FINITELY GENERATED COMMUTATIVE MONOIDS

J.C. Rosales
and
P.A. García-Sánchez

Nova Science Publishers, Inc.

FINITELY GENERATED COMMUTATIVE MONOIDS

UNIVERSITAT DE BARCELONA

Biblioteca de Matemàtiques

Gran Via de les Corts Catalanes, 585 -
08007 Barcelona

FINITELY GENERATED COMMUTATIVE MONOIDS

J. C. ROSALES AND P. A. GARCÍA-SÁNCHEZ

Universitat de Barcelona

Gran Via de les Corts Catalanes, 585
08007 Barcelona

Nova Science Publishers, Inc.
Commack, New York

30 KUS

Editorial Production: Susan Boriotti
Office Manager: Annette Hellinger
Graphics: Frank Grucci and John T'Lustachowski
Information Editor: Tatiana Shohov
Book Production: Donna Dennis, Patrick Davin, Christine Mathosian and Tammy Sauter
Circulation: Maryanne Schmidt
Marketing/Sales: Cathy DeGregory

Library of Congress Cataloging-in-Publication Data
available upon request

ISBN 1-56072-670-9

Algebra [illegible] [illegible]
Semigroups Monoids

Copyright © 1999 by Nova Science Publishers, Inc.
6080 Jericho Turnpike, Suite 207
Commack, New York 11725
Tele. 516-499-3103 Fax 516-499-3146
e-mail: Novascience@earthlink.net
e-mail: Novascil@aol.com
Web Site: http://www.nexusworld.com/nova

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means: electronic, electrostatic, magnetic, tape, mechanical photocopying, recording or otherwise without permission from the publishers.

The authors and publisher have taken care in preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained in this book.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered herein. It is sold with the clear understanding that the publisher is not engaged in rendering legal or any other professional services. If legal or any other expert assistance is required, the services of a competent person should be sought. FROM A DECLARATION OF PARTICIPANTS JOINTLY ADOPTED BY A COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND A COMMITTEE OF PUBLISHERS.

Printed in the United States of America

Contents

Preface ix

Acknowledgements xiii

Chapter 1. Basic definitions and results 1
Remarks 6
Exercises 6

Chapter 2. Finitely generated commutative groups 9
1. Bases and rank of a subgroup of $\mathbb{Z}^n$ 9
2. Equivalence of matrices with integer entries and invariant factors 12
3. Some practical results concerning the computation of a basis 20
Remarks 23
Exercises 23

Chapter 3. Finitely generated cancellative monoids 25
1. Finitely generated cancellative torsion free monoids 27
2. Finitely generated cancellative reduced monoids 28
3. Finite cancellative monoids 32
Remarks 33
Exercises 33

Chapter 4. Minkowski-Farkas' lemma and its applications to monoids 35
1. Main result and algorithms 35
2. Applications to monoids 41
Remarks 45
Exercises 45

Chapter 5. Finitely generated monoids are finitely presented 47
1. Linear admissible orders 47
2. Rédei's theorem 50
3. The word problem for monoids 52
4. Cyclic monoids 53
Remarks 54
Exercises 54

Chapter 6. The word problem for monoids 57

1. Reduced systems of generators of a congruence 57
2. Canonical systems of generators of a congruence 59
3. The group of units of a monoid 65
Remarks 69
Exercises 70

Chapter 7. Nonnegative integer solutions of systems of linear equations 73
1. Nonnegative integer solutions of a system of linear homogeneous Diophantine equations 73
2. The monoid of nonnegative elements of a subgroup of $\mathbb{Z}^n$ 77
3. Nonnegative integer solutions of systems of linear Diophantine equations 80
4. Normal affine semigroups 81
Remarks 83
Exercises 84

Chapter 8. Computing presentations of finitely generated cancellative monoids 85
1. Primitive elements of a congruence 85
2. Computing presentations of finitely generated cancellative monoids 87
3. Deciding whether a monoid is cancellative 90
Remarks 91
Exercises 91

Chapter 9. Minimal presentations of finitely generated cancellative reduced monoids 93
1. Characterization of minimal presentations of finitely generated cancellative reduced monoids 93
2. The affine case 96
Remarks 102
Exercises 103

Chapter 10. Numerical semigroups 105
1. Minimal presentations of numerical semigroups 108
2. A bound for the cardinality of minimal presentations of numerical semigroups 110
3. Numerical semigroups with maximal embedding dimension 113
Remarks 116
Exercises 117

Chapter 11. Projections of congruences 119
1. Presentations of finitely generated cancellative monoids as projections of affine semigroups 119
2. Lifting some projections 123
Remarks 127
Exercises 127

Chapter 12. Finite torsion free monoids 129
1. Presentations of finite torsion free monoids 129
2. Finite lattices 130
3. Finite Boolean algebras 133
4. Boolean monoids 137
Remarks 139
Exercises 140

Chapter 13. Archimedean Components 143
1. Computing the Archimedean components of a finitely generated monoid 145
Remarks 150
Exercises 150

Chapter 14. Separative monoids 153
1. Separative monoids and their Archimedean components 153
2. Deciding whether the quotient of an ideal of $\mathbb{N}^n$ by a congruence is cancellative 155
3. Elimination 158
4. Deciding whether a finitely generated monoid is separative 158
5. Deciding whether a finitely generated monoid is torsion free 160
6. $\mathcal{N}$-semigroups 162
Remarks 167
Exercises 167

Appendix A. Graphs 169

Bibliography 171

Index of notation 175

Index of main results and algorithms 177

Index 183

Preface

There is a large amount of bibliography related to Semigroup Theory. Apart from Redei's book [**39**], almost all the existing publications in this field are devoted to the study of semigroups not necessarily commutative. Some of them have several chapters involving commutative semigroups, but the theory developed there is too general and few of them focus their attention on finitely generated commutative semigroups. Thus when one tries to study this kind of semigroups one has to "swallow" many concepts that are not suitable and that, in many cases, turn out to be trivial for finitely generated commutative monoids. In addition, there is a lack of effective methods for studying properties of finitely generated commutative monoids. These were in fact the chief reasons for developing a self-contained book on finitely generated commutative monoids with the theory and algorithms needed for the study of the main classical problems related to this kind of monoid.

All semigroups and monoids considered here are commutative. Hence we shall omit the adjective commutative.

This book is not only addressed to people working in Semigroup Theory. The only knowledge required to follow and understand its contents is basic Linear Algebra. Thus any student of second year of Mathematics or Computer Science might find the book easy to understand. This monograph can also be used as a textbook of a course on finitely generated monoids.

