Bollettino
Unione Matematica Italiana

J. C. Rosales

Commutative monoids with zero-divisors

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **5-B** (2002), n.3, p. 773–788.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2002_8_5B_3_773_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2002.

Bollettino U. M. I.
(8) 5-B (2002), 773-788

Commutative Monoids with Zero-Divisors.

J. C. ROSALES (*)

Sunto. – *Vengono descritti alcuni algoritmi per il calcolo del nilradicale e dei divisori dello zero di uno* $\emptyset$*-monoide commutativo fintamente generato. Tali algoritmi vengono utilizzati per decidere se un ideale assegnato di uno* $\emptyset$*-monoide commutativo fintamente generato é primo, radicale o primario.*

Summary. – *We describe algorithms for computing the nilradical and the zero-divisors of a finitely generated commutative* $\emptyset$*-monoid. These algorithms will be used for deciding if a given ideal of a finitely generated commutative* $\emptyset$*-monoid is prime, radical or primary.*

Introduction.

All semigroups, monoids and groups appearing in this paper are commutative. For this reason, in the sequel we will omit this adjective. We denote by $\mathbb{Z}$ and $\mathbb{N}$ the set of integers and nonnegative integers, respectively.

In the first third of this century some works like [2, 4] started to develop the theory of ideals of semigroups. This theory is very similar to ideal theory in rings. For this reason many theorems and definitions in Commutative Algebra have their counterpart in the theory of semigroup ideals. In this way, it is not amazing that concepts like prime ideal, radical ideal, primary ideal, zero-divisors and nilradical play an important rôle in the theory of semigroup ideals. The study of these concepts have yielded a large amount of papers and books related to this subject (see for instance [1, 7, 9, 10]). In addition, the problem of factorization in domains is starting to be studied from a «monoid» point of view (see for instance [3, 6, 11]).

Rédei proves in [12] that every finitely generated monoid is finitely presented. Our main goal in this paper is to give algorithmic methods for deciding from a presentation of a given semigroup if one of its ideals

(*) The author would like to thank P. A. García-Sánchez and the referee for their comments and suggestions. This paper was supported by the project BFM2000-1469.

is prime, radical or primary. We are also interested in computing the set of zero-divisors of a monoid and its nilradical.

The contents of this paper are distributed as follows. In Section 3 we introduce the concept of $\emptyset$-monoid to denote the monoids $(M, \cdot)$ which have an element $\emptyset$ such that $m\emptyset = \emptyset$ for all $m \in M$ (we use $\emptyset$ instead of 0 in order to distinguish this element from the element $0 = (0, \ldots, 0) \in \mathbb{N}^p$). Our aim in that section is to give an algorithm for deciding whether a finitely generated monoid is a $\emptyset$-monoid or not. Section **2** is the most relevant part of this paper, and there we give an algorithmic method for computing the set of zero-divisors of a finitely presented $\emptyset$-monoid. In Section **3** we study the nilradical of a $\emptyset$-monoid. We present two algorithmic methods for computing the nilradical of a finitely presented $\emptyset$-monoid; one of them leans on the results given in Section **2**, while the other relies on the concept of Archimedean component (this is due to the fact that the nilradical of a $\emptyset$-monoid turns out to be its maximal Archimedean component). In Section **4** we study reduced $\emptyset$-monoids, that is, $\emptyset$-monoids with trivial nilradical. We explain two methods for deciding whether a $\emptyset$-monoid is reduced or not, one of which is a consequence of the results appearing in Section **2**, and the other comes from the methods developed in Section **3**. Using the concept of Archimedean component, we describe how is the set of zero-divisors of a reduced $\emptyset$-monoid. We finish this section studying those reduced $\emptyset$-monoids whose set of zero-divisors is trivial, and call them integral monoids. We also give a method for deciding whether a finitely presented $\emptyset$-monoid is an integral monoid or not. Finally, in Section **5**, for a given ideal I of a monoid $(M, \cdot)$ we show that the monoid M/R_I, with R_I the Rees congruence associated to I, is a $\emptyset$-monoid, and this fact enables us to study whether I is prime, radical or primary in terms of being M/R_I an integral monoid, reduced or fulfilling that its nilradical equals its set of zero-divisors. We show how a presentation of M/R_I can be computed from a presentation of M and thus using the methods exposed in the preceding sections we obtain algorithmic procedures for deciding whether an ideal of a finitely presented monoid is prime, radical or primary.

Preliminaries.

Let $(M, \cdot)$ be a monoid generated by $\{m_1, \ldots, m_p\}$. We have that the map

$$\varphi : \mathbb{N}^p \to M, \ \varphi(k_1, \ldots, k_p) = m_1^{k_1} \ldots m_p^{k_p}$$

is a monoid epimorphism and M is isomorphic to $(\mathbb{N}^p/\sigma, +)$, where σ is the kernel congruence of φ ($a\sigma b$ holds if $\varphi(a) = \varphi(b)$). Rédei proves in [12] that every congruence on $\mathbb{N}^p$ is finitely generated and thus there exists $\varrho =$

$\{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\} \subset \mathbb{N}^p \times \mathbb{N}^p$ such that σ is the least congruence on $\mathbb{N}^p$ containing ϱ. Moreover σ can be constructed from ϱ in the following way (see [5]).

(1) Set $\varrho_0 = \varrho \cup \varrho^{-1} \cup \Delta$, where $\varrho^{-1} = \{(a, b) \mid (b, a) \in \varrho\}$ and $\Delta = \{(a, a) \mid a \in \mathbb{N}^p\}$.

(2) Set $\varrho_1 = \{(a + c, b + c) \mid (a, b) \in \varrho_0, c \in \mathbb{N}^p\}$.

(3) The pair $(a, b) \in \sigma$ if and only if there exist $v_0, \ldots, v_k \in \mathbb{N}^p$ such that $a = v_0$, $b = v_k$ and $(v_i, v_{i+1}) \in \varrho_1$ for all $i \in \{0, \ldots, k-1\}$.

We now sketch a procedure given in [14] (see also [13]; there the notation is slightly different from the one used here) for solving the word problem in $\mathbb{N}^p/\sigma$, that is, given $a, b \in \mathbb{N}^p$ decide whether $a\sigma b$ holds or not. From ϱ one can construct a canonical system of generators $\overline{\varrho} = \{(\overline{\alpha_1}, \overline{\beta_1}), \ldots, (\overline{\alpha_l}, \overline{\beta_l})\}$ of σ with respect to a given linear admissible order $\leqslant$ on $\mathbb{N}^p$ (linear order means that for all $a, b \in \mathbb{N}^p$, either $a \leqslant b$ or $b \leqslant a$; an admissible order on $\mathbb{N}^p$ is an order such that $0 \leqslant a$ for all $a \in \mathbb{N}^p$ and $a \leqslant b$ implies $a + c \leqslant b + c$ for all $a, b, c \in \mathbb{N}^p$; every linear admissible order on $\mathbb{N}^p$ is a well order and therefore for any $A \subset \mathbb{N}^p$ there exists $\min_{\leqslant} A$, the minimum of A with respect to A). This new system of generators of σ allows us to construct the map $NF_{\overline{\varrho}}\colon \mathbb{N}^p \to \mathbb{N}^p$ as follows:

(1) if $x - \overline{\alpha_i} \notin \mathbb{N}^p$ for all $i \in \{1, \ldots, l\}$, then $NF_{\overline{\varrho}}(x) = x$,

(2) if $x - \overline{\alpha_j} \notin \mathbb{N}^p$ for all $j \leqslant i$ and $x - \overline{\alpha_{i+1}} \in \mathbb{N}^p$, then $NF_{\overline{\varrho}}(x) = NF_{\overline{\varrho}}(x - \overline{\alpha_{i+1}} + \overline{\beta_{i+1}})$.

