j)$ con $a_{(i,j)},b_{(i,j)},c_{(i,j)}\in\mathbb{N}$.*

DEMOSTRACIÓN. Sea $H=\{[xe_i+ye_j]_\sigma\mid x,y\in\mathbb{N},\ y\geq 1\}\cup\{[0]_\sigma\}$. Claramente H es un submonoide de $\mathbb{N}^p/\sigma$ y por tanto es finitamente generado, de donde deducimos que al menos uno de los siguientes enunciados es cierto:

- $\{[xe_i+e_j]_\sigma\mid x\in\mathbb{N}\}$ es un conjunto finito.
- En $\mathbb{N}^p/\sigma$ existe una igualdad $[pe_i+qe_j]_\sigma+[re_i+se_j]_\sigma=[xe_i+e_j]_\sigma$ con $q,s\in\mathbb{N}\setminus\{0\}$.

En ambos casos las proposición es cierta. □

Nuestro principal objetivo es probar el recíproco de la la proposición anterior. Esto lo probaremos en el Teorema 2.7. Para ello necesitamos probar antes algunos resultados.

LEMA 2.2. *Sea* σ *una congruencia sobre* $\mathbb{N}^p$ *y*

$$\rho = \{((a_{11},\ldots,a_{1p}),(b_{11},\ldots,b_{1p})),\ldots,((a_{t1},\ldots,a_{tp}),(b_{t1},\ldots,b_{tp}))\} \subseteq \mathbb{N}^p \times \mathbb{N}^p$$

un sistema canónico de generadores suyo. Si $(ae_i + be_j)\sigma(ce_i + de_j)$ *es una relación no trivial de* σ*, entonces existe* $r \in \{1,\ldots,t\}$ *tal que*

$$\begin{gathered} a_{r1} = 0,\ldots,a_{ri-1} = 0, a_{ri} \leq \max\{a,c\}, \\ a_{ri+1} = 0,\ldots,a_{rj-1} = 0, \\ a_{rj} \leq \max\{b,d\}, a_{rj+1} = 0,\ldots,a_{rn} = 0. \end{gathered}$$

DEMOSTRACIÓN. Tenemos que $(ae_i + be_j)\sigma(ce_i + de_j)$ es una relación no trivial. Entonces $ae_i + be_j \neq ce_i + de_j$, y por tanto $\mathrm{NF}_\rho(ae_i + be_j) \neq ae_i + be_j$ ó $\mathrm{NF}_\rho(ce_i + de_j) \neq ce_i + de_j$. Supongamos que $\mathrm{NF}_\rho(ae_i + be_j) \neq ae_i + be_j$. Usando ahora la definición de NF_ρ, tenemos que existe $r \in \{1,\ldots,t\}$ tal que $a_{r1} = 0,\ldots,a_{ri-1} = 0$, $a_{ri} \leq a$, $a_{ri+1} = 0,\ldots,a_{rj-1} = 0,\ldots,a_{rj} \leq b$, $a_{rj+1} = 0,\ldots,a_{rn} = 0$. □

LEMA 2.3. *Supongamos que para todo* $\{i,j\} \subseteq \{1,\ldots,n\}$ *con* $i \neq j$ *existe una relación no trivial* $(a_{\{i,j\}}e_i + b_{\{i,j\}}e_j)\sigma(c_{\{i,j\}}e_i + d_{\{i,j\}}e_j)$*. Sean*

$$m_1 = \max\{a_{11},\ldots,a_{t1}\},\ldots,m_n = \max\{a_{1n},\ldots,a_{tn}\}.$$

Dados $x_1,\ldots,x_n \in \mathbb{N}$*, si para algún* $i \neq j$ *tenemos que* $x_i \geq m_i$ *y* $x_j \geq m_j$*, entonces* $x_1e_1 \cdots + x_pe_p \notin \mathrm{Im}(\mathrm{NF}_\rho)$.

DEMOSTRACIÓN. Por el Lema 2.2 existe un elemento en ρ de la forma

$$(a_{ri}e_i + a_{rj}e_j, b_{r1}e_1 + \cdots + b_{rn}e_n).$$

Además tenemos que $x_i \geq m_i \geq a_{ri}$ y que $x_j \geq m_j \geq a_{rj}$. Lo cual implica que

$$\mathrm{NF}_\rho(x_1e_1 + \ldots + x_ne_n) \neq x_1e_1 + \cdots + x_ne_n.$$

□

Para todo elemento $x \in \mathbb{N}^p$ el conjunto $\mathrm{Im}(\mathrm{NF}_\rho)$ contiene un único elemento $\mathrm{NF}_\rho(x)$ relacionado con él. Esto implica que el conjunto cociente $\mathbb{N}^p/\sigma$ es igual a

$$\{[x_1e_1 + \cdots + x_pe_p]_\sigma \mid x_1e_1 + \cdots + x_ne_n \in \mathrm{Im}(\mathrm{NF}_\rho)\}.$$

Además, bajo las hipótesis del lema anterior tenemos que $\mathbb{N}^p/\sigma = A_1 \cup A_2 \cup \ldots \cup A_n$ donde:

$$\begin{aligned} A_1 &= \{[x_1e_1 + \cdots + x_pe_p]_\sigma \mid x_1 \in \mathbb{N}, x_2 < m_2,\ldots,x_p < m_p\}, \\ A_2 &= \{[x_1e_1 + \cdots + x_pe_p]_\sigma \mid x_1 < m_1, x_2 \in \mathbb{N}, x_3 < m_3,\ldots,x_p < m_p\}, \\ &\vdots \\ A_p &= \{[x_1e_1 + \cdots + x_pe_p]_\sigma \mid x_1 < m_1,\ldots,x_{p-1} < m_{p-1}, x_p \in \mathbb{N}\}. \end{aligned}$$

Cada conjunto A_i puede ser expresado de la forma siguiente:

$$A_1 = \bigcup_{(d_2,\ldots,d_p)\in\{0,\ldots,m_2-1\}\times\cdots\times\{0,\ldots,m_p-1\}} A^1_{(d_2,\ldots,d_p)}$$
$$\text{donde } A^1_{(d_2,\ldots,d_p)} = \{[xe_1 + d_2e_2 + \cdots + d_pe_p]_\sigma \mid x \in \mathbb{N}\},$$
$$A_2 = \bigcup_{(d_1,,d_3\ldots,d_p)\in\{0,\ldots,m_1-1\}\times\{0,\ldots,m_3-1\}\times\cdots\times\{0,\ldots,m_p-1\}} A^2_{(d_1,d_3,\ldots,d_p)}$$
$$\text{donde } A^2_{(d_1,d_3,\ldots,d_n)} = \{[d_1e_1 + xe_2 + d_3e_3 + \cdots + d_pe_p]_\sigma \mid x \in \mathbb{N}\},$$
$$\vdots$$
$$A_p = \bigcup_{(d_1,\ldots,d_{p-1})\in\{0,\ldots,m_1-1\}\times\cdots\times\{0,\ldots,m_{p-1}-1\}} A^p_{(d_1,\ldots,d_{p-1})}$$
$$\text{donde } A^p_{(d_1,\ldots,d_{p-1})} = \{[d_1e_1 + \cdots + d^p_{p-1}e_{p-1} + xe_p]_\sigma \mid x \in \mathbb{N}\}.$$

Así tenemos que $\mathbb{N}^p/\sigma$ puede ser expresado como una unión finita de conjuntos de la forma $A^i_{(d_1,\ldots,d_p)}$, los cuales están formados por σ-clases de elementos con todos sus coeficientes fijos excepto el i-ésimo que es variable. Estos conjuntos jugarán un papel importante en la demostración del Teorema 2.7 ya que en él se probará que bajo ciertas hipótesis, la intersección de todo submonoide H de $\mathbb{N}^p/\sigma$ con estos conjuntos puede ser generado finitamente.

LEMA 2.4. *Consideremos las mismas hipótesis que en el Lema 2.3. Si existe una relación no trivial de la forma* $(he_1+e_i)\sigma(ke_1+e_i)$ *para algún* $i \in \{2,\ldots,n\}$, *entonces* $A^1_{(d_2,\ldots,d_n)}$ *es finito ó* $d_i = 0$.

DEMOSTRACIÓN. Supongamos que $(he_1+e_i)\sigma(ke_1+e_i)$ es una relación no trivial con $h > k$. Si $d_i \neq 0$, entonces para todo $[xe_1 + d_2e_2 + \ldots + d_ne_n]_\sigma \in A^1_{(d_2,\ldots,d_n)}$ con $x > h$, aplicando la sustitución $he_1 + e_i \to ke_1 + e_i$, podemos encontrar un elemento $ye_1 + d_2e_2 + \cdots + d_ne_n$ con $y < h$ y tal que $[xe_1 + d_2e_2 + \cdots + d_ne_n]_\sigma = [ye_1 + d_2e_2 + \cdots + d_ne_n]_\sigma$. Por tanto $A^1_{(d_2,\ldots,d_n)} = \{[xe_1 + d_2e_2 + \cdots + d_ne_n]_\sigma \mid x < h\}$, el cual es un conjunto finito. □

LEMA 2.5. *Bajo las mismas hipotesis del Lema 2.3, si* σ *tiene las siguientes relaciones no triviales*

$$(a_2e_1 + (b_2+1)e_2)\sigma(c_2e_1 + e_2),$$
$$(a_3e_1 + (b_3+1)e_3)\sigma(c_3e_1 + e_3),$$
$$\vdots$$
$$(a_pe_1 + (b_p+1)e_p)\sigma(c_pe_1 + e_p),$$

$A^1_{(d_2,\ldots,d_p)}$ *no es finito y* $(d_2,\ldots,d_p) \neq (0,\ldots,0)$, *entonces:*

(1) Existen $N,k,y \in \mathbb{N}\setminus\{0\}$ *tal que si* $x \geq N$, *entonces*

$$((xe_1 + d_2e_2 + \cdots + d_pe_p) + k(xe_1 + d_2e_2 + \cdots + d_pe_p))\sigma$$
$$((x+y)e_1 + d_2e_2 + \cdots + d_pe_p).$$

(2) Sea $x \in \mathbb{N}$ *verificando la condición anterior. Si tomamos* $z \geq x$ *y* $a \in \mathbb{N}$, *entonces*

$$((ze_1 + d_2e_2 + \cdots + d_pe_p) + ak(xe_1 + d_2e_2 + \cdots + d_pe_p))\sigma$$
$$((z+ay)e_1 + d_2e_2 + \cdots + d_pe_p).$$

DEMOSTRACIÓN.

(1) Supongamos que $A^1_{(d_2,\ldots,d_p)}$ no es finito. Por el Lema 2.4 tenemos que si $b_i = 0$, entonces $d_i = 0$. Al ser $(d_2,\ldots,d_p) \neq (0,\ldots,0)$, deducimos que existe $i \in \{2,\ldots,p\}$ tal que $b_i \neq 0$. Supongamos que $b_2,\ldots,b_r \neq 0$ y $b_{r+1} = \ldots = b_p = 0$. Tomemos $k = b_2 \cdots b_r$. Utilizando la sustitución $a_2e_1 + (b_2+1)e_2 \to c_2e_1 + e_2$, a partir de

$$(k+1)xe_1 + (k+1)d_2e_2 + \cdots + (k+1)d_pe_p$$

obtenemos el elemento

$$((k+1)x - a_2 + c_2)e_1 + ((k+1)d_2 - b_2)e_2 + (k+1)d_3e_3 + \cdots + (k+1)d_pe_p.$$

Tras realizar p_2 veces la anterior sustitución nos queda

$$((k+1)x + p_2(-a_2+c_2))e_1 + ((k+1)d_2 - p_2b_2)e_2 + (k+1)d_3e_3 + \cdots + (k+1)d_pe_p.$$

Tomando ahora $p_2 = b_3 \cdots b_r d_2$ tenemos el elemento $(k+1)d_2 - p_2b_2 = d_2$. Claramente si $x > p_2a_2$, entonces podemos realizar las sustituciones anteriores. Repetiendo este mismo proceso en el resto de coordenadas y tomando x lo suficientemente grande (para poder realizar las sustituciones), obtenemos el que el resultado es cierto.

(2) Si $z \geq x$ y $a \in \mathbb{N}\setminus\{0\}$, entonces

$$\begin{gathered}
ze_1 + d_2e_2 + \ldots + d_pe_p + ak(xe_1 + d_2e_2 + \ldots d_pe_p) = \\
(z-x)e_1 + xe_1 + d_2e_2 + \ldots + d_pe_p + k(xe_1 + d_2e_2 + \ldots + d_pe_p) + \\
(a-1)k(xe_1 + d_2e_2 + \ldots + d_pe_p)\ \sigma \\
(z-x)e_1 + (x+y)e_1 + d_2e_2 + \ldots + d_pe_p + (a-1)k(xe_1 + d_2e_2 + \ldots + d_pe_p) = \\
(z+y)e_1 + d_2e_2 + \ldots + d_pe_p + (a-1)k(xe_1 + d_2e_2 + \ldots + d_pe_p).
\end{gathered}$$

Repitiendo este proceso tantas veces como sea necesario, obtenemos el resultado deseado.

□

LEMA 2.6. *Bajo las mismas hipótesis que en el Lema 2.3, supongamos que las siguientes relaciones son no triviales en* σ

$$\begin{gathered}
(a_2e_1 + (b_2+1)e_2)\ \sigma\ (c_2e_1 + e_2), \\
(a_3e_1 + (b_3+1)e_3)\ \sigma\ (c_3e_1 + e_3), \\
\vdots \\
(a_pe_1 + (b_p+1)e_p)\ \sigma\ (c_pe_1 + e_p),
\end{gathered}$$

y sea H *un submonoide de* $\mathbb{N}^p/\sigma$. *Entonces existen* $x_1,\ldots,x_s$ *tales que*

(1) $[x_1e_1 + d_2e_2 + \ldots + d_pe_p]_\sigma, \ldots, [x_se_1 + d_2e_2 + \ldots + d_pe_p]_\sigma \in H \cap A^1_{(d_2,\ldots,d_p)}$.

(2) El submonoide generado por

$$\{[x_1e_1+d_2e_2+\ldots d_pe_p]_\sigma,\ldots,[x_se_1+d_2e_2+\ldots+d_pe_p]_\sigma\}$$

contiene a $H\cap A^1_{(d_2,\ldots,d_p)}$.

DEMOSTRACIÓN. Supongamos que $H\cap A^1_{(d_2,\ldots,d_p)}$ es un conjunto no finito (caso de ser finito el resultado es trivial). Si $b_i=0$ para todo $i\in\{2,\ldots,n\}$, entonces por el Lema 2.4 tenemos que $d_2=\ldots=d_p=0$. Sabemos que $H\cap A^1_{(0,\ldots,0)}=\{[xe_1]_\sigma \mid [xe_1]_\sigma\in H\}$. Sea $S=\{x\in\mathbb{N}\mid [xe_1]_\sigma\in H\}$. Claramente S es un submonoide de $\mathbb{N}$ y por tanto es finitamente generado. Así, si $\{x_1,\ldots,x_s\}$ es un sistema de generadores de S, es fácil comprobar que $H\cap A^1_{(0,\ldots,0)}\subseteq\{[x_1e_1]_\sigma,\ldots,[x_se_s]_\sigma\}$. Sea ahora $i\in\{2,\ldots,n\}$ tal que $b_i\neq 0$. Aplicando el Lema 2.5, existe $x\in\mathbb{N}$ tal que

(a) $[xe_1+d_2e_2+\ldots+d_pe_p]_\sigma\in H$.
(b) $[xe_1+d_2e_2+\ldots+d_pe_p]_\sigma+k[xe_1+d_2e_2+\ldots+d_pe_p]_\sigma=[(x+y)e_1+d_2e_2+\ldots+d_pe_p]_\sigma$.
(c) Si $z\geq x$ y $a\in\mathbb{N}$, entonces $[ze_1+d_2e_2+\ldots+d_pe_p]_\sigma+ak[xe_1+d_2e_2+\ldots+d_pe_p]_\sigma=[(z+ay)e_1+d_2e_2+\ldots+d_pe_p]_\sigma$.

Sea el conjunto

$$\{i_1,\ldots,i_q\}=\left\{\ i\in\{0,\ldots,y-1\}\ \middle|\ \begin{array}{c}\text{existe } z\geq x,\ x\equiv i(\mathrm{mod}\ y)\\ [ze_1+d_2e_2+\cdots+d_pe_p]_\sigma\in H\end{array}\ \right\}.$$

Para todo $j\in\{1,\ldots,q\}$ definimos $z_{ij}=\min\{z\geq x\mid z\equiv i_j(\mathrm{mod}\ y)$ y $[ze_1+d_2e_2+\ldots+d_pe_p]_\sigma\in H\}$. Ahora probamos que si $z\geq x$ y $[ze_1+d_2e_2+\ldots+d_pe_p]_\sigma\in H$, entonces $[ze_1+d_2e_2+\cdots+d_pe_p]_\sigma$ pertenece a el submonoide generado por

$$\{[xe_1+d_2e_2+\ldots+d_pe_p]_\sigma,[z_{i1}e_1+d_2e_2+\ldots+d_pe_p]_\sigma,\ldots,[z_{iq}e_1+d_2e_2+\ldots+d_pe_p]_\sigma\}.$$

Si $z\equiv i_j(\mathrm{mod}\ y)$, entonces existe $a\in\mathbb{N}$ tal que $z=z_{ij}+ay$. Así tenemos que

$$[ze_1+d_2e_2+\ldots+d_pe_p]_\sigma=[z_{ij}e_1+d_2e_2+\ldots+d_pe_p]_\sigma+ak[xe_1+d_2e_2+\ldots+d_pe_p]_\sigma.$$

Como el conjunto $\{[ze_1+d_2e_2+\ldots+d_pe_p]_\sigma\mid z<x\}$ es finito, el lema está probado. □

Con estos resultados ya podemos probar que lo que teníamos en la Proposición 2.1 era en realidad una equivalencia.

TEOREMA 2.7. *Sea* σ *una congruencia sobre* $\mathbb{N}^p$. *Los siguientes enunciados son equivalentes:*

(1) $\mathbb{N}^p/\sigma$ *es un HFG-monoide.*
(2) Para todo $(i,j)\in\{1,\ldots,p\}\times\{1,\ldots,p\}$ *con* $i\neq j$, *existe en* σ *una relación no trivial de la forma*

$$(a_{(i,j)}e_i+(b_{(i,j)}+1)e_j)\ \sigma\ (c_{(i,j)}e_i+e_j).$$

DEMOSTRACIÓN. El que (1) implica (2) está probado en 2.1.

Supongamos que σ verifica (2). Entonces σ satisface las hipótesis del todos los lemas anteriores. Así si H es un submonoide de $\mathbb{N}^p/\sigma$, entonces H puede expresarse como unión de conjuntos de la forma $H \cap A^i_{(y_2,\ldots,y_p)}$. Por el Lema 2.6 cada uno de los monoides generados por los anteriores conjuntos son finitamente generados como submonoides de H y por tanto H también lo es. □

2. Cómo comprobar si un monoide es un HFG-monoide

En esta sección damos un método para comprobar, a partir de una presentación de un monoide, si éste satisface la segunda condición del Teorema 2.7. Sean $i, j \in \{1,\ldots,p\}$ con $i \neq j$. Denotamos por F_{ij} el submonoide de $\mathbb{N}^p$ generado por $\{e_i, e_j\}$ y por σ_{ij} la restricción de σ a F_{ij}, esto es, $(ae_i + be_j)\sigma_{ij}(ce_i + de_j)$ si y sólo si $(ae_i + be_j)\sigma(cd_i + de_j)$ (obsérvese que ésta es la congruencia obtenida a partir de σ eliminando todas las coordenadas excepto la i-ésima y la j-ésima).

Como consecuencia del Teorema 2.7 obtenemos el siguiente resultado.

COROLARIO 2.8. *Las siguientes afirmaciones son equivalentes.*

(1) $\mathbb{N}^p/\sigma$ *es un HFG-monoide.*

(2) $\mathbb{N}^2/\sigma_{ij}$ *es un HFG-monoide para todo* $i, j \in \{1,\ldots,p\}$ *con* $i \neq j$.

Todos los monoides que aparecen en el segundo punto del resultado anterior son cocientes de monoides libres generados por dos elementos. La siguiente proposición muestra como determinar, a partir de una presentación de uno estos monoides, cuando tenemos un HFG-monoide.

PROPOSICIÓN 2.9. *Sea R una congruencia sobre un monoide libre generado por* $\{e_1, e_2\}$ *y*

$$\gamma = \{(a_{11}e_1 + a_{12}e_2, b_{11}e_1 + b_{12}e_2), \ldots, (a_{r1}e_1 + a_{r2}e_2, b_{r1}e_1 + b_{r2}e_2)\}$$

un sistema de generadores de R formada por relaciones no triviales. Son equivalentes:

(1) existe una relación no trivial de la forma $(ae_1 + (b+1)e_2)R(ce_1 + e_2)$,

(2) $\{a_{12},\ldots,a_{r2},b_{12},\ldots,b_{r2}\} \cap \{0,1\} \neq \emptyset$.

DEMOSTRACIÓN.

(1) implica (2). Si $(ae_1 + (b+1)e_2)R(ce_1 + e_2)$ es una relación no trivial, usando las susticiones de γ, podemos obtener $ae_1 + (b+1)e_2$ a partir de $ce_1 + e_2$. Así deducimos que existe $i \in \{1,\ldots,r\}$ tal que $(a_{i1}, a_{i2}) \leq (c, 1)$ ó $(b_{i1}, b_{i2}) \leq (c, 1)$, de donde obtenemos que $a_{i2} \in \{0,1\}$ ó que $b_{i2} \in \{0,1\}$.

(2) implica (1). Se nos presentan las siguientes situaciones:

- Si $a_{i2} = 0$, entonces $a_{i1}e_1 R(b_{i1}e_1 + b_{i2}e_2)$ es una relación no trivial y por tanto $(a_{i1}e_1 + e_2)R(b_{i1}e_1 + (b_{i2}+1)e_2)$ es también no trivial.
- Si existe $i \in \{1,\ldots,r\}$ tal que $b_{i2} = 0$, repetimos el razonamiento anterior.
- Si $a_{i2} = 1$ y $b_{i2} \neq 0$, entonces $(a_{i1}e_1 + e_2)R(b_{i1}e_1 + ((b_{i2}-1)+1)e_2)$.
- Si existe $i \in \{1,\ldots,r\}$ tal que $b_{i2} = 1$ y $a_{i2} \neq 0$, repetimos el razonamiento anterior.

□

Así, para saber cuándo un monoide $\mathbb{N}^p/\sigma$ es un HFG-monoide sólo hemos de calcular una presentación de σ_{ij} para todo $i \neq j$ (esto último puede ser calculado usando eliminación como se explica en el Capítulo 1).

Veamos con un ejemplo cómo se aplica lo anterior.

EJEMPLO 2.10. Sea σ la congruencia sobre $\mathbb{N}^3$ generada por

$$\rho = \{((7,3,0),(1,2,0)),((0,5,1),(0,7,3)),((4,0,2),(3,0,4))\}$$

y $S \cong \mathbb{N}^3/\sigma$. Comprobemos si S es un HFG-monoide. Un sistema canónico de generadores de σ es el conjunto

$$\begin{aligned}\rho' = \{&((0,7,3),(0,5,1)),((1,2,23),(1,2,1)),\\ &((1,3,1),(1,2,11)),((2,2,1),(1,3,15)),\\ &((4,0,2),(3,0,4)),((7,3,0),(1,2,0))\}.\end{aligned}$$

Apliquemos eliminación sobre σ y veamos si los monoides $\mathbb{N}^2/\sigma_{ij}$ son todos HFG-monoides. En este caso tenemos las siguientes congruencias

$$\begin{aligned}\sigma_{12} &= \{((7,3),(1,2))\}\\ \sigma_{21} &= \{((3,7),(2,1))\}\\ \sigma_{13} &= \{((4,2),(3,4))\}\\ \sigma_{31} &= \{((2,4),(4,3))\}\\ \sigma_{23} &= \{((7,3),(5,1))\}\\ \sigma_{32} &= \{((3,7),(1,5))\}.\end{aligned}$$

Usando ahora el la Proposición 2.9 tenemos que σ_{12}, σ_{13}, σ_{31} y σ_{32} no verifican las condiciones para que $\mathbb{N}^3/\sigma$ sea un HFG-monoide, por lo que ha de tener algún submonoide no finitamente generado. Uno de ellos es el submonoide generado por $\{[e_1]_\sigma,[e_2]_\sigma\}$. □

3. HFG-monoides cancelativos

Dado M un subgrupo de $\mathbb{Z}^p$ denotamos por rango(M) el rango de M como subgrupo de $\mathbb{Z}^p$. Consideremos un monoide finitamente generado cancelativo. Este monoide ha de ser de la forma $\mathbb{N}^p/\sim_M$. La siguiente proposición nos da un método para determinar a partir de M si el monoide $\mathbb{N}^p/\sim_M$ es un HFG-monoide.

PROPOSICIÓN 2.11. *Sea M un subgrupo de $\mathbb{Z}^n$. Los siguientes enunciados son equivalentes.*

(1) $\mathbb{N}^p/\sim_M$ es un HFG-monoide.

(2) rango$(M) \geq n-1$.

DEMOSTRACIÓN. *(1) implica (2).* Si para todo $i \in \{1,\ldots,n\}$ existe $k_i \in \mathbb{N}\setminus\{0\}$ tal que $k_i[e_i]_\sigma = [0]_\sigma$, entonces

$$(k_1,0,\ldots,0),(0,k_2,0,\ldots,0),\ldots,(0,\ldots,0,k_p) \in M$$

y por tanto rango$(M) = n$. Si por el contrario existe $i \in \{1, \ldots, n\}$ tal que $k[e_i]_\sigma \neq 0$ para todo $k \in \mathbb{N} \setminus \{0\}$ (supongamos que $i = 1$), usando el Teorema 2.7, existen relaciones no triviales de la forma

$$\begin{gathered}(a_2e_1 + (b_2+1)e_2) \sim_M (c_2e_1 + e_2),\\ (a_3e_1 + (b_3+1)e_3) \sim_M (c_3e_1 + e_3),\\ \ldots\\ (a_pe_1 + (b_p+1)e_p) \sim_M (c_pe_1 + e_p).\end{gathered}$$

Probemos ahora que $b_i \neq 0$ para todo $i \in \{2, \ldots, n\}$. Si $b_i = 0$, deducimos que $a_ie_1 \sim_M c_ie_1$. Como esta última relación es no trivial tenemos que $a_i \neq c_i$. Si $a_i > c_i$, entonces $(a_i - c_i)e_1 \sim_M 0$ lo cual es absurdo ya que $k[e_1]_\sigma \neq [0]_\sigma$ para todo $k \in \mathbb{N} \setminus \{0\}$. Así tenemos que

$$\{(a_2 - c_2, b_2, 0, \ldots, 0), (a_3 - c_3, 0, b_3, 0, \ldots, 0), \ldots, (a_p - c_p, 0, \ldots, 0, b_p)\} \subseteq M$$

con $b_i \neq 0$ para todo $i \in \{2, \ldots, n\}$ lo cual implica que rango$(M) \geq n - 1$.

(2) implica (1). Si rango$(M) \geq n-1$, entonces $\mathbb{N}^n / \sim_M$ es un submonoide de $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times Z$. Si probamos que $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z}$ es un HFG-monoide tendremos probado que $\mathbb{N}^n / \sim_M$ es un HFG-monoide. Sea

$$\rho = \{(d_1e_1, 0), \ldots, (d_re_r, 0), (e_{r+1} + e_{r+2}, 0)\} \subseteq \mathbb{N}^{r+2} \times \mathbb{N}^{r+2}.$$

Tenemos que $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z} \equiv \mathbb{N}^{r+2}/\langle\rho\rangle$. Claramente $\langle\rho\rangle$ satisface la segunda condición del Teorema 2.7 y por tanto $\mathbb{N}^{r+2}/\langle\rho\rangle$ es un HFG-monoide. □

CAPÍTULO 3

Una generalización de los $\mathcal{N}$-semigrupos de Tamura

Un $\mathcal{N}$-semigrupo es un semigrupo cancelativo, arquimediano y sin idempotentes. Todo $\mathcal{N}$-semigrupo es isomorfo a uno obtenido de la siguiente forma (ver [**81**] para más detalles).
Consideremos $(G,+)$ un grupo abeliano e $\mathrm{I}: G\times G\to\mathbb{N}$ una función satisfaciendo:

(T1) para todo $g_1,g_2\in G$, $\mathrm{I}(g_1,g_2)=\mathrm{I}(g_2,g_1)$,
(T2) para todo $g_1,g_2,g_3\in G$, $\mathrm{I}(g_1,g_2)+\mathrm{I}(g_1+g_2,g_3)=\mathrm{I}(g_2,g_3)+\mathrm{I}(g_1,g_2+g_3)$,
(T3) para todo $g\in G$, $\mathrm{I}(0,g)=1$,
(T4) para todo $g\in G$ existe $k\in\mathbb{N}\setminus\{0\}$ tal que $\mathrm{I}(g,kg)\geq 1$.

Sobre el conjunto $\mathbb{N}\times G$ definimos la siguiente operación

$$(a_1,g_1)+_{\mathrm{I}}(a_2,g_2)=(a_1+a_2+\mathrm{I}(g_1,g_2),g_1+g_2);$$

entonces $(\mathbb{N}\times G,+_{\mathrm{I}})$ es un $\mathcal{N}$-semigrupo.

En este capítulo caracterizaremos los semigrupos isomorfos a uno de la forma $(\mathbb{N}\times G,+_{\mathrm{I}})$ con G un grupo e $\mathrm{I}: G\times G\to\mathbb{N}$ satisfaciendo sólo las propiedades (T1) y (T2). A esta nueva clase de semigrupos la llamaremos $\mathcal{N}$-semigrupos generalizados (obsérvese que todo $\mathcal{N}$-semigrupo es un $\mathcal{N}$-semigrupo generalizado). Probaremos que la clase de los $\mathcal{N}$-semigrupos generalizados coincide con la de los semigrupos cancelativos que no son grupos y que contienen al menos un elemento arquimediano. Además, veremos que al imponerle a I la condición $\mathrm{I}(0,0)\in\{0,1\}$ se obtiene de nuevo toda la clase de los $\mathcal{N}$-semigrupos generalizados. Usando esta condición distinguiremos entre los semigrupos con elemento neutro ($\mathrm{I}(0,0)=0$) y los que no tienen ($\mathrm{I}(0,0)=1$). Caso de tener S un $\mathcal{N}$-semigrupo generalizado sin elemento neutro siempre podemos completarlo y añadirle un nuevo elemento 0 que sea el elemento neutro de $S\cup\{0\}$, es por ello que sólo estudiaremos $\mathcal{N}$-semigrupos generalizados con elemento neutro.

Los contenidos de este capítulos pueden encontrarse en [**61**].

1. $\mathcal{N}$-semigrupos generalizados

Un **$\mathcal{N}$-semigrupo generalizado** es un semigrupo cancelativo que no es un grupo y que contiene al menos un elemento arquimediano.

Sea $(G,+)$ un grupo abeliano e $\mathrm{I}: G\times G\to\mathbb{N}$ una aplicación verificando

(1) $\mathrm{I}(g_1,g_2)=\mathrm{I}(g_2,g_1)$ para todo $g_1,g_2\in G$,
(2) $\mathrm{I}(g_1,g_2)+\mathrm{I}(g_1+g_2,g_3)=\mathrm{I}(g_2,g_3)+\mathrm{I}(g_1,g_2+g_3)$ para todo $g_1,g_2,g_3\in G$.

Definimos en el conjunto $\mathbb{N}\times G$ la siguiente operación

$$(a_1,g_1)+_{\mathrm{I}}(a_2,g_2)=(a_1+a_2+\mathrm{I}(g_1,g_2),g_1+g_2).$$

Puede probarse fácilmente que el par $(\mathbb{N}\times G,+_{\mathrm{I}})$ es un semigrupo cancelativo y que este semigrupo es un monoide si y sólo si $\mathrm{I}(0,0)=0$.

TEOREMA 3.1. *Todo semigrupo de la forma* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es un* $\mathcal{N}$*-semigrupo generalizado.*

DEMOSTRACIÓN. Sabemos que $(\mathbb{N}\times G,+_{\mathrm{I}})$ es un semigrupo cancelativo. Por tanto, sólo nos queda probar que no es un grupo y que contiene al menos un elemento arquimediano.

- Supongamos que $(\mathbb{N}\times G,+_{\mathrm{I}})$ es un grupo. En particular tenemos un monoide por lo que $\mathrm{I}(0,0)=0$ y $(0,0)$ es su elemento neutro. Además el elemento $(1,0)$ debe de tener un inverso. Sin embargo, si $(1,0)+_{\mathrm{I}}(a,g)=(0,0)$, entonces $a+1+\mathrm{I}(0,g)=0$ y por tanto $\mathrm{I}(0,g)=-a-1\notin\mathbb{N}$. Lo cual es una contradicción.
- Sea $(a,g)\in\mathbb{N}\times G$. Por inducción sobre $b\in\mathbb{N}$, es fácil probar que

  $$b(1,0)=(b+(b-1)\mathrm{I}(0,0),0).$$

  Sean $k,\overline{k}\in\mathbb{N}\setminus\{0\}$ tales que

  $$a+\overline{k}+\mathrm{I}(g,-g)=k+(k-1)\mathrm{I}(0,0).$$

  De lo anterior obtenemos que

  $$\begin{aligned}&(a,g)+_{\mathrm{I}}(\overline{k},-g)\\ &=(a+\overline{k}+\mathrm{I}(g,-g),0)=(k+(k-1)\mathrm{I}(0,0),0)=k(1,0),\end{aligned}$$

  obteniendo así que el elemento $(1,0)$ es arquimediano.

□

Probaremos ahora que esta construcción caracteriza, salvo isomorfismos, todos los $\mathcal{N}$-semigrupos generalizados. En lo que resta de capítulo, supondremos que $(S,+)$ es un $\mathcal{N}$-semigrupo generalizado y que m es un elemento arquimediano suyo. Como todo semigrupo cancelativo puede ser embebido en un grupo abeliano (véase [**20**]) y ya que la condición de ser un $\mathcal{N}$-semigrupo generalizado se preserva bajo isomorfismos, asumiremos que S es un subsemigrupo de un grupo. Recordemos que ésto nos permitía el uso de expresiones como $x-y,0x=0,x+0,x-0$, etc.

Definamos en S la siguiente relación binaria

$$xR_my \text{ si y sólo si } x+km=y+k'm \text{ para algún } k,k'\in\mathbb{N}.$$

Fácilmente se puede comprobar que R_m es una congruencia sobre S, lo cual nos permite definir el semigrupo cociente $(S/R_m,+)$, el cual es un monoide y $[m]_{R_m}$ su elemento neutro. Usando que m es arquimediano, obtenemos que además es un grupo.

LEMA 3.2. *Para todo* $x\in S$ *existe* $k_x=\max\{k\in\mathbb{N}\mid x-km\in S\}$. *Además, si* xR_my, *entonces* $x+k_ym=y+k_xm$.

DEMOSTRACIÓN. Por ser m un elemento arquimediano de S, existen $k \in \mathbb{N}\setminus\{0\}$ e $y \in S$ tales que $km = x+y$. Supongamos que existe $\overline{k} > k$ tal que $x - \overline{k}m \in S$. Entonces $(k-\overline{k})m \in S$. Pero $\overline{k} > k$ y por tanto $(\overline{k}-k)m \in S$. De donde deducimos que $0 = (k-\overline{k})m + (\overline{k}-k)m \in S$. Además $(\overline{k}-k-1)m \in S$ y $m+(\overline{k}-k-1)m+(k-\overline{k})m = 0$ y por tanto m tiene un inverso, digamos c. Tomemos ahora $a \in S$. Como m es arquimediano, existen $t \in \mathbb{N}\setminus\{0\}$ y $b \in S$ tales que $tm = a+b$, de donde obtenemos que $b+tc$ es el inverso de a. Así, llegamos a que S es un grupo contradiciendo el que S es un $\mathcal{N}$-semigrupo generalizado.

Supongamos que $xR_m y$. Fácilmente deducimos que $x+k_y m R_m y + k_x m$, por lo que existen $k, k' \in \mathbb{N}$ tales que $x+k_y m+km = y+k_x m+k'm$. Si $k' > k$, entonces $x-(k_x+k'-k)m = y-k_y m \in S$, lo cual contradice la maximalidad de k_x. Así, $k' \leq k$ y de forma análoga se puede probar que $k \leq k'$. Por tanto $k = k'$. Usando ahora que S es cancelativo obtenemos que $x+k_y m = y+k_x m$. □

El Lema 3.2 nos permite definir la siguiente aplicación:

$$A_S^m : S/R_m \to S,$$
$$A_S^m([x]_{R_m}) = x - k_x m.$$

Obsérvese que $\mathrm{Im}(A_S^m) = \{s \in S \mid s-m \notin S\}$. Como veremos a continuación, el papel de estos conjuntos es el mismo que el de los conjuntos de Apéry en semigrupos numéricos.

LEMA 3.3. *Para todo $s \in S$ existe un único elemento $(k,x) \in \mathbb{N}\times \mathrm{Im}(A_S^m)$ tal que $s = km+x$.*

DEMOSTRACIÓN. Claramente, $s = k_s m + (s-k_s m)$. Supongamos que $km+x = k'm+y$ donde $x, y \in \mathrm{Im}(A_S^m)$. Si $k' > k$, entonces $x-(k'-k)m = y \in S$, lo cual contradice el que $k_x = 0$. Por tanto $k' \leq k$. De igual manera puede ser probado que $k \leq k'$. En consecuencia tenemos, $k = k'$ y por la cancelatividad de S nos queda que $x = y$. □

Los Lemas 3.2 y 3.3 y $k_{x+y} \geq k_x + k_y$, nos permiten definir la siguiente aplicación:

$$\mathrm{I} : S/R_m \times S/R_m \to \mathbb{N},$$
$$\mathrm{I}([x]_{R_m}, [y]_{R_m}) = k_{x+y} - k_x - k_y.$$

El lector puede probar sin dificultad que la aplicación I verifica lo siguiente:

(1) $\mathrm{I}([x]_{R_m}, [y]_{R_m}) = \mathrm{I}([y]_{R_m}, [x]_{R_m})$,
(2) $\mathrm{I}([x]_{R_m}, [y]_{R_m}) + \mathrm{I}([x+y]_{R_m}, [z]_{R_m}) = \mathrm{I}([y]_{R_m}, [z]_{R_m}) + \mathrm{I}([x]_{R_m}, [y+z]_{R_m})$.

Por el Lema 3.3, sabemos que para todo $s \in S$ existe un único elemento $(k,x) \in \mathbb{N}\times \mathrm{Im}(A_S^m)$ tal que $s = km+x$. De esta forma podemos definir la aplicación

$$\theta : S \to \mathbb{N}\times S/R_m,$$
$$\theta(s) = (k, [x]_{R_m}).$$

Además se puede probar fácilmente que esta aplicación es un isomorfismo de semigrupos habiendo así probado el siguiente resultado.

TEOREMA 3.4. *El semigrupo $(S,+)$ es isomorfo a $(\mathbb{N}\times S/R_m, +_{\mathrm{I}})$.*

Los Teoremas 3.1 y 3.4 son teoremas de estructura para los $\mathcal{N}$-semigrupos generalizados, nos disponemos ahora a mejorar estos resultados.

Como se ha indicado anteriormente, podemos suponer que S es un subsemigrupo de un grupo abeliano $(H,+)$. Si 0 es el elemento neutro de H, entonces puede ocurrir que $0 \in S$ ó que $0 \notin S$. Si $0 \in S$, entonces $k_{2m} = 2$ y $k_m = 1$, de donde $\mathrm{I}([m]_{R_m}, [m]_{R_m}) = k_{2m} - k_m - k_m = 0$ (basta recordar que si $-m \in S$, entonces S es un grupo). Si $0 \notin S$, entonces $k_{2m} = 1$ y $k_m = 0$. En este caso tendríamos que $\mathrm{I}([m]_{R_m}, [m]_{R_m}) = k_{2m} - k_m - k_m = 1$. Consecuencia de todo lo expuesto es que la aplicación I ha de verificar que $\mathrm{I}([m]_{R_m}, [m]_{R_m}) \in \{0,1\}$.

Para completar esta sección introducimos el concepto de $\mathcal{N}$-monoide. Si $(S,+)$ es un semigrupo sin elemento neutro, entonces podemos añadirle un nuevo elemento y obtener un monoide de la siguiente forma. Añadimos a S un nuevo elemento, digamos 0, y definimos $0+s = s+0 = s$ para todo $s \in S \cup \{0\}$. Claramente el par $(S \cup \{0\}, +)$ es un monoide cuyo elemento neutro es 0.

LEMA 3.5. *Si $(S,+)$ es un semigrupo cancelativo sin elementos idempotentes, entonces $x+y \neq x$ para todo $x,y \in S$.*

DEMOSTRACIÓN. Supongamos que $x+y = x$, entonces $x+2y = x+y$. Aplicando ahora que S es cancelativo, obtenemos $2y = y$ y por tanto S contendría elementos idempotentes. □

El siguiente resultado se deduce a partir del Lema 3.5.

COROLARIO 3.6. *Sea $(S,+)$ es un $\mathcal{N}$-semigrupo generalizado sin elementos idempotentes. Entonces $(S \cup \{0\}, +)$ es un $\mathcal{N}$-semigrupo generalizado con elemento neutro.*

Estos últimos resultados nos llevan a definir un **$\mathcal{N}$-monoide** como un monoide cancelativo que no es grupo y que contiene al menos un elemento arquimediano.

2. Algunos tipos de $\mathcal{N}$-monoides

En esta sección, G denotará un grupo abeliano e $\mathrm{I} : G \times G \to \mathbb{N}$ una aplicación verificando:

(1) $\mathrm{I}(g_1,g_2) = \mathrm{I}(g_2,g_1)$,
(2) $\mathrm{I}(g_1,g_2) + \mathrm{I}(g_1+g_2,g_3) = \mathrm{I}(g_2,g_3) + \mathrm{I}(g_1,g_2+g_3)$,
(3) $\mathrm{I}(0,g) = 0$ para todo $g \in G$.

Puede probarse que la propiedad (3) de I es equivalente a que $\mathrm{I}(0,0) = 0$.

Recordemos que todo monoide cancelativo es isomorfo a un submonoide de un grupo abeliano. A continuación veremos que caso de partir de un $\mathcal{N}$-monoide de la forma $(\mathbb{N} \times G, +_{\mathrm{I}})$ podemos de forma directa conocer el grupo más pequeño que lo contiene.

PROPOSICIÓN 3.7. *El conjunto $\mathbb{Z} \times G$ tiene estructura de grupo con la siguiente operación*

$$(z_1,g_1) +_{\mathrm{I}} (z_2,g_2) = (z_1+z_2+\mathrm{I}(g_1,g_2), g_1+g_2).$$

Además, $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es un submonoide de* $(\mathbb{Z}\times G,+_{\mathrm{I}})$ *y todo elemento de* $(\mathbb{Z}\times G,+_{\mathrm{I}})$ *puede ser expresado como diferencia de dos elementos de* $(\mathbb{N}\times G,+_{\mathrm{I}})$.

DEMOSTRACIÓN. Sólo hemos de tener en cuenta $(z,g)\in\mathbb{Z}\times G$. Tenemos

$$(z,g)+_{\mathrm{I}}(-z-\mathrm{I}(g,-g),-g)=(z-z-\mathrm{I}(g,-g)+\mathrm{I}(g,-g),g-g)=(0,0)$$

y que si $(z,g)\in\mathbb{Z}\times G$, tomando $a,b\in\mathbb{N}$ tales $a-b=z$, los elementos (a,g) y $(b,0)$ pertenecen a $\mathbb{N}\times G$ y además

$$(a,g)+_{\mathrm{I}}(-(b,0))=(a,g)+_{\mathrm{I}}(-b-\mathrm{I}(0,0),0)=(a-b+\mathrm{I}(g,0),g)=(z,g).$$

□

Como consecuencia de la Proposición 3.7 obtenemos que $(\mathbb{Z}\times G,+_{\mathrm{I}})$ es el grupo de cocientes de $(\mathbb{N}\times G,+_{\mathrm{I}})$.

A continuación impondremos condiciones sobre el grupo G y/o sobre la aplicación I para obtener clases de submonoides de grupo abelianos.

La siguiente proposición nos dice bajo qué condiciones el grupo $(\mathbb{Z}\times G,+_{\mathrm{I}})$ es finitamente generado.

PROPOSICIÓN 3.8. *El grupo* $(\mathbb{Z}\times G,+_{\mathrm{I}})$ *es finitamente generado si y sólo si lo es* G.

DEMOSTRACIÓN. Supongamos que $(\mathbb{Z}\times G,+_{\mathrm{I}})$ es finitamente generado y sean $\{(z_1,g_1),\ldots,(z_n,g_n)\}$ un sistema de generadores suyo. Si $g\in G$, entonces existen $a_1,\ldots,a_n\in\mathbb{Z}$ tales que $(0,g)=a_1(z_1,g_1)+_{\mathrm{I}}\cdots+_{\mathrm{I}}(z_n,g_n)$. Por tanto $a_1g_1+\cdots+a_ng_n=g$, de donde $\{g_1,\ldots,g_n\}$ es un sistema de generadores de G.

Recíprocamente, sea $\{g_1,\ldots,g_n\}$ un sistema de generadores de G. Veamos que $\{(1,0),(0,g_1),\ldots,(0,g_n)\}$ es un sistema de generadores de $\mathbb{Z}\times G$. Si $(x,g)\in\mathbb{Z}\times G$, entonces existen $a_1,\ldots,a_n\in\mathbb{Z}$ tales que $g=a_1g_1+\cdots+a_ng_n$. Así, $a_1(0,g_1)+_{\mathrm{I}}\cdots+_{\mathrm{I}}a_n(0,g_n)=(\overline{x},g)$ lo cual hace que $(x-\overline{x})(1,0)+_{\mathrm{I}}(\overline{x},g)=(x+\mathrm{I}(0,g),g)=(x,g)$ y por tanto $(x,g)=a_1(0,g_1)+_{\mathrm{I}}\cdots+_{\mathrm{I}}a_n(0,g_n)+_{\mathrm{I}}(x-\overline{x})(1,0)$. □

Ya podemos enunciar el primer resultado que nos da la primera familia de semigrupos que obtendremos usando la estructura de los $\mathcal{N}$-monoides.

COROLARIO 3.9. *El monoide* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es un submonoide de grupo finitamente generado si y sólo si el grupo* G *es finitamente generado. Además, todo submonoide de un grupo finitamente generado que no sea a su vez un grupo es isomorfo a un monoide de esta forma.*

Veamos ahora qué propiedad adicional debe verificar la aplicación I para que $(\mathbb{N}\times G,+_{\mathrm{I}})$ sea reducido.

LEMA 3.10. *El conjunto* $\mathcal{U}(\mathbb{N}\times G)$ *es igual a* $\{(0,g)\in\mathbb{N}\times G\mid \mathrm{I}(g,-g)=0\}$.

DEMOSTRACIÓN. Sea $(a,g)\in\mathcal{U}(\mathbb{N}\times G)$. Existe $(b,\overline{g})$ tal que $(a,g)+_{\mathrm{I}}(b,\overline{g})=(0,0)$. Por tanto $(a+b+\mathrm{I}(g,\overline{g}),g+\overline{g})=(0,0)$ y entonces nos queda $a=0$, $\overline{g}=-g$ e $\mathrm{I}(g,-g)=0$.

Sea ahora $(0,g)$ tal que $\mathrm{I}(g,-g)=0$. Tenemos que $(0,g)+(0,-g)=(0+\mathrm{I}(g,-g),0)=(0,0)$, de donde deducimos que $(0,g)\in\mathcal{U}(\mathbb{N}\times G)$. □

Usando este resultado es fácil deducir la siguiente proposición

PROPOSICIÓN 3.11. *El monoide* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es reducido si y sólo si* $\mathrm{I}(g,-g)\neq 0$ *para todo* $g\in G\setminus\{0\}$.

Basta imponerle a I la condición $\mathrm{I}(g,-g)\neq 0$ para todo $g\in G\setminus\{0\}$ para obtener la siguiente familia de semigrupos.

COROLARIO 3.12. *Un monoide de la forma* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es un submonoide reducido de un grupo finitamente generado si y sólo si* G *es un grupo finitamente generado y la aplicación* I *verifica que* $\mathrm{I}(g,-g)\neq 0$ *para todo* $g\in G\setminus\{0\}$. *Además, todo submonoide reducido de un grupo finitamente generado es isomorfo a uno de esta forma.*

Un monoide $(S,+)$ es **libre de torsión** si $kx=ky$ con $k\in\mathbb{N}\setminus\{0\}$ implica que $x=y$. Además, sabemos que un monoide conmutativo y cancelativo es libre de torsión si y sólo si su grupo cociente es un grupo abeliano libre de torsión (véase [**65**]).

Sea $g\in G$, definimos el orden de g como el número

$$O(g)=\min\{k\in\mathbb{N}\setminus\{0\}\mid kg=0\}.$$

Si este mínimo no existe, entonces decimos que $O(g)=\infty$.

PROPOSICIÓN 3.13. *El grupo* $(\mathbb{Z}\times G,+_{\mathrm{I}})$ *es libre de torsión si y sólo si* $O(g)\notin\{1,\infty\}$ *implica que* $\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig)\not\equiv 0\pmod{O(g)}$.

DEMOSTRACIÓN. Supongamos que existen $a\in\mathbb{N}$ y $g\in G$ tales que $\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig)=aO(g)$. Entonces,

$$O(g)(-a,g)=(-O(g)a+\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig),O(g)g)=(0,0)$$

y por tanto $(\mathbb{Z}\times G,+_{\mathrm{I}})$ no es libre de torsión.

Recíprocamente, si $k(z,g)=(0,0)$ entonces $kg=0$ y $\sum_{i=1}^{k-1}\mathrm{I}(g,ig)=k(-z)$. Como $kg=0$, tenemos que $k=lO(g)$ y por tanto

$$\sum_{i=1}^{k-1}\mathrm{I}(g,ig)=\sum_{i=1}^{lO(g)-1}\mathrm{I}(g,ig)=l\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig),$$

de donde deducimos que $\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig)\equiv 0(\mathrm{mod}\ O(g))$. □

Usando la Proposición 3.7, que un monoide cancelativo es libre de torsión si y sólo si su grupo cociente es libre de torsión y que todo subgrupo de un grupo abeliano libre de torsión es libre de torsión, deducimos el siguiente resultado.

PROPOSICIÓN 3.14. *El monoide* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es libre de torsión si y sólo si* $O(g)\notin\{1,\infty\}$ *implica que* $\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig)\not\equiv 0(\mathrm{mod}\ O(g))$. *Además, todo submonoide de un grupo abeliano libre de torsión que no sea un grupo y con al menos un elemento arquimediano es isomorfo a un monoide de esta forma.*

Como consecuencia del Corolario 3.9 y usando el que todo grupo abeliano finitamente generado libre de torsión es isomorfo a $(\mathbb{Z}^n,+)$ para algún $n\in\mathbb{N}$, obtenemos el siguiente resultado.

COROLARIO 3.15. *El monoide* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es isomorfo a un submonoide de* $(\mathbb{Z}^n,+)$ *para algún* $n\in\mathbb{N}$ *si y sólo si* G *es finitamente generado y* $O(g)\notin\{1,\infty\}$ *implica que* $\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig)\not\equiv 0(\mathrm{mod}\ O(g))$. *Además, todo submonoide de* $(\mathbb{Z}^n,+)$ *que no sea un grupo es isomorfo a uno de esta forma.*

Los submonoides finitamente generados de $(\mathbb{N}^n,+)$ se caracterizan, salvo isomorfismos, por ser los monoides cancelativos, finitamente generados, libres de torsión y reducidos (véase **[34]** o **[58]**). Haciendo uso de esto podemos enunciar el siguiente resultado.

COROLARIO 3.16. *Un monoide* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es isomorfo a un submonoide finitamente generado de* $(\mathbb{N}^n,+)$ *para algún* $n\in\mathbb{N}$ *si y sólo si es finitamente generado,* $\mathrm{I}(g,-g)\neq 0$ *para todo* $g\in G\setminus\{0\}$ *y* $O(g)\notin\{1,\infty\}$ *implica que* $\sum_{i=1}^{O(g)-1}\mathrm{I}(g,ig)\not\equiv 0(\mathrm{mod}\ O(g))$. *Además, todo submonoide finitamente generado de* $(\mathbb{N}^n,+)$ *es isomorfo a uno de esta forma.*

3. Monoides de valoración reducidos

Comenzamos esta sección definiendo el concepto de monoide de valoración reducido. Para ello recordamos los siguientes resultados y definiciones.

Un **grupo abeliano ordenado** es una terna $(H,+,\leq)$ tal que $(H,+)$ es un grupo abeliano y $\leq$ una relación binaria que satisface las siguientes propiedades:

(1) $h\leq h$ para todo $h\in H$,
(2) si $h_1\leq h_2$ y $h_2\leq h_1$, entonces $h_1=h_2$,
(3) si $h_1\leq h_2$ y $h_2\leq h_3$, entonces $h_1\leq h_3$,
(4) si $h_1\leq h_2$, entonces $h_1+h_3\leq h_2+h_3$ para todo $h_3\in H$.

Además, si $\leq$ verifica la siguiente propiedad adicional, diremos que $(H,+,\leq)$ es un **grupo abeliano linealmente ordenado**.

(5) Para todo $h_1,h_2\in H$, se tiene que $h_1\leq h_2$ ó $h_2\leq h_1$.

El siguiente resultado es fácil de probar.

PROPOSICIÓN 3.17. *Si* $(H,+,\leq)$ *es un grupo abeliano ordenado, entonces* $S=\{h\in H\mid h\geq 0\}$ *es un submonoide reducido de* H.

PROPOSICIÓN 3.18. *Sea* $(H,+)$ *un grupo abeliano y* S *un submonoide reducido de* H. *Entonces* $(H,+,\leq)$ *es grupo abeliano ordenado con* $\leq$ *definido como*

$$h_1\leq h_2 \text{ si } h_2-h_1\in S.$$

Además $S=\{h\in H\mid h\geq 0\}$.

Si queremos obtener similares resultados para grupos abelianos linealmente ordenados, debemos imponer más condiciones sobre el monoide S.

Sea H un grupo abeliano y S un submonoide de H. Decimos que S es un **monoide de valoración** de H si para todo $h \in H$ tenemos que $\{h, -h\} \cap S \neq \emptyset$. Nótese que si S es reducido, entonces el cardinal de $\{h, -h\} \cap S$ es igual a uno para todo $h \in H$.

Las siguientes dos proposiciones pueden ser probadas sin dificultad.

PROPOSICIÓN 3.19. *Sea $(H, +, \leq)$ un grupo abeliano linealmente ordenado. Entonces $S = \{h \in H \mid h \geq 0\}$ es un monoide de valoración reducido de H.*

PROPOSICIÓN 3.20. *Sea $(H, +)$ un grupo abeliano y S un monoide de valoración reducido suyo. Entonces $(H, +, \leq)$ es un grupo abeliano linealmente ordenado donde $\leq$ está definido por*

$$h_1 \leq h_2 \text{ si y sólo si } h_2 - h_1 \in S.$$

Además, $S = \{h \in H \mid h \geq 0\}$.

Los dos siguientes resultados pueden encontrarse en [**30**].

TEOREMA 3.21. *Sea H un grupo abeliano. Entonces H contiene un monoide de valoración reducido si y sólo si H es un grupo abeliano libre de torsión.*

TEOREMA 3.22. *Si H es un grupo abeliano libre de torsión y S es un monoide reducido suyo, entonces S está contenido en un monoide de valoración reducido de H.*

Estamos ya en condiciones de saber qué condiciones hemos de imponer a la aplicación I para obtener un monoide de valoración reducido.

TEOREMA 3.23. *Un monoide de la forma $(\mathbb{N} \times G, +_{\mathrm{I}})$ es un monoide de valoración reducido de $(\mathbb{Z} \times G, +_{\mathrm{I}})$ si y sólo si $\mathrm{I}(g, -g) = 1$ para todo $g \in G \setminus \{0\}$.*

DEMOSTRACIÓN. Supongamos que $\mathrm{I}(g, -g) = 1$ para todo $g \in G \setminus \{0\}$. Ya que $\mathrm{I}(g, -g) \neq 0$ para todo $g \in G \setminus \{0\}$, $(\mathbb{N} \times G, +_{\mathrm{I}})$ es un monoide reducido. Sea $(a, g) \in \mathbb{Z} \times G$. Si $(a, g) \notin \mathbb{N} \times G$, entonces $a < 0$. Por tanto,

$$-(a, g) = (-a - \mathrm{I}(g, -g), -g) = (-a - 1, -g) \in \mathbb{N} \times G.$$

Recíprocamente, si $\mathrm{I}(g, -g) = r \geq 2$, entonces $(-1, g) \notin \mathbb{N} \times G$ y

$$-(-1, g) = (1 - r, -g) \notin \mathbb{N} \times G.$$

□

Obsérvese que por la Condición (2) que cumple I, se tiene que $\mathrm{I}(-g, g) + \mathrm{I}(0, g') = \mathrm{I}(g, g') + \mathrm{I}(-g, g + g')$. Si $\mathrm{I}(g, -g) = 1$, entonces $\mathrm{I}(g, g') \in \{0, 1\}$. En consecuencia obtenemos el siguiente resultado.

COROLARIO 3.24. *Sea $(\mathbb{N} \times G, +_{\mathrm{I}})$ un monoide de valoración reducido de $(\mathbb{Z} \times G, +_{\mathrm{I}})$. Entonces $\mathrm{Im}(\mathrm{I}) \subseteq \{0, 1\}$.*

Resumiendo los anteriores resultados obtenemos ahora la siguiente clase de semigrupos.

TEOREMA 3.25. *Todo monoide de valoración reducido de un grupo abeliano que contenga al menos un elemento arquimediano es isomorfo a un $\mathcal{N}$-monoide $(\mathbb{N} \times G, +_I)$ tal que $\mathrm{I}(g, -g) = 1$ para todo $g \in G \setminus \{0\}$.*

Usando la Proposición 3.21 tenemos que un grupo finitamente generado admite un monoide de valoración reducido si y sólo si es libre.

COROLARIO 3.26. *Un monoide es un monoide de valoración reducido de* $(\mathbb{Z}^n,+)$ *si y sólo si es isomorfo a un* $\mathcal{N}$*-monoide* $(\mathbb{N}\times G,+_I)$ *en el que* $\mathrm{I}(g,-g)=1$ *para todo* $g\in G$ *y* G *es un grupo finitamente generado.*

4. Monoides de valoración reducidos de $\mathbb{Z}^n$

En esta sección, nuestro objetivo es dar explícitamente un grupo G y una aplicación I para los monoides de valoración reducidos de $\mathbb{Z}^n$. Más tarde en la Sección 5, usaremos estos calculos para describir G e I para los submonoides reducidos de $\mathbb{Z}^n$.

Recordemos que en la Sección 1, el grupo G era el monoide cociente S/R_m (el hecho de que m fuese arquimediano aseguraba que este monoide cociente era un grupo).