Our goals can be classified as:

- compute presentations for finitely generated cancellative monoids,
- from a presentation of a monoid decide whether this monoid is cancellative, reduced, separative, finite, torsion free, group, affine, full, normal, etc.

This material is not only interesting from the semigroup point of view; it has many applications to other fields in Algebra, as the theory stems from problems in these fields of research. Some of the connections with other parts of Mathematics are the following.

1. *Algebraic Geometry*: There is a bijective correspondence between affine semigroups and affine varieties parametrized by monomials. One of the first authors dealing with this equivalence was Herzog who proved in [**24**] that giving a presentation of an affine semigroup is equivalent to giving a system of generators of the ideal associated to the corresponding affine variety. These ideals are generated by binomials and are generally known as binomial ideals. An extensive study of this kind of ideal can be found in [**14**].

2. *Commutative algebra*: As a generalization of the ring of coordinates of affine varieties parametrized by monomials, arises the definition of semigroup ring. Semigroup rings are a large store of examples in Commutative Algebra. Gilmer studies in [**19**] semigroup rings and how their properties can be expressed in terms of those of the semigroup. After that, many authors have focused their attention on the characterization of algebraic properties of semigroup rings in terms of properties of the semigroup (see, as examples of the theory developed in this line, [**26**], [**64**] and [**65**]).
3. *Number theory*: The concepts of full and normal affine semigroup are tightly related to the concept of semigroups with divisor-theory. The relationship of this kind of semigroup and number theory first appeared in [**7**] and [**8**]. The equivalence between normal affine semigroups and affine semigroups with divisor-theory is derived from [**33**]. In addition, part of this work is devoted to the computation of nonnegative solutions of systems of diophantine equations and its applications to finitely generated monoids.
4. *Computational algebra*: The theory presented here is fully constructive. As we have mentioned before, the chief motivation for developing this monograph was to provide a set of algorithms that enables us to solve many problems related to finitely generated monoids. Some of the algorithms appearing in the book have been inspired by existing algorithms. This is the case of the algorithm for computing a canonical system of generators of a congruence, which is the translation of the critical pair completion (see [**28**]) to congruences.

The contents of the book are organized as follows. In Chapter 1 we introduce the concepts and basic results of the theory of monoids. We show that every finitely generated monoid is isomorphic to a quotient of $\mathbb{N}^n$ by a congruence. If, in addition, the given monoid is cancellative, then it is isomorphic to a submonoid of a finitely generated Abelian group.

Chapter 2 is devoted to the structure theorem of finitely generated Abelian groups. We also show how to compute a basis and the equations of a given subgroup of $\mathbb{Z}^n$, which is used repeatedly in the sequel.

In Chapter 3 we study finitely generated cancellative monoids and focus our attention on determining whether a given finitely generated monoid can be embedded in $\mathbb{N}^k$ or $\mathbb{Z}^k$. In this characterization the properties of being cancellative, torsion free and/or reduced play an important role. In order to achieve these results we use Minkowski-Farkas' lemma. The proof of this statement and some of its applications to monoids and resolution of systems of diophantine equations is given in Chapter 4.

Rédei's theorem ensures that every finitely generated monoid is finitely presented. This result is fundamental to the theory of finitely generated monoids and is proven in Chapter 5. Associated to Rédei's theorem, arises the word problem for finitely generated monoids. The solution to this problem is presented in Chapter 6.

At this stage we already know, up to isomorphisms, all finitely generated monoids and we have an algorithm to solve the word problem for them. The rest of the book

is focused on the computation of a presentation of a given finitely generated cancellative monoid and in determining properties of the monoid from a given presentation. The computation of nonnegative integer solutions of systems of diophantine equations plays an important role in the resolution of these two problems. The study of these systems of equations is performed in Chapter 7; full and normal affine semigroups come into scene.

In Chapter 8 we use the results obtained in Chapter 7 to give algorithms for computing a presentation of a finitely generated cancellative monoid and to decide from a presentation of a finitely generated monoid whether it is or is not cancellative.

In Chapter 9 we give a characterization of minimal presentations of finitely generated reduced cancellative monoids. As a particular example we analyze minimal presentations of affine semigroups and give an algorithm for computing them.

Numerical semigroups are a subclass of affine semigroups. Chapter 10 is devoted to them. We show how to particularize the algorithm for finding a minimal presentation of an affine semigroup to the numerical case. This particularization allows us to give bounds for the cardinality of minimal presentations of numerical semigroups as a function of the multiplicity and embedding dimension of the given semigroup. We show that this bound is sharp since it is reached by numerical semigroups with maximal embedding dimension.

In Chapter 11 we show that presentations of finitely generated cancellative monoids are projections of presentations of affine semigroups. The same idea used in the proof of this result is employed to give an alternative method for computing a presentation of a numerical semigroup.

The last three chapters are devoted to the study of torsion of a finitely generated monoid. In Chapter 12 we show that the concept of finite torsion free monoid coincides with that of finite lattice. The concept of Boolean algebra is also recalled and it is utilized to introduce the concept of Boolean monoid. Being asymptotic free of torsion is a weaker condition than being torsion free and it coincides with being separative. Separative monoids are precisely monoids all of whose Archimedean components are cancellative. Chapter 13 is devoted to the study and computation of Archimedean components from a presentation of a given monoid. These results are used in Chapter 14 in order to determine whether a finitely generated monoid is torsion free and/or separative. We terminate this chapter presenting the concept of $\mathcal{N}$-semigroups, which plays an important role in separative monoids since every finitely generated separative monoid is a finite lattice of groups and $\mathcal{N}$-semigroups.

Since we use some basic concepts of Graph Theory, at the end of the book we have appended a brief recall of the definitions and results used.

All the works appearing in the bibliography are cited at least once in the text, usually in the remarks sections. We have avoided using unproved results (with the consequent use of citations) so that the book is self contained. At the end of each chapter we have included a list of exercises that provide a quick recall of the chapter, emphasizing some concepts and the motivating subsequent chapters. Finally, we have included three indexes at the end of the book: the first one is on notation, so that the

reader can have a quick review of the symbolism used in the book; the second is a list of most relevant results and algorithms; and the third is a glossary of most important terms.

Acknowledgements

This book was written in the Department of Algebra at the University of Granada. During its development, the authors were partially funded by the project PB96-1424 of the DGES (Spain). We would like to acknowledge the help of Juan Ignacio García-García for proofreading and correcting some errors and missprints in the draft versions.

We would also like to thank our students Javier Bueno Tíscar and Antonio J. García Cruz for the development of the library `monoid.lib` for the software `SINGULAR` ([**20**]). With this library one can compute presentations of affine semigroups, decide whether a finitely generated monoid is reduced and/or cancellative. For finitely generated cancellative monoids the library can determine the group of units of the monoid and decide whether it is reduced, torsion free and/or affine. This library has been used for the examples and exercises.

