Reprinted from JOURNAL OF ALGEBRA
Vol. 13, No. 2, October 1969
Printed in Belgium


# Rational Sets in Commutative Monoids*

SAMUEL EILENBERG

*Department of Mathematics, Columbia University, New York, New York 10027*

AND

M. P. SCHÜTZENBERGER

*Faculté des Sciences de Paris, Paris, France*

*Communicated by Saunders MacLane*

Received August 3, 1969

## 1. RATIONAL SETS

Let $M$ be a monoid, i.e. a set with an associative multiplication and a two sided unit. The class of *rational* subsets of $M$ is the least class $\mathscr{E}$ of subsets of $M$ satisfying the following conditions:

(1R) The empty set is in $\mathscr{E}$;

(2R) Each single element set is in $\mathscr{E}$;

(3R) If $X, Y \in \mathscr{E}$ then $X \cup Y \in \mathscr{E}$;

(4R) If $X, Y \in \mathscr{E}$ then $XY \in \mathscr{E}$;

(5R) If $X \in \mathscr{E}$ then $X^* \in \mathscr{E}$.

We recall that

$$XY = \{m \mid m = xy, x \in X, y \in Y\},$$

$$X^* = \text{submonoid of } M \text{ generated by } X.$$

Kleene's theorem asserts that if $M$ is free and finitely generated, then the rational sets are precisely the subsets of $M$ recognizable by finite state automata.

Inspired by the notion of unambiguous context-free languages as introduced by Chomsky, we define the smaller class of *unambiguously rational* subsets of $M$ by leaving conditions (1R) and (2R) as they are but replacing conditions (3R)–(5R) by stronger conditions (3UR)–(5UR) as follows:

(3UR) If $X, Y \in \mathscr{E}$ and $X \cap Y = \varnothing$ then $X \cup Y \in \mathscr{E}$;

(4UR) If $X, Y \in \mathscr{E}$ and the product $XY$ is unambiguous (i.e.,

* Work supported in part by contracts NONR 266(57) and AF 61(052)-945.

$x_1y_1 = x_2y_2$ for $x_1, x_2 \in X, y_1, y_2 \in Y$ implies $x_1 = x_2, y_1 = y_2$), then $XY \in \mathscr{E}$;

(5UR) If $X \in \mathscr{E}$ and $X$ is the basis of a free submonoid $X^*$ of $M$, then $X^* \in \mathscr{E}$.

UNAMBIGUITY THEOREM. *In a free monoid $M$ every rational set is unambiguously rational.*

This theorem is stated here for background only as it will not be used in the sequel.

The conclusion of the theorem is false without the assumption of freeness. Indeed let $M$ be the monoid obtained from the free monoid on three generators by collapsing to a single point the ideal $I = \{uwwv \mid w \neq 1\}$. In $M$ every cyclic submonoid is finite and therefore every unambiguously national set is finite. However $X \backslash I$ is known to be infinite [1, p. 30, Satz 18] so that $M$ is infinite. Since $M$ is finitely generated, it is rational without being unambiguously so.

For future use, we tabulate here some elementary properties of rational sets.

(1.1) If $X$ is a rational subset of $M$, then there exists a finitely generated submonoid $M'$ of $M$ containing $X$.

(1.2) $M$ is a rational subset of itself if and only if it is finitely generated.

(1.3) If $\varphi : M' \to M$ is a morphism of monoids and $X'$ is a rational subset of $M'$, then $X = \varphi X'$ is a rational subset of $M$.

(1.4) If $\varphi : M' \to M$ is a surjective morphism of monoids and if $X$ is a rational subset of $M$, then there is a rational subset $X'$ of $M'$ such that $X = \varphi X'$.

(1.5) If $X_1, X_2$ are rational subsets of $M_1, M_2$ respectively, then $X_1 \times X_2$ is a rational subset of $M_1 \times M_2$.

## 2. COMMUTATIVE MONOIDS

The objective of this paper is to study rational subsets in commutative monoids. We shall use additive notation throughout. In line with this in conditions (4R) and (4UR), $XY$ is to be replaced by $X + Y$.

The main result of this paper is that in all commutative monoids, rational sets are unambiguously rational (Theorem IV below).

The study of rational sets in a commutative monoid $M$ is simplified by the following notions. A subset

$$X = a + B^* \tag{2.1}$$

with $a \in M$, $B \subset M$, $B$ finite, is called *linear*. Here and in the sequel we write $a + B^*$ instead of $\{a\} + B^*$. If further the sum in (2.1) is unambiguous and the elements of $B$ are linearly independent (i.e., $B^*$ is a free commutative monoid with basis $B$), then $X$ is called *simple*. If $B = \{b_1, \ldots, b_r\}$ is a set of $r$ elements, then every element $x \in X$ may be written as

$$x = a + n_1 b_1 + \cdots + n_r b_r$$

with $n_i \in N$ (i.e., $n_i \geqslant 0$). If $X$ is simple, then $n_1, \ldots, n_r$ are unique.

A finite union of linear sets is called *semi-linear*. A finite *disjoint* union of simple sets is called *semi-simple*.

Clearly every semi-linear set is rational and every semi-simple set is unambiguously rational. The converse is also true. To see that, let $\mathscr{E}$ (respectively $\mathscr{E}'$) denote the class of semi-linear (respectively semi-simple) subsets of $M$. Clearly $\mathscr{E}$ satisfies conditions (1R), (2R) and (3R) while $\mathscr{E}'$ satisfies conditions (1R), (2R), and (3UR). Next assume that

$$X = \cup (a_i + B_i^*), \qquad Y = \cup (c_j + D_j^*) \tag{2.2}$$

the unions being finite as well as the sets $B_i$, $D_j$. Then

$$X + Y = \bigcup_{i,j} [a_i + c_j) + (B_i \cup D_j)^*] \tag{2.3}$$

which shows that $X + Y$ is semi-linear. If in (2.2) $X$ and $Y$ are given in semi-simple decompositions and if the sum $X + Y$ is unambiguous, then the union in (2.3) is disjoint and the sets in brackets are simple. Thus $X + Y$ is semi-simple.