Consideremos S un monoide de valoración reducido de $\mathbb{Z}^n$. Por la Proposición 3.20 el monoide S define un orden sobre $\mathbb{Z}^n$, por ello usaremos $[0,m[$ para representar el conjunto

$$\{x\in S\mid 0\leq x<m\}=\{x\in S\mid x-m\notin S\}.$$

PROPOSICIÓN 3.27. *El conjunto* $[0,m[$ *es un grupo con la siguiente operación:*

$$a+b=\begin{cases} a+b & si\ a+b<m,\\ a+b-m & si\ a+b\geq m.\end{cases}$$

Además, todo elemento de S/R_m *tiene un único representante en* $[0,m[$.

DEMOSTRACIÓN. En primer lugar veamos que la operación $+$ está bien definida. Debemos probar que si $a,b\in[0,m[$ y $a+b\geq m$, entonces $a+b-m\in[0,m[$. Efectivamente, si $a+b-m<0$, entonces $a+b<m$. Si $a+b-m\geq m$, entonces $a+b\geq 2m$, pero $a<m$ y $b<m$ implica que $a+b<2m$.

Para terminar la demostración sólo nos queda probar que todo elemento de S/R_m tiene un único representate en $[0,m[$.

- Sea $x\in S$, entonces $x-k_xm\in[0,m[$ y $x-k_xmR_mx$ (recuérdese como se definió k_x en el Lema 3.2).
- Veamos ahora la unicidad del representate. Supongamos que xR_my. Entonces existen $k,\overline{k}\in\mathbb{N}$ tales que $x+km=y+\overline{k}m$. Ya que el monoide $[0,m[$ es cancelativo, existe $t\in\mathbb{N}$ tal que $x=y+tm$. Pero $x<m$ e $y\geq 0$ implican que $t=0$. En consecuencia $x=y$.

□

Definamos la siguiente aplicación:

$$c:[0,m[\times[0,m[\to\{0,1\},$$
$$c(x,y)=\begin{cases} 0 & \text{if } x+y<m,\\ 1 & \text{if } x+y\geq m.\end{cases}$$

El siguiente resultado puede ser probado fácilmente.

PROPOSICIÓN 3.28. *La aplicación c verifica las siguientes siguientes propiedades:*

(1) $c(x,y) = c(y,x)$,
(2) $c(x,y) + c(x+y,z) = c(y,z) + c(x,y+z)$,
(3) $c(x,0) = 0$ *para todo* $g \in G$.
(4) $c(x,-x) = 1$ *para todo* $x \neq 0$.

Por el Teorema 3.25 y la Proposición 3.28, podemos afirmar que $(\mathbb{N}\times[0,m[,+_c)$ es un monoide de valoración reducido de $(\mathbb{Z}\times[0,m[,+_c)$. Es más, tenemos el siguiente resultado.

TEOREMA 3.29. *El monoide* $(\mathbb{N}\times[0,m[,+_c)$ *es isomorfo a S.*

DEMOSTRACIÓN. Definamos

$$f : \mathbb{N}\times[0,m[\to S,$$
$$f(k,a) = km + a.$$

Claramente se tiene que f es biyectiva. Veamos que es un isomorfismo,

$$f(k_1,a_1) + f(k_2,a_2) = k_1m + a_1 + k_2m + a_2 = (k_1+k_2)m + a_1 + a_2 =$$
$$f(k_1 + k_2 + c(a_1,a_2), a_1 + a_2) = f((k_1,a_1) +_c (k_2,a_2)).$$

□

5. Submonoides reducidos de $\mathbb{Z}^n$

Sea S un submonoide reducido de $\mathbb{Z}^n$. Como el grupo generado por S es un grupo abeliano libre de rango menor o igual que n, podemos suponer sin perdida de generalidad que el grupo generado por S es $\mathbb{Z}^n$. El Teorema 3.22 nos dice que si S es un submonoide reducido de un grupo G libre de torsión, entonces S está contenido en un monoide de valoración reducido de G. Sea $\overline{S}$ un monoide de valoración reducido de $\mathbb{Z}^n$ que contiene a S, m un elemento arquimediano de S, $a \in \overline{S}$ y $\mathcal{G}(S)$ el grupo cociente de S. Existen $x,y \in S$ tales que $a = x - y$. Al ser m arquimediano, existe $k \in \mathbb{N}$ y $c \in S$ tales que $x + c = km$. Así, $km - a = km - x + y \in S \subseteq \overline{S}$ y por tanto m también es arquimediano en $\overline{S}$.

Al ser $\overline{S}$ un monoide de valoración reducido podemos definir como antes el conjunto $[0,m[\subseteq \overline{S}$.

PROPOSICIÓN 3.30. *Sea* $G = \{x \in [0,m[\mid x + km \in S \text{ para algún } k \in \mathbb{N}\}$. *Entonces G es un subgrupo de* $[0,m[$.

DEMOSTRACIÓN. Como $m \in S$, tenemos que $0 \in G$. Si $x,y \in G$, entonces $x + km \in S$ y $y + \overline{k}m \in S$. Por tanto $x + y + (k+\overline{k})m \in S$ y así $x + y \in G$. Veamos ahora que todo elemento de G tiene inverso. Tomemos $x \in G$, entonces $x + km \in S$ para algún $k \in \mathbb{N}$. Usando el que m es arquimediano, existe $\overline{k} \in \mathbb{N}\setminus\{0\}$ tal que $\overline{k}m - x - km \in S$. Por tanto $(\overline{k} - k)m - x \in S$. Tomando $\overline{k}$ lo suficientemente grande, obtenemos que $(\overline{k} - k - 1)m + m - x \in S$. □

Definamos la aplicación

$$\varphi : G \to \mathbb{N},$$
$$\varphi(x) = \min\{k \in \mathbb{N} \mid x + km \in S\}.$$

El siguiente resultado puede ser fácilmente probado.

PROPOSICIÓN 3.31. *La aplicación* φ *verifica las siguientes propiedades:*

(1) $\varphi(0) = 0$,
(2) $\varphi(x) + \varphi(y) + c(x,y) - \varphi(x+y) \geq 0$.

La Proposición 3.31 nos permite definir la siguiente aplicación

$$\mathrm{I} : G \times G \to \mathbb{N},$$
$$\mathrm{I}(x,y) = \varphi(x) + \varphi(y) + c(x,y) - \varphi(x+y).$$

De la definición de φ y de las propiedades de c se deduce que la aplicación I verifica las propiedades para obtener un $\mathcal{N}$-monoide reducido. Es más, se obtiene que $(\mathbb{N} \times G, +_I)$ es isomorfo a S.

CAPÍTULO 4

Extensiones decimales del grupo aditivo de los enteros

En este capítulo introducimos el concepto de extensión decimal del grupo aditivo de los enteros. Denotaremos por $\mathbb{Q}$ y $\mathbb{R}$ el cuerpo de los números racionales y el de los reales, respectivamente. Un **sistema decimal** de $(\mathbb{Z},+)$ es una terna $(H,\oplus,d)$ con $(H,\oplus)$ un grupo abeliano y $d : H \times H \to \{0,1\}$ una aplicación verificando las siguientes condiciones:

(1) $d(h_1,h_2) = d(h_2,h_1)$,
(2) $d(h_1,h_2) + d(h_1 \oplus h_2,h_3) = d(h_2,h_3) + d(h_1,h_2 \oplus h_3)$,
(3) $d(0,h) = 0$,
(4) $d(h,-h) = 1$ para todo $h \neq 0$,

donde 0 denota el elemento neutro de $(H,\oplus)$ y $-h$ el inverso de h. Al igual que en capítulo anterior, definimos sobre $\mathbb{Z} \times H$ la siguiente operación:

$$(z_1,h_1) +_d (z_2,h_2) = (z_1 + z_2 + d(h_1,h_2), h_1 \oplus h_2),$$

y obtenemos que $(\mathbb{Z} \times H, +_d)$ es un grupo abeliano. Además, por la Condición (3) de d, todo elemento (z,h) de este grupo puede ser expresado de la forma $(z,h) = (z,0) +_d (0,h)$. En esta situación, diremos que $(z,0)$ y $(0,h)$ son la **parte entera** y la **parte decimal** de (z,h), respectivamente. Lo que pretendemos con esta construcción es generalizar los sistemas decimales clásicos de $(\mathbb{Z},+)$ cuando éste es embebido en $(\mathbb{R},+)$ ó $(\mathbb{Q},+)$. Esto surge del hecho de que $(\mathbb{Z} \times (\mathbb{Q}/\mathbb{Z}), +_d)$ es isomorfo a $\mathbb{Q}$ con $d : \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \to \{0,1\}$ definido por $d([h_1],[h_2]) = 1$ para todo $h_1,h_2 \in [0,1[$ tal que $h_1 + h_2 \geq 1$, y $d([h_1],[h_2]) = 0$ en otro caso.

Todos estos comentarios dan lugar a que digamos que un grupo abeliano $(G,+)$ es una **extensión decimal** de $(\mathbb{Z},+)$ si existe un sistema decimal $(H,\oplus,d)$ de $(\mathbb{Z},+)$ tal que $(G,+)$ es isomorfo a $(\mathbb{Z} \times H, +_d)$. Nuestro objetivo en este capítulo es estudiar este tipo de grupos, dentro de los cuales definiremos un nuevo tipo al que llamaremos extensiones racionales a los que prestaremos mayor atención.

Los contenidos de este capítulo pueden encontrarse en **[60]**.

1. Extensiones decimales

Sea $(G,+,\leq)$ un grupo abeliano linealmente ordenado y $m \in G$ tal que $m > 0$. Al igual que en el capítulo anterior, denotaremos por $[0,m[$ al conjunto $\{g \in G \mid 0 \leq g < m\}$. Por la Proposición 3.27, tenemos que $([0,m[,\oplus)$ es un grupo abeliano con la

operación

$$x \oplus y = \begin{cases} x+y & \text{si } x+y < m, \\ x+y-m & \text{si } x+y \geq m. \end{cases}$$

Además la Proposición 3.28 nos dice que la aplicación

$$d : [0,m[\times[0,m[\to \{0,1\},$$
$$d(x,y) = \begin{cases} 0 & \text{si } x+y < m, \\ 1 & \text{si } x+y \geq m \end{cases}$$

verifica las condiciones (1), (2), (3) y (4) anteriores.

Así, claramente obtenemos el siguiente resultado.

PROPOSICIÓN 4.1. *La terna* $([0,m[,\oplus,d)$ *es un sistema decimal de* $(\mathbb{Z},+)$.

No sólamente podemos enunciar esta proposición sino que además vamos a ver que éstos son los únicos sistemas decimales de $(\mathbb{Z},+)$. Para ello usaremos algunos resultados del capítulo anterior.

Dado $(H,\oplus,+_d)$ un sistema decimal de $(\mathbb{Z},+)$, al verificar d la Condición (4), aplicando el Teorema 3.23 tenemos que $(\mathbb{N}\times H,+_d)$ es un monoide de valoración reducido de $(\mathbb{Z}\times H,+_d)$. Usando la Proposición 3.20, tenemos que $(\mathbb{Z}\times H,+_d,\leq)$ es un grupo linealmente ordenado con el orden siguiente:

$$(z_1,h_1) \leq (z_2,h_2) \text{ si } (z_2,h_2) -_d (z_1,h_1) \in \mathbb{N}\times H.$$

Ya tenemos un orden para definir intervalos en $\mathbb{Z}\times H$.

LEMA 4.2. *El conjunto*

$$[(0,0),(1,0)[= \{(a,h) \in \mathbb{Z}\times H \mid (0,0) \leq (a,h) < (1,0)\}$$

es igual a $\{(0,h) \mid h \in H\}$.

DEMOSTRACIÓN. Tomemos $(0,h) \in \mathbb{N}\times H$. Tenemos que $(0,h) \geq (0,0)$. Además $(1,0) -_d (0,h) = (1,0) +_d (-1,-h) = (0,-h) \in \mathbb{N}\times H$, lo cual implica que $(0,h) < (1,0)$.

Tomemos ahora $(a,h) \in [(0,0),(1,0)[$. Entonces $(0,0) \leq (a,h)$ y $(a,h) < (1,0)$. Por tanto, $(a,h) \in \mathbb{N}\times H$ y $(1,0) -_d (a,h) = (-a,-h) \in \mathbb{N}\times H$. De ahí que $(a,h),(-a,h) \in \mathbb{N}\times H$ y así tengamos que $a = 0$. □

LEMA 4.3. *Sean* $h_1,h_2 \in H$. *Entonces* $d(h_1,h_2) = 0$ *si y sólo si* $(0,h_1) +_d (0,h_2) < (1,0)$.

DEMOSTRACIÓN. Si $d(h_1,h_2) = 0$, entonces $(0,h_1) +_d (0,h_2) = (0,h_1 \oplus h_2)$. Aplicando el Lema 4.2, obtenemos que $(0,h_1) +_d (0,h_2) < (1,0)$.

Tomemos $h_1,h_2 \in H$ tales que $(0,h_1) +_d (0,h_2) < (1,0)$. Entonces $(d(h_1,h_2),h_1 \oplus h_2) < (1,0)$. Por el Lema 4.2, nos queda que $d(h_1,h_2) = 0$. □

Estamos ya en condiciones de probar el siguiente resultado que nos dará la clave para caracterizar los sistemas decimales de $(\mathbb{Z},+)$.

PROPOSICIÓN 4.4. *La aplicación* $\varphi : H \to [(0,0),(1,0)[$ *definida por* $\varphi(h) = (0,h)$ *es un isomorfismo de grupos. Además,*

$$d(h_1,h_2) = \begin{cases} 0 & si\ \varphi(h_1) +_d \varphi(h_2) < (1,0), \\ 1 & si\ \varphi(h_1) +_d \varphi(h_2) \geq (1,0). \end{cases}$$

DEMOSTRACIÓN. Como consecuencia del Lema 4.2, la aplicación φ está bien definida y además es biyectiva. Es más,

$$\varphi(h_1 \oplus h_2) = (0,h_1) \oplus (0,h_2) = \varphi(h_1) \oplus \varphi(h_2)$$

y por tanto φ es un isomorfismo. Finalmente, por el Lema 4.3, la función d satisface la Condición (1). □

Como consecuencia de las Proposiciones 4.1 y 4.4, podemos asegurar que la construcción dada en el párrafo anterior a la Proposición 4.1 caracteriza los sistemas decimales de $(\mathbb{Z},+)$.

Sabemos que todo grupo abeliano $(G,+)$ admite una relación binaria $\leq$ tal que $(G,+,\leq)$ es un grupo abeliano linealmente ordenado si y sólo si $(G,+)$ es libre de torsión (véase [**30**]). Si $(G,\leq,+)$ es un grupo abeliano linealmente ordenado, entonces diremos que un elemento $g \in G$ es arquimediano si para todo $g' \in G$ existe $k \in \mathbb{N}\setminus\{0\}$ tal que $g' \leq kg$.

A continuación damos un resultado que caracteriza todas las extensiones decimales de $(\mathbb{Z},+)$.

PROPOSICIÓN 4.5. *Un grupo abeliano* $(G,+)$ *es una extensión decimal de* $(\mathbb{Z},+)$ *si y sólo si es libre de torsión y existe una relación binaria* $\leq$ *en* G *tal que* $(G,+,\leq)$ *es un grupo abeliano linealmente ordenado con al menos un elemento arquimediano.*

DEMOSTRACIÓN. Supongamos que $(G,+)$ es una extensión decimal $(\mathbb{Z},+)$, entonces existe un sistema decimal $(H,\oplus,d)$ de $(\mathbb{Z},+)$ tal que $(G,+)$ es isomorfo a $(\mathbb{Z}\times H,+_d)$. Sabemos que podemos definir sobre $(\mathbb{Z}\times H,+_d)$ un relación binaria $\leq$ tal que $(\mathbb{Z}\times H,+_d,\leq)$ sea un grupo abeliano linealmente ordenado (recordemos que $\leq$ fue definido por $(z_1,h_1) \leq (z_2,h_2)$ si $(z_2,h_2) -_d (z_1,h_1) \in \mathbb{N}\times H$). Esto hace que $(\mathbb{Z}\times H,+_d)$ sea libre de torsión. Veamos ahora que $(1,0)$ es un elemento arquimediano. Tomemos $(z,h) \in \mathbb{Z}\times H$. Si $z<0$, entonces $(z,h) \leq (1,0)$. Si $(a,h) \in \mathbb{N}\times H$, entonces $(a,h)+_d(0,-h) = (a+d(h,-h),'=)a+d(h,-h))(1,0)$. Deducimos así, que $(a+d(h,-h))(1,0) \geq (a,h)$, lo cual prueba que $(1,0)$ es arquimediano.

Sea $(G,+,\leq)$ un grupo abeliano linealmente ordenado y m un elemento arquimediano de G. Por la Proposición 4.1, $([0,m[,\oplus,d)$ es un sistema decimal de $(\mathbb{Z},+)$. Probemos que $(G,+)$ es isomorfo a $(\mathbb{Z}\times[0,m[,+_d)$. Para ello definimos

$$f : \mathbb{Z}\times[0,m[\to G,$$
$$f((z,h)) = zm+h.$$

Veamos que f es un isomorfismo:

- f es inyectiva: si $f((z_1,h_1)) = f((z_2,h_2))$, entonces $z_1m+h_1 = z_2m+h_2$. Ya que $h_1,h_2 \in [0,m[$, deducimos que $z_1 = z_2$ y que $h_1 = h_2$.

- f es sobreyectiva: sea $g \in G$, distinguimos dos casos:
  (a) Supongamos que $g \geq 0$. Por ser m un elemento arquimediano, existe $k \in \mathbb{N}$ tal que $km \leq g$ y $g < (k+1)m$. Por tanto $g - km \in [0, m[$ y $f((k, g - km)) = g$.
  (b) Supongamos $g < 0$. Claramente $-g > 0$. Usando (a), existen $k \in \mathbb{N}$ y $h \in [0, m[$ tales que $-g = km + h$. Por tanto, $g = -(k+1)m + (m-h)$. Si $h = 0$, entonces $f(-k, 0) = g$; si $h \neq 0$. Como $h \in [0, m[$, se tiene $m - h \in [0, m[$ y así $f((-(k+1), m-h)) = g$.
- f es un homomorfismo:

$$f((z_1, h_1) +_d (z_2, h_2)) = f((z_1 + z_2 + d(h_1, h_2), h_1 \oplus h_2)) =$$
$$= (z_1 + z_2 + d(h_1, h_2))m + (h_1 \oplus h_2) = z_1 m + z_2 m + d(h_1, h_2)m + (h_1 \oplus h_2) =$$
$$= z_1 m + z_2 m + h_1 + h_2 = z_1 m + h_1 + z_2 m + h_2 = f((z_1, h_1)) + f((z_2, h_2)).$$

□

2. Extensiones racionales

Centramos ahora nuestro estudio en los subgrupos de $(\mathbb{Q}, +)$. Diremos que un grupo $(G, +)$ es una **extensión racional** de $(\mathbb{Z}, +)$, si $(G, +)$ es isomorfo a un subgrupo no trivial de $(\mathbb{Q}, +)$. Si G es un subgrupo no trivial de $(\mathbb{Q}, +)$ y $\leq$ es el orden usual de $\mathbb{Q}$, entonces $(G, +, \leq)$ es un grupo abeliano linealmente ordenado con todos sus elementos positivos arquimedianos, de ahí que, por la Proposición 4.5, todo subgrupo no trivial de $(\mathbb{Q}, +)$ sea una extensión decimal de $(\mathbb{Z}, +)$. Veamos en primer lugar cómo caracterizar las extensiones racionales de $(\mathbb{Z}, +)$.

PROPOSICIÓN 4.6. *Un grupo $(G, +)$ es una extensión racional de $(\mathbb{Z}, +)$ si y sólo si $(G, +)$ es libre de torsión y para todo $(g_1, g_2) \in (G \setminus \{0\}) \times (G \setminus \{0\})$ existe $(z_1, z_2) \in (\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z} \setminus \{0\})$ tal que $z_1 g_1 = z_2 g_2$.*

DEMOSTRACIÓN. Supongamos que $(G, +)$ es una extensión racional de $(\mathbb{Z}, +)$. Claramente todo subgrupo no trivial de $(\mathbb{Q}, +)$ verifica estas condiciones, las cuales además se preservan bajo isomorfismos.

Recíprocamente, tomemos $a \in G \setminus \{0\}$. Si $g \in G$, entonces existe $(x, y) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ tal que $xa = yg$. Definimos la siguiente aplicación

$$f : G \to \mathbb{Q}, f(g) = \tfrac{x}{y}.$$

Veamos que f es un monomorfismo de grupos.

- f está bien definida: si $xa = yg$ y $\bar{x}a = \bar{y}g$, entonces $(x\bar{y})a = (y\bar{y})g$ y $(\bar{x}y)a = (y\bar{y})g$. Por tanto $(x\bar{y})a = (\bar{x}y)a$. Ya que $(G, +)$ es libre de torsión, tenemos que $x\bar{y} = \bar{x}y$, de donde deducimos que $\frac{x}{y} = \frac{\bar{x}}{\bar{y}}$.
- f es inyectiva: si $f(g_1) = \frac{x_1}{y_1} = \frac{x_2}{y_2} = f(g_2)$, entonces $x_1 a = y_1 g_1$, $x_2 a = y_2 g_2$ y $x_1 y_2 = x_2 y_1$. Por tanto $(x_1 y_2)a = (y_1 y_2)g_1$, $(x_2 y_1)a = (y_1 y_2)g_2$ y $(y_1 y_2)g_1 = (y_1 y_2)g_2$. Como $(G, +)$ es libre de torsión, obtenemos que $g_1 = g_2$.

- f es un homomorfismo: sean $g_1, g_2 \in G$. Supongamos que $f(g_1) = \frac{x_1}{y_1}$ y $f(g_2) = \frac{x_2}{y_2}$. Tenemos entonces que $x_1 a = y_1 g_1$ y $x_2 a = y_2 g_2$. Por tanto $(x_1 y_2)a = (y_1 y_2)g_1$, $(x_2 y_1)a = (y_1 y_2)g_2$ y $(x_1 y_2 + x_2 y_1)a = (y_1 y_2)(g_1 + g_2)$, de ahí que

$$f(g_1) + f(g_2) = \frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 y_2 + x_2 y_1}{y_1 y_2} = f(g_1 + g_2).$$

□

Para terminar esta sección damos el siguiente resultado que nos dice qué condición ha de cumplir un sistema decimal de $(\mathbb{Z}, +)$ para que el grupo que se define a partir de él sea una extensión racional. Antes de probarlo necesitamos recordar el concepto de grupo abeliano periódico.

Sea $(G, +)$ un grupo abeliano y $g \in G$. Recordemos que $O(g)$ se definía como

$$O(g) = \min\{k \in \mathbb{N} \setminus \{0\} \mid kg = 0\}.$$

Si $kg \neq 0$ para todo $k \in \mathbb{N} \setminus \{0\}$, decimos que $O(g) = \infty$. Un grupo abeliano $(G, +)$ es **periódico** si $O(g) \neq \infty$ para todo $g \in G$.

PROPOSICIÓN 4.7. *Sea $(H, \oplus, d)$ un sistema decimal de $(\mathbb{Z}, +)$. Entonces $(\mathbb{Z} \times H, +_d)$ es una extensión racional de $(\mathbb{Z}, +)$ si y sólo si $(H, \oplus)$ es un grupo abeliano periódico.*

DEMOSTRACIÓN. Sea $h \in H$. Por la Proposición 4.6, existen $z_1, z_2 \in \mathbb{Z} \setminus \{0\}$ tales que $z_1(0, h) = z_2(1, 0)$. En consecuencia $z_1 h = 0$.

Para lo otra implicación, tomemos $(H, \oplus)$ un grupo abeliano periódico.

- Veamos que $(\mathbb{Z} \times H, +_d)$ es libre de torsión. Sea $k \in \mathbb{N} \setminus \{0\}$ y $(z, h) \in (\mathbb{Z} \times H) \setminus \{(0,0)\}$. Si $kh = 0$, entonces $d(h, (k-1)h) = 1$. Usando que $d(h, ih) \in \{0, 1\}$, obtenemos que $kz + \sum_{i=1}^{k-1} d(h, ih) \neq 0$ y por tanto $k(z, h) = (kz + \sum_{i=1}^{k-1} d(h, ih), kh) \neq (0, 0)$.
- Ahora probamos que si $(z_1, h_1), (z_2, h_2) \in (\mathbb{Z} \times H) \setminus \{(0,0)\}$, entonces existen $x_1, x_2 \in (\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z} \setminus \{0\})$ tal que $x_1(z_1, h_1) = x_2(z_2, h_2)$. Para ello usamos las siguientes observaciones.
  - Sea $(a, h) \in (\mathbb{N} \times H) \setminus \{(0,0)\}$. Ya que H es periódico, existe $k \in \mathbb{N} \setminus \{0\}$ tal que $kh = 0$. Por tanto $k(a, h) = (ka + \sum_{i=1}^{k-1} d(h, ih), 0) = \overline{k}(1, 0)$ con $\overline{k} = ka + \sum_{i=1}^{k-1} d(h, ih)$. En consecuencia tenemos que para todo $(a, h) \in (\mathbb{N} \times H) \setminus \{(0,0)\}$ existen $k, \overline{k} \in \mathbb{N} \setminus \{0\}$ tales que $k(a, h) = \overline{k}(1, 0)$.
  - Sean $a \in \mathbb{N} \setminus \{0\}$ y $h \in H$. Sabemos que $-_d(-a, h) \in (\mathbb{N} \times H) \setminus \{(0,0)\}$. Por tanto existen $k, \overline{k} \in \mathbb{N} \setminus \{0\}$ tales que

$$k(-_d(-a, h)) = k(a - d(h, -h), -h) = \overline{k}(1, 0)$$

y por consiguiente $(-k)(-a, h) = \overline{k}(1, 0)$. Acabamos de probar que para todo $a \in \mathbb{N} \setminus \{0\}$ y $h \in H$, existen $z \in \mathbb{Z} \setminus \{0\}$ y $\overline{k} \in \mathbb{N} \setminus \{0\}$ tales que $z(-a, h) = \overline{k}(1, 0)$.

Tomemos ahora $(z_1,h_1),(z_2,h_2) \in (\mathbb{Z}\times H)\setminus\{(0,0)\}$. Usando las dos observaciones anterios, existen $k_1,\overline{k}_1,k_2,\overline{k}_2 \in \mathbb{Z}\setminus\{0\}$ tales que $k_1(z_1,h_1)=\overline{k}_1(1,0)$ y $k_2(z_2,h_2)=\overline{k}_2(1,0)$ y así $(k_1\overline{k}_2)(z_1,h_1)=(k_2\overline{k}_1)(z_2,h_2)$.

□

3. El grupo aditivo de los números racionales

Las Proposiciónes 4.5 y 4.7 nos dicen que la construcción de $(\mathbb{Z}\times H,+_d)$ con $(H,\oplus)$ un grupo periódico y $d: H\times H\to\{0,1\}$ verificando (1), (2), (3) y (4) clasifica, salvo isomorfismos, todos los subgrupos no triviales de $(\mathbb{Q},+)$. En esta sección, nuestro objetivo es mostrar que sobre H podemos imponer una nueva condición para que $(\mathbb{Z}\times H,+_d)$ sea isomorfo a $(\mathbb{Q},+)$.

Sea $[0,1[=\{x\in\mathbb{Q}\mid 0\le x<1\}$. Sabemos que este conjunto es un grupo abeliano con la operación:

$$x\oplus y=\begin{cases} x+y & \text{si } x+y<1,\\ x+y-1 & \text{si } x+y\ge 1.\end{cases}$$

Además, el grupo $([0,1[,\oplus)$ es isomorfo a $(\mathbb{Q}/\mathbb{Z},+)$.

En el siguiente lema se prueba una interesante propiedad que verifica este grupo.

LEMA 4.8. *Sea G un subgrupo de $([0,1[,\oplus)$. Entonces $G=[0,1[$ si y sólo si para todo $k\in\mathbb{N}\setminus\{0\}$ existe $g\in G$ tal que $O(g)=k$.*

DEMOSTRACIÓN. *Necesidad.* Trivial.

Suficiencia. Recíprocamente, todo elemento de $[0,1[$ es de la forma $\frac{x}{y}$ con $y\in\mathbb{N}\setminus\{0,1\}$ y $0\le x<y$. Ya que G es un subgrupo de $[0,1[$, para ver que $G=[0,1[$, sólo hemos de probar que $\frac{1}{k}\in G$ para todo $k\in\mathbb{N}\setminus\{0,1\}$. Sea $k\in\mathbb{N}\setminus\{0,1\}$ y $g\in G$ tal que $O(g)=k$. Existe $a\in\mathbb{N}$ satifaciendo que $0<a<k$, $g=\frac{a}{k}$ y $\mathrm{mcd}(a,k)=1$ (donde mcd denota el máximo común divisor). Además, si $\mathrm{mcd}(a,k)=1$, entonces existen $u,v\in\mathbb{Z}\setminus\{0\}$ tales que $au=1+kv$. Como $\frac{a}{k}=g\in G$, deducimos que $\frac{1}{k}=u\frac{1}{k}\in G$. □

Para probar la Proposición 4.10 necesitamos el siguiente lema.

LEMA 4.9. *Sea $(H,\oplus,d)$ un sistema decimal de $(\mathbb{Z},+)$ con $(H,\oplus)$ un grupo abeliano periódico y $f:(\mathbb{Z}\times H,+_d)\to(\mathbb{Q},+)$ un monomorfismo con $f((1,0))=1$. Entonces:*

(1) $\{f((0,h))\mid h\in H\}=[0,1[\cap\mathrm{Im}(f)$,
(2) $d(h_1,h_2)=0$ *si y sólo si* $f((0,h_1))+f((0,h_2))<1$,
(3) $[0,1[\cap\mathrm{Im}(f)$ *es un subgrupo de* $([0,1[,\oplus)$,
(4) $(H,\oplus)$ *es isomorfo a* $[0,1[\cap\mathrm{Im}(f)$.

DEMOSTRACIÓN. (1) Sea $(z,h) \in \mathbb{Z} \times H$. Entonces

$$O(h)f((z,h)) = f(O(h)(z,h)) = f((O(h)z + \sum_{i=1}^{O(h)-1} d(h,ih),0)) =$$

$$f((O(h)z + \sum_{i=1}^{O(h)-1} d(h,ih))(1,0)) = O(h)z + \sum_{i=1}^{O(h)-1} d(h,ih).$$

Por lo que

$$f((z,h)) = z + \frac{\sum_{i=1}^{O(h)-1} d(h,ih)}{O(h)}$$

y como $(\sum_{i=1}^{O(h)-1} d(h,ih))/O(h) \in [0,1[$, obtenemos que $f((z,h)) \in [0,1[$ si y sólo si $z = 0$.

(2) Supongamos que $d(h_1,h_2) = 0$. Entonces $(0,h_1) +_d (0,h_2) = (0,h_1 \oplus h_2)$. Usando que f es un homomorfismo y (1), deducimos que $f((0,h_1)) + f((0,h_2)) = f((0,h_1 \oplus h_2)) \in [0,1[$.

Recíprocamente, si $f((0,h_1)) + f((0,h_2)) < 1$, entonces $f((0,h_1) +_d (0,h_2)) < 1$ y por tanto $f((d(h_1,h_2),h_1 \oplus h_2)) < 1$. Por (1), obtenemos que $d(h_1,h_2) = 0$.

(3) Ya que para todo $x \in [0,1[\cap \mathrm{Im}(f)$ tenemos que $O(x) < \infty$ con la operación $\oplus$, sólo hemos de probar que si $x,y \in [0,1[\cap \mathrm{Im}(f)$, entonces $x \oplus y \in [0,1[\cap \mathrm{Im}(f)$. Para probarlo, veamos que si $h_1,h_2 \in H$, entonces $f((0,h_1)) \oplus f((0,h_2)) = f((0,h_1 \oplus h_2))$. Sabemos que $f((0,h_1)) \oplus f((0,h_2))$ es igual a $f((0,h_1)) + f((0,h_2))$ o $f((0,h_1)) + f((0,h_2)) - 1$ de acuerdo con que $f((0,h_1)) + f((0,h_2)) < 1$ o $f((0,h_1)) + f((0,h_2)) \geq 1$. Así, por (2), obtenemos que

$$f((0,h_1)) \oplus f((0,h_2)) = \begin{cases} f((0,h_1) +_d (0,h_2)) & \text{si } d(h_1,h_2) = 0, \\ f((0,h_1) +_d (0,h_2) -_d (1,0)) & \text{si } d(h_1,h_2) = 1. \end{cases}$$

Por tanto $f((0,h_1)) \oplus f((0,h_2)) = f((0,h_1 \oplus h_2))$ en ambos casos.

(4) Definimos la función $g : H \to [0,1[\cap \mathrm{Im}(f)$ por $g(h) = f((0,h))$. Usando que f es un monomorfismo y (1), podemos asegurar que g es biyectiva. Veamos ahora que g es un homomorfismo. Sea $h_1,h_2 \in H$. Tenemos que

$$g(h_1) \oplus g(h_2) = f((0,h_1)) \oplus f((0,h_2)) =$$

$$= \begin{cases} f((0,h_1)) + f((0,h_2)) & \text{if } f((0,h_1)) + f((0,h_2)) < 1, \\ f((0,h_1)) + f((0,h_2)) - f((1,0)) & \text{if } f((0,h_1)) + f((0,h_2)) \geq 1. \end{cases}$$

Ahora, usando (2)

$$g(h_1) \oplus g(h_2) = \begin{cases} f((0,h_1)) + f((0,h_2)) & \text{if } d(h_1,h_2) = 0, \\ f((0,h_1)) + f((0,h_2)) - f((1,0)) & \text{if } d(h_1,h_2) = 1. \end{cases}$$

En ambos casos obtenemos que

$$g(h_1) \oplus g(h_2) = f((0,h_1 \oplus h_2)) = g(h_1 \oplus h_2).$$

□

Veamos la condición que ha de verificar el grupo que se obtiene a partir de un sistema decimal para no ser sólo subgrupo de $(\mathbb{Q},+)$ sino además isomorfo a éste.

PROPOSICIÓN 4.10. *Sea $(H,\oplus,d)$ un sistema decimal de $(\mathbb{Z},+)$ con $(H,\oplus)$ un grupo abeliano periódico. Entonces $(\mathbb{Z}\times H,+_d)$ es isomorfo a $(\mathbb{Q},+)$ si y sólo si para todo $k\in\mathbb{N}\setminus\{0\}$ existe $h\in H$ tal que $O(h)=k$.*

DEMOSTRACIÓN. Sea $q\in\mathbb{Q}\setminus\{0\}$. La aplicación $h:\mathbb{Q}\to\mathbb{Q}$ definida por $h(x)=qx$ es un automorfismo de $\mathbb{Q}$. Por tanto, podemos suponer que existe un isomorfismo $\theta:\mathbb{Z}\times H\to\mathbb{Q}$ verificando que $\theta((1,0))=1$. Usando (4) del Lema 4.9 y el que $\mathrm{Im}(\theta)=\mathbb{Q}$, deducimos que $(H,\oplus)$ es isomorfo a $([0,1[,\oplus)$. Finalmente, aplicando el Lema 4.8 concluimos con que para todo $k\in\mathbb{N}\setminus\{0\}$ existe $h\in H$ tal que $O(h)=k$.

Recíprocamente, usando la Proposición 4.7, sabemos que existe un monomorfismo de $(\mathbb{Z}\times H,+_d)$ en $(\mathbb{Q},+)$. Como antes, podemos suponer que este monomorfismo envía $(1,0)$ en 1. Sea $f:\mathbb{Z}\times H\to\mathbb{Q}$ un monomorfismo tal que $f((1,0))=1$. Por (4) del Lema 4.9, obtenemos que la aplicación $g:H\to[0,1[\cap\mathrm{Im}(f)$ definida por $g(h)=f((0,h))$ es un isomorfismo. En consecuencia $\mathrm{Im}(g)$ es un subgrupo de $([0,1[,\oplus)$ verificando que para todo $k\in\mathbb{N}\setminus\{0\}$ existe $x\in\mathrm{Im}(g)$ tal que $O(x)=k$. Aplicando el Lema 4.8, tenemos que $\mathrm{Im}(g)=[0,1[$. Finalmente, repetiendo el razonamiento usado en la demostración de (1) del Lema 4.9, obtenemos que f es sobreyectiva y por tanto es un isomorfismo. □

CAPÍTULO 5

Extensiones ideales conmutativas de grupos abelianos

En este capítulo caracterizamos las extensiónes ideales de los grupos abelianos. Las extensiones ideales fueron introducidas por Clifford en [**19**] y desde entonces han sido muy estudiadas (véasen por ejemplo [**33**] y [**53**]). Probaremos que estas extensiones son aquellos semigrupos E que cumplen que E/R es un grupo abeliano, donde R es la más pequeña congruencia que hace E/R cancelativo. Estas caracterizaciones nos llevan a obtener un algoritmo para decidir a partir de una presentación de un monoide finitamente generado si éste es o no una extensión de un grupo abeliano. Dicho algoritmo nos llevará a presentar de forma natural un procedimiento que nos permitirá calcular el conjunto de idempotentes de un monoide finitamente generado. Este capítulo sigue un poco la línea de los algoritmos presentados en [**65**] y gran parte de sus contenidos se encuentra en [**69**].

1. Extensiones ideales de grupos abelianos

Sea S un semigrupo. Una **extensión ideal** de S es un semigrupo E que cumple que S es uno de sus ideales. En esta sección vamos a caracterizar los semigrupos que son extensiones ideales de grupos abelianos.

Vemos a continuación que existe una fuerte relación entre el concepto de extensión ideal de grupos abelianos y de existencia de elementos idempotentes y arquimedianos.

TEOREMA 5.1. *Sea E un semigrupo. Entonces E es una extensión ideal de un grupo abeliano si y sólo si E tiene un elemento arquimediano e idempotente.*

DEMOSTRACIÓN. Supongamos que E es una extesión ideal de un grupo G. Sea u el elemento neutro de G. Claramente u es un idempotente de E. Tomemos $x \in E$. Como G es un ideal de E, tenemos que $u+x \in G$. Así deducimos que existe $y \in G$ tal que $u+x+y=u$, y por tanto $1u = x+(u+y)$. Lo cual implica que u es un elemento arquimediano de E.

Recíprocamente, si u es un elemento arquimediano idempotente de E, entonces u pertenece a todo ideal de E y $u+E$ es un ideal minimal de E, lo cual hace que sea un grupo. □

Veamos otra caracterización de este tipo de extensiones ideales.

TEOREMA 5.2. *Sea E un semigrupo y R la más pequeña congruencia sobre E tal que E/R es cancelativo (esto es, $x\,R\,y$ si $x+z=y+z$ para algún $z \in E$). Entonces E es una extensión ideal de un grupo abeliano si y sólo si E/R es un grupo abeliano y E tiene al menos un elemento arquimediano.*

DEMOSTRACIÓN. Supongamos que E es una extensión ideal de un grupo abeliano G. Sea u el elemento neutro de G, el cual en vista de la demostración del Teorema 5.1 es arquimediano. Además tenemos que el elemento $[u]_R$ es un elemento idempotente en un semigrupo cancelativo, por tanto él es el único idempotente y por el ejercicio 2.6.1 de [**43**] un elemento neutro. El que E/R es un grupo se deduce del hecho de que u es arquimediano.

Recíprocamente, por el Teorema 5.1, es suficiente probar que E tiene un elemento arquimediano e idempotente. Por hipótesis, E tiene un elemento arquimediano m. Sea $[u]_R$ el elemento neutro de E/R. Entonces existe $x \in E$ tal que $[m]_R + [x]_R = [u]_R$, lo cual implica que $m+x+y = u+y$ para algún $y \in E$. Además $[u]_R + [u]_R = [u]_R$ y por tanto $2u+z = u+z$ para algún $z \in E$. Se sigue que

$$m+x+y+z+u = 2u+y+z = u+y+z.$$

Tomando $s = u+y+z$, tenemos que $m+x+s = s$. Ya que m es arquimediano $m+x$ también lo es y existe $k \in \mathbb{N} \setminus \{0\}$ y $v \in E$ tal que $k(m+x) = s+v$. Usando el que $m+x+s = s$, obtenemos $m+x+s+v = s+v$. Sustituyendo $s+v$ por $k(m+x)$, llegamos a que $(k+1)(m+x) = k(m+x)$. Por inducción sobre n, se puede probar que $(k+n)(x+m) = k(x+m)$; en particular $2(k(x+m)) = k(x+m)$, de donde tenemos que $k(x+m)$ es idempotente. El que $k(x+m)$ es arquimediano se demuestra fácilmente utilizando que m es arquimediano. □

COROLARIO 5.3. *Sea E un semigrupo finitamente generado. Entonces E es una extensión ideal de un grupo abeliano si y sólo si E/R es un grupo (con R definido como en el Teorema 5.2).*

DEMOSTRACIÓN. Si $s_1, \ldots, s_n$ son los generadores de E, entonces $s_1 + \cdots + s_n$ es un elemento arquimediano de E. En vista del Teorema 5.2, obtenemos el resultado deseado. □

2. Cálculo del conjunto de idempotentes de un monoide finitamente generado

Sea $x = (x_1, \ldots, x_p) \in \mathbb{Z}^p$. Recordemos que el soporte de x es el conjunto

$$\mathrm{Supp}(x) = \{i \in \{1, \ldots, p\} \mid x_i \neq 0\}.$$

Decimos que x es un elemento **positivo** de $\mathbb{N}^p$ si $\mathrm{Supp}(x) = \{1, \ldots, p\}$.

Sea σ una congruencia en $\mathbb{N}^p$ y $\rho = \{(a_1, b_1), \ldots, (a_t, b_t)\}$ uno de sus sistemas de generadores. Damos a continuación un algoritmo para, a partir de ρ, calcular todos los idempotentes de $\mathbb{N}^p/\sigma$. Lo primero que haremos será dar un método para decidir si $\mathbb{N}^p/\sigma$ tiene un elemento arquimediano idempotente, lo cual por el Teorema 5.1 es equivalente a decidir si $\mathbb{N}^p/\sigma$ es una extensión ideal de un grupo abeliano.

PROPOSICIÓN 5.4. *Sea σ una congruencia en $\mathbb{N}^p$. El monoide $\mathbb{N}^p/\sigma$ tiene un elemento arquimediano e idempotente si y sólo si M_σ tiene un elemento positivo.*

DEMOSTRACIÓN. Sea $[m]_\sigma$ un elemento idempotente y arquimediano de $\mathbb{N}^p/\sigma$. Entonces existe $k \in \mathbb{N}\setminus\{0\}$ y $c \in \mathbb{N}^p$ tal que $k[m]_\sigma = [m]_\sigma = [c+e_1+\cdots+e_p]_\sigma$. Por tanto $[c+e_1+\cdots+e_p]_\sigma$ es un idempotente de $\mathbb{N}^p/\sigma$ verificando que

$$2(c+e_1+\cdots+e_p)\sigma(c+e_1+\cdots+e_p).$$

Así, $(c+e_1+\cdots+e_p)$ es un elemento positivo de M_σ.

Recíprocamente, sea x un elemento de $M_\sigma \cap \mathbb{N}^p$ tal que $\mathrm{Supp}(x) = \{1,\ldots,p\}$. Tenemos que $(x,0) \in {\sim_{M_\sigma}}$, de lo cual, por el Lema 1.4, existe $c \in \mathbb{N}^p$ tal que $(x+c,c) \in \sigma$. Ya que $\mathrm{Supp}(x) = \{1,\ldots,p\}$, existe $k \in \mathbb{N}$ y $d \in \mathbb{N}^p$ tal que $kx = c+d$ (nótese que $[x]_\sigma$ es un elemento arquimediano de $\mathbb{N}^p/\sigma$). Por tanto

$$[(k+1)x]_\sigma = [x+c+d]_\sigma = [c+d]_\sigma = [kx]_\sigma.$$

Usando ahora inducción sobre n, deducimos que $[(k+n)x]_\sigma = [kx]_\sigma$ para todo $n \in \mathbb{N}$, lo cual, en particular, implica que $[2(kx)]_\sigma = [kx]_\sigma$ y por tanto $[kx]_\sigma$ es arquimediano. □

Como consecuencia del Teorema 5.1 y la Proposición 5.4, obtenemos un método para decidir a partir de ρ si un monoide $\mathbb{N}^p/\sigma$ es una extensión ideal de un grupo abeliano. Basta con determinar si M_σ tiene un elemento positivo y, una vez tenemos un sistema de generadores de M_σ, esto puede ser realizado usando el algoritmo MCP (presentado en [**58**]) o calculando el conjunto de elementos minimales de $M_\sigma \cap \mathbb{N}^p$ como se explica en [**67**] y ver si $m_1+\cdots+m_t$ es positivo.

El resto de la sección está dedicado al cálculo del conjunto de idempotentes de $\mathbb{N}^p/\sigma$. Para ello lo que haremos es buscar en todas y cada una de las componentes arquimedianas de $\mathbb{N}^p/\sigma$ y usaremos el hecho, ya comentado en el Capítulo 1, de que cada una de estas componentes tiene a lo sumo un elemento idempotente.

Dada una componente arquimediana C de $\mathbb{N}^p/\sigma$, definimos

$$\mathrm{Supp}(C) = \cup_{[x]\in C}\mathrm{Supp}(x),$$
$$\mathbb{N}^C = \{(x_1,\ldots,x_p) \in \mathbb{N}^p \mid x_i = 0 \text{ para todo } i \notin \mathrm{Supp}(C)\}.$$

El conjunto $\mathbb{N}^C$ es un subsemigrupo de $\mathbb{N}^p$ isomorfo a $\mathbb{N}^r$, con r el cardinal de $\mathrm{Supp}(C)$ (véase el Capítulo 1). Si $[x]_\sigma \in C$, entonces $x \in \mathbb{N}^C$. Denotamos por $\sigma_{\mathbb{N}^C}$ la restricción de σ a $\mathbb{N}^C$, esto es, para $a,b \in \mathbb{N}^C$, $a\sigma_{\mathbb{N}^C}b$ si y sólo si $a\sigma b$.

LEMA 5.5. *Sea σ una congruencia en $\mathbb{N}^p$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces C es una componente arquimediana de $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$.*

DEMOSTRACIÓN. Ya que $[x]_\sigma \in C$ implica que $x \in \mathbb{N}^C$, podemos pensar en C como un subconjunto de $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$. La demostración concluye teniendo en cuenta que C es una componente arquimediana de $\mathbb{N}^p/\sigma$. □

LEMA 5.6. *Sea σ una congruencia sobre $\mathbb{N}^p$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces C contiene un elemento arquimediano de $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$.*

DEMOSTRACIÓN. Sea $\{i_1,\ldots,i_r\} = \mathrm{Supp}(C)$. A partir de la definición de $\mathrm{Supp}(C)$ y de $\mathbb{N}^C$, tenemos que para todo $i_j \in \mathrm{Supp}(C)$ existe $[x_j]_\sigma \in C$ tal que su i_j-ésima coordenada no es igual a cero. El elemento $x = x_1+\cdots+x_r$ cumple que

$[x]_\sigma \in C$ y $\mathrm{Supp}(x) = \mathrm{Supp}(C)$. Fácilmente se puede comprobar que $[x]_\sigma$ es un elemento arquimediano de $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$. □

Si a es un elemento arquimediano de un semigrupo de S y $a\mathcal{N}b$, entonces b es también un elemento arquimediano de S. Así obtenemos el siguiente resultado.

COROLARIO 5.7. *Sea σ una congruencia sobre $\mathbb{N}^p$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces*

$$C = \{[x]_\sigma \mid [x]_\sigma \text{ es un elemento arquimediano de } \mathbb{N}^C/\sigma_{\mathbb{N}^C}\}.$$

Como ya sabemos, si a es un elemento arquimediano de un semigrupo S, entonces también lo es $a+c$ para todo $c \in S$.

COROLARIO 5.8. *Sea σ una congruencia sobre $\mathbb{N}^p$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces C es un ideal de $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$.*

Nótese que si σ es una congruencia de $\mathbb{N}^p$ y C una componente arquimediana, no tiene por qué ser un ideal de $\mathbb{N}^p/\sigma$ (eso sólo ocurre con la componente maxima).

Como consecuencia de estos dos últimos resultados podemos enunciar lo siguiente.

COROLARIO 5.9. *Sea σ una congruencia sobre $\mathbb{N}^p$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces C tiene un elemento idempotente si y sólo si $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$ tiene un elemento arquimediano e idempotente.*

El conjunto $\mathrm{Supp}(C)$ puede ser calculado a partir de ρ, tal y como se explica en [**65**], y un sistema de generadores ρ^C de $\sigma_{\mathbb{N}^C}$ puede ser obtenido de ρ usando eliminación sobre las coordenadas no pertenecientes a $\mathrm{Supp}(C)$ (véase el Capítulo 1). El concepto de elemento positivo de $M_{\sigma_{\mathbb{N}^C}}$ se traslada a un elemento de $M_{\sigma_{\mathbb{N}^C}} \cap \mathbb{N}^C$ tal que su soporte coincide con $\mathrm{Supp}(C)$. De esta forma, usando la Proposición 5.4 y el comentario hecho tras ella, podemos decir cuándo $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$ tiene un elemento arquimediano e idempotente y por tanto decir cuándo C tiene un idempotente. Supuesto que tal elemento existe, para calcularlo, siguiendo la Proposición 5.4, es suficiente encontrar un elemento positivo $x \in M_{\sigma_{\mathbb{N}^C}}$ (en este caso un elemento $x \in \mathbb{N}^C \cap M_{\sigma_{\mathbb{N}^C}}$ tal que $\mathrm{Supp}(x) = \mathrm{Supp}(C)$) y entonces encontrar $k \in \mathbb{N}\setminus\{0\}$ para el que $(k+1)x = kx$. Ya que sabemos calcular el conjunto de componentes arquimedianas de $\mathbb{N}^p/\sigma$ una vez conocido ρ (véase [**65**]), podemos calcular el conjunto de todos los idempotentes de $\mathbb{N}^p/\sigma$, ya que cada componente arquimediana contiene a lo sumo un elemento idempotente.

ALGORITMO 5.10. Sea $\rho = \{(a_1,b_1),\ldots,(a_r,b_r)\} \subset \mathbb{N}^p \times \mathbb{N}^p$ un sistema de generadores de la congruencia σ. Este algoritmo nos devuelve el conjunto de elementos idempotentes de $\mathbb{N}^p/\sigma$.

(1) Calcular las componentes arquimedianas $\{C_1,\ldots,C_s\}$ de $\mathbb{N}^p/\sigma$.
(2) Para todo $i \in \{1,\ldots,s\}$ calcular $\sigma_{\mathbb{N}^{C_i}}$.
(3) Para todo $i \in \{1,\ldots,s\}$ calcular las ecuaciones de definición de $M_{\sigma_{\mathbb{N}^{C_i}}}$.
(4) Para todo $i \in \{1,\ldots,s\}$ calcular las soluciones minimales no negativas $\{m_1^{C_i},\ldots,m_{t_{C_i}}^{C_i}\}$ del sistema de ecuaciones de $M_{\sigma_{\mathbb{N}^{C_i}}}$ (usamos para ello [**67**]).

(5) Para todo $i \in \{1,\ldots,s\}$, si $\operatorname{supp}(m_1^{C_i}+\ldots+m_{t_{C_i}}^{C_i}) = \operatorname{supp}(C)$, entonces encontrar $k \in \mathbb{N}\backslash\{0\}$ tal que $(k+1)(m_1^{C_i}+\ldots+m_{t_{C_i}}^{C_i})\sigma_{\mathbb{N}^{C_i}} k(m_1^{C_i}+\ldots+m_{t_{C_i}}^{C_i})$ y devolver $k(m_1^{C_i}+\ldots+m_{t_{C_i}}^{C_i})$.

□

EJEMPLO 5.11. Sea $\rho = \{((3,5,3),(1,4,2)),((5,0,0),(0,7,0))\}$ un sistema de generadores de la congruencia σ. Aplicamos el anterior algoritmo para calcular el conjunto de idempotentes de $\mathbb{N}^p/\sigma$.

(1) Las componentes arquimedianas de $\mathbb{N}^p/\sigma$ son

$$C_1 = \{[(0,0,0)]\},$$
$$C_2 = \{[(0,0,z)] \mid z \geq 0\},$$
$$C_3 = \{[(x,y,0)] \mid x \geq 1, y \geq 1\}$$
$$C_4 = \{[(x,y+1,z+1)] \mid (x,y,z) \in \mathbb{N}^3\} \cup$$
$$\cup\{[(x+1,y,z+1)] \mid (x,y,z) \in \mathbb{N}^3\} \cup \{[(x+1,y+1,z+1)] \mid (x,y,z \in \mathbb{N}^3\}.$$

(2) Obtenemos que

$$\sigma_{\mathbb{N}^{C_1}} = \langle((0,0,0),(0,0,0))\rangle,$$
$$\sigma_{\mathbb{N}^{C_2}} = \langle((0,0,0),(0,0,0))\rangle,$$
$$\sigma_{\mathbb{N}^{C_3}} = \langle((0,7,0),(5,0,0))\rangle$$

y

$$\sigma_{\mathbb{N}^{C_4}} = \langle(((3,5,2),(1,4,2)),((5,0,0),(0,7,0))\rangle.$$

(3) Calculamos ahora las ecuaciones de $M_{\sigma_{\mathbb{N}^{C_3}}}$ y $M_{\sigma_{\mathbb{N}^{C_4}}}$, las cuales están generadas por $\{(5,-7,0)\}$ y $\{(2,-1,0),(5,-7,0)\}$, respectivamente. Éstas son $7x_1+5x_2=0$ y $-7x_1-5x_2+19x_3=0$, respectivamente.

(4) Al calcular el conjunto de soluciones minimales del anterior sistema de ecuaciones, obtenemos $\{(0,0,1)\}$ para $M_{\sigma_{\mathbb{N}^{C_3}}}$ y

$$\{(0,19,5),(1;10,3),(2,1,1),(19,0,7)\}$$

para $M_{\sigma_{\mathbb{N}^{C_4}}}$

(5) Para $M_{\sigma_{\mathbb{N}^{C_3}}}$ no obtenemos ningún idempotente y para $M_{\sigma_{\mathbb{N}^{C_4}}}$ obtenemos el elemento $(22,30,16)$ el cual satisface que $(22,30,16)\sigma_{\mathbb{N}^{C_4}} 2(22,30,16)$. Obtenemos así que $[(22,30,16)]_\sigma$ es el único elemento idempotente y arquimediano de $\mathbb{N}^3/\sigma$.

□

CAPÍTULO 6

Semigrupos finitamente generados débilmente reductivos

Dado un semigrupo S decimos que una aplicación $\lambda : S \to S$ es una traslación si verifica que $\lambda(x+y) = \lambda(x) + y$ para todo $x, y \in S$. El conjunto $\{\lambda \mid \lambda$ es una traslación de $S\}$ es conocido como la **envolvente de traslaciones de** S y verifica ser, junto con la operación composición, un monoide commutativo (véase **[33]**, **[42]**, **[53]** ó **[55]**). Los semigrupos débilmente reductivos han sido muy estudiados debido a que el semigrupo que forma su envolvente de traslaciones forma una extensión ideal suya. Es por ello que estos semigrupos juegan un papel muy importante en la teoría de extensiones de ideales (véase por ejemplo **[33]** ó **[53]**). Nuestro principal objetivo en este capítulo es dar un algoritmo para determinar a partir de una presentación de un semigrupo finitamente generado cuándo éste es débilmente reductivo. Probaremos que si imponemos a un semigrupo finitamente generado y reductivo la condición de ser arquimediano, entonces obtenemos un semigrupo cancelativo. Estos resultados y el concepto de $\mathcal{N}$-semigrupo nos permitirá dar un teorema de estructura para los semigrupos finitamente generados débilmente reductivos.

1. Un algoritmo previo

Sea $(S,+)$ un semigrupo finitamente generado. Sabemos que existe $p \in \mathbb{N}$ y una congruencia sobre $\mathbb{N}^p \setminus \{0\}$ tal que $S \cong \mathbb{N}^p \setminus \{0\}/\sigma$. Sea $\preceq$ un orden lineal admisible sobre $\mathbb{N}^p$ verificando que para todo $z \in \mathbb{N}^p$ el conjunto $\{y \in \mathbb{N}^p \mid y \preceq z\}$ es finito. Un ejemplo de este tipo de órdenes es el orden grado total de $\mathbb{N}^p$, que se define como $(a_1,\ldots,a_p) \preceq_{td} (b_1,\ldots,b_p)$ si y sólo si $\sum_{i=1}^p a_i < \sum_{i=1}^p b_i$ ó $(a_1,\ldots,a_p) \preceq_{lex} (b_1,\ldots,b_p)$ caso que $\sum_{i=1}^p a_i = \sum_{i=1}^p b_i$.

Dado $x \in \mathbb{N}^p \setminus \{0\}$, nos interesa saber cómo calcular el conjunto

$$A_x = \{y \in \mathbb{N}^p \setminus \{0\} \mid y\sigma x,\ y \preceq x\}.$$

Para ello vamos a suponer que $\rho = \{(\alpha_1,\beta_1),\ldots,(\alpha_t,\beta_t)\}$ es un sistema canónico de generadores de σ con respecto a $\preceq$. Un algoritmo para calcular el conjunto A_x es el siguiente.

ALGORITMO 6.1. La entrada es un elemento $x \in \mathbb{N}^p \setminus \{0\}$. El algoritmo nos devuelve el conjunto A_x.

(1) Calcular $\mathrm{NF}_\rho(x)$.
(2) $A_x = \{\mathrm{NF}_\rho(x)\}$.
(3) $B = \{\mathrm{NF}_\rho(x)\}$.
(4) Mientras $B \neq \emptyset$ hacer

Elegir $u \in B$.
$B := (B \backslash \{u\}) \cup \{u - \beta_j + \alpha_j \mid u - \beta_j \in \mathbb{N}^p,\ u - \beta_j + \alpha_j \preceq x\}$.
$A_x := A_x \cup \{u - \beta_j + \alpha_j \mid u - \beta_j \in \mathbb{N}^p,\ u - \beta_j + \alpha_j \preceq x\}$.
(5) Devolver A_x.

□

Téngase en cuenta la importancia de que el conjunto $\{y \in \mathbb{N}^p \mid y \preceq x\}$ sea finito. Si tomásemos un orden que no cumpliese esta condición para ciertos elementos $x \in \mathbb{N}^p \setminus \{0\}$ el algoritmo nunca terminaría. Por esta razón, en el resto del capítulo supondremos que estamos usando un orden de este tipo como por ejemplo el orden total. Un ejemplo de orden que no cumple esta propiedad es el lexicográfico sobre $\mathbb{N}^p$ cuando $p \geq 2$.

2. Un algoritmo para determinar si un semigrupo finitamente generado es débilmente reductivo

Un semigrupo $(S,+)$ es **débilmente reductivo** si siempre que $x+s = y+s$ para todo $s \in S$ se tiene que $x = y$.

Sea $(S,+)$ un semigrupo como el de la sección anterior y $\rho = \{(\alpha_1,\beta_1),\ldots,(\alpha_t,\beta_t)\}$ un sistema canónico de generadores de σ con respecto a un orden lineal admisible $\preceq$ sobre $\mathbb{N}^p$ cumpliendo la condición impuesta en el Algoritmo 6.1 (por ejemplo el orden total). En lo que queda de capítulo denotaremos por I al conjunto $\mathbb{N}^p \setminus \{0\}$. Nuestro objetivo es dar un algoritmo para determinar a partir de ρ cuando el semigrupo I/σ (y como consecuencia S) es débilmente reductivo.