We are indebted to Pablo Rogríguez Archilla for implementing some algorithms for finding the set of nonnegative integer solutions of linear systems of equations, for finding a system of generators of the semigroups of the form $M \cap \mathbb{N}^n$ with M a subgroup of $\mathbb{Z}^n$ and for deciding whether an affine semigroup is normal. While writing these lines, he is still implementing some other algorithms in C, as the ones corresponding to Chapter 8.

The algorithm for computing the cardinality of a minimal presentation for a numerical semigroup was implemented in PASCAL by Javier Fernández Baldomero in the eighties. We would like to express our gratitude to him for beginning this line of programs/libraries for finitely generated monoids.

The second author wishes to thank Professor Andrés García-Granados for softening his duties and "giving" him time for the development of the book.

Special thanks are due to Mario Petrich for his comments and suggestions.

UNIVERSITAT DE BARCELONA

CHAPTER 1

Basic definitions and results

Usually, the first concepts studied when one is initiated in groups, rings or vector spaces are the concepts of subgroup, subring, ideal, subspace, quotient and maps (morphisms) conserving the structure of these objects. Following this sequence of definitions, assumed to be known to most readers, we introduce the concepts of monoid, submonoid, quotient of a monoid and morphism of monoids. In order to define the quotient of a group, the concept of normal subgroup is needed, and for rings the definition of ideal is required. Congruences play this role for monoids; as a matter of fact, a normal subgroup and an ideal are a way of defining a congruence on a group and a ring, respectively. After defining all these concepts, we focus our attention on finitely generated monoids, and give a representation result which states that every finitely generated monoid is a quotient of $\mathbb{N}^n$. Next we proceed with results concerning the concepts studied in the following two chapters: finitely generated groups and cancellative monoids.

A **semigroup** is a pair $(S,+)$, with S a nonempty set and $+$ a binary operation defined on S verifying the **associative** law, that is to say, for any $a,b,c \in S$ we have that $(a+b)+c = a+(b+c)$. If, in addition, there exists an element, which is usually denoted by 0, in S such that $a+0 = 0+a = a$ for all $a \in S$, we say that $(S,+)$ is a **monoid**. As we mentioned in the Preface, in this book we deal only with commutative monoids and therefore for every pair $a,b \in S$ the element $a+b$ is equal to $b+a$. The element 0 is usually referred to as the **identity element** and if it exists, it is unique. In order to simplify notation, a given monoid $(S,+)$ will be denoted only by S. Hence, when we say that S is a monoid, we mean that in S there is a binary operation $+$ and that $(S,+)$ a commutative monoid.

A simple example of monoid is the set of nonnegative integers together with the addition.

A monoid S is **cancellative** if whenever the equality $a+c = b+c$ holds for some $a,b,c \in S$, then $a = b$.

A monoid S is a **group** if every element in S has an inverse, that is to say, for every $a \in S$ there exists $b \in S$ such that $a+b = 0$. If an element in a monoid has an inverse, it is unique. Due to this uniqueness, we use a special notation for the inverse of the element a, say $-a$. It is clear that a group is always a cancellative monoid. As an example of group we mention the group of integers under addition $(\mathbb{Z},+)$.

As usual, a **submonoid** of a monoid S is a set $H \subseteq S$ such that $0 \in H$ and for any $a,b \in H$ the element $a+b$ is again in H. Note that a submonoid of a monoid is itself

a monoid and that the intersection of a family of submonoids of a given monoid S is again a submonoid of S.

Given a subset A of a monoid S, the **monoid generated** by A, denoted by $\langle A\rangle$, is the least (with respect to inclusion) submonoid of S containing A. It is clear that this submonoid is the intersection of all submonoids of S containing A. Furthermore, if we define na recurrently as $0a = 0$ and $(n+1)a = na + a$, it is easy to prove that

$$\langle A\rangle = \left\{ \sum_{i=1}^{r} n_i a_i \mid r \in \mathbb{N}, n_i \in \mathbb{N}, a_i \in A, \text{ for all } 1 \leq i \leq r \right\}.$$

When $S = \langle A\rangle$, we say that S is **generated** by A or that A is a **system of generators** of S. Clearly, $S = \langle S\rangle$. We say that S is **minimally generated** by A if $\langle A\rangle = S$ and there exist no proper subset of A that generates S. In this setting, we will also say that A is a **minimal system of generators** of S. The monoid S is **finitely generated** if it has a finite system of generators.

As expected, a **subgroup** of a group S is a submonoid H of S verifying that the inverse of each of its elements lies in H. This is equivalent to saying that for every $a, b \in H$, we get that $a + (-b) = a - b$ is again in H. Note that a subgroup of a group is again a group with the same identity element and operation. As before, the intersection of subgroups is again a subgroup, which motivates the definition of the **group generated** by a subset of a group. If A is a subset of a group S, we denote by $\mathbf{G}(A)$ the subgroup of S generated by A and we say, as for monoids, that A is a **system of generators** of the group S. This is the least subgroup of S containing A, and coincides with the intersection of all subgroups of S containing A. If we denote, for every $n \in \mathbb{N}$ and $a \in A$, the element $n(-a)$ by $(-n)a$, then it is straightforward to show that

$$\mathbf{G}(A) = \left\{ \sum_{i=1}^{r} z_i a_i \mid r \in \mathbb{N}, z_i \in \mathbb{Z}, a_i \in A, \text{ for all } 1 \leq i \leq r \right\}.$$

If A is finite and $S = \mathbf{G}(A)$, we say that S is a **finitely generated group**.

If $S_1, \ldots, S_n$ is a sequence of monoids, in the Cartesian product $S_1 \times \cdots \times S_n$ of the sets $S_1, \ldots, S_n$ we can define the operation

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n).$$

Clearly, $(S_1 \times \cdots \times S_n, +)$ is a monoid, called the **direct product** of $S_1, \ldots, S_n$. It is easy to show that if all the monoids $S_1, \ldots, S_n$ are cancellative, then so is the monoid $S_1 \times \cdots \times S_n$. The same holds if the monoids S_i are all groups or if they are all finitely generated. As usual, if all the monoids S_i are the same and there are n components, we denote $S \times \cdots \times S$ as S^n.