Next note that $X^* = E^*$ where $E = \bigcup [\{a_i\} \cup B_i]$. Thus $X^* \in \mathscr{E}$ so that $\mathscr{E}$ satisfies condition (5R).

Suppose now that the decomposition of $X$ given in (2.2) is semi-simple and that $X$ is the basis of a free submonoid $X^*$ of $M$. Since $M$ is commutative, it follows that $X$ is a single point and $X^*$ is simple. This concludes the argument.

## 3. The Main Results

We recall that a congruence $Q$ in a monoid $M$ is an equivalence relation in $M$ which when viewed as a subset of $M \times M$ is a submonoid.

THEOREM I. *Every congruence $Q$ in a finitely generated commutative monoid $M$ has a rational cross-section*; i.e., *a rational set containing exactly one element from each equivalence class* mod $Q$.

THEOREM II. *Every congruence $Q$ in a finitely generated commutative monoid $M$ is a rational subset of $M \times M$.*

THEOREM III. *If $X$ and $Y$ are rational subsets of a commutative monoid $M$, then their intersection $X \cap Y$ and difference $Y \backslash X$ also are rational subsets of $M$.*

THEOREM IV. *In a commutative monoid $M$ every rational set is unambiguously rational.*

Sections 4 and 5 are devoted to preparations. Theorem I is proved in Section 6. In Section 7 the important notion of a slice is introduced and Theorem II is proved in Section 8. After more preparation in Section 9, Theorems III and IV are proved in Section 10. The proofs of these theorems for finitely generated free monoids are independent of Theorems I and II. Theorems I and II are used to pass to arbitrary commutative monoids. Sections 11–14 are devoted to corollaries, counterexamples, and other applications.

Theorem III, in the case of finitely generated free commutative monoids, was proved by Ginsburg and Spanier [2]. Some of their arguments are reproduced here in order to make this paper entirely self-contained.

## 4. ORDER PROPERTIES OF $N^k$

We denote by $Z^k$ the free commutative group on $k$ letters. The elements of $Z^k$ are then $n$-tuples $x = (x_1, \ldots, x_k)$ of integers. The conditions $0 \leqslant x_i$, $i = 1, \ldots, k$, determine the submonoid $N^k$ which is the free commutative monoid on $k$ letters.

In $N^k$ we define the (partial) order $x \leqslant y$ by the condition $x_i \leqslant y_i$ for $i = 1, \ldots, k$. We shall write $x < y$ if $x \leqslant y$ and $x \neq y$.

Let $X \subset N^k$ and let $y \in N^k$. The sets

$$X^{\nu} = \{x \mid x \in X, y \leqslant x\}, \qquad X_y = \{x \mid x \in X, y \text{ non} \leqslant x\}$$

will be called the *upper* and the *lower part* of $X$ relative to $y$. Clearly

$$X^{\nu} = y + (X - y) \tag{4.1}$$

where $X - y = \{z \mid z \in N^k, z + y \in X\}$. The lower part $X_y$ will be decomposed into disjoint components as follows.

Consider all pairs

$$(i, s),\ 1 \leqslant i \leqslant k,\ 0 \leqslant s < y_i \tag{4.2}$$

and define

$$y_{is} = (y_1, \ldots, y_{i-1}, s, 0, \ldots, 0) \in N^k.$$

If $x \in X_y$, then there exists exactly one pair $(i, s)$ such that

$$y_t \leqslant x_t \quad \text{for} \quad t < i, \qquad x_i = s < y_i$$

or equivalently

$$x = y_{is} + x' \qquad \text{with} \qquad x' \in N^k, x_i' = 0.$$

If we denote by $N_i^k$ the submonoid of $N^k$ determined by the condition $x_i = 0$, then we find that $X_y$ is the disjoint union of the sets

$$y_{is} + (X - y_{is}) \cap N_i^k. \tag{4.3}$$

These are the *components* of $X_y$.

This decomposition of $X$ according to an element $y \in N^k$ will be used systematically as a tool in the proofs. As a first example, we prove (the well known)

PROPOSITION 4.1. *Every set $X$ in $N^k$ of mutually incomparable elements is finite.*

*Proof.* Let $y \in X$. Since the elements of $X$ are incomparable, we have $X - y = \{0\}$ and thus

$$X^y = y + (X - y) = \{y\}.$$

For any $(i, s)$, the set $X - y_{is}$ is composed of mutually incomparable elements and thus the same holds for $(X - y_{is}) \cap N_i^k$. Thus by recursion, this set is finite. Consequently, all the components of (4.3) are finite and so is $X$.

PROPOSITION 4.2. *For any subset $X$ of $N^k$, the set $V$ of minimal elements of $X$ is finite and $X \subset V + N^k$.*

The finiteness of $V$ follows from Proposition 4.1. The inclusion is clear.

## 5. IDEALS

A subset $I$ of a commutative monoid $M$ is called an *ideal* if $I + M \subset I$.

PROPOSITION 5.1. *In a finitely generated monoid $M$ every ideal $I$ has the form $F + M$ where $F$ is a finite subset of $M$.*

*Proof.* Since $M$ is finitely generated, there exists a surjective morphism $\varphi : N^k \to M$. For every ideal $I$ in $M$ the set $\varphi^{-1}I$ is an ideal in $N^k$. Thus it suffices to consider $M = N^k$.

Let then $I$ be an ideal in $N^k$ and let $F$ be the set of minimal elements in $I$. Then by Proposition 4.2, $F$ is finite and $I \subset F + N^k$. Since $I$ is an ideal, we have $F + N^k \subset I + N^k \subset I$. Thus $I = F + N^k$.