One can prove that $NF_{\overline{\varrho}}(x) = \min_{\leqslant} [x]_\sigma$ ($[x]_\sigma$ denotes the σ-class of x in $\mathbb{N}^p$; if there is no possible misunderstanding, we will simply write $[x]$), and therefore $x\sigma y$ holds if and only if $NF_{\overline{\varrho}}(x) = NF_{\overline{\varrho}}(y)$.

For general results about semigroups and monoids see [5, 16, 8, 14].

1. – Finitely generated $\emptyset$-monoids.

Let $(M, \cdot)$ be a monoid and let 1 be its identity element. The monoid M is a **$\emptyset$-monoid** if there exists $m \in M$ such that $mx = m$ for all $x \in M$. This element is unique and will be denoted by $\emptyset$.

Assume that M is generated by $\{m_1, \ldots, m_p\}$ and let φ, σ and ϱ be as in the preliminaries. The main goal in this section is to give an algorithm for deciding from ϱ whether $\mathbb{N}^p/\sigma$ (and therefore M) is a $\emptyset$-monoid or not. The key for achieving this goal is Theorem 1. Before stating and proving this theorem we need some concepts and results.

If R is a congruence on $\mathbb{N}^n$, then

$$G_R = \{a - b \in \mathbb{Z}^n \mid (a, b) \in R\}$$

if a subgroup of $\mathbb{Z}^n$. Conversely for a given subgroup H of $\mathbb{Z}^n$, we can define the congruence on $\mathbb{N}^n$

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

It is easy to prove (see for instance [12] or [14]) that $R \subseteq \sim_{G_R}$ and that if $a \sim_{G_R} b$, then there exists $c \in \mathbb{N}^n$ such that $(a+c)R(b+c)$. As a consequence of this fact one obtains that $\mathbb{N}^n/R$ is cancellative if and only if $R = \sim_{G_R}$.

Denote by e_i the element of $\mathbb{N}^n$ all of whose coordinates are equal to zero with the exception of the ith component, which is equal to one.

THEOREM 1. – *The monoid $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid if and only if $\{e_1, \ldots, e_p\} \subseteq G_\sigma$.*

PROOF. – *Necessity.* If $x \in \mathbb{N}^p$ is such that $[x] = \emptyset$, then $[x] + [e_i] = [x]$ for all i and therefore $x + e_i - x = e_i \in G_\sigma$.

Sufficiency. If $e_i \in G_\sigma$, then $e_i \sim_{G_\sigma} 0$, whence there exists $\lambda_i \in \mathbb{N}^p$ such that $(e_i + \lambda_i)\, \sigma \lambda_i$. Clearly $[e_i] + [\lambda_1 + \ldots + \lambda_p] = [\lambda_1 + \ldots + \lambda_p]$ for all $i \in \{1, \ldots, p\}$. From this it is easily shown that $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid. ■

Let us show now how can we decide from ϱ whether $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid or not. In [14] it is proved that G_σ is the subgroup of $\mathbb{Z}^p$ generated by $\{\alpha_1 - \beta_1, \ldots, \alpha_t - \beta_t\}$. Using Theorem 1, the monoid $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid if and only if $G_\sigma = \mathbb{Z}^p$ and this can be checked out by just computing the equations of G_σ or its invariant factors.

Assume henceforward in this section that $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid. Our next goal is to give an algorithm for computing from ϱ an element $x \in \mathbb{N}^p$ such that $[x] = \emptyset$. The following proposition gives the key to solve this problem.

PROPOSITION 2. – *If $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid, then the following conditions hold.*

(1) *There exists $\lambda \in \mathbb{N}$ such that $\lambda(e_1 + \ldots + e_p)\, \sigma (\lambda + 1)(e_1 + \ldots + e_p)$.*

(2) *If $\mu \in \mathbb{N}$ and $\mu(e_1 + \ldots + e_p)\, \sigma (\mu + 1)(e_1 + \ldots + e_p)$, then $[\mu(e_1 + \ldots + e_p)] = \emptyset$.*

PROOF. – (1) Let $x = (x_1, \ldots, x_p) \in \mathbb{N}^p$ be such that $[x] = \emptyset$ and set $\lambda = \max\{x_1, \ldots, x_p\}$ (where $\max(A)$ stands for the maximum of the set A). Then there exits $y \in \mathbb{N}^p$ such that $\lambda(e_1 + \ldots + e_p) = x + y$. Hence $[\lambda(e_1 + \ldots + e_p)] = [x] + [y] = \emptyset$. In the same way one proves that $[(\lambda + 1)(e_1 + \ldots + e_p)] = \emptyset$, whence $\lambda(e_1 + \ldots + e_p)\, \sigma (\lambda + 1)(e_1 + \ldots + e_p)$.

(2) Note that $(\mu + k)(e_1 + \ldots + e_p)\, \sigma \mu(e_1 + \ldots + e_p)$ for all $k \in \mathbb{N}$. Let $x \in \mathbb{N}^p$ be such that $[x] = \emptyset$. Then there exists $k \in \mathbb{N}$ and $y \in \mathbb{N}^p$ such that $(\mu + k)(e_1 + \ldots + e_p) = x + y$, whence $[(\mu + k)(e_1 + \ldots + e_p)] = \emptyset$ and consequently $[\mu(e_1 + \ldots + e_p)] = \emptyset$. ■

As we already mentioned in the preliminaries, we have a procedure for checking whether $a \sigma b$ holds or not for any $a, b \in \mathbb{N}^p$, and therefore we can compute the least nonnegative integer k such that $k(e_1 + \ldots + e_p)\, \sigma (k + 1)(e_1 + \ldots + e_p)$ holds. Applying Proposition 2, we get that $[k(e_1 + \ldots + e_p)] = \emptyset$. We can always decide whether $[y] = \emptyset$ or not for some $y \in \mathbb{N}^p$, since we only have to check if $y \sigma k(e_1 + \ldots + e_p)$ holds.

2. – The zero-divisors of a $\emptyset$-monoid.

An element x in a $\emptyset$-monoid $(M, .)$ is a **zero-divisor** if there exists $y \in M \setminus \{\emptyset\}$ such that $xy = \emptyset$. The set of zero-divisors of M is denoted by $\mathcal{ZD}(M)$.

The main goal of this section is to give an algorithmic method for computing the set $\mathcal{ZD}(M)$ for a given finitely generated $\emptyset$-monoid.

An **ideal** I of a monoid M is a subset of M fulfilling that for every $x \in I$ and $s \in M$, the element xs is again in I. An ideal I is a **prime ideal** if for every $x, y \in M$ such that $xy \in I$, we have that either $x \in I$ or $y \in I$.

LEMMA 3. – *If M is a $\emptyset$-monoid, then $\mathcal{ZD}(M)$ is a prime ideal of M.*

PROOF. – If $x \in \mathcal{ZD}(M)$ and $s \in M$, then there exists $y \in M \setminus \{\emptyset\}$ such that $xy = \emptyset$. Hence $(xs)y = \emptyset$ and therefore $xs \in \mathcal{ZD}(M)$. Now take $x, y \in M$ such that $xy \in \mathcal{ZD}(M)$. Then there exists $z \in M \setminus \{\emptyset\}$ such that $(xy)z = \emptyset$. If $yz \neq \emptyset$, then $x \in \mathcal{ZD}(M)$; otherwise $y \in \mathcal{ZD}(M)$. ■

In the sequel we assume that all $\emptyset$-monoids appearing in this paper are nontrivial, that is, they are not equal to $\{\emptyset\}$ and consequently $1 \neq \emptyset$.

Given a nonempty subset A of a monoid $(M, \cdot)$, we denote by

$$AM = \{as \mid a \in A,\ s \in M\}.$$

It is clear that AM is an ideal of M (it is in fact the smallest ideal of M containing A). We will refer to AM as the **ideal generated** by A.