A **binary relation** σ on a monoid S is a subset of $S \times S$. An alternative notation for $(a, b) \in \sigma$ is $a \,\sigma\, b$. The binary relation σ is **reflexive** if $a \,\sigma\, a$ for all $a \in S$; **symmetric** if for every $a, b \in S$ such that $a \,\sigma\, b$ we have that $b \,\sigma\, a$; and **transitive** if for every $a, b, c \in S$, $a \,\sigma\, b$ and $b \,\sigma\, c$ imply that $a \,\sigma\, c$. If σ verifies these three properties, it is an **equivalence relation**. A **congruence** σ on S is an equivalence relation on S compatible

with the operation $+$, that is to say, if $a \sigma b$, then $(a+c) \sigma (b+c)$ for all $c \in S$. Note that this is equivalent to saying that if $a \sigma b$ and $c \sigma d$, then $(a+c) \sigma (b+d)$. This compatibility of the congruence with the structure of the monoid enables us to construct quotients. For a given congruence σ on a monoid S, we define for each $a \in S$ the equivalence class of a modulo σ as

$$[a]_\sigma = \{b \in S \mid a \sigma b\}.$$

When there is no possible misunderstanding, we will simplify the notation and denote $[a]_\sigma$ by $[a]$. The set of classes of elements of S modulo σ is denoted by S/σ. We define on S/σ the following operation, which by abuse of notation, we denote once more by $+ : [a]+[b] = [a+b]$. Due to the fact that σ is compatible with the structure of S, one can easily prove that $(S/\sigma, +)$ is a commutative monoid. The monoid S/σ is known as the **quotient monoid** of S modulo σ. It is also easy to show that if S is a group, then so is S/σ, and the same holds for the property of being finitely generated.

Given two monoids S and S' a map f from S to S' is a **monoid morphism** if $f(0) = 0$ and $f(a+b) = f(a)+f(b)$ for all $a,b \in S$. We say that f is a **monomorphism**, **epimorphism** or **isomorphism** if f is injective, surjective or bijective, respectively. Clearly, if f is an isomorphism so is its inverse f^{-1}. Two monoids are **isomorphic** if there exists an isomorphism between them. The properties of being cancellative, group and finitely generated are preserved under isomorphisms. Given $f : S \to S'$ a morphism of monoids, we define the binary relation $\mathrm{Ker}(f)$ on S as

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

Using the fact that f is a morphism, it is straightforward to demonstrate that $\mathrm{Ker}(f)$ is a congruence. This congruence is known as the **kernel congruence** of f. We define the **image** of f as the set

$$\mathrm{Im}(f) = \{f(a) \mid a \in S\}.$$

Clearly, $\mathrm{Im}(f)$ is a monoid since f is a morphism. The following result relates these two concepts. The proof is left as an easy exercise to the reader.

THEOREM 1.1. *Let $f : S \to S'$ be a monoid morphism. Then*

$$\overline{f} : S/\mathrm{Ker}(f) \to \mathrm{Im}(f),\ \overline{f}([a]) = f(a)$$

is an isomorphism of monoids.

This isomorphism theorem yields the basic idea of presentation of a finitely generated monoid. It also enables us to ensure that every finitely generated monoid is, up to isomorphism, a quotient monoid of $\mathbb{N}^n$, where n is the number of generators of the given monoid. (Needless to say that $\mathbb{N}^n$ is a monoid.) This fact is stated in the following theorem.

THEOREM 1.2. *Let S be a monoid generated by $\{s_1, \ldots, s_n\}$. Then there exists a congruence σ on $\mathbb{N}^n$ such that S is isomorphic to $\mathbb{N}^n/\sigma$.*

PROOF. We define the map

$$f : \mathbb{N}^n \to S,\ f(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i s_i.$$

This map is an epimorphism of monoids and therefore taking σ as $\mathrm{Ker}(f)$ and using the Theorem 1.1, we get the desired result. □

Hence, studying properties of congruences on $\mathbb{N}^n$ is almost the same as studying properties of finitely generated monoids. This idea shall be used several times in this book. We start by using it with the cancellative property. For this purpose, we introduce the concepts of subgroup of $\mathbb{Z}^n$ associated to a congruence and congruence associated to a subgroup of $\mathbb{Z}^n$.

Let σ be a congruence on $\mathbb{N}^n$. We define

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

where $a - b$ denotes the subtraction in $\mathbb{Z}^n$ performed componentwise. Since σ is a congruence, it follows easily that M_σ is a subgroup of $\mathbb{Z}^n$.

Conversely, given a subgroup H of $\mathbb{Z}^n$, we define the binary relation

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

Clearly, $\sim_H$ is a congruence on σ. Immediately the question arises: what happens if we construct $\sim_{M_\sigma}$? Do we recover σ? And what about $M_{\sim_H}$? The last question is easy to answer, since $x \in M_{\sim_H}$ if and only if $x = a - b$ for some $(a,b) \in \sim_H$, and this occurs if and only if $x = a - b \in H$. Hence, $M_{\sim_H} = H$. However, the equality $\sigma = \sim_{M_\sigma}$ is not true in general. As a matter of fact, we will show that this equality holds if and only if $\mathbb{N}^n/\sigma$ is cancellative. To this end, we need a result that points out the relationship between σ and $\sim_{M_\sigma}$.

LEMMA 1.3. *Let σ be a congruence on $\mathbb{N}^n$.*

1. $\sigma \subseteq \sim_{M_\sigma}$,
2. *For every $(a,b) \in \sim_{M_\sigma}$, there exists $c \in \mathbb{N}^n$ such that $(a+c, b+c) \in \sigma$.*

PROOF. Take $(a,b) \in \sigma$. By the definition of M_σ, it is clear that $a - b \in M_\sigma$, and therefore $(a,b) \in \sim_{M_\sigma}$.

Now, take $(a,b) \in \sim_{M_\sigma}$. Then $a - b \in M_\sigma$ and therefore, by the definition of M_σ, there exists $(x,y) \in \sigma$ such that $a - b = x - y$. Since σ is a congruence, $(x+a, y+a) \in \sigma$, and consequently $(x+a, x+b) \in \sigma$, because $y + a = x + b$. Taking $c = x$, we get that $(a+c, b+c) \in \sigma$. □

With this result one already sees that there is a connection between cancellativity and the equality of σ and $\sim_{M_\sigma}$.

PROPOSITION 1.4. *Let σ be a congruence on $\mathbb{N}^n$. The monoid $\mathbb{N}^n/\sigma$ is cancellative if and only if $\sigma = \sim_{M_\sigma}$.*

PROOF. Let us assume that $\mathbb{N}^n/\sigma$ is cancellative. We already know that $\sigma \subseteq \sim_{M_\sigma}$, and therefore we only have to prove the other inclusion. Take $(a,b) \in \sim_{M_\sigma}$. By Lemma 1.3, there exists an element $c \in \mathbb{N}^n$ such that $(a+c, b+c) \in \sigma$, that is to say, the elements $[a+c] = [a]+[c]$ and $[b+c] = [b]+[c]$ are the equal in $\mathbb{N}^n/\sigma$. By cancellativity, we get that $[a] = [b]$ and therefore $(a,b) \in \sigma$.