PROPOSITION 5.2. *In a finitely generated commutative monoid $M$ the ideals satisfy the ascending chain condition.*

*Proof.* Let $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ be ideals in $M$, and let $I = \bigcup I_n$. Then $I$ is an ideal in $M$. Thus $I = F + M$ where $F$ is a finite subset. Consequently, $F \subset I_n$ for some integer $n$. Thus $I \subset I_n$ and $I = I_n$.

## 6. PROOF OF THEOREM I

PROPOSITION 6.1. *Every congruence $Q$ in $N^k$ has a cross-section $A$ such that $N^k \backslash A$ is an ideal.*

*Proof.* In $N^k$ we consider the lexicographic order $x \prec y$ given by $x = y$ or

$$x_1 = y_1, \ \ldots \ x_{i-1} = y_{i-1}, \ \ x_i < y_i$$

for some $i = 1,\ldots, k$. We note that this is a well-ordering of $N^k$ satisfying

$$x \prec y \Leftrightarrow x + z \prec y + z$$

for any $x, y, z \in N^k$.

Given a congruence $Q$ in $N^k$ and given $x \in N^k$ let $\rho x$ denote the smallest element in the lexicographic order such that $\rho x \sim x \pmod{Q}$. We thus have

$$\rho x \prec x, x \sim \rho x, \ \ \rho\rho x = \rho x.$$

Let $x, y \in N^k$. Then $\rho(x + y) \sim x + y \sim \rho x + \rho y$ and therefore

$$\rho(x + y) \prec \rho x + \rho y. \tag{6.1}$$

Let

$$A = \{x \mid x \in N^k, x = \rho x\}.$$

Clearly $A$ is a cross-section for $Q$. Let $x \in N^k \backslash A, y \in N^k$. Then $\rho x \prec x, \rho x \neq x$. Consequently

$$\rho(x + y) \prec \rho x + \rho y \prec x + \rho y \prec x + y.$$

Since $\rho x \neq x$, we have $\rho x + \rho y \neq x + \rho y$. Therefore, $\rho(x + y) \neq x + y$ so that $x + y \in N^k \backslash A$. Thus $N^k \backslash A$ is an ideal.

*Proof of Theorem* I. Let $Q$ be a congruence in a finitely generated monoid $M$. Choose a surjective morphism $\varphi : N^k \to M$ and let $Q'$ be the congruence in $N^k$ defined by

$$x \sim y \Leftrightarrow \varphi x \sim \varphi y.$$

Let $A$ be the cross-section for $Q'$ as given by Proposition 6.1. Then clearly $\varphi A$ is a cross-section for $Q$. To show that $\varphi A$ is rational, it suffices to show that $A$ is a rational subset of $N^k$. Since $I = N^k \backslash A$ is an ideal, it follows from Proposition 5.1 that $I$ is rational. Since $A = N^k \backslash I$ the rationality of $A$ follows from Theorem III. The reader will have to be careful to note that Theorem I is not used until *after* Theorem III has been proved.

## 7. Subtractive Submonoids and Slices

Let $S$ be a submonoid of a commutative monoid $M$. We shall say that $S$ is *subtractive*, if $x, x + y \in S$, $y \in M$, imply $y \in S$. This may equivalently be rephrased as $S - S \subset S$ or $S - S = S$.

Proposition 7.1. *Every subtractive submonoid $S$ of a finitely generated monoid $M$ is itself finitely generated.*

*Proof.* Let $\varphi : N^k \to M$ be a surjective morphism and let $S' = \varphi^{-1}S$. Then $S'$ is a subtractive submonoid of $N^k$ and if $S'$ is finitely generated, then so is $S = \varphi S'$. Thus we may assume that $M = N^k$.

Let $A$ be the set of all minimal elements in $S \backslash \{0\}$. Then $A$ is finite and $A^* \subset S$. Assume $A^* \neq S$ and let $x$ be a minimal element of the set $S \backslash A^*$. Then $a \leqslant x$ for some element $a \in A$, so that $x = a + y$ with $y \in N^k$. Since $S$ is subtractive, we have $y \in S$. Since $y < x$ we have $y \in A^*$. Thus $x = a + y \in A^*$, a contradiction.

A *slice* in a commutative monoid $M$ is a subset $S$ such that $s, s + x$, $s + y \in S$ imply $s + x + y \in S$. Equivalently, $S$ is a slice if and only if for every $s \in S$ the set $S - s$ is a submonoid of $M$. An element $s$ of a slice $S$ is called *stable* if the submonoid $S - s$ is subtractive.

Proposition 7.2. *Every slice $S$ in $N^k$ has a stable element.*

*Proof.* For every $s \in S$, consider the ideal

$$I_s = [(S - s) \backslash \{0\}] + N^k.$$

Let $s \leqslant s'$, $s' \in S$, and let $y \in S - s$. Then $s' = s + x$ and $s + y \in S$. Thus $s' + y = s + x + y \in S$ or equivalently $y \in S - s'$. Thus $S - s \subset S - s'$ so that $I_s \subset I_s'$.

Since the ideals in $N^k$ satisfy the ascending chain condition (Proposition 5.2), there exists $s \in S$ such that $I_s' = I_s$ for every $s' \in S$, $s \leqslant s'$. We shall show that such an $s$ is stable.