LEMMA 4. – *Let $(M, \cdot)$ be a nontrivial $\emptyset$-monoid generated by $\{m_1, \ldots, m_p\}$ and such that $\{m_1, \ldots, m_p\} \cap \mathcal{ZD}(M) = \{m_{i_1}, \ldots, m_{i_r}\}$. Then*

$$\mathcal{ZD}(M) = \{m_{i_1}, \ldots, m_{i_r}\}\, M .$$

PROOF. – Clearly $\{m_{i_1}, \ldots, m_{i_r}\} M \subseteq \mathcal{Z}\mathcal{D}(M)$. To prove the other inclusion take $x \in \mathcal{Z}\mathcal{D}(M)$. Then there exists $(k_1, \ldots, k_p) \in \mathbb{N}^p \setminus \{0\}$ such that $x = m_1^{k_1} \ldots m_p^{k_p}$ (1 can not be in $\mathcal{Z}\mathcal{D}(M)$ and for this reason $(k_1, \ldots, k_p) \neq 0$). Since $\mathcal{Z}\mathcal{D}(M)$ is a prime ideal, we can find $i \in \{1, \ldots, p\}$ for which $m_i \in \mathcal{Z}\mathcal{D}(M)$. Hence $i \in \{i_1, \ldots, i_r\}$ and $x \in \{m_1\} M \subseteq \{m_{i_1}, \ldots, m_{i_r}\} M$. ■

Under the same hypothesis of Lemma 4, set

$$\Im(\emptyset) = \{(k_1, \ldots, k_p) \in \mathbb{N}^p \mid m_1^{k_1} \ldots m_p^{k_p} = \emptyset\} .$$

The set $\Im(\emptyset)$ is equal to $\varphi^{-1}(\emptyset)$, where as above φ is the map $\varphi : \mathbb{N}^p \to M$, $\varphi(k_1, \ldots, k_p) = m_1^{k_1} \ldots m_p^{k_p}$; whence $\Im(\emptyset)$ is an ideal of $(\mathbb{N}^p, +)$. By Dickson's lemma (see for instance [14]) the set of minimal elements with respect to the usual partial order of $\Im(\emptyset)$ is finite (recall that the usual partial order on $\mathbb{N}^p$ is defined by $(a_1, \ldots, a_p) \leqslant (b_1, \ldots, b_p)$ if $a_i \leqslant b_i$ for all i).

For an element $x = (x_1, \ldots, x_p) \in \mathbb{N}^p$, write $\operatorname{Supp}(x) = \{i \mid x_i \neq 0\}$.

THEOREM 5. – *Let* $(M, \cdot)$ *be a nontrivial* $\emptyset$*-monoid generated by* $\{m_1, \ldots, m_p\}$ *and such that* $\operatorname{Minimals}_{\leqslant} \Im(\emptyset) = \{\lambda_1, \ldots, \lambda_r\}$ *(*$\operatorname{Minimals}_{\leqslant} A$ *denotes the set of minimal elements of A with respect to the order* $\leqslant$*). Then* $m_i \in \mathcal{Z}\mathcal{D}(M)$ *if and only if* $i \in \operatorname{Supp}(\lambda_1) \cup \ldots \cup \operatorname{Supp}(\lambda_r)$.

PROOF. – *Necessity.* If $m_i \in \mathcal{Z}\mathcal{D}(M)$, then there exists $x = m_1^{k_1} \ldots m_p^{k_p} \in M \setminus \{\emptyset\}$ such that $m_i x = 0$. Thus $(k_1, \ldots, k_{i-1}, k_i + 1, k_{i+1}, \ldots, k_p) \in \Im(\emptyset)$ and therefore there exists $j \in \{1, \ldots, r\}$ and $y \in \mathbb{N}^p$ such that $(k_1, \ldots, k_i + 1, \ldots, k_p) = \lambda_j + y$. If $i \in \operatorname{Supp}(y)$, then $(k_1, \ldots, k_i, \ldots, k_p) = \lambda_i + (y - e_i) \in \Im(\emptyset)$, which leads to $x = \emptyset$, contradicting the fact that $x \neq \emptyset$. Therefore $i \notin \operatorname{Supp}(y)$ and consequently $i \in \operatorname{Supp}(\lambda_j)$.

Sufficiency. Let $j \in \{1, \ldots, r\}$ and $i \in \operatorname{Supp}(\lambda_j)$. Then $\lambda_j - e_i \notin \Im(\emptyset)$, because $\lambda_j \in \operatorname{Minimals}_{\leqslant} \Im(\emptyset)$. Hence if $\lambda_j = (a_1, \ldots, a_p)$, we get

$$x = m_1^{a_1} \ldots m_{i-1}^{a_{i-1}} m_i^{a_i - 1} m_{i+1}^{a_{i+1}} \ldots m_p^{a_p} \neq \emptyset \text{ and } x m_i = \emptyset .$$

Thus $m_i \in \mathcal{Z}\mathcal{D}(M)$. ■

Applying Theorem 5 and Lemma 4, we can compute $\mathcal{Z}\mathcal{D}(M)$ from the set $\operatorname{Minimals}_{\leqslant} \Im(\emptyset)$. Thus we focus our attention on finding a procedure for computing $\operatorname{Minimals}_{\leqslant} \Im(\emptyset)$. We take φ and σ as in the preliminaries, and let $\varrho = \{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$ be a canonical system of generators of σ with respect to a given linear admissible order $\preccurlyeq$. For $x = (x_1, \ldots, x_p)$, $y = (y_1, \ldots, y_p) \in \mathbb{N}^p$, set

$$x \vee y = (\max\{x_1, y_1\}, \ldots, \max\{x_p, y_p\}) .$$

LEMMA 6. – *If* $x \in \Im(\emptyset)$, $x - \beta_i \in \mathbb{N}^p$ *and* $x - \beta_i + \alpha_i \in \mathrm{Minimals}_{\leqslant} \Im(\emptyset)$, *then* $x = \lambda \vee \beta_i$ *for some* $\lambda \in \mathrm{Minimals}_{\leqslant} \Im(\emptyset)$.

PROOF. – If $x \in \Im(\emptyset)$, then there exits $\lambda \in \mathrm{Minimals}_{\leqslant} \Im(\emptyset)$ and $y \in \mathbb{N}^p$ such that $x = \lambda + y$. Hence $x - \lambda \in \mathbb{N}^p$ and by hypothesis $x - \beta_i \in \mathbb{N}^p$. Thus there exits $z \in \mathbb{N}^p$ such that $x = (\lambda \vee \beta_i) + z$. We prove that $z = 0$. Since $\lambda \in \Im(\emptyset)$, and $\Im(\emptyset)$ is an ideal of $\mathbb{N}^p$, we get $\lambda \vee \beta_i \in \Im(\emptyset)$. In addition, $(\alpha_i, \beta_i) \in \varrho \subseteq \sigma$ and thus $(((\lambda \vee \beta_i) - \beta_i) + \alpha_i)\ \sigma(\lambda \vee \beta_i)$, whence $((\lambda \vee \beta_i) - \beta_i) + \alpha_i \in \Im(\emptyset)$. This yields $x - \beta_i + \alpha_i = ((\lambda \vee \beta_i) - \beta_i) + \alpha_i + z$. Since $x - \beta_i + \alpha_i \in \mathrm{Minimals}_{\leqslant} \Im(\emptyset)$, we deduce that $z = 0$. ■

LEMMA 7. – *If* $\{\lambda_1, \ldots, \lambda_r\} = \mathrm{Minimals}_{\leqslant} \Im(\emptyset)$ *and* $\lambda_1 < \lambda_2 < \ldots < \lambda_r$ *(*$a < b$ *means* $a \leqslant b$ *and* $a \neq b$*), then* $x \in \Im(\emptyset)$ *if and only if there exists a sequence* $(\alpha_{i_1}, \beta_{i_1}), \ldots, (\alpha_{i_q}, \beta_{i_q})$ *of elements in* ϱ *fulfilling the following conditions:*

(1) $x + \sum_{j=1}^{q} (-\alpha_{i_j} + \beta_{i_j}) = \lambda_1$,

(2) $x - \alpha_{i_1} \in \mathbb{N}^p$,

(3) $x + \sum_{j=1}^{l} (-\alpha_{i_j} + \beta_{i_j}) - \alpha_{i_{l+1}} \in \mathbb{N}^p$ *for all* $l \in \{1, \ldots, q-1\}$.