Now, let $\sigma = \sim_{M_\sigma}$. If $[a]+[c] = [b]+[c]$, then $(a+c, b+c) \in \sigma$, and therefore $(a+c)-(b+c) = a-b \in M_\sigma$, which implies $(a,b) \in \sim_{M_\sigma} = \sigma$. Hence $[a] = [b]$. □

This result can be restated in a more transparent way. For a given subgroup H of $\mathbb{Z}^n$, we can define the following binary relation on $\mathbb{Z}^n$:

$$a \equiv_H b \text{ if and only if } a-b \in H.$$

As pointed out for $\sim_H$, it is easy to show that $\equiv_H$ is a congruence and therefore $\mathbb{Z}^n/\equiv_H$ is a monoid. Furthermore, since

$$[a-a]_{\equiv_H} = [a]_{\equiv_H} + [-a]_{\equiv_H} = [0]_{\equiv_H},$$

we get that $\mathbb{Z}^n/\equiv_H$ is a group. Usually, this group is denoted by $\mathbb{Z}^n/H$ and is called the **quotient group** of $\mathbb{Z}^n$ over H. Observe that this construction can be performed for Abelian groups in general. The next result shows the connection between $\sim_M$ and $\equiv_M$.

PROPOSITION 1.5. *Let H be a subgroup of $\mathbb{Z}^n$. The correspondence*

$$i : \mathbb{N}^n/\sim_H \to \mathbb{Z}^n/\equiv_H,\ i([a]_{\sim_H}) = [a]_{\equiv_H}$$

is a monoid monomorphism.

PROOF. Note that if $[a]_{\sim_H} = [b]_{\sim_H}$, then $a-b \in H$ and therefore $[a]_{\equiv_H} = [b]_{\equiv_H}$. Hence i is well defined. Clearly, i is a morphism of monoids. Observe also that if $[a]_{\equiv_H} = [b]_{\equiv_H}$, with $a,b \in \mathbb{N}^n$, then $a-b \in H$ and therefore $[a]_{\sim_H} = [b]_{\sim_H}$. Thus, i is a monomorphism. □

With this, we get the following result, which is also true for non-finitely generated monoids.

COROLLARY 1.6. *Let S be finitely generated monoid. Then S is cancellative if and only if S is isomorphic to a submonoid of a group.*

PROOF. By Theorem 1.2, S is isomorphic to $\mathbb{N}^n/\sigma$ for some positive integer n and some congruence σ on $\mathbb{N}^n$. Observe also that due to Proposition 1.4, $\sigma = \sim_{M_\sigma}$ and therefore S is isomorphic to $\mathbb{N}^n/\sim_{M_\sigma}$. Proposition 1.5 ensures that $\mathbb{N}^r/\sim_{M_\sigma}$ is a isomorphic to a submonoid of $\mathbb{Z}^n/M_\sigma$ which concludes the proof. □

The following result is devoted to the "shape" of groups, which we already know to be a special kind of cancellative monoids. We say that an element of $\mathbb{Z}^n$ is **strongly positive** if all its coordinates are positive. Analogously we say that an element of $\mathbb{Z}^n$ is **nonnegative** whenever its coordinates are nonnegative.

PROPOSITION 1.7. *Let S be a finitely generated monoid. The following statements are equivalent.*

(i) *S is a group.*
(ii) *S is isomorphic to $\mathbb{N}^n/\sim_H$ for some positive integer n and some subgroup H of $\mathbb{Z}^n$ containing a strongly positive element.*
(iii) *S is isomorphic to $\mathbb{Z}^n/H$ for some positive integer n and some subgroup H of $\mathbb{Z}^n$.*

PROOF. *(i) implies (ii)* From the proof of the Corollary 1.6, we get that S is isomorphic to $\mathbb{N}^n/\sim_{M_\sigma}$ for some positive integer n and some congruence σ on $\mathbb{N}^n$. Since S is a group, $\mathbb{N}^n/\sim_{M_\sigma}$ is also a group and therefore the element $[(1,\dots,1)]_{\sim_{M_\sigma}}$ must have an inverse. Let $[(a_1,\dots,a_n)]_{\sim_{M_\sigma}}$ be such inverse. Hence

$$[(a_1+1,\dots,a_n+1)]_{\sim_{M_\sigma}} = [(1,\dots,1)]_{\sim_{M_\sigma}} + [(a_1,\dots,a_n)]_{\sim_{M_\sigma}} = [(0,\dots,0)]_{\sim_{M_\sigma}}$$

and consequently $(a_1+1,\dots,a_n+1)\sim_{M_\sigma}(0,\dots,0)$, which by the definition of M_σ means that $(a_1+1,\dots,a_n+1)-(0,\dots,0)\in M_\sigma$. Clearly, $(a_1+1,\dots,a_n+1)$ is a strongly positive element of M_σ.

(ii) implies (iii) It is enough to show that if H contains a strongly positive element, then the map i of Proposition 1.5 is surjective. Let $a\in H$ be a strongly positive element. Take $[x]_{\equiv_H}\in\mathbb{Z}^n/H$. Since all the coordinates of a are positive, there must exist an element $k\in\mathbb{N}$ such that $ka+x\in\mathbb{N}^n$. We get $[ka+x]_{\equiv H}=[x]_{\equiv_H}$, since $ka\in H$. Note that

$$i([ka+x]_{\sim_H}) = [ka+x]_{\equiv_H} = [x]_{\equiv_H}.$$

This shows that i is an isomorphism.

(iii) implies (i) It is clear that if S is isomorphic to $\mathbb{Z}^n/H$ for some subgroup H of $\mathbb{Z}^n$, then S is a group. □

Remarks

We have presented some basic concepts related with the theory of finitely generated (commutative) monoids. The reader surely has noticed the existence of two subclasses of finitely generated monoids which are groups and cancellative monoids. These subclasses shall be studied in this order in the next chapters. The knowledge of groups shall be used to know the wider class of cancellative monoids and later this one shall be used for a better understanding of finitely generated monoids in general. An obligatory reference for the contents of this chapter are the books **[9]** and **[39]**.

Exercises

1. Compute a minimal system of generators of $(\mathbb{N}^n,+)$.
2. Prove that

$$(\{(n,m)\in\mathbb{N}^2 \mid n\geq 1, m\geq 1\}\cup\{(0,0)\},+)$$

is a monoid which is not finitely generated.