Indeed, let $x, x + y \in S - s$. If $y = 0$ then $y \in S - s$ and we are finished. Thus, we may assume $y \neq 0$. We have $s + x \in S$ and $s + x + y \in S$ so that $y \in S - (s + x)$. Since $y \neq 0$ we have $y \in I_{s+x} = I_s$. Consequently, $y = u + w$ with $u \in S - s$, $w \in N^k$, $u \neq 0$. Further, we may choose such a decomposition of $y$ with a shortest possible $w$. If $w = 0$ then $y \in S - s$ and we are finished. Thus, we may assume $w \neq 0$. Since $y + s \in S$, we have $u + w + s \in S$; i.e., $w \in S - (s + u)$. Since $w \neq 0$ and $s + u \in S$ we have $w \in I_{s+u} = I_s$. Thus $w = u' + w'$ with $u' \in S - s$, $u' \neq 0$. Then

$$y = u + u' + w' \qquad \text{with} \qquad u + u' \in S - s.$$

Thus contradicts the assumption that $w$ was the shortest possible.

PROPOSITION 7.3. *A slice $S$ in a finitely generated monoid $M$ is a rational subset of $M$.*

*Proof.* Let $\varphi : N^k \to M$ be a surjective morphism. Then $\varphi^{-1}S$ is a slice in $N^k$, and it suffices to prove the rationality of $\varphi^{-1}S$. Thus we may assume $M = N^k$. By Proposition 7.2, $S$ contains a stable element $y$. We decompose $S$ according to the element $y$. The upper part is

$$y + (S - y). \tag{7.1}$$

Since $S - y$ is a subtractive submonoid of $N^k$, it is finitely generated by Proposition 7.1. Thus $S - y$ is rational and so is (7.1). The components of the lower part are

$$y_{is} + (S - y_{is}) \cap N_i^k. \tag{7.2}$$

Each of the sets $S - y_{is}$ is a slice. Indeed, if $s, s + x, s + z \in S - y_{is}$, then $s + y_{is}, s + y_{is} + x, s + y_{is} + z \in S$. Then $s + y_{is} + x + z \in S$ so that $s + x + z \in S - y_{is}$. Consequently $(S - y_{is}) \cap N_i^k$ also is a slice. This slice being in $N^{k-1}$ we may assume by induction that it is rational. Thus (7.2) is rational, and therefore $S$ is rational.

## 8. PROOF OF THEOREM II

The theorem follows directly from Proposition 7.3 in view of

PROPOSITION 8.1. *A congruence $Q$ in a commutative monoid $M$ is a slice in $M \times M$.*

*Proof.* Let $(x_1, x_2), (x_1 + y_1, x_2 + y_2), (x_1 + z_1, x_2 + z_2) \in Q$. Then

$$x_1 + y_1 + z_1 \sim x_2 + y_2 + z_1 \sim x_1 + y_2 + z_1 \sim x_2 + y_2 + z_2 .$$

Thus $(x_1 + y_1 + z_1, x_2 + y_2 + z_2) \in Q$.

## 9. Preparation for Theorems III and IV

Proposition 9.1 (Ginsburg–Spanier). *If $X = a + B^*$ is a linear subset of $Z^k$, then $X$ is the finite union of simple sets $c + D^*$ with $D \subset B$.*

*Proof.* Without loss of generality, we may assume $a = 0$. Let $B = \{b_1, ..., b_p\}$. If the elements of $B$ are linearly independent, then $X$ is simple and there is nothing to prove. Thus we may assume that

$$t_1 b_1 + \cdots + t_q b_q = t_{q+1} b_{q+1} + \cdots + t_p b_p$$

for some

$$0 < q < p, \quad (t_1, ..., t_p) \in N^p, \quad t_1 > 0.$$

For $j = 1, ..., q$ define

$$A_j = \{s b_j \mid 0 < s < t_j\}, \qquad B_j = B \backslash \{b_j\}$$
$$Y_j = A_j + B_j^*, \qquad Y = \bigcup Y_j$$

Arguing by induction on $p$, it suffices to show that $X = Y$. Clearly $A_j \subset X$ and $B_j \subset X$. Since $X$ is a submonoid of $Z^k$, it follows that $Y_j \subset X$ and thus $Y \subset X$.

Let $d \in X$, $d = \sum r_i b_i$, $r_i \geqslant 0$. If $t_j \leqslant r_j$ for all $j = 1, ..., q$ then we may rewrite $d$ as

$$d = \sum_{j \leqslant q} (r_j - t_j) b_j + \sum_{q < l} (r_l + t_l) b_l$$

and thereby diminish the sum $\sum_{j \leqslant q} r_j$. Thus we may assume that $r_j < t_j$ for some $j \leqslant q$. Then $d = r_j b_j + d'$ for some $d' \in B_j^*$. Thus $d \in Y_j$.

Lemma 9.2. *Let $M_i$, $i = 1, ..., p$, be commutative monoids and let $M = M_1 \times \cdots \times M_p$. Let $X_i \subset M_i$ be semi-simple subsets of $M_i$ such that $Y_i = M_i \backslash X_i$ also are semi-simple. Then $X = X_1 \times \cdots \times X_p$ is a semi-simple subset of $M$ and $M \backslash X$ also is semi-simple.*

*Proof.* By induction, it suffices to consider the case $p = 2$. We regard $M_1$ and $M_2$ as submonoids of $M$ in the obvious way. Then for

$$a_1 + B_1^* \subset M_1, \qquad a_2 + B_2^* \subset M_2$$

we have

$$(a_1 + B_1^*) \times (a_2 + B_2^*) = (a_1 + a_2) + (B_1 \cup B_2)^*.$$

This shows that $X = X_1 \times X_2$ is semi-simple. Further $M\backslash X$ is the disjoint union

$$Y_1 \times Y_2 \cup X_1 \times Y_2 \cup Y_1 \times X_2$$

so that $M\backslash X$ also is semi-simple.