Una primera aproximación a la solución de este problema nos la da el siguiente resultado.

LEMA 6.2. *Las siguientes afirmaciones son equivalentes.*

(1) El semigrupo I/σ es débilmente reductivo.
(2) Si $x,y \in I$ y $x+e_i \sigma y+e_i$ para todo $i \in \{1,\ldots,p\}$, entonces $x\sigma y$.

DEMOSTRACIÓN. *(1) implica (2).* Si $x+e_i\sigma y+e_i$ para todo $i \in \{1,\ldots,p\}$, entonces $[x]_\sigma + [e_i]_\sigma = [x+e_i]_\sigma = [y+e_i]_\sigma = [y]_\sigma + [e_i]_\sigma$ para todo $i \in \{1,\ldots,p\}$. Por tanto $[x]_\sigma + [z]_\sigma = [y]_\sigma + [z]_\sigma$ para todo $[z]_\sigma \in I/\sigma$. Usando que I/σ es débilmente reductivo, deducimos que $[x]_\sigma = [y]_\sigma$ y por tanto $x\sigma y$.

(2) implica (1). Si $[x]_\sigma + [z]_\sigma = [y]_\sigma + [z]_\sigma$ para todo $[z]_\sigma \in I/\sigma$, entonces $x+e_i\sigma y+e_i$ para todo $i \in \{1,\ldots,p\}$. En consecuencia $x\sigma y$ y así $[x]_\sigma = [y]_\sigma$. □

Por el Lema 6.2, podemos decir que si I/σ no es débilmente reductivo, entonces existen $a,b \in I$ tales que $(a+e_i, b+e_i) \in \sigma$ para todo $i \in \{1,\ldots,p\}$ y $(a,b) \notin \sigma$. Ya que $(a,b) \notin \sigma$, tenemos que $(\mathrm{NF}_\rho(a), \mathrm{NF}_\rho(b)) \notin \sigma$. Además, $(\mathrm{NF}_\rho(a)+e_i, \mathrm{NF}_\rho(b)+e_i) \in \sigma$ para todo $i \in \{1,\ldots,p\}$, debido a que $(a+e_i, b+e_i) \in \sigma$. Como $(\mathrm{NF}_\rho(a), \mathrm{NF}_\rho(b)) \notin \sigma$, obtenemos que $\mathrm{NF}_\rho(a) \neq \mathrm{NF}_\rho(b)$. Sin pérdida de generalidad, podemos suponer que $\mathrm{NF}_\rho(b) \prec \mathrm{NF}_\rho(a)$ y por ello que $\mathrm{NF}_\rho(b)+e_i \prec \mathrm{NF}_\rho(a)+e_i$. En consecuencia, $\mathrm{NF}_\rho(a)+e_i \neq \mathrm{NF}_\rho(a+e_i)$ y por tanto $\mathrm{NF}_\rho(a)+e_i \notin \mathrm{Im}(\mathrm{NF}_\rho)$. Nótese también que trivialmente $\mathrm{NF}_\rho(a) \in \mathrm{Im}(\mathrm{NF}_\rho)$.

Tenemos por tanto el siguiente resultado.

LEMA 6.3. *El semigrupo I/σ no es débilmente reductivo si y sólo si existe $(x,y) \in I \times I$ cumpliendo la siguiente condición:*

(1) $(x,y) \notin \sigma$,
(2) $x \in \mathrm{Im}(\mathrm{NF}_\rho)$,
(3) $x+e_i \notin \mathrm{Im}(\mathrm{NF}_\rho)$ *para todo* $i \in \{1,\ldots,p\}$,
(4) $(x+e_i, y+e_i) \in \sigma$ *para todo* $i \in \{1,\ldots,p\}$,
(5) $y \prec x$.

Veremos a continuación que sólo existe un número finito de elementos de I que satisfagan las condiciones (2) y (3) del Lema anterior.

Dados $x = (x_1,\ldots,x_p)$, $y = (y_1,\ldots,y_p) \in \mathbb{N}^p$, denotamos por $x \vee y$ al elemento $(\text{máximo}\{x_1,y_1\},\ldots,\text{máximo}\{x_p,y_p\})$.

LEMA 6.4. *Si $x \in \mathrm{Im}(\mathrm{NF}_\rho)$ y $x+e_i \notin \mathrm{Im}(\mathrm{NF}_\rho)$ para todo $i \in \{1,\ldots,p\}$, entonces existe $\{\alpha_{l_1},\ldots,\alpha_{l_p}\} \subseteq \{\alpha_1,\ldots,\alpha_t\}$ cumpliendo las siguientes condiciones:*

(1) para todo $j,k \in \{1,\ldots,p\}$ con $j \neq k$ se tiene que $(\alpha_{l_k})_j < (\alpha_{l_j})_j$,
(2) $x = ((\alpha_{l_1})_1 - 1,\ldots,(\alpha_{l_p})_p - 1)$.

DEMOSTRACIÓN. Recordemos que

$$\mathrm{Im}(\mathrm{NF}_\rho) = \{x \in I \mid x - \alpha_i \notin \mathbb{N}^p \text{ para todo } i \in \{1,\ldots,t\}\}.$$

Tomemos $j \in \{1,\ldots,p\}$, como $x+e_j \notin \mathrm{Im}(\mathrm{NF}_\rho)$, entonces existen $l_j \in \{1,\ldots,t\}$ y $d_j \in \mathbb{N}^p$ tales que $x+e_j = \alpha_{l_j} + d_j$. Así, debido a que $x \in \mathrm{Im}(\mathrm{NF}_\rho)$, tenemos que $\alpha_{l_j} - e_j \in \mathbb{N}^p$. Por tanto, $x = (\alpha_{l_1} - e_1) + d_1 = \cdots = (\alpha_{l_p} - e_p) + d_p$, de donde $x = ((\alpha_{l_1} - e_1) \vee \ldots \vee (\alpha_{l_p} - e_p)) + y$ para algún $y \in \mathbb{N}^p$. Si $y \neq 0$, entonces existe $j \in \{1,\ldots,p\}$ tal que $y - e_j \in \mathbb{N}^p$, por lo que $x - \alpha_{l_j} \in \mathbb{N}^p$, lo cual es absurdo ya que $x \in \mathrm{Im}(\mathrm{NF}_\rho)$. Ha de suceder por tanto que $x = (\alpha_{l_1} - e_i) \vee \ldots \vee (\alpha_{l_p} - e_p)$, llegando a que $(x)_k \geq (\alpha_{l_j})_k$ para todo $k \neq j$ y $(x)_j \geq (\alpha_{l_j})_j - 1$.

Probemos ahora (1). Si $(\alpha_{l_j})_j \leq (\alpha_{l_k})_j$ para algun $k \neq j$, entonces

$$(\alpha_{l_j})_j - 1 < (\alpha_{l_k})_j \leq \text{máximo}\{(\alpha_{l_1})_j,\ldots,(\alpha_{l_j})_j - 1,\ldots,(\alpha_{l_p})_j\} = (x)_j$$

y por tanto $(\alpha_{l_j})_j \leq (x)_j$. En consecuencia $(\alpha_{l_j})_k \leq (x)_k$ para todo $k \in \{1,\ldots,p\}$. Esto implica que $x - \alpha_{l_j} \in \mathbb{N}^p$, contradiciendo el que $x \in \mathrm{Im}(\mathrm{NF}_\rho)$.

Finalmente, para probar (2), sólamente hemos de tener en cuenta que $x = (\alpha_{l_1} - e_1) \vee \ldots \vee (\alpha_{l_p} - e_p)$ y aplicar (1). □

COROLARIO 6.5. *Sea σ una congruencia sobre I que admite un sistema canónico de generadores con cardinal menor que p. Entonces I/σ es débilmente reductivo.*

DEMOSTRACIÓN. Por el Lema 6.3, sabemos que si I/σ no es débilmente reductivo, entonces existe $x \in \mathrm{Im}(\mathrm{NF}_\rho)$ tal que $x+e_i \notin \mathrm{Im}(\mathrm{NF}_\rho)$ para todo $i \in \{1,\ldots,p\}$. Usando el Lema 6.4 y ya que el conjunto $\{\alpha_{l_1},\ldots,\alpha_{l_p}\}$ tiene p elementos, el cardinal de ρ es mayor o igual que p. □

Completamos esta sección con un algoritmo que nos permitirá decidir cuando un semigrupo finitamente generado es o no débilmente reductivo.

ALGORITMO 6.6. Sea $\rho = \{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$ un sistema canónico de generadores de una congruencia σ sobre $I = \mathbb{N}^p \setminus \{0\}$ con respecto a un orden lineal admisible $\preceq$. El algoritmo nos devolverá "VERDADERO" caso de que el el semigrupo I/σ sea débilmente reductivo y "FALSO" en otro caso.

(1) Calcular el conjunto

$$X = \{x \in I \mid x \in \mathrm{Im}(\mathrm{NF}_\rho),\ x + e_i \notin \mathrm{Im}(\mathrm{NF}_\rho) \text{ para todo } i \in \{1, \ldots, p\}\}$$

(téngase en cuenta que el Lema 6.4 nos da un método para calcular X).

(2) Para todo $x \in X$ e $i \in \{1, \ldots, p\}$, calcular el conjunto

$$C_x = \bigcap_{i=1}^{p} \{z - e_i \in \mathbb{N}^p \setminus \{0\} \mid z \in A_{x+e_i}\}$$

(usamos el Algoritmo 6.1 para calcular A_{x+e_i}).

(3) Para todo $x \in X$ e $y \in C_x \setminus \{x\}$, calcular cuando $(x, y) \in \sigma$. Si para algún par $(x, y) \notin \sigma$, devolver "FALSO".

(4) Devolver "VERDADERO".

□

Veamos a continuación algunos ejemplos de utilización de este algoritmo.

EJEMPLO 6.7. Sea σ la congruencia generada sobre $I = \mathbb{N} \setminus \{0\}$ por $\rho = \{(4, 2)\}$. Fácilmente se puede comprobar que ρ es un sistema canónico de generadores de σ con respecto al orden usual de $\mathbb{N}$. Aplicando ahora el Algoritmo 6.6 obtenemos:

(1) $X = \{3\}$.

(2) Para $x = 3$ tenemos que $A_4 = \{z \in [4] \mid z \leq 4\} = \{2, 4\}$ y $C_3 = \{1, 3\}$.

(3) Hemos de ver si el par $(3, 1)$ pertenece a σ. Claramente $(3, 1) \notin \sigma$.

Por tanto el algoritmo devuelve "FALSO" y por ello el semigrupo I/σ no es débilmente reductivo. Además del algoritmo se deduce también que $[3]_\sigma \neq [1]_\sigma$ y que $[3]_\sigma + [1]_\sigma = [1]_\sigma + [1]_\sigma$. En este caso $x = 3$ e $y = 1$. □

EJEMPLO 6.8. Tomemos ahora σ la congruencia generada sobre $I = \mathbb{N}^2 \setminus \{0\}$ por

$$\rho = \{((7, 7), (3, 8)), ((3, 12), (5, 7)), ((5, 11), (3, 7)), ((15, 2), (11, 3))\}.$$

Puede probarse que ρ es un sistema canónico de generadores de σ con respecto al orden total de $\mathbb{N}^2$. Aplicamos ahora el Algoritmo 6.6.

(1) Usamos el Lema 6.4 para calcular X. Obtenemos que X es un subconjunto de

$$\{(6, 11), (6, 10), (6, 1), (2, 6), (2, 10), (2, 1),$$
$$(4, 6), (4, 11), (4, 1), (14, 6), (14, 11), (14, 10)\}.$$

Eliminamos de este conjunto los elementos z tales que $z \notin \mathrm{Im}(\mathrm{NF}_\rho)$ y aquellos que $z + e_1 \in \mathrm{Im}(\mathrm{NF}_\rho)$ ó $z + e_2 \in \mathrm{Im}(\mathrm{NF}_\rho)$. Así,

$$X = \{(6, 10), (4, 11), (14, 6)\}.$$

(2) Calculamos ahora $C_{(6,10)}$, $C_{(4,11)}$ y $C_{(14,6)}$. Para ello aplicamos el Algoritmo 6.1 a los elementos $x + e_1$ y $x + e_2$ con $x \in X$.

- Para $x = (6,10)$ tenemos que $A_{x+e_1} = \{(7,10),(3,11)\}$ y $A_{x+e_2} = \{(6,11),(4,7)\}$, llegando a que $C_{(6,10)} = \{(6,10)\}$.
- Para $x = (4,11)$ tenemos que $A_{x+e_1} = \{(5,11),(3,7)\}$ y $A_{x+e_2} = \{(4,12),(6,7)\}$. Obtenemos que $C_{(4,11)} = \{(4,11)\}$.
- Para $x = (14,6)$

$$A_{x+e_1} = \{(15,6),(3,9),(3,18),(5,13),(7,8),(9,12)\},$$
$$A_{x+e_2} = \{(14,7),(4,14),(6,9),(8,13),(10,8)\}.$$

Por tanto, $C_{(14,6)} = \{(14,6),(4,13),(6,8),(8,12),(10,7)\}$.

(3) Si encontramos dos elementos $x \in X$ y $y \in C_x \backslash \{x\}$ tales que $(x,y) \notin \sigma$, entonces el algoritmo devuelve "FALSO". Tomamos $x = (14,6)$ e $y = (6,8) \in C_{(14,6)}$. Claramente $(14,6),(6,8) \in \mathrm{Im}(\mathrm{NF}_\rho)$ y $(14,6) \neq (6,8)$. Por tanto, $((14,6),(6,8)) \notin \sigma$ y el algoritmo nos devuelve "FALSO".

Por tanto el semigrupo I/σ no es débilmente reductivo. □

EJEMPLO 6.9. Veamos ahora un ejemplo de un semigrupo débilmente reductivo. Sea σ la congruencia de $I = \mathbb{N}^3 \backslash \{0\}$ con sistema de generadores

$$\rho = \{((1,0,1),(0,2,0)),((2,1,0),(0,0,2)),$$
$$((3,0,0),(0,1,1)),((1,3,0),(0,0,3)),(0,5,0),(0,0,4))\}.$$

Puede probarse que ρ es un sistema canónico de generadores de σ con respecto a el orden total de $\mathbb{N}^3$. Aplicando el Algoritmo 6.6, obtenemos lo siguiente:

(1) Usando el Lema 6.4, llegamos a que X es un subconjunto de

$$\{(1,2,0),(1,4,0),(2,0,0),(2,2,0),(2,4,0),(0,4,0)\}.$$

Eliminando de este conjunto los elementos z tales que $z \notin \mathrm{Im}(\mathrm{NF}_\rho)$ y aquellos tales que $z+e_1 \in \mathrm{Im}(\mathrm{NF}_\rho)$ ó $z+e_2 \in \mathrm{Im}(\mathrm{NF}_\rho)$ ó $z+e_3 \in \mathrm{Im}(\mathrm{NF}_\rho)$, obtenemos que

$$X = \{(1,2,0),(2,0,0)\}.$$

(2) Calculamos ahora los conjuntos C_x para cada uno de los elementos de X.
- Para $x = (1,2,0)$, tenemos que $A_{x+e_1} = \{(2,2,0),(0,1,2)\}$, $A_{x+e_2} = \{(1,3,0),(0,0,3)\}$ y $A_{x+e_3} = \{(1,2,1),(0,4,0)\}$. Así obtenemos que $C_{(1,2,0)} = \{(1,2,0)\}$.
- Para $x = (2,0,0)$, $A_{x+e_1} = \{(3,0,0),(0,1,1)\}$, $A_{x+e_2} = \{(2,1,0),(0,1,2)\}$ y $A_{x+e_3} = \{(2,0,1),(1,2,1)\}$, llegando a que $C_{(2,0,0)} = \{(2,0,0)\}$.

(3) Ya que para todo $x \in X$ los conjuntos C_x contienen solamente un elemento, no hay pares de elementos x,y tales que $x \in X$ y $y \in C_x$ con $(x,y) \notin \sigma$.

(4) Devolver "VERDADERO".

El algoritmo nos devuelve "VERDADERO" y por tanto el semigrupo I/σ es débilmente reductivo. □

3. Semigrupos finitamente generados débilmente reductivos y arquimedianos

Claramente, todo semigrupo cancelativo es débilmente reductivo. Nuestro objetivo en esta sección es probar que caso de que el semigrupo sea arquimediano y finitamente generado, el recíproco también es cierto.

TEOREMA 6.10. *Sea* $(S,+)$ *un semigrupo finitamente generado, débilmente reductivo y arquimediano. Entonces* $(S,+)$ *es un semigrupo cancelativo.*

DEMOSTRACIÓN. Sea $\{s_1,\ldots,s_p\}$ un sistema de generadores de S. Si S no es cancelativo, entonces existen $s,t,x \in S$ tales que $s \neq t$ y $s+x=t+x$. Ya que S es arquimediano, para todo $i \in \{1,\ldots,p\}$ existe $k_i \in \mathbb{N}\setminus\{0\}$ e $y_i \in S$ tal que $k_i s_i = x+y_i$. Por tanto $s+k_1s_1 = t+k_1s_1,\ldots,s+k_ps_p = t+k_ps_p$ y así si $s+(a_1s_1+\ldots+a_ps_p) \neq t+(a_1s_1+\ldots+a_ps_p)$, entonces $(a_1,\ldots,a_p) \leq (k_1,\ldots,k_p)$ ($\leq$ denota el orden usual de $\mathbb{N}^p$). Como el conjunto de p-tuplas menores ó iguales que $(k_1,\ldots,k_p)$ (con el orden usual de $\mathbb{N}^p$) es finito y S es débilmente reductivo, el conjunto

$$M = \text{maximales}_{\leq}\left\{ (a_1,\ldots,a_p) \in \mathbb{N}^p\setminus\{0\} \;\middle|\; \begin{array}{l} s+(a_1s_1+\ldots+a_ps_p) \neq \\ \neq t+(a_1s_1+\ldots+a_ps_p) \end{array} \right\}.$$

es finito y no vacío. Si $(d_1,\ldots,d_p) \in M$, entonces $s+d_1s_1+\ldots+d_ps_p \neq t+d_1s_1+\ldots+d_ps_p$ y por la maximalidad de $(d_1,\ldots,d_p)$ tenemos que

$$(s+d_1e_1+\ldots+d_pe_p)+e_i = (t+d_1e_1+\ldots+d_pe_p)+e_i$$

para todo $i \in \{1,\ldots,p\}$. Usando ahora que S es débilmente reductivo y aplicando el Lema 6.2, obtenemos que $s+d_1e_1+\ldots+d_ps_p = t+d_1s_1+\ldots+d_ps_p$, lo cual contradice el que $(d_1,\ldots,d_p) \in M$. □

Nos disponemos ahora a dar una descripción de la estructura de los semigrupos finitamente generados, débilmente reductivos y arquimedianos. Para ello necesitamos recordar previamente algunos conceptos y resultados.

PROPOSICIÓN 6.11. *Un semigrupo cancelativo arquimediano tiene un idempotente si y sólo si es un grupo.*

Recordemos que un $\mathcal{N}$-semigrupo es un semigrupo cancelativo arquimediano sin elementos idempotentes (ver capítulo 3). La siguiente Proposición, probada por Tamura en [**79**], caracteriza a todos los $\mathcal{N}$-semigrupos.

PROPOSICIÓN 6.12. *Sea* $(G,\oplus)$ *un grupo e* $\mathrm{I}: G\times G \to \mathbb{N}$ *una aplicación satisfaciendo las siguientes condiciones:*

(T.1) $\mathrm{I}(g_1,g_2) = \mathrm{I}(g_2,g_1)$ *para todo* $g_1,g_2 \in G$.
(T.2) $\mathrm{I}(g_1,g_2)+\mathrm{I}(g_1\oplus g_2,g_3) = \mathrm{I}(g_2,g_3)+\mathrm{I}(g_1,g_2\oplus g_3)$ *para todo* $g_1,g_2,g_3 \in G$.
(T.3) $\mathrm{I}(0,g) = 1$ *para todo* $g \in G$ *(donde* 0 *denota el elemento neutro de* G*).*
(T.4) *Para todo* $g \in G$*, existe* $k \in \mathbb{N}\setminus\{0\}$ *tal que* $\mathrm{I}(g,kg) > 0$.

Sobre el conjunto $\mathbb{N}\times G$ *definimos la siguiente operación*

$$(a_1,g_1)+_{\mathrm{I}}(a_2,g_2) = (a_1+a_2+\mathrm{I}(g_1,g_2),g_1\oplus g_2).$$

Entonces $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es un* $\mathcal{N}$*-semigrupo y todo* $\mathcal{N}$*-semigrupo es isomorfo a un semigrupo de esta forma.*

Sea $(H,+)$ un grupo abeliano y $h\in H$. Recordemos que un grupo H es periódico si para todo $h\in H$ existe $k\in\mathbb{N}\setminus\{0\}$ tal que $kh=0$. Es claro que todo grupo finito es periódico.

Aunque por los resultados del capítulo 3 no sabíamos cuándo un $\mathcal{N}$-semigrupo generalizado $\mathbb{N}\times G$ era finitamente generado, sí sabíamos cuándo el grupo que generaba $\mathbb{Z}\times G$ lo era (ver Proposición 3.8). Para los $\mathcal{N}$-semigrupos tenemos que la condición que se debe cumplir para ser finitamente generado es que el grupo G sea finito (véase **[18]**).

PROPOSICIÓN 6.13. *Consideremos las mismas hipótesis que en la Proposición 6.12. El semigrupo* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *es finitamente generado si y sólo si* G *es finito.*

Como consecuencia de lo expuesto en esta sección obtenemos el siguiente resultado.

TEOREMA 6.14. *El par* $(S,+)$ *es finitamente generado, débilmente reductivo y arquimediano si y sólo si* S *es un grupo finitamente generado o un* $\mathcal{N}$*-semigrupo. Además, bajo estas hipótesis se cumplen las siguientes condiciones:*

(1) S *es un grupo si y sólo si* S *tiene un elemento idempotente,*

(2) S *es un* $\mathcal{N}$*-semigrupo si y sólo si* S *es isomorfo a un semigrupo de la forma* $(\mathbb{N}\times G,+_{\mathrm{I}})$ *con* G *un grupo finito e* $\mathrm{I}:G\times G\to\mathbb{N}$ *satisfaciendo (T.1), (T.2) y (T.3).*

DEMOSTRACIÓN. Por el Teorema 6.10 sabemos que todo semigrupo finitamente generado, débilmente reductivo y arquimediano es cancelativo. Por tanto, dependiendo de la existencia de elementos idempotentes tendremos un grupo o un $\mathcal{N}$-semigrupo (esto también prueba la Condición (1)).

El recíproco es trivial.

Veamos si se cumple la Condición (2). Claramente, al ser S un $\mathcal{N}$-semigrupo finitamente generado, existe un grupo finito y una aplicación $\mathrm{I}:G\times G\to\mathbb{N}$ verificando (T.1), (T.2), (T.3) y (T.4). Además de (T.4) podemos prescindir puesto que es consecuencia directa del ser G finito. □

CAPÍTULO 7

Ideales de monoides conmutativos finitamente generados

Todo monoide finitamente generado tiene una presentación finita en el sentido de que puede determinarse completamente a partir de un conjunto finito de objetos (en este caso pares de tuplas de números enteros no negativos). Sin embargo, como ya sabemos hay subsemigrupos de semigrupos finitamente generados que no son finitamente generados. Uno de los más claros ejemplos de subsemigrupos que no han de ser necesariamente finitamente generados lo constituyen los ideales, los cuales van a ser de nuevo objeto de estudio en este capítulo. Nuestro objetivo no es sólamente extender la idea de presentación finita a los ideales, sino también presentar una serie de métodos para la descripción y estudio de un ideal en función de cualquier presentación suya.

Los contenidos de este capítulo generalizan los resultados presentados en [**63**].

1. Presentaciones de ideales de monoides finitamente generados

Para toda congruencia κ de $\mathbb{N}^p$ y todo subsemigrupo A de $\mathbb{N}^p$, la restricción de κ a A es igual a $\kappa_A = \kappa \cap (A \times A)$, la cual es una congruencia sobre A. El siguiente resultado prueba que $\kappa_I = \langle \kappa_I \rangle_I$ para todo ideal I de $\mathbb{N}^p$ ($\langle \rho \rangle$ denota como hasta ahora la congruencia generada por ρ en $\mathbb{N}^p$).

LEMA 7.1. *Sea I un ideal de $\mathbb{N}^p$, κ una congruencia en $\mathbb{N}^p$ y σ la congruencia de $\mathbb{N}^p$ generada por κ_I. Entonces $\kappa_I = \sigma_I$.*

DEMOSTRACIÓN. Para todo $(x,y) \in I \times I$, si $(x,y) \in \kappa_I$, entonces $(x,y) \in \sigma$, lo que implica que $(x,y) \in \sigma_I$. En consecuencia $\kappa_I \subseteq \sigma_I$. Usando ahora el que σ es la congruencia generada por κ_I y como κ es una congruencia que contiene a κ_I, deducimos que $\sigma \subseteq \kappa$, lo cual hace que $\sigma_I = \sigma \cap (I \times I) \subseteq \kappa \cap (I \times I) = \kappa_I$. □

Nuestro objetivo en esta sección es probar que un semigrupo isomorfo a un ideal de un monoide finitamente generado está completamente determinado, salvo isomorfismos, por un par (I, ρ), con I un ideal de $\mathbb{N}^p$ para algún entero p no negativo y ρ un subconjunto finito de $I \times I$.

LEMA 7.2. *Sea I un ideal de $\mathbb{N}^p$ y κ una congruencia en $\mathbb{N}^p$ generada por $\rho \subseteq I \times I$. Sean $x, y \in \mathbb{N}^p$. Entonces $x \kappa y$ si y sólo si se cumple una de las siguientes condiciones:*

(i) $\{x,y\} \not\subseteq I$ *y* $x = y$,
(ii) $\{x,y\} \subseteq I$ *y* $x \kappa_I y$.

DEMOSTRACIÓN. La demostración se obtiene fácilmente usando que $\rho \subseteq I \times I$ y de la construcción de $\langle \rho \rangle$ dada en la Proposición 1.3. □

Una interesante consecuencia de este último lema es el siguiente resultado.

COROLARIO 7.3. *Sea I un ideal de $\mathbb{N}^p$ y κ la congruencia en $\mathbb{N}^p$ generada por $\rho \subseteq I \times I$. Para todo $x \in \mathbb{N}^p$ tenemos lo siguiente:*

(i) si $x \notin I$, entonces $[x]_\kappa = \{x\}$,
(ii) si $x \in I$, entonces $[x]_\kappa = [x]_{\kappa_I}$.

Con este resultado podemos probar que I/κ_I es un ideal de $\mathbb{N}^p/\kappa$.

TEOREMA 7.4. *Sea I un ideal de $\mathbb{N}^p$, κ la congruencia sobre $\mathbb{N}^p$ generada por $\rho \subseteq I \times I$ y $\kappa_I = \kappa \cap I \times I$. Entonces el semigrupo I/κ_I es un ideal de $\mathbb{N}^p/\kappa$.*

DEMOSTRACIÓN. Por el Corolario 7.3, tenemos que $I/\kappa_I \subseteq \mathbb{N}^p/\kappa$. Tomemos ahora $x \in I$ e $y \in \mathbb{N}^p$, entonces $x+y \in I$. Tenemos así que $[x+y]_\kappa = [x+y]_{\kappa_I}$, lo cual implica que $[x]_{\kappa_I} + [y]_\kappa = [x+y]_{\kappa_I} \in I/\kappa_I$. □

El par (I, ρ) determina completamente al ideal I/κ_I del monoide $\mathbb{N}^p/\kappa$. A continuación veremos que todo ideal de un monoide finitamente generado es isomorfo a un ideal de la forma I/κ_I, con κ una congruencia sobre $\mathbb{N}^p$ generada por un subconjunto finito ρ de $I \times I$.

Sea S un monoide generado por $\{s_1, \ldots, s_p\}$ y $H = \{h_1, \ldots, h_r\} + S$ un ideal de S. Definimos

$$\varphi : \mathbb{N}^p \to S,$$
$$\varphi(x_1, \ldots, x_p) = \textstyle\sum_{i=1}^{p} x_i s_i.$$

Tenemos que si κ es la congruencia núcleo de φ, entonces $\mathbb{N}^p/\kappa$ es isomorfo a S. Ya que $\{h_1, \ldots, h_r\} \subseteq S$ y φ es sobreyectiva, existen $m_1, \ldots, m_r$ tales que $\varphi(m_i) = h_i$ para todo $i \in \{1, \ldots, r\}$. Consideremos $I = \{m_1, \ldots, m_r\} + \mathbb{N}^p$ y σ la congruencia de $\mathbb{N}^p$ generada κ_I. Sabemos que σ es finitamente generada (véase [**56**]). Es más, como σ es la congruencia generada por κ_I y la clase de todo elemento $x \notin I$ es igual a $\{x\}$ (ver Corolario 7.3), tenemos que σ está generada por un subconjunto finito ρ de $I \times I$. De esta forma, asociado a H, existe un par (I, ρ). Definimos

$$\psi : I/\sigma_I \to H,$$
$$\psi([x]_{\sigma_I}) = \varphi(x).$$

A partir de las siguientes dos observaciones puede deducirse que esta aplicación está bien definida.

- Para todo $x \in I$, existe $a \in \mathbb{N}^p$ y $m_i \in \{m_1, \ldots, m_r\}$ tal que $x = m_i + a$. Por tanto $\varphi(x) = \varphi(m_i + a) = h_i + \varphi(a) \in H$.
- Si $x \sigma_I y$, entonces por el Lema 7.1, tenemos que $x \kappa_I y$, de donde $x \kappa y$ y por tanto $\varphi(x) = \varphi(y)$.

Usando que la aplicación φ es un morfismo de grupos, deducimos que ψ también lo es. Veamos ahora que ψ es sobreyectiva. Tenemos que para todo $h \in H$, existe $b \in S$ y $h_i \in \{h_1, \ldots, h_r\}$ tal que $h = h_i + b$. Como φ es sobreyectiva, $b = \varphi(a)$ para todo $a \in \mathbb{N}^p$, de donde obtenemos que

$$\psi([a + m_i]_{\sigma_I}) = \varphi(a + m_i) = b + h_i = h.$$

Finalmente, si $\psi([x]_{\sigma_I}) = \psi([y]_{\sigma_I})$, entonces $\varphi(x) = \varphi(y)$, lo cual implica que $x\kappa_I y$ y por el Lema 7.1 nos queda que $[x]_{\sigma_I} = [y]_{\sigma_I}$.

Hemos probado por tanto que ψ es un isomorfismo de semigrupos. En consecuencia podemos enuciar el siguiente resultado.

TEOREMA 7.5. *Todo semigrupo isomorfo a un ideal de un monoide finitamente generado está determinado, salvo isomorfismos, por un par* (I,ρ), *con* I *un ideal de* $\mathbb{N}^p$ *y* ρ *un subconjunto finito de* $I \times I$.

Como sabemos, los ideales de monoides finitamente generados no han de ser necesariamente finitamente generados, por ello no pueden ser presentados de forma finita en el sentido de Rédei. Los resultados de esta sección nos dicen que todo ideal de un monoide finitamente generado queda determinado, salvo isomorfismos, por un par de la forma (I,ρ), donde I es un ideal de $\mathbb{N}^p$ y ρ un subconjunto finito de $\mathbb{N}^p \times \mathbb{N}^p$. Además todo ideal de $\mathbb{N}^p$ es finitamente generado como ideal por lo que puede determinarse a partir de un subconjunto finito de $\mathbb{N}^p$. Al ser ρ finito e I reconstruirse a partir de un número finito de datos, los pares de la forma (I,ρ) pueden ser considerados presentaciones finitas para los semigrupos que sean isomorfos a algún ideal de un monoide finitamente generado.

Nuestro siguiente objetivo es mostrar cómo dado un ideal H de un monoide finitamente generado $\mathbb{N}^p/\kappa$ podemos obtener una presentación de este tipo para este ideal y dar a partir de ella métodos para decidir si H verifica propiedades tales como ser cancelativo, libre de torsión, ser monoide, ser grupo, etc.

2. Cálculo de la presentación de un ideal

Dado un ideal I de $\mathbb{N}^p$ y una congruencia κ de $\mathbb{N}^p$, veremos cómo construir un sistema de generadores finito ρ de la congruencia σ de $\mathbb{N}^p$ generada por κ_I. Recordemos que el par (I,ρ) es una presentación del ideal I/σ_I y de cualquier semigrupo isomorfo a él.

Para simplificar, dado un elemento $x = (x_1,\ldots,x_p) \in \mathbb{N}^p$ y $n \in \mathbb{N}$, denotaremos al elemento $(x_1,\ldots,x_p,n) \in \mathbb{N}^{p+1}$ por (x,n).

LEMA 7.6. *Sea* κ *la congruencia de* $\mathbb{N}^p$ *generada por* $\tau = \{(a_1,b_1),\ldots,(a_r,b_r)\}$ *e* $I = \{m_1,\ldots,m_s\} + \mathbb{N}^p$ *un ideal de* $\mathbb{N}^p$. *Definimos*

$$\begin{aligned}\theta \;=\; & \{((a_1,1),(b_1,1)),\ldots,((a_r,1),(b_r,1)),\\ & ((m_1,0),(m_1,1)),\ldots,((m_s,0),(m_s,1))\},\end{aligned}$$

y sea γ *la congruencia generada por* θ *en* $\mathbb{N}^{p+1}$. *Entonces para todo* $x,y \in \mathbb{N}^p$ *verificando que* $(x,1)\gamma(y,1)$ *se tiene que* $x\kappa y$.

DEMOSTRACIÓN. Supongamos que $(x,1)\gamma(y,1)$. La Proposición 1.3 nos dice que existen $(z_1,n_1),\ldots,(z_t,n_t) \in \mathbb{N}^{p+1}$ tales que $(z_1,n_1) = (x,1),\ldots,(z_t,n_t) = (y,1)$ y $((z_i,n_i),(z_{i+1},n_{i+1})) \in \gamma_1$ para todo $i \in \{1,\ldots,t-1\}$. De la propia definición de γ_1 obtenemos que para todo $i \in \{1,\ldots,t-1\}$ se cumple una de las siguientes condiciones:

(1) $(z_i,n_i) = (z_{i+1},n_{i+1})$,

(2) existe $((a_j,1),(b_j,1)) \in \theta$ y $(c,n) \in \mathbb{N}^{p+1}$ tal que $((z_i,n_i,(z_{i+1},n_{i+1})) = ((a_j,1)+(c,n),(b_j,1)+(c,n))$, ó $((z_i,n_i),(z_{i+1},n_{i+1})) = ((b_j,1)+(c,n),(a_j,1)+(c,n))$,
(3) existe $((m_i,1),(m_i,0)) \in \theta$ y $(c,n) \in \mathbb{N}^{p+1}$ tal que $((z_i,n_i),(z_{i+1},n_{i+1})) = ((m_i,1)+(c,n),(m_i,0)+(c,n))$, o $((z_i,n_i),(z_{i+1},n_{i+1})) = ((m_i,0),(c,n),(m_i,1)+(c,n))$.

Usando ahora la Proposición 1.3, para concluir la demostración sólo hemos de probar que $(z_i,z_{i+1}) \in \tau_1$. Para la condición (1) es claro que $(z_i,z_{i+1}) \in \tau_1$. Si estamos en (2), entonces o se cumple que $z_i = a_j + c$ y $z_{i+1} = b_j + c$ o se cumple que $z_i = b_j + c$ y $z_{i+1} = a_j + c$ para algún $j \in \{1,\ldots,r\}$. Por último en (3) tenemos que $z_i = m_k + c = z_{i+1}$ para algún $k \in \{1,\ldots,s\}$. En cualquier caso tenemos que $(z_i,z_{i+1}) \in \tau_1$. □

TEOREMA 7.7. *Sea* κ *una congruencia sobre* $\mathbb{N}^p$ *generada por* $\tau = \{(a_1,b_1),\ldots,(a_r,b_r)\}$ *e* $I = \{m_1,\ldots,m_s\} + \mathbb{N}^p$ *un ideal de* $\mathbb{N}^p$. *Definimos*

$$\begin{aligned}\theta \;=\; & \{((a_1,1),(b_1,1)),\ldots,((a_r,1),(b_r,1)),\\ & ((m_1,0),(m_1,1)),\ldots,((m_s,0),(m_s,1))\},\end{aligned}$$

y sea γ *la congruencia generada por* θ. *Entonces la congruencia* σ *definida por* $x\sigma y$ *si y sólo si* $(x,0)\gamma(y,0)$ *es la congruencia generada por* κ_I.

DEMOSTRACIÓN. Sean $x,y \in \mathbb{N}^p$ tales que $(x,y) \in \sigma$. Entonces $((x,0),(y,0)) \in \gamma$. Distinguimos dos casos:

- Supongamos en primer lugar que $\{x,y\} \not\subseteq I$. Sin perdida de generalidad podemos suponer que $x \notin I$ y que $y \neq x$. Por la Proposición 1.3, tenemos que existen $(z_1,n_1),\ldots,(z_t,n_t) \in \mathbb{N}^{p+1}$ tales que $(z_1,n_1) = (x,0)$, $(z_t,n_t) = (y,0)$ y $((z_i,n_i),(z_{i+1}),(z_{i+1},n_{i+1})) \in \gamma_1$ para todo $i \in \{1,\ldots,t-1\}$ (además podemos suponer que $(z_i,n_i) \neq (z_{i+1},n_{i+1})$ ya que $x \neq y$). Así tenemos que $n_1 = 0$ de donde, utilizando la definición de θ y γ_1, obtenemos que $x = z_1 = m_j + c$ para algún $j \in \{1,\ldots,s\}$ y $c \in \mathbb{N}^p$, lo cual contradice que $x \notin I$. Por tanto $x = y$, de donde (x,y) pertenece a la congruencia generada por κ_I.
- Supongamos ahora que $\{x,y\} \subseteq I$. Ya que $(x,0)\gamma(y,0)$ y γ es una congruencia, tenemos que $(x,1)\gamma(y,1)$, lo cual por el Lema 7.6 implica que $x\kappa y$ y por tanto $(x,y) \in \kappa \cap (I \times I) = \kappa_I$.

Tomemos ahora (x,y) perteneciente a la congruencia generada por κ_I. Por el Corolario 7.3, si $\{x,y\} \not\subseteq I$, entonces $x = y$, lo cual implica que $(x,y) \in \sigma$. Si $\{x,y\} \subseteq I$, entonces $x\kappa y$. Por la Proposición 1.3 tenemos que existen $z_1,\ldots,z_t \in \mathbb{N}^p$ tales que $z_1 = x, z_t = y$ y $(z_i,z_{i+1}) \in \kappa_I$ para todo $i\{1,\ldots,t-1\}$. Veamos que $((z_i,1),(z_{i+1})) \in \gamma_1$ y tendremos por tanto que $(x,1)\gamma(y,1)$.

(1) Si $z_i = z_{i+1}$, entonces $((z_i,1),(z_{i+1},1)) \in \gamma_1$.
(2) Si $(z_i,z_{i+1}) = (a+c,b+c)$, con $(a,b) \in \tau$ o $(b,a) \in \tau$, y $c \in \mathbb{N}^p$, entonces $((a,1),(b,1))$ o $((b,1),(a,1))$ está en θ, lo cual implica que

$$((z_i,1),(z_{i+1},1)) = ((a,1)+(c,0),(b,1)+(c,0)) \in \gamma_1.$$

Como $x, y \in I$, existen $a, b \in \mathbb{N}^p$ e $i, j \in \{1, \ldots, s\}$ tales que $x = m_i + a$ e $y = m_j + b$. Claramente se tiene que $((m_i + a, 1), (m_i + a, 0)) \in \gamma$ y $((m_j + b, 1), (m_j + b, 0)) \in \gamma$ ya que $((m_i, 1), (m_i, 0)), ((m_j, 1), (m_j, 0))$ están en θ. Hemos visto entonces que $(x, 1)\gamma(y, 1)$, $(x, 1)\gamma(x, 0)$ y $(y, 1)\gamma(y, 0)$, de donde por transitividad se obtiene que $(x, 0)\gamma(y, 0)$ y por tanto $x\sigma y$. □

Así, una vez conocida τ un sistema de generadores de κ y $\{m_1, \ldots, m_s\}$ un sistema de generadores de $I \subseteq \mathbb{N}^p$, para calcular una presentación de $I/\kappa_I = I/\sigma_I$ hacemos lo siguiente.

(1) Construimos θ como en el Teorema 7.7.
(2) Usamos eliminación en la última variable de la congruencia generada por θ y consideramos ρ el resultado es esta eliminación.
(3) El par (I, ρ) es una presentación para todo ideal isomorfo a I/κ_I.

Recuérdese que por el Lema 7.1, $\sigma_I = \kappa_I$ y por el Teorema 7.4, $I/\kappa_I (= I/\sigma_I)$ es un ideal de $\mathbb{N}^p/\sigma$. Ésta es la razón por la que en adelante usaremos σ en lugar de la congruencia original κ; obsérvese que σ está generada por elementos de $I \times I$. De esta forma estamos cambiando el semigrupo que contiene el ideal: vamos desde $\mathbb{N}^p/\kappa$ hasta $\mathbb{N}^p/\sigma$; el ideal original H de $\mathbb{N}^p/\kappa$ es isomorfo a I/κ_I, el cual coincide con I/σ_I, un ideal de $\mathbb{N}^p/\sigma$. Veremos que las propiedades de H estudiadas en las siguientes secciones dependerán sólamente de σ (por supuesto, σ se obtiene de κ).

3. Componentes arquimedianas de un ideal

En esta sección daremos un método para calcular las componentes arquimedianas de un ideal de un monoide finitamente presentado por un par (I, ρ), esto es, un semigrupo isomorfo a I/σ_I, con I un ideal de $\mathbb{N}^p$ y σ una congruencia de $\mathbb{N}^p$ generada por $\rho \subseteq I \times I$. El procedimiento que presentaremos aquí está basado en el método dado en **[65]**.

Lo primero que vamos a probar es que las componentes arquimedianas de un ideal H de un semigrupo S no son más que la intersección de las componentes de S con H.

LEMA 7.8. *Sea S un semigrupo y H uno de sus ideales. Entonces toda componente arquimediana de H es la intersección de una componente arquimediana de S con H.*

DEMOSTRACIÓN. Sea $C_H$una componente arquimediana de H. Entonces existe una componente C_S de S tal que $C_H \subseteq C_S$. Probemos ahora que $C_S \cap H = C_H$. Sólo queda probar que $C_S \cap H \subseteq C_H$. Tomemos $a \in C_H$ y $b \in C_S \cap H$ y veamos que $a \mathcal{N}_H b$. Ya que ambos a y b están en C_S, entonces $a \mathcal{N} b$, lo cual significa que existen $k, l \in \mathbb{N} \setminus \{0\}$ y $c, d \in S$ tales que $ka = b + c$ y $lb = a + d$. Por tanto $(k+1)a = b + (c + a)$ y $(l+1)b = a + (d + b)$. Usando ahora el que $c + a, b + d \in H$, obtenemos que $a \mathcal{N}_H b$. □

LEMA 7.9. *Sea S un semigrupo y H uno de sus ideales. Si C es una componente arquimediana de S tal que $C \cap H$ es no vacío, entonces $C \cap H$ es una componente arquimediana de H.*

DEMOSTRACIÓN. Tomemos $a,b \in C \cap H$. Entonces $a\mathcal{N}b$, lo cual implica que existe $k \in \mathbb{N}\setminus\{0\}$ y $c \in S$ tal que $ka = b+c$ y por tanto $(k+1)a = b+(c+a)$. En consecuencia $C \cap H$ es un subsemigrupo arquimediano de H y por tanto existe una componente arquimediana C_H de H tal que $C \cap H \subseteq C_H$. Sea C_S una componetne arquimediana de S que contiene C_H. Entonces $C \cap C_S$ es no vacío, de lo cual obtenemos que $C = C_S$, ya que las componentes arquimedianas son clases de equivalencia, y por tanto $C_H = C_S \cap H$. □

Recordemos que el soporte de un elemento $x = (x_1,\ldots,x_p) \in \mathbb{N}^p$ estaba definido como

$$\mathrm{Supp}(x) = \{i \in \{1,\ldots,p\} \mid x_i \neq 0\}.$$

Como ya comentamos en el Capítulo 1, en [**65**] se da un algoritmo para calcular el conjunto de componentes arquimedianas de $\mathbb{N}^p/\sigma$ a partir de un sistema de generadores ρ de σ. Además, dijimos que si C es una componente arquimediana de $\mathbb{N}^p/\sigma$, entonces existen $A_1^C,\ldots,A_l^C,A^C \subseteq \{1,\ldots,p\}$ (conjuntos computables a partir de ρ, ver Proposición 1.6) tales que

(A) $\bigcup_{i=1}^{l} A_i^C \subseteq A^C$,
(B) $[x]_\sigma \in C$ si y sólo si $\mathrm{Supp}(x) \subseteq A^C$ y $A_i^C \subseteq \mathrm{Supp}(x)$ para algún $i \in \{1,\ldots,l\}$.

A continuación vemos como toda esta información puede ser usada para calcular el conjunto de componentes arquimedianas de I/σ_I.

LEMA 7.10. *Sea $I = \{m_1,\ldots,m_r\} + \mathbb{N}^p$ un ideal de $\mathbb{N}^p$, σ la congruencia generada por un subconjunto finito de $I \times I$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$. Entonces $C \cap I/\sigma_I$ es no vacío si y sólo si $\mathrm{Supp}(m_i) \subseteq A^C$ para algún $i \in \{1,\ldots,r\}$.*

DEMOSTRACIÓN. Tomemos $x \in I$ tal que $[x]_\sigma \in C$. Entonces existen $y \in \mathbb{N}^p$ e $i \in \{1,\ldots,r\}$ tales que $x = m_i + y$. Por la condición (B), $\mathrm{Supp}(x) \subseteq A^C$, de donde deducimos que $\mathrm{Supp}(m_i) \subseteq A^C$.

Recíprocamente, supongamos que $\mathrm{Supp}(m_i) \subseteq A^C$. Sea $x = \sum_{i \in A_1^C} e_i$. Entonces $A_1^C \subseteq \mathrm{Supp}(m_i + x) \subseteq A^C$, lo cual por la condición (B), implica que $[x+m_i]_\sigma \in C$. Ya que $x + m_i \in I$, obtenemos que $[x+m_i]_{\sigma_I} \in C \cap I/\sigma_I$. □

Usando estos lemas y a partir de [**65**, §13], las componentes arquimedianas de I/σ_I pueden ser calculadas y por tanto conocer si este semigrupo es o no arquimediano. La siguiente descripción de las componentes arquimedianas de I/σ_I será usada en las siguientes secciones.

PROPOSICIÓN 7.11. *Sea I un ideal de $\mathbb{N}^p$, σ una congruencia de $\mathbb{N}^p$ generada por un subconjunto finito de $I \times I$ y C una componente arquimediana de $\mathbb{N}^p/\sigma$ tal que $C \cap I/\sigma_I$ es no vacío. Definimos como en el Capítulo 5*

$$\mathbb{N}^C = \{x \in \mathbb{N}^p \mid \mathrm{Supp}(x) \subseteq A^C\}$$

y a partir de él, el conjunto

$$I^C = \{x \in \mathbb{N}^C \cap I \mid A_i^C \subseteq \mathrm{Supp}(x) \text{ para algún } i \in \{1,\ldots,l\}\}.$$

Entonces

$$C \cap \frac{I}{\sigma_I} = \frac{I^C}{(\sigma_{\mathbb{N}^C})_{I^C}}.$$

DEMOSTRACIÓN. La demostración es inmediata a partir de las condiciones (A) y (B), el Lema 7.10 y la definición de I^C. □

Usando estos resultados y el procedimiento de [**65**, §13], el cual da un método para el calculo de las componentes arquimedianas de un monoide finitamente generado, podemos calcular las componentes arquimedianas de I/σ_I y en particular podemos decidir si I/σ_I es arquimediano a partir de un sistema de generadores de I y ρ. Los pasos a seguir son los siguientes.

(1) A partir de ρ y usando el procedimiento de [**65**, §13], calcular el conjunto de componentes arquimedianas de $\mathbb{N}^p/\langle\rho\rangle = \mathbb{N}^p/\sigma$.
(2) Para toda componente arquimediana C de $\mathbb{N}^p/\sigma$ usar el Lema 7.10 para decidir si $C \cap \mathrm{I}/\sigma_I$ es no vacío.
(3) Caso de que este conjunto sea no vacío calcular el conjunto $\mathbb{N}^C$ (el cual es isomorfo a $\mathbb{N}^k$ si $A^C = \{i_1, \ldots, i_k\}$) y el conjunto I^C (el cual es isomorfo a un ideal de $\mathbb{N}^C$. Usando eliminación, calcular un sistema de generadores de $\sigma_{\mathbb{N}^C}$.
(4) La Proposición 7.11 nos da una descripción de $C \cap I/\sigma_I$. Todas las componentes arquimedianas de I/σ_I son de esta forma.

4. Cálculo del conjunto de idempotentes de un ideal de un monoide finitamente generado

Nuestro objetivo en esta sección es dar un método para el cálculo del conjunto de idempotentes de un ideal de un monoide finitamente generado a partir de una de sus presentaciones (I, ρ), lo cual es igual al problema de encontrar el conjunto de idempotentes de un semigrupo de la forma I/σ_I, con I un ideal de $\mathbb{N}^p$ y σ una congruencia generada por un conjunto finito $\rho \subseteq I \times I$.

Recordemos que como se vió en el Capítulo 1, todo semigrupo arquimediano tiene a lo sumo un elemento idempotente. Además, también vimos que las componentes arquimedianas de I/σ_I son semigrupos arquimedianos. Por tanto, resolver el problema de decidir si una componente arquimediana de I/σ_I tiene o no un idempotente y si lo tiene calcularlo, nos da respuesta al problema del cálculo de los idempotentes de I/σ_I. Por la Proposición 7.11, toda componente arquimediana de I/σ_I es de la forma $J/(\sigma_{\mathbb{N}^k})_J$, con k un entero no negativo y J un ideal de $\mathbb{N}^k$. Como anteriormente hemos visto en la sección 2, sabemos cómo calcular un sistema de generadores de $\sigma_{\mathbb{N}^k}$ y J. De ahí que centraremos nuestra atención en determinar cuándo un semigrupo arquimediano de la forma J/κ_J tiene un idempotente y caso de tenerlo cómo calcularlo.

Sea $x = (x_1, \ldots, x_p) \in \mathbb{Z}^p$. Como en el Capítulo 5, decimos que x es positivo si $x \in \mathbb{N}^p$ y $\mathrm{Supp}(x) = \{1, \ldots, p\}$.

PROPOSICIÓN 7.12. *Sea J un ideal de $\mathbb{N}^p$, κ una congruencia en $\mathbb{N}^p$ generada por un subconjunto finito de $J \times J$ tal que J/κ_J es arquimediano. Entonces J/κ_J tiene un idempotente si y sólo si M_κ tiene un elemento positivo.*

DEMOSTRACIÓN. En primer lugar supongamos que $[x]_\kappa$ es un idempotente de J/κ_J. Tomemos $a \in J$ y sea $m = e_1 + \ldots + e_p$. Entonces $a+m \in J$, de donde tenemos que existe $k \in \mathbb{N}\setminus\{0\}$ y $c \in \mathbb{N}^p$ tal que $k[x]_\kappa = [x]_\kappa = [a+c+m]_\kappa$. Por tanto $[a+c+m]_\kappa$ es un elemento idempotente de $\mathbb{N}^p$, lo cual implica que $2(a+c+m)\kappa(a+c+m)$ y en consecuencia $a+c+m$ es un elemento positivo de M_κ.

Recíprocamente, tomemos x un elemento positivo de M_κ. Entonces $(x,0) \in {\sim_{M_\kappa}}$, lo cual por la Proposición 1.4 hace que $(x+c,c) \in \kappa$ para algún $c \in \mathbb{N}^p$. Ya que $\mathrm{Supp}(x) = \{1,\ldots,p\}$, existe $k \in \mathbb{N}$ y $d \in \mathbb{N}^p$ tal que $kx = c+d \in J$ y así

$$[(k+1)x]_\kappa = [x+c+d]_\kappa = [c+d]_\kappa = [kx]_\kappa.$$

Por inducción sobre n, se deduce fácilmente que $[(k+n)x]_\kappa = [kx]_\kappa$ para todo $n \in \mathbb{N}$, lo que en particular implica que $[2(kx)]_{\kappa_J} = [kx]_{\kappa_J}$. □

Con toda esta información ya estamos en condiciones de calcular el conjunto de idempotentes de un ideal I/σ_I una vez conocida una de sus presentaciones (I,ρ).

(1) Calcular el conjunto de componentes arquimedianas de I/σ_I.
(2) Para toda componente arquimediana J/κ_J de I/σ_I (J y κ se obtienen a partir de la Proposición 7.11), el algoritmo MCP de **[58]** nos permite saber si M_κ tiene un elemento positivo y caso de tenerlo calcularlo.
(3) Una vez conocido este elemento (caso de que exista alguno) encontrar $k \in \mathbb{N}\setminus\{0\}$ tal que kx pertenezca a J y $[(k+1)x]_\kappa = [kx]_\kappa$ (saber si se da la igualdad se puede hacer calculando las formas normales de estos dos elementos y viendo si coinciden). Ahora a partir de la demostración de la Proposición 7.12 se obtiene que $[kx]_\kappa$ es un idempotente de I/σ_I.

5. Ideales de monoides finitamente generados que son monoides

Usando los resultados de la sección anterior vamos a dar un método que nos permita decidir cuándo un ideal de un monoide finitamente generado tiene un elemento neutro (lo cual significa que es un monoide). Sabemos que todo ideal de un monoide finitamente generado es de la forma I/σ_I con I un ideal de $\mathbb{N}^p$ y $\sigma_I = \sigma \cap (I \times I)$ con σ una congruencia generada por $\rho \subseteq I \times I$. Por la sección anterior tenemos que el conjunto de idempotentes de I/σ_I puede ser calculado. Además caso de que I/σ_I tenga elemento neutro, éste es uno de sus idempotentes. El siguiente resultado nos va a permitir comprobar si I/σ_I es un monoide.

PROPOSICIÓN 7.13. *Sea $I = \{m_1,\ldots,m_r\} + \mathbb{N}^p$ un ideal de $\mathbb{N}^p$, σ una congruencia generada por un conjunto finito de $I \times I$. Entonces $[u]_{\sigma_I}$ es el elemento neutro de I/σ_I si y sólo si $[m_i+u]_{\sigma_I} = [m_i]_{\sigma_I}$ para todo $i \in \{1,\ldots,r\}$.*

DEMOSTRACIÓN. Si $[u]_{\sigma_I}$ es el elemento neutro de I/σ_I, entonces claramente $[m_i]_{\sigma_I} + [u]_{\sigma_I} = [m_i]_{\sigma_I}$.

Supongamos ahora que $[u]_{\sigma_I}$ verifica que $[m_i+u]_{\sigma_I} = [m_i]_{\sigma_I}$ para todo $i \in \{1,\dots,r\}$. Tomemos $x \in I$. Existe $a \in \mathbb{N}^p$ e $i \in \{1,\dots,r\}$ tales que $x = a + m_i$ y por tanto

$$[x]_{\sigma_I} + [u]_{\sigma_I} = [m_i + a]_{\sigma_I} + [u]_{\sigma_I} = [m_i + u]_{\sigma_I} + [a]_{\sigma_I} = [m_i + a]_{\sigma_I} = [x]_{\sigma_I}.$$

□

Una vez conocidos los idempotentes de I/σ_I e (I,ρ) una presentación suya con $I = \{m_1,\dots,m_r\} + \mathbb{N}^p$ y $\rho \subseteq I \times I$ hacemos lo siguiente:

(1) Calcular un sistema canónico de generadores η de σ.
(2) Para todo idempotente $[e] \in I/\sigma_I$, ver si $\mathrm{NF}_\eta(e) = \mathrm{NF}_\eta(e + m_i)$ para todo $i \in \{1,\dots,r\}$. Caso de que algún elemento e verifique esta condición, tendremos que $[e]_{\sigma_I}$ es el elemento neutro de I/σ_I.

EJEMPLO 7.14. Consideremos κ la congruencia sobre $\mathbb{N}^3$ generada por

$$\{((3,0,0),(0,2,0)),((0,2,4),(0,5,1)),((4,1,0),(2,7,0))\}.$$

Sean $S \cong \mathbb{N}^3/\kappa$ y J el ideal $\{[(2,0,0)]_\kappa\} + S$. Veamos a continuación si este ideal es o no un monoide. En primer lugar hemos de dar una presentación para este ideal. Para ello consideramos la congruencia de $\mathbb{N}^4$ generada por

$$\begin{aligned}\theta \;=\; & \{((3,0,0,1),(0,2,0,1)),((0,2,4,1),(0,5,1,1)),\\ & ((4,1,0,1),(2,7,0,1)),((2,0,0,0),(2,0,0,1))\}.\end{aligned}$$

Aplicamos eliminación en su última variable y obtenemos

$$\begin{aligned}\rho \;=\; & \{((2,2,46),(2,2,4)),((2,3,1),(2,2,16)),((2,17,0),(2,3,0)),\\ & ((3,0,4),(2,3,25)),((3,3,0),(2,13,0)),((4,1,0),(2,7,0)),\\ & ((5,0,0),(2,2,0))\}.\end{aligned}$$

Por tanto el par (I,ρ) con $I = \{(2,0,0)\} + \mathbb{N}^3$ es una presentación de J y $\sigma = \langle\rho\rangle$. Calculemos ahora las componentes arquimedianas de I. Para ello en primer lugar vemos cuales son las componentes arquimedianas de $\mathbb{N}^3/\sigma_I$. Estas son:

$$\begin{aligned}C_0 &= \{[(0,0,0)]_\sigma\},\\ C_1 &= \{[(x,y,0)]_\sigma \mid x \in \mathbb{N}\setminus\{0\},\ y \in \mathbb{N}\},\\ C_2 &= \{[(0,y,0)]_\sigma \mid y \in \mathbb{N}\setminus\{0\}\},\\ C_3 &= \{[(0,0,z)]_\sigma \mid z \in \mathbb{N}\setminus\{0\}\},\\ C_4 &= \{[(x,y,z)]_\sigma \mid x,z \in \mathbb{N}\setminus\{0\},\ y \in \mathbb{N}\},\\ C_5 &= \{[(0,y,z)]_\sigma \mid y,z \in \mathbb{N}\setminus\{0\}\}.\end{aligned}$$

Por el Lema 7.11, las componentes arquimedianas que cortan a J son C_1 y C_4. Aplicando el Lema 7.10 y la Proposición 7.11 tenemos que si

$$\begin{aligned}I^{C_1} &= \{(2,0)\} + \mathbb{N}^2,\\ I^{C_4} &= \{(2,0,1)\} + \mathbb{N}^3,\end{aligned}$$

$$\begin{aligned}\rho_1 &= \{((2,17),(2,3)),((3,3),(2,13)),\\ &\quad ((4,1),(2,7)),((5,0),(2,2))\},\\ \rho_4 &= \{((2,2,46),(2,2,4)),((2,3,1),(2,2,16)),\\ &\quad ((3,0,4),(2,4,10)),((4,1,1),(2,4,4)),\\ &\quad ((5,0,1),(2,2,1))\},\end{aligned}$$

entonces (I^{C_1},ρ_1) y (I^{C_4},ρ_4) son presentaciones de $C_1\cap J$ y $C_4\cap J$, respectivamente. Vemos a continuación para cada una de estas componentes arquimedianas si hay o no en ellas elementos idempotentes. Sea $\kappa_1=\langle\rho_1\rangle$ y $\kappa_4=\langle\rho_4\rangle$. Usando la proposición 7.12 (para ello usamos el algoritmo MCP de [**58**]), obtenemos que tanto en $J\cap C_1$ como en $J\cap C_4$ tienen idempotentes. Para la primera de estas componentes obtenemos el elemento $[(1,4)]_{\kappa_1}$ y para la segunda el $[(1,1,3)]_{\kappa_4}$. Además estos elementos verifican que

$$\begin{gathered}3(1,4)\kappa_1 2(1,4) \text{ y } 2(1,4)\in I^{C_1},\\ 3(1,1,3)\kappa_2 2(1,1,3) \text{ y } 2(1,1,3)\in I^{C_4}.\end{gathered}$$

Lo cual implica que $[(2,8,0)]_{\sigma_I}$ y $[(2,2,6)]_{\sigma_I}$ son todos los idempotentes de I/σ_I. Por último, ya que

$$\begin{gathered}(2,8,0)\not\sigma_I(2,8,0)+(2,0,0)\\ (2,2,6)\not\sigma_I(2,2,6)+(2,0,0),\end{gathered}$$

por la Proposición 7.13, ninguno de estos dos elementos verifica la condición de ser elemento neutro, de ahí que el ideal J no sea un monoide. □

6. Ideales de monoides finitamente generados que son grupos

Sea S un semigrupo. Si S es un grupo, entonces S tiene elemento neutro y además este elemento es arquimediano. El recíproco es también cierto. Además un semigrupo es arquimediano si y sólo si tiene una única componente arquimediana. Por tanto, como ya tenemos métodos para probar si un ideal de un monoide finitamente generado es arquimediano (Sección 3) y para probar si tiene elemento neutro (Sección 5), podemos saber para cualquier ideal de este tipo si es o no un grupo.