3. Show that the pair

$$(\{n \in \mathbb{N} \mid n \geq 4\} \cup \{0\}, +)$$

is a finitely generated monoid.

4. Find a minimal set of generators of the monoid $(\mathbb{Z}, +)$.
5. Show that $(\mathbb{N}, \times)$ is a monoid which is not cancellative.
6. Prove that $(\mathbb{N} \setminus \{0\}, \times)$ is a cancellative monoid which is not finitely generated.
7. Let $H = \{(x,y,z) \in \mathbb{Z}^3 \mid x+y-z=0\}$.
   (a) Show that H is a subgroup of $\mathbb{Z}^3$.
   (b) Show that $\mathbb{N}^3 / \sim_H$ is a group.
8. Let σ be the binary relation defined on $\mathbb{N}^2$ as

$$(a,b)\ \sigma\ (c,d) \text{ if and only if } a-c+b-d=0.$$

   Prove that:
   (a) σ is a congruence,
   (b) $\mathbb{N}^2/\sigma$ is cancellative,
   (c) $\mathbb{N}^2/\sigma$ is not a group.
9. Let σ be the binary relation defined on $\mathbb{N}$ as:
   - If a and b are greater than or equal to 7, then $a\ \sigma\ b$ if and only if $a-b \equiv 0 (\mathrm{mod}\ 3)$.
   - If a or b are smaller than 7, then $a\ \sigma\ b$ if and only if $a=b$.

   Show that:
   (a) σ is a congruence.
   (b) $\mathbb{N}/\sigma$ is not cancellative.
10. Let $(S,+)$ be a semigroup without identity element and let x be an element not belonging to S. We can extend $+$ to $S \cup \{x\}$ defining $x+x=x$, $x+s=s$ and $s+x=s$. Show that $(S \cup \{x\}, +)$ is a monoid.
11. Let S be the set of nonnegative integer solutions of the equation $2x-3y=0$. Show that S is a monoid and find a minimal system of generators of S.
12. Let H be the subgroup of $\mathbb{Z}^2$ generated by $\{(1,1)\}$. Show that $\mathbb{N}^2 / \sim_H$ is a monoid isomorphic to $\mathbb{Z}$.
13. Let S_1 and S_2 be two monoids. Prove that:
   (a) $S_1 \times S_2$ is cancellative if and only if S_1 and S_2 are cancellative,
   (b) $S_1 \times S_2$ is a group if and only if S_1 and S_2 are groups,
   (c) $S_1 \times S_2$ is finitely generated if and only if S_1 and S_2 are finitely generated.
14. Let S be a monoid and let σ be a congruence on S. Show that
   (i) if S is finitely generated, then so is S/σ,
   (ii) the converse of (i) is not true.
15. Let S_1 and S_2 be two submoniods of the monoid S. Prove that

$$S_1 + S_2 = \{s_1 + s_2 \mid s_1 \in S_1,\ s_2 \in S_2\}$$

is a submonoid of S. Furthermore, if S_1 and S_2 are finitely generated, then so is S_1+S_2. Find a monoid S and two submonoids S_1 and S_2 of S such that S_1+S_2 is finitely generated but S_1 or S_2 is not finitely generated.

16. Let S be a monoid. We define on S the following binary relation: $a\ \sigma\ b$ if and only if $a+c=b+c$ for some $c \in S$. Prove that σ is a congruence on S and that S/σ is cancellative.

CHAPTER 2

Finitely generated commutative groups

In view of the last result proved in the preceding chapter, studying finitely generated commutative groups is equivalent to studying group quotients of the form $\mathbb{Z}^k/H$. We deal here with a classical result in Group Theory: the structure theorem for finitely generated commutative groups. We are not only interested in the structure theorem itself, but also in some of the results that lead to its proof. In particular, the procedure to compute the defining equations of a given subgroup of $\mathbb{Z}^n$ shall be used later. The reader acquainted with these statements and concepts can skip this chapter. The mentioned result states that every finitely generated Abelian group is isomorphic to a group of the form $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$, where $d_1, \dots, d_r, k$ are positive integers such that d_i divides d_{i+1} and $\mathbb{Z}_{d_i}$ denotes the quotient group $\mathbb{Z}/\mathbf{G}(\{d_i\})$.

The ideas used to demonstrate the structure theorem are the following.

1. Proposition 1.7 states that every finitely generated group is of the "form" $\mathbb{Z}^n/H$ for H a subgroup of $\mathbb{Z}^n$.
2. If $\{f_1, \dots, f_n\}$ is a basis of $\mathbb{Z}^n$ and $H = \mathbf{G}(\{d_1 f_1, \dots, d_r f_r\})$ with d_i positive integer number, then $\mathbb{Z}^n/H$ is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$.
3. Every subgroup of $\mathbb{Z}^n$ has a basis of the form $\{d_1 f_1, \dots, d_r f_r\}$ with $\{f_1, \dots, f_n\}$ a basis of $\mathbb{Z}^n$.

The first point has been treated already in the last chapter. The preceding two ideas are tightly related to the concepts of basis and invariant factors of a subgroup of $\mathbb{Z}^n$.

1. Bases and rank of a subgroup of $\mathbb{Z}^n$

Let M be a subgroup of $\mathbb{Z}^n$. We say that $\{m_1, \dots, m_r\} \subset M$ is a **basis** of M if every element in M can be written in a unique way as $m = \sum_{i=1}^r z_i m_i$ for some $z_1, \dots, z_r \in \mathbb{Z}$. The element $(z_1, \dots, z_r) \in \mathbb{Z}^r$ is usually known as **coordinates** of m with respect to the basis $\{m_1, \dots, m_r\}$. Observe that $\{m_1, \dots, m_r\}$ is a basis of M if and only if

1. every element $m \in M$ admits an expression of the form $m = \sum_{i=1}^r z_i m_i$ for some $z_1, \dots, z_r \in \mathbb{Z}$,
2. if $\sum_{i=1}^r z_i m_i = 0$ for some $z_1, \dots, z_r \in \mathbb{Z}$, then $z_i = 0$ for all i.

The first condition is telling us that the set $\{m_1, \dots, m_r\}$ is a system of generators of the group M, that is to say, $M = \mathbf{G}(\{m_1, \dots, m_r\})$. If $\{m_1, \dots, m_r\}$ satisfies the second condition, we say that the elements $m_1, \dots, m_r$ are **linearly independent**. Observe that $m_1, \dots, m_r \in \mathbb{Z}^n$ are linearly independent if and only if they are linearly independent as vectors in $\mathbb{Q}^n$ viewed as a vector space over $\mathbb{Q}$.