Since $N = 1^*$ and $Z\backslash N = (-1) + (-1)^*$ we see that $N$ and $Z\backslash N$ are simple subsets of $Z$. Also $N\backslash\{0\} = 1 + N$ is simple. Thus Lemma 9.2 yields the semi-simplicity of the following subsets of $Z^k$:

$$Z^k, \quad Z^k\backslash N^k, \quad N^p \times N^q\backslash N^p \times 0 \qquad \text{for} \quad p + q = k. \tag{6.1}$$

LEMMA 9.3. *If $X$ is a simple subset of $Z^k$, then $Z^k\backslash X$ is semi-simple.*

*Proof.* Let $X = a + B^*$ with $B$ a linearly independent subset of $Z^k$. Since $Z^k\backslash X = a + (Z^k\backslash B^*)$ it suffices to consider the case $a = 0$, $X = B^*$.

Let $B = \{b_1, \ldots, b_p\}$. First consider the case $p = k$. Let $B^\circ$ be the subgroup of $Z^k$. generated by $B$. Then

$$Z^k\backslash B^* = (Z^k\backslash B^\circ) \cup (B^\circ\backslash B^*).$$

Since the union is disjoint, it suffices to show that each component is semi-simple. Since $b_1, \ldots, b_k$ are linearly independent, $B^\circ$ is isomorphic with $Z^k$ under an isomorphism mapping $B^*$ onto $N^k$. Since by (6.1), $Z^k\backslash N^k$ is semi-simple, it follows that $B^\circ\backslash B^*$ is semi-simple.

Next consider $Z^k\backslash B^\circ$. Since $p = k$, the quotient group $Z^k\backslash B^\circ$ is finite. Therefore $Z^k\backslash B^\circ$ is a disjoint finite union of cosets $c + B^\circ$. Thus it suffices to show that $c + B^\circ$ is semi-simple. For this it is enough to show that $B^\circ$ is semi-simple. However, $B^\circ \approx Z^k$, so the conclusion follows from (6.1).

Next assume $k = p + q$, $q > 0$. We can then find elements $b_{p+1}, \ldots, b_k$ so that the set $C = \{b_1, \ldots, b_k\}$ is linearly independent. Then

$$Z^k\backslash B^* = (Z^k\backslash C^*) \cup (C^*\backslash B^*).$$

By the above, $Z^k\backslash C^*$ is semi-simple. The monoid $C^*$ is isomorphic with $N^k = N^p \times N^q$ under an isomorphism carrying $B^*$ onto $N^p \times 0$. Thus by (6.1), $C^*\backslash B^*$ is semi-simple.

LEMMA 9.4. *Given a morphism $\varphi : N^k \to Z^m$ and an element $c \in Z^m$ the set*

$$X = \{x \mid x \in N^k, \varphi x = c\}$$

*is semi-simple.*

*Proof.* If $X$ is finite, then it clearly is semi-simple. If $X$ is infinite, then by Proposition 4.1, there exists elements $x, x' \in X$ with $x < x'$. Thus $x + y = x'$ for some $y \in N^k, y \neq 0$. Thus we have $y \neq 0$, $\varphi y = 0$. For any $x \in X$ we have a unique representation

$$x = ny + z, \quad n \in N, \quad z \in X, \quad y \text{ non} \leqslant z.$$

We thus have the unambiguous sum $X = y^* + X_y$ so it suffices to prove that $X_y$ is semi-simple. The (disjoint) components of the lower part of $X$ are

$$y_{is} + (X - y_{is}) \cap N_i^k.$$

Since

$$(X - y_{is}) \cap N_i^k = \{x \mid x \in N_i^k, \varphi x = c + \varphi y_{is}\}$$

these sets are semi-simple by recursion. Thus $X_y$ is semi-simple as required.

LEMMA 9.5. *If $X$ and $Y$ are semi-simple subsets of $Z^k$ then so is $X \cap Y$.*

*Proof.* We may assume that $X$ and $Y$ are simple subsets of $Z^k$. Then

$$X = a + \alpha N^p, \qquad Y = b + \beta N^q$$

where $\alpha : N^p \to Z^k, \beta : N^q \to Z^k$ are injective morphisms. Define the morphisms

$$\varphi : N^p \times N^q \to Z^k \qquad \varphi(x, y) = \alpha x - \beta y$$
$$\tau : N^p \times N^q \to Z^k \qquad \tau(x, y) = \alpha x$$

and let

$$W = \{(x, y) | (x, y) \in N^p \times N^q, \varphi(x, y) = b - a\}$$
$$= \{(x, y) | (x, y) \in N^p \times N^q, a + \alpha x = b + \beta y\}.$$

By Lemma 9.4, $W$ is semi-simple. Further, $a + \tau W = X \cap Y$. Since $\alpha$ and $\beta$ are injective, it follows that $\tau$ is injective on the set $W$. Therefore $a + \tau W$ is semi-simple.

## 10. PROOF OF THEOREMS III AND IV

We first consider the case $M = Z^k$. Let then $X$ be a rational subset of $Z^k$. Then $X$ is semi-linear and by Proposition 9.1, $X$ is a finite union

$X_1 \cup \cdots \cup X_p$ of (not necessarily disjoint) simple sets. By Lemma 9.3 each of the sets $Z^k \backslash X_i$ is semi-simple. Therefore, by Lemma 9.5 the set

$$X' = Z^k \backslash X = \bigcap (Z^k \backslash X_i)$$

is semi-simple. Since $X'$ also is rational, by the above $X = Z^k \backslash X'$ is semi-simple. If $Y$ is another rational subset of $Z^k$ then $Y$ is semi-simple and by Lemma 9.5 the sets

$$Y \cap X, \quad Y \backslash X = Y \cap X'$$

are semi-simple.

The next case to consider is $M = N^k$. This follows from the case $M = Z^k$ in virtue of the following observation: If $a + B^* \subset N^k$ for $a \in Z^k$, $B \subset Z^k$, then $a \in N^k$ and $B \subset N^k$. Clearly $a \in N^k$. Let $b \in B$. Then $a + nb \in N^k$ for all positive integers $n$. This implies that all the coordinates of $b$ are non-negative and thus $b \in N^k$.