7. El grupo de unidades de un ideal de un monoide finitamente generado

Se puede probar que el grupo de unidades de un monoide es igual a la componente arquimediana que contiene el elemento neutro. Usando los resultados de la sección 5, podemos saber si uno de estos ideales es o no un monoide. Además durante el proceso hemos de calcular sus componentes arquimedianas. La componente que contenga a su elemento neutro, caso de que lo tenga, es igual al grupo de sus unidades. Caso de no haber elemento neutro no hay unidades.

8. Ideales cancelativos de un monoide finitamente generado

Recordemos que un semigrupo S es cancelativo si para todo $a,b,c\in S, a+c=b+c$ se tiene que $a=b$. Sabemos que todo monoide finitamente generado es isomorfo a uno de la forma $\mathbb{N}^p/\sigma$ con σ una congruencia en $\mathbb{N}^p$, y que este es cancelativo si y sólo

si $\sim_{M_\sigma} = \sigma$ (ver capítulo 1). Un resultado similar puede ser probado para ideales de monoides finitamente generados (véase [**65**, §14]).

PROPOSICIÓN 7.15. *Sea I un ideal de $\mathbb{N}^p$ y σ una congruencia sobre $\mathbb{N}^p$ generada por un subconjunto finito de $I \times I$. Entonces I/σ_I es cancelativo si y sólo si $(\sim_{M_\sigma})_I = \sigma_I$.*

A continuación presentamos el procedimiento para comprobar si I/σ_I es cancelativo (una vez conocido (I,ρ)).

- El conjunto ρ es un sistema de generadores de $\langle \sigma_I \rangle = \sigma$. Para calcular un sistema de generadores de $\langle (\sim_{M_\sigma}) \rangle$ debemos en primer lugar calcular un sistema de generadores de $\sim_{M_\sigma}$. Para ello se pueden usar los resultados que aparecen en [**72**, §8].
- Combinando lo anterior con los resultados de la sección 2, podemos determinar un sistema de generadores de $\langle (\sim_{M_\sigma})_I \rangle$.
- Una vez que tenemos un sistema de generadores de $\langle \sigma_I \rangle$ y $\langle (\sim_{M_\sigma})_I \rangle$, podemos determinar, calculando para cada una un sistema canónico de generadores con respecto al mismo orden, si esas dos congruencias coinciden (véase [**65**, §6]). Caso de coincidir el ideal I/σ_I es cancelativo, en otro caso no lo es.

9. Ideales separativos de monoides finitamente generados

Un semigrupo es **separativo** si para todo $x, y \in S$, las igualdades $2x = x + y = 2y$ implican que $x = y$. Con todos los resultados que ya conocemos estamos en condiciones de decidir cuándo un ideal de un monoide finitamente generado es separativo. Esto es debido a la siguiente caracterización de separatividad (véase [**33**]).

PROPOSICIÓN 7.16. *Un semigrupo es separativo si y sólo si sus componentes arquimedianas son cancelativas.*

Dada una presentación de ideal de un monoide finitamente generado, (I,ρ), podemos calcular, usando los resultados de la sección 3, todas sus componentes arquimedianas y calcular presentaciones de la forma (J,κ_J) con J un ideal de $\mathbb{N}^n$ con n natural positivo y κ_J una congruencia generada por elementos de $J \times J$. Usando ahora la sección anterior podemos decidir si todas estas componentes arquimedianas son o no cancelativas.

Veamos a continuación con un ejemplo una aplicación de lo expuesto.

EJEMPLO 7.17. Sea de nuevo κ la congruencia sobre $\mathbb{N}^3$ generada por el conjunto

$$\{((3,0,0),(0,2,0)),((0,2,4),(0,5,1)),((4,1,0),(2,7,0))\},$$

S el monoide $\mathbb{N}^3/\kappa$ y $J = \{[(3,6,5)]_\kappa\} + S$ un ideal suyo. Veamos si J es un semigrupo separativo. En primer lugar calculamos una presentación suya. Para ello consideramos la congruencia de $\mathbb{N}^4$ generada por

$$\begin{aligned}\theta \;=\; & \{((3,0,0,1),(0,2,0,1)),((0,2,4,1),(0,5,1,1)),\\ & ((4,1,0,1),(2,7,0,1)),((3,6,5,0),(3,6,5,1))\}.\end{aligned}$$

Aplicando eliminación en la última variable obtenemos

$$\rho = \{((3,6,26),(3,6,5)),((3,8,5),(3,6,8)),((4,6,5),(3,6,20))\}.$$

Tomemos $\sigma = \langle \rho \rangle$. Una presentación del ideal J es (I,ρ) con $I = \{(3,6,5)\} + \mathbb{N}^3$. Tras calcular las componentes arquimedianas de $\mathbb{N}^3/\sigma_I$ obtenemos que este monoide tiene ocho componentes arquimedianas de las cuales sólo una tiene intersección no vacía con I. Esta componente es

$$C = \{(x,y,z) \mid x,y,z \in \mathbb{N} \setminus \{0\}\}.$$

Lo cual significa que J es un semigrupo arquimediano y que $J \cap C = J$, y por tanto $(\sigma_I)_C$ es de nuevo σ_I. Por tanto, nuestro ideal será separativo si es cancelativo. Para ello calculamos $\sim_{M_{\sigma_I}}$. Usando el método dado en [**72**, §8], obtenemos que este conjunto está generado por

$$\tau = ((0,0,21),(0,0,0)),((0,2,0),(0,0,24)),((1,0,0),(0,8,3))\}.$$

Por último, sólo basta calcular un sistema de generadores de $\langle (\sim_{M_{\sigma_I}})_I \rangle$, tal y como se hizo en el ejemplo anterior, y usar el procedimiento dado en [**65**, §6] para ver que efectivamente coincide con ρ, obteniendo de esta forma que J es separativo. □

10. Ideales de monoides finitamente generados libres de torsión

Recordemos que un semigrupo S es libre de torsión si $kx = ky$ con $k \in \mathbb{N} \setminus \{0\}$ implica que $x = y$. El siguiente resultado nos da la clave para poder decidir si un ideal de un monoide finitamente generado es libre de torsión.

LEMA 7.18. *Un semigrupo es libre de torsión si y sólo si sus componentes arquimedianas son libre de torsión.*

DEMOSTRACIÓN. Sea S un semigrupo libre de torsión. Todo subsemigrupo suyo es libre de torsión, en particular sus componentes arquimedianas que son subsemigrupos suyos.

Recíprocamente, consideremos S un semigrupo tal que todas sus componentes arquimedianas suyas libres de torsión. Tomemos $x,y \in S$ y $k \in \mathbb{N} \setminus \{0\}$ tal que $kx = ky$. Entonces x,y,kx,ky están en la misma componente arquimediana C de S. Por hipótesis C es libre de torsión y por tanto $x = y$. □

En consecuencia debemos de estudiar cuándo las componentes arquimedianas de ideales finitamente generados son libres de torsión. Usando que todo semigrupo arquimediano tiene a lo sumo un idempotente (ver Capítulo 1), el siguiente resultado nos da la solución a este problema.

PROPOSICIÓN 7.19. *Sea J un ideal de $\mathbb{N}^p$ y κ una congruencia de $\mathbb{N}^p$ generada por un subconjunto finito de $J \times J$ tal que J/κ_J es arquimediano. Entonces J/κ_J es libre de torsión si y sólo si J/κ_J es cancelativo y $\mathbb{N}^p / \sim_{M_\kappa}$ es libre de torsión.*

DEMOSTRACIÓN. Supongamos que J/κ_J es libre de torsión, J/κ_J es separativo lo cual por la Proposición 7.16, implica que sus componentes arquimedianas son cancelativas, de donde J/κ_J es cancelativo y arquimediano.

Supongamos ahora que $kx \sim_{M_\kappa} ky$ para algún $k \in \mathbb{N} \setminus \{0\}$ con $x, y \in \mathbb{N}^p$. Por la Proposición 1.3, existe $c \in \mathbb{N}^p$ tal que $(kx+c, ky+c) \in \kappa$. Tomando c lo suficientemente grande para que $c \in J$ y así tener $(kx+kc, ky+kc) \in \kappa_J$. Como J/κ_J es libre de torsión, deducimos que $(x+c, y+c) \in \kappa$ lo cual implica que $x \sim_{M_\kappa} y$.

Recíprocamente, supongamos que $(kx, ky) \in \kappa_J$ para algún $k \in \mathbb{N} \setminus \{0\}$ y $x, y \in J$. Entonces $(kx, ky) \in \sim_{M_\kappa}$ y ya que $\mathbb{N}^p / \sim_{M_\kappa}$ es libre de torsión, obtenemos que $(x, y) \in \sim_{M_\kappa}$. En consecuencia $(x, y) \in \sim_{M_\kappa} \cap (J \times J) = (\sim_{M_\kappa})_J$. Por la Proposición 7.15, obtenemos que $(\sim_{M_\kappa})_J = \kappa_J$ y por tanto $(x, y) \in \kappa_J$. □

El monoide $\mathbb{N}^p / \sim_{M_\kappa}$ es libre de torsión si y sólo si $\mathbb{Z}^p / M_\kappa$ es libre de torsión (véase [**58**]). En consecuencia $\mathbb{N}^p / \sim_{M_\kappa}$ es libre de torsión si y sólo si los factores invariantes de M_κ son iguales a 1. Además los factores invariantes de M_κ pueden ser calculados a partir de un sistema de generadores de M_κ, los cuales pueden ser obtenidos a partir de un sistema de generadores de κ. Obsérvese que la Proposición 7.19, junto con la información obtenida hasta ahora, nos proporciona un método para decidir si un ideal de un monoide finitamente generado es libre de torsión.

EJEMPLO 7.20. Retomemos el ejemplo anterior en el que I/σ_I era arquimediano y veamos si este ideal es o no libre de torsión. Teníamos que I/σ_I era cancelativo. Veamos si $\mathbb{N}^p / \sim_{M_\sigma}$ es libre de torsión. La congruencia $\sim_{M_\sigma}$ está generada por

$$\{((0,0,21),(0,0,0)),((0,2,0),(0,0,24)),((1,0,0),(0,8,3))\}.$$

Por tanto un sistema de generadores de M_σ es

$$\{(0,0,21),(0,2,-24),(1,-8,-3)\}.$$

Calculando la forma normal de Smith de la matriz

$$\begin{pmatrix} 0 & 0 & 21 \\ 0 & 2 & -24 \\ 1 & -8 & -3 \end{pmatrix},$$

obtenemos la matriz

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 42 \end{pmatrix}.$$

Por tanto el semigrupo I/σ_I no es libre de torsión. □

CAPÍTULO 8

Ideales primos y radicales

Existe un gran parecido entre la teoría de ideales de semigrupos y la de ideales de anillos conmutativos. Muchas definiciones y teoremas relativos a semigrupos tienen su contraparte en Álgebra Conmutativa (véase por ejemplo [7]). Aquí vamos a usar este paralelismo para definir el concepto de topología de Zariski en el espectro primo de un semigrupo. Si S es un cero-monoide (un semigrupo con identidad y cero), entonces definimos el espectro primo de S, el cual denotamos por $\mathrm{Spec}(S)$, como el conjunto de todos los ideales primos propios de S. Dado un ideal I de S definimos

$$\mathcal{V}(I) = \{P \in \mathrm{Spec}(S) \mid I \subseteq P\}.$$

Estos conjuntos son los cerrados de la topología que introducimos en $\mathrm{Spec}(S)$. Bajo estas condiciones definimos el concepto de cero-monoides homeomorfos como aquellos cuyos espectros son homeomorfos como espacios topológicos. Es nuestro propósito describir este concepto topológico en términos semigrupistas.

1. El espectro primo de un cero-monoide

Tal y como se hace normalmente al aparecer cero-elementos, usaremos notación multiplicativa en este capítulo.

Consideremos un monoide $(S, \cdot)$. Un elemento x de un semigrupo $(S, \cdot)$ es una **identidad** si $xy = y$ para todo $y \in S$. Decimos que $x \in S$ es un **cero** si $xy = x$ para todo $y \in S$. Se puede comprobar fácilmente que en caso de que exista alguno de estos elementos, su unicidad se da automáticamente. Un **cero-monoide** no es más que un semigrupo con identidad y cero (la identidad no es más que el elemento neutro de S).

A lo largo de esta sección $(S, \cdot)$ denotará un cero-monoide, por 1 denotaremos su elemento identidad y por 0 el cero.

Con esta notación, un subconjunto no vacío I de S es un ideal si dados $a \in I$ y $x \in S$, tenemos que $ax \in I$. Denotaremos por $\mathrm{Id}(S)$ el conjunto de todos los ideales de S. Recordemos que un ideal I es primo si siempre que $xy \in I$, o bien x ó y están en I. Dado un elemento $a \in S$ en este capítulo aS denotará el ideal generado por a.

Los dos siguientes resultados son de sobra conocidos.

LEMA 8.1. *Sea $(S, \cdot)$ un cero-monoide.*

- *La unión de un conjunto de ideales de S es un ideal de S.*
- *La intersección de un conjunto de ideales de S es un ideal de S.*
- *La unión de un conjunto de ideales primos de S es un ideal primo de S.*

NOTA 8.2. Nótese que cualquier ideal de S contiene al cero y por tanto la intersección de cualquier conjunto de ideales es no vacía.

LEMA 8.3. *Sea $(S,\cdot)$ un cero-monoide e I_1, I_2, P ideales de S de forma que P es primo. Si $I_1 \cap I_2 \subseteq P$, entonces $I_1 \subseteq P$ ó $I_2 \subseteq P$.*

Definimos el **espectro primo** de S como

$$\mathrm{Spec}(S) = \{P \subseteq S \mid P \text{ es un ideal primo propio de } S\}.$$

Dado un ideal I de S, definimos

$$\mathcal{V}(I) = \{P \in \mathrm{Spec}(S) \mid I \subseteq P\}.$$

Un subconjunto C de $\mathrm{Spec}(S)$ es **cerrado** si $C = \mathcal{V}(I)$ para algún ideal I de S.

NOTA 8.4. Claramente $S \setminus \mathcal{U}(S)$ es el único ideal maximal propio de S, es más, este ideal es primo. Por tanto se tiene que $\mathcal{V}(I) = \emptyset$ si y sólo si $I = S$.

PROPOSICIÓN 8.5. *Sea $(S,\cdot)$ un cero-monoide.*

- *La unión finita de conjuntos cerrados es de nuevo cerrada.*
- *La intersección de un número arbitrario de cerrados es cerrado.*

DEMOSTRACIÓN. Es sencillo probarlo a partir de lo siguiente:

- $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2)$ (ver el Lema 8.3).
- $\cap_j \mathcal{V}(I_j) = \mathcal{V}(\cup_j I_j)$.

□

Así, obtenemos que los conjuntos $\mathcal{V}(I)$ son los cerrados de una topología en $\mathrm{Spec}(S)$, a la que llamamos **topología de Zariski**. El conjunto de los cerrados de $\mathrm{Spec}(S)$ lo denotaremos por $\mathrm{CS}(S)$.

Dado un ideal I de S, definimos el **radical** de I como

$$\mathrm{Rad}(I) = \{x \in S \mid x^k \in I \text{ para algún entero } k\}.$$

Es fácil comprobar que $\mathrm{Rad}(I)$ es también un ideal de S. Como ya definimos en el Capítulo 1, un ideal I es radical si $\mathrm{Rad}(I) = I$. De esta forma todo ideal primo es radical. Al conjunto de ideales radicales de S lo denotamos por $\mathrm{RI}(S)$.

El siguiente resultado se puede encontrar en [**75**].

PROPOSICIÓN 8.6. *Sea S un cero-monoide e I un ideal de S. Entonces $\mathrm{Rad}(I)$ es la intersección de todos los ideales primos de S que contienen a I.*

Si X es un subconjunto no vacío de $\mathrm{Spec}(S)$, definimos $\mathfrak{I}(X)$ como la intersección de todos los ideales que están en X. Dados $X_1, X_2 \subseteq \mathrm{Spec}(S)$, claramente $\mathfrak{I}(X_1 \cap X_2) = \mathfrak{I}(X_1) \cup \mathfrak{I}(X_2)$.

NOTA 8.7. De la Proposición 8.6 se deduce que si I es un ideal propio de S, entonces $\mathfrak{I}(\mathcal{V}(I)) = \mathrm{Rad}(I)$. Si convenimos que $\mathfrak{I}(\emptyset) = S$, entonces llegamos a que $\mathfrak{I}(\mathcal{V}(S)) = S = \mathrm{Rad}(S)$.

Como consecuencia de esto obtenemos el siguiente resultado.

TEOREMA 8.8. *Sea S un cero-monoide. Existe una correspondencia biyectiva entre el conjunto* $\mathrm{CS}(S)$ *de cerrados de* $\mathrm{Spec}(S)$ *y el conjunto* $\mathrm{RI}(S)$ *de ideales radicales de S. Es más, la aplicación*

$$\mathcal{V} : \mathrm{RI}(S) \to \mathrm{CS}(S)$$

es inversa de

$$\mathcal{I} : \mathrm{CS}(S) \to \mathrm{RI}(S),$$

y ambas invierten las inclusiones.

Un espacio topológico T es **irreducible** si no puede ser expresado como unión de dos subconjuntos propios que sean cerrados. Un subconjunto de un espacio topológico es irreducible si lo es con la topología inducida. Los subconjuntos irreducibles maximales de T se conocen como **componentes irreducibles** de T.

El siguiente resultado aparece en [**48**].

LEMA 8.9. *Sea T un espacio topológico.*

- *Las componentes irreducibles de T son cerradas.*
- *Cualquier subconjunto irreducible de T está contenido en una componente irreducible.*
- *Cualquier espacio topológico es la unión de sus componentes irreducibles.*

Es inmediato comprobar que si X es un subconjunto no vacío de $\mathrm{Spec}(S)$, entonces $\mathcal{V}(\mathcal{I}(X))$ es la clausura de X (a saber, el menor cerrado de $\mathrm{Spec}(S)$ que contiene X), y la denotamos por $\overline{X}$.

TEOREMA 8.10. *Sea S un cero-monoide. Un subconjunto X de* $\mathrm{Spec}(S)$ *es irreducible si y sólo si $\mathcal{I}(X)$ es un ideal primo.*

DEMOSTRACIÓN. Supongamos que $ab \in \mathcal{I}(X)$ y que $P \in X$, entonces $ab \in P$ y por tanto tenemos que $a \in P$ ó $b \in P$. En consecuencia obtenemos que

$$X = (X \cap \mathcal{V}(aS)) \cup (X \cap \mathcal{V}(bS)).$$

Aplicando que X es irreducible, obtenemos que $X = X \cap \mathcal{V}(aS)$ ó $X = X \cap \mathcal{V}(bS)$, de donde se tiene que $X \subseteq \mathcal{V}(aS)$ ó $X \subseteq \mathcal{V}(bS)$. Por lo que deducimos que $\mathcal{I}(\mathcal{V}(aS)) \subseteq \mathcal{I}(X)$ ó que $\mathcal{I}(\mathcal{V}(bS)) \subseteq \mathcal{I}(X)$. Así $a \in \mathcal{I}(X)$ ó $b \in \mathcal{I}(X)$ e $\mathcal{I}(X)$ es un ideal primo.

Recíprocamente, si $X = X_1 \cup X_2$ con X_1 y X_2 subconjuntos cerrados de X la topología inducida, entonces

$$\mathcal{I}(X) = \mathcal{I}(X_1 \cup X_2) = \mathcal{I}(X_1) \cap \mathcal{I}(X_2).$$

Aplicando ahora el Lema 8.3, obtenemos que $\mathcal{I}(X) = \mathcal{I}(X_1)$ ó $\mathcal{I}(X) = \mathrm{I}(X_2)$. Por consiguiente, $\mathcal{V}(\mathcal{I}(X)) = \mathcal{V}(\mathcal{I}(X_1))$ ó $\mathcal{V}(\mathcal{I}(X)) = \mathcal{V}(\mathcal{I}(X_2))$ y por tanto $\overline{X} = \overline{X}_1$ ó $\overline{X} = \overline{X}_2$. Podemos concluir que

$$X_1 = X \cap X_1 = X \cap \overline{X} = \overline{X}$$

ó

$$X_2 = X \cap \overline{X}_2 = X \cap \overline{X} = X,$$

obteniendo que X es irreducible. □

2. El semiretículo asociado a un semigrupo

Recuérdese que un semirretículo es un semigrupo que cumple que todos sus elementos son idempotentes (véase Capítulo 1). Además dado un semigrupo S el conjunto $S/\mathcal{N}$ junto con la operación heredada de S era un semirretículo al que llamabamos el semirretículo asociado a S. En [**65**, §12] se prueba que si $(A,\cdot)$ es un semirretículo, entonces la relación binaria $\leq$ definida por

$$a \leq b \text{ si } ab = b$$

es una relación de orden (es reflexiva, antisimétrica y transitiva) y verifica que $\sup\{a,b\} = ab$.

NOTA 8.11. Si S es un cero-monoide, entonces $S/\mathcal{N}$ es también un cero-monoide, de hecho, $[0]_{\mathcal{N}} = \max_{\leq}(S/\mathcal{N})$ y $[1]_{\mathcal{N}} = \min_{\leq}(S/\mathcal{N})$ (recuérdese que $\mathcal{N}$ fue definido en el Capítulo 1).

Nuestro principal objetivo en esta sección es probar que existe una aplicación biyectiva entre el conjunto de ideales de $S/\mathcal{N}$ y el conjunto de ideales radicales de S. Nótese que cualquier ideal de un semirretículo es radical.

LEMA 8.12. *Sea S un semigrupo e I un ideal de $S/\mathcal{N}$. Entonces el conjunto $\bigcup_{C\in I} C$ es un ideal radical de S.*

DEMOSTRACIÓN. En primer lugar veamos que $\bigcup_{C\in I} C$ es un ideal de S. Tomemos $s \in S$ y $x \in \bigcup_{C\in I} C$. Entonces $[s]_{\mathcal{N}} \in S/\mathcal{N}$ y $[x]_{\mathcal{N}} \in I$. Ya que I es un ideal de $S/\mathcal{N}$, obtenemos que $[xs]_{\mathcal{N}} \in I$. En consecuencia $xs \in \bigcup_{C\in I} C$.

Probemos ahora que $\bigcup_{C\in I} C$ es un ideal radical. Tomemos k un entero positivo y $s \in S$ tal que $s^k \in \bigcup_{C\in I} C$. Usando ahora que $([s]_{\mathcal{N}})^k = [s]_{\mathcal{N}}$, obtenemos que $[s]_{\mathcal{N}} \in I$ y por tanto $s \in \bigcup_{C\in I} C$. □

Este lema nos permite definir la siguiente aplicación.

$$\varphi : \mathrm{Id}(S/\mathcal{N}) \to \mathrm{RI}(S),$$
$$\varphi(I) = \bigcup_{C\in I} C.$$

LEMA 8.13. *Sea S un semigrupo, J un ideal radical de S e $I = \{C \in S/\mathcal{N} \mid C \cap J \neq \emptyset\}$. Entonces I es un ideal de $S/\mathcal{N}$ y $\varphi(I) = J$.*

DEMOSTRACIÓN. Veamos que I es un ideal de $S/\mathcal{N}$. Sean $C \in I$ y $\overline{C} \in S/\mathcal{N}$. Como $C \in I$, se tiene que $C \cap J \neq \emptyset$. Tomemos ahora $x \in J$ y $s \in S$ tal que $[x]_{\mathcal{N}} = C$ y $[s]_{\mathcal{N}} = \overline{C}$. Ya que J es un ideal de S, $xs \in J$. Por tanto, $[xs]_{\mathcal{N}} \cap J \neq \emptyset$, de donde

$$C\overline{C} = [x]_{\mathcal{N}}[s]_{\mathcal{N}} = [xs]_{\mathcal{N}} \in I.$$

Probemos a continuación que $\varphi(I) = J$. Tomemos C una componente arquimediana de S tal que $C \cap J \neq \emptyset$. Sea $y \in C$ y $x \in C \cap J$. Tenemos que $y\mathcal{N}x$, por lo que existe $k \in \mathbb{N}\setminus\{0\}$ tal que $y^k = xs$. Como J es un ideal de S, se tiene que $y^k \in J$. Por último el que J es radical implica que $y \in J$ y por tanto $C \subseteq J$. □

TEOREMA 8.14. *Sea S un semigrupo. La aplicación*

$$\varphi : \mathrm{Id}(S/\mathcal{N}) \to \mathrm{RI}(S)$$

es una biyección que preserva inclusiones.

DEMOSTRACIÓN. Por el Lema 8.17, sabemos que φ es una aplicación. Como consecuencia del Lema 8.13, obtenemos que φ es sobreyectiva. Ya que las componentes arquimedianas son disjuntas, tenemos que φ es sobreyectiva. Finalmente el que φ preserva inclusiones es inmediato a partir de la definición de φ. □

El siguiente resultado nos asegura que φ manda primos a primos.

PROPOSICIÓN 8.15. *Sea S un semigrupo. Un ideal I de $S/\mathcal{N}$ es primo si y sólo si $\varphi(I)$ es un ideal primo de S.*

DEMOSTRACIÓN. Sea I un ideal de $S/\mathcal{N}$ y $x, y \in \varphi(I)$. Tenemos que $[x]_{\mathcal{N}}[y]_{\mathcal{N}} \in I$. Ya que I es un ideal primo, se llega a que $[x]_{\mathcal{N}} \in I$ ó $[y]_{\mathcal{N}} \in I$ y en consecuencia $x \in \varphi(I)$ ó $y \in \varphi(I)$.

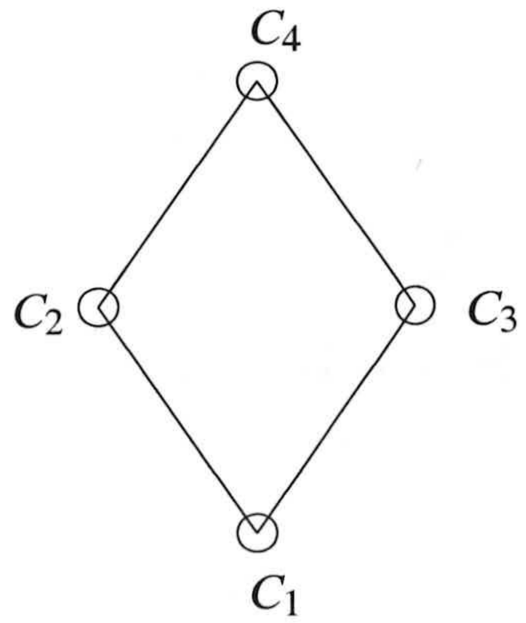
Reciprocamente, supongamos que $\varphi(I)$ es un ideal primo de S. Sean $C_1, C_2 \in S/\mathcal{N}$ tales que $C_1C_2 \in I$ y $a \in C_1$ y $b \in C_2$. Entonces $[ab]_{\mathcal{N}} = [a]_{\mathcal{N}}[b]_{\mathcal{N}} = C_1C_2 \in I$ y por tanto $ab \in \varphi(I)$. Usando ahora el que $\varphi(I)$ es un ideal primo, deducimos que $a \in \varphi(I)$ ó $b \in \varphi(I)$. En consecuencia se tiene que $C_1 = [a]_{\mathcal{N}} \in I$ ó $C_2 = [b]_{\mathcal{N}} \in I$. □

Para finalizar esta sección damos un ejemplo ilustrativo.

EJEMPLO 8.16. Sea $(S, \cdot)$ el monoide $(\mathbb{N}^2, +)$ con $+$ la suma coordenada a coordenada. Se puede probar que $\mathbb{N}^2/\mathcal{N} = \{C_1, C_2, C_3, C_4\}$ con

$$\begin{aligned} C_1 &= \{(0,0)\}, \\ C_2 &= \{(x,0) \mid x \in \mathbb{N}\backslash\{0\}\}, \\ C_3 &= \{(0,y) \mid y \in \mathbb{N}\backslash\{0\}\}, \\ C_4 &= \{(x,y) \mid x \in \mathbb{N}\backslash\{0\}, y \in \mathbb{N}\backslash\{0\}\}. \end{aligned}$$

El diagrama de Hasse del conjunto ordenado $\mathbb{N}^2/\mathcal{N}$, es



Los ideales de este semirretículo son:

$$I_1 = \{C_4\},\ I_2 = \{C_2, C_4\},\ I_3 = \{C_3, C_4\},\ I_4 = \{C_2, C_3, C_4\} \text{ y } I_5 = \{C_1, C_2, C_3, C_4\}.$$

Por tanto, los ideales radicales de $\mathbb{N}^2$ son:

$$\varphi(I_1) = C_4, \varphi(I_2) = C_2 \cup C_4, \varphi(I_3) = C_3 \cup C_4,$$
$$\varphi(I_4) = C_2 \cup C_3 \cup C_4 \text{ y } \varphi(I_5) = C_1 \cup C_2 \cup C_3 \cup C_4.$$

□

3. Cero-monoides homeomorfos

Dos cero-monoides son **homeomorfos** si sus respectivos espectros son homeomorfos como espacios topológicos. Recuérdese que f es un homeomorfismo entre espacios topológicos si es biyectiva, continua y su inversa también es continua. Nuestro objetivo en esta sección es caracterizar este concepto topológico desde un punto de vista semigrupista.

A lo largo de esta sección $(S, \cdot)$ y $(\overline{S}, \cdot)$ son dos cero-monoides con identidad 1 y cero 0. Tal como hicimos en la Sección 2, $S/\mathcal{N}$ y $\overline{S}/\mathcal{N}$ denotan sus respectivos semirretículos asociados, que también son cero-monoides con identidad $[1]_{\mathcal{N}}$ y cero $[0]_{\mathcal{N}}$.

TEOREMA 8.17. *Sea S un cero-monoide. La aplicación*

$$f : \mathrm{Spec}(S/\mathcal{N}) \to \mathrm{Spec}(S),$$
$$f(P) = \bigcup_{C \in P} C$$

es un homeomorfismo.

DEMOSTRACIÓN. Por el Teorema 8.14 y la Proposición 8.15, deducimos que la función f es biyectiva. Es más, sabemos que f es la restricción de

$$\varphi : \mathrm{Id}(S/\mathcal{N}) \to \mathrm{RI}(S),$$
$$\varphi(I) = \bigcup_{C \in I} C,$$

lo cual implica que $f(\mathcal{V}(I)) = \mathcal{V}(\varphi(I))$. En consecuencia tenemos que f es cerrada y por tanto f^{-1} es continua. Por la Proposición 8.6, si I es un ideal de S, entonces $\mathcal{V}(I) = \mathcal{V}(\mathrm{Rad}(I))$ y en consecuencia

$$f^{-1}(\mathcal{V}(I)) = f^{-1}(\mathcal{V}(\mathrm{Rad}(I)) = \mathcal{V}(\varphi^{-1}(\mathrm{Rad}(I))).$$

Por tanto, f es continua. □

COROLARIO 8.18. *Dos cero-monoides son homeomorfos si y sólo si sus semirretículos asociados lo son.*

El siguiente resultado es bien conocido y a la vez fácil de probar.

LEMA 8.19. *Sea S un cero monoide.*

- *La unión de ideales radicales de S es de nuevo un ideal radical de S.*
- *La intersección de ideales radicales de S es de nuevo un ideal radical de S.*

En virtud del Lema 8.19 el conjunto de ideales radicales de S con el orden inclusión es un retículo, en el que el supremo de dos ideales es su unión y el ínfimo su intersección. Nuestro propósito ahora es probar que dos cero-monoides S y $\overline{S}$ son homeomorfos si y sólo si los retículos $(\mathrm{RI}(S), \subseteq)$ y $(\mathrm{RI}(\overline{S}), \subseteq)$ son isomorfos como retículos, a saber, existe una aplicación biyectiva θ entre dichos retículos verificando que $I \subseteq J$ si y sólo si $\theta(I) \subseteq \theta(J)$.

El siguiente resultado es el primer paso para conseguir nuestro propósito.

LEMA 8.20. *Las siguientes afirmaciones son equivalentes.*

(1) Los cero-monoides S y $\overline{S}$ son homeomorfos.

(2) Existe una aplicación

$$\theta : \mathrm{RI}(S) \to \mathrm{RI}(\overline{S})$$

verificando:

(i) *θ es biyectiva,*

(ii) *para cualesquiera $I, J \in \mathrm{RI}(S)$, $I \subseteq J$ si y sólo si $\theta(I) \subseteq \theta(J)$,*

(iii) *I es un ideal primo si y sólo si $\theta(I)$ es un ideal primo.*

DEMOSTRACIÓN. *(1) implica (2).* Sea $f : \mathrm{Spec}(S) \to \mathrm{Spec}(\overline{S})$ un homeomorfismo. La aplicación

$$g : \mathrm{CS}(S) \to \mathrm{CS}(\overline{S}),$$
$$g(\mathcal{V}(I)) = f_*(\mathcal{V}(I))$$

es una aplicación biyectiva y por tanto, por el Teorema 8.8, la aplicación

$$\theta : \mathrm{RI}(S) \to \mathrm{RI}(\overline{S}),$$
$$\theta(\mathfrak{I}(\mathcal{V}(I))) = \mathfrak{I}(g(\mathcal{V}(I)))$$

es biyectiva (nótese que $\mathfrak{I}(\mathcal{V}(I)) = \mathrm{Rad}(I)$ y por tanto si I es ideal radical, $\theta(I) = \mathfrak{I}(g(\mathcal{V}(I)))$). Veamos ahora que θ verifica *(ii)* y *(iii)*.

- Si $I \subseteq J$, entonces $\mathcal{V}(J) \subseteq \mathcal{V}(I)$ y por tanto $g(\mathcal{V}(J)) \subseteq g(\mathcal{V}(I))$. En consecuencia $\mathfrak{I}(g(\mathcal{V}(I))) \subseteq \mathfrak{I}(g(\mathcal{V}(J)))$, de ahí que $\theta(I) \subseteq \theta(J)$.
- Si $\theta(I) \subseteq \theta(J)$, entonces $\mathfrak{I}(g(\mathcal{V}(I))) \subseteq \mathfrak{I}(g(\mathcal{V}(J)))$ y por tanto $g(\mathcal{V}(J)) \subseteq g(\mathcal{V}(I))$. Usando la definición de g, obtenemos que $\mathcal{V}(J) \subseteq \mathcal{V}(I)$, de donde

$$I = \mathfrak{I}(\mathcal{V}(I)) \subseteq \mathfrak{I}(\mathcal{V}(J)) = J.$$

- Ya que f es un homeomorfismo, $\mathcal{V}(I)$ es irreducible si y sólo si $g(\mathcal{V}(I)) = f_*(\mathcal{V}(I))$ es irreducible. Por el Teorema 8.10, deducimos que $\mathfrak{I}(\mathcal{V}(I))$ es primo si y sólo si $\mathfrak{I}(g(\mathcal{V}(I))$ es primo. En consecuencia I es primo si y sólo si $\theta(I)$ es primo.

(2) implica (1). Definimos $f : \mathrm{Spec}(S) \to \mathrm{Spec}(\overline{S})$ por $f(P) = \theta(P)$. A partir de (i) y (iii), deducimos que f está bien definida y es biyectiva. Si I es un ideal radical de S, aplicando (ii) y (iii), deducimos que $f_*(\mathcal{V}(I)) = \mathcal{V}(\theta(I))$. Por tanto f es cerrada, de donde se obtiene que f^{-1} es continua. Obsérvese ahora que $f^{-1}(P) = \theta^{-1}(P)$ y que θ^{-1} satisface (i), (ii) y (iii). Repetiendo este argumento, obtenemos que f^{-1} es cerrado y por tanto f es continua. □

Para probar que dos cero-monoides S y $\overline{S}$ son homeomorfos si y sólo si $(\mathrm{RI}(S),\subseteq)$ y $(\mathrm{RI}(\overline{S}),\subseteq)$ son isomorfos como retículos, basta probar que (iii) se puede deducir de (i) y (ii). Para ello necesitamos introducir algunos conceptos y resultados concernientes a éstos.

Recordemos que un ideal I de un semigrupo S es irreducible, si no puede ser expresado como intersección de dos ideales que lo contengan propiamente. En vista del Lema 8.3, es fácil demostrar que cualquier ideal primo es irreducible. En general, el recíproco de este hecho no es cierto, pero veremos que en el caso en que S sea un semirretículo, ambos conceptos coinciden.

LEMA 8.21. *Si $(A,\cdot)$ es un semirretículo y $a,b\in A$, entonces $aS\cap bS=abS$.*

DEMOSTRACIÓN. Claramente, tenemos que $ab\in aS\cap bS$ y por tanto $abS\subseteq aS\cap bS$. Tomemos ahora

$$x=as=b\overline{s}\in aS\cap bS.$$

Tenemos que $a(as)=a(b\overline{s})$. Aplicando que $a^2=a$, obtenemos $x=as=(ab)\overline{s}\in abS$. □

LEMA 8.22. *Sea $(A,\cdot)$ un semirretículo. Un ideal I de A es irreducible si y sólo si es primo.*

DEMOSTRACIÓN. Sea I un ideal irreducible de A. Tomemos $a,b\in A$ tales que $ab\in I$. Por el Lema 8.21, tenemos que

$$I=I\cup abS=I\cup(aS\cap bS)=(I\cup aS)\cap(I\cup bS).$$

Usando que I es irreducible se deduce que $I=I\cup aS$ ó $I=I\cup bS$, de donde tenemos que $a\in I$ ó $b\in I$.

El recíproco es inmediato a partir del Lema 8.3. □

El siguiente resultado es bien conocido en teoría de retículos.

LEMA 8.23. *Sean $S,\overline{S}$ cero-monoides, $\theta:\mathrm{RI}(S)\to\mathrm{RI}(\overline{S})$ una aplicación biyectiva e I,J dos ideales de S. Las siguientes afirmaciones son equivalentes.*

(1) $I\subseteq J$ si y sólo si $\theta(I)\subseteq\theta(J)$.
(2) $\theta(I\cup J)=\theta(I)\cup\theta(J)$ y $\theta(I\cap J)=\theta(I)\cap\theta(J)$.
(3) $\theta(I\cup J)=\theta(I)\cup\theta(J)$.
(4) $\theta(I\cap J)=\theta(I)\cap\theta(J)$.

TEOREMA 8.24. *Sean S y $\overline{S}$ dos cero-monoides. Las siguientes condiciones son equivalentes.*

(1) S es homeomorfo a $\overline{S}$.
(2) Los retículos $(\mathrm{Id}(S/\mathcal{N}),\subseteq)$ e $(\mathrm{Id}(\overline{S}/\mathcal{N}),\subseteq)$ son isomorfos.
(3) Los retículos $(\mathrm{RI}(S),\subseteq)$ y $(\mathrm{RI}(\overline{S}),\subseteq)$ son isomorfos.

DEMOSTRACIÓN. *(1) implica (2).* Por el Corolario 8.18, tenemos que $S/\mathcal{N}$ es homeomorfo a $\overline{S}/\mathcal{N}$. Usando el Lema 8.20 y el hecho de que en un semiretículo

todo ideal es radical, obtenemos que existe una aplicación biyectiva $\theta : \mathrm{Id}(S/\mathcal{N}) \to \mathrm{Id}(\overline{S}/\mathcal{N})$ tal que $I \subseteq J$ si y sólo si $\theta(I) \subseteq \theta(J)$.

(2) implica (1). Sea $\theta : \mathrm{Id}(S/\mathcal{N}) \to \mathrm{Id}(\overline{S}/\mathcal{N})$ un isomorfismo de retículos. Tenemos que θ es una aplicación biyectiva cumpliendo que $I \subseteq J$ si y sólo si $\theta(I) \subseteq \theta(J)$. Por el Lema 8.23, sabemos que $\theta(I \cap J) = \theta(I) \cap \theta(J)$. Veamos ahora que I es un ideal primo si y sólo si $\theta(I)$ es primo. Por el Lema 8.22, sólo hemos de probar que I es irreducible si y sólo si $\theta(I)$ es irreducible. Pero esto se deduce de que $I = J \cap K$ si y sólo si $\theta(I) = \theta(J) \cap \theta(K)$. Usando ahora el Lema 8.20, deducimos que $S/\mathcal{N}$ y $\overline{S}/\mathcal{N}$ son homeomorfos, de donde deducimos que S y $\overline{S}$ son homeomorfos.

(2) si y sólo si (3). Es inmediato a partir del hecho que

$$\varphi : \mathrm{Id}(S/\mathcal{N}) \to \mathrm{RI}(S),$$
$$\varphi(I) = \bigcup_{C \in I} C$$

es un isomorfismo de retículos (ver Teorema 8.14). □

Como consecuencia inmediata del Lema 8.23 y el Teorema 8.24 obtenemos el siguiente resultado.

COROLARIO 8.25. *Sean S y $\overline{S}$ dos cero-monoides. Equivalen:*

(1) S es homeomorfo a $\overline{S}$,
(2) los semigrupos $(\mathrm{RI}(S), \cup)$ y $(\mathrm{RI}(\overline{S}), \cup)$ son isomorfos,
(3) los semigrupos $(\mathrm{RI}(S), \cap)$ y $(\mathrm{RI}(\overline{S}), \cap)$ son isomorfos.

4. El caso noetheriano

Un espacio topológico T es **noetheriano** si cualquier cadena descendente de conjuntos cerrados de T es estacionaria. Un cero-monoide $(S, \cdot)$ es **noetheriano** si $\mathrm{Spec}(S)$ es noetheriano.

El siguiente resultado aparece en [**48**].

LEMA 8.26. *Un espacio topológico noetheriano tiene un número finito de componentes irreducibles, es más, cualquiera de ellas no está contenida en la unión del resto.*

A lo largo de esta sección $(S, \cdot)$ es un cero-monoide. Si I es un ideal de S, los elementos de $\mathcal{V}(I)$ se llaman **divisores primos** de I.

LEMA 8.27. *Sea S un cero-monoide noetheriano. Todo ideal propio de S tiene un número finito de divisores primos minimales.*

DEMOSTRACIÓN. Sea I un ideal propio de S. Por el Lema 8.26, $\mathcal{V}(I)$ tiene un número finito de componentes irreducibles, digamos $C_1, \ldots, C_r$. Tenemos así que $\mathcal{V}(I) = C_1 \cup \ldots \cup C_r$ y en consecuencia

$$\mathrm{Rad}(I) = \mathfrak{I}(\mathcal{V}(I)) = \mathfrak{I}(C_1 \cup \ldots \cup C_r) = \mathfrak{I}(C_1) \cap \ldots \cap \mathfrak{I}(C_r).$$

Aplicando el Teorema 8.10, obtenemos que $\{\mathfrak{I}(C_1), \ldots, \mathfrak{I}(C_r)\} \subseteq \mathrm{Spec}(S)$. Por la Proposición 8.6 y el Lema 8.26, concluimos que $\{\mathfrak{I}(C_1), \ldots, \mathfrak{I}(C_r)\}$ es el conjunto de divisores primos minimales de I. □

En vista del Lema 8.1 y la Nota 8.4, obtenemos que si $P_1, P_2 \in \mathrm{Spec}(S)$, entonces $P_1 \cup P_2 \in \mathrm{Spec}(S)$. Por tanto $(\mathrm{Spec}(S), \cup)$ es un semigrupo.

TEOREMA 8.28. *Sean $(S, \cdot)$ y $(\overline{S}, \cdot)$ dos cero-monoides noetherianos. Las siguientes afirmaciones son equivalentes.*

(1) S y $\overline{S}$ son homeomorfos.
(2) Los semigrupos $(\mathrm{Spec}(S), \cup)$ y $(\mathrm{Spec}(\overline{S}), \cup)$ son isomorfos.

DEMOSTRACIÓN. *(1) implica (2).* Por los Lemas 8.20 y 8.23, existe una aplicación biyectiva $\theta : \mathrm{Spec}(S) \to \mathrm{Spec}(\overline{S})$ tal que $\theta(P_1 \cup P_2) = \theta(P_1) \cup \theta(P_2)$. En consecuencia θ es un isomorfismo de semigrupos.

(2) implica (1). Sea $\theta : \mathrm{Spec}(S) \to \mathrm{Spec}(\overline{S})$ una aplicación biyectiva tal que $\theta(P_1 \cup P_2) = \theta(P_1) \cup \theta(P_2)$. Dados $P, Q \in \mathrm{Spec}(S)$ tenemos que $P \subseteq Q$ si sólo si $\theta(P) \subseteq \theta(Q)$. Usando este argumento y el Lema 8.3, obtenemos que si $P_1, \ldots, P_r, Q_1, \ldots, Q_s \in \mathrm{Spec}(S)$ y $P_1 \cap \ldots \cap P_r = Q_1 \cap \ldots \cap Q_s$, entonces $\theta(P_1) \cap \ldots \cap \theta(P_r) = \theta(Q_1) \cap \ldots \cap \theta(Q_s)$. Esto nos permite definir una aplicación $f : \mathrm{RI}(S) \to \mathrm{RI}(\overline{S})$ como sigue. Si I es un ideal propio y radical de S, entonces sabemos por la Proposición 8.6 y el Lema 8.27 que existen $P_1, \ldots, P_r \in \mathrm{Spec}(S)$ tales que $I = P_1 \cap \ldots \cap P_r$ con $P_1, \ldots, P_r$ divisores primos minimales de I. Usando esto, definimos

$$f(I) = \theta(P_1) \cap \ldots \cap \theta(P_r).$$

Finalmente, sea $f(S) = \overline{S}$. Es fácil probar que f es una aplicación biyectiva y que $f(I \cap J) = f(I) \cap f(J)$. Por el Corolario 8.25 tenemos que S y $\overline{S}$ son homeomorfos. □

5. Semigrupos con un número finito de ideales radicales

En esta sección $(A, \cdot)$ denota un semirretículo y $\leq$ la relación de orden en A definida por $a \leq b$ si $ab = b$. Dado $a \in A$, definimos $\mathcal{B}(a) = \{x \in A \mid x \leq a\}$.

LEMA 8.29. *Sea A un semirretículo, I un ideal de A y $a \notin I$. Entonces $I \cap \mathcal{B}(a) = \emptyset$.*

DEMOSTRACIÓN. Supongamos que existe $b \in I \cap \mathcal{B}(a)$. Ya que I es un ideal, $ab \in I$. Además, $b \leq a$, lo cual implica que $ab = a$. Por tanto $a \in I$, en contradicción con que $a \notin I$. □

LEMA 8.30. *Sea A un semirretículo y $a \in A$ tal que $a \neq \max(A)$. Entonces $I = A \setminus \mathcal{B}(a)$ es un ideal primo de A.*

DEMOSTRACIÓN. Como $a \neq \max(A)$, tenemos que $\mathcal{B}(a) \neq A$ y por tanto $I = A \setminus \mathcal{B}(a) \neq \emptyset$. Sea $b \in I$ y $x \in A$. Si $bx \notin I$, entonces $bx \leq a$ y por tanto $b \leq a$, lo cual, por el Lema 8.29, es imposible. En consecuencia $bx \in I$ e I es un ideal de A. Veamos ahora que I es primo. Sean $x \notin I$ e $y \notin I$. Tenemos que $x \leq a$ e $y \leq a$, lo cual implica que $xy \leq a$ y por tanto $xy \notin I$. □

PROPOSICIÓN 8.31. *Sea $(S, \cdot)$ un semigrupo. Son equivalentes las siguientes condiciones.*

(1) El conjunto $S/\mathcal{N}$ es finito.
(2) S tiene un número finito de ideales radicales.

(3) S tiene un número finito de ideales primos.

DEMOSTRACIÓN. *(1) implica (2).* Inmediato a partir del Teorema 8.14.

(2) implica (3). Sólo hay que recordar que todo ideal primo es radical.

(3) implica (1). Por el Teorema 8.14 y la Proposición 8.15, sabemos que si S tiene un número finito de ideales primos, entonces su semiretículo asociado $S/\mathcal{N}$ tiene también un número finito de ideales primos. Usando el Lema 8.30 y el que si $\mathcal{B}(a) = \mathcal{B}(b)$, entonces $a = b$, deducimos que $S/\mathcal{N}$ es un conjunto finito. □

NOTA 8.32. Obsérvese que si $(A,\cdot)$ es un semirretículo finito y $A = \{a_1,\cdots,a_k\}$, entonces $a_1a_2\ldots a_k = \max(A)$.

PROPOSICIÓN 8.33. *Sea $(A,\cdot)$ un semirretículo finito. El ideal I es un ideal primo propio de A si y sólo si existe $a \in A$ tal que $a \neq \max(A)$ e $I = A \setminus \mathcal{B}(a)$.*

DEMOSTRACIÓN. Supongamos que I es un ideal propio de A. Consideremos $H = A \setminus I = \{h_1,\ldots,h_n\}$. Ya que I es un ideal primo de A, H es un subsemigrupo de A y por tanto $a = h_1\cdots h_n \in H$. Probemos ahora que $I = A \setminus \mathcal{B}(a)$.

- Como $a \in H = A \setminus I$, obtenemos que $a \notin I$. Usando el Lema 8.29 deducimos que $\mathcal{B}(a) \cap I = \emptyset$ y por tanto $I \subseteq A \setminus \mathcal{B}(a)$.
- Si $h \in H$, entonces $h = h_i$ para algún $i \in \{1,\ldots,n\}$. En consecuencia $h \leq h_1\cdots h_n = a$ y por tanto $h \in \mathcal{B}(a)$. Así que $H \subseteq \mathcal{B}(a)$, de donde $A \setminus \mathcal{B}(a) \subseteq A \setminus H = I$.

El recíproco es inmediato a partir del Lema 8.30. □

Como consecuencia de la Proposición 8.33, obtenemos el siguiente resultado.

COROLARIO 8.34. *Sea $(S,\cdot)$ un semigrupo y supongamos que $S/\mathcal{N}$ tiene n elementos. Entonces S tiene exactamente n ideales primos.*

Un subconjunto $\{a_1,\ldots,a_n\}$ de A está formado por elementos incomparables si para todo $i,j \in \{1,\ldots,n\}$, $a_i \leq a_j$ lleva a $i = j$.

PROPOSICIÓN 8.35. *Sea $(A,\cdot)$ un semirretículo finito. El ideal I es un ideal propio de A si y sólo si existe un subconjunto $\{a_1,\ldots,a_n\}$ de $A \setminus \{\max(A)\}$ de elementos incomparables tal que $I = A \setminus (\mathcal{B}(a_1) \cup \ldots \cup \mathcal{B}(a_n))$.*

DEMOSTRACIÓN. Ya que I es un ideal de A y este último conjunto es un semiretículo, I es un ideal radical suyo. Por la Proposición 8.6, I se puede expresar como intersección de ideales primos. Usando ahora la Proposición 8.33, deducimos que existe $\{a_1,\ldots,a_n\}$ un subconjunto de $A \setminus \{\max(A)\}$ tal que

$$I = (A \setminus \mathcal{B}(a_1)) \cap \ldots \cap (A \setminus \mathcal{B}(a_n)) = A \setminus (\mathcal{B}(a_1) \cup \ldots \cup \mathcal{B}(a_n)).$$

Además como $a_i \leq a_j$ implica $\mathcal{B}(a_i) \subseteq \mathcal{B}(a_j)$, podemos elegir el conjunto $\{a_1,\ldots,a_n\}$ de manera que esté formado por elementos incomparables y así tener que $A \setminus \mathcal{B}(a_j) \subseteq A \setminus \mathcal{B}(a_i)$ y $(A \setminus \mathcal{B}(a_j)) \cap (A \setminus \mathcal{B}(a_i)) = A \setminus \mathcal{B}(a_j)$. En consecuencia el elemento a_i puede ser eliminado.

El recíproco es trivial. □

6. Semirretículos finitos homeomorfos

Sean $(A,\cdot)$ y $(B,\cdot)$ dos semirretículos que a su vez son cero monoides. Obsérvese que un semirretículo es un cero-monoide si y sólo si tiene máximo y mínimo.

TEOREMA 8.36. *Sean A y B como antes. Si ambos son finitos, entonces las siguientes afirmaciones son equivalentes.*

(1) A y B son semigrupos isomorfos.
(2) A y B son semigrupos homeomorfos.

DEMOSTRACIÓN. *(1) implica (2).* Es trivial.

(2) implica (1). Por el Teorema 8.28 (obsérvese que finito implica noetheriano), tenemos que existe una aplicación biyectiva $\theta : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ tal que $\theta(P_1 \cup P_2) = \theta(P_1) \cup \theta(P_2)$. En consecuencia $P_1 \subseteq P_2$ si y sólo si $\theta(P_1) \subseteq \theta(P_2)$. Definimos $f : A \to B$ como sigue. Si $a \in A \setminus \{\max(A)\}$, entonces por la Proposición 8.33 sabemos que $\theta(A \setminus \mathcal{B}(a)) = B \setminus \mathcal{B}(b)$ para algún $b \in B$. Usando esto podemos definir $f(a) = b$ y $f(\max(A)) = \max(B)$. Claramente se tiene que esta función es biyectiva. Veamos que $f(xy) = f(x)f(y)$.

- Tenemos que $A \setminus \mathcal{B}(xy) \subseteq A \setminus \mathcal{B}(x)$. Por tanto $B \setminus \mathcal{B}(f(xy)) \subseteq B \setminus \mathcal{B}(f(x))$, de donde$f(x) \leq f(xy)$.
- Tenemos que $A \setminus \mathcal{B}(xy) \subseteq A \setminus \mathcal{B}(y)$. Por tanto $B \setminus \mathcal{B}(f(xy)) \subseteq B \setminus \mathcal{B}(f(y))$, de donde $f(y) \leq f(xy)$.

A partir de lo anterior podemos deducir que $f(x)f(y) \leq f(xy)$. Tomemos ahora $z \in A$ tal que $f(z) = f(x)f(y)$. Tenemos que $f(x) \leq f(z) \leq f(xy)$ y $f(y) \leq f(z) \leq f(xy)$. A partir de la definición de f y ya que θ preserva inclusiones, deducimos que $x \leq z \leq xy$ e $y \leq z \leq xy$ y por tanto $z = xy$. Por consiguiente f es un isomorfismo de semigrupos. □

7. Comentarios finales

Finalizamos este capítulo con algunos comentarios.

NOTA 8.37. Dado un semigrupo $(S,\cdot)$ y dos indeterminadas $x, y \notin S$, el conjunto $S \cup \{x,y\}$ tiene estructura de cero-monoide con la operación $*$ definida de la siguiente forma

$$a * b = \begin{cases} ab & \text{si } a,b \in S, \\ y & \text{si } a = y \text{ ó } b = y, \\ b & \text{si } a = x, \\ a & \text{si } b = x. \end{cases}$$

Con esta operación x es el elemento identidad de $S \cup \{x,y\}$ e y es el cero. A $(S \cup \{x,y\}, *)$ lo llamamos el **cero-monoide asociado** a S y lo denotamos por $C(S)$.

Decimos que dos semigrupos S y $\overline{S}$ son homeomorfos si $C(S)$ y $C(\overline{S})$ son homeomorfos.

Es fácil demostrar lo siguiente:

- S es isomorfo a $\overline{S}$ si y sólo si $C(S)$ es isomorfo a $C(\overline{S})$,
- $C(S/\mathcal{N})$ es isomorfo a $C(S)/\mathcal{N}$.

Por tanto, dos semigrupos S y $\overline{S}$ son homeomorfos si y sólo si $C(S/\mathcal{N})$ y $C(\overline{S}/\mathcal{N})$ son homeomorfos.

NOTA 8.38. Si S es un semigrupo finitamente generado, entonces el semirretículo $S/\mathcal{N}$ es finito y puede ser calculado a partir de una presentación de S (véase [**65**, §13]). En consecuencia, podemos determinar algorítmicamente si dos semigrupos finitamente generados son o no homeomorfos (nótese que dos de esos semigrupos son homeomorfos si y sólo si sus semirretículos asociados son isomorfos). Usando ese mismo hecho, los resultados de este capítulo también nos proporcionan un método para determinar si un determinado ideal de un monoide finitamente generado es primo o radical.

NOTA 8.39. Dado un cero-monoide $A \neq \{0\}$, definimos la **dimensión de Krull** de A, $\dim(A)$, como el supremo de las longitudes n de todas las cadenas

$$P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n$$

verificando que $P_0, P_1, \ldots, P_n \in \operatorname{Spec}(A)$. Obsérvese que a partir de esta definición tenemos que $\dim(A) \geq 0$. Si S es un semigrupo, entonces definimos $\dim(S) = \dim(C(S)) - 2$. Es fácil probar que S es un semigrupo arquimediano si y sólo si $\dim(S) = -1$. Usando la Proposición 8.33 y la Nota 8.38, podemos asegurar que la dimensión de un semigrupo finitamente generado puede ser calculada algorítmicamente a partir de cualquiera de sus presentaciones.

CAPÍTULO 9

Ideales Irreducibles de monoides conmutativos finitamente generados

1. Introducción

La descomposición de un ideal en ideales irreducibles ha sido normalmente usada en la literatura para probar la existencia de descomposiciones primarias de ideales de anillos y monoides (véase por ejemplo [**7, 9**]). Existen procedimientos para calcular descomposiciones primarias de ideales en álgebras afines y métodos para decidir cuando un ideal dado es primario (ver [**10**]). Sin embargo, el estudio de los ideales irreducibles y la descomposición de ideales en éstos fué casi olvidada hasta [**39**]. En este capítulo, daremos caracterizaciónes de ideales irreducibles de monoides finitamente generados y un procedimiento tal que dado un ideal nos devuelva una de sus descomposiciones en irreducibles.