PROOF. – Clearly $\Im(\emptyset) = [\lambda_1]$ and since $\leqslant$ is a linear admissible order on $\mathbb{N}^p$, we get $\lambda_1 = \min_{\leqslant} [\lambda_1]$. Hence $x \in \Im(\emptyset)$ if and only if $x \sigma \lambda_1$ holds, or equivalently, $NF_\varrho(x) = \lambda_1$. The proof follows from the definition of NF_ϱ (see the preliminaries). ■

The following theorem is the last piece needed to give a procedure for computing $\Im(\emptyset)$.

THEOREM 8. – *If* $\mathrm{Minimals}_{\leqslant} \Im(\emptyset) = \{\lambda_1 < \ldots < \lambda_r\}$, *then* $\lambda_{k+1} = (\lambda_i \vee \beta_j) - \beta_j + \alpha_j$ *for some* $i \in \{1, \ldots, k\}$ *and* $j \in \{1, \ldots, t\}$.

PROOF. – Applying Lemma 7, we deduce that $\lambda_{k+1} = x - \beta_j + \alpha_j$ for some $x \in \Im(\emptyset)$ and some $j \in \{1, \ldots, t\}$ such that $x - \beta_j \in \mathbb{N}^p$. Using Lemma 6, we get that $x = \lambda \vee \beta_j$ for some $\lambda \in \mathrm{Minimals}_{\leqslant} \Im(\emptyset)$. Since ϱ is a canonical system of generators of σ with respect to $\leqslant$, we have $\beta_i < \alpha_i$ (see [13] or [14]). Thus

$$\lambda \leqslant \lambda \vee \beta_j = x < x - \beta_j + \alpha_j = \lambda_{k+1},$$

which means that $\lambda \in \{\lambda_1, \ldots, \lambda_k\}$. ■

With all these results we can finally give an algorithm for computing the set $\mathrm{Minimals}_{\leqslant} \Im(\emptyset)$.

Algorithm 9.

INPUT: A canonical system of generators $\varrho = \{(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t)\}$ of a congruence σ on $\mathbb{N}^p$ with respect to a given linear admissible order $\leqslant$. We assume that $\mathbb{N}^p/\sigma$ is a nontrivial $\emptyset$-monoid.

OUTPUT: The set $\text{Minimals}_{\leqslant}\{x \in \mathbb{N}^p \mid [x] = \emptyset\}$.

Step 1: Find $x \in \mathbb{N}^p$ such that $[x] = \emptyset$ (see Section **1**).

Step 2: Compute $m_1 = \min_{\leqslant}[x] = NF_{\varrho}(x)$.

Step 3: Set $A = \{m_1\}$.

Step 4: Compute $B = \{(a \vee \beta_j) - \beta_j + \alpha_j \mid a \in A, j \in \{1, \ldots, t\}\}$.

Step 5: Compute $C = B \cap \text{Minimals}_{\leqslant}\{x \in \mathbb{N}^p \mid [x] = \emptyset\}$ (note that an element $b \in B$ is in $\text{Minimals}_{\leqslant}\{x \in \mathbb{N}^p \mid [x] = \emptyset\}$ if and only if for all $y < b$, $NF_{\varrho}(y) \neq m_1$).

Step 6: If $C \subseteq A$, then return A; stop.

Step 7: $A := A \cup C$; go to Step 4.

3. – The nilradical of a $\emptyset$-monoid.

An element x of a $\emptyset$-monoid $(M, \cdot)$ is **nilpotent** if there exists $k \in \mathbb{N} \setminus \{0\}$ such that $x^k = \emptyset$. The set of nilpotent elements of M is called the **nilradical** of M and it is denoted by $\text{Nil}(M)$. For I an ideal of M, set

$$\sqrt{I} = \{x \in M \mid x^k \in I \text{ for some } k \in \mathbb{N} \setminus \{0\}\},$$

the **radical** of I. The set $\sqrt{I}$ is also an ideal of M and we say that I is a **radical ideal** if $\sqrt{I} = I$. Clearly $\sqrt{I}$ is a radical ideal for every ideal I of M. In particular, $\text{Nil}(M) = \sqrt{\{\emptyset\}}$.

We start this section giving an algorithmic method for computing the nilradical of a finitely generated $\emptyset$-monoid, which is inspired in the results obtained in the preceding section.

Assume henceforward in this section that M is a nontrivial $\emptyset$-monoid generated by $\{m_1, \ldots, m_p\}$ and take $\Im(\emptyset)$ as above. Let $\{\lambda_1, \ldots, \lambda_r\}$ be the set of minimal elements of $\Im(\emptyset)$ with respect to $\leqslant$. For every $i \in \{1, \ldots, r\}$ define $\mu_i = \sum_{j \in \text{Supp}(\lambda_i)} e_j$. Set

$$\Im(\text{Nil}(M)) = \{(k_1, \ldots, k_p) \in \mathbb{N}^p \mid m_1^{k_1} \cdots m_p^{k_p} \in \text{Nil}(M)\}.$$

Note that $\Im(\text{Nil}(M)) = \varphi^{-1}(\text{Nil}(M))$ and that it is a radical ideal of $\mathbb{N}^p$ that contains $\Im(\emptyset)$.

PROPOSITION 10. – *Under the above hypothesis,* $\Im(\text{Nil}(M)) = \{\mu_1, \ldots, \mu_r\} + \mathbb{N}^p$.

PROOF. – Take $x \in \Im(\mathrm{Nil}(M))$. Then $kx \in \Im(\emptyset)$ for some $k \in \mathbb{N}\setminus\{0\}$. Therefore there exist $i \in \{1, \ldots, r\}$ and $y \in \mathbb{N}^p$ such that $kx = \lambda_i + y$. It is clear that $\mathrm{Supp}(\lambda_i) \subseteq \mathrm{Supp}(x)$, whence $x \in \{\mu_i\} + \mathbb{N}^p \subseteq \{\mu_1, \ldots, \mu_r\} + \mathbb{N}^p$.

To prove the other inclusion, take $x \in \{\mu_1, \ldots, \mu_r\} + \mathbb{N}^p$. Then there exist $i \in \{1, \ldots, r\}$ and $y \in \mathbb{N}^p$ such that $x = \mu_i + y$. This leads to $\mathrm{Supp}(\lambda_i) = \mathrm{Supp}(\mu_i) \subseteq \mathrm{Supp}(x)$ and for this reason we can find $k \in \mathbb{N}\setminus\{0\}$ and $z \in \mathbb{N}^p$ for which $kx = \lambda_i + z$. Hence $kx \in \Im(\emptyset) \subseteq \Im(\mathrm{Nil}(M))$, and since $\Im(\mathrm{Nil}(M))$ is radical, we conclude that $x \in \Im(\mathrm{Nil}(M))$. ∎

Let φ and σ be as in the preliminaries and let ϱ be a system of generators of σ. Applying the last proposition and the results obtained in the preceding section, the reader can check that we have a procedure for computing from ϱ the ideal $\Im(\mathrm{Nil}(M))$ and thus $\mathrm{Nil}(M)$.

Our next goal is to describe how *Nil*(M) is distributed inside M. To this end we recall the concept of Archimedean component of a semigroup.