Next, consider an arbitrary commutative monoid $M$ and let $X$ and $Y$ be rational subsets of $M$. There exists then a finitely generated submonoid $M'$ of $M$ such that $X, Y \subset M'$. Hence we may assume that $M$ is finitely generated.

Let $\varphi : N^k \to M$ be a surjective morphism and let $Q$ be the congruence in $N^k$ defined by

$$x \sim y \Leftrightarrow \varphi x = \varphi y.$$

Given any rational subset $X$ of $M$, choose a rational set $R$ in $N^k$ such that $\varphi R = X$. Then note that

$$\varphi^{-1} X = \pi[Q \cap (N^k \times R)]$$

where $\pi : N^k \times N^k \to N^k$ is given by $\pi(x, y) = x$. Since by Theorem II, $Q$ is a rational subset of $N^k \times N^k$, it follows that $\varphi^{-1} X$ is rational. If $Y$ is another rational subset of $M$, then $\varphi^{-1} Y$ is rational. Since $\varphi$ is surjective, we have

$$X \cap Y = \varphi[\varphi^{-1} X \cap \varphi^{-1} Y], \qquad Y \backslash X = \varphi[\varphi^{-1} Y \backslash \varphi^{-1} X]$$

so that $X \cap Y$ and $Y \backslash X$ are rational. This concludes the proof of Theorem III in full generality. We note that Theorem I has not been employed.

To complete the proof of Theorem IV we need one more step. Conserving the notation above, we apply Theorem I to obtain a rational cross-section $A$ for $Q$. Then for any set $X \subset M$ we have $X = \varphi W$ where $W = A \cap \varphi^{-1} X$. If $X$ is rational then so is $\varphi^{-1} X$. Then $W$ is a rational subset of $N^k$ and therefore $W$ is semi-simple. Since $W \subset A$, $\varphi$ is injective on $W$ and thus $\varphi W$ also is semi-simple.

## 11. Corollaries of Theorem III

Corollary III.1. *In a finitely generated monoid $M$ the class of rational sets is closed under Boolean operations.*

Indeed, $M$ is then a rational set and therefore $M\backslash X$ is rational for every rational set $X$.

Corollary III.2. *If $\varphi : M' \to M$ is a morphism of commutative monoids, $M'$ is finitely generated and $X$ is a rational subset of $M$, then $\varphi^{-1}X$ is a rational subset of $M'$.*

Indeed, consider the morphisms

$$\mu : M' \to M' \times M, \qquad \mu x = (x, \varphi x),$$
$$\gamma : M' \times M \to M', \qquad \pi(x, y) = x.$$

Then $\varphi^{-1}X = \pi Y$ where $Y = \mu M' \cap (M' \times X)$. Since $M'$ is a rational subset of itself, $\mu M'$ and $M' \times X$ are rational subsets of $M' \times M$. Thus, $Y$ is rational and so is $\pi Y$.

Corollary III.3. *If $M'$ is a finitely generated submonoid of a commutative monoid $M$ and if $X \subset M'$ is a rational subset of $M$, then $X$ is also a rational subset of $M'$.*

In the previous Corollary, choose $\varphi : M' \to M$ to be the inclusion morphism.

Given subset $X$, $Y$ of a commutative monoid $M$, we define

$$Y - X = \{m \mid x + m \in Y \text{ for some } x \in X\}.$$

Corollary III.4. *If $X$ and $Y$ are rational subsets of a finitely generated commutative monoid $M$, then $Y - X$ is rational.*

Indeed, consider the morphisms

$$\varphi : M \times M \to M, \qquad \varphi(x, y) = x + y,$$
$$\pi : M \times M \to M, \qquad \pi(x, y) = y.$$

Then

$$Y - X = \pi[(\varphi^{-1}Y) \cap (X \times M)],$$

which shows that $Y - X$ is rational.

It should be noted that Theorem II is itself a corollary of Corollary III.2. Indeed, if $Q$ is a congruence in $M$, consider the natural morphism $\varphi : M \to R = M/Q$, and define $\psi : M \times M \to R \times R$ by $\psi(m_1, m_2) = (\varphi m_1, \varphi m_2)$. Then $Q = \psi^{-1}\Delta$ where $\Delta$ is the diagonal submonoid of $R \times R$.

Since $M$ is finitely generated, so is $R$ and thus also $\Delta$. Therefore, $\Delta$ is rational and by Corollary III.2 so is $\psi^{-1}\Delta = Q$.

## 12. Ascending Chain Conditions

Proposition 12.1. *A rational slice $S$ in a commutative monoid $M$ is finitely defined*; i.e., *there exists a finite subset $F$ of $M$ such that $S$ is the least slice in $M$ containing $F$.*

*Proof.* Since $S$ is rational, it is the finite union of sets

$$a_i + B_i^*,\ a_i \in M,\ B_i \subset M,\ B_i \text{ finite.}$$

Let

$$F = \bigcup \{a_i\} \cup (a_i + B_i).$$

Then $F \subset S$. Let $S'$ be any slice in $M$ containing $F$. For each index $i$ we then have $a_i \in S'$ and $a_i + B_i \subset S'$. Thus $B_i \subset S - a_i$ and since $S - a_i$ is a submonoid, we have $B_i^* \subset S' - a_i$; i.e., $a_i + B_i^* \subset S'$. Consequently, $S \subset S'$.