Aunque existe un paralelismo entre la teoría de ideales de anillos y la de ideales de monoides (ver por ejemplo [**7**]), las pequeñas diferencias entre ellas hacen que el estudio que aquí se realiza no se pueda, en principio, llevar a cabo en anillos (la principal diferencia se encuentra en el Lema 9.9).

En primer lugar vamos a concentrarnos en el estudio de ideales irreducibles de $\mathbb{N}^p$ y en la descomposición de un ideal cualquiera como intersección de éstos. Después generalizaremos estos resultados para monoides finitamente generados arbitrarios y por último discutiremos algunos aspectos computacionales para el cálculo de tales descomposiciones.

2. Ideales irreducibles de $\mathbb{N}^p$

Empezamos esta sección recordando la definición de ideal irreducible de un monoide. A continuación nos centraremos en dar una caracterización de los ideales irreducibles de $\mathbb{N}^p$ y un método para calcular una descomposición de un ideal arbitrario de $\mathbb{N}^p$ en intersección de irreducibles.

Dado un ideal I de un monoide S, decíamos que I es irreducible si no existen ideales J, K de S que contengan propiamente a I y tales que $I = J \cap K$.

Debido a que hemos de realizar intersección de ideales, necesitamos saber cómo calcular la intersección de dos ideales de $\mathbb{N}^p$ a partir de un sistema de generadores de cada uno de ellos.

Recuérdese que dados $a = (a_1, \ldots, a_p)$, $b = (b_1, \ldots, b_p) \in \mathbb{N}^p$, denotabamos por $a \vee b$ al elemento $(\text{máximo}\{a_1, b_1\}, \ldots, \text{máximo}\{a_p, b_p\})$.

LEMA 9.1. *Sean* $A = \{x_1, \ldots, x_r\} + \mathbb{N}^p$ *y* $B = \{y_1, \ldots, y_s\} + \mathbb{N}^p$ *dos ideales de* $\mathbb{N}^p$. *Entonces*

$$A \cap B = \{x_i \vee y_j \mid i \in \{1, \ldots, r\}, j \in \{1, \ldots, s\}\} + \mathbb{N}^p.$$

DEMOSTRACIÓN. Sea $C = \{x_i \vee y_j \mid i \in \{1, \ldots, r\}, j \in \{1, \ldots, s\}\} + \mathbb{N}^p$. Si $x \in A \cap B$, entonces $x \geq x_i$ y $x \geq y_j$ para algún $i \in \{1, \ldots, r\}$ y $j \in \{1, \ldots, s\}$. Así, $x \geq x_i \vee y_j$ y por tanto $x \in C$.

Si tomamos ahora $x \in C$, entonces $x \geq x_i \vee y_j$ para algún i, j. Es por ello que $x \geq x_i$ y $x \geq y_j$, lo cual hace que $x \in A \cap B$. □

PROPOSICIÓN 9.2. *Sea* J *un ideal de* $\mathbb{N}^p$. *Las siguientes condiciones son equivalentes.*

(1) J *es irreducible.*

(2) Existen $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, p\}$ *y* $k_1, \ldots, k_r \in \mathbb{N}$ *tales que*

$$J = \{k_1 e_{i_1}, \ldots, k_r e_{i_r}\} + \mathbb{N}^p.$$

DEMOSTRACIÓN. *(1) implica (2).* Supongamos $J = \{x_1, \ldots, x_r\} + \mathbb{N}^p$ y $\#\mathrm{Supp}(x_1) \geq 2$. Tomemos $i, j \in \mathrm{Supp}(x_1)$ con $i \neq j$, usando ahora el Lema 9.1, obtenemos que $J = A \cap B$, donde

$$A = \{x_1 - e_i, x_2, \ldots, x_r\} + \mathbb{N}^p,\ B = \{x_1 - e_j, x_2, \ldots, x_r\} + \mathbb{N}^p.$$

(2) implica (1). Si $J = A \cap B$ con A, B conteniendo propiamente a J, entonces existen $x \in \mathrm{Minimales}_{\leq}(A)$ e $y \in \mathrm{Minimales}_{\leq}(B)$ tales que $x, y \notin J$. Finalmente, teniendo en cuenta que $x \vee y \in (A \cap B) \setminus J$ concluimos la demostración. □

NOTA 9.3. En vista de la Proposición 9.2, si I y J son ideales irreducibles de $\mathbb{N}^p$, también lo es $I \cup J$ (téngase en cuenta que un sistema de generadores de $I \cup J$ es la unión de los sistemas de generadores de I y J).

El siguiente resultado no sólamente prueba la existencia de descomposiciones de un ideal en irreducibles, su demostración da también un procedimiento para el cálculo de tales descomposiciónes.

COROLARIO 9.4. *Sea* J *un ideal de* $\mathbb{N}^p$. *Entonces existen* $J_1, \ldots, J_s$ *ideales irreducibles de* $\mathbb{N}^p$ *tales que* $J = J_1 \cap \ldots \cap J_s$.

DEMOSTRACIÓN. Supongamos que $J = \{x_1, \ldots, x_r\} + \mathbb{N}^p$. Si J no es irreducible, por la Proposición 9.2, tenemos que existen j, k, l tales que $k, l \in \mathrm{Supp}(x_j)$ y $k \neq l$. Si $x_j = \sum_{i=1}^{p} \lambda_i e_i$, por el Lema 9.1, $J = J_1 \cap J_2$, con $J_1 = \{x_1, \ldots, x_j - \lambda_k e_k, \ldots, x_r\} + \mathbb{N}^p$ y $J_2 = \{x_1, \ldots, x_j - \lambda_l e_l, \ldots, x_r\} + \mathbb{N}^p$. Repitiendo este proceso para J_1 y J_2, después de un número finito de pasos obtenemos que $J = J_{i_1} \cap \ldots \cap J_{i_s}$ con J_{i_k} verificando que sus elementos minimales tienen soporte de cardinal uno. Aplicando ahora la Proposición 9.2, obtenemos que estos ideales son irreducibles. □

EJEMPLO 9.5. Sea I el ideal de $\mathbb{N}^2$ generado por $\{(3,0), (1,2), (0,5)\}$. Entonces

$$\begin{aligned} I &= (\{(3,0), (1,0), (0,5)\} + \mathbb{N}^2) \cap (\{(3,0), (0,2), (0,5)\} + \mathbb{N}^2) \\ &= (\{(1,0), (0,5)\} + \mathbb{N}^2) \cap (\{(3,0), (0,2)\} + \mathbb{N}^2). \end{aligned}$$

□

El resto de la sección está dedicado a dar una caracterización alternativa de ideal irreducible de $\mathbb{N}^p$. Esta nueva caracterización será la que generalizaremos en las siguientes secciones para monoides cualesquiera.

Dado un elemento x de un monoide S, recordemos que

$$\mathcal{B}(x) = \{y \in S \mid y \leq x\}.$$

Obsérvese que $S \setminus \mathcal{B}(x)$ es un ideal de S.

PROPOSICIÓN 9.6. *Sea* $J = \{k_1 e_{i_1}, \ldots, k_r e_{i_r}\} + \mathbb{N}^p$ *un ideal de* $\mathbb{N}^p$. *Supongamos que* $\{j_1, \ldots, j_s\} = \{1, \ldots, p\} \setminus \{i_1, \ldots, i_r\}$ *y definamos para todo* $n \in \mathbb{N}$,

$$t_n = (k_1 - 1)e_{i_1} + \cdots + (k_r - 1)e_{i_r} + n(e_{j_1} + \cdots + e_{j_s}).$$

Entonces

$$J = \bigcap_{n \in \mathbb{N}} (\mathbb{N}^p \setminus \mathcal{B}(t_n)).$$

DEMOSTRACIÓN. Tomemos $s \in J$. Entonces para todo $n \in \mathbb{N}$, tenemos que $s \leq t_n$ y en consecuencia $s \notin \mathcal{B}(t_n)$. Por tanto $s \in \bigcap_{n \in \mathbb{N}} (\mathbb{N}^p \setminus \mathcal{B}(t_n))$.

Supongamos ahora que $s = (x_1, \ldots, x_p) \notin J$. Entonces $x_{i_1} < k_1, \ldots, x_{i_r} < k_r$. Tomando $n \in \mathbb{N}$ tal que $n >$ máximo$\{x_{j_1}, \ldots, x_{j_s}\}$, obtenemos que $s \in \mathcal{B}(t_n)$ y por tanto $s \notin \bigcap_{n \in \mathbb{N}} (S \setminus \mathcal{B}(t_n))$. □

Obsérvese que para cualquier par x, y de elementos de un monoide S, si $x \leq y$, entonces $\mathcal{B}(x) \subseteq \mathcal{B}(y)$. Esto implica que la sucesión $\{\mathbb{N}^p \setminus \mathcal{B}(t_n)\}_{n \in \mathbb{N}}$ de la Proposición 9.6 es una sucesión decreciente (estrictamente si $r < p$) de ideales. Usando esto y la Proposición 9.2, obtenemos lo siguiente.

COROLARIO 9.7. *Sea* J *un ideal irreducible de* $\mathbb{N}^p$. *Entonces existe una sucesión* $\{x_n\}_{n \in \mathbb{N}}$ *de elementos de* $\mathbb{N}^p$ *tal que* $x_n \leq x_{n+1}$ *para todo* $n \in \mathbb{N}$ *y tal que*

$$J = \bigcap_{n \in \mathbb{N}} (\mathbb{N}^p \setminus \mathcal{B}(x_n)).$$

3. Algunos ideales irreducibles

Vemos ahora que los ideales que aparecen en la Proposición 9.6 y en el Corolario 9.7 son siempre irreducibles, incluso en una situación más general.

PROPOSICIÓN 9.8. *Sea* S *un monoide y* $a \in S$. *Entonces* $S \setminus \mathcal{B}(a)$ *es un ideal irreducible de* S.

DEMOSTRACIÓN. Ya sabemos que $S \setminus \mathcal{B}(a)$ es un ideal de S. El que además es irreducible se deduce del hecho de que todo ideal que contiene propiamente a $S \setminus \mathcal{B}(a)$ debe contener a a. □

El lector familiarizado con la teoría de ideales de anillos puede encontrar el siguiente resultado y su demostración particularmente extraños.

LEMA 9.9. *Sea I un ideal de un monoide S. Las siguientes condiciones son equivalentes.*

(1) I es irreducible.
(2) Para todo $a,b \in S$, si $(a+S)\cap(b+S) \subseteq I$, entonces o bien $a+S \subseteq I$ ó $b+S \subseteq I$.

DEMOSTRACIÓN. *(1) implica (2).* Supongamos que $(a+S)\cap(b+S) \subseteq I$, $a+S \not\subseteq I$ y $b+S \not\subseteq I$. Entonces $A = I \cup (a+S)$ y $B = I \cup (b+S)$ son dos ideales que contienen estrictamente a I. Además, $A \cap B = I \cup ((a+S)\cap(b+S)) = I$, lo cual implica que I no es irreducible.

(2) implica (1). Supongamos que I no es irreducible. Entonces $I = A \cap B$ con A, B ideales de S conteniendo a I propiamente. Tomemos $a \in A \setminus I$ y $b \in B \setminus I$. Entonces $(a+S)\cap(b+S) \subseteq A \cap B = I$, pero ni $a+S \subseteq I$ ni $b+S \subseteq I$. □

PROPOSICIÓN 9.10. *Sea S un monoide e $\{I_n\}_{n\in\mathbb{N}}$ una sucesión de ideales irreducibles de S tales que $I_{n+1} \subseteq I_n$ para todo $n \in \mathbb{N}$. Entonces $\bigcap_{n\in\mathbb{N}} I_n$ es un ideal irreducible de S.*

DEMOSTRACIÓN. En vista del Lema 9.9, es suficiente probar que si $(a+S)\cap(b+S) \subseteq \bigcap_{n\in\mathbb{N}} I_n$, entonces ó bien $a+S \subseteq \bigcap_{n\in\mathbb{N}} I_n$ ó $b+S \subseteq \bigcap_{n\in\mathbb{N}} I_n$. Ya que $(a+S)\cap(b+S) \subseteq \bigcap_{n\in\mathbb{N}} I_n$, entonces $(a+S)\cap(b+S) \subseteq I_n$ para todo $n \in \mathbb{N}$. En consecuencia, por el Lema 9.9, ó $a+S \subseteq I_n$ ó $b+S \subseteq I_n$. Si $a+S \subseteq I_n$ para todo n, entonces hemos terminado. Supongamos por el contrario que para algún $k \in \mathbb{N}$ tenemos que $a+S \not\subseteq I_k$ (con k el menor entero no negativo cumpliendo esta condición), entonces como $\{I_n\}_{n\in\mathbb{N}}$ es una sucesión decreciente, obtenemos que $a+S \not\subseteq I_{k+l}$ para todo $l \in \mathbb{N}$. Usando el Lema 9.9, llegamos a que $b+S \subseteq I_{k+l}$ para todo $l \in \mathbb{N}$ y así $b+S \subseteq I_j$ para todo $j \in \{0,\ldots,k-1\}$. Por tanto $b+S \subseteq \bigcap_{n\in\mathbb{N}} I_n$. □

4. Ideales irreducibles y descomposición en irreducibles

En esta sección probaremos que en el caso finitamente generado los ideales irreducibles pueden expresarse de la forma en la que aparecen en la Proposición 9.10. En primer lugar damos una generalización de la descomposición en irreducibles estudiada para $\mathbb{N}^p$ (Corolarios 9.4 y 9.7). Para ello hemos de recordar que dado $S = \langle s_1,\ldots,s_p\rangle$ con $S \cong \mathbb{N}^p/\sigma$, sabemos que existe una aplicación $\varphi : \mathbb{N}^p \to S$ definida de la forma $\varphi(x_1,\ldots,x_p) = \sum_{i=1}^p x_i s_i$. Dado un ideal I de S, definimos $\mathrm{E}(I)$ como el conjunto $\varphi^{-1}(I)$, que es un ideal de $\mathbb{N}^p$.

TEOREMA 9.11. *Sea I un ideal del monoide $S = \langle s_1,\ldots,s_p\rangle$. Supongamos que $\mathrm{E}(I) = \bigcap_{i=1}^r J_i$ con J_i un ideal irreducible de $\mathbb{N}^p$ para todo $i \in \{1,\ldots,r\}$ (ver Corolario 9.4) y tales que $J_i = \bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(x_n^i))$ para alguna sucesión ascendente $\{x_n^i\}_{n\in\mathbb{N}} \subseteq \mathbb{N}^p$ (ver Corolario 9.7). Entonces*

$$I = \bigcap_{i=1}^{r} \Big(\bigcap_{n\in\mathbb{N}} (S \setminus \mathcal{B}(\varphi(x_n^i))) \Big).$$

DEMOSTRACIÓN. Sea $K = \bigcap_{i=1}^{r}(\bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(\varphi(x_n^i))))$. Usando las Proposiciones 9.7 y 9.9 y el que $\{\varphi(x_n)\}$ es una sucesión ascendente, K es intersección de irreducibles de la forma $\bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(\varphi(x_n^i)))$. Consideremos $s \in I$ y supongamos que existen i,k tales que $s \notin S \setminus \mathcal{B}(\varphi(x_k^i))$. Entonces $s \in \mathcal{B}(\varphi(x_k^i))$, ya que en otro caso existiría $t \in S$ tal que $s+t = \varphi(x_k^i)$. Al ser φ es sobreyectiva, $s = \varphi(a)$ y $t = \varphi(b)$ para algún $a,b \in \mathbb{N}^p$. En consecuencia $\varphi(a+b) = \varphi(x_k^i)$. Claramente, $x_k^i \notin \mathrm{E}(I)$, de donde $a+b \notin \mathrm{E}(I)$, lo cual hace que $a \notin \mathrm{E}(I)$, contradiciendo que $\varphi(a) = s \in I$. Por tanto $s \in S \setminus \mathcal{B}(\varphi(x_k^i))$ para todo i,k y así $I \subseteq K$.

Supongamos ahora que $s \notin I$ y tomemos $a \in \mathbb{N}^p$ tal que $\varphi(a) = s$. Esto implica que $a \notin \mathrm{E}(I)$ y que existen i,k tales que $a \notin S \setminus \mathcal{B}(x_k^i)$, esto es, $a \in \mathcal{B}(x_k^i)$. En consecuencia $x_k^i = a+b$ para algún $b \in \mathbb{N}^p$ y por tanto $\varphi(a)+\varphi(b) = \varphi(x_k^i)$, lo que hace que $s \in \mathcal{B}(\varphi(x_k^i))$. Por esta razón $s \notin K$, llegando a que $K \subseteq I$. □

Obsérvese que la Proposición 9.10 nos dice que la descomposición de I dada en la Teorema 9.11 es justamente una descomposición de este ideal en irreducibles de S. Como consecuencia de este resultado podemos describir todo ideal irreducible de un monoide S tal y como aparece a continuación.

COROLARIO 9.12. *Sea S un monoide finitamente generado. Las siguientes condiciones son equivalentes.*

(1) I es un ideal irreducible de S.

(2) Existe una sucesión $\{s_n\}_{n\in\mathbb{N}} \subset S$ tal que $I = \bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(s_n))$ y $s_n \leq s_{n+1}$ para todo $n \in \mathbb{N}$.

DEMOSTRACIÓN. *(1) implica (2).* Usando el Teorema 9.11, el ideal I puede expresarse como

$$I = \bigcap_{i=1}^{r}\Big(\bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(\varphi(x_n^i)))\Big).$$

Ya que I es irreducible, existe $i \in \{1,\ldots,r\}$ tal que $I = \bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(\varphi(x_n^i)))$. Además como $x_n^i \leq x_{n+1}^i$ tenemos que $\varphi(x_n^i) \leq \varphi(x_{n+1}^i)$. Tomando $s_n = \varphi(x_n^i)$ obtenemos el resultado deseado.

(2) implica (1). Por la Proposición 9.8, los ideales $S \setminus \mathcal{B}(s_n)$ son irreducibles. Usando que $s_n \leq s_{n+1}$, se tiene que $\mathcal{B}(s_n) \subseteq \mathcal{B}(s_{n+1})$, por lo que $S \setminus \mathcal{B}(s_{n+1}) \subseteq S \setminus \mathcal{B}(s_n)$. La Proposición 9.9 nos dice que $\bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(s_n))$ es un ideal irreducible de S. □

Dado un ideal I de un monoide finitamente generado S, para calcular una descomposición de I en irreducibles, hemos de encontrar en primer lugar $\mathrm{E}(I)$. Téngase en cuenta que la descomposición de I en S está relacionada con la descomposición de $\mathrm{E}(I)$ en $\mathbb{N}^p$. En particular, si $\mathrm{E}(I)$ es irreducible también lo es I. Sin embargo, como el siguiente ejemplo prueba, puede suceder que I sea un irreducible de S, pero $\mathrm{E}(I)$ no lo sea en $\mathbb{N}^p$.

EJEMPLO 9.13. Sea $S = \mathbb{N}^2/\sigma$, donde σ es la congruencia de $\mathbb{N}^2$ generada por $\{((2,0),(0,3))\}$ (en esta situación φ es la proyección natural: $\varphi(x) = [x]_\sigma$). Tomemos

$I = \{[(1,2)]_\sigma\} + S$. Entonces $\mathrm{E}(I) = \{(3,0),(1,2),(0,5)\} + \mathbb{N}^2$ (en la siguiente sección veremos como se puede calcular $\mathrm{E}(I)$), el cual es el ideal del ejemplo 9.5. En consecuencia

$$\mathrm{E}(I) = (\{(1,0),(0,5)\} + \mathbb{N}^2) \cap (\{(3,0),(0,2)\} + \mathbb{N}^2)$$

y por la Proposición 9.6, obtenemos que

$$\mathrm{E}(I) = (\mathbb{N}^2 \setminus \mathcal{B}((0,4))) \cap (\mathbb{N}^2 \setminus \mathcal{B}((2,1))).$$

El Teorema 9.11 nos dice que

$$I = (S \setminus \mathcal{B}([(0,4)]_\sigma)) \cap (S \setminus \mathcal{B}([(2,1)]_\sigma))$$

(con $x_n^1 = (0,4)$ y $x_n^2 = (2,1)$ para todo $n \in \mathbb{N}$) y ya que $(0,4)\sigma(2,1)$ tenemos que $I = S \setminus \mathcal{B}([(0,4)]_\sigma)$. Por tanto, usando la Proposición 9.8, deducimos que I es un ideal irreducible de S. □

5. Algunos aspectos computacionales

En esta sección describimos un método para calcular la descomposición en irreducibles de un ideal I de un monoide finitamente generado S (conocida una presentación del monoide y un sistema de generadores del ideal). El procedimiento consiste en hacer efectiva la expresión obtenida en el Teorema 9.11. Lo primero que haremos será calcular el conjunto $\mathrm{E}(I)$ para después centrarnos en el cálculo de los ideales $\bigcap_{n\in\mathbb{N}}(S \setminus \mathcal{B}(\varphi(x_n^i))) = S \setminus (\cup_{n\in\mathbb{N}}\mathcal{B}(\varphi(x_n^i)))$.

Sea $S \cong \mathbb{N}^p/\sigma$ y tomemos ρ un sistema de generadores de σ. Supongamos que el ideal I está generado por $\{[\lambda_1]_\sigma,\ldots,[\lambda_r]_\sigma\}$ y definamos ahora la congruencia de Rees $\sigma_{\mathcal{R}_I}$ a partir de los λ_i y de ρ (ver Capítulo 1) como la congruencia generada por

$$\rho_{\mathcal{R}_I} = \{(\lambda_1,\lambda_2),\ldots,(\lambda_1,\lambda_r),(\lambda_1,\lambda_1+e_1),\ldots,(\lambda_1,\lambda_1+e_p)\} \cup \rho.$$

Sea κ un sistema canónico de $\sigma_{\mathcal{R}_I}$ con respecto a $\preceq$ un orden lineal admisible dado (recuérdese que $S/\mathcal{R}_I$ es isomorfo a $\mathbb{N}^p/\sigma_{\mathcal{R}_I}$).

Téngase en cuenta que en general $\mathrm{E}(I)$ contiene al ideal de $\mathbb{N}^p$ generado por $\{\lambda_1,\ldots,\lambda_r\}$.

Los siguientes dos resultados son la clave para el cálculo de $\mathrm{E}(I)$. Ya que $\mathrm{E}(I)$ es un ideal de $\mathbb{N}^p$, es suficiente conocer el conjunto $\mathrm{Minimales}_{\leq}\mathrm{E}(I)$.

LEMA 9.14. *Sean S, I, ρ, σ, $\rho_{\mathcal{R}_I}$, $\sigma_{\mathcal{R}_I}$ y κ tal y como acabamos de definirlos. Si $x \in \mathrm{E}(I)$, $x-\beta \in \mathbb{N}^p$ y $x-\beta+\alpha \in \mathrm{Minimales}_{\leq}\mathrm{E}(I)$ para algún $(\alpha,\beta) \in \kappa$, entonces $x = \mu \vee \beta$, para algún $\mu \in \mathrm{Minimales}_{\leq}\mathrm{E}(I)$.*

DEMOSTRACIÓN. Tenemos que $x \in \mathrm{E}(I)$, por tanto existe $\mu \in \mathrm{Minimales}_{\leq}\mathrm{E}(I)$ tal que $x-\mu \in \mathbb{N}^p$. Por hipótesis, $x-\beta$ pertenece también a $\mathbb{N}^p$ y por tanto $x = (\mu \vee \beta)+z$ para algún $z \in \mathbb{N}^p$. Como $\mu \in \mathrm{E}(I)$ y $\mathrm{E}(I)$ es un ideal de $\mathbb{N}^p$, obtenemos que $\mu \vee \beta \in \mathrm{E}(I)$. El que $(\alpha,\beta) \in \sigma_{\mathcal{R}_I}$ hace que $((\mu \vee \beta)-\beta+\alpha, \mu \vee \beta) \in \sigma_{\mathcal{R}_I}$, lo cual implica que $[(\mu \vee \beta)-\beta+\alpha]_\sigma \in I$. Por tanto $(\mu \vee \beta)-\beta+\alpha \in \mathrm{E}(I)$. Finalmente, $x-\beta+\alpha = ((\mu \vee \beta)-\beta+\alpha)+z \in \mathrm{Minimales}_{\leq}\mathrm{E}(I)$, lo cual junto con que $(\mu \vee \beta)-\beta+\alpha \in \mathrm{E}(I)$ hace que $z = 0$. □

PROPOSICIÓN 9.15. *Sean S, I,* ρ, σ, $\rho_{\mathcal{R}_I}$, $\sigma_{\mathcal{R}_I}$, κ *y* $\preceq$ *definidos como antes. Si el conjunto* $\text{Minimales}_{\leq}\text{E}(I) = \{\mu_1 \prec \ldots \prec \mu_s\}$, *entonces* $\mu_{k+1} = (\mu_i \vee \beta) - \beta + \alpha$, *para algún* $(\alpha, \beta) \in \kappa$ *e* $i \in \{1, \ldots, k\}$.

DEMOSTRACIÓN. Como $\mu_{k+1} \in \text{E}(I)$, tenemos que $\text{NF}_\kappa(\mu_{k+1}) = \text{NF}_\kappa(\mu_1) = \mu_1$. Por tanto, existe $(\alpha, \beta) \in \kappa$ tal que $\mu_{k+1} - \alpha \in \mathbb{N}^p$. Tomemos $\mu_{k+1} - \alpha + \beta = x \in \mathbb{N}^p$. Como $(\alpha, \beta)\sigma_{\mathcal{R}_I}$ y $\mu_{k+1} - \alpha \in \mathbb{N}^p$, obtenemos que $[x]_{\sigma_{\mathcal{R}_I}} = [\mu_{k+1} - \alpha + \beta]_{\sigma_{\mathcal{R}_I}} = [\mu_{k+1}]_{\sigma_{\mathcal{R}_I}}$, lo cual hace que $[x]_\sigma \in I$, o en otras palabras, $x \in \text{E}(I)$. Aplicando ahora el Lema 9.14 a x, tenemos que $x = (\mu_i \vee \beta)$ para algún $i \in \{1, \ldots, s\}$. Además

$$\mu_i \preceq \mu_i \vee \beta \prec (\mu_i \vee \beta) - \beta + \alpha = \mu_{k+1},$$

lo cual implica que $i < k+1$. □

Con estos dos resultados damos el siguiente algoritmo para el cálculo de $\text{E}(I)$.

ALGORITMO 9.16. Sean $S, I, \rho, \sigma, \rho_{\mathcal{R}_I}, \sigma_{\mathcal{R}_I}, \kappa$ y $\preceq$ definidos como antes.

ENTRADA: El conjunto $\{[\lambda_1]_\sigma, \ldots, [\lambda_r]_\sigma\}$ (el sistema de generadores de I) y un sistema canónico de generadores $\kappa = \{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$ de la congruencia $\sigma_{\mathcal{R}_I}$ sobre $\mathbb{N}^p$ con respecto a un orden lineal admisible$\preceq$.

SALIDA: El conjunto $\text{Minimales}_{\leq}\text{E}(I)$.

(1) Calcular $\mu_1 = \text{NF}_\kappa(\lambda_1)$.
(2) Tomemos $A = \{\mu_1\}$.
(3) Calcular $B = \{(a \vee \beta_j) - \beta_j + \alpha_j \mid a \in A, j \in \{1, \ldots, t\}\}$.
(4) Calcular $C = B \cap \text{Minimales}_{\leq}\{x \in \mathbb{N}^p \mid \text{NF}_\kappa(x) = \mu_1\}$ (nótese que un elemento $b \in B$ está en $\text{Minimales}_{\leq}\{x \in \mathbb{N}^p \mid \text{NF}_\kappa(x) = \mu_1\}$ si y sólo si para todo $y < b$, $\text{NF}_\kappa(y) \neq \mu_1$).
(5) Si $C \subseteq A$, entonces devolver A.
(6) $A := A \cup C$; ir a paso 3.

□

Una vez conocido cómo calcular $\text{E}(I)$, lo siguiente que nos dice el Teorema 9.11 que hemos de hacer es encontrar un modo de calcular los ideales la forma $S \setminus (\cup_{n \in \mathbb{N}} \mathcal{B}(\varphi(x_n))) = \mathbb{N}^p/\sigma \setminus (\cup_{n \in \mathbb{N}} \mathcal{B}([x_n]_\sigma))$. En primer lugar veamos como son los conjutos $\mathcal{B}([x]_\sigma)$.

LEMA 9.17. *Sea* $x \in \mathbb{N}^p$. *Entonces*

$$\mathcal{B}([x]_\sigma) = \{[a]_\sigma \mid \text{ existe } b \in [x]_\sigma \text{ tal que } a \leq b\}.$$

DEMOSTRACIÓN. Supongamos que $[a]_\sigma \in \mathcal{B}([x]_\sigma)$. Entonces $[a]_\sigma \leq [x]_\sigma$, de donde $[a]_\sigma + [c]_\sigma = [x]_\sigma$ para algún $c \in \mathbb{N}^p$. En consecuencia $a + c \in [x]_\sigma$ y claramente $a \leq a + c$.

Si $a \leq b$ y $b \in [x]_\sigma$, entonces $[a]_\sigma \leq [b]_\sigma = [x]_\sigma$. □

A continuación damos algunas definiciones y resultados auxiliares necesarios para simplificar notación.

Dado $n \in \mathbb{N}$, sean π_i y Π_i, $1 \leq i \leq n$, las aplicaciones

$$\pi_i : (\mathbb{N} \cup \{\infty\})^n \to (\mathbb{N} \cup \{\infty\}),\ \pi_i(x_1, \ldots, x_n) = x_i,$$

$$\Pi_i : (\mathbb{N} \cup \{\infty\})^n \to (\mathbb{N} \cup \{\infty\})^{n-1}, \Pi_i(x_1, \ldots, x_n) = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).$$

Para una congruencia dada sobre $\mathbb{N}^p$, sea $\Pi_i(\sigma)$ la congruencia sobre $\mathbb{N}^{p-1}$ definida por

$$(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_p)\Pi_i(\sigma)(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_p)$$

si existen $d, d' \in \mathbb{N}$ tales que

$$(a_1, \ldots, a_{i-1}, d, a_{i+1}, \ldots, a_p)\sigma(b_1, \ldots, b_{i-1}, d', b_{i+1}, \ldots, b_p).$$

Puede probarse que si $\{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$ es un sistema de generadores de σ, entonces $\{(\Pi_i(\alpha_1), \Pi_i(\beta_1)), \ldots, (\Pi_i(\alpha_t), \Pi_i(\beta_t))\}$ es un sistema de generadores de $\Pi_i(\sigma)$ (véase **[65]** ó **[72]**).

Dada una sucesión creciente $\{x_n\}_{n\in\mathbb{N}} \subseteq \mathbb{N}^p$, cada una de las p sucesiones $\{\pi_i(x_n)\}_{n\in\mathbb{N}}$, $1 \leq i \leq p$ son sucesiones crecientes de $\mathbb{N}$ que tienen límite $z_i \in \mathbb{N} \cup \{\infty\}$. El límite de la sucesión $\{x_n\}_{n\in\mathbb{N}}$ es el elemento de $(\mathbb{N} \cup \{\infty\})^p$ con coordenadas $(z_1, \ldots, z_p)$.

LEMA 9.18. *Supongamos que $\{x_n\}_{n\in\mathbb{N}}$ y $\{x'_n\}_{n\in\mathbb{N}}$ tienen el mismo límite. Entonces*

$$\bigcup_{n\in\mathbb{N}} \mathcal{B}([x_n]_\sigma) = \bigcup_{n\in\mathbb{N}} \mathcal{B}([x'_n]_\sigma).$$

DEMOSTRACIÓN. Supongamos que $[x]_\sigma \in \cup_{n\in\mathbb{N}} \mathcal{B}([x_n]_\sigma)$. Entonces existe $k \in \mathbb{N}$ tal que $[x]_\sigma \in \mathcal{B}([x_k]_\sigma)$. En consecuencia $[a]_\sigma + [b]_\sigma = [x_k]_\sigma$ para algún $b \in \mathbb{N}^p$. Ya que tanto $\{x_n\}_{n\in\mathbb{N}}$ como $\{x'_n\}_{n\in\mathbb{N}}$ tienen el mismo límite, existe $m \in \mathbb{N}$ tal que $x_k \leq x'_m$. Por tanto, $[a]_\sigma \leq [x_k]_\sigma \leq [x'_n]_\sigma$, lo cual hace que $[a]_\sigma \in \cup_{n\in\mathbb{N}} \mathcal{B}([x'_n]_\sigma)$. La otra inclusión se prueba de la misma forma. □

Si $\{x_n\}_{n\in\mathbb{N}} \subseteq \mathbb{N}^p$ es una sucesión con límite $z \in (\mathbb{N} \cup \{\infty\})^p$, escribiremos $\mathcal{B}([z]_\sigma)$ en vez de $\cup_{n\in\mathbb{N}} \mathcal{B}([x_n]_\sigma)$. Usando esta notación, el Teorema 9.11 nos diría que asociado a un ideal I de $\mathbb{N}^p/\sigma$ existen $z^1, \ldots, z^r \in (\mathbb{N} \cup \{\infty\})^p$ tales que

$$I = \bigcap_{i=1}^{r} (\mathbb{N}^p/\sigma \setminus \mathcal{B}([z^i]_\sigma).$$

Obsérvese que las sucesiones $\{x^i_n\}_{n\in\mathbb{N}}$ que aparecen en el Teorema 9.11 no son arbitrarias, provienen de la descomposición en irreducibles de $\mathrm{E}(I)$ obtenida del Corolario 9.4 y la Proposición 9.6. En consecuencia una vez calculado en conjunto $\mathrm{E}(I)$, los elementos z^i se obtienen fácilmente.

Todo lo anterior hace que el siguiente paso para el cálculo de una descomposición en irreducibles sea la obtención de $\mathcal{B}([z]_\sigma)$, con z el límite de un sucesión ascendente de $\mathbb{N}^p$. Una de las dificultades que podemos encontrar a la hora de realizar este cálculo es que incluso si $z \in \mathbb{N}^p$ puede ocurrir que $[z]_\sigma$ no sea finito y por ello el Lema 9.17 no se pueda aplicar de manera fácil e inmediata. Otro de los problemas con que nos tropezamos es la duda de sobre qué hacer cuando z tiene alguna coordenada igual a

infinito. El hecho es que estos dos problemas están de alguna forma conectados tal y como veremos a continuación.

Por el Lema 9.17, parece razonable que una de las cosas que tenemos de hacer es encontrar un método para calcular la σ-clase de un elemento $a \in \mathbb{N}^p$. Recordemos que ρ es un sistema canónico de generadores con respecto a un orden lineal admisible $\preceq$ de $\mathbb{N}^p$ dado. Supongamos que $\rho = \{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$. Sabemos decidir si un elemento $b \in \mathbb{N}^p$ pertenece o no a $[a]_\sigma$; simplemente hemos de calcular $\mathrm{NF}_\rho(a)$ y $\mathrm{NF}_\rho(b)$, y ver si coinciden. La definición de NF_ρ nos dice que esto es equivalente a que exista una sucesión $i_1, \ldots, i_q$ de elementos de $\{1, \ldots, t\}$, no es necesario que todos sean diferentes, tales que

(1) $b + \sum_{k=1}^{q} (-\alpha_{i_k} + \beta_{i_k}) = \mathrm{NF}_\rho(a)$,
(2) $b + \sum_{k=1}^{r} (-\alpha_{i_k} + \beta_{i_k}) - \alpha_{i_{r+1}} \in \mathbb{N}^p$ para todo $r \in \{0, \ldots, q-1\}$.

Esto equivale a decir que b reescribe a $\mathrm{NF}_\rho(a)$ mediante ρ. Fijándonos en este proceso hacia atrás, obtenemos el siguiente resultado.

LEMA 9.19. *El elemento $b \in \mathbb{N}^p$ pertenece a $[a]_\sigma$ si y sólo si existe una sucesión $(\alpha_{i_1}, \beta_{i_1}), \ldots, (\alpha_{i_q}, \beta_{i_q})$ de elementos de ρ tal que*

(1) $\mathrm{NF}_\rho(a) + \sum_{k=1}^{q} (-\beta_{i_k} + \alpha_{i_k}) = b$,
(2) $\mathrm{NF}_\rho(a) + \sum_{k=1}^{r} (-\beta_{i_k} + \alpha_{i_k}) - \beta_{i_{r+1}} \in \mathbb{N}^p$ *para todo* $r \in \{0, \ldots, q-1\}$.

Este resultado nos proporciona un método para obtener recurrentemente todos los elementos de $[a]_\sigma$. La implementación del mismo se tiene en el siguiente algoritmo.

ALGORITMO 9.20. Sean S, I, ρ, σ, $\rho_{\mathcal{R}_I}$, $\sigma_{\mathcal{R}_I}$, κ y $\preceq$ como antes.
Entrada: ρ y $a \in \mathbb{N}^p$.
Salida: $[a]_\sigma$ caso de que tenga un número finito de elementos, en otro caso el algoritmo nunca para y construimos recurrentemente en A el conjunto $[a]_\sigma$.

(1) Calcular $\mathrm{NF}_\rho(a)$.
(2) Sea $A := B := \{\mathrm{NF}_\rho(a)\}$.
(3) Mientras $B \neq \emptyset$
    elegir $u \in B$,
    sea $B := (B \setminus \{u\}) \cup \{u - \beta_j + \alpha_j \mid u - \beta_j \in \mathbb{N}^p, j \in \{1, \ldots, t\}\}$,
    sea $A := A \cup \{u - \beta_j + \alpha_j \mid u - \beta_j \in \mathbb{N}^p, j \in \{1, \ldots, t\}\}$.
(4) Devolver A.

□

El siguiente resultado nos da la clave para saber cuándo la clase de un elemento es o no finita. Nótese que en caso de que $[a]_\sigma$ sea finito, $[a]_\sigma = \mathrm{Minimales}_{\leq}[a]_\sigma = \mathrm{Maximales}_{\leq}[a]_\sigma$.

LEMA 9.21. *El conjunto $[a]_\sigma$ tiene un número finito de elementos si y sólo si en algún paso del bucle* Mientras *del Algoritmo 9.20 obtenemos que $\mathrm{NF}_\rho(a) + x \in A$ para algún $x \in \mathbb{N}^p \setminus \{0\}$.*

DEMOSTRACIÓN. *Necesidad.* Si $[a]_\sigma$ no tiene un número finito de elementos, entonces aplicando el Lema de Dickson, existe $b \in [a]_\sigma$ y $x \in \mathbb{N}^p \setminus \{0\}$ tal que

$b+x \in [a]_\sigma$. En consecuencia, $\mathrm{NF}_\rho(a)\sigma b$ y $(\mathrm{NF}_\rho(a)+x)\sigma(b+x)$, lo cual implica que $\mathrm{NF}_\rho(a)\sigma\mathrm{NF}_\rho(a)+x$. Ya que el Algoritmo 9.20 calcula el conjunto $[a]_\sigma$ recurrentemente, debe suceder que $\mathrm{NF}_\rho(a)+x \in A$ en algún paso.

Suficiencia. Claramente $\mathrm{NF}_\rho(a)+kx \in [a]_\sigma$ para todo $k \in \mathbb{N}$ y por tanto $[a]_\sigma$ tiene un número no finito de elementos. □

Con este resultado podemos modificar el Algoritmo 9.20 y obtener un nuevo algoritmo que nos devuelva $[a]_\sigma$, caso de que este conjunto tenga un número finito de elementos y que en caso contrario nos diga que $[a]_\sigma$ tiene un número no finito de elementos. Para ello basta con añadir la siguiente línea al bucle *Mientras*:

> Comprobar si para algún elemento $x \in A$, el elemento $x - \mathrm{NF}_\rho(a) \in \mathbb{N}^p \setminus \{0\}$. Si es así, devolver "El conjunto $[a]_\sigma$ tiene un número no finito de elementos".

LEMA 9.22. *Supongamos que $\{x_n\}_{n\in\mathbb{N}}$ es una sucesión creciente de elementos de $\mathbb{N}^p$ con límite $z=(z_1,\ldots,z_p) \in \mathbb{N}^p$ y tal que existe $x \in \mathbb{N}^p \setminus \{0\}$ verificando que $z+x \in [z]_\sigma$. Supongamos además que $\mathrm{Supp}(x)=\{1,\ldots,r\}$ y tomemos $y_n = x_n + n(e_1+\cdots+e_r)$ para todo $n \in \mathbb{N}$. Entonces*

$$\bigcup_{n\in\mathbb{N}} \mathcal{B}([x_n]_\sigma) = \bigcup_{n\in\mathbb{N}} \mathcal{B}([y_n]_\sigma),$$

ó equivalentemente, si $z'=(\infty,\ldots,\infty,z_{r+1},\ldots,z_p)$, entonces $\mathcal{B}([z]_\sigma)=\mathcal{B}([z']_\sigma)$.

DEMOSTRACIÓN. En primer lugar téngase en cuenta que ya que $z+x \in [z]_\sigma$, entonces $[z+nx]_\sigma = [z]_\sigma$ para todo $n \in \mathbb{N}$. A partir de la definición de y_n, tenemos que $\mathcal{B}([x_n]_\sigma) \subseteq \mathcal{B}([y_n]_\sigma)$, por lo que $\bigcup_{n\in\mathbb{N}} \mathcal{B}([x_n]_\sigma) \subseteq \bigcup_{n\in\mathbb{N}} \mathcal{B}([y_n]_\sigma)$. Tomemos $[a]_\sigma \in \mathcal{B}([y_n]_\sigma)$, entonces $[a]_\sigma \leq [y_n]_\sigma = [x_n+n(e_1+\cdots+e_r)]_\sigma$. Lo cual junto con que $x_n \leq z$ hace que $x_n+n(e_1+\cdots+e_r) \leq z+n(e_1+\cdots+e_r)$. Tomando ahora σ-clases, obtenemos que $[x_n+n(e_1+\cdots+e_r)]_\sigma \leq [z+n(e_1+\cdots+e_r)]_\sigma$. Además, $z+n(e_1+\cdots+e_r) \leq z+nx$. Esto nos lleva a que $[a]_\sigma \leq [x_n+n(e_1+\cdots+e_r)]_\sigma \leq [z+n(e_1+\cdots+e_r)]_\sigma \leq [z+nx]_\sigma$, por tanto $[a]_\sigma \leq [z]_\sigma$ y finalmente $[a]_\sigma \in \mathcal{B}([z]_\sigma) = \bigcup_{n\in\mathbb{N}} \mathcal{B}([x_n]_\sigma)$. □

Este resultado nos dice que caso de que $z \in \mathbb{N}^p$ y la σ-clase de z sea infinita, entonces podemos trasladar el problema a otro donde el límite ya no pertenece a $\mathbb{N}^p$. A continuación mostramos como olvidarnos de aquellas coordenadas que son igual a infinito en los límites de las sucesiones $\{x_n\}_{n\in\mathbb{N}}$.

LEMA 9.23. *Supongamos que $\{x_n\}_{n\in\mathbb{N}^p}$ es una sucesión creciente de elementos de $\mathbb{N}^p$ con límite $z=(z_1,\ldots,z_p) \in (\mathbb{N}\cup\{\infty\})^p$ y $z_1=\infty$. Entonces $[a]_\sigma \in \mathcal{B}([z]_\sigma)$ si y sólo si $[\Pi_1(a)]_{\Pi_1(\sigma)} \in \mathcal{B}([\Pi_1(z)]_{\Pi_1(\sigma)})$.*

DEMOSTRACIÓN. Supongamos que $[a]_\sigma \in \cup_{n\in\mathbb{N}}\mathcal{B}([x_n]_\sigma)$. Entonces existen $k \in \mathbb{N}$ y $c \in \mathbb{N}^p$ tales que $[a+c]_\sigma = [x_k]_\sigma$. Por consiguiente $[\Pi_1(a)+\Pi_1(c)]_{\Pi_1(\sigma)} = [\Pi_1(x_k)]_{\Pi_1(\sigma)}$.

Supongamos ahora que $[\Pi_1(a)]_{\Pi_1(\sigma)} \in \bigcup_{n\in\mathbb{N}} \mathcal{B}([\Pi_1(x_n)]_{\Pi_1(\sigma)})$. Esto implica que existe $k \in \mathbb{N}$ y $(c_1,\ldots,c_p) \in \mathbb{N}^{p-1}$ tal que $\Pi_1(a)+(c_2,\ldots,c_p)\Pi_1(\sigma)\Pi_1(x_k)$. Tomemos $d,d' \in \mathbb{N}$ tales que $de_1+\Pi_1(a)+(0,c_2,\ldots,c_p)\sigma d'e_1+\Pi_1(x_k)$. Teniendo en cuenta que podemos elegir $d \geq \pi_1(a)$, tenemos que existe $c_1 \in \mathbb{N}$ verificando que $\pi_1(a)+c_1 = d$. Como $z_1 = \infty$, podemos encontrar $m \in \mathbb{N}$ tal que $\pi_1(x_m) \geq d'$. Finalmente, llegamos a que $a+(c_1,\ldots,c_p)\sigma d'e_1+\Pi(x_k) \leq x_m$. □

Usando este último resultado para $p = 1$, obtenemos que si $z_1 = \infty$, entonces $\mathcal{B}([z]_\sigma)$ coincide con $\mathbb{N}/\sigma$. Con todo esto, ya estamos preparados para dar un algoritmo que calcule el conjunto Maximales$_{\leq}$(E($\mathcal{B}([z]_\sigma)$)) y describir así el conjunto $\mathcal{B}([z]_\sigma)$ para un z límite de una sucesión creciente de $\mathbb{N}^p$.

ALGORITMO 9.24. Sean S, I, ρ, σ, $\rho_{\mathcal{R}_I}$, $\sigma_{\mathcal{R}_I}$, κ y $\preceq$ definidos como antes y tomemos $z \in (\mathbb{N}\cup\{\infty\})^p$, el límite de una sucesión creciente de $\mathbb{N}^p$. Este algoritmo nos devuelve el conjunto Maximales$_{\leq}$(E($\mathcal{B}([z]_\sigma)$)).

(1) Si $z \in \mathbb{N}^p$, aplicar el Algoritmo 9.20 a z. Si $[z]_\sigma$ es finito, entonces devolver $[z]_\sigma$. En otro caso proceder como en el Lema 9.22, esto es, si $z+x \in [z]_\sigma$ (el elemento x está determinado en el Algoritmo 9.20), entonces hacer todas las coordenadas de z que están en Supp(x) iguales a ∞.
(2) Tomar el más pequeño $i \in \{1,\ldots,p\}$ tal que $z_i = \infty$. Calcular $\Pi_i(z)$ (y $\Pi(\sigma)$, calcular de nuevo un sistema canónico de generadores para $\Pi(\sigma)$ para usarlo en el Algoritmo 9.20) y aplicar este algoritmo con entrada $\Pi_i(z)$. Si A es la salida del algoritmo entonces delvover

$$\{(a_1,\ldots,a_{i-1},\infty,a_{i+1},\ldots,a_p) \mid (a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_p) \in A\}.$$

□

Una vez conocido el modo de calcular $\mathcal{B}([z]_\sigma) = \cup_{n\in\mathbb{N}}\mathcal{B}([x_n]_\sigma)$, estamos interesados en calcular cuales son las expresiones de su ideal asociado, esto es E($\mathbb{N}^p/\sigma \setminus \mathcal{B}([z]_\sigma)$) (éste conjunto coincide con $\mathbb{N}^p \setminus$ E($\mathcal{B}([z]_\sigma)$)). Damos a continuación un método para poder describir este conjunto. Como el conjunto E($\mathbb{N}^p/\sigma \setminus \mathcal{B}([z]_\sigma)$) es un ideal de $\mathbb{N}^p$, parar determinar dicho conjunto basta con dar un sistema de generadores suyo. Supongamos que $\{m_1,\ldots,m_r\}$ son los elementos maximales del conjunto E($\mathcal{B}([z]_\sigma)$). Un elemento $(a_1,\ldots,a_p)$ pertenece a $\mathbb{N}^p \setminus$E($\mathcal{B}([z]_\sigma)$) si y sólo si pertenece al conjunto $\bigcap_{i=1}^r \mathbb{N}^p \setminus \{x \in \mathbb{N}^p \mid x \not\leq m_i\}$. En el Lema 9.1 se muestra como realizar la intersección de dos ideales de $\mathbb{N}^p$. En consecuencia sólo nos queda explicar cómo para un elemento dado $k = (k_1,\ldots,k_p) \in (\mathbb{N}\cup\{\infty\})^p$ es posible calcular el conjunto de elementos minimales de $\mathbb{N}^p \setminus \{x \in \mathbb{N}^p \mid x \not\leq k\}$. Si $x \not\leq k$, entonces existe $i \in \{1,\ldots,p\}$ tal que $x_i > k_i$ y por tanto $k_i \neq \infty$. Así obtenemos que

$$\mathbb{N}^p \setminus \{x \in \mathbb{N}^p \mid x \not\leq k\} = \bigcup_{\substack{i=1 \\ k_i\neq\infty}}^{p} \{(0,\ldots,0,k_i+1,0,\ldots,0)\} + \mathbb{N}^p.$$

Éste es el último paso que necesitábamos para dar un método que realize la descomposición en ideales irreducibles de un ideal de un monoide finitamente generado

(supuesto conocido un sistema de generadores suyo como ideal). Resumiendo, los pasos a seguir son

(1) Calcular

$$I = \bigcap_{i=1}^{r} \left(\bigcap_{n\in\mathbb{N}} (\mathbb{N}^p/\sigma \setminus \mathcal{B}([x_n^i]_\sigma)) \right) = \bigcap_{i=1}^{r} (\mathbb{N}^p/\sigma \setminus \mathcal{B}[z^i]_\sigma).$$

(2) Para todo $i \in \{1,\dots,r\}$ calcular

$$\text{Maximales}\left(\mathrm{E}(\mathcal{B}([z^i]_\sigma))\right).$$

(3) Para todo $i \in \{1,\dots,r\}$ calcular

$$\mathrm{E}(\mathbb{N}^p/\sigma \setminus \mathcal{B}([z^i]_\sigma))$$

lo cual nos dice quien es $\mathbb{N}^p/\sigma \setminus \bigcup_{n\in\mathbb{N}} \mathcal{B}([x_n^i]_\sigma)$.

EJEMPLO 9.25. Sea σ la congruencia generada por

$$\{((5,0,0,0),(0,7,0,0)),((0,0,6,0),(0,0,1,0))\},$$

S el monoide $\mathbb{N}^4/\sigma$ e I el ideal $[(3,3,6,5)]_\sigma + S$. En primer lugar, usando el algoritmo 9.16, calculamos el conjunto $\text{Minimales}_{\leq}\mathrm{E}(I)$, obteniendo que éste conjunto es igual a $\{(8,0,1,5),(0,10,1,5),(3,3,1,5)\}$ y por tanto

$$\mathrm{E}(I) = \{(8,0,1,5),(0,10,1,5),(3,3,1,5)\} + \mathbb{N}^4.$$

Por el Colorario 9.4, tenemos que la descomposición en irreducibles de $\mathrm{E}(I)$ es

$$\mathrm{E}(I) = (\{(0,0,0,5)\} + \mathbb{N}^4) \cap (\{(0,0,1,0)\} + \mathbb{N}^4)$$
$$\cap(\{(0,10,0,0),(3,0,0,0)\} + \mathbb{N}^4) \cap (\{(8,0,0,0),(0,3,0,0)\} + \mathbb{N}^4).$$

Usando ahora la Proposición 9.6, tenemos que la descomposición de $\mathrm{E}(I)$ en irreducibles es igual a

$$(\mathbb{N}^4 \setminus \bigcup_{n\in\mathbb{N}} \mathcal{B}(x_n^1)) \cap (\mathbb{N}^4 \setminus \bigcup_{n\in\mathbb{N}} \mathcal{B}(x_n^2)) \cap (\mathbb{N}^4 \setminus \bigcup_{n\in\mathbb{N}} \mathcal{B}(x_n^3)) \cap (\mathbb{N}^4 \setminus \bigcup_{n\in\mathbb{N}} \mathcal{B}(x_n^4)).$$

con $x_n^1 = (n,n,n,4)$, $x_n^2 = (n,n,0,n)$, $x_n^3 = (2,9,n,n)$ y $x_n^4 = (7,2,n,n)$. En consecuencia, por el Teorema 9.11, obtenemos

$$I = (\mathbb{N}^4/\sigma \setminus \mathcal{B}[z^1]_\sigma) \cap (\mathbb{N}^4/\sigma \setminus \mathcal{B}[z^2]_\sigma) \cap (\mathbb{N}^4/\sigma \setminus \mathcal{B}[z^3]_\sigma) \cap (\mathbb{N}^4/\sigma \setminus \mathcal{B}[z^4]_\sigma)$$

con $z^1 = (\infty,\infty,\infty,4)$, $z^2 = (\infty,\infty,0,\infty)$, $z^3 = (2,9,\infty,\infty)$ y $z^4 = (7,2,\infty,\infty)$.

Calculamos ahora los conjuntos $\text{Maximales}(\mathrm{E}(\mathcal{B}([z^i]_\sigma)))$ para $i = 1,2,3,4$.

Ya que $z^1 \notin \mathbb{N}^4$ y sus coordenadas primera, segunda y tercera son iguales a ∞, el Algoritmo 9.20 nos dice que hemos de calcular $\Pi_1(\Pi_1(\Pi_1(\sigma)))$, la cual es la congruencia trivial de $\mathbb{N}$. Además, $\Pi_1(\Pi_1(\Pi_1(z^1))) = 4$, de donde

$$\text{Maximales}(\mathrm{E}(\mathcal{B}([z^1]_\sigma))) = \{(\infty,\infty,\infty,4)\}.$$

El cálculo de $\text{Maximales}(\mathrm{E}(\mathcal{B}([z^2]_\sigma)))$ se realiza de forma análoga al del anterior caso. Obtenemos

$$\text{Maximales}(\mathrm{E}(\mathcal{B}([z^2]_\sigma))) = \{(\infty,\infty,0,\infty)\}.$$

Para $i = 3$, calculamos $\Pi_3(\Pi_3(\sigma))$, la cual es igual a la congruencia τ generada por

$$\{((5,0),(0,7))\}.$$

Tenemos también que $\Pi_3(\Pi_3(z^3)) = (2,9)$, un elemento cuya τ-clase es igual a $\{(2,9),(7,2)\}$. Así,

$$\text{Maximales}(\text{E}(\mathcal{B}([z^3]_\sigma))) = \{(7,2,\infty,\infty),(2,9,\infty,\infty)\}.$$

El caso $i = 4$ es muy similar al caso $i = 3$. Para este caso el resultado es el mismo que para $i = 3$,

$$\text{Maximales}(\text{E}(\mathcal{B}([z^4]_\sigma))) = \{(7,2,\infty,\infty),(2,9,\infty,\infty)\}.$$

En consecuencia, deducimos que I no es irreducible y que

$$I = (\mathbb{N}^4/\sigma \setminus \mathcal{B}([z^1]_\sigma)) \cap (\mathbb{N}^4/\sigma \setminus \mathcal{B}([z^2]_\sigma)) \cap (\mathbb{N}^4/\sigma \setminus \mathcal{B}([z^3]_\sigma)).$$

Usando el comentario que hicimos tras el Algoritmo 9.24 obtenemos que

$$S \setminus \mathcal{B}([z^1]) = [(0,0,0,5)]_\sigma + S,$$
$$S \setminus \mathcal{B}([z^2]) = [(0,0,1,0)]_\sigma + S,$$

y

$$S \setminus \mathcal{B}([z^3]) = \{[(8,0,0,0)]_\sigma, [(3,3,0,0)]_\sigma, [(0,10,0,0)]_\sigma\} + S.$$

Por tanto, la decomposición de I puede ser también expresada como

$$\begin{aligned} I \;=\; & ([(0,0,0,5)]_\sigma + S) \cap ([(0,0,1,0)]_\sigma + S) \\ & \cap (\{[(8,0,0,0)]_\sigma, [(3,3,0,0)]_\sigma, [(0,10,0,0)]_\sigma\} + S). \end{aligned}$$

□

CAPÍTULO 10

Ideales primarios de monoides conmutativos finitamente generados

El concepto de ideal primario juega un papel importante en la teoría de ideales de semigrupos, además recientemente algunos problemas de factorización en dominios ha sido transladado, en un contexto más general, a problemas de factorización en monoides (ver [**14, 26, 35, 49**]). Por esta razón nuevos e interesantes conceptos aparecen. Uno de ellos es el de elemento primario de un monoide.

En este capítulo, nuestro objetivo es explicar lo siguiente:

(1) Describir un método algorítmico para determinar si un ideal de $\mathbb{N}^p/\sigma$ es primario.
(2) Dar un algoritmo para calcular el conjunto de elementos primarios de $\mathbb{N}^p/\sim_M$.

El primero de estos dos algoritmos está esencialmente basado en dos resultados: una caracterización algorítmica de los ideales primarios de $\mathbb{N}^p$ y el Algoritmo 9.16 del capítulo anterior. El concepto de componente arquimediana (ver [**82**]) juega un papel muy importante en nuestro segundo algoritmo. Para obtenerlo necesitamos calcular a partir de un sistema de generadores de $\sim_M$ las componentes arquimedianas de $\mathbb{N}^p/\sim_M$. Una vez calculadas, este algoritmo usa el algoritmo de la sección anterior y nos devuelve el conjunto de los elementos primarios de $\mathbb{N}^p/\sim_M$.

Los contenidos de este capítulo son una mejora de lo que puede encontrarse en [**64**].

1. Ideales primarios de monoides finitamente generados

Como ya definimos en el Capítulo 1, un ideal I de un monoide S es un ideal primario si satisface que para todo $x, y \in S$ con $x+y \in I$ y $x \notin I$, existe $k \in \mathbb{N}\setminus\{0\}$ tal que $ky \in I$.

En el resto de esta sección supondremos que σ es una congruencia sobre $\mathbb{N}^p$, I un ideal de $\mathbb{N}^p/\sigma$ y $\mathrm{E}(I) = \{x \in \mathbb{N}^p \mid [x]_\sigma \in I\}$ donde $[x]_\sigma$ como hasta ahora denota la σ-clase de $\mathbb{N}^p$ que contiene a x. Usando que $\mathrm{E}(I)$ es un ideal de $\mathbb{N}^p$ puede probarse el siguiente resultado.

PROPOSICIÓN 10.1. *Un ideal I es un ideal primario de $\mathbb{N}^p/\sigma$ si y sólo si $\mathrm{E}(I)$ es un ideal primario de $\mathbb{N}^p$.*

La siguiente proposición caracteriza a los ideales primarios de $\mathbb{N}^p$.

Denotamos por $\leq$ el orden sobre $\mathbb{N}^p$ definido por $(a_1,\ldots,a_p) \leq (b_1,\ldots,b_p)$ si $a_i \leq b_i$ para todo $i \in \{1,\ldots,p\}$. Por el lema de Dickson, si A es un subconjunto de $\mathbb{N}^p$, entonces $\mathrm{Minimales}_{\leq}(A)$, el conjunto de elementos minimales de A con respecto a $\leq$, es un conjunto finito.