An element x of a semigroup $(S, \cdot)$ is **Archimedean** (see [16]) if for all $y \in S$ there exist $k \in \mathbb{N}\setminus\{0\}$ and $z \in S$ such that $x^k = yz$ (observe that if $<_S$ is defined by $a <_S b$ if $ac = b$ for some $c \in S$, then the above condition translates to $y <_S x^k$ for some $k \in \mathbb{N}\setminus\{0\}$). A semigroup is Archimedean provided that all its elements are Archimedean. The element x is **idempotent** if $x^2 = x$. A **semilattice** is a semigroup all of whose elements are idempotent. For a semigroup $(S, \cdot)$, we define the binary relation $\mathcal{N}$ on S by $a\mathcal{N}b$ if there exist $k, l \in \mathbb{N}\setminus\{0\}$ and $c, d \in S$ such that $a^k = bc$ and $b^l = ad$. Tamura and Kimura proved in [15] that $\mathcal{N}$ is a congruence on S and that the quotient semigroup $S/\mathcal{N}$ is a semilattice. The $\mathcal{N}$-classes of S are called the **Archimedean components** of S. They are Archimedean subsemigroups of S.

It is easy to check that if $(A, \cdot)$ is a semilattice, then the binary relation $\leqslant$, defined by $a \leqslant b$ if $ab = b$, is an order relation on A (that is, it is reflexive, transitive and antisymmetric). Moreover $ab = \mathrm{supremum}_{\leqslant}\{a, b\}$ (see for instance [14]; $\mathrm{supremum}_{\leqslant}\{a, b\}$ denotes the supremum of $\{a, b\}$ with respect to $\leqslant$).

PROPOSITION 11. – *If* $(S, \cdot)$ *is a* $\emptyset$*-monoid, then* $\mathrm{Nil}(S) = \max\limits_{\leqslant_{\mathcal{N}}}(S/\mathcal{N})$, *where* $[x]_{\mathcal{N}} \leqslant_{\mathcal{N}} [y]_{\mathcal{N}}$ *if* $[x]_{\mathcal{N}}[y]_{\mathcal{N}} = [y]_{\mathcal{N}}$.

PROOF. – We first prove that $\mathrm{Nil}(S) = [\emptyset]_{\mathcal{N}}$. Take $x \in \mathrm{Nil}(S)$. Then there exists $k \in \mathbb{N}\setminus\{0\}$ such that $x^k = \emptyset$. Clearly this implies that $x\mathcal{N}\emptyset$ holds and this means that $x \in [\emptyset]_{\mathcal{N}}$. Conversely, if $x \in [\emptyset]_{\mathcal{N}}$, then there exist $k \in \mathbb{N}\setminus\{0\}$ and $y \in S$ for which $x^k = \emptyset y$. Therefore $x^k = \emptyset$ and for this reason $x \in \mathrm{Nil}(S)$.

We now prove that $[\emptyset]_{\mathcal{N}} = \max_{\leqslant_{\mathcal{N}}}(S/\mathcal{N})$. If $[x]_{\mathcal{N}} \in S/\mathcal{N}$, then $[x]_{\mathcal{N}}[\emptyset]_{\mathcal{N}} = [x\emptyset]_{\mathcal{N}} = [\emptyset]_{\mathcal{N}}$, whence $[x]_{\mathcal{N}} \leqslant_{\mathcal{N}} [\emptyset]_{\mathcal{N}}$. ∎

Using this result we give an alternative way for computing the nilradical of a finitely generated $\emptyset$-monoid. Assume that ϱ is a canonical system of generators of a congruence σ over $\mathbb{N}^p$. In [14] there is an algorithmic procedure for computing the Archimedean components of $\mathbb{N}^p/\sigma$ from ϱ. In particular, there it is shown that if C is an Archimedean component of $\mathbb{N}^p/\sigma$, then there exist $A_1^C, \ldots, A_l^C, A^C \subseteq \{1, \ldots, p\}$ (which can be computed from ϱ) such that:

(1) $\bigcup_{i=1}^{l} A_i^C = A^C$,

(2) $[x]_\sigma \in C$ if and only if $\mathrm{Supp}(x) \subseteq A^C$ and $A_i^C \subseteq \mathrm{Supp}(x)$ for some $i \in \{1, \ldots, l\}$.

Observe that C is the maximal Archimedean component of $\mathbb{N}^p/\sigma$ if and only if $A^C = \{1, \ldots, p\}$. Applying Proposition 11, we deduce the following algorithm.

Algorithm 12.

INPUT: A canonical system of generators of a congruence σ on $\mathbb{N}^p$ with respect to a given linear admissible order $\preccurlyeq$. We assume that $\mathbb{N}^p/\sigma$ is a nontrivial $\emptyset$-monoid.

OUTPUT: A set $\{\mu_1, \ldots, \mu_r\} \subset \mathbb{N}^p$ such that $\Im(\mathrm{Nil}(\mathbb{N}^p/\sigma)) = \{\mu_1, \ldots, \mu_r\} + \mathbb{N}^p$.

Step 1: Compute $A_1^C, \ldots, A_r^C$ for the maximal Archimedean component C of $\mathbb{N}^p/\sigma$ (see [14]).

Step 2: Set $\mu_i = \sum_{j \in A_i^C} e_j$ for every $i \in \{1, \ldots, r\}$.

Step 3: Return $\{\mu_1, \ldots, \mu_r\}$; stop.

4. – Reduced $\emptyset$-monoids.

A $\emptyset$-monoid $(M, \cdot)$ is **reduced** if $\mathrm{Nil}(M) = \{\emptyset\}$. Like the definitions given abover, this one is also motivated by Ring Theory. However in the literature one can find different definitions of reduced monoid. The most common definition is that of monoid without units. In this paper a reduced $\emptyset$-monoid means $\emptyset$-monoid without nilpotent elements.

As usual we start this section giving a procedure for deciding whether a finitely generated $\emptyset$-monoid is reduced or not.

PROPOSITION 13. – *Let $(M, \cdot)$ be a $\emptyset$-monoid generated by $\{m_1, \ldots, m_p\}$ and let $\Im(\emptyset)$ be as above. Assume that $\{\lambda_1, \ldots, \lambda_r\}$ is the set of minimal elements of $\Im(\emptyset)$ with respect to $\preccurlyeq$. The following conditions are equivalent.*

(i) *M is a reduced $\emptyset$-monoid.*

(ii) *For all $i \in \{1, \ldots, r\}$, the element λ_i belongs to $\{0, 1\}^p$ (or equivalently $\lambda_i = \mu_i$, using the notation of the preceding section).*

PROOF. – (i) *implies* (ii). Assume that $\lambda_i \notin \{0, 1\}^p$. Then there exits $j \in \{1, \dots, p\}$ such that $\lambda_i - 2e_j \in \mathbb{N}^p$. It is clear that $\lambda_i - e_j \notin \Im(\emptyset)$ and $\lambda_i + (\lambda_i - 2e_j) = 2(\lambda_i - e_j) \in \Im(\emptyset)$. Hence

$$m_1^{\lambda_{i_1}} \dots m_{j-1}^{\lambda_{i_{j-1}}} m_j^{\lambda_{i_j}-1} m_{j+1}^{\lambda_{i_{j+1}}} \dots m_p^{\lambda_{i_p}} \in \mathrm{Nil}(M) \backslash \{\emptyset\}.$$

(ii) *implies* (i). Assume that $x = m_1^{k_1} \dots m_p^{k_p} \in \mathrm{Nil}(M)$. Then there exists $k \in \mathbb{N} \backslash \{0\}$ such that $x^k = \emptyset$, whence $k(k_1, \dots, k_p) \in \Im(\emptyset)$. Thus we can find $i \in \{1, \dots, r\}$ and $y \in \mathbb{N}^p$ such that $(kk_1, \dots, kk_p) = \lambda_i + y$. Since $\lambda_i \in \{0, 1\}^p$, there exists $z \in \mathbb{N}^p$ for which $(k_1, \dots, k_p) = \lambda_i + z$. This implies $(k_1, \dots, k_p) \in \Im(\emptyset)$ and consequently $x = \emptyset$. ■

Let σ be a congruence on $\mathbb{N}^p$ such that $\mathbb{N}^p/\sigma$ is a $\emptyset$-monoid and ϱ a system of generators of σ. With the results shown in Section **2**, we can compute from ϱ the set of minimal elements of $\Im(\emptyset)$ with respect to $\leqslant$. Thus Proposition 13 gives an effective method for deciding whether $\mathbb{N}/\sigma$ is a reduced $\emptyset$-monoid or not.