This, combined with Proposition 7.3, yields

Corollary 12.2. *In a finitely generated commutative monoid every slice is finitely defined.*

An equivalent statement is

Corollary 12.3. *The slices in a finitely generated commutative monoid satisfy the ascending chain condition.*

In particular, for congruences, we obtain, by Proposition 8.1,

Theorem V. *Every congruence $Q$ in a finitely generated commutative monoid $M$ is finitely defined*; i.e., *there exists a finite subset $F$ of $M \times M$ such that $Q$ is the least congruence containing $F$.*

Corollary V.1. *The congruences in a finitely generated commutative monoid $M$ satisfy the ascending chain condition.*

Given a congruence $Q$ in a commutative monoid $M$ and given $m \in M$, define the congruence $Q_m$ in $M$ by setting

$$Q_m = \{(x, y) | (x + m, y + m) \in Q\}.$$

Clearly

$$Q \subset Q_m \subset Q_{m+m'} = (Q_m)_{m'}.$$

$Q$ is called *cancellative* if $Q = Q_m$ for all $m \in M$.

COROLLARY V.2. *Let $Q$ be a congruence in a finitely generated commutative monoid $M$. The class of congruences $\{Q_m\}$, $m \in M$, contains exactly one cancellative congruence $Q'$. Further, $Q_m \subset Q'$ for every $m \in M$.*

The existence of $Q'$ follows from the ascending chain condition. Since $Q \subset Q'$, we have $Q_m \subset Q_{m'} = Q'$. This implies the uniqueness of $Q'$.

Theorem V and its corollaries were proved by L. Redei [3].

Theorem V may also be deduced from the Hilbert basis theorem as follows. Let $R$ be any commutative ring (with $0 \neq 1$). Writing the monoid $M$ multiplicatively, construct the $R$-algebra $R[M]$. Given a congruence $Q$ in $M$, let $I(Q)$ denote the ideal in $R[M]$ generated by elements $x - y$ with $(x, y) \in Q$. We assert that

$$Q = \{(x, y) | \, x, y \in M, x - y \in I(Q)\}. \tag{12.1}$$

Indeed, let $Q'$ be the right-hand side of (12.1). Then $Q'$ is a congruence in $M$, $Q \subset Q'$ and $I(Q') = I(Q)$. There results a commutative triangle of surjective morphisms

$$\begin{array}{ccc} & M & \\ {\scriptstyle \pi}\swarrow & & \searrow{\scriptstyle \pi'} \\ M/Q & \xrightarrow[\varphi]{} & M/Q' \end{array}$$

from which we obtain the commutative triangle of surjective $R$-algebra morphisms

$$\begin{array}{ccc} & R[M] & \\ {\scriptstyle R[\pi]}\swarrow & & \searrow{\scriptstyle R[\pi']} \\ R[M/Q] & \xrightarrow[R[\varphi]]{} & R[M/Q'] \end{array}$$

Since $I(Q) = I(Q')$ is both the kernel of $R[\pi]$ and $R[\pi']$, it follows that $R[\varphi]$ is an isomorphism. It follows that $\varphi$ also is an isomorphism and thus $Q = Q'$.

It follows from (12.1) that the set of all congruences in $M$ is mapped by $Q \to IQ$ injectively into the set of ideals in $R[M]$. If $M$ is finitely generated and $R$ is noetherian and $R[M]$ also is noetherian and the ideals in $R[M]$

satisfy the ascending chain condition. Thus the congruences in $M$ also satisfy the ascending chain condition.

The above proof was known to a number of mathematicians including Peter Freyd and Michael O. Rabin.

## 13. Other Applications

Call a commutative monoid $M$ *cancellative* if $x + y = x + z$ implies $y = z$.

THEOREM VI. *The intersection $M_1 \cap M_2$ of two finitely generated submonoids $M_1$, $M_2$ of a cancellative commutative monoid $M$ is a finitely generated submonoid of $M$.*

*Proof.* Choose morphisms

$$\varphi_i : N^{k_i} \to M \qquad i = 1, 2$$

such that $\varphi_i N^{k_i} = M_i$ for $i = 1, 2$. Consider the product $N^k = N^{k_1} \times N^{k_2}$, $k = k_1 + k_2$ and define

$$\psi_i : N^k \to M \qquad i = 1, 2$$

by

$$\psi_i(x_1, x_2) = \varphi_i x_i .$$

Define

$$S = \{x \mid x \in N^k, \psi_1 x = \psi_2 x\}.$$

Note that $M_1 \cap M_2 = \psi_1 S = \psi_2 S$. Thus it suffices to show that $S$ is finitely generated. By Proposition 7.1 it, therefore, suffices to show that $S$ is a subtractive submonoid of $N^k$. Let then $x, x + y \in S$. Then

$$\varphi_1 x_1 = \varphi_2 x_2 , \varphi_1 x_1 + \varphi_1 y_1 = \varphi_2 x_2 + \varphi_2 y_2 .$$

Since $M$ is cancellative, it follows that $\varphi_1 y_1 = \varphi_2 y_2$ ; i.e., $y \in S$.

The conclusion of Theorem VI is false without the assumption that $M$ is cancellative. Indeed, consider the "simplest" example of a noncancellative monoid $M$ given by three generators $x, y, z$ and the single relation $x + y = x + z$.

We may regard $M$ as the quotient monoid of $N^3$ by the relation $Q$ defined by the single pair (1, 1, 0), (1, 0, 1). The congruence $Q$ may be made explicit as follows:

$$(a, b, c) \sim (a', b', c')$$

if and only if either

$$a = a', \qquad b + c = b' + c'$$

or

$$a = a' = 0, \quad b = b', c = c'.$$

This implies that $x, y, z$ are pairwise linearly independent.

Let $V = \{x, y\}^* \cap \{x, z\}^*$. Viewed as a submonoid of $\{x, y\}^*$, $V$ may be identified with the submonoid of $N^2$ given as follows:

$$V = \{(a, b) | (a, b, 0) \sim (a', 0, c')\}.$$

Inspecting the congruence we see that we must have $a = a'$, $b = c'$. Thus

$$V = \{(a, b) | (a, b, 0) \sim (a, 0, b)\}.$$

Again, going back to the congruence, we see that

$$V = \{(a, b) |\ a = b = 0 \qquad \text{or} \qquad a > 0\}.$$

This submonoid of $N^2$ is not finitely generated since any generating set must contain the sequence $\{(1, n)\}$.