Let e_i denote the element having all its coordinates equal to zero but the i-th coordinate which is equal to one. Note that $\{e_1, \dots, e_n\}$ is a basis of $\mathbb{Z}^n$. Let us recall some basic results related to this concept.

PROPOSITION 2.1. *Let M be a subgroup of $\mathbb{Z}$. Then there exists $z \in M$ such that $M = \mathbf{G}(\{z\})$.*

PROOF. Note that if $M = \{0\}$, then $M = \mathbf{G}(\{0\})$. Assume that $M \neq 0$. Clearly, the set $\{h \in M \mid h > 0\}$ is not empty and therefore it has a minimum, say z. We show that $M = \mathbf{G}(\{z\})$. The inclusion $\mathbf{G}(\{z\}) \subseteq M$ is trivial. Take $h \in M$. By the division algorithm in $\mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < z$ and $h = qz + r$. Since $0 \leq r = h - qz < z$ and z is the minimum element in M greater than zero, we have $r = 0$ and therefore $h = qz \in \mathbf{G}(\{z\})$. □

Observe that a basis for $\{0\} \subset \mathbb{Z}^n$ is the empty set. The following result gives a bound for the number of elements appearing in a basis of a subgroup of $\mathbb{Z}^n$.

PROPOSITION 2.2. *Let M be a subgroup of $\mathbb{Z}^n$. Then M has a basis with at most n elements.*

PROOF. For each $j \in \{1, \dots, n\}$, we define $M_j = M \cap \mathbf{G}(\{e_1, \dots, e_j\})$. Observe that $M_n = M$. Let us show, using induction, that M_i has a basis with at most i elements.

If $M_1 = \{0\}$, then a basis for M_1 is the empty set which has less than one element. If $M_1 \neq \{0\}$, let $H = \{k \in \mathbb{Z} \mid ke_1 \in M_1\}$. Clearly, H is a subgroup of $\mathbb{Z}$ and by Proposition 2.1, it is equal to $\mathbf{G}(\{z\})$ for some $z \in \mathbb{Z} \setminus \{0\}$. It is straightforward to show that $M_1 = \mathbf{G}(\{ze_1\})$ and consequently that $\{ze_1\}$ is a basis of M_1. This shows that the statement is true for $i = 1$.

Assume that M_k has a basis $\{m_1, \dots, m_r\}$ with $r \leq k$. Note that if $M_{k+1} = \{0\}$, then so is M_k and therefore $r = 0$ and a basis of M_{k+1} is the empty set. Assume that $M_{k+1} \neq \{0\}$ and define

$$H = \{z \in \mathbb{Z} \mid y + ze_{k+1} \in M \text{ for some } y \in \mathbf{G}(\{e_1, \dots, e_k\})\}.$$

Once more H is a subgroup of $\mathbb{Z}$ and therefore $H = \mathbf{G}(\{z\})$ for some $z \in \mathbb{Z}$. If $z = 0$, then $M_{k+1} = M_k$, which trivially implies that M_{k+1} has a basis with r elements and $r \leq k \leq k+1$. If $z \neq 0$, then there exists an element $y \in \mathbf{G}(\{e_1, \dots, e_k\})$ such that $w = y + ze_{k+1} \in M_{k+1}$. Let us show that $\{m_1, \dots, m_r, w\}$ is a basis of M_{k+1}.

- Take $m \in M_{k+1}$. Hence $m \in \mathbf{G}(\{e_1, \dots, e_{k+1}\})$, which means that $m = \sum_{i=1}^{k+1} z_i e_i$ for some $z_1, \dots, z_{k+1} \in \mathbb{Z}$. Therefore, $z_{k+1} \in H$ which implies that $z_{k+1} = zt$ for some $t \in \mathbb{Z}$. Thus, $m = \sum_{i=1}^{k} z_i e_i - ty + tw$ and consequently

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

  Since $\{m_1, \dots, m_r\}$ is a basis of M_k, there exist $t_1, \dots, t_r \in \mathbb{Z}$ such that $m - tw = \sum_{i=1}^{r} t_i m_i$, which leads to $m = \sum_{i=1}^{r} t_i m_i + tw$.

- Assume that there exist $s_1, \dots, s_{r+1} \in \mathbb{Z}$ such that $\sum_{i=1}^r s_i m_i + s_{r+1} w = 0$. Since $\sum_{i=1}^r s_i m_i \in \mathbf{G}(\{e_1, \dots, e_k\})$ and w is the only element with the $k+1$-th coordinate different from zero, we get that $s_{r+1} = 0$. Consequently $\sum_{i=1}^r s_i m_i = 0$ and this implies that $s_1 = \cdots = s_r = 0$, since $\{m_1, \dots, m_r\}$ is a basis of M_k.

We have shown that $\{m_1, \dots, m_r, w\}$ is a basis of M_{k+1} with $r+1$ elements and $r+1 \leq k+1$. □

The next result is the translation of a well known result of bases of vector spaces. Its proof leans on concepts related to Linear Algebra. We denote by

$$\mathbf{L}_{\mathbb{Q}}(A) = \{\sum_{i=1}^n q_i a_i \mid n \in \mathbb{N}, a_i \in A, q_i \in \mathbb{Q}\}$$

the subspace of $\mathbb{Q}^n$ spanned by A.

PROPOSITION 2.3. *Let M be a subgroup of $\mathbb{Z}^n$. Then all bases of M have the same cardinality.*

PROOF. Assume that $B = \{m_i \mid i \in I\}$ and $B' = \{n_i \mid i \in I'\}$ are two different bases of M. Since the elements in B are linearly independent as vectors in $\mathbb{Q}^n$, we have that there can be, at most, n elements in B. The same holds for B'. Observe also that B is a basis of the vector space $V = \mathbf{L}_{\mathbb{Q}}(B)$ and since $B' \subset M = \mathbf{G}(\{m_1, \dots, m_r\}) \subset \mathbf{L}_{\mathbb{Q}}(B)$ is a set of linearly independent vectors of V, the cardinality of B' must be less than or equal to the cardinality of B. Analogously, we can show the opposite inequality. □

Since the cardinality of all bases of a subgroup M of $\mathbb{Z}^n$ is the same, we can define the **rank** of M, denoted by $\operatorname{rank}(M)$, as the number of elements appearing in one of its bases. Note that $\operatorname{rank}(M) \leq n$.

As for vector subspaces, a subgroup of $\mathbb{Z}^n$ of rank k is isomorphic to $\mathbb{Z}^k$.