Another way to decide whether $\mathbb{N}^p/\sigma$ is a reduced $\emptyset$-monoid or not is achieved with the help of the following proposition.

PROPOSITION 14. – *Let* $(M, \cdot)$ *be a* $\emptyset$*-monoid generated by* $\{m_1, \dots, m_p\}$ *and let* $\Im(\mathrm{Nil}(M))$ *be as above. Assume that* $\Im(\mathrm{Nil}(M)) = \{\lambda_1, \dots, \lambda_r\} + \mathbb{N}^p$. *The following conditions are equivalent.*

(i) M *is a reduced* $\emptyset$*-monoid.*

(ii) *For all* $i \in \{1, \dots, r\}$, $(m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}})^2 = m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}}$, *where* $(\lambda_{i_1}, \dots, \lambda_{i_p}) = \lambda_i$.

PROOF. – (i) *implies* (ii). If $\mathrm{Nil}(M) = \{\emptyset\}$, then $m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}} = \emptyset$ and clearly $\emptyset^2 = \emptyset$.

(ii) *implies* (i). If $(m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}})^2 = m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}}$, then $m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}}$ is an idempotent element of $\mathrm{Nil}(M)$. Recall that $\mathrm{Nil}(M)$ is an Archimedean component of M and thus an Archimedean semigroup. In [16] it is shown that every Archimedean semigroup has at most an idempotent element, and since $\emptyset$ is an idempotent element of $\mathrm{Nil}(M)$, we conclude that $\emptyset = m_1^{\lambda_{i_1}} \dots m_p^{\lambda_{i_p}}$. ■

Using the results obtained in Section **3** and Proposition 14 we can decide whether $\mathbb{N}^p/\sigma$ is a reduced $\emptyset$-monoid or not: we can compute $\lambda_1, \dots, \lambda_r$ such that $\Im(\mathrm{Nil}(\mathbb{N}^p/\sigma)) = \{\lambda_1, \dots, \lambda_r\} + \mathbb{N}^p/\sigma$; thus we only have to check whether $\lambda_i \sigma 2\lambda_i$ holds or not for all i and this can be achieved using NF_ϱ with ϱ a canonical system of generators of σ.

Our next goal is to describe the set $\mathcal{ZD}(M)$ in the case M is a reduced $\emptyset$-monoid.

Given a monoid $(M, \cdot)$, set

$$\mathcal{U}(M) = \{x \in M \mid xy = 1 \text{ for some } y \in M\},$$

which is a group called the **group of units** of M. If M is a $\emptyset$-monoid, we already know that $\mathrm{Nil}(M) = \max_{\leq_{\mathcal{N}}}(M/\mathcal{N})$. It can be easily proved that $\mathcal{U}(N) = \min_{\leq_{\mathcal{N}}}(M/\mathcal{N})$. In [14] it is shown that a finite semilattice with maximum and minimum is a lattice and therefore there exists the supremum and infimum of every pair of elements. Observe that this is the case for $(M/\mathcal{N}, \leq_{\mathcal{N}})$ with M a finitely generated monoid.

THEOREM 15. – *Let $(M, \cdot)$ be a finitely generated reduced $\emptyset$-monoid and let*

$$\{C_1, \ldots, C_r\} = \mathrm{Maximals}_{\leq_{\mathcal{N}}}(M/\mathcal{N} \setminus \{\mathrm{Nil}(M)\})$$

($\mathrm{Maximals}_{\leq_{\mathcal{N}}}(A)$ *stands for the set of maximal elements of the set A with respect to the order $\leq_{\mathcal{N}}$). If $C = \mathrm{infimum}_{\leq_{\mathcal{N}}}\{C_1, \ldots, C_r\}$ (*$\mathrm{infumum}_{\leq_{\mathcal{N}}} A$ *denotes the infimum of A with respect to $\leq_{\mathcal{N}}$), then the following conditions are equivalent:*

(i) $x \notin \mathcal{ZD}(M)$,

(ii) $[x]_{\mathcal{N}} \leq_{\mathcal{N}} C$.

PROOF. – (*i*) *implies* (*ii*). Assume that $[x]_{\mathcal{N}} \leq_{\mathcal{N}} C$ does not hold. Then there exists $j \in \{1, \ldots, r\}$ such that $[x]_{\mathcal{N}} \leq_{\mathcal{N}} C_j$ does not hold. Hence for $y \in C_j$, we obtain $[x]_{\mathcal{N}}[y]_{\mathcal{N}} = \mathrm{Nil}(M) = \{\emptyset\}$ and therefore $xy = \emptyset$. Since $y \neq \emptyset$, we get $x \in \mathcal{ZD}(M)$.

(*ii*) *implies* (*i*). If $y \neq \emptyset$, then $y \notin \{\emptyset\} = \mathrm{Nil}(M)$, whence $[y]_{\mathcal{N}} \leq_{\mathcal{N}} C_j$ for some $j \in \{1, \ldots, r\}$. This leads to the fact $[x]_{\mathcal{N}}[y]_{\mathcal{N}} \leq C_j$ and consequently $xy \neq \emptyset$. ■

We conclude this section studying a special kind of reduced $\emptyset$-monoids, the so called **integral monoids**, which are those $\emptyset$-monoids such that $\mathcal{ZD}(M) = \{\emptyset\}$. Every integral monoid is a reduced $\emptyset$-monoid.

PROPOSITION 16. – *Let $(M, \cdot)$ be a $\emptyset$-monoid. The following conditions are equivalent.*

(i) *M is an integral monoid.*

(ii) *M is reduced and $\{[\emptyset]_{\mathcal{N}}\}$ is a prime ideal of $M/\mathcal{N}$.*

PROOF. – (*i*) *implies* (*ii*). If M is an integral monoid, then it is reduced and $[\emptyset]_{\mathcal{N}} = \mathrm{Nil}(M) = \{\emptyset\}$. Assume that there exists $x, y \in M$ such that $[x]_{\mathcal{N}}[y]_{\mathcal{N}} = \{\emptyset\}$ and $[x]_{\mathcal{N}} \neq \{\emptyset\} \neq [y]_{\mathcal{N}}$. Then $xy = \emptyset$, but $x \neq \emptyset \neq y$, which contradicts the fact that M is an integral monoid.

(*ii*) *implies* (*i*). If $xy = \emptyset$, then $\{\emptyset\} = [\emptyset]_{\mathcal{N}} = [x]_{\mathcal{N}}[y]_{\mathcal{N}}$. Hence either $[x]_{\mathcal{N}} = \{\emptyset\}$ or $[y]_{\mathcal{N}} = \{\emptyset\}$ and consequently either $x = \emptyset$ or $y = \emptyset$. ■

We now give an algorithmic procedure for deciding whether a finitely generated $\emptyset$-monoid is an integral monoid or not. From the results obtained at the beginning of this section we can already check whether a finitely generated $\emptyset$-monoid is reduced or not. Using Proposition 16 it is enough to give a method for finding out if $\{[\emptyset]_{\mathcal{N}}\}$ is a prime ideal of $M/\mathcal{N}$. This method is derived from the following proposition.