THEOREM VII. *Let $M$ be a finitely generated commutative monoid, $X$ a rational subset of $M$, and $P$ a set of strictly positive integers. Then the set*

$$P^{-1}X = \{m \in M \mid pm \in X \text{ for some } p \in P\}$$

*is rational*

*Proof.* Let $\varphi : N^k \to M$ be a surjective morphism. Then $\varphi^{-1}(P^{-1}X) = P^{-1}(\varphi^{-1}X)$. Thus by Corollary IV.2, it suffices to consider the case $M = N^k$.

Since $P^{-1}(X \cup Y) = P^{-1}X \cup P^{-1}Y$, it suffices to consider the case when $X = a + B^*$ is simple with $B = \{b_1, ..., b_k\}$ linearly independent. Let

$$C = \{y \mid py = a + \sum n_i b_i, \quad \text{for some} \quad p \in P \quad \text{and} \quad 0 \leqslant n_i < p\}.$$

For $y \in C$ we have $y \leqslant a + \sum b_i$ and therefore the set $C$ is finite.

Since $C \subset P^{-1}X$ and $pB^* \subset B^*$ for every $p$, it follows that $C + B^* \subset P^{-1}X$. Conversely, let $y \in P^{-1}X$. Then for some $p \in P$ we have $py = a + \sum q_i b_i$, $0 \leqslant q_i$. Write $q_i = n_i + r_i p$ with $0 \leqslant n_i < p$. Then

$$py = a + \sum n_i b_i + p\,(\sum r_i b_i).$$

Thus setting $b = \sum r_i b_i$, $c = y - b$ we have $c \in C, b \in B^*$, $y = c + b$. Thus $P^{-1}X = C + B^*$ and $P^{-1}X$ is rational.

The conclusion of Theorem VII is false without the assumption of finite generation. Indeed, let $M$ be an infinite set with distinguished elements 0, $w$, $0 \neq w$. Define $0 + x = x = x + 0$ and $x + y = w$ if $x \neq 0 \neq y$. Then $M$ is a commutative monoid and $X = \{w, 0\}$ is a rational subset of $M$. Taking $P = \{2\}$ we have $P^{-1}X = M$ which is not rational.

## 14. Some Counterexamples

We first show that the hypothesis of finite generation is essential in all the theorems and corollaries in which it is made.

In connection with Theorems I and II, consider a monoid $M$. Then the only cross-section for the congruence $Q = \{(x, x)\}$ is $M$. Thus $Q$ does not have a rational cross-section. On the other hand, the congruence $Q = M \times M$ is not rational.

If $M$ is a commutative monoid which is not finitely generated, then $\varnothing$ is rational subset of $M$ while $M = M \setminus \varnothing$ is not. This shows that Corollary III.1 fails.

In $N^2$ consider the submonoid

$$Q = \{(0, 0)\} \cup [(1, 1) + N^2].$$

Clearly $Q$ is a rational subset of $N^2$. However, $Q$ is not finitely generated, as indeed any generating set for $Q$ must contain all the elements $(n, 1)$ and $(1, n)$ for $n = 1, 2, \ldots$. Therefore $Q$ is not a rational subset of itself. Therefore, Corollaries III.3 and III.2 fail. Incidentally, $Q$ is a congruence in $N$ and is defined by the single pair (1, 2). This shows that for a congruence $Q$, "finitely generated" is a much stronger notion than "finitely defined."

For Corollary III.4, consider a commutative monoid $M$ which is not finitely generated and which contains an element $w$ such that $M + w = w$. Then taking $X = Y = \{w\}$ we have $Y \setminus X = M$. Thus $X$ and $Y$ are rational while $Y \setminus X$ is not.

For Theorem V and its corollaries, consider the free commutative monoid $M$ generated by the letters $x_i, y_i, z_i$, $i = 1, 2, \ldots$, and consider the congruence $Q$ defined by the set of pairs $(x_i + z_i, y_i + z_i)$, $i = 1, 2, \ldots$. Then for any $m \in M$ the congruence $Q_m$ is not cancellative. Therefore, Corollary V.2 fails in $M$, and therefore, also, Corollary V.1 and Theorem V.

To conclude, we give an example of a submonoid $M$ of $N^2$ which is not rational. Let

$$M = \{(x, y) \mid y \leqslant x^2\}.$$

Consider the "slope" function defined on $M$ by setting

$$\varphi(0, 0) = 0$$

$$\varphi(x, y) = \frac{y}{x} \quad \text{if} \quad x \neq 0.$$

Then $\varphi$ is unbounded on $M$. However, on every set $a + B^*$ with $a \in N^2$, $B \subset N^2$, $B$ finite and $a + B^* \subset M$ the function $\varphi$ is bounded. Thus $\varphi$ is bounded on any rational subset of $N^2$ which is in $M$. Consequently, $M$ is not rational.

In the same way, we can show that for every irrational number $r > 0$ the submonoid

$$M = \{(x, y) \in N^2, y \leqslant rx\}$$

is not rational.

## References


1. Thue, Axel. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, *Videnskapsselskapets Skrifter I Mat. Naturv. Klasse* **1912**, 1–67.
2. Ginsburg and Spanier. Bounded ALGOL-like languages. *Trans. Am. Math. Soc.* **113** (1964), 333–368.
3. Redei, L. "The Theory of Finitely Generated Commutative Semi-Groups," Theorems 72, 95 and 60. Oxford–Edinburgh–New York, 1965.


PRINTED IN BRUGES, BELGIUM, BY THE ST. CATHERINE PRESS, LTD.