PROPOSICIÓN 10.2. *Sea J un ideal de $\mathbb{N}^p$. Las siguientes afirmaciones son equivalentes:*

(1) J es un ideal primario de $\mathbb{N}^p$,
(2) si $(x_1,\dots,x_p) \in \text{Minimales}_{\leq}(J)$ y $x_i \neq 0$, entonces $te_i \in \text{Minimales}_{\leq}(J)$ para algún $t \in \mathbb{N}\setminus\{0\}$.

DEMOSTRACIÓN. *(1) implica (2).* Sea $x=(x_1,\dots,x_p) \in \text{Minimales}_{\leq}(J)$ y $x_i \neq 0$. Entonces $x-e_i, e_i \in \mathbb{N}^p$, $(x-e_i)+e_i \in J$ y $x-e_i \notin J$. Usando el que J es un ideal primario, deducimos que existe $t \in \mathbb{N}\setminus\{0\}$ tal que $te_i \in J$. Tomemos $k=\text{minimo}\{t \in \mathbb{N} \mid te_i \in J\}$. Téngase en cuenta que $t \neq 0$ ya que en otro caso obtendriamos que $(0,\dots,0) \in J$ lo que contradice la minimalidad de x. Esto nos lleva a que $te_i \in \text{Minimales}_{\leq}(J)$.

(2) implica (1). Sean $x,y \in \mathbb{N}^p$ tales que $x+y \in J$ y $x \notin J$. Usando el que $x+y \in J$ tenemos que $x+y=m+z$ paar algún $m \in \text{Minimales}_{\leq}(J)$ y algún $z \in \mathbb{N}^p$. Además, como $x \notin J$, $x \not< x$ y $m < x+y$, existe $i \in \{1,\dots,p\}$ tal que $\{y-e_i, m-e_i\} \subseteq \mathbb{N}^p$. Por hipótesis existe $k \in \mathbb{N}\setminus\{0\}$ tal que $ke_i \in \text{Minimales}_{\leq}(J) \subset J$. Finalmente, usando que $y-e_i \in \mathbb{N}^p$, obtenemos $ky \in J = k(y-e_i)ke_i$. □

Dado I un ideal de $\mathbb{N}^p/\sigma$ del que conocemos $\{[\lambda_1]_\sigma,\dots,[\lambda_r]_\sigma\}$ un sistema de generadores suyo, usando el Algoritmo 9.16 obtenemos el conjunto $\text{Minimales}_{\leq}(\text{E}(I))$. A partir de este conjunto es inmediato comprobar si se verifica la Condición 2 de 10.2. Obtenemos de esta forma un algoritmo para determinar si un ideal es primario. Terminamos esta sección ilustrando este método con un ejemplo.

EJEMPLO 10.3. Como en el ejemplo 9.25, tomemos σ la congruencia generada por

$$\{((5,0,0,0),(0,7,0,0)),((0,0,6,0),(0,0,1,0))\},$$

S el monoide $\mathbb{N}^4/\sigma$ e I el ideal $[(3,3,6,5)]_\sigma+S$. Usando el algoritmo 9.16, teníamos que el conjunto $\text{Minimales}_{\leq}\text{E}(I)$ era igual a $\{(8,0,1,5),(0,10,1,5),(3,3,1,5)\}$ y por tanto

$$\text{E}(I)=\{(8,0,1,5),(0,10,1,5),(3,3,1,5)\}+\mathbb{N}^4.$$

El elemento $(3,3,1,5)$ verifica tener todas sus coordenadas no nulas, por lo que caso de ser I primario en el conjunto $\text{E}(I)$ existirían elementos de la forma t_1e_1, t_2e_2, t_3e_3, t_4e_4 con $t_1,t_2,t_3,t_4 \in \mathbb{N}\setminus\{0\}$. Claramente ésto no se cumple y por tanto I no es un ideal primario. □

Para finalizar la sección comentar que de las caracterizaciones obtenidas en este capítulo para ideales primarios y de las del capítulo anterior para ideales irreducibles se deduce fácilmente que todo ideal irreducible es primario. Un sencillo ejemplo de ideal primario que no es irreducible lo tenemos en $\mathbb{N}^2$ con el ideal $I=\{(5,0),(0,5),(2,2)\}+\mathbb{N}^2$.

2. Elementos primarios de un monoide cancelativo

Sea $(S,+)$ un monoide. Un elemento $a \in S\setminus\mathcal{U}(S)$ es un **elemento primario** de S si $\{a\}+S$ es un ideal primario de S. En esta sección nuestro objetivo es mostrar cómo se distribuyen este tipo de elementos en un monoide cancelativo.

Recordemos también que en todo monoide S se tenía que $\mathcal{U}(S) = [0]_{\mathcal{N}}$.

LEMA 10.4. *Si $(S,+)$ es un monoide cancelativo y a es un elemento primario, entonces $[a]_{\mathcal{N}} \in \text{Minimales}_{\leq}(S/\mathcal{N} \setminus \{[0]_{\mathcal{N}}\})$ con $\leq$ definido por $[a]_{\mathcal{N}} \leq [b]_{\mathcal{N}}$ si $[a+b]_{\mathcal{N}} = [b]_{\mathcal{N}}$.*

DEMOSTRACIÓN. Sea $[b]_{\mathcal{N}} \in S \setminus \{[0]_{\mathcal{N}}\}$ tal que $[b]_{\mathcal{N}} \leq [a]_{\mathcal{N}}$. Usando que $[b]_{\mathcal{N}} \leq [a]_{\mathcal{N}}$, podemos decir que $[a+b]_{\mathcal{N}} = [a]_{\mathcal{N}} + [b]_{\mathcal{N}} = [a]_{\mathcal{N}}$ y así $(a+b)\mathcal{N}a$. Por ello existe $k \in \mathbb{N}\{0\}$ y $s \in S$ tal que $ka = a+b+s$. Si para todo $t \in \mathbb{N}$ tenemos que $s - ta \in S$, entonces $s-(k-1)a = s' \in S$ y $ka = a+b+(k-1)a+s'$. En consecuencia $b+s' = 0$, lo que contradice el que $[b]_{\mathcal{N}} \neq [0]_{\mathcal{N}} = \mathcal{U}(S)$. Es por ello que ha de existir $t \in \mathbb{N}$ y $c \notin \{a\}+S$ tal que $s = ta+c$. Por tanto, $(k-t-1)a = b+c$ con $c \notin \{a\}+S$. Usando que $k-t-1 > 0$ (ya que en otro caso $b \in \mathcal{U}(S)$), obtenemos que $b+c \in \{a\}+S$. Como $\{a\}+S$ es un ideal primario, existe $\bar{k} \in \mathbb{N} \setminus \{0\}$ tal que $\bar{k}b \in \{a\}+S$. De ahí que $\bar{k}b = a+\bar{s}$ para algún $\bar{s} \in S$. Finalmente, ya que $ka = b+(a+s)$, concluimos que $a\mathcal{N}b$ y así $[a]_{\mathcal{N}} = [b]_{\mathcal{N}}$. □

Los siguientes dos resultados se deducen de la Proposición 1.2 de [**36**].

LEMA 10.5. *Sea $(S,+)$ un monoide cancelativo y $a,b \in S$ dos elementos primarios suyos tales que $a\mathcal{N}b$. El elemento $a+b$ es también un elemento primario de S.*

LEMA 10.6. *Sea $(S,+)$ un monoide cancelativo y a,b elementos de S tales que $a \in S \setminus \mathcal{U}(S)$ y $a+b$ es primario. El elemento a es un elemento primario de S.*

LEMA 10.7. *Sea $(S,+)$ un monoide cancelativo, $a \in S$ un elemento primario y $b \in S$ tal que $a\mathcal{N}b$. Entonces b es un elemento primario de S.*

DEMOSTRACIÓN. Sabemos que ha de existir $k \in \mathbb{N} \setminus \{0\}$ y $c \in S$ tal que $ka = b+c$. Como a es primario, por el Lema 10.5, el elemento ka es también primario. De ahí que $b+c$ también lo sea y que $b \notin \mathcal{U}(S)$. Finalmente usando el Lema 10.6 concluimos que b es un elemento primario. □

El siguiente teorema resume todos los resultados dados hasta el momento en esta sección.

TEOREMA 10.8. *Sea $(S,+)$ un monoide cancelativo y $\mathrm{P}(S)$ el conjunto de elementos primarios de S. Entonces existe una familia $\{C_i \mid i \in \Delta\}$ de elementos de $\text{Minimales}_{\leq}(S/\mathcal{N} \setminus \{[0]_{\mathcal{N}}\})$ tal que $\mathrm{P}(S) = \cup_{i \in \Delta} C_i$.*

Terminamos esta sección describiendo un algoritmo para el cálculo del conjunto de elementos primarios de un monoide finitamente generado cancelativo.

En primer lugar, obsérvese que a partir de [**65**] (véase también el Capítulo 1) se deduce que si $C_1, C_2 \in S/\mathcal{N}$, entonces $C_1 \leq C_2$ si y sólo si $\text{Supp}(C_1) \subseteq \text{Supp}(C_2)$ (recuérdese que $\text{Supp}(C)$ era el conjunto de coordenadas que un elemento de C podía tener no nulas). Podemos así determinar el conjunto $\text{Minimales}_{\leq}(S/\mathcal{N} \setminus \{[0]_{\mathcal{N}}\})$ (recordar que por el Teorema 10.8 sabemos que todos los elementos primarios de S pertenecen a alguna de estas componentes arquimedianas). Supongamos que $\text{Minimales}_{\leq}(S/\mathcal{N} \setminus \{[0]_{\mathcal{N}}\}) = \{C_1, \ldots, C_l\}$ y sean $m_1 \in C_1, \ldots, m_l \in C_l$ (téngase en

cuenta que si $\mathrm{Supp}(C) = \{e_{i_1}, \ldots, e_{i_r}\}$, entonces $[e_{i_1} + \cdots + e_{i_r}] \in C$). Utilizando el método explicado en la sección anterior podemos determinar cuáles de los ideales $\{m_1\} + S, \ldots, \{m_l\} + S$ son ideales primarios. Supongamos que estos son $\{m_{i1}\} + S, \ldots, \{m_{ik}\} + S$. Entonces el Teorema 10.8 nos asegura que $\mathrm{P}(S) = C_{i_1} \cup \ldots \cup C_{i_k}$.

EJEMPLO 10.9. Sea M el subgrupo de $\mathbb{Z}^6$ generado por

$$\{(2,5,-3,-2,0,0),(0,0,0,0,2,-8)\}$$

y $S \cong \mathbb{N}^6 / \sim_M$. M está definido por las ecuaciones

$$\begin{aligned} x_5 &\equiv 0 (\mathrm{mod} 2), \\ -x_1 + x_2 + x_3 &= 0, \\ x_1 + x_4 &= 0, \\ 5x_1 - 2x_2 &= 0, \\ 4x_5 + x_6 &= 0. \end{aligned}$$

En primer lugar calculamos $\mathrm{Minimales}_{\leq}(S/\mathcal{N} \setminus \{[0]_{\mathcal{N}}\})$, obteniendo:

$$\begin{aligned} C_1 &= \{[(x_1,0,0,0,0,0)]_{\sim_M} \mid x_1 \geq 1\} \\ C_2 &= \{[(0,x_2,0,0,0,0)]_{\sim_M} \mid x_2 \geq 1\} \\ C_3 &= \{[(0,0,x_3,0,0,0)]_{\sim_M} \mid x_3 \geq 1\} \\ C_4 &= \{[(0,0,0,x_4,0,0)]_{\sim_M} \mid x_4 \geq 1\} \\ C_5 &= \{[(0,0,0,0,x_5,x_6)]_{\sim_M} \mid x_5 \geq 1 \text{ or } x_6 \geq 1\}. \end{aligned}$$

Por el Lema 10.4, si un elemento $a \in S$ es primario, entonces existe $i \in \{1,2,3,4,5\}$ tal que $a \in C_i$. También tenemos que si $a \in C_i$ es un elemento primario, entonces $C_i \subseteq \mathrm{P}(S)$. Tomemos ahora los elementos $x_1 = [(1,0,0,0,0,0)]_{\sim_M}$, $x_2 = [(0,1,0,0,0,0)]_{\sim_M}$, $x_3 = [(0,0,1,0,0,0)]_{\sim_M}$, $x_4 = [(0,0,0,1,0,0)]_{\sim_M}$ y $x_5 = [(0,0,0,0,1,0)]_{\sim_M}$ los cuales pertenecen a C_1, C_2, C_3, C_4 y C_5, respectivamente. Usando el método explicado en la sección anterior para comprobar si el ideal generado por cada uno de estos elementos es primario, obtenemos:

x_i	$\mathrm{Minimales}_{\leq}(\mathrm{E}(x_i + S))$	¿Es x_i primario?
$[(1,0,0,0,0,0)]$	$\{(1,0,0,0,0,0),(0,0,3,2,0,0)\}$	NO
$[(0,1,0,0,0,0)]$	$\{(0,1,0,0,0,0),(0,0,3,2,0,0)\}$	NO
$[(0,0,1,0,0,0)]$	$\{(0,0,1,0,0,0),(2,5,0,0,0,0)\}$	NO
$[(0,0,0,1,0,0)]$	$\{(0,0,0,1,0,0),(2,5,0,0,0,0)\}$	NO
$[(0,0,0,0,1,0)]$	$\{(0,0,0,0,1,0),(0,0,0,0,0,8)\}$	SÍ

Así, obtenemos que $\mathrm{P}(S) = C_5$. □

CAPÍTULO 11

Monoides de ideales principales

1. Introducción

El objeto de este capítulo es estudiar un tipo especial de monoides: monoides que contengan únicamente ideales principales, a los que llamaremos MIP para abreviar. La resolución de este problema se alcanzó en [**77**], pero sólo para algunos casos especiales. En este capítulo daremos una solución general para el mismo.

Las razones para este estudio son entre otras las siguientes. En ellos el estudio de sus ideales resulta más sencillo que en monoides en general y además para todo par de elementos a, b podemos decir que x es máximo común divisor si el ideal generado por $\{a,b\}$ coincide con el que genera $\{x\}$.

Lo que haremos será caracterizar aquellos monoides que sólo contienen ideales principales y dar un algoritmo para decidir a partir de una presentación de un monoide finitamente generado si es o no un MIP.

Los contenidos de este capítulo se pueden encontrar en [**70**].

2. Caracterización

Recordemos que un ideal de un monoide S se dice principal si existe $a \in S$ tal que $I = a + S$. Así, decimos que S es un **MIP** si todos sus ideales son principales. Nuestro objetivo en esta sección es estudiar este tipo de monoides, centrando nuestra atención en monoides finitamente generados.

LEMA 11.1. *Sea $(S,+)$ un MIP. Entonces para todo $a,b \in S$, tenemos que $a \in b+S$ ó $b \in a+S$.*

DEMOSTRACIÓN. Ya que S es un MIP, el ideal $\{a,b\}+S$ es un ideal principal. Así tenemos que existe $c \in S$ tal que $\{a,b\}+S = c+S$. De esta última igualdad obtenemos que existen $x,y \in S$ para los que $a = c+x$ y $b = c+y$. Además, $c \in \{a,b\}+S$ y por tanto se tiene una de las siguientes igualdades

- $c = a+z$ para algún $z \in S$,
- $c = b+t$ para algún $t \in S$.

Sin pérdida de generalidad, podemos suponer que $c = a+z$ obteniendo que $b = c+y = a+z+y$ y así el que $b \in a+S$. □

El siguiente resultado es fácil de probar.

LEMA 11.2. *Sea $(S,+)$ un monoide y $a,b,c \in S$ tales que $a \in b+S$ y $b \in c+S$. Entonces $a \in c+S$.*

El siguiente resultado se obtiene por inducción sobre n.

LEMA 11.3. *Sea $\{x_1,\dots,x_n\}$ un subconjunto de un monoide $(S,+)$ satisfaciendo que para todo $i,j\in\{1,\dots,n\}$, $x_i\in x_j+S$ ó $x_j\in x_i+S$. Entonces se cumplen las siguientes condiciones:*

(1) existe $i\in\{1,\dots,n\}$ tal que $x_j\in x_i+S$ para todo $j\in\{1,\dots,n\}$,
(2) existe $i\in\{1,\dots,n\}$ tal que $x_i\in x_j+S$ para todo $j\in\{1,\dots,n\}$.

En el caso de monoides finitamente generados el recíproco del Lema 11.1 también es cierto como muestra el siguiente resultado.

PROPOSICIÓN 11.4. *Sea $(S,+)$ un monoide finitamente generado. Las siguientes condiciones son equivalentes.*

(1) S es un MIP.
(2) Para todo $a,b\in S$ se tiene que $a\in b+S$ ó $b\in a+S$.

DEMOSTRACIÓN. *(1) implica (2).* Probado en el Lema 11.1.

(2) implica (1). Tomemos I un ideal de S y veamos que I es principal. S es finitamente generado, por lo que existe $\{x_1,\dots,x_n\}\subseteq S$ tal que $I=\{x_1,\dots,x_n\}+S$ (véase [**30**]). Además el conjunto $\{x_1,\dots,x_n\}$ satisface las hipótesis del Lema 11.3, por tanto ha de existir $i\in\{1,\dots,n\}$ tal que $x_j\in x_i+S$ para todo $j\in\{1,\dots,n\}$. Claramente se deduce que $I=x_i+S$. □

La proposición anterior caracteriza a los MIP, pero caso de tener un monoide que no sea finito la condición (2) es imposible de comprobar. El siguiente resultado nos dice que sólo hemos de ver cuando un sistema minimal de generadores de S cumple esta condición.

TEOREMA 11.5. *Sea $(S,+)$ un monoide y $\{s_1,\dots,s_p\}$ un sistema minimal de generadores de S. Las siguientes afirmaciones son equivalentes.*

(1) S es un MIP.
(2) Para todo $i,j\in\{1,\dots,p\}$ ó bien $s_i\in s_j+S$ ó bien $s_j\in s_i+S$.

DEMOSTRACIÓN. *(1) implica (2).* Consecuencia del Lema 11.1.

(2) implica (1). Por la Proposición 11.4, para probar que S es un MIP sólamente hemos de ver que para todo $a,b\in S$, o bien $a\in b+S$ o bien $b\in S$. Usando que $a,b\in S$, tenemos que $a=a_1s_1+\cdots+a_ps_p$ y que $b=b_1s_1+\cdots+b_ps_p$ para algún $(a_1,\dots,a_p),(b_1,\dots,b_p)\in\mathbb{N}^p$. Consideremos el conjunto

$$\{i_1,\dots,i_r\}=\{i\in\{1,\dots,p\}\mid a_i+b_i\neq 0\}.$$

El conjunto $\{s_{i_1},\dots,s_{i_r}\}$ satisface las hipótesis del Lema 11.3 y por tanto existe $i_k\in\{i_1,\dots,i_r\}$ tal que $s_{i_k}\in s_{i_j}+S$ para todo $i_j\in\{i_1,\dots,i_r\}$. Como $a_{ik}+b_{ik}\neq 0$, obtenemos que $a_{ik}\neq 0$ ó $b_{ik}\neq 0$. Sin perdida de generalidad, podemos suponer que $a_{i_k}\geq b_{i_k}\geq 0$. Veamos que $a\in b+S$. Sabemos que si $i_j\in\{i_1,\dots,i_r\}\setminus\{i_k\}$, entonces $s_{ik}\in s_{i_j}+S$ y en consecuencia $s_{ik}=x_1s_1+\cdots+x_ps_p$ para algún $(x_1,\dots,x_p)\in\mathbb{N}^p$ con $x_{i_j}\neq$

0. Aplicando ahora el que $\{s_1,\ldots,s_p\}$ es un sistema minimal de generadores de S, deducimos que $x_{i_k}\neq 0$. Así tenemos que

$$\begin{aligned} a &= a_1s_1 + cldots + a_ps_p \\ &= (a_1+x_1)s_1+\cdots+(a_{i_{k-1}}+x_{i_{k-1}})s_{i_{k-1}}+(a_{i_k}-1+x_{i_k})s_{i_k} \\ &\quad +(a_{i_{k+1}}+x_{i_{k+1}})s_{i_{k+1}}+\cdots+(a_p+x_p)s_p, \end{aligned}$$

con $a_{i_j}+x_{i_j}>a_{i_j}$ y $(a_{i_k}-1+x_{i_k})\geq a_{i_k}\neq 0$. Repitiendo este razonamiento n veces obtenemos

$$a=(a_1+c_1)s_1+\ldots+(a_p+c_p)s_p.$$

Tomando n tan grande como sea necesario nos queda que $a_{i_j}+nx_{i_j}\geq b_{i_j}$. Llevando a cabo el anterior procedimiento para todo $i_j\in\{i_1,\ldots,i_r\}\backslash\{i_k\}$ obtenemos que

$$a=(a_1+c_1)s_1+\ldots+(a_p+c_p)s_p,$$

con $a_i+c_i\geq b_i$ para todo $i\in\{1,\ldots,p\}$, de donde se sigue que $a\in b+S$. □

El siguiente resultado nos dice que en el anterior teorema podemos prescindir de la condición de que el sistema de generadores sea minimal.

COROLARIO 11.6. *Sea $(S,+)$ un monoide y $\{s_1,\ldots,s_p\}$ un sistema de generadores suyo. Las siguientes condiciones son equivalentes.*

(1) S es un MIP.
(2) Para todo $i,j\in\{1,\ldots,p\}$ o bien $s_i\in s_j+S$ o bien $s_j\in s_i+S$.

DEMOSTRACIÓN. *(1) implica (2).* Se obtiene como consecuencia del Lema 11.1

(2) implica (1). Si $\{s_{i_1},\ldots,s_{i_r}\}$ es un sistema minimal de generadores de S, entonces satisface la Condición (2) del Teorema 11.5 y por tanto S es un MIP. □

3. Algoritmo

Una vez que tenemos una presentación de un monoide finitamente generado, la idea es usar el Corolario 11.6 para encontrar un procedimiento que permita decidir cuando un monoide es o no un MIP.

Consideremos $(S,+)$ un monoide finitamente generado ρ una de sus presentaciones. Para resolver el anterior problema, en primer lugar hemos de saber comprobar cuándo dados dos elementos $a,b\in\mathbb{N}^p/\sigma$ tenemos que $b\in a+S$. Esto se consigue tomando κ un sistema canónico de generadores de la congruencia de Rees asociada al ideal $\{[a]_\sigma\}+\mathbb{N}^p/\sigma$ y comprobando si $\mathrm{NF}_\rho(b)=\mathrm{NF}_\rho(a)$. Recordemos que κ se obtenía calculando un sistema canónico de generadores de la congruencia generada por

$$\rho_{\mathcal{R}_a}=\{(a+e_1,a),\ldots,(a+e_p,a)\}\cup\rho$$

(ver Capítulo 1).

Sea $\sigma_{\mathcal{R}_{e_i}}$ la congruencia de Rees asociada al ideal $[e_i]_\sigma+\mathbb{N}^p/\sigma$ y $\rho_{\mathcal{R}_{e_i}}$ un sistema de generadores suyo (véase Capítulo 1). Si tenemos que $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ es un sistema minimal de generadores de S, por el Corolario 11.6, $S=\mathbb{N}^p/\sigma$ es un MIP si y sólo si para todo $i,j\in\{1,\ldots,p\}$ se cumple que o bien $(e_i,e_j)\in\sigma_{\mathcal{R}_{e_i}}$ o bien $(e_i,e_j)\in\sigma_{\mathcal{R}_{e_j}}$.

Por tanto el problema de decidir si $\mathbb{N}^p/\sigma$ es un MIP, conocido ρ, queda reducido a resolver el problema de palabras en $\mathbb{N}^p/\sigma_{\mathcal{R}_{e_i}}$ para todo $i \in \{1,\ldots,p\}$, lo cual sabemos que puede resolverse (ver 1).

ALGORITMO 11.7. Un subconjunto finito ρ de $\mathbb{N}^p$ es dado. Si σ es la congruencia generada por ρ, el algoritmo devuelve "VERDADERO" si $\mathbb{N}^p/\sigma$ es un MIP, y "FALSO" en otro caso.

(1) Para todo $i \in \{1,\ldots,p\}$, calcula un sistema canónico de generadores para $\sigma_{\mathcal{R}_{e_i}}$ a partir de $\rho_{\mathcal{R}_{e_i}}$ (tal y como se explica en [**65**]). Lo denotamos por κ_i.
(2) Para todo $i,j \in \{1,\ldots,p\}$, $i<j$, si $\mathrm{NF}_{\kappa_i}(e_i) \neq \mathrm{NF}_{\kappa_i}(e_j)$ y $\mathrm{NF}_{\kappa_j}(e_i) \neq \mathrm{NF}_{\kappa_j}(e_j)$, entonces decuelve "FALSO".
(3) Devuelve "VERDADERO".

□

Este algoritmo ha sido implimentado en GAP (ver [**83**]). A continuación damos un par de ejemplos que ilustran su funcionamiento.

EJEMPLO 11.8. Sea

$$\rho = \{((0,1,1),(0,1,0)),((1,0,1),(1,0,0)),((1,1,0),(1,0,0)),$$
$$((3,0,0),(2,0,0)),((0,0,4),(0,0,3))\}.$$

```
gap> pim([[[0,1,1],[0,1,0]],[[1,0,1],[1,0,0]],
  [[1,1,0],[1,0,0]],[[3,0,0],[2,0,0]],
  [[0,0,4],[0,0,3]]]);
k[1]=[ [ [ 0, 1, 1 ], [ 0, 1, 0 ] ],
       [ [ 0, 0, 4 ], [ 0, 0, 3 ] ],
       [ [ 2, 0, 0 ], [ 1, 0, 0 ] ],
       [ [ 1, 1, 0 ], [ 1, 0, 0 ] ],
       [ [ 1, 0, 1 ], [ 1, 0, 0 ] ] ]
k[2]=[ [ [ 1, 0, 0 ], [ 0, 1, 0 ] ],
       [ [ 0, 0, 4 ], [ 0, 0, 3 ] ],
       [ [ 0, 2, 0 ], [ 0, 1, 0 ] ],
       [ [ 0, 1, 1 ], [ 0, 1, 0 ] ] ]
k[3]=[ [ [ 0, 1, 0 ], [ 0, 0, 1 ] ],
       [ [ 1, 0, 0 ], [ 0, 0, 1 ] ],
       [ [ 0, 0, 2 ], [ 0, 0, 1 ] ] ]
true
```

El monoide $\mathbb{N}^3/\sigma$, con σ la congruencia generada por ρ, es entonces un MIP. □

EJEMPLO 11.9. Tomemos ahora ρ el conjunto

$$\{((0,1,1),(0,1,0)),((1,0,1),(1,0,0)),$$
$$((3,0,0),(2,0,0)),((0,0,4),(0,0,3))\}.$$

```
gap> pim([[[0,1,1],[0,1,0]],[[1,0,1],[1,0,0]],
       [[3,0,0],[2,0,0]],[[0,0,4],[0,0,3]]]);

k[1]=[ [ [ 0, 1, 1 ], [ 0, 1, 0 ] ],
       [ [ 0, 0, 4 ], [ 0, 0, 3 ] ],
       [ [ 2, 0, 0 ], [ 1, 0, 0 ] ],
       [ [ 1, 1, 0 ], [ 1, 0, 0 ] ],
       [ [ 1, 0, 1 ], [ 1, 0, 0 ] ] ]
k[2]=[ [ [ 1, 0, 1 ], [ 1, 0, 0 ] ],
       [ [ 3, 0, 0 ], [ 2, 0, 0 ] ],
       [ [ 0, 0, 4 ], [ 0, 0, 3 ] ],
       [ [ 1, 1, 0 ], [ 0, 1, 0 ] ],
       [ [ 0, 2, 0 ], [ 0, 1, 0 ] ],
       [ [ 0, 1, 1 ], [ 0, 1, 0 ] ] ]
k[3]=[ [ [ 0, 1, 0 ], [ 0, 0, 1 ] ],
       [ [ 1, 0, 0 ], [ 0, 0, 1 ] ],
       [ [ 0, 0, 2 ], [ 0, 0, 1 ] ] ]

fails on 1 - 2
false
```

La salida "fallo en 1-2" significa que $[e_1] \notin [e_2] + \mathbb{N}^3/\sigma$ y que $[e_2] \notin [e_1] + \mathbb{N}^3/\sigma$ y por tanto $\mathbb{N}^3/\sigma$ (σ es la congruencia generada por ρ) no es un MIP. □

CAPÍTULO 12

Monoides atómicos

Inspirado en los trabajos [**12**] y [**52**], Zaks introduce en [**86**] el concepto de dominios semifactoriales. Ese trabajo estudia el concepto de factorización, el cual puede ser visto desde una perspectiva más amplia en la teoría de monoides conmutativos. Incluso en el caso en el que queramos concentrarnos en dominios, la generalización del concepto de dominio de Dedeking nos lleva al estudio de factorizaciones en monoides. Estas ideas han dado lugar a una gran cantidad de trabajos, ver por ejemplo [**6, 14, 17, 28, 27, 35, 47, 49**]. El uso del lenguaje de los monoides, en lugar del de los dominios, no sólo es un problema de generalización sino más bien de simplicidad y utilidad, tal y como se explica en los capítulos de Halter-Koch y de Chapman y Geroldinger de [**6**].

En este capítulo estudiaremos problemas de factorización en monoides. Daremos un método para comprobar si un monoide es atómico y calcularemos su conjunto de elementos irreducibles. Además, construiremos el monoide reducido asociado a un monoide y probaremos que la mayoría de las propiedades relativas a la factorización que cumple un monoide son heredadas por su monoide reducido asociado. Por último nos restringiremos al caso cancelativo donde veremos que los conceptos de factorización resultan ser mucho más sencillos.

1. Sistemas minimales de generadores y factorización

Consideremos un monoide S isomorfo a $\mathbb{N}^p/\sigma$. Supongamos que σ está generada por $\rho \subseteq \mathbb{N}^p \times \mathbb{N}^p$. El decidir cuándo un conjunto A es un sistema minimal de generadores de S es equivalente a decidir si el conjunto $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$, lo que equivale a que no exista $i \in \{1, \ldots, p\}$ tal que

$$[e_i]_\sigma \in \langle \{[e_1]_\sigma, \ldots, [e_{i-1}]_\sigma, [e_{i+1}]_\sigma, \ldots, [e_p]_\sigma\} \rangle.$$

Veamos cómo decidir si $[e_p]_\sigma \in \langle [e_1]_\sigma, \ldots, [e_{p-1}]_\sigma \rangle$. En primer lugar tomemos un orden que cumpla que $e_i \prec e_p$ para todo $i \neq p$ (por ejemplo el orden lexicográfico inverso) y un sistema canónico de generadores κ de la congruencia σ con respecto a $\preceq$. Se tiene que $[e_p]_\sigma \in \langle [e_1]_\sigma, \ldots, [e_{p-1}]_\sigma \rangle$ si y sólo si $\mathrm{NF}_\kappa(e_p) \neq e_p$. Si éste es nuestro caso, definimos el morfismo de monoides

$$f : \mathbb{N}^{p-1} \longrightarrow \mathbb{N}^p/\sigma,\ f(e_i) = [e_i].$$

y la congruencia τ por

$$(a_1, \ldots, a_{p-1}) \tau (b_1, \ldots, b_{p-1}) \text{ si } f(a_1, \ldots, a_{p-1}) = f(b_1, \ldots, b_{p-1}),$$

ó en otras palabras, $(a_1,\dots,a_{p-1},0)\sigma(b_1,\dots,b_{p-1},0)$. Además, la congruencia τ puede ser calculada a partir de σ por eliminación tal y como vimos en el Capítulo 1. Ya que $\mathbb{N}^{p-1}/\tau$ es isomorfo a $\mathbb{N}^p/\sigma$, podemos ver si un generador $[e_i]_\tau$ de $\mathbb{N}^{p-1}/\tau$ puede ser obtenido a partir del resto de los generadores. Esto puede hacerse repetiendo el proceso realizado para $[e_p]_\sigma$. Tras un número finito de pasos obtendremos finalmente una congruencia δ y un entero r tal que $\mathbb{N}^p/\sigma$ isomorfo a $\mathbb{N}^r/\delta$, con $\{[e_1]_\delta,\dots,[e_r]_\delta\}$ un sistema minimal de generadores suyo.

Dados $a,b\in S$, diremos que a **divide** a b si existe $c\in S$ tal que $b=a+c$, o equivalentemente que $b\in a+S$. En este caso escribiremos $a|b$. Los elementos $a,b\in S$ son asociados si $a|b$ y $b|a$, lo denotaremos por $a\simeq b$. Obsérvese que esto ocurre si y sólo si $a+S=b+S$.

Diremos que un elemento $x\in S$ es **irreducible** (o un átomo) si verifica las siguientes condiciones:

(i) $x\notin \mathcal{U}(S)$,
(ii) si $a|x$, entonces $a\in\mathcal{U}(S)$ ó $a\simeq x$ (esto es, $a+S=x+S$).

Obsérvese que la Condición (ii) no equivale en general a

(ii') si $x=a+b$, entonces $a\in\mathcal{U}(S)$ ó $b\in\mathcal{U}(S)$

(aunque veremos que sí en el caso cancelativo).

Denotaremos por $\mathcal{A}(S)$ al conjunto de elementos irreducibles de S. El monoide S es **atómico** si el semigrupo $S\setminus\mathcal{U}(S)$ está generado por $\mathcal{A}(S)$ (el conjunto $S\setminus\mathcal{U}(S)$ es siempre un ideal de S y por tanto un semigrupo).

Sea S un monoide atómico. Los elementos irreducibles $d_1,\dots,d_r$ forman una **descomposición** de $a\in S$, si $a=d_1+\cdots+d_r$. El monoide S decimos que es **semifactorial** si siempre que $\sum_{i=1}^n x_i=\sum_{i=1}^m y_i$, para algún $x_1,\dots,x_n,y_1,\dots,y_m\in\mathcal{A}(S)$, se tiene que $n=m$. Dos descomposiciones $a=n_1x_1+\cdots+n_rx_r$ y $a=m_1y_1+\cdots+m_sy_s$ son **descomposiciones asociadas**, si $r=s$ y, renumerando si es necesario, $x_i\simeq y_i$ y $n_ix_i\simeq m_iy_i$ para $i=1,\dots,r$. Una **factorización** de a es una clase de equivalencia formada por sus descomposiciones asociadas. S es llamado **factorial**, si todo elemento $a\in S$ tiene exactamente una sola factorización.

2. Monoides atómicos finitamente generados

A lo largo de esta sección, S denotará un monoide con sistema minimal de generadores $\{s_1,\dots,s_p\}$ tal que $\mathcal{U}(S)\cap\{s_1,\dots,s_p\}=\{s_{r+1},\dots,s_p\}$.

Centramos ahora nuestra atención en encontrar un método algorítmico que nos permita decidir si un monoide es o no atómico a partir de una sus presentaciones.

LEMA 12.1. *Sea $x\in S\setminus\mathcal{U}(S)$. Las siguientes condiciones son equivalentes:*
(1) x es irreducible,
(2) para todo $y\in S$, si $x+S\subsetneq y+S$, entonces $y\in\mathcal{U}(S)$.

DEMOSTRACIÓN. *(1) implica (2).* Si $x+S\subsetneq y+S$, entonces $x=y+z$ para algún $z\in S$ y $x+S\neq y+S$, de donde, usando que x es irreducible, $y\in\mathcal{U}(S)$.

(2) implica (1). Si $x = y+z$, entonces $x+S \subseteq y+S$ y por tanto, ó bien $x+S = y+S$ ó $x+S \subsetneq y+S$. En consecuencia, ó bien $x+S = y+S$ ó $y \in \mathcal{U}(S)$, lo que significa que x es irreducible. □

Nótese que si $y \in \mathcal{U}(S)$, entonces $y+S = S$, lo cual, usando el Lema 12.1, hace que los ideales maximales propios y principales de S sean exactamente aquellos generados por elementos irreducibles.

Como consecuencia directa de este último resultado obtenemos lo siguiente.

COROLARIO 12.2. *Si $x \simeq y$, entonces x es irreducible si y sólo si y es irreducible. En particular, si $x \in \mathcal{A}(S)$ y $u \in \mathcal{U}(S)$, entonces $x+u \in \mathcal{A}(S)$.*

LEMA 12.3. *Si $x \in S \setminus \mathcal{U}(S)$ y x no es irreducible, entonces $x+y$ no es irreducible para todo $y \in S$.*

DEMOSTRACIÓN. Por el Lema 12.1, existe $z \notin \mathcal{U}(S)$ tal que $x+S \subsetneq z+S$. Así, $x+y+S \subseteq x+S \subsetneq z+S$, de donde $x+y \notin \mathcal{A}(S)$. □

Usando estos lemas, ya estamos en condiciones de dar la primera de las caracterizaciones de monoide atómico finitamente generado.

PROPOSICIÓN 12.4. *El monoide S es atómico si y sólo si $\{s_1, \ldots, s_r\} \subseteq \mathcal{A}(S)$.*

DEMOSTRACIÓN. *Necesidad.* Tomemos $i \in \{1, \ldots, r\}$. Entonces $s_i \in S \setminus \mathcal{U}(S)$ y por tanto existen $a_1, \ldots, a_k \in \mathcal{A}(S)$ tales que $s_i = a_1 + \cdots + a_k$, debido a que S es atómico. Ya que $\{s_1, \ldots, s_p\}$ es sistema minimal de generadores de S, existe $j \in \{1, \ldots, k\}$ tal que $a_j = s_i + s$ para algún $s \in S$. Como $a_j = s_i + s$ es irreducible, el Lema 12.3 nos asegura que s_i es también irreducible.

Suficiencia. Tomemos $s \in S \setminus \mathcal{U}(S)$. Entonces $s = a_1 s_1 + \cdots + a_p s_p$ para algún $a_1, \ldots, a_p \in \mathbb{N}$ y existe $i \in \{1, \ldots, r\}$ tal que $a_i \neq 0$. Sea $u = a_{r+1} s_{r+1} + \cdots + a_p s_p$. Claramente $u \in \mathcal{U}(S)$ y por el Corolario 12.2, tenemos que $s_i + u \in \mathcal{A}(S)$. Llegamos así a que

$$s = a_1 s_1 + \cdots + a_{i-1} s_{i-1} + (a_i - 1) s_i + a_{i+1} s_{i+1} + \cdots + a_r s_r + (s_i + u) \in \langle \mathcal{A}(S) \rangle,$$

por lo que S es atómico. □

Lo que haremos ahora será intentar transformar esta caracterización en otra más fácilmente comprobable.

LEMA 12.5. *Si x es irreducible, entonces $x \simeq s_i$ para algún $i \in \{1, \ldots, r\}$.*

DEMOSTRACIÓN. Tenemos que $x \in \mathcal{A}(S)$, por lo que $x \notin \mathcal{U}(S)$ y ha de existir $i \in \{1, \ldots, r\}$ tal que $x = s_i + s$ para algún $s \in S$. Por tanto $x+S \subseteq s_i+S$ y $s_i \notin \mathcal{U}(S)$, lo cual, por el Lema 12.1, implica que $x+S = s_i+S$. □

LEMA 12.6. *Sea $i \in \{1, \ldots, r\}$. Las siguientes condiciones son equivalentes:*

(1) $s_i \notin \mathcal{A}(S)$,
(2) existe $j \in \{1, \ldots, r\}$ *tal que* $s_i + S \subsetneq s_j + S$.

DEMOSTRACIÓN. *(1) implica (2).* Por el Lema 12.1, existe $x \notin \mathcal{U}(S)$ tal que $s_i + S \subsetneq x + S$. Como $x \notin \mathcal{U}(S)$, existe $j \in \{1, \ldots, r\}$ tal que $x = s_j + s$ para algún $s \in S$. Por tanto $s_i + S \subsetneq x + S \subseteq s_j + S$.

(2) implica (1). Es consecuencia inmediata del Lema 12.1. □

Ya estamos en condiciones de dar una caracterización alternativa a la condición de ser monoide atómico. A partir de ella obtendremos un procedimiento que nos dirá cuando un monoide finitamente generado es o no atómico.

TEOREMA 12.7. *Sea S un monoide finitamente generado con sistema minimal de generadores $A = \{s_1, \ldots, s_p\}$ y tal que $\mathcal{U}(S) \cap A = \{s_{r+1}, \ldots, s_p\}$. Las siguientes condiciones son equivalentes:*

(1) S es atómico,
(2) para todo $i, j \in \{1, \ldots, r\}$, si $s_i | s_j$, entonces $s_j | s_i$.

DEMOSTRACIÓN. *(1) implica (2).* Si $s_i | s_j$, entonces $s_j = s_i + s$ para algún $s \in S$. Por ello $s_j + S \subseteq s_i + S$. Usando la Proposición 12.4 y el Lema 12.1, obtenemos que $s_j + S = s_i + S$, de donde $s_i \in s_j + S$, o equivalentemente $s_j | s_i$.

(2) implica (1). Veamos que para todo $i \in \{1, \ldots, r\}$, se tiene que $s_i \in \mathcal{A}(S)$, lo cual por la Proposición 12.4 significa que S es atómico. Supongamos que $s_i \notin \mathcal{A}(S)$. El Lema 12.6 nos dice que existe $j \in \{1, \ldots, r\}$ tal que $s_i + S \subsetneq s_j + S$. Esto implica que $s_j | s_i$. Por hipótesis $s_i | s_j$ y por ello $s_j + S \subseteq s_i + S \subsetneq s_j + S$, lo cual es una contradicción. □

Sea $S = \langle s_1, \ldots, s_p \rangle$ y ρ una presentación de un monoide S como en los preliminares. El que se tenga que $s_i | s_j$ para algún i, j es lo mismo que $[e_j]_\sigma \in [e_i]_\sigma + \mathbb{N}^p/\sigma$. Para comprobar ésto sólo hemos de ver si $(e_i, e_j) \in \sigma_{\mathcal{R}_{e_i}}$, con $\sigma_{\mathcal{R}_{e_i}}$ la congruencia de Rees asociada al ideal $[e_i]_\sigma + \mathbb{N}^p/\sigma$ (ver Capítulo 11, Sección 3). Recordemos de nuevo que un sistema de generadores κ_i de $\sigma_{\mathcal{R}_{e_i}}$ se obtenía calculando un sistema canónico de generadores a partir de

$$\rho_{\mathcal{R}_{l_i}} = \{(e_i + e_1, e_i), \ldots, (e_i + e_p, e_i)\} \cup \rho.$$

ALGORITMO 12.8. Sea ρ un subconjunto finito de $\mathbb{N}^p \times \mathbb{N}^p$ tal que si σ es la congruencia que genera, entonces el conjunto $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$. El algoritmo nos devuelve "VERDADERO" si $\mathbb{N}^p/\sigma$ es atómico, y "FALSO" en otro caso.

(1) Calcular $U = \{i \mid [e_i]_\sigma \notin \mathcal{U}(\mathbb{N}^p/\sigma)\}$.
(2) Para todo $i \in U$, calcular un sistema canónico de generadores κ_i de $\rho_{\mathcal{R}_{e_i}}$.
(3) Para todo $i, j \in U$,
    si $\mathrm{NF}_{\kappa_i}(e_i) = \mathrm{NF}_{\kappa_i}(e_j)$, entonces
        si $\mathrm{NF}_{\kappa_j}(e_i) \neq \mathrm{NF}_{\kappa_j}(e_j)$, devolver "FALSO".
(4) Devolver "VERDADERO".

□

EJEMPLO 12.9. Sea S el monoide $\mathbb{N}^3/\sigma$, donde σ está generada por

$$\rho = \{((2,0,0),(0,1,1)),((1,1,0),(3,0,1))\}.$$

El conjunto $A = \{[e_1]_\sigma, [e_2]_\sigma, [e_3]_\sigma\}$ es un sistema minimal de generadores de S (ver Capítulo 1) y $\mathcal{U}(S) \cap A = \emptyset$. Los conjuntos $\rho_{\mathcal{R}_{e_i}}$ son

$$\rho_{\mathcal{R}_{e_1}} = \{((2,0,0),(1,0,0)),((1,1,0),(1,0,0)),((1,0,1),(1,0,0))\} \cup \rho,$$
$$\rho_{\mathcal{R}_{e_2}} = \{((1,1,0),(0,1,0)),((0,2,0),(0,1,0)),((0,1,1),(0,1,0))\} \cup \rho,$$
$$\rho_{\mathcal{R}_{e_3}} = \{((1,0,1),(0,0,1)),((0,1,1),(0,0,1)),((0,0,2),(0,0,1))\} \cup \rho,$$

Calculando un sistema canónico de generadores de σ_i para $i \in \{1,2,3\}$ con respecto a un orden lineal admisible fijado de $\mathbb{N}^3$ y usando la función NF, obtenemos que $(e_i, e_j) \notin \sigma_{\mathcal{R}_{e_i}}$ para $i \neq j$ y por tanto $\mathbb{N}^3/\sigma$ es atómico por el Teorema 12.7. □

EJEMPLO 12.10. Tomemos ahora

$$\rho = \{((1,0,0),(1,1,0)),((0,0,3),(0,0,0))\}.$$

En este cado $A = \{[e_1]_\sigma, [e_2]_\sigma, [e_3]_\sigma\}$ es de nuevo un sistema minimal de generadores de S, pero $\mathcal{U}(S) \cap A = \{[e_3]_\sigma\}$. Por tanto sólo hemos de tomar en cuenta $\sigma_{\mathcal{R}_{e_1}}$ y $\sigma_{\mathcal{R}_{e_2}}$, los cuales están generados por

$$\{((1,0,0),(1,1,0)),((0,0,3),(0,0,0)),$$
$$((2,0,0),(1,0,0)),((1,1,0),(1,0,0)),((1,0,1),(1,0,0))\},$$
$$\{((1,0,0),(1,1,0)),((0,0,3),(0,0,0)),$$
$$((1,1,0),(0,1,0)),((0,2,0),(0,1,0)),((0,1,1),(0,1,0))\},$$

respectivamente. Aquí obtenemos que $(e_2, e_1) \notin \sigma_{\mathcal{R}_{e_1}}$, lo que significa que $[e_1]_\sigma \not| [e_2]_\sigma$. Sin embargo $(e_1, e_2) \in \sigma_{\mathcal{R}_{e_2}}$ ó equivalentemente $[e_2]_\sigma | [e_1]_\sigma$. Usando el Teorema 12.7 obtenemos que S no es atómico. □

EJEMPLO 12.11. Si en el anterior ejemplo modificamos ligeramente ρ y tomamos

$$\{((1,0,0),(1,1,0)),((0,1,1),(0,0,0))\},$$

entonces A sigue siendo un sistema minimal de generadores y $\mathcal{U}(S) = \langle [e_2]_\sigma, [e_3]_\sigma \rangle$. Ya que en este caso el entero r que aparece en el Teorema 12.7 es igual a uno, obtenemos que S es trivialmente atómico. □

3. Monoide reducido asociado a un monoide

En esta sección vemos que algunas de las propiedades concernientes a elementos irreducibles de un monoide S pueden estudiarse en el monoide que se obtiene a partir de S eliminando sus unidades. Esto será útil en las siguientes secciones y capítulos, ya que nos permitirá suponer que los monoides que tenemos son siempre reducidos.

Sea S un monoide. Sobre S definimos las relación binaria R definida por xRy, si existe $u, v \in \mathcal{U}(S)$ tal que $x + u = y + v$. Es fácil probar que R es una congruencia sobre S. Al monoide S/R lo denotaremos por $S/\mathcal{U}(S)$ y nos referiremos a él como el **monoide reducido asociado** a S.

LEMA 12.12. *El monoide $S/\mathcal{U}(S)$ es reducido.*

DEMOSTRACIÓN. Tomemos $[x]_R, [y]_R \in S/\mathcal{U}(S)$ tales que $[x]_R + [y]_R = [0]_R$. Entonces existen $u, v \in \mathcal{U}(S)$ tales que $x + y + u = 0 + v$, de donde $x + y \in \mathcal{U}(S)$ y por tanto, x como y son unidades de S, lo que significa que $[x]_R = [y]_R = [0]_R$. □

A continuación veremos que S es atómico si y sólo si $S/\mathcal{U}(S)$ es atómico. Antes necesitamos probar un par de resultados que nos indican la relación existente entre los átomos de S y los de su monoide reducido asociado.

LEMA 12.13. *Para todo $x, y \in S$, $x \simeq y$ si y sólo si $[x]_R \simeq [y]_R$ (en $S/\mathcal{U}(S)$).*

DEMOSTRACIÓN. Claramente, si $x + S = y + S$, entonces $[x]_R + S/\mathcal{U}(S) = [y]_R + S/\mathcal{U}(S)$.

Recíprocamente, tomemos $x + s \in x + S$. Entonces $[x]_R + [s]_R \in [x]_R + S/\mathcal{U}(S) = [y]_R + S/\mathcal{U}(S)$, lo que implica que $[x]_R + [s]_R = [y]_R + [z]_R$ para algún $z \in S$. Así, existen $u, v \in \mathcal{U}(S)$ tales que $x + s + u = y + z + v$, de donde $x + s = y + z + v - u$ con $v - u \in S$ y por tanto $x + s \in y + S$. La otra inclusión se prueba de la misma forma. □

LEMA 12.14. *El conjunto $\mathcal{A}(S/\mathcal{U}(S))$ es igual a $\{[x]_R \mid x \in \mathcal{A}(S)\}$.*

DEMOSTRACIÓN. Sea $[x]_R \in \mathcal{A}(S/\mathcal{U}(S))$. Probemos que $x \in \mathcal{A}(S)$. Supongamos que $y|x$ para algún $y \in S$. Entonces $x = y + z$ para algún $z \in S$, de donde $[x]_R = [y]_R + [z]_R$ y como $[x]_R$ es irreducible, ó bien $[y]_R \in \mathcal{U}(S/\mathcal{U}(S))$ ó $[x]_R \simeq [y]_R$. Aplicando los Lemas 12.12 y 12.13, llegamos a que $y \in \mathcal{U}(S)$ ó a que $x \simeq y$. □

PROPOSICIÓN 12.15. *El monoide S es atómico si y sólo si su monoide reducido asociado es atómico.*

DEMOSTRACIÓN. *Necesidad.* Sea $[x]_R \in S/\mathcal{U}(S)$, con $[x]_R \neq [0]_R$. Veamos que $[x]_R \in \langle \mathcal{A}(S/\mathcal{U}(S)) \rangle$. Como $[x]_R \neq [0]_R$, entonces $x \notin \mathcal{U}(S)$ y por tanto $x \in \langle \mathcal{A}(S) \rangle$. Así tenemos que existen $a_1, \ldots, a_k \in \mathcal{A}(S)$ tales que $x = a_1 + \cdots + a_k$. Esto hace que $[x]_R = [a_1]_R + \cdots + [a_k]_R$, y por el Lema 12.14, $[a_1]_R, \ldots, [a_k]_R \in \mathcal{A}(S/\mathcal{U}(S))$.

Suficiencia. Tomemos $s \in S \setminus \mathcal{U}(S)$ y veamos que $x \in \langle \mathcal{A}(S) \rangle$. Ya que $x \in S \setminus \mathcal{U}(S)$, $[x]_R \neq [0]_R$ y $S/\mathcal{U}(S)$ es reducido, tenemos que existen $[a_1]_R, \ldots, [a_k]_R \in \mathcal{A}(S/\mathcal{U}(S))$ tales que $[x]_R = [a_1]_R + \cdots + [a_k]_R$, de donde $x + u = a_1 + \cdots + a_k + v$ para algún $u, v \in \mathcal{U}(S)$. Obsérvese que $x = a_1 + \cdots + a_{k-1} + (a_k + v - u)$. Por el Lema 12.14, $a_1, \ldots, a_k \in \mathcal{A}(S)$ y como $v - u \in \mathcal{U}(S)$, el Corolario 12.2 nos dice que $a_k + v - u \in \mathcal{A}(S)$ y por tanto $x \in \langle \mathcal{A}(S) \rangle$. □

Si S es un monoide atómico, entonces todo elemento $x \in S \setminus \mathcal{U}(S)$ tiene una descomposición de la forma $x = a_1 + \cdots + a_k$ con $a_1, \ldots, a_k \in \mathcal{A}(S)$. El entero k es conocido como la **longitud** de la descomposición. Denotamos por $\mathrm{L}_S(x)$ el conjunto de longitudes de las descomposiciones de x en S. Como consecuencia de la demostración realizada de la Proposición 12.15, obtenemos el siguiente resultado.

COROLARIO 12.16. *Si S es atómico y $x \in S \setminus \mathcal{U}(S)$, entonces*

$$\mathrm{L}_S(x) = \mathrm{L}_{S/\mathcal{U}(S)}([x]_R).$$

Otra de las consecuencias de los Lemas 12.13 y 12.14 y la Proposición 12.15 es la siguiente.

COROLARIO 12.17. *Sea S un monoide atómico. Entonces*

(1) S es semifactorial si y sólo si $S/\mathcal{U}(S)$ es semifactorial,
(2) S es factorial si y sólo $S/\mathcal{U}(S)$ es factorial.

Como el lector puede esperar, dado un sistema minimal de generadores de S, podemos obtener un sistema minimal de generadores de $S/\mathcal{U}(S)$ simplemente tomando las clases de los elementos de este sistema de generadores que no pertenezcan al grupo de unidades de S.

PROPOSICIÓN 12.18. *Sea S un monoide con sistema minimal de generadores $\{s_1,\ldots,s_p\}$ y supongamos que $\mathcal{U}(S)\cap\{s_1,\ldots,s_p\}=\{s_{r+1},\ldots,s_p\}$. Entonces el conjunto $\{[s_1]_R,\ldots,[s_r]_R\}$ es un sistema minimal de generadores de $S/\mathcal{U}(S)$.*

DEMOSTRACIÓN. En primer lugar probemos que $\{[s_1]_R,\ldots,[s_r]_R\}$ es un sistema minimal de generadores de $S/\mathcal{U}(S)$. Tomemos $[x]_R\in S/\mathcal{U}(S)$. Entonces

$$x=a_1s_1+\cdots+a_rs_r+a_{r+1}s_{r+1}+\cdots+a_ps_p$$

para algún $(a_1,\ldots,a_p)\in\mathbb{N}^p$. Por tanto $x=a_1s_1+\cdots+a_rs_r+u$ con $u\in\mathcal{U}(S)$ y así $[x]_R=a_1[s_1]_R+\cdots+a_r[s_r]_R$.

Supongamos ahora que existe $i\in\{1,\ldots,r\}$ tal que

$$[s_i]_R=a_1[s_1]_R+\cdots+a_{i-1}[s_{i-1}]_R+a_{i+1}[s_{i+1}]_R+\cdots+a_r[s_r]_R$$

para algunos $a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_p\in\mathbb{N}$. Entonces

$$s_i=a_1s_1+\cdots+a_{i-1}s_{i-1}+a_{i+1}s_{i+1}+\cdots+a_rs_r+u$$

para algún $u\in\mathcal{U}(S)$. Como $u\in\mathcal{U}(S)$, existen $a_{r+1},\ldots,a_p\in\mathbb{N}$ tales que $u=a_{r+1}s_{r+1}+\cdots+a_ps_p$ y entonces

$$s_i=a_1s_1+\cdots+a_{i-1}s_{i-1}+a_{i+1}s_{i+1}+\cdots+a_rs_r+a_{r+1}s_{r+1}+\cdots+a_ps_p,$$

lo que contradice el que $\{s_1,\ldots,s_p\}$ sea un sistema minimal de generadores de S. □

Finalizamos esta sección explicando un método para encontrar una presentación de $S/\mathcal{U}(S)$ una vez conocida una presentación de S. Supongamos que $\{s_1,\ldots,s_p\}$ es un sistema minimal de generadores de S y que $\rho\subset\mathbb{N}^p\times\mathbb{N}^p$ es una presentación de S. Entonces S es isomorfo a $\mathbb{N}^p/\sigma$, donde σ es la congruencia generada por ρ. Ya sabemos que si $\mathcal{U}(S)\cap\{s_1,\ldots,s_p\}=\{s_{r+1},\ldots,s_p\}$, entonces un sistema minimal de generadores de $S/\mathcal{U}(S)$ es $\{s_1,\ldots,s_r\}$. En consecuencia hemos de buscar un conjunto $\overline{\rho}$ tal que $S/\mathcal{U}(S)$, ó equivalentemente $(\mathbb{N}^p/\sigma)/(\mathcal{U}(\mathbb{N}^p/\sigma))$, sea isomorfo a $\mathbb{N}^r/\overline{\sigma}$ con $\overline{\sigma}=\langle\overline{\rho}\rangle$. Sabemos que $\overline{\sigma}$ es justamente la congruencia núcleo del morfismo

$$\overline{\varphi}:\mathbb{N}^r\to S/\mathcal{U}(S),\ \overline{\varphi}(a_1,\ldots,a_r)=a_1[s_1]_R+\cdots+a_r[s_r]_R.$$

Dado $X\subseteq\mathbb{N}^{n+k}\times\mathbb{N}^{n+k}$ y $X'\subseteq\mathbb{N}^n\times\mathbb{N}^n$, recuérdese que X' es la proyección de X sobre $\mathbb{N}^n$ si se cumple la siguiente condición:

(*) $((x_1,\dots,x_n),(y_1,\dots,y_n)) \in X'$ si y sólo si existen

$$x_{n+1},\dots,x_{n+k},y_{n+1},\dots,y_{n+k}$$

tales que

$$((x_1,\dots,x_n,x_{n+1},\dots,x_{n+k}),(y_1,\dots,y_n,y_{n+1},\dots,y_{n+k})) \in X.$$

Puede probarse que si R es una congruencia sobre $\mathbb{N}^{n+k}$ y R' es su proyección sobre $\mathbb{N}^n$, entonces R' es de nuevo una congruencia sobre $\mathbb{N}^n$. Además, si γ es un sistema de generadores de R, entonces su proyección γ' sobre $\mathbb{N}^n$ es un sistema de generadores de R' (véase [**72**] ó [**65**]).

A continuación vemos que $\overline{\sigma}$ es precisamente la proyección de σ sobre $\mathbb{N}^r$.

PROPOSICIÓN 12.19. *La congruencia $\overline{\sigma}$ es la proyección de σ sobre $\mathbb{N}^r$.*

DEMOSTRACIÓN. Debemos probar que el par σ, $\overline{\sigma}$ cumple la condición (*).

Necesidad. Supongamos que $(x_1,\dots,x_r)\overline{\sigma}(y_1,\dots,y_r)$. Entonces

$$x_1[s_1]_{\overline{\sigma}}+\cdots+x_r[s_r]_{\overline{\sigma}} = y_1[s_1]_{\overline{\sigma}}+\cdots+y_r[s_r]_{\overline{\sigma}}$$

y por tanto existen $u,v \in \mathcal{U}(S)$ tales que

$$x_1s_1+\cdots+x_rs_r+u = y_1s_1+\cdots+y_rs_r+v.$$

Como $u,v \in \mathcal{U}(S)$, existen elementos $x_{r+1},\dots,x_p,y_{r+1},\dots,y_p$ verificando que $u = x_{r+1}s_{r+1}+\cdots+x_ps_p$ y $v = y_{r+1}s_{r+1}+\cdots+y_ps_p$. Así,

$$x_1s_1+\cdots+x_rs_r+x_{r+1}s_{r+1}+\cdots+x_ps_p = y_1s_1+\cdots+y_rs_r+y_{r+1}s_{r+1}+\cdots+y_ps_p$$

y por consiguiente $(x_1,\dots,x_r,x_{r+1},\dots,x_p)\sigma(y_1,\dots,y_r,y_{r+1},\dots,y_p)$.