PROPOSITION 17. – *Let* $(M, \cdot)$ *be a nontrivial finitely generated* $\emptyset$*-monoid. Then* $\{[\emptyset]_{\mathcal{N}}\}$ *is a prime ideal of* $M/\mathcal{N}$ *if and only if there is only one maximal element in* $M/\mathcal{N}\setminus\{[\emptyset]_{\mathcal{N}}\}$.

PROOF. – Recall that $[\emptyset]_{\mathcal{N}} = \max_{\leqslant_{\mathcal{N}}}(M/\mathcal{N})$ and that $\mathcal{U}(M) = [1]_{\mathcal{N}} = \min_{\leqslant_{\mathcal{N}}}(M/\mathcal{N})$. Note also that $[1]_{\mathcal{N}} \neq [\emptyset]_{\mathcal{N}}$ and that $M/\mathcal{N}$ is finite.

Necessity. If $[x]_{\mathcal{N}}, [y]_{\mathcal{N}} \in \mathrm{Maximals}_{\leqslant_{\mathcal{N}}}(M/\mathcal{N}\setminus\{[\emptyset]_{\mathcal{N}}\})$ and $[x]_{\mathcal{N}} \neq [y]_{\mathcal{N}}$, then applying the definition of $\leqslant_{\mathcal{N}}$ we obtain $[x]_{\mathcal{N}}[y]_{\mathcal{N}} = [\emptyset]_{\mathcal{N}}$, whence $\{[\emptyset]_{\mathcal{N}}\}$ is not a prime ideal of $M/\mathcal{N}$.

Sufficiency. Take C to be the only maximal element of $M/\mathcal{N}\mathcal{N}\{[\emptyset]_{\mathcal{N}}\}$ with respect to $\leqslant_{\mathcal{N}}$. If $[x]_{\mathcal{N}} \neq [\emptyset]_{\mathcal{N}} \neq [y]_{\mathcal{N}}$, then $[x]_{\mathcal{N}} \leqslant_{\mathcal{N}} C$ and $[y]_{\mathcal{N}} \leqslant_{\mathcal{N}} C$. Thus $[x]_{\mathcal{N}}[y]_{\mathcal{N}} \leqslant_{\mathcal{N}} C$ and for this reason $[x]_{\mathcal{N}}[y]_{\mathcal{N}} \neq [\emptyset]_{\mathcal{N}}$. ■

Let σ be a congruence on $\mathbb{N}^p$ and C_1, C_2 be two Archimedean components of $\mathbb{N}^p/\sigma$. Using the same notation introduced at the end of Section 3, it is easy to show that $C_1 \leqslant_{\mathcal{N}} C_2$ if and only if $A^{C_1} \subseteq A^{C_2}$.

Algorithm 18.

INPUT: A canonical system of generators of a congruence σ on $\mathbb{N}^p$ with respect to a given linear admissible order $\leqslant$. We assume that $\mathbb{N}^p/\sigma$ is a nontrivial $\emptyset$-monoid.

OUTPUT: «$\mathbb{N}^p/\sigma$ is an integral monoid» or «$\mathbb{N}^p/\sigma$ is not an integral monoid».

Step 1: Compute $A = \{A^C \mid C$ is an Archimeden component of $\mathbb{N}^p/\sigma\}$ (see [14]).

Step 2: Compute $B = \mathrm{Maximals}_{\subseteq}(A\ \{1, \ldots, p\})$ (maximals with respect to the set-inclusion order).

Step 3: If B has more than two elements, then Return «$\mathbb{N}^p/\sigma$ is not an integral monoid»; stop.

Step 4: Check if $\mathbb{N}^p/\sigma$ is reduced.

Step 5: If $\mathbb{N}^p/\sigma$ is not reduced, Return «$\mathbb{N}^p/\sigma$ is not an integral monoid»; stop.

Step 6: Return «$\mathbb{N}^p/\sigma$ is an integral monoid»; stop.

5. – Radical, prime and primary ideals of a monoid.

In this section we apply the results obtained above in order to decide whether a given ideal of a finitely generated monoid is prime, radical or primary. To this end we recall the concept of Rees congruence associated to an ideal.

Given an ideal I of a monoid $(A, \cdot)$, the **Rees congruence** associated to I (see for instance [8]) is defined by $a \mathcal{R}_I b$ if either $\{x, y\} \subseteq I$ or $x = y$.

LEMMA 19. – *Let I be an ideal of a monoid $(A, \cdot)$. Then the monoid $A/\mathcal{R}_I$ is a $\emptyset$-monoid.*

PROOF. – Take $x \in I$. Since I is an ideal, for all $a \in A$, we have $xa \in I$. This implies that $[a]_{\mathcal{R}_I}[x]_{\mathcal{R}_I} = [x]_{\mathcal{R}_I}$ and thus $[x]_{\mathcal{R}_I} = \emptyset$. ∎

The following result points out the connection between the concepts of prime, radical and primary ideal, and the concepts studied in the preceding sections. An ideal I of a monoid $(A, \cdot)$ is **primary** if whenever $xy \in I$ for some $x, y \in A$ and $x \notin I$, we get $y^k \in I$ for some $k \in \mathbb{N} \setminus \{0\}$.

PROPOSITION 20. – *Let I be an ideal of the monoid $(A, \cdot)$.*

(1) *I is a prime ideal if and only if $A/\mathcal{R}_I$ is an integral monoid.*

(2) *I is a radical ideal if and only if $A/\mathcal{R}_I$ is a reduced $\emptyset$-monoid.*

(3) *I is a primary ideal if and only if* $\mathrm{Nil}(A/\mathcal{R}_I) = \mathcal{ZD}(A/\mathcal{R}_I)$.

PROOF. – (1) *Necessity.* Let $[x]_{\mathcal{R}_I} \in \mathcal{ZD}(A/\mathcal{R}_I)$. Then there exists $y \notin I$ such that $[x]_{\mathcal{R}_I}[y]_{\mathcal{R}_I} = \emptyset$. Hence $xy \in I$ and $y \notin I$, which implies that $x \in I$, whence $[x]_{\mathcal{R}_I} = \emptyset$. Thus $\mathcal{ZD}(A/\mathcal{R}_I) = \{\emptyset\}$ and consequently $A/\mathcal{R}_I$ is an integral monoid.

Sufficiency. If $xy \in I$, then $[x]_{\mathcal{R}_I}[y]_{\mathcal{R}_I} = \emptyset$ and therefore either $[x]_{\mathcal{R}_I} = \emptyset$ or $[y]_{\mathcal{R}_I} = \emptyset$, which leads to either $x \in I$ or $y \in I$.

(2) *Necessity.* If $[x]_{\mathcal{R}_I} \in \mathrm{Nil}(A/\mathcal{R}_I)$, then there exists $k \in \mathbb{N} \setminus \{0\}$ such that $x^k \in I$. By hypothesis, this implies $x \in I$ and thus $[x]_{\mathcal{R}_I} = \emptyset$.

Sufficiency. If $x^k \in I$ for some $k \in \mathbb{N} \setminus \{0\}$, then $[x]^k_{\mathcal{R}_I} = \emptyset$. This means $[x]_{\mathcal{R}_I} \in \mathrm{Nil}(A/\mathcal{R}_I) = \{\emptyset\}$, whence $x \in I$.

(3) *Necessity.* Take $[x]_{\mathcal{R}_I} \in \mathcal{Z}\mathcal{D}(A/\mathcal{R}_I)$. Then there exists $y \notin I$ such that $[x]_{\mathcal{R}_I}[y]_{\mathcal{R}_I} = \emptyset$. Hence $xy \in I$ and $y \notin I$. Since I is primary, there exists $k \in \mathbb{N}\setminus\{0\}$ such that $x^k \in I$, which leads to $[x]^k_{\mathcal{R}_I} = \emptyset$ and therefore $[x]_{\mathcal{R}_I} \in \mathrm{Nil}(A/\mathcal{R}_I)$. The other inclusion follows from the definition of $\mathrm{Nil}(A/\mathcal{R}_I)$ and $\mathcal{Z}\mathcal{D}(A/\mathcal{R}_I)$.