PROPOSITION 2.4. *Let M be a subgroup of $\mathbb{Z}^n$ of rank k. Then M is isomorphic to $\mathbb{Z}^k$.*

PROOF. Let $B = \{m_1, \dots, m_k\}$ be a basis of M. The fact that every element in M has unique coordinates with respect to B, implies that the map

$$f : \mathbb{Z}^k \to M,\ f(z_1, \dots, z_k) = \sum_{i=1}^k z_i m_i$$

is an isomorphism of groups. □

With this result it is straightforward to show the following consequence.

COROLLARY 2.5. *Let M and M' be two subgroups of $\mathbb{Z}^n$. Then M and M' are isomorphic if and only if* $\operatorname{rank}(M) = \operatorname{rank}(M')$.

2. Equivalence of matrices with integer entries and invariant factors

In order to introduce the concept of invariant factors of a subgroup of $\mathbb{Z}^n$ and prove the structure theorem for finitely generated groups, we need to recall some results concerning matrices with integer entries. The underlying idea is to transform a basis of the given subgroup of $\mathbb{Z}^n$, using "elementary" operations, into a basis which is of the form described at the beginning of the chapter. These operations will be performed in terms of a transformation of the matrix whose rows are the elements of a basis of the given subgroup. The process is very similar to that of Gaussian elimination.

For a given positive integer n and $1 \leq i, j \leq n, (i \neq j)$ we define the following matrices:

1. $R_{i\leftrightarrow j}$ is the matrix obtained from the identity matrix I_n interchanging the rows i and j,
2. $R_{i\leftarrow -i}$ is the matrix obtained from the identity matrix by multiplying its i-th row by -1,
3. $R_{j\leftarrow j+zi}$ is the matrix obtained from the identity matrix by adding to the j-th row the i-th row multiplied by $z \in \mathbb{Z}$.

$C_{i\leftrightarrow j}$, $C_{i\leftarrow -i}$ and $C_{j\leftarrow j+zi}$ are defined likewise but using columns instead of rows. $R_{i\leftrightarrow j}$, $R_{i\leftarrow -i}$ and $R_{j\leftarrow j+zi}$ are known as **row elementary matrices** and $C_{i\leftrightarrow j}$, $C_{i\leftarrow -i}$ and $C_{j\leftarrow j+zi}$ as **column elementary matrices**.

The proof of the following result is left as an exercise for the reader.

PROPOSITION 2.6. *Let i, j be two positive integers. Let z be an element in $\mathbb{Z}$, A be a $n \times n$-matrix with integer coefficients and let* $\det(B)$ *denote the determinant of a matrix B. Then,*

1. $\det(R_{i\leftrightarrow j}) = \det(C_{i\leftrightarrow j}) = -1$.
2. $R_{i\leftrightarrow j}^{-1} = R_{j\leftrightarrow i}$ *and* $C_{i\leftrightarrow j}^{-1} = C_{j\leftrightarrow i}$.
3. $\det(R_{i\leftarrow -i}) = \det(C_{i\leftarrow -i}) = -1$.
4. $R_{i\leftarrow -i}^{-1} = R_{i\leftarrow -i}$ *and* $C_{i\leftarrow -i}^{-1} = C_{i\leftarrow -i}$.
5. $\det(R_{j\leftarrow j+zi}) = \det(C_{j\leftarrow j+zi}) = 1$.
6. $R_{j\leftarrow j+zi}^{-1} = R_{j\leftarrow j-zi}$ *and* $C_{j\leftarrow j+zi}^{-1} = C_{j\leftarrow j-zi}$.
7. *The matrix $R_{i\leftrightarrow j}A$ is the matrix obtained from A by interchanging its rows i and j. The matrix $AC_{i\leftrightarrow j}$ is the matrix resulting from interchanging the columns i and j in the matrix A.*
8. *The matrix $R_{i\leftarrow -i}A$ is the matrix obtained from A by multiplying its i-th row by -1. The matrix $AC_{i\leftarrow -i}$ is the matrix that results when we multiply the i-th column of A by -1.*
9. *The matrix $R_{j\leftarrow j+iz}A$ is the matrix obtained from A by adding to its j-th row the i-th row multiplied by z. The matrix $AC_{j\leftarrow j+iz}$ is the matrix that results when we add to the j-th column the i-th column multiplied by z.*

Given two matrices A and B with integer entries, we say that they are **equivalent** if there exists $P_1, \ldots, P_r$ row elementary matrices and $Q_1, \ldots, Q_s$ column elementary

matrices such that $B = P_1 \cdots P_r A Q_1 \cdots Q_s$. Using Proposition 2.6, it is easy to show that the binary relation $A \sim B$ if and only if A and B are equivalent is an equivalence relation.

When multiplying by matrices of the form R_* we will say that we are performing elementary operations on the rows of the given matrix. Similarly, when we use the matrices C_* instead, we will say that we are performing elementary operations on the columns of the matrix.

The main difference between working over the integers and over the rationals (or over an arbitrary field) is that in the latter case, the matrices of the form $R_{i \leftarrow qi}$ and $C_{i \leftarrow qi}$, with q an element of the field different from zero, are also elementary matrices. Hence, when one performs Gauss-Jordan elimination on a matrix with entries over a field, the first step to follow is to put a nonzero entry in the upper left position of the matrix. This is achieved using elementary matrices of the form $R_{i \leftrightarrow j}$ and $C_{i \leftrightarrow j}$, that is to say, interchanging positions between rows and columns so that we move a nonzero entry of the matrix to the upper left corner. Then we can divide the first column or row by this amount and get 1 in the upper left corner. Once we have this, we only have to use matrices of the form $R_{j \leftarrow j+z1}$ and $C_{j \leftarrow j+z1}$ in order to get a matrix equivalent to the original one and verifying that the first column and row have all entries, but the first one, equal to zero. After that, the same procedure is repeated with the submatrix obtained by eliminating the first row and column of the former matrix. For the integer case, the procedure is not so easy. Usually, we cannot divide a row or a column by a number different from 1 or -1 and get an equivalent matrix. The procedure to follow in the integer case is described in the next result.

PROPOSITION 2.7. *Let A be a matrix with s rows and t columns and with integer entries. Then A is equivalent to a matrix of the form*

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

where $r \leq \min\{s,t\}$, $\{d_1, \ldots, d_r\} \subset \mathbb{N} \setminus \{0\}$ and d_i divides d_{i+1} for all i.

PROOF. As usual, we denote by a_{ij} the entry of the matrix lying in the intersection of the i-th row and the j-th column. Note that if A is the zero matrix, then the result follows for $r = 0$. Now, assume that A has a nonzero entry. Using elementary operations over A, we can move the smallest, in absolute value, entry to the (1,1) position, that is to say, to the upper left corner of the matrix. The resulting matrix B is equivalent to A. Next, we check whether there is an element in the first row which is not divided by this element. If this is not so, suppose, without