Suficiencia. Si $(x_1,\dots,x_r,x_{r+1},\dots,x_p)\sigma(y_1,\dots,y_r,y_{r+1},\dots,y_p)$, entonces

$$x_1s_1+\cdots+x_rs_r+x_{r+1}s_{r+1}+\cdots+x_ps_p = y_1s_1+\cdots+y_rs_r+y_{r+1}s_{r+1}+\cdots+y_ps_p$$

donde tanto $x_{r+1}s_{r+1}+\cdots+x_ps_p$ como $y_{r+1}s_{r+1}+\cdots+y_ps_p$ pertenecen a $\mathcal{U}(S)$, lo que hace que $x_1[s_1]_{\overline{\sigma}}+\cdots+x_r[s_r]_{\overline{\sigma}} = y_1[s_1]_{\overline{\sigma}}+\cdots+y_r[s_r]_{\overline{\sigma}}$, o equivalentemente $(x_1,\dots,x_r)\overline{\sigma}(y_1,\dots,y_r)$. □

4. Monoides cancelativos finitamente generados

Nuestro objetivo en esta sección es particularizar los resultados obtenidos hasta el momento al caso de monoides cancelativos y finitamente generados. Una de las ventajas de trabajar con este tipo de monoides es que los algoritmos y resultados que se obtienen para ellos son mucho más fáciles de implementar y de demostrar. Otra característica muy importante que cumplen estos monoides es que son siempre atómicos.

Dejamos al lector la demostración del siguiente resultado.

LEMA 12.20. *Si S es un monoide cancelativo, entonces también lo es $S/\mathcal{U}(S)$.*

Esta propiedad hace que para estudiar elementos irreducibles de monoides cancelativos podamos restringirnos a estudiar sólo monoides cancelativos reducidos. Como vamos a ver a continuación, esta restricción simplifica bastante la caracterización de elemento irreducible

LEMA 12.21. *Si S es un monoide cancelativo reducido y $x \simeq y$ para algún $x, y \in S$, entonces $x = y$.*

DEMOSTRACIÓN. Si $x \simeq y$, entonces $x = y + a$ e $y = x + b$ para algún $a, b \in S$. Entonces $x = y + a = x + b + a$ y como S es cancelativo, $a + b = 0$. Aplicando ahora que S también es reducido, obtenemos que $a = b = 0$ y por tanto $x = y$. □

PROPOSICIÓN 12.22. *Sea S un monoide cancelativo y reducido. Tomemos $x \in S \setminus \{0\}$. Las siguientes condiciones son equivalentes:*

(1) $x \in \mathcal{A}(S)$,
(2) si $x = a + b$, *entonces* $a = 0$ *ó* $b = 0$.

DEMOSTRACIÓN. Se tiene usando la definición de elemento irreducible, el Lema 12.21 y el que S es reducido. □

A partir de la proposición anterior, el Lema 12.14 y la definición de $S/\mathcal{U}(S)$ obtenemos la siguiente consecuencia.

COROLARIO 12.23. *Sea S un monoide cancelativo y x un elemento de $S \setminus \mathcal{U}(S)$. Las siguientes condiciones son equivalentes:*

(1) $x \in \mathcal{A}(S)$,
(2) si $x = a + b$, *entonces* $a \in \mathcal{U}(S)$ *ó* $b \in \mathcal{U}(S)$.

TEOREMA 12.24. *Sea S un monoide cancelativo reducido con sistema minimal de generadores $\{s_1, \ldots, s_p\}$. Entonces S es atómico y además $\mathcal{A}(S) = \{s_1, \ldots, s_p\}$.*

DEMOSTRACIÓN. Veamos que $\{s_1, \ldots, s_p\} \subseteq \mathcal{A}(S)$. Si para algún s_i se tiene que $s_i = x + y$, entonces como $\{s_1, \ldots, s_p\}$ es un sistema minimal de generadores, deducimos que ó bien $x \in s_i + S$ ó $y \in s_i + S$. Sin pérdida de generalidad, podemos suponer que $x \in s_i + S$. Entonces $x = s_i + z$ para algún $z \in S$ y $s_i = s_i + z + y$, lo que hace que $z + y = 0$. Usando ahora el que S es reducido, obtenemos que $y = 0$ y, por la Proposición 12.22, $s_i \in \mathcal{A}(S)$.

Probemos ahora que $\mathcal{A}(S) \subseteq \{s_1, \ldots, s_p\}$. Si $x \in \mathcal{A}(S)$, entonces $x \neq 0$ y por tanto existe $i \in \{1, \ldots, p\}$ e $y \in S$ tal que $x = s_i + y$. Por la Proposición 12.22 obtenemos que $y = 0$ y por tanto $x = s_i$.

El que S es atómico es consecuencia directa de la Proposición 12.4. □

Por la Proposición 12.15, S es atómico si y sólo si $S/\mathcal{U}(S)$ es atómico. Sabemos que si S es cancelativo, entonces $S/\mathcal{U}(S)$ es cancelativo y reducido. Con estas dos ideas obtenemos la siguiente consecuencia.

COROLARIO 12.25. *Todo monoide finitamente generado y cancelativo es atómico.*

Pasamos a continuación a dar una serie de algoritmos que nos servirán para determinar propiedades factoriales de este tipo de monoides. El lector debe recordar que todo monoide cancelativo era de la forma $\mathbb{N}^p / \sim_M$ con M un subgrupo de $\mathbb{Z}^p$.

4.1. Cómo comprobar si $\{[e_1]_{\sim_M},\dots,[e_p]_{\sim_M}\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sim_M$. Estudiamos ahora el caso $\sigma=\sim_M$ (caso cancelativo) debido a que el método que obtendremos será mucho más fácil que el explicado en la Sección 1. Tal y como allí hicimos vamos a ver cómo comprobar si $[e_p]_{\sim_M}$ pertenece o no al monoide generado por $\{[e_1]_{\sim_M},\dots,[e_{p-1}]_{\sim_M}\}$ y, caso de pertenecer cómo eliminar el generador redundate $[e_p]_{\sim_M}$. Obsérvese que $[e_p]_{\sim_M}$ está en $\langle[e_1]_{\sim_M},\dots,[e_{p-1}]_{\sim_M}\rangle$ si y sólo si un elemento de la forma $(c_1,\dots,c_{p-1},-1)$, con $c_i\geq 0$, pertenece a M. Si

$$\begin{array}{rcl}
a_{11}x_1+\cdots+a_{1p}x_p & \equiv & 0\ (\mathrm{mod}\ d_1),\\
 & \vdots & \\
a_{r1}x_1+\cdots+a_{rp}x_p & \equiv & 0\ (\mathrm{mod}\ d_r),\\
a_{(r+1)1}x_1+\cdots+a_{(r+1)p}x_p & = & 0,\\
 & \vdots & \\
a_{(r+k)1}x_1+\cdots+a_{(r+k)p}x_p & = & 0,
\end{array}$$

son las ecuaciones que definen a M, entonces $(c_1,\dots,c_{p-1},-1)\in M$ si y sólo si el sistema de ecuaciones

$$\begin{array}{rcl}
a_{11}x_1+\cdots+a_{1(p-1)}x_{p-1} & \equiv & a_{1p}\ (\mathrm{mod}\ d_1),\\
 & \vdots & \\
a_{r1}x_1+\cdots+a_{rp}x_{p-1} & \equiv & a_{rp}\ (\mathrm{mod}\ d_r),\\
a_{(r+1)1}x_1+\cdots+a_{(r+1)(p-1)}x_{p-1} & = & a_{(r+1)p},\\
 & \vdots & \\
a_{(r+k)1}x_1+\cdots+a_{(r+k)(p-1)}x_{p-1} & = & a_{(r+k)p},
\end{array}$$

tiene una solución con todas sus coordenadas formadas por enteros no negativos, lo cual puede comprobarse usando los resultados que aparecen en [**85**]. Caso de que $[e_p]_{\sim_M}$ pertenezca a $\langle[e_1]_{\sim_M},\dots,[e_{p-1}]_{\sim_M}\rangle$, la aplicación

$$f:\mathbb{N}^{p-1}\to S,\ f(e_i)=[e_i]_{\sim_M},$$

es un epimorfismo cuyo núcleo es la congruencia τ definida por

$$(a_1,\dots,a_{p-1})\tau(b_1,\dots,b_{p-1}) \text{ si y sólo si } (a_1,\dots,a_{p-1},0)\sim_M(b_1,\dots,b_{p-1},0),$$

ó equivalentemente, $(a_1-b_1,\dots,a_{p-1}-b_{p-1},0)\in M$. Por tanto la congruencia τ es la congruencia $\sim_N$, donde N es el subgrupo de $\mathbb{N}^{p-1}$ definido por las ecuaciones

$$\begin{array}{rcl}
a_{11}x_1+\cdots+a_{1(p-1)}x_{p-1} & \equiv & 0\ (\mathrm{mod}\ d_1),\\
 & \vdots & \\
a_{r1}x_1+\cdots+a_{r(p-1)}x_{p-1} & \equiv & 0\ (\mathrm{mod}\ d_r),\\
a_{(r+1)1}x_1+\cdots+a_{(r+1)(p-1)}x_{p-1} & = & 0,\\
 & \vdots & \\
a_{(r+k)1}x_1+\cdots+a_{(r+k)(p-1)}x_{p-1} & = & 0
\end{array}$$

(otra forma de ver esto es que S es, por la Proposición 3.1 de **[65]**, isomorfo al submonoide de $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ generado por las columnas de las ecuaciones de M; así elimininar el generador $[e_p]_{\sim_M}$ equivale a eliminar la última columna de M).

Repitiendo el proceso obtendremos $\mathbb{N}^r / \sim_P$ con $\{[e_1]_{\sim_P}, \ldots, [e_r]_{\sim_P}\}$ un sistema minimal de generadores de $\mathbb{N}^r / \sim_P \cong S$.

Obsérvese que este procedimiento nos permite calcular el conjunto $\mathcal{A}(\mathbb{N}^p / \sim_M)$ para todo subgrupo M de $\mathbb{Z}^p$ (y por tanto, para todo monoide cancelativo y finitamente generado) una vez que conozcamos $\mathcal{U}(\mathbb{N}^p / \sim_M)$.

4.2. Cómo calcular $\mathcal{U}(\mathbb{N}^p / \sim_M)$ y $(\mathbb{N}^p / \sim_M)/\mathcal{U}(\mathbb{N}^p / \sim_M)$. Sea $x = (x_1, \ldots, x_p)$ un elemento de $M \cap \mathbb{N}^p$ con máximo número de coordenadas no nulas (este elemento puede ser calculado usando el algoritmo MCP que aparece en **[58]**). Tras reordenar coordenadas podemos suponer que $x_1 = \cdots = x_r = 0$ y que el resto de las coordenadas son no nulas. En este contexto puede probarse que $\mathcal{U}(\mathbb{N}^p / \sim_M)$ está generado por $\{[e_{r+1}]_{\sim_M}, \ldots, [e_p]_{\sim_M}\}$. Tomemos $\{m_1, \ldots, m_q\}$ una base de M y sea $\overline{M}$ el subgrupo de $\mathbb{Z}^r$ generado por los elementos $\{\overline{m}_1, \ldots, \overline{m}_q\}$, donde $\overline{m}_i$ es la proyección sobre las primeras r coordenadas de m_i. Por la Proposición 12.19, sabemos que $(\mathbb{N}^p / \sim_M)/\mathcal{U}(\mathbb{N}^p / \sim_M)$ es isomorfo a $\mathbb{N}^p / \overline{\sim_M}$ con $\overline{\sim_M}$ la proyección sobre $\mathbb{N}^r$ de la congruencia $\sim_M$. El lector puede comprobar que $\overline{\sim_M} = \sim_{\overline{M}}$.

4.3. Cómo comprobar si $\mathbb{N}^p / \sim_M$ es factorial. Como consecuencia del Lema 12.21, los conceptos de descomposición y factorización de un elemento en un monoide cancelativo y reducido coinciden. Con esta idea, es fácil probar el siguiente resultado.

PROPOSICIÓN 12.26. *Sea $S \cong \mathbb{N}^p / \sim_M$ un monoide cancelativo, reducido y finitamente generado con sistema minimal de generadores $\{[e_1]_{\sim_M}, \ldots, [e_p]_{\sim_M}\}$. Entonces S es factorial si y sólo si $M = 0$, esto es, $S \cong \mathbb{N}^p$.*

DEMOSTRACIÓN. Supongamos que $M \neq 0$. Ha de existir $(x_1, \ldots, x_p) \in M$ con $(x_1, \ldots, x_p) \neq 0$. Supongamos, sin perdida de generalidad, que $x_1 > 0$. Sea $a = x_1[e_1]_{\sim_M} + \text{máximo}\{x_2, 0\}[e_2]_{\sim_M} + \cdots + \text{máximo}\{x_p, 0\}[e_p]_{\sim_M}$ y $b = \max\{-x_2, 0\}[e_2]_{\sim_M} + \cdots + \max\{-x_p, 0\}[e_p]_{\sim_M}$. Tenemos entonces que $[a]_{\sim_M} = [b]_{\sim_M}$, el cual es un elemento con dos descomposiciones no asociadas. Así, el monoide $\mathbb{N}^p / \sim_M$ no es semifactorial.

Recíprocamente, si S no es factorial, han de existir dos descomposiciones no asociadas de un mismo elemento, digamos $a = n_1[e_1]_{\sim_M} + \cdots + n_p[e_p]_{\sim_M}$ y $a = m_1[e_1]_{\sim_M} + \cdots + m_p[e_p]_{\sim_M}$ con $n_i \neq m_i$ para algún $i \in \{1, \ldots, p\}$. Por consiguiente, $(m_1 - n_1, \ldots, m_p - n_p) \in M$ y $m_i - n_i \neq 0$. □

La Proposicion 12.26 puede usarse para comprobar si un monoide cancelativo y finitamente generado $\mathbb{N}^p / \sim_M$ es factorial tal y como explicamos a continuación.

(1) A partir de M calcular N como en 4.1. Obtenemos así que $\mathbb{N}^r / \sim_N$ es isomorfo a $\mathbb{N}^p / \sim_M$ y tal que $\{[e_1]_{\sim_N}, \ldots, [e_r]_{\sim_N}\}$ es un sistema minimal suyo.

(2) Usar 4.2 para obtener $\overline{N}$ tal que $(\mathbb{N}^r / \sim_N)/\mathcal{U}(\mathbb{N}^r / \sim_N)$ es isomorfo a $\mathbb{N}^s / \sim_{\overline{N}}$. Por el Corolario 12.17, $\mathbb{N}^p / \sim_M$ es factorial si y sólo si $\mathbb{N}^s / \sim_{\overline{N}}$ es factorial, lo que por la Proposición 12.26 ocurre si y sólo si $\overline{N} = 0$.

Como consecuencia de la Proposición 12.26 obtenemos el siguiente corolario.

COROLARIO 12.27. *Sea S un monoide cancelativo y finitamente generado. S es factorial si y sólo si existe un grupo finitamente generado y $r \in \mathbb{N}$ tal que $S \cong \mathbb{N}^r \times G$.*

EJEMPLO 12.28. Sea M el subgrupo de $\mathbb{Z}^3$ generado por

$$\{(-2,0,3),(0,0,4),(4,0,1)\}.$$

Sus ecuaciones son

$$x \equiv 0 (\mathrm{mod}\ 2),$$
$$y = 0.$$

Un elemento con el máximo número de coordenadas positivas de M es $(2,0,1)$ y por tanto $\mathcal{U}(\mathbb{N}^3 / \sim_M) = \{[e_1]_{\sim_M}, [e_3]_{\sim_M}\}$. Como la ecuación $y = 0$ es una de las ecuaciones de M, tenemos que $\mathbb{N}^3 / \sim_M$ es un monoide factorial isomorfo a $\mathbb{N} \times \mathcal{U}(\mathbb{N}^3 / \sim_M)$. También podemos ver esto directamente si usamos la Proposición 3.1 de 12.22, la cual nos dice que $\mathbb{N}^3 / \sim_M$ es isomorfo al submonoide de $\mathbb{Z}_2 \times \mathbb{Z}$ generado por las "columnas" de las ecuaciones de M, lo que en este caso significa que $\mathbb{N}^3 / \sim_M$ es el submonoide de $\mathbb{Z}_2 \times \mathbb{Z}$ generado por $\{(1,0),(0,1)\}$ y por tanto $\mathbb{N}^3 / \sim_M$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{N}$. □

4.4. Como comprobar si $\mathbb{N}^p / \sigma$ es semifactorial. De manera análoga al resultado 12.26 podemos dar un resultado concerniente al hecho de ser semifactorial.

PROPOSICIÓN 12.29. *Sea $S \cong \mathbb{N}^p / \sim_M$ un monoide finitamente generado, cancelativo y reducido con sistema minimal de generadores $\{[e_1]_{\sim_M}, \ldots, [e_p]_{\sim_M}\}$. El monoide S es semifactorial si y sólo si para todo $(x_1, \ldots, x_p) \in M$ se tiene que $x_1 + \cdots + x_p = 0$.*

DEMOSTRACIÓN. Si existe $(a_1, \ldots, a_p) \in M$ tal que $a_1 + \cdots + a_p \neq 0$, entonces $\max\{a_1, 0\}[e_1]_{\sim_M} + \cdots + \max\{a_p, 0\}[e_p]_{\sim_M}$ y $\max\{-a_1, 0\}[e_1]_{\sim_M} + \cdots + \max\{-a_p, 0\}[e_p]_{\sim_M}$ son dos elementos asociados que tienen descomposiciones de diferentes longitudes.

Supongamos ahora que para todo $(x_1, \ldots, x_p) \in M$, $x_1 + \cdots + x_r = 0$, y que $n_1[e_1]_{\sim_M} + \cdots + n_p[e_p]_{\sim_M} = m_1[e_1]_{\sim_M} + \cdots + m_p[e_p]_{\sim_M}$ para algún $n_i, m_i \in \mathbb{N}$. Entonces $(m_1 - n_1, \ldots, m_p - n_p) \in M$ y por tanto $m_1 + \cdots + m_r = n_1 + \cdots + n_r$. □

El procedimiento para ver si $\mathbb{N}^p / \sim_M$ es semifactorial es el siguiente.

(1) A partir de M, procediendo como en 4.1, calcular N tal que $\mathbb{N}^r / \sim_N$ es isomorfo a $\mathbb{N}^p / \sim_M$ y $\{[e_1]_{\sim_N}, \ldots, [e_r]_{\sim_N}\}$ sea un sistema minimal de generadores de $\mathbb{N}^r / \sim_N$.
(2) Usar 4.2 para obtener $\overline{N}$ tal que $(\mathbb{N}^r / \sim_N)/\mathcal{U}(\mathbb{N}^r / \sim_N)$ sea isomorfo a $\mathbb{N}^s / \sim_{\overline{N}}$. Por el Corolario 12.17, $\mathbb{N}^p / \sim_M$ es semifactorial si y sólo si $\mathbb{N}^s / \sim_{\overline{N}}$ es semifactorial. Por la Proposición 12.29 esto ocurre si y sólo si $\overline{N}$ satisface la ecuación $x_1 + \cdots + x_p = 0$. Para ver si esto se cumple sólo hemos de ver si un sistema de generadores de $\overline{N}$ lo cumple.

EJEMPLO 12.30. Sea M el subgrupo de $\mathbb{Z}^4$ generado por

$$\{(1,-2,2,-1),(-3,1,1,1)\}.$$

Un conjunto de ecuaciones que definen a M es

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

Usando 4.1, obtenemos que $\{[e_1]_{\sim_N},[e_2]_{\sim_N},[e_3]_{\sim_N},[e_4]_{\sim_N}\}$ es un sistema minimal de generadores de $\mathbb{N}^4/\sim_M$. Además, como $x_1+x_2+x_3+x_4=0$ es una ecuación de M, tenemos que $M\cap\mathbb{N}^4=\{0\}$ y por tanto $\mathcal{U}(\mathbb{N}^4/\sim_M)=\{0\}$. Por la Proposición 12.29 llegamos a que $\mathbb{N}^4/\sim_M$ es semifactorial. □

4.5. Cómo calcular $[a]_{\sim_M}\in\mathbb{N}^p/\sim_M$ para todo $a\in\mathbb{N}^p$. En el caso en el que $\mathbb{N}^p/\sim_M$ sea reducido, por el Teorema 12.24, calcular $[a]_{\sim_M}$ es equivalente a encontrar todas las posibles descomposiciones del elemento $[a]_{\sim_M}\in\mathbb{N}^p/\sim_M$, lo que por el Lema 12.21 significa encontrar todas las posibles factorizaciones de este elemento. Vemos a continuación un método para realizar esto.

Sean

$$\begin{aligned} \gamma_{11}x_1+\cdots+\gamma_{1p}x_p &\equiv 0 \pmod{\delta_1},\\ &\vdots\\ \gamma_{k1}x_1+\cdots+\gamma_{kp}x_p &\equiv 0 \pmod{\delta_k},\\ \gamma_{(k+1)1}x_1+\cdots+\gamma_{(k+1)p}x_p &= 0,\\ &\vdots\\ \gamma_{n}x_1+\cdots+\gamma_{np}x_p &= 0, \end{aligned}$$

las ecuaciones de M y $a=(a_1,\ldots,a_p)\in\mathbb{N}^p$. Para calcular $[a]_{\sim_M}$ hemos de encontrar los elementos $x=(x_1,\ldots,x_p)\in\mathbb{N}^p$ tales que $a-x\in M$. Estos elementos son exactamente aquellos $(x_1,\ldots,x_p)$ tales que

$$\begin{aligned} \gamma_{11}x_1+\cdots+\gamma_{1p}x_p &\equiv \gamma_{11}a_1+\cdots+\gamma_{1p}a_p \pmod{\delta_1},\\ &\vdots\\ \gamma_{k1}x_1+\cdots+\gamma_{kp}x_p &\equiv \gamma_{k1}a_1+\cdots+\gamma_{kp}a_p \pmod{\delta_k},\\ \gamma_{(k+1)1}x_1+\cdots+\gamma_{(k+1)p}x_p &= \gamma_{(k+1)1}a_1+\cdots+\gamma_{(k+1)p}a_p,\\ &\vdots\\ \gamma_{n1}x_1+\cdots+\gamma_{np}x_p &= \gamma_{n1}a_1+\cdots+\gamma_{np}a_p. \end{aligned}$$

Supongamos que

$$\begin{aligned} \gamma_{11}a_1+\cdots+\gamma_{1p}a_p &\equiv b_1 \pmod{\delta_1},\\ &\vdots\\ \gamma_{k1}a_1+\cdots+\gamma_{kp}a_p &\equiv b_k \pmod{\delta_k},\\ \gamma_{(k+1)1}a_1+\cdots+\gamma_{(k+1)p}a_p &= b_{k+1},\\ &\vdots\\ \gamma_{n}a_1+\cdots+\gamma_{np}a_p &= b_n \end{aligned}$$

Tenemos que calcular los elementos $(x_1,\dots,x_p)\in\mathbb{N}^p$ tales que

$$(1)\qquad \begin{array}{rcl} \gamma_{11}x_1+\cdots+\gamma_{1p}x_p & \equiv & b_1 \pmod{\delta_1},\\ & \vdots & \\ \gamma_{k1}x_1+\cdots+\gamma_{kp}x_p & \equiv & b_k \pmod{\delta_k},\\ \gamma_{(k+1)1}x_1+\cdots+\gamma_{(k+1)p}x_p & = & b_{k+1},\\ & \vdots & \\ \gamma_n x_1+\cdots+\gamma_{np}x_p & = & b_n \end{array}$$

En consecuencia podemos decir que el problema que tenemos es encontrar soluciones no negativas de este sistema de ecuaciones en congruencias. Podemos construir un nuevo sistema de ecuaciones:

$$(2)\qquad \begin{array}{rcl} \gamma_{11}x_1+\cdots+\gamma_{1p}x_p+\delta_1y_1-\delta_1z_1 & = & b_1,\\ & \vdots & \\ \gamma_{k1}x_1+\cdots+\gamma_{kp}x_p+\delta_ky_k-\delta_kz_k & = & b_k,\\ \gamma_{(k+1)1}x_1+\cdots+\gamma_{(k+1)p}x_p & = & b_{k+1},\\ & \vdots & \\ \gamma_{n1}x_1+\cdots+\gamma_{np}x_p & = & b_n. \end{array}$$

Claramente, si $(x_1,\dots,x_p)\in\mathbb{N}^p$ es una solución de (1), entonces existe $c_i\in\mathbb{Z}$ tal que $\gamma_{i1}x_1+\cdots+\gamma_{ip}x_p=b_i+c_i\delta_i$. Si $c_i<0$, entonces tomamos $y_i=-c_i$ y $z_i=0$, en otro caso $y_i=0$ y $z_i=c_i$, de donde $(x_1,\dots,x_p,y_1,\dots,y_k,z_1,\dots,z_k)$ es una solución de (2) con todos sus coordenadas no negativas. Supongamos ahora que $(x_1,\dots,x_p,y_1,\dots,y_t,z_1,\dots,z_k)$ es una solución de (2). Tenemos que $\gamma_{i1}x_1+\cdots+\gamma_{ip}x_p=b_i+(z_i-y_i)\delta_i$, lo cual hace que $(x_1,\dots,x_p)$ sea una solución de (1) si y sólo si es la proyección de una solución de (2). Para obtener el conjunto $[a]_{\sim_M}$, sólo hemos de calcular en conjunto de soluciones no negativos distintas de cero de (2) y proyectar estas soluciones sobre sus primeras p coordenadas (el cálculo de las soluciones de este último sistema de ecuaciones puede ser realizado usando los métodos que aparecen en [**22**]).

CAPÍTULO 13

Factorizaciones en monoides atómicos

Con el objeto de medir la desviación de un dominio atómico de ser semifactorial, Valenza introduce en [**84**] el concepto de elasticidad. Desde entonces, algunos artículos han aparecido en los que se estudia la elasticidad de un dominio (ver por ejemplo [**1, 2, 5**]).

En este capítulo estamos especialmente interesados en el cálculo de esta medida y en saber si un monoide dado tiene o no elasticidad aceptable (lo que significa que exista un elemento del monoide que alcance la elasticidad del mismo) y en particular, como consecuencia inmediata demostraremos que la elasticidad es siempre un número racional, resultado que se probó de forma independiente y utilizando ideas distintas en [**2**] y [**29**]. Como en el capítulo anterior, podremos suponer que nuestro monoide es reducido para estudiar con más facilidad sus propiedades. Aunque la mayoría del trabajo presentado en este capítulo se realiza con monoides finitamente generados, los resultados obtenidos pueden usarse en el caso no finitamente generado. Por ejemplo, usando el capítulo de Chapman y Geroldinger de [**6**], puede probarse que los conjunto de longitudes de factorizaciones en un dominio de Krull con grupo de clase de divisores finitamente generado coincide con el del monoide de bloques de un grupo abeliano finito, el cual por definición es un monoide cancelativo finitamente generado (y por tanto fuertemente reducido; en el siguiente capítulo veremos una aplicación en este tipo de monoides).

1. Monoides finitamente generados de elasticidad finita

Dado un monoide atómico S y $x \in S \setminus \mathcal{U}(S)$, la **elasticidad** de x se define como

$$\varepsilon(x) = \sup\left\{ \frac{m}{n} \;\middle|\; \begin{array}{l} \text{existen } a_1, \ldots, a_m, b_1, \ldots, b_n \in \mathcal{A}(S) \\ \text{con } x = a_1 + \cdots + a_m = b_1 + \cdots + b_n \end{array} \right\}$$

(sup denota el supremo). La **elasticidad del monoide** S es

$$\varepsilon(S) = \sup\{\varepsilon(x) \mid x \in S \setminus \mathcal{U}(S)\}.$$

Obsérvese que $\varepsilon(x) = \sup(\mathrm{L}_S(x))/\inf(\mathrm{L}_S(x))$ (inf denota el ínfimo; véase la definición de L_S en el capítulo anterior), lo que por el Corolario 12.16 implica que $\varepsilon(S) = \varepsilon(S/\mathcal{U}(S))$ y por tanto para el estudio de la elasticidad podemos restringirnos al caso reducido.

Dada una congruencia σ sobre $\mathbb{N}^p$, σ es un submonoide $\mathbb{N}^p \times \mathbb{N}^p$ y por tanto es cancelativo y reducido. Por la Proposición 12.22, un elemento $(a,b) \neq (0,0)$ de la congruencia σ es irreducible si no puede ser expresado de la forma $(a,b) =$

$(a_1,b_1)+(a_2,b_2)$ con $(a_1,b_1),(a_2,b_2) \in \sigma \setminus \{(0,0)\}$. El conjunto $\mathcal{A}(\sigma)$ es un sistema de generadores de σ como monoide. En [**65**] se muestra que en el caso en el que $\mathbb{N}^p/\sigma$ es cancelativo, entonces $\mathcal{A}(\sigma)$ (allí denotado por $\mathcal{I}_\sigma$) es finito y además se da un procedimiento para calcularlo (ver la Proposición 8.4 y el Corolario 8.8 de [**65**], los elementos irreducibles son calculados encontrando el conjunto minimal de soluciones no negativas de un sistema lineal de ecuaciones obtenido a partir de las ecuaciones de M_σ).

Una congruencia σ de $\mathbb{N}^p$ es **fuertemente reducida** si para todo $x, y \in \mathbb{N}^p$, $x+y\sigma x$ implica que $y=0$ (este concepto fue introducido en [**73**]). Obsérvese que si σ es fuertemente reducida, entonces $\mathbb{N}^p/\sigma$ es reducido. Una de las más importantes características de las congruencias fuertemente reducidas es la que damos en el siguiente resultado.

LEMA 13.1. *Sea σ una congruencia sobre $\mathbb{N}^p$. Entonces σ es fuertemente reducida si y sólo si para todo $x \in \mathbb{N}^p$, el conjunto $[x]_\sigma$ tiene un número finito de elementos.*

DEMOSTRACIÓN. *Necesidad.* Sean $a,b \in [x]_\sigma$. Supongamos que $a<b$ con respecto al orden parcial usual de $\mathbb{N}^p$. Entonces $b-a \in \mathbb{N}^p$ y por tanto $(b-a)+a = b\sigma a$, lo que hace que $b-a=0$, contradiciendo el que $a<b$. Así tenemos que todos los elementos de $[x]_\sigma$ son incomparables con respecto al orden $<$ y por el Lema de Dickson sólo hay un número finito de ellos.

Suficiencia. Si σ no es fuertemente reducido, entonces han de existir $x, y \in \mathbb{N}^p$ con $y \neq 0$ tales que $x+y\sigma x$. Por tanto $x+ky\sigma x$ para todo $k \in \mathbb{N}$ y así $[x]_\sigma$ tiene un número infinito de elementos. □

Otra propiedad importante de las congruencias fuertemente reducidas es que son congruencias σ para las que $\mathbb{N}^p/\sigma$ tiene elasticidad finita. Esto es lo que probaremos en el Teorema 13.6. Antes de hacer esto necesitamos algunos resultados previos.

Lo primero que vamos a probar es que para toda congruencia fuertemente reducida σ, el monoide $\mathbb{N}^p/\sigma$ es atómico.

Dado un elemento $x=(x_1,\ldots,x_p) \in \mathbb{N}^p$, denotaremos por $|x|$ al número $\sum_{i=1}^p x_i$.

PROPOSICIÓN 13.2. *Sea σ una congruencia fuertemente reducida sobre $\mathbb{N}^p$ tal que el conjunto $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$. Entonces*

(1) *para todo $a,b \in \mathbb{N}^p$, si $[a]_\sigma \simeq [b]_\sigma$, entonces $[a]_\sigma = [b]_\sigma$,*
(2) *$[e_i]_\sigma | [e_j]_\sigma$ implica $i=j$,*
(3) *$\mathbb{N}^p/\sigma$ es atómico,*
(4) *$\mathcal{A}(\mathbb{N}^p/\sigma) = \{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$,*
(5) *para todo $x \in \mathbb{N}^p \setminus \{0\}$,*

$$\varepsilon([x]_\sigma) = \sup\left\{\frac{|a|}{|b|} \mid a,b \in [x]\right\}.$$

DEMOSTRACIÓN. (1) Si $[a]_\sigma \simeq [b]_\sigma$, entonces $[a]_\sigma = [b]_\sigma + [c]_\sigma$ y $[b]_\sigma = [a]_\sigma + [d]_\sigma$ para algún $c, d \in \mathbb{N}^p$, de donde $[a]_\sigma = [a]_\sigma + [c+d]_\sigma$. Como σ es fuertemente reducida obtenemos que $c+d=0$, lo que hace que $c=d=0$.

(2) Supongamos que $[e_i]_\sigma | [e_j]_\sigma$ con $i \neq j$. Entonces $[e_j]_\sigma = [e_i]_\sigma + [x]_\sigma$. Ya que $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$, tenemos que $x \neq 0$ y que $[x]_\sigma = [e_j]_\sigma + [y]_\sigma$ para algún $y \in \mathbb{N}^p$. Así $[e_j]_\sigma = [e_j]_\sigma + [e_i]_\sigma + [y]_\sigma$ y como σ es fuertemente reducido, concluimos que $e_i + y = 0$, lo cual es imposible.

(3) Se obtiene como consecuencia de (1) del Teorema 12.7.

(4) Como $\mathbb{N}^p/\sigma$ es atómico y reducido, por la Proposición 12.4, tenemos que $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\} \subseteq \mathcal{A}(\mathbb{N}^p/\sigma)$. Para la otra inclusión, tomamos $[x]_\sigma \in \mathcal{A}(\mathbb{N}^p/\sigma)$. Por el Lema 12.5 existe $i \in \{1, \ldots, p\}$ tal que $[x]_\sigma \simeq [e_i]_\sigma$. Usando (1) deducimos que $[x]_\sigma = [e_i]_\sigma$.

(5) Se obtiene a partir de (3) y de la definición de $\varepsilon([x]_\sigma)$. Obsérvese que como $x \neq 0$ y σ es fuertemente reducido, tenemos $[x]_\sigma \in (\mathbb{N}^p/\sigma) \setminus \mathcal{U}(\mathbb{N}^p/\sigma)$.

□

PROPOSICIÓN 13.3. *Sea σ una congruencia sobre $\mathbb{N}^p$ tal que $\mathbb{N}^p/\sigma$ es un monoide atómico reducido con sistema minimal de generadores $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$. Si $\varepsilon(\mathbb{N}^p/\sigma)$ es finito, entonces σ es fuertemente reducida.*

DEMOSTRACIÓN. Supongamos que σ no es fuertemente reducida. Entonces existen $x, y \in \mathbb{N}^p$ (los cuales pueden tomarse distintos de cero al ser $\mathbb{N}^p/\sigma$ reducido) tales que $x + y \sigma y$. Claramente $kx + y \sigma y$ para todo $k \in \mathbb{N}$, llegando así a que $\varepsilon([y]_\sigma)$ es infinito. □

En vista de esta proposición, si queremos estudiar monoides atómicos finitamente generados con elasticidad finita, hemos de restringirnos a monoides de la forma $\mathbb{N}^p/\sigma$, con σ una congruencia fuertemente reducida.

LEMA 13.4. *Sea σ una congruencia sobre $\mathbb{N}^p$.*

(1) Si σ es fuertemente reducida, entonces para todo $x \in \mathbb{N}^p$ tal que $(x,0) \in \sim_{M_\sigma}$, se tiene que $x = 0$.

(2) Si $\mathbb{N}^p/\sigma$ es reducido y $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$, entonces para todo $x \in \mathbb{N}^p$ tal que $(x,0) \in \sigma$, se tiene $x = 0$.

DEMOSTRACIÓN. (1) Si $(x,0) \in \sim_{M_\sigma}$, entonces existe $y \in \mathbb{N}^p$ tal que $(x+y, y) \in \sigma$ (Lema 1.4) y como σ es fuertemente reducido, obtenemos que $x = 0$.

(2) Si $(x,0) \in \sigma$ con $x \neq 0$, entonces como $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$, tenemos que no existe $i \in \{1, \ldots, p\}$ cumpliendo que $(e_i, 0) \in \sigma$ y por tanto han de existir $i \in \{1, \ldots, p\}$ e $y \in \mathbb{N}^p \setminus \{0\}$ tales que $x = e_i + y$, llegando a que $[e_i]_\sigma + [y]_\sigma = [0]_\sigma$ y contradiciendo el que $\mathbb{N}^p/\sigma$ es reducido.

□

El lector puede probar fácilmente el siguiente resultado.

LEMA 13.5. *Sean $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{N} \setminus \{0\}$. Las siguientes afirmaciones son ciertas.*

(1) Si $\frac{a_1}{b_1} = \cdots = \frac{a_n}{b_n}$, *entonces*

$$\frac{a_1 + \cdots + a_n}{b_1 + \cdots + b_n} = \frac{a_1}{b_1}.$$

(2)

$$\frac{a_1 + \cdots + a_n}{b_1 + \cdots + b_n} \leq \max\{\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\}.$$

(3) Si existe $i \in \{1, \ldots, n\}$ *tal que* $\frac{a_i}{b_i} < \max\{\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\}$, *entonces*

$$\frac{a_1 + \cdots + a_n}{b_1 + \cdots + b_n} < \max\{\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\}.$$

Si σ es una congruencia fuertemente reducida, entonces como hemos visto al comienzo de esta sección, el conjunto $\mathcal{A}(\sim_{M_\sigma})$ tiene un número finito de elementos. Es más, por el Lema 13.4, para todo $(a,b) \in \mathcal{A}(\sim_{M_\sigma})$, se tiene que $b \neq 0$. Lo mismo se tiene para todo $(a,b) \in \sigma \setminus \{(0,0)\}$.

TEOREMA 13.6. *Sea* σ *una congruencia fuertemente reducida sobre* $\mathbb{N}^p$ *tal que* $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ *es un sistema minimal de generadores de* $\mathbb{N}^p/\sigma$. *Entonces* $\varepsilon(\mathbb{N}^p/\sigma)$ *es finito y además*

$$\varepsilon(\mathbb{N}^p/\sigma) = \max\left\{\frac{|\alpha|}{|\beta|} \mid (\alpha,\beta) \in \mathcal{A}(\sim_{M_\sigma})\right\}.$$

DEMOSTRACIÓN. Veamos primero que para todo $(a,b) \in \sigma \setminus \{(0,0)\}$ tenemos que $|a|/|b| \leq |\alpha|/|\beta|$ para algún $(\alpha,\beta) \in \mathcal{A}(\sim_{M_\sigma})$. Ya que $(a,b) \in \sigma$, tenemos $(a,b) \in \sim_{M_\sigma}$ y por tanto existen $(\alpha_1,\beta_1), \ldots, (\alpha_t,\beta_t) \in \mathcal{A}(\sim_{M_\sigma})$ tales que $(a,b) = \sum_{i=1}^t (\alpha_i,\beta_i)$. Por tanto $|a| \leq |b| = (\sum_{i=1}^t |\alpha_i|)/(\sum_{i=1}^t |\beta_i|)$, lo que por el Lema 13.5 es menor o igual que algún $|\alpha_i|/|\beta_i|$.

Tomemos ahora $(\alpha,\beta) \in \mathcal{A}(\sim_{M_\sigma})$ tal que $|\alpha|/|\beta| = \text{máximo}\{|\alpha|/|\beta| \mid (\alpha,\beta) \in \mathcal{A}(\sim_{M_\sigma})$. Debido a que para todo $(a,b) \in \sigma$ se tiene que $|a|/|b| \leq |\alpha|/|\beta|$, deducimos que $\varepsilon(\mathbb{N}^p/\sigma) \leq |\alpha| \leq |\beta|$. En particular esto prueba que la elasticidad de $\mathbb{N}^p/\sigma$ es finita. Para probar la otra desigualdad usamos un pequeño truco. Ya que $(\alpha,\beta) \in \sim_{M_\sigma}$, existe $c \in \mathbb{N}^p$ tal que $(\alpha+c, \beta+c) \in \sigma$ (ver Proposición 1.4). A partir de ahí llegamos a que $(k\alpha+c, k\beta+c) \in \sigma$ para todo $k \in \mathbb{N}$. Finalmente, obsérvese que

$$\lim_{k\to\infty} \frac{|k\alpha+c|}{|k\beta+c|} = \lim_{k\to\infty} \frac{k|\alpha|+|c|}{k|\beta|+|c|} = \frac{|\alpha|}{|\beta|},$$

lo que prueba la otra desigualdad. □

Este resultado y el Lema 13.1 nos dicen que en un monide finitamente generado reducido y atómido $\mathbb{N}^p/\sigma$, el tener elasticidad finita es equivalente a que para todo elemento $x \in \mathbb{N}^p$, su σ-clase tenga un número finito de elementos. Es más, en este caso la elasticidad siempre es un número racional.

COROLARIO 13.7. *Sea σ una congruencia sobre $\mathbb{N}^p$ tal que $\mathbb{N}^p/\sigma$ es reducido, atómico y con $\{[e_1]_\sigma,\dots,[e_p]_\sigma\}$ un sistema minimal de generadores suyo. Entonces $\mathbb{N}^p/\sigma$ es atómico con elasticidad finita si y sólo si σ es fuertemente reducido. Es más,*

$$\varepsilon(\mathbb{N}^p/\sigma)=\max\left\{\frac{|\alpha|}{|\beta|}\mid(\alpha,\beta)\in\mathcal{A}(\sim_{M_\sigma})\right\}.$$

DEMOSTRACIÓN. Este resultado es consecuencia directa de las Proposiciones 13.2 y 13.3 y del Teorema 13.6. □

Otra consecuencia que se deduce a partir de estos resultados y del que en un monoide cancelativo el ser reducido es equivalente a ser fuertemente reducido es el siguiente corolario.

COROLARIO 13.8. *Todo monoide cancelativo finitamente generado tiene elasticidad finita.*

Como acabamos de ver, las congruencias fuertemente reducidas juegan un papel muy importante en el estudio de la elasticidad. A continuación damos una caracterización de este tipo de congruencias que nos dará un método efectivo para el cálculo de la elasticidad en monoides atómicos finitamente generados.

PROPOSICIÓN 13.9. *Sea σ una congruencia sobre $\mathbb{N}^p$ tal que $\{[e_1]_\sigma,\dots,[e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$. Las siguientes condiciones son equivalentes.*

(1) σ es fuertemente reducido.
(2) Si $(a,b)\in\mathcal{A}(\sim_{M_\sigma})$, entonces $a\neq 0\neq b$.

DEMOSTRACIÓN. *(1) implica (2).* Es consecuencia directa del Lema 13.4.
(2) implica (1). Si $(x+y,x)\in\sigma$, entonces $(y,0)\in\sim_{M_\sigma}$. Por tanto $(y,0)$ pertenece al monoide generado por $\mathcal{A}(\sim_{M_\sigma})$, de donde $y=0$. □

NOTA 13.10. Explicamos ahora cómo calcular $\varepsilon(\mathbb{N}^n/R)$ con R una congruencia sobre $\mathbb{N}^n$ tal que $\mathbb{N}^n/R$ es atómico. En primer lugar hemos de calcular R' y p de forma que $\mathbb{N}^n/R$ sea isomorfo a $\mathbb{N}^p/R'$ y $\{[e_1]_{R'},\dots,[e_p]_{R'}\}$ sea un sistema minimal de generadores suyo. Sin pérdida de generalidad podemos suponer que $\mathcal{U}(\mathbb{N}^p/R')\cap\{[e_1]_{R'},\dots,[e_p]_{R'}\}=\{[e_{r+1}]_{R'},\dots,[e_p]_{R'}\}$. Usando los resultados de la Sección 4.2 del capítulo anterior podemos calcular una congruencia $\overline{R}$ de $\mathbb{N}^r$ tal que $(\mathbb{N}^p/R')/\mathcal{U}(\mathbb{N}^p/R')$ sea isomorfo a $\mathbb{N}^r/\overline{R}$. En **[65]** se da un método para calcular $\mathcal{A}(\sim_{M_{\overline{R}}})$. Usando la Proposición 13.9, podemos decir si $\overline{R}$ es o no fuertemente reducido. Si no lo es, entonces $\varepsilon(\mathbb{N}^n/R)=\infty$. En otro caso,

$$\varepsilon(\mathbb{N}^n/R)=\max\{|a|/|b|\mid(a,b)\in\mathcal{A}(\sim_{M_{\overline{R}}})\}.$$

EJEMPLO 13.11. Sea $\sigma=\langle(2,1)\rangle$. El monoide $\mathbb{N}/\sigma=\{[0]_\sigma,[1]_\sigma\}$ es atómico, pero no fuertemente reducido por lo que no tiene elasticidad finita (obsérvese que $k[1]_\sigma=[1]_\sigma$ para todo $k\in\mathbb{N}$). □

EJEMPLO 13.12. Sea $\rho = \{((3,0),(1,3))\}$ y σ la congruencia de $\mathbb{N}^2$ generada por ρ. El grupo M_σ es el subgrupo de $\mathbb{Z}^2$ generado por $(2,-3)$. Tenemos además que

$$\mathcal{A}(\sim_{M_\sigma}) = \{(e_1,e_1),(e_2,e_2),(2e_1,3e_2),(3e_2,2e_1)\}.$$

Es fácil ver que $\{[e_1]_\sigma,[e_2]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^2/\sigma$. Por la Proposición 13.9, la congruencia σ es fuertemente reducida. La Proposición 13.2 nos asegura entonces que $\mathbb{N}^2/\sigma$ es atómico y el Teorema 13.6 nos dice que $\varepsilon(\mathbb{N}^2/\sigma) = 3/2$. □

Si sólo estamos interesados en ver si una congruencia es o no fuertemente reducida, la siguiente caracterización junto con el algoritmo MCP de [**58**] puede usarse para ese propósito.

PROPOSICIÓN 13.13. *Sea σ una congruencia sobre $\mathbb{N}^p$. Las siguientes condiciones son equivalentes.*

(1) σ es fuertemente reducido.
(2) $M_\sigma \cap \mathbb{N}^p = \{0\}$.

DEMOSTRACIÓN. *(1) implica (2).* Supongamos que existe $y \in M_\sigma \cap \mathbb{N}^p$ con $y \neq 0$. Entonces $(y,0) \in \sim_{M_\sigma}$ y por el Lema 1.4, $(x+y,x) \in \sigma$ para algún $x \in \mathbb{N}^p$, contradiciendo el que σ sea fuertemente reducida.

(2) implica (1). Si $(x+y,x) \in \sigma$ para algún $x,y \in \mathbb{N}^p$, entonces $y = x+y-x \in M_\sigma$ y por tanto $y = 0$. □

2. Monoides finitamente generados de elasticidad aceptable

Un monoide S tiene elasticidad aceptable si existe $a \in S \setminus \mathcal{U}(S)$ tal que $\varepsilon(S) = \varepsilon(a)$. Como consecuencia del Teorema 13.6 obtenemos el siguiente resultado, el cual nos proporciona además una amplia familia de monoides atómicos con elasticidad aceptable.

COROLARIO 13.14. *Sea σ una congruencia sobre $\mathbb{N}^p$ tal que $\mathbb{N}^p/\sigma$ es cancelativo, reducido y donde $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ es un sistema minimal de generadores suyo. Entonces $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable.*

DEMOSTRACIÓN. Como $\mathbb{N}^p/\sigma$ es cancelativo, σ y $\sim_{M_\sigma}$ coinciden. Además $\sigma = \sim_{M_\sigma}$ es fuertemente reducido y $\mathcal{A}(\sigma)$ es finito, así que

$$\varepsilon(\mathbb{N}^p/\sigma) = \max\left\{\frac{|\alpha|}{|\beta|} \mid (\alpha,\beta) \in \mathcal{A}(\sim_{M_\sigma})\right\} = \max\left\{\frac{|\alpha|}{|\beta|} \mid (\alpha,\beta) \in \mathcal{A}(\sigma)\right\},$$

lo que hace que $\mathbb{N}^p/\sigma$ tenga elasticidad aceptable. □

Obsérvese que si σ es una congruencia sobre $\mathbb{N}^p$ no fuertemente reducida, a partir de la Proposición 13.3 podemos probar que existe un elemento $[x]_\sigma \in \mathbb{N}^p/\sigma$ tal que $\varepsilon([x]_\sigma) = \infty = \varepsilon(\mathbb{N}^p/\sigma)$. Tenemos así probado el siguiente resultado.

COROLARIO 13.15. *Sea σ una congruencia sobre $\mathbb{N}^p$ no fuertemente reducida y tal que $\mathbb{N}^p/\sigma$ es un monoide atómico. Entonces $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable.*

Ya conocemos dos grandes familias de monoides con elasticidad aceptable. El siguiente resultado nos va a dar otra familia de monoides con esa propiedad.

PROPOSICIÓN 13.16. *Sea* σ *una congruencia sobre* $\mathbb{N}^p$ *generada por* $\rho = \{(a_1, b_1), \ldots, (a_n, b_n)\}$ *y tal que* $\mathbb{N}^p/\sigma$ *es atómico, reducido y con* $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ *un sistema minimal de generadores suyo. Las siguientes condiciones son equivalentes.*

(1) $\mathbb{N}^p/\sigma$ *es semifactorial,*
(2) $\varepsilon(\mathbb{N}^p/\sigma) = 1$,
(3) σ *es fuertemente reducido y* $|a_i| = |b_i|$ *para todo* $i \in \{1, \ldots, n\}$.

DEMOSTRACIÓN. Al ser $\mathbb{N}^p/\sigma$ reducido y $[e_i]_\sigma \neq 0$ para todo $i \in \{1, \ldots, n\}$, tenemos que $a_i \neq 0 \neq b_i$ para todo $i \in \{1, \ldots, n\}$.

(1) implica (2). Se tiene claramente a partir de la definición de elasticidad.

(2) implica (3). Como $\varepsilon(\mathbb{N}^p/\sigma)$ es finito, el Corolario 13.7 nos dice que σ es fuertemente reducido. Por la Proposición 13.2, tenemos que $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\} = \mathcal{A}(\mathbb{N}^p/\sigma)$. Así, para todo $(a, b) \in \rho$, $a \neq b$, tenemos dos descomposiciones de $[a]_\sigma$. Supongamos que $|a_i| \neq |b_i|$ para algún i. Entonces ó bien $|a_i| < |b_i|$ ó $|a_i| > |b_i|$, lo que hace que ó $|a_i|/|b_i| < 1$ ó $|a_i|/|b_i| > 1$. En ambos casos llegamos a que $\varepsilon(\mathbb{N}^p/\sigma) > 1$ (obsérvese que por el Lema 13.4 los elementos a_i y b_i son distintos de cero).

(3) implica (1). Por la Proposición 13.2, tenemos que $\mathcal{A}(\mathbb{N}^p/\sigma) = \{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$. Así, para probar que $\mathbb{N}^p/\sigma$ es semifactorial sólo hemos de probar que para todo $(a, b) \in \sigma$, $[a]_\sigma \neq 0$, se tiene $|a| = |b|$. Al ser ρ un sistema de generadores de σ, existen $v_0, \ldots, v_s \in \mathbb{N}^p$ tales que $v_0 = a$, $v_s = b$ y $(v_i, v_{i+1}) \in \rho_1$. Por tanto para todo $i \in \{1, \ldots, s\}$ existen $(c_i, d_i) \in \rho_0$ y f_i tales que $(v_i, v_{i+1}) = (c_i + f_i, d_i + f_i)$ (ver Proposición 1.3), de donde por hipótesis y de la definición de ρ_0, obtenemos que $|v_i| = |c_i| + |f_i| = |d_i| + |f_i| = |v_{i+1}|$. Por transitividad, concluimos con que $|a| = |b|$. □

Por el Corolario 12.17, la condición de ser reducido no tiene importancia en la Proposición 13.16. La Proposición 13.16 junto con la 13.13 nos da un procedimiento para comprobar a partir de la presentación de un monoide finitamente generado si éste es o no semifactorial.

Nuestro objetivo en el resto de esta sección es dar una caracterización y un método algorítmico para comprobar si un determinado monoide finitamente generado tiene o no elasticidad aceptable.

EJEMPLO 13.17. Sean ρ y σ como en el ejemplo 13.12. Sabemos que $\varepsilon(\mathbb{N}^2/\sigma) = 3/2$. Supongamos que existe $(a, b) \in \sigma$ tal que $|a|/|b| = 3/2$. Entonces $(a, b) \in \sim_{M_\sigma}$ y sabemos que esta congruencia está generada como monoide por $\mathcal{A}(\sim_{M_\sigma})$. Por tanto existen $k_1, k_2, k_3, k_4 \in \mathbb{N}$ tales que

$$(a, b) = k_1(e_1, e_1) + k_2(e_2, e_2) + k_3(2e_1, 3e_2) + k_4(3e_2, 2e_1).$$

Así $3/2 = |a|/|b| = (k_1 + k_2 + 2k_3 + 3k_4)/(k_1 + k_2 + 3k_2 + 2k_4)$, de donde $3k_1 + 3k_2 + 9k_3 + 6k_4 = 2k_1 + 2k_2 + 4k_3 + 6k_4$ y por tanto $k_1 + k_2 + 5k_3 = 0$, lo que hace que

$k_1 = k_2 = k_3 = 0$. Por tanto, $(a,b) = k_4(3e_2, 2e_1)$, el cual no pertenece a σ. Esto implica que $\mathbb{N}^2/\sigma$ no tiene elasticidad aceptable. □

Como hemos visto en el Corolario 13.15, los monoides $\mathbb{N}^p/\sigma$ finitamente generados, atómicos y con σ una congruencia que no es fuertemente reducida tienen siempre elasticidad aceptable. Por tanto vamos a centrar nuestra atención en monoides finitamente generados $\mathbb{N}^p/\sigma$ con σ una congruencia fuertemente reducida (los cuales ya sabemos que son atómicos).

PROPOSICIÓN 13.18. *Sea σ una congruencia fuertemente reducida sobre $\mathbb{N}^p$ para la que $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$. Supongamos que $\mathcal{A}(\sim_{M_\sigma}) = \{(\alpha_1,\beta_1), \ldots, (\alpha_t,\beta_t)\}$ y que los elementos de $\mathcal{A}(\sim_{M_\sigma})$ son tales que $\{1,\ldots,r\} = \{i \in \{1,\ldots,t\} \mid |\alpha_i|/|\beta_i| = \varepsilon(\mathbb{N}^p/\sigma)\}$ (ver Teorema 13.6). El monoide $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable si y sólo si σ contiene un elemento de la forma $k_1(\alpha_1,\beta_1) + \cdots + k_r(\alpha_r,\beta_r)$ con $(k_1,\ldots,k_r) \in \mathbb{N}^r \setminus \{0\}$.*

DEMOSTRACIÓN. *Necesidad.* Sea $(a,b) \in \sigma$ tal que $|a|/|b| = \varepsilon(\mathbb{N}^p/\sigma)$. Ya que $(a,b) \in \sigma$, entonces (a,b) también está en $\sim_{M_\sigma}$ y por tanto existen $k_1,\ldots,k_t \in \mathbb{N}$ tales que $(a,b) = \sum_{i=1}^t k_i(\alpha_i,\beta_i)$, de donde $\varepsilon(\mathbb{N}^p/\sigma) = |a|/|b| = (\sum_{i=1}^t k_i|\alpha_i|)/(\sum_{i=1}^t k_i|\beta_i|)$. Aplicando el Lema 13.5, obtenemos que $k_{r+1} = \ldots = k_t = 0$. En consecuencia $k_1(\alpha_1,\beta_1) + \cdots + k_r(\alpha_r,\beta_r) = (a,b) \in \sigma$ y como $(a,b) \neq (0,0)$, concluimos que existe $i \in \{1,\ldots,r\}$ tal que $k_i \neq 0$.

Suficiencia. Tomemos $(a,b) = k_1(\alpha_1,\beta_1) + \cdots + k_r(\alpha_r,\beta_r) \in \sigma$. Entonces

$$\frac{|a|}{|b|} = \frac{\sum_{i=1}^r k_i|\alpha_i|}{\sum_{i=1}^r k_i|\beta_i|},$$

lo que por el Lema 13.5 es igual a $|\alpha_1|/|\beta_1| = \varepsilon(\mathbb{N}^p/\sigma)$. Esto hace que $\varepsilon([a]) = \varepsilon(\mathbb{N}^p/\sigma)$, por lo que $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable. □

Recordemos que para un elemento $x = (x_1,\ldots,x_p) \in \mathbb{N}^p$ el soporte de x se define como

$$\operatorname{Supp}(x) = \{i \mid x_i \neq 0\}.$$

TEOREMA 13.19. *Consideremos las mismas hipótesis que en la Proposición 13.18. El monoide $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable si y sólo si existe $(a,b) \in \sigma \setminus \{(0,0)\}$ tal que $\operatorname{Supp}(a) \subseteq \bigcup_{i=1}^r \operatorname{Supp}(\alpha_i)$ y $\operatorname{Supp}(b) \subseteq \bigcup_{i=1}^r \operatorname{Supp}(\beta_i)$.*

DEMOSTRACIÓN. *Necesidad.* Es consecuencia directa de la Proposición 13.18.

Suficiencia. Sea $(a,b) \in \sigma \setminus \{(0,0)\}$ tal que $\operatorname{Supp}(a) \subseteq \bigcup_{i=1}^r \operatorname{Supp}(\alpha_i)$ y $\operatorname{Supp}(b) \subseteq \bigcup_{i=1}^r \operatorname{Supp}(\beta_i)$. Tomemos $(\lambda_1,\ldots,\lambda_r) \in \mathbb{N}^r$ tal que $\sum_{i=1}^r \lambda_i\alpha_i \geq a$ y $\sum_{i=1}^r \lambda_i\beta_i \geq b$ (con el orden usual de $\mathbb{N}^p$). Entonces existen $x,y \in \mathbb{N}^p$ cumpliendo que $(a+x,b+y) = \sum_{i=1}^r \lambda_i(\alpha_i,\beta_i)$. Ya que $(a+x,b+y) \in \sim_{M_\sigma}$, por el Lema 13.5 y el Teorema 13.6, tenemos que

$$\frac{|a+x|}{|b+y|} = \frac{\sum_{i=1}^r \lambda_i|\alpha_i|}{\sum_{i=1}^r \lambda_i|\beta_i|} = \frac{|\alpha_1|}{|\beta_1|} = \varepsilon(\mathbb{N}^p/\sigma).$$

Como $(a,b) \in \sim_{M_\sigma}$ y $(a+x,b+y) \in \sim_{M_\sigma}$, tenemos que $(x,y) \in \sim_{M_\sigma}$. Así tanto $|a|/|b|$ como $|x|/|y|$ son menores o iguales que $(|a|+|x|)/(|b|+|y|) = \varepsilon(\mathbb{N}^p/\sigma)$ (ver la demostración del Teorema 13.6). Usando una vez más el Lema 13.5, concluimos que $|a|/|b| = |x|/|y| = \varepsilon(\mathbb{N}^p/\sigma)$ y por tanto $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable. □

Los siguientes lemas nos darán la llave para construir un algoritmo para poder comprobar cuándo un monoide $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable.

LEMA 13.20. *Bajo las mismas hipótesis que en la Proposición 13.18, si* $\varepsilon(\mathbb{N}^p/\sigma) > 1$, *entonces*

$$(\bigcup_{i=1}^{r} \mathrm{Supp}(\alpha_i)) \cap (\bigcup_{i=1}^{r} \mathrm{Supp}(\beta_i)) = \emptyset.$$

DEMOSTRACIÓN. Sea $a = \sum_{i=1}^r \alpha_i$ y $b = \sum_{i=1}^r \beta_i$. Basta con probar que $\mathrm{Supp}(a) \cap \mathrm{Supp}(b)$ es un conjunto vacío. Si éste no es el caso, debe existir $\alpha, \beta, x \in \mathbb{N}^p$, $x \neq 0$, tal que $(a,b) = (\alpha+x, \beta+x)$. Como tenemos que $(\alpha,\beta) \in \sim_{M_\sigma}$, a partir de la demostración del Teorema 13.6 deducimos que $|\alpha|/|\beta| \leq |\alpha_i|/|\beta_i|$ para todo $i \in \{1,\ldots,r\}$. Además por el Lema 13.5, obtenemos que

$$\frac{|\alpha|+|x|}{|\beta|+|x|} = \frac{\sum_{i=1}^r \alpha_i}{\sum_{i=1}^r \beta_i} = \frac{|\alpha_i|}{|\beta_i|}$$

para todo $i \in \{1,\ldots,r\}$. Por tanto

$$|\alpha||\beta_1| + |x||\beta_1| = |\beta||\alpha_1| + |x||\alpha_1| \geq |\alpha||\beta_1| + |x||\alpha_1|$$

y así $|x||\alpha_1| \leq |x||\beta_1|$ lo que hace que

$$1 < \frac{|\alpha_1|}{|\beta_1|} \leq \frac{|x|}{|x|} = 1,$$

lo cual es una contradicción. □

Como ya sabemos, a partir de un sistema de generadores de una congruencia σ de $\mathbb{N}^p$ podemos calcular el conjunto de componentes arquimedianas de $\mathbb{N}^p/\sigma$ como se explica en [**65**], además de poder comprobar si dos elementos dados están o no en la misma componente arquimediana.

LEMA 13.21. *Sea* σ *una congruencia sobre* $\mathbb{N}^p$ *y* $\pi : \{1,\ldots,p\} \to \mathbb{N}^p/\sigma$ *definida como* $\pi(\{i_1,\ldots,i_s\}) = [\sum_{j=1}^s e_{i_j}]_\sigma$. *Si* $(a,b) \in \sigma$, *entonces* $\pi(\mathrm{Supp}(a))$ *y* $\pi(\mathrm{Supp}(b))$ *están en la misma componente arquimediana de* $\mathbb{N}^p/\sigma$ *conteniendo a* $[a+b]_\sigma$.

DEMOSTRACIÓN. Como $[2a]_\sigma \mathcal{N} [a]_\sigma \mathcal{N} \pi(\mathrm{Supp}(a))$ y $[2b]_\sigma \mathcal{N} [b]_\sigma \mathcal{N} \pi(\mathrm{Supp}(b))$, tenemos que

$$\pi(\mathrm{Supp}(a)) \mathcal{N} [2a]_\sigma = [a+b]_\sigma = [2b]_\sigma \mathcal{N} \pi(\mathrm{Supp}(b)).$$

□

LEMA 13.22. *Sea* σ *una congruencia sobre* $\mathbb{N}^p$, $A = \{1,\ldots,r\}$ *y* $B = \{r+1,\ldots,p\}$. *Las siguientes condiciones son equivalentes.*

(1) Existe $(a,b) \in \sigma$ *tal que* $\mathrm{Supp}(a) = A$ *y* $\mathrm{Supp}(b) = B$.

(2) Existe $(u,v) \in \sim_{M_\sigma}$ *con* $\mathrm{Supp}(u) = A$ *y* $\mathrm{Supp}(v) = B$ *tal que* $[u]_\sigma, [v]_\sigma$ *son elementos arquimedianos de* $\mathbb{N}^p/\sigma$.

DEMOSTRACIÓN. *(1) implica (2).* Tomemos $(u,v) = (a,b)$. Como $[2a]_\sigma = [a+b]_\sigma = [2b]_\sigma$ y $\mathrm{Supp}(a+b) = \{1,\dots,p\}$, es fácil probar que tanto $[a]_\sigma$ como $[b]_\sigma$ son arquimedianos.

(2) implica (1). Tenemos que $(u,v) \in \sim_{M_\sigma}$, por lo que existe $c \in \mathbb{N}^p$ tal que $(u+c, v+c) \in \sigma$ (Lema 1.4), esto es, $[u]_\sigma + [c]_\sigma = [v]_\sigma + [c]_\sigma$ en $\mathbb{N}^p/\sigma$, de donde $k[u]_\sigma + [c]_\sigma = k[v]_\sigma + [c]_\sigma$ para todo $k \in \mathbb{N}$. Como $[u]_\sigma$ y $[v]_\sigma$ son arquimedianos en $\mathbb{N}^p/\sigma$, existe $t \in \mathbb{N}\setminus\{0\}$ y $x,y \in \mathbb{N}^p$ tales que $t[u]_\sigma = [c]_\sigma + [x]_\sigma$ y $t[v]_\sigma = [c]_\sigma + [y]_\sigma$. Por tanto,

$$t(t+1)[u]_\sigma = t(t[u]_\sigma + [u]_\sigma) = t([c]_\sigma + [x]_\sigma + [u]_\sigma) = t([c]_\sigma + [x]_\sigma + [v]_\sigma)$$
$$= t(t[u]_\sigma + [v]_\sigma) = t^2[u]_\sigma + t[v]_\sigma$$
$$= t^2[u]_\sigma + [c]_\sigma + [y]_\sigma = t^2[v]_\sigma + [c]_\sigma + [y]_\sigma = t^2[v]_\sigma + t[v]_\sigma = t(t+1)[v]_\sigma.$$

Llegando así a que $(t(t+1)u, t(t+1)v) \in \sigma$ y claramente $\mathrm{Supp}(t(t+1)u) = \mathrm{Supp}(u) = A$ y $\mathrm{Supp}(t(t+1)v) = \mathrm{Supp}(v) = B$. □

Vemos ahora cómo comprobar si se cumple la Condición (2) del Lema 13.22. Supongamos que M_σ está definido por las ecuaciones

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1p}x_p &\equiv 0 \pmod{d_1},\\ &\vdots\\ a_{s1}x_1 + \cdots + a_{sp}x_p &\equiv 0 \pmod{d_s},\\ a_{(s+1)1}x_1 + \cdots + a_{(s+1)p}x_p &= 0,\\ &\vdots\\ a_{(s+k)1}x_1 + \cdots + a_{(s+k)p}x_p &= 0. \end{aligned}$$

Tenemos que existe un elemento $(u,v) \in \sim_{M_\sigma}$ tal que $\mathrm{Supp}(u) = \{1,\dots,r\}$ y $\mathrm{Supp}(v) = \{r+1,\dots,p\}$ si y sólo si el sistema de ecuaciones

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1r}x_r - a_{1(r+1)}x_{r+1} - \cdots - a_{1p}x_p &\equiv 0 \pmod{d_1},\\ &\vdots\\ a_{s1}x_1 + \cdots + a_{sr}x_r - a_{s(r+1)}x_{r+1} - \cdots - a_{sp}x_p &\equiv 0 \pmod{d_s},\\ a_{(s+1)1}x_1 + \cdots + a_{(s+1)r}x_r - a_{(s+1)(r+1)}x_{r+1} - \cdots - a_{(s+1)p}x_p &= 0,\\ &\vdots\\ a_{(s+k)1}x_1 + \cdots + a_{(s+k)r}x_r - a_{(s+k)(r+1)}x_{r+1} - \cdots - a_{(s+k)p}x_p &= 0, \end{aligned}$$

tiene alguna solución con todas sus coordenadas positivas (esto puede comprobarse usando el algoritmo MCP de [**58**]). Para ver cuándo $[u]_\sigma$ y $[v]_\sigma$ son arquimedianos, sólo hemos de comprobar si $[e_1 + \cdots + e_r]_\sigma$ y $[e_{r+1} + \cdots + e_p]_\sigma$ están en la misma componente arquimediana de $[e_1 + \cdots + e_p]_\sigma$ (obsérvese que $[u]_\sigma \mathcal{N} [e_1 + \cdots + e_r]_\sigma$, $[v]_\sigma \mathcal{N} [e_{r+1} + \cdots + e_p]_\sigma$ y que $[e_1 + \cdots + e_p]_\sigma$ es un elemento arquimediano de $\mathbb{N}^p/\sigma$).

Veamos cómo usar toda esta información para construir un algoritmo que compruebe si $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable.

ALGORITMO 13.23. Supongamos que $\rho = \{(a_1, b_1), \ldots, (a_l, b_l)\}$ es un sistema de generadores de una congruencia σ para la que $\mathbb{N}^p/\sigma$ es reducido y $\{[e_1]_\sigma, \ldots, [e_p]_\sigma\}$ es un sistema minimal de generadores suyo.

(1) Si σ no es fuertemente reducido (podemos comprobar esto usando la Proposición 13.13), entonces
   (a) Si $\mathbb{N}^p/\sigma$ es atómico (usar el Algoritmo 12.8), por el Corolario 13.15 $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable. Devolver "$\mathbb{N}^p/\sigma$ tiene elasticidad aceptable y $\varepsilon(\mathbb{N}^p/\sigma) = \infty$."
   (b) Devolver "$\mathbb{N}^p/\sigma$ no es atómico".

(2) En el resto del algoritmo σ es fuertemente reducido. Si $|a_i| = |b_i|$ para todo $i \in \{1, \ldots, l\}$, entonces $\varepsilon(\mathbb{N}^p/\sigma) = 1$ (ver la Proposición 13.16) y $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable. Devolver "$\mathbb{N}^p/\sigma$ es semifactorial y tiene elasticidad aceptable".

(3) Calcular $\mathcal{A}(\sim_{M_\sigma})$ y consideremos

$$\{(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)\} = \left\{(\alpha, \beta) \in \mathcal{A}(\sim_{M_\sigma}) \mid \frac{|\alpha|}{|\beta|} = \varepsilon(\mathbb{N}^p/\sigma)\right\}$$

(ver la Nota 13.10). Observar que $\varepsilon(\mathbb{N}^p/\sigma) > 1$ y por el Lema 13.20

$$\Big(\bigcup_{i=1}^{r} \mathrm{Supp}(\alpha_i)\Big) \cap \Big(\bigcup_{i=1}^{r} \mathrm{Supp}(\beta_i)\Big) = \emptyset.$$

(4) Calcular el subsemigrupo $\mathcal{S}$ de $(\mathcal{P}(\{1, \ldots, p\})^2, \cup)$ generado por

$$\{(\mathrm{Supp}(\alpha_1), \mathrm{Supp}(\beta_1)), \ldots, (\mathrm{Supp}(\alpha_r), \mathrm{Supp}(\beta_r))\}$$

($\mathcal{P}(X)$ denota el conjunto de subconjuntos del conjunto X y la operación $\cup$ sobre $\mathcal{P}(\{1, \ldots, p\})^2$ es realizada componente a componente). Además $\mathcal{S}$ tiene un número finito de elementos.

(5) Calcular las componentes arquimedianas de $\mathbb{N}^p/\sigma$ (como se explica en [**65**]).

(6) Sea

$$C = \left\{(A, B) \in \mathcal{S} \mid \begin{array}{c}\pi(A), \pi(B) \text{ están en la misma} \\ \text{componente arquimediana de } \mathbb{N}^p/\sigma\end{array}\right\}$$

(para la definición de π ver el Lema 13.21).

(7) Si C es vacío, entonces por el Lema 13.21 y la Proposición 13.18, $\mathbb{N}^p/\sigma$ no tiene elasticidad aceptable. Devolver "$\mathbb{N}^p/\sigma$ no tiene elasticidad aceptable".

(8) Para todo $(A, B) \in C$ hacer lo siguiente.
   (a) Supongamos que $A = \{i_1, \ldots, i_s\}$ y $B = \{i_{s+1}, \ldots, i_n\}$. Calcular la restricción de σ a las coordenadas que pertenezcan a $A \cup B$ (esto se hace usando eliminación, ver Capítulo 1) y denotarla por $\sigma_{A \cup B}$; reordenar las coordenadas de forma que $A = \{1, \ldots, s\}$ y $B = \{s+1, \ldots, n\}$.

(b) Usar el Lema 13.22 para ver si existe $(u,v) \in \sim_{M_{\sigma_{A\cup B}}}$ con $\mathrm{Supp}(u) = A$ y $\mathrm{Supp}(v) = B$ tal que $[u]_\sigma$ y $[v]_\sigma$ son elementos arquimedianos de $\mathbb{N}^n/\sigma_{A\cup B}$. Si éste es el caso, a partir de la definición de $\sigma_{A\cup B}$ y del Lema 13.22, existe $(a,b) \in \sigma$ tal que $\mathrm{Supp}(a) = A$ y $\mathrm{Supp}(b) = B$. Por el Teorema 13.19 esto significa que $\mathbb{N}^p/\sigma$ tiene elasticidad aceptable. Devolver "$\mathbb{N}^p/\sigma$ tiene elasticidad aceptable".

(9) Devolver "$\mathbb{N}^p/\sigma$ no tiene elasticidad aceptable".

□

EJEMPLO 13.24. Sea σ una congruencia generada por

$$\rho = \{((0,6,1),(0,0,3)),((3,4,0),(1,0,2)),\\ ((4,3,0),(0,1,2)),((7,0,0),(1,0,2))\}$$

y $S \cong \mathbb{N}^3/\sigma$. Aplicamos el algoritmo anterior a S.

(1) El grupo M_σ está generado por

$$\{(0,6,-2),(2,4,-2),(4,2,-2),(6,0,-2)\}$$

y sus ecuaciones son

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

Usando la primera ecuación y aplicando la Proposición 13.13 deducimos que σ es fuertemente reducida.

(2) Como $((0,6,0),(0,0,2)) \in \sigma$ y $|(0,6,0)| = 6 \neq 2 = |(0,0,2)|$, S no es semifactorial.

(3) Calculamos ahora $\mathcal{A}(\sim_{M_\sigma})$ y obtenemos

$$\{(e_1,e_1),(e_2,e_2),(e_3,e_3),((0,0,2),(0,6,0)),((0,0,2),(2,4,0)),\\ ((0,0,2),(6,0,0)),((0,0,2),(4,2,0)),((0,6,0),(0,0,2)),((0,2,0),(2,0,0)),\\ ((2,4,0),(0,0,2)),((6,0,0),(0,0,2)),((4,2,0),(0,0,2)),((2,0,0),(0,2,0))\}.$$

Por tanto $\varepsilon(S) = 3$, $r = 4$ y

$$\{(\alpha_1,\beta_1),(\alpha_2,\beta_2),(\alpha_3,\beta_3),(\alpha_4,\beta_4)\} =\\ \{((0,6,0),(0,0,2)),((2,4,0),(0,0,2)),((6,0,0),(0,0,2)),((4,2,0),(0,0,2))\}.$$

(4) Obtenemos el semigrupo

$$\mathcal{S} = \{(\{1\},\{3\}),(\{2\},\{3\}),(\{1,2\},\{3\})\}.$$

(5) S tiene las siguientes componentes arquimedianas: $C_1 = \{[(0,0,0)]_\sigma\}$, $C_2 = \{[x] \mid \mathrm{Supp}(x) = \{2\}\}$ y $C_3 = S\backslash(C_1 \cup C_2)$.

(6) Claramente, $C = \{(\{1\},\{3\}),(\{1,2\},\{3\})\}$ (e_2 y e_3 no están en la misma componente arquimediana).

(7) Ya que $C \neq \emptyset$, saltamos al paso 8.

(8) Tomemos ahora $(\{1,2\},\{3\}) \in C$ (probamos primero con este conjunto debido a que $A \cup B = \{1,2,3\}$ y no necesitamos eliminación). Los elementos $(1,1,0)$ y $(0,0,1)$ están en la misma componente arquimediana. Tenemos también que $((2,4,0),(0,0,2)) \in \sim_{M_\sigma}$. Por tanto S tiene elasticidad aceptable.

Usando la primera ecuación y aplicando el Lema 13.22 sabemos que existe un múltiplo de $((2,4,0),(0,0,2))$ que pertenece a σ. El lector puede probar que $((4,8,0),(0,0,4)) \in \sigma$ y que $[(4,8,0)]_\sigma$ es un elemento que alcanza la elasticidad de $\mathbb{N}^p/\sigma$. □

NOTA 13.25. Sea σ una congruencia tal que $\mathbb{N}^p/\sigma$ es atómico, reducido y con $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ un sistema minimal de generadores suyo. Si $\mathbb{N}^p/\sigma$ tiene elasticidad finita, por el Corolario 13.7, σ es fuertemente reducido y entonces es fácil probar que $[a]_\sigma \simeq [b]_\sigma$ si y sólo si $[a]_\sigma = [b]_\sigma$. En este contexto, factorizaciones y descomposiciones coinciden y por tanto $\mathbb{N}^p/\sigma$ es factorial si y sólo si σ es trivial, esto es $\mathbb{N}^p/\sigma = \mathbb{N}^p$. Esto significa que los únicos monoides finitamente generados, atómicos, con elasticidad finita y factoriales son aquellos de la forma $\mathbb{N}^r \times G$ con $r \in \mathbb{N}$ y G un grupo (el grupo de unidades del monoide) tal y como ocurría en el caso anterior.

3. Cálculo de los elementos irreducibles de un monoide atómico

A lo largo de esta sección supondremos que $\mathbb{N}^p/\sigma$ es un monoide atómico con sistema minimal de generadores $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$. Estamos interesados en calcular el conjunto $\mathcal{A}(\mathbb{N}^p/\sigma)$. En vista del Lema 12.14 podemos suponer que $\mathbb{N}^p/\sigma$ es reducido, y por tanto, aplicando la Proposición 12.4, tenemos que $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\} \subseteq \mathcal{A}(\mathbb{N}^p/\sigma)$. La Proposición 13.2 nos dice que si σ es fuertemente reducido, entonces $\mathcal{A}(\mathbb{N}^p/\sigma) = \{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$. Veamos que podemos hacer en el caso no fuertemente reducido. Los siguientes lemas serán de gran ayuda en nuestro estudio. Los dos primeros nos dirán cómo son los átomos $[x]_\sigma$ de $\mathbb{N}^p/\sigma$ para los que $\mathrm{Supp}(x)$ tiene más de un elemento. El tercero describe aquellos átomos que no están en $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ y para los que $\mathrm{Supp}(x)$ tiene sólo un elemento.

LEMA 13.26. *Sea* $x = (x_1,\ldots,x_p) \in \mathbb{N}^p$ *tal que* $[x]_\sigma \in \mathcal{A}(\mathbb{N}^p/\sigma)$. *Entonces* $[e_i]_\sigma \simeq [e_j]_\sigma$ *para todo* $i,j \in \mathrm{Supp}(x)$.

DEMOSTRACIÓN. Probamos que $[x]_\sigma + \mathbb{N}^p/\sigma = [e_i]_\sigma + \mathbb{N}^p/\sigma$ para todo $i \in \mathrm{Supp}(x)$. Claramente, $[x]_\sigma + \mathbb{N}^p/\sigma \subseteq [e_i]_\sigma + \mathbb{N}^p/\sigma$. La igualdad se obtiene a partir del Lema 12.1. □

LEMA 13.27. *Si* $[e_{i_1}]_\sigma \simeq \cdots \simeq [e_{i_r}]_\sigma$ *y* $r \geq 2$, *entonces* $[x_1 e_{i_1} + \cdots + x_r e_{i_r}] \in \mathcal{A}(\mathbb{N}^p/\sigma)$ *para todo* $(x_1,\ldots,x_r) \in \mathbb{N}^r \setminus \{0\}$.

DEMOSTRACIÓN. Ya que $[e_{i_1}]_\sigma \in [e_{i_2}]_\sigma + \mathbb{N}^p/\sigma$, tenemos que $[e_{i_1}]_\sigma = [e_{i_2}]_\sigma + [x]_\sigma$ para algún $x \in \mathbb{N}^p$. El conjunto $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ es un sistema minimal de generadores de $\mathbb{N}^p/\sigma$ y por esta razón $[x]_\sigma = [e_{i_1}]_\sigma + [\lambda_2]_\sigma$ para algún $\lambda_2 \in \mathbb{N}^p$. Por tanto $(e_{i_1}, e_{i_1} +$

$e_{i_2}+\lambda_2)\in\sigma$. Razonando de la misma manera para e_{i_j}, $j\in\{2,\dots,r\}$, obtenemos que $\lambda_j\in\mathbb{N}^p$ para los que $\lambda_j\in\mathbb{N}^p$. A partir de esto deducimos que

$$(e_{i_1},e_{i_1}+k_2(e_{i_2}+\lambda_2)+\cdots+k_r(e_{i_r}+\lambda_r))\in\sigma$$

para todo $k_2,\dots,k_r\in\mathbb{N}$. Análogamente, podemos probar que existe $\lambda_1\in\mathbb{N}^p$ tal que $(e_{i_2},e_{i_2}+e_{i_1}+\lambda_1)$, de donde $(e_{i_2},e_{i_2}+k_1(e_{i_1}+\lambda_1))\in\sigma$ para todo $k_1\in\mathbb{N}$. En consecuencia obtenemos que

$$(e_{i_1}+e_{i_2},e_{i_1}+e_{i_2}+k_1(e_{i_1}+\lambda_1)+k_2(e_{i_2}+\lambda_2)+\cdots+k_r(e_{i_r}+\lambda_r))\in\sigma.$$

Veamos ahora que $[e_{i_1}+e_{i_2}]_\sigma+\mathbb{N}^p/\sigma=[e_{i_1}]_\sigma+\mathbb{N}^p/\sigma$. Como $[e_{i_1}]_\sigma=[e_{i_1}+e_{i_2}+\lambda_2]_\sigma$, tenemos que $[e_{i_1}]_\sigma+\mathbb{N}^p/\sigma\subseteq[e_{i_1}+e_{i_2}]_\sigma+\mathbb{N}^p/\sigma$. La igualdad se obtiene usando el que $\mathbb{N}^p/\sigma$ es reducido, $[e_{i_1}]_\sigma\mathcal{A}(\mathbb{N}^p/\sigma)$ y el Lema 12.1.

Finalmente, si tomamos $(x_1,\dots,x_r)\in\mathbb{N}^r\setminus\{0\}$, podemos encontrar $k_1,\dots,k_r\in\mathbb{N}$ e $y\in\mathbb{N}^p$ tales que

$$x_1e_{i_1}+\cdots+x_re_{i_r}+y=e_{i_1}+e_{i_2}+k_1(e_{i_1}+\lambda_1)+\cdots+k_r(e_{i_r}+\lambda_r).$$

Por tanto,

$$\begin{aligned}[e_{i_1}]_\sigma+\mathbb{N}^p/\sigma&=[e_{i_1}+e_{i_2}]_\sigma+\mathbb{N}^p/\sigma\\&=[e_{i_1}+e_{i_2}+k_1(e_{i_1}+\lambda_1)+\cdots+k_r(e_{i_r}+\lambda_r)]_\sigma+\mathbb{N}^p/\sigma\\&\subseteq[x_1e_{i_1}+\cdots+x_re_{i_r}]_\sigma+\mathbb{N}^p/\sigma.\end{aligned}$$

La igualdad se obtiene una vez más a partir del Lema 12.1. □

A partir de estos dos lemas tenemos que $[x]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ con $\#\mathrm{Supp}(x)\geq 2$ si y sólo si $[x]_\sigma\simeq[e_i]_\sigma$ para todo $i\in\mathrm{Supp}(x)$.

LEMA 13.28. *Las siguientes condiciones son equivalentes.*

(1) $[ke_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ *para algún* $k\geq 2$.
(2) $[2e_i]_\sigma\simeq[e_i]_\sigma$.
(3) $[ke_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ *para todo* $k\geq 1$.

DEMOSTRACIÓN. *(1) implica (2).* Si $[ke_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ para algún $k\geq 2$, entonces por el Lema 12.3, $[2e_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$. Como $[2e_i]_\sigma+\mathbb{N}^p/\sigma\subseteq[e_i]_\sigma+\mathbb{N}^p/\sigma$, $[2e_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ y $\mathbb{N}^p/\sigma$ es reducido, el Lema 12.1 nos asegura que $[2e_i]_\sigma+\mathbb{N}^p/\sigma=[e_i]_\sigma+\mathbb{N}^p/\sigma$.

(2) implica (3). Como $[2e_i]_\sigma\simeq[e_i]_\sigma$, obtenemos que $[e_i]_\sigma=[2e_i]_\sigma+[x]_\sigma$ para algún $x\in\mathbb{N}^p$. Por tanto $(e_i,e_i+e_i+x)\in\sigma$ y entonces $(e_i,e_i+k(e_i+x))\in\sigma$ para todo $k\in\mathbb{N}$, de donde $[e_i]_\sigma+\mathbb{N}^p/\sigma\subseteq[ke_i]_\sigma+\mathbb{N}^p/\sigma$. Teniendo en cuenta que $[e_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ y usando el Lema 12.1, obtenemos que $[e_i]_\sigma+\mathbb{N}^p/\sigma=[ke_i]_\sigma+\mathbb{N}^p/\sigma$ y por tanto, usando el Corolario 12.2, concluimos con que $[ke_i]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$ para todo $k\in\mathbb{N}\setminus\{0\}$.

(3) implica (1). Trivial □

Sobre el conjunto $A=\{1,\dots,p\}$ definimos la siguiente relación de equivalencia:

$$i\,R\,j \text{ si y sólo si } [e_i]_\sigma\simeq[e_j]_\sigma.$$

Sean $A_1,\ldots,A_l$ elementos de A/R con cardinal mayor o igual que dos, y $A_{l+1},\ldots,A_{l+q}$ elementos de A/R con cardinal uno que cumplen que si $A_{l+j}=\{k\}$, entonces $[e_k]_\sigma+\mathbb{N}^p/\sigma=[2e_k]_\sigma+\mathbb{N}^p/\sigma$. Recordemos que en el párrafo anterior al Algoritmo 12.8 se explicó un método para calcular los conjuntos $A_1,\ldots,A_{l+q}$. Como consecuencia de los resultados presentados en esta sección tenemos la siguiente caracterización que nos decribe los átomos de un monoide finitamente generado.

TEOREMA 13.29. *Sea σ una congruencia sobre $\mathbb{N}^p$ tal que $\mathbb{N}^p/\sigma$ es un monoide atómico, reducido, finitamente generado y con $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ un sistema minimal de generadores suyo. Consideremos además $x\in\mathbb{N}^p\setminus\{0\}$. Entonces las siguientes condiciones son equivalentes.*

(1) $[x]_\sigma\in\mathcal{A}(\mathbb{N}^p/\sigma)$,
(2) $\mathrm{Supp}(x)\subseteq A_i$, *para algún* $i\in\{1,\ldots,l+q\}$ *ó* $x=e_j$ *para algún* $j\in\{1,\ldots,p\}$.

4. Factorizaciones de un elemento de elasticidad finita

En esta sección supondremos que $\mathbb{N}^p/\sigma$ es atómico, reducido y que el conjunto $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ es un sistema minimal de generadores suyo (obsérvese que estas dos últimas condiciones no son restrictivas).

Si σ es una congruencia fuertemente reducida, sabemos que $\mathcal{A}(\mathbb{N}^p/\sigma)=\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ y que toda σ-clase es finita. Así, encontrar el conjunto de las descomposiciones (y factorizaciones) de $[a]_\sigma\in\mathbb{N}^p/\sigma$ es equivalente a calcular el conjunto $[a]_\sigma$. En el caso en el que σ no es fuertemente reducido, tenemos que ver primero si $[a]_\sigma$ es o no finito. Esto puede realizarse usando el Algoritmo 9.20 y el Lema 9.21.

Así, sólo nos queda mostrar cómo son las diferentes descomposiciones de $[a]_\sigma$ caso de que $[a]_\sigma$ tenga un número finito de elementos. Como apuntábamos antes, si σ es fuertemente reducido, entonces los elementos de $[a]_\sigma$ nos dan las diferentes factorizaciones de $[a]_\sigma$. Si σ no es fuertemente reducido, puede suceder que existan elementos irreducibles que no estén en $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ y por tanto parece que en principio se requerirá más trabajo. Como vamos a ver en el siguiente resultado, esto nunca sucede cuando $[a]_\sigma$ tiene un número finito de elementos, ya que en este caso en toda descomposición de $[a]_\sigma$ no hay pares de átomos no asociados y por tanto las descomposiciones son factorizaciones.

PROPOSICIÓN 13.30. *Sean $A_1,\ldots,A_l,A_{l+1},\ldots,A_{l+q}$ conjuntos definidos como al final de la Sección anterior y $a\in\mathbb{N}^p\setminus\{0\}$. Si $[a]_\sigma$ tiene un número finito de elementos, entonces* $\mathrm{Supp}(a)\cap(A_1\cup\ldots\cup A_{l+q})$ *es vacío.*

DEMOSTRACIÓN. Supongamos que $a=(a_1,\ldots,a_p)$, con $a_i\neq 0$ para algún $i\in A_1\cup\ldots\cup A_{l+q}$. Tenemos dos posibles casos.

- Si $i\in A_k$ para algún $k\in\{1,\ldots,l\}$, entonces existe al menos $j\in A_k$ tal que $j\neq i$. Usando un argumento similar al usado en la demostración del Lema 13.27, obtenemos que existe $x\in\mathbb{N}^p$ tal que $(e_i,e_i+e_j+x)\in\sigma$, por lo que $(a,a+e_j+x)\in\sigma$ y así $(a,a+k(e_j+x))\in\sigma$ para todo $k\in\mathbb{N}$. En consecuencia $[a]_\sigma$ no tiene un número finito de elementos.

- Si $i \in A_k$ para algún $k \in \{l+1,\ldots,l+q\}$, entonces $[e_i]_\sigma + \mathbb{N}^p/\sigma = [2e_i]_\sigma + \mathbb{N}^p/\sigma$. Por tanto $(e_i, 2e_i+x) \in \sigma$ para algún $x \in \mathbb{N}^p$, de donde $(a, a+e_i+x) \in \sigma$, teniendo así que $[a]_\sigma$, al igual que antes, no tiene un número finito de elementos.

□

Dado ρ y $a \in \mathbb{N}^p \setminus \{0\}$, ya sabemos decidir si la σ-clase de un elemento $a \in \mathbb{N}^p$ tiene o no un número finito de elementos. En el caso en el que $[a]_\sigma$ no tenga un número finito de elementos, $\varepsilon([a]_\sigma)$ es infinito (esto se debe a que podemos encontrar descomposiciones de $[a]_\sigma$ en términos de átomos de la forma $[e_i]_\sigma$ con longitudes tan grandes como queramos). Si $[a]_\sigma$ tiene un número finito de elementos, el Teorema 13.29 y la Proposición 13.30 nos dicen que hay una correspondencia uno a uno entre los elementos de $[a]_\sigma$ y las factorizaciones del elemento $[a]_\sigma \in \mathbb{N}^p/\sigma$. El Algoritmo 9.20 nos permite calcular $[a]_\sigma$ y por tanto $\varepsilon([a]_\sigma)$.

COROLARIO 13.31. *Sea σ una congruencia sobre $\mathbb{N}^p$ tal que $\mathbb{N}^p/\sigma$ es reducido, atómico, con $\{[e_1]_\sigma,\ldots,[e_p]_\sigma\}$ un sistema minimal de generadores suyo. Si $a \in \mathbb{N}^p$ satisface que $\#[a]_\sigma = n$, entonces el número de factorizaciones del elemento $[a]_\sigma$ es exactamente n.*

CAPÍTULO 14

Cálculo de la elasticidad de un monoide de Krull

Siguiendo la línea del capítulo anterior y usando algunos resultados de Geroldinger (véase [**22**]) que tratan sobre las longitudes de las factorizaciones de los monoides, proporcionamos en este capítulo un algoritmo para calcular la elasticidad de un monoide de Krull con grupo de clases finitamente generado y tal que el conjunto de clases que contienen divisores primos es finito. Además sobre estos monoides, sabemos que su elasticidad es racional y aceptable, esto es $\varepsilon(S) = m/n$ con $m \in \mathbb{Z}$ y $n \in \mathbb{N}$ y existen irreducibles $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ con $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$ (ver el Teorema principal de [**2**]). Aunque ya existen métodos para el cálculo específico de $\varepsilon(S)$ para monoides de Krull, hasta el momento no se había dado un método general para calcular este número. De hecho, en un artículo reciente [**4**], Chapman y Anderson tratan el problema de determinar el conjunto de elasticidades de un dominio de Krull con un grupo de clases de divisores cíclico.

1. Monoides de Krull, cero-secuencias minimales y elasticidad

Un monoide S es un **monoide de Krull** si existe un monoide libre D y un homomorfismo $\partial : S \to D$ tal que

(1) $x|y$ en S si y sólo si $\partial(x)|\partial(y)$ en D,
(2) todo elemento de D es el máximo común divisor de algún conjunto finito de elementos de $\partial(S)$.

Dado un sistema minimal de generadores de D, sus elementos son llamados **divisores primos** de S y al cociente $D/\partial(S)$ el **grupo de clases de divisores** de S y denotado por $Cl(S)$ (la congruencia $\partial(S)$ está definida por $x\partial(S)y$, si existen $h, h' \in \partial(S)$ tales que $x + h = y + h'$). Dado S un monoide de Krull y x un elemento suyo que no es unidad, entonces existe un único conjunto $p_1, \ldots, p_k$ de divisores primos de S y únicos enteros positivos $n_1, \ldots, n_k$ tales que

$$\partial(x) = p_1^{n_1} \cdots p_k^{n_k}. \tag{3}$$

Obsérvese que (3) implica que $n_1[p_1]_{\partial(S)} + \cdots + n_k[p_k]_{\partial(S)} = 0$ en $Cl(S)$. El lector interesado puede encontrar más información sobre monoides de Krull en [**37**].

Recordemos que si S es era un monoide atómico y x un elemento no unidad de S, definíamos

$$\mathrm{L}_S(x) = \{n \mid \text{ existen } \alpha_1, \ldots, \alpha_n \in \mathcal{A}(S) \text{ con } x = \alpha_1 \cdots \alpha_n\}.$$

Definimos ahora

$$\mathcal{L}(S) = \{\mathrm{L}_S(x) \mid x \text{ no es unidad de } S\}.$$

De la anterior discusión, si S es un monoide de Krull y x no es una unidad de S, la estructura del conjunto $\mathrm{L}_S(x)$ (y por tanto la de $\mathcal{L}(S)$) depende del comportamiento de un número finito de sucesiones de elementos de $Cl(S)$ que suman cero. Consideremos G un grupo abeliano finitamente generado y $T = \{g_1, \ldots, g_t\}$ un sistema de generadores de G. Un elemento $(n_1, \ldots, n_t) \subseteq \mathbb{N}^t$ es una **cero-secuencia** en G de elementos de T, si $\sum_{i=1}^{t} n_i g_i = 0$. Al conjunto de cero secuencias de elementos de T lo denotaremos por $\mathcal{B}(G,T)$. Si $x = (x_1, \ldots, x_t)$ e $y = (y_1, \ldots, y_t)$ pertenecen a $\mathcal{B}(G,T)$, podemos definir $x+y = (x_1+y_1, \ldots, x_t+y_t)$, obteniendo que $(\mathcal{B}(G,T), +)$ es un monoide conmutativo y cancelativo. Este monoide es conocido como el **monoide de bloques de G sobre T** (en [**25**] puede encontrarse más información sobre estos monoides). Una cero-secuencia $(n_1, \ldots, n_t)$ es **minimal** si no hay ninguna otra cero-secuencia tal que $(n'_1, \ldots, n'_t) < (n_1, \ldots, n_t)$ (con el orden parcial usual de $\mathbb{N}^t$). Si $\mathcal{M}(G,T)$ es el conjunto de cero-secuencias minimales de $\mathcal{B}(G,T)$, entonces $\mathcal{M}(G,T) = \mathcal{A}(\mathcal{B}(G,T))$. La longitud de la más larga cero-secuencia minimal de $\mathcal{M}(G,T)$ es llamada la **Constante de Davenport** de G con respecto a T, la denotaremos $D_T(G)$.

PROPOSICIÓN 14.1. *Sea S un monoide de Krull con grupo de clase de divisores G finitamente generado tal que el conjunto T de clases de divisores de G que contiene divisores primos es finito.*

(1) [**13**, Lemma 4.2] $\mathcal{L}(S) = \mathcal{L}(\mathcal{B}(G,T))$ *y por tanto* $\varepsilon(S) = \varepsilon(\mathcal{B}(G,T))$.

(2) [**4**, Proposition 3] $1 \leq \varepsilon(\mathcal{B}(G,T)) \leq \frac{D_T(G)}{2}$.

(3) [**4**, Proposition 3] $\varepsilon(\mathcal{B}(G,T)) = \frac{D_T(G)}{2}$ *si y sólo si existe una cero-secuencia minimal $(g_1, \ldots, g_{D_T(G)})$ en $\mathcal{M}(G,T)$ con $-g_i \in T$ para todo $1 \leq i \leq D_T(G)$.*

Por tanto, para el cálculo de la elasticidad de un monoide de Krull S que satisfaga las hipótesis de la Proposición 14.1, sólo necesitamos considerar el monoide de bloques apropiado.

2. Elasticidad de semigrupos afines plenos

Un monoide S es un **semigrupo afín pleno** si existe $p \in \mathbb{N}$ y N un subgrupo de $\mathbb{Z}^p$ tales que $S = N \cap \mathbb{N}^p$. Puede probarse que si S no es trivial, entonces está generado por el conjunto minimal de elementos de $(N \cap \mathbb{N}^p) \setminus \{0\}$ con respecto al orden parcial usual de $\mathbb{N}^p$. Por el Lema de Dickson, este conjunto de elementos minimales es siempre finito y por tanto todo semigrupo afín pleno es finitamente generado, además de ser siempre cancelativos y reducidos por estar incluidos en $\mathbb{N}^p$. El conjunto de elementos minimales no nulos de estos monoides forman un sistema minimal de generadores de los mismos. Así, por la Proposición 12.24 tenemos lo siguiente.

PROPOSICIÓN 14.2. *Sea S un semigrupo pleno no trivial. Entonces*

$$\mathrm{Minimales}_{\leq}(S \setminus \{0\}) = \mathcal{A}(S).$$

En particular, esto implica que S es atómico.

Supongamos que S es un semigrupo afín pleno y que $\text{Minimales}_{\leq}(S \setminus \{0\}) = \{m_1, \ldots, m_s\}$.

Definimos

$$\varphi : \mathbb{N}^s \to S,\ \varphi(a_1, \ldots, a_s) = \sum_{i=1}^{s} a_i m_i.$$

Obsérvese que si $x \in S$ y si tenemos una factorización de x de la forma $x = \sum_{i=1}^{s} a_i m_i$, entonces $(a_1, \ldots, a_s) \in \varphi^{-1}(x)$. Nótese que $((a_1, \ldots, a_s), (b_1, \ldots, b_s))$ pertenece al núcleo de la congruencia de φ si y sólo si $\sum_{i=1}^{s} a_i m_i = \sum_{i=1}^{s} b_i m_i$, lo que se tiene si y sólo si $(a_1 - b_1, \ldots, a_s - b_s)$ pertenece al subgrupo M de $\mathbb{Z}^s$ dado por la ecuaciones

$$M \equiv m_1 x_1 + \cdots + m_s x_s = 0.$$

Por lo que

$$\text{Ker}(\varphi) = \sim_M = \{(a, b) \in \mathbb{N}^s \times \mathbb{N}^s \mid a - b \in M\},$$

de donde tenemos que S es isomorfo a $\mathbb{N}^s / \sim_M$. Recuérdese que un elemento dado $a = (a_1, \ldots, a_s) \in \mathbb{N}^s$, teníamos $|a| = \sum_{i=1}^{s} a_i$. La Proposición 13.6 nos decía que

$$\varepsilon(S) = \max\left\{ \frac{|a|}{|b|} \mid (a, b) \in \mathcal{A}(\sim_M) \right\}.$$

Dado un semigrupo afín pleno $S = N \cap \mathbb{Z}^p$, el conjunto $\text{Minimales}_{\leq}(S \setminus \{0\})$ puede calcularse usando el procedimiento que se describe en [**22**] para encontrar soluciones minimales no triviales de sistemas lineales de ecuaciones diofánticas. También pueden usarse los métodos de [**65**] ó [**67**].

2.1. La elasticidad de los monoides de Krull. Sea G un grupo abeliano finitamente generado y $T = \{g_1, \ldots, g_t\}$ un sistema de generadores de G. Supongamos que $G = \mathbb{Z}^n \times \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$ y que N es el subgrupo de $\mathbb{Z}^t$ definido por las siguientes ecuaciones

$$\begin{aligned}
a_{11}x_1 + \cdots + a_{1t}x_t &= 0,\\
&\vdots\\
a_{n1}x_1 + \cdots + a_{nt}x_t &= 0,\\
a_{(n+1)1}x_1 + \cdots + a_{(n+1)t}x_t &\equiv 0 \pmod{d_1},\\
&\vdots\\
a_{(n+r)1}x_1 + \cdots + a_{(n+r)t}x_t &\equiv 0 \pmod{d_r},
\end{aligned}$$

con $(a_{1i}, \ldots, a_{(n+r)i}) = g_i$. Entonces $\mathcal{B}(G, T)$ es el monoide formado por las soluciones enteras no negativas del anterior sistema de ecuaciones. Esto es, $\mathcal{B}(G, T) = N \cap \mathbb{N}^t$ y $\mathcal{M}(G, T) = \text{Minimales}_{\leq}((N \cap \mathbb{N}^p) \setminus \{0\})$. Supongamos que $\mathcal{M}(G, T) = \{m_1, \ldots, m_s\}$. Entonces, $\mathcal{B}(G, T) = \langle m_1, \ldots, m_s \rangle$ y por tanto es isomorfo a $\mathbb{N}^s / \sim_M$, donde M es el subgrupo de $\mathbb{Z}^s$ definido por las ecuaciones

$$(m_1 \cdots m_s) \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = 0.$$

Por el Teorema 13.6, para calcular la elasticidad de $\mathcal{B}(G,T)$, sólo hemos de calcular $\mathcal{A}(\sim_M)$, teniendo así que

$$\varepsilon(\mathcal{B}(G,T)) = \max\left\{ \frac{|a|}{|b|} \mid (a,b) \in \mathcal{A}(\sim_M) \right\}.$$

Como consecuencia tenemos que la elasticidad de este tipo de monoides es racional.

EJEMPLO 14.3. Sea $G = \mathbb{Z}_6$ y $T = \{\overline{1}, \overline{2}\}$. Entonces N es el subgrupo de $\mathbb{Z}^2$ definido por

$$x_1 + 2x_2 \equiv 0 \pmod 6.$$

Tenemos que $\mathcal{B}(G,T) = N \cap \mathbb{N}^2 = \langle (0,3),(2,2),(4,1),(6,0) \rangle \cong \mathbb{N}^4 / \sim_M$, donde M es el subgrupo de $\mathbb{Z}^4$ con ecuaciones

$$\begin{pmatrix} 0 & 2 & 4 & 6 \\ 3 & 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0.$$

Calculando $\mathcal{A}(\sim_M)$ obtenemos

$$\begin{aligned} \mathcal{A}(\sim_M) = \{ \quad & (e_1,e_1),(e_2,e_2),(e_3,e_3),(e_4,e_4), \\ & ((0,0,2,0),(0,1,0,1)),((0,0,3,0),(1,0,0,2)),((0,1,0,1),(0,0,2,0)), \\ & ((0,1,1,0),(1,0,0,1)),((0,3,0,0),(2,0,0,1)),((0,2,0,0),(1,0,1,0)), \\ & ((1,0,0,2),(0,0,3,0)),((1,0,0,1),(0,1,1,0)),((2,0,0,1),(0,3,0,0)), \\ & ((1,0,1,0),(0,2,0,0))\} \end{aligned}$$

Por tanto,

$$\varepsilon(\mathcal{B}(G,T)) = \max\{1\} = 1$$

y así $\mathcal{B}(G,T)$ es semifactorial (el que $\varepsilon(\mathcal{B}(G,T)) = 1$ también se tiene a partir de [**16**, Theorem 3.8]). □

EJEMPLO 14.4. Tomemos ahora $G = \mathbb{Z}_6$ y $T = \{\overline{1}, \overline{4}\}$. En este caso N es el subgrupo de $\mathbb{Z}^3$ definido por la ecuación

$$x_1 + 4x_2 \equiv 0 \pmod 6.$$

Aquí $\mathcal{M}(G,T) = \{(0,3),(2,1),(6,0)\}$ y por tanto $\mathcal{B}(G,T)$ es isomorfo a $\mathbb{N}^4 / \sim_M$, donde M está definido por las ecuaciones

$$\begin{pmatrix} 0 & 2 & 6 \\ 3 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 0.$$

Calculando el conjunto $\mathcal{A}(\sim_M)$, obtenemos

$$\begin{aligned} \mathcal{A}(\sim_M) = \{ \quad & ((0,0,1),(0,0,1)),((0,1,0),(0,1,0)),((0,3,0),(1,0,1)), \\ & ((1,0,1),(0,3,0)),((1,0,0),(1,0,0))\}, \end{aligned}$$

de donde $\varepsilon(\mathcal{B}(G,T)) = \varepsilon([(1,0,1)]) = \varepsilon((6,3)) = 3/2$. El lector puede ver que tal y como ya sabiamos por la Proposición 14.1 tenemos

$$1 < \varepsilon(\mathcal{B}(G,T)) < \frac{D_T(\mathbb{Z}_6)}{2} = 3.$$

□

2.2. La elasticidad de un monoide diofántico. Un monoide S es un **monoide diofántico** si es un semigrupo afín pleno $N \cap \mathbb{N}^p$ para algún $p \in \mathbb{N}$ donde N es un subgrupo de $\mathbb{Z}^p$ tal que los factores invariantes de N son iguales a uno. En otras palabras, S puede definirse como el conjunto de soluciones no negativas de un sistema lineal de ecuaciones diofánticas. Como todo monoide diofántico es un monoide afín pleno, podemos usar el procedimiento descrito antes para calcular su elasticidad.

EJEMPLO 14.5. Sea S el monoide diofántico dado por las ecuaciones

$$x_1 + x_2 + x_5 - 2x_6 = 0,\ x_3 + x_4 + x_5 - 2x_7 = 0.$$

Entonces

$$\begin{aligned}\mathcal{A}(S) = \{\ & (0,0,0,0,2,1,1),(0,0,0,2,0,0,1),(0,0,1,1,0,0,1),(0,0,2,0,0,0,1),\\ & (0,1,0,1,1,1,1),(0,1,1,0,1,1,1),(0,2,0,0,0,1,0),(1,0,0,1,1,1,1),\\ & (1,0,1,0,1,1,1),(1,1,0,0,0,1,0),(2,0,0,0,0,1,0)\}\end{aligned}$$

y por tanto $S = \langle \mathcal{A}(S) \rangle$ es isomorfo a $\mathbb{N}^{11} / \sim_M$, donde M es el subgrupo de $\mathbb{Z}^{11}$ cuyas ecuaciones de definición son

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{11} \end{pmatrix} = 0$$

Calculando $\mathcal{A}(\sim_M)$ obtenemos

$$\varepsilon(S) = \varepsilon([(0,0,0,0,0,1,0,0,1,0,0)]) = \varepsilon((1,1,2,0,2,2,2)) = 3/2.$$

□

Bibliografía

[1] D.D. Anderson and D.F. Anderson, Elasticity of factorizations in integral domains, J. Pure Appl. Algebra **80**(1992), 217–235.

[2] D.D Anderson, D.F. Anderson, S.T. Chapman and W.W. Smith, Rational elasticity of factorizations in Krull domains, Proc. Amer. Math. Soc. **117**(1993), 37–43.

[3] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, en "Factorization in Integral Domains", Lecture Notes in Pure and Applied Mathematics, Marcel Dekker **189**(1997), 1–30.

[4] D.F. Anderson and S.T. Chapman, On the elasticities of Krull domains with finite cyclic divisor class group, por aparecer en Comm. Algebra.

[5] D. F. Anderson and P. Pruis, Length functions on integral domains, Proc. Amer. Math. Soc. **113**(1991), 933-937.

[6] D. D. Anderson (ed.), "Factorization in integral domains", Lecture Notes in Pure and Appl. Math. **189**, Marcel Dekker, 1997.

[7] D. D. Anderson and E. W. Johnson, Ideal theory in commutative semigroups, Semigroup Forum **30**(1984) 127–158.

[8] I. Arnold, Ideale in Kommutative Halbgruppen, Mat. Sb. **36**(1929), 401–408.

[9] M. F. Atiyah and I. G. Macdonald, "Introduction to commutative algebra", Addison-Wesley, 1969.

[10] T. Becker and W. Weispfenning, "Gröbner bases: a computational approach to commutative algebra", Springer, Berlin-Heidelberg-New York, 1993.

[11] J. Bertin and P. Carbone, Semi-groupes d'entiers et application aux branches, Journal of Algebra **49**(1977), 81-95.

[12] L. Carlitz, A characterization of algebraic number fields with class number two, Proc. Amer. Math. Soc. **11**(1960), 391-392.

[13] S.T. Chapman and A. Geroldinger, Krull monoids, their sets of lengths and associated combinatorial problems, en "Factorization in Integral Domains", Lecture Notes in Pure and Applied Mathematics, Marcel Dekker **189**(1997), 73–112.

[14] S. T. Chapman, U. Krause, E. Oeljeklaus, Monoids determined by a homogeneous linear Diophantine equation and the half-factorial property, por aparecer en J. Pure Appl. Algebra.

[15] S.T. Chapman and W.W. Smith, An analysis using the Zaks-Skula constant of element factorizations in Dedekind domains, J. Algebra **159**(1993), 176–190.

[16] S.T. Chapman and W.W. Smith, Factorization in Dedekind domains with finite class group, Israel J. Math. **71**(1990), 65–95.

[17] L. G. Chouinard II, Krull Semigroups and divisor class groups, Canad. J. Math. **33**(1981) 1459–1468.

[18] J. L. Chrislock, On medial semigroups, J. Algebra **12**(1969), 1–9.

[19] Clifford, A. H., Extensions of semigroups, Trans. Amer. Math. Soc. **68**(1950), 165–173

[20] A .H. Clifford and G.B. Preston, The Algebraic Theory of Semigroups, Amer. Math. Soc. Mathematical Surveys **7**, 1961.

[21] A. H. Clifford, Arithmetical and ideal theory of commutative semigroups, Ann. Math. **39**(1938), 594–610.

[22] E. Contejean and H. Devie, An efficient incremental algorithm for solving systems of linear Diophantine equations, Inform. and Comput. **113**(1994), 143-172.
[23] D. Cox, J. Little and D. O'Shea. "Ideals, Varieties and Algorithms. Springer-Verlag", New York, 1992.
[24] D. Eisenbud and B. Sturmfels, Binomial ideals, Duke Math. Journal **84**(1) (1996) 1-45.
[25] A. Geroldinger and F. Halter-Koch, Non-unique factorizations in block semigroups and arithmetical applications, Math. Slovaca **42**(1992), 641–661.
[26] A. Geroldinger, On the structure and arithmetic of finitely primary monoids, Czech. Math. J. **46**(1996), 677–695.
[27] A. Geroldinger and G. Lettl, Factorization problems in semigroups, Semigroup Forum **40**(1990), 23–38.
[28] A. Geroldinger and F. Halter-Koch, Arithmetical theory of monoid homomorphisms, Semigroup Forum **48**(1994) 333-362.
[29] A. Geroldinger, On the arithmetic of certain not integrally closed noetherian integral domains, Comm. Algebra **19**:685-698 (1991).
[30] R. Gilmer, "Commutative semigroup rings", Chicago Lectures in Mathematics, 1984.
[31] R. Gilmer, "Multiplicative ideal theory", Marcel Dekker, New York, 1972.
[32] G. M. Greuel, G. Pfister, and H. Schönemann, Singular version 1.2 User Manual, In *Reports On Computer Algebra*, number 21. Centre for Computer Algebra, University of Kaiserslautern, June 1998. http://www.mathematik.uni-kl.de/ zca/Singular
[33] Grillet, P. A., "Semigroups. An introduction to the structure theory", Dekker, 1995
[34] P.A. Grillet, The free envelope of a finitely generated commutative semigroup, Trans. of the Amer. Math. Soc., **149**(1970), 665-682.
[35] F. Halter-Koch, "Ideal systems an introduction to multiplicative ideal theory", Marcel Dekker Inc., 1998.
[36] F. Halter-Koch, Divisor theories with primary elements and weakly Krull domains, Boll. U. M. I. **7** 9-b (1995), 417-441.
[37] F. Halter-Koch, Halbgruppen mit Divisorentheorie, Expo. Math. **8**(1990), 27–66.
[38] F. Halter-Koch, Elasticity of factorizations in atomic monoids and integral domains, J. Théorie des Nombres Bordeaux **7**(1995), 367–385.
[39] W. Heinzer, L.J. Ratliff, Jr., K. Shah, On the irreducible components of an ideal, Comm. Algebra **25**(1997), 1609-1634.
[40] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, Manuscripta Math., **3**(1970), 175-193.
[41] E. Hewitt and H. S. Zuckerman, The l_1-algebra of a commutative semigroup, Trans. Amer. Math. Soc., **83**(1956), 70-97.
[42] J. A. Hildebrant, The translational degree of a semigroup, Semigroup Forum **30**(1984), 331–349.
[43] Howie, J. M., "Fundamentals of semigroup theory", The Clarendon Press, Oxford University Press, New York, 1995
[44] N. Jacobson. "Basic algebra I", W. H. Freeman and Company, 1974.
[45] P. Jaffard, Contribution a l'étude des groupes ordonnés, J. Math. Pures Appl. **32**(1953), 203–280.
[46] D. E. Knuth and P. B. Bendix, Simple word problems in universal algebras, "Proc. of the Conf. on Computational Problems in Abstract Algebra", Oxford 1967, J. Leech(ed.), Pergamon Press, 1970, 263-298.
[47] U. Krause, On monoids of finite real character, Proc. Amer. Math. Soc. **105**(1989), 546-554.
[48] E. Kunz, "Introduction to Commutative Algebra and Algebraic Geometry", Birkhäuser Boston, 1985.
[49] G. Lettl, Subsemigroups of finitely generated groups with divisor theory, Mh. Math. **106**(1988), 205-210.

[50] F. Levi, Arithmetische Gesetze im Gebiet discreter Gruppen, Reud. Circ. Mat. Palermo, **25**(1913), 225–236.
[51] D. Michel and J.L. Steffan, Repartition des ideaux premiers parmi les classes de ideaux dans un anneau de Dedekind et equidecomposition, J. Algebra **98**(1986), 82–94.
[52] W. Narkiewicz, Some unsolved problems, Bull. Soc. Math. France, **25**(1971), 159-164.
[53] M. Petrich, "Introduction to semigroups", Merrill, Columbus, Ohio (1973).
[54] M. Petrich, On the structure of a class of commutative semigroups, Czech. Math. J. **14**(1964), 147-152.
[55] M. Petrich, The translational Hull in Semigroups and Rings, Semigrupo Forum, **4**(1970), 283-360.
[56] L. Rédei, "The theory of finitely generated commutative semigroups", Pergamon, Oxford-Edinburgh-New York, 1965.
[57] J. C. Rosales, Function minimum associated to a congruence on integral n-tuple space, Semigroup Forum **51**(1995), 87-95.
[58] J. C. Rosales, On finitely generated submonoids of $\mathbb{N}^k$, Semigroup Forum **50**(1995) 251-262.
[59] J. C. Rosales, On linear equations in natural numbers, Int. J. Algebra and Comput. **7**(1997), 25–31.
[60] J. C. Rosales, J. I. García-García, Decimal extensions of the additive group of integers, por aparecer en Communications in Algebra.
[61] J. C. Rosales and J. I. García-García, Generalized $\mathcal{N}$-semigroups, por aparecer en Proceedings of ICS'99, Word Scientific.
[62] J. C. Rosales and J. I. García-García, Hereditarily finitely generated commutative semigroups, J. Algebra **221**, 723-732 (1999).
[63] J. C. Rosales and J. I. García-García, Principal ideals of finitely generated commutative monoids, por aparecer en Cz. Math. J.
[64] J. C. Rosales and J. I. García-García, Primary ideals of finitely generated commutative cancellative monoids, por aparecer en Linear Alg. and Appl.
[65] J. C. Rosales and P.A. García-Sánchez, "Finitely generated commutative monoids". Novascience Publishers, New York, 1999.
[66] J. C. Rosales and P. A. García-Sánchez, Nonnegative Elements of Subgroups of $\mathbb{Z}^n$, Linear Algebra and its Applications **270**:351-357(1998).
[67] J. C. Rosales and P. A. García-Sánchez, On normal affine semigroups, Linear Algebra Appl. **286**(1999), 175-186.
[68] J. C. Rosales and P. A. García Sánchez, Presentations for subsemigroups of finitely generated commutative semigroups, Israel J. Math. **113** (1999), 269-283.
[69] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, Commutative ideals extensions of abelian groups, por aparecer en Semigroup Forum.
[70] J. C. Rosales, P. A. García-Sánchez and J. I. García-García, How to check if a finitely generated commutative monoids is a principal ideal commutative monoid, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation 288-291, ACM-Press.
[71] J. C. Rosales, P. A. García-Sánchez and J. I. García-García, Irreducible ideals of finitely generated commutative monoids, por aparecer en J. Algebra.
[72] J. C. Rosales and J. M. Urbano-Blanco, A deterministic algorithm to decide if a finitely presented Abelian monoid is cancellative, Comm. Algebra **24**(13) (1996), 4217-4224.
[73] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco, On presentations of commutative monoids, Internat. J. Algebra Comput. **9** (1999), 539-553.
[74] M. Satyanarayana, A class of commutative semigroups in which the idempotents are linearly ordered, Czech. Math. J. **21**(1971), 633-637.
[75] M. Satnarayana, Commutative primary semigroups, Czech. Math. J. **22**(97) (1972).
[76] M. Satyanarayana, On commutative semigroups which are unions of a finite number of principal ideals, Czech. Math. J. **27**(1977), 61-68.

[77] M. Satyanarayana, Structure and ideal theory of commutative monoids, Czech. Math. J. **28**(1978), 171-180.
[78] Š. Schwarz, Prime ideal and maximal ideals in semigroups, Czech. Math. J. **19**(1969), 72-79.
[79] T. Tamura, Commutative nonpotent archimedean Semigroups with cancelation law, Journ. of Gakugei, Tokushima Univ. **8**(1957), 5–11.
[80] T. Tamura, Notes on Translations of a Semigroup, Kodai Math. Sem. Rep. **10**(1958), 9-26.
[81] T. Tamura, Nonpotent Archimedean Semigroups with cancellative law, I.J. Gakugei Tokushima Univ. **8**(1957), 5-11.
[82] T. Tamura. and N. Kimura, On decompositions of a commutative semigroup, Kodai Math. Sem. Rep. (1954), 109-112.
[83] The GAP Group, GAP — Groups, Algorithms, and Programming, Version4.1; Aachen, St Andrews, 1999. (http://www-gap.dcs.st-and.ac.uk/∼gap)
[84] R. J. Valenza, Elasticity of factorizations in number fields, J. Number Theory **39**(1990), 212-218.
[85] A. Vigneron-Tenorio, Semigroup ideals and linear Diophantine equations, Linear Algebra Appl. **295**(1999), 133-144.
[86] A. Zaks, Half-factorial domains, Bull. Amer. Math. Soc. **82**(1976), 721-724.

Índice de definiciones