Sufficiency. If $xy \in I$ and $x \notin I$, then $[x]_{\mathcal{R}_I}[y]_{\mathcal{R}_I} = \emptyset$ and $[x]_{\mathcal{R}_I} \neq \emptyset$. Hence $[y]_{\mathcal{R}_I} \in \mathcal{Z}\mathcal{D}(A/\mathcal{R}_I) = \mathrm{Nil}(A/\mathcal{R}_I)$, which yields $[y]^k_{\mathcal{R}_I} = \emptyset$ for some $k \in \mathbb{N}\setminus\{0\}$. Therefore $y^k \in I$. ■

If we want to apply Proposition 20 to a finitely generated monoid $A = \mathbb{N}^p/\sigma$ for which a system of generators ϱ of σ is known, we still need to figure out how to construct $A/\mathcal{R}_I$ for any ideal I of A. The following will be of great help for this purpose. If $\varrho = \{(\alpha_1, \beta_1), \dots, (\alpha_t, \beta_t)\}$ and $I = \{[\lambda_1]_\sigma, \dots, [\lambda_r]_\sigma\} + A$, define

$$\varrho_I = \{(\lambda_1, \lambda_2), \dots, (\lambda_1, \lambda_r), (\lambda_1 + e_1, \lambda_1), \dots, (\lambda_1 + e_p, \lambda_1)\},$$

set $\overline{\varrho} = \varrho \cup \varrho_I$, and let $\overline{\sigma}$ be the congruence on $\mathbb{N}^p$ generated by $\overline{\varrho}$.

LEMMA 21. – *Let A, σ, ϱ, I, ϱ_I, $\overline{\varrho}$ and $\overline{\sigma}$ be as above. For every $x, y \in \mathbb{N}^p$, $[x]_{\overline{\sigma}} = [y]_{\overline{\sigma}}$ if and only if either $[x]_\sigma = [y]_\sigma$ or $\{[x]_\sigma, [y]_\sigma\} \subseteq I$.*

PROOF. – *Necessity.* Assume that $[x]_{\overline{\sigma}} = [y]_{\overline{\sigma}}$ and that $[x]_\sigma \neq [y]_\sigma$. We must prove that $\{[x]_\sigma, [y]_\sigma\} \subseteq I$. Since $x\overline{\sigma}y$ holds, there exist $v_0, \dots, v_l \in \mathbb{N}^p$ such that $v_0 = x$, $v_l = y$ and $(v_i, v_{i+1}) \in \overline{\varrho}_1$ for all $i \in \{0, \dots, l-1\}$ (see the preliminaries). Moreover $[x]_\sigma \neq [y]_\sigma$ and thus there is an $i \in \{1, \dots, l-1\}$ such that $(v_i, v_{i+1}) \notin \varrho_1$. Set $k = \min\{i \mid (v_i, v_{i+1}) \notin \varrho_1\}$. Then $x\sigma v_k$ holds and since $(v_k, v_{k+1}) \notin \varrho_1$, we get that there exist $(a, b) \in \varrho_I \cup \varrho_I^{-1}$ and $c \in \mathbb{N}^p$ such that $(v_k, v_{k+1}) = (a + c, b + c)$. This implies that $[x]_\sigma = [v_k]_\sigma \in I$. In a similar way one gets $[y]_\sigma \in I$.

Sufficiency. Clearly $\sigma \subseteq \overline{\sigma}$ and thus $[x]_\sigma = [y]_\sigma$ implies $[x]_{\overline{\sigma}} = [y]_{\overline{\sigma}}$. If $\{[x]_\sigma, [y]_\sigma\} \subseteq I$, then there exist $i, j \in \{1, \dots, r\}$ and $z, t \in \mathbb{N}^p$ such that $[x]_\sigma = [\lambda_i]_\sigma + [z]_\sigma$ and $[y]_\sigma = [\lambda_j]_\sigma + [t]_\sigma$. This means that $x\sigma(\lambda_i + z)$ and that $y\sigma(\lambda_j + t)$. Applying that $\varrho_I \subseteq \overline{\varrho}$ one can easily deduce that $(\lambda_i + z)\overline{\sigma}\lambda_1$ and $(\lambda_j + t)\overline{\sigma}\lambda_1$ hold. Hence $[x]_{\overline{\sigma}} = [y]_{\overline{\sigma}}$. ■

THEOREM 22. – *Under the same hypothesis of Lemma 21, the monoid $A/\mathcal{R}_I$ is isomorphic to $\mathbb{N}^p/\overline{\sigma}$.*

PROOF. – Define $f : A \to \mathbb{N}^p/\overline{\sigma}$, $f([x]_\sigma) = [x]_{\overline{\sigma}}$. Using that $\sigma \subseteq \overline{\sigma}$, we deduce that f is well defined. Moreover f is a monoid epimorphism. To conclude the proof, it suffices to show that the kernel congruence of f is exactly $\mathcal{R}_I$. But this follows easily from Lemma 21. ■

Summarizing, Proposition 20, Theorem 22 and the algorithms given in the preceding sections provide us with effective methods for deciding whether the ideal $I = \{[\lambda_1]_\sigma, \ldots, [\lambda_r]_\sigma\} + \mathbb{N}^p/\sigma$ is prime, radical or primary once we know a system of generators of σ.

REFERENCES

[1] D. D. ANDERSON - E. W. JOHNSON, *Ideal Theory in commutative semigroups*, Semigroup Forum, **30** (1984), 127-158.
[2] I. ARNOLD, *Ideale in kommutative Halbgruppen*, Mat. Sb., **35** (1929), 401-408.
[3] S. T. CHAPMAN - U. KRAUSE - E. OELJEKLAUS, *Monoids determined by a homogeneus linear Diophantine equation and the half factorial property*, to appear in J. Pure Appl. Algebra.
[4] A. H. CLIFFORD, *Arithmetic and ideal theory of commutative semigroups*, Ann. of Math., **39** (1938), 594-610.
[5] A. H. CLIFFORD - G. B. PRESTON, *The algebraic theory of semigroups*, Amer. Math. Soc., Providence, 1961.
[6] A. GEROLDINGER, *On the structure and arithmetic of finitely primary monoids*, Czech. Math. J., **46** (1996), 677-695.
[7] R. GILMER, *Multiplicative ideal theory*, Marcel Dekker, New York, 1972.
[8] R. GILMER, *Commutative semigroup rings*, Chicago Lectures in Mathematics, 1984.
[9] F. HALTER-KOCH, *Ideal systems. An introduction to multiplicative ideal theory*, Marcel Dekker Inc., 1998.
[10] M. D. LARSEN - P. J. MCCARTHY, *Multiplicative theory of ideals*, Academic Press, New York and London, 1971.
[11] G. LETTL, *Subsemigroups of finitely generated groups with divisor-theory*, Monatsh. Math., **106** (1988), 205-210.
[12] L. RÉDEI, *The theory of finitely generated commutative semigroups*, Pergamon, Oxford-Edinburgh-New York, 1965.
[13] J. C. ROSALES, *Function minimum associated to a congruence on integral n-tuple space*, Semigroup Forum, **51** (1995), 87-95.
[14] J. C. ROSALES - P. A. GARCÍA-SÁNCHEZ, *Finitely generated commutative monoids*, Nova Science Publishers, New York, 1999.
[15] T. TAMURA - N. KIMURA, *On decompositions of a commutative semigroup*, Kodai Math. Sem. Rep., 1954, 109-112.
[16] P. A. GRILLET, *Semigroups. An introduction to the structure theory*, Dekker, 1995.

Departamento de Álgebra, Universidad de Granada, E-18071 Granada, Spain
E-mail: jrosales@ugr.es

Pervenuta in Redazione
il 9 aprile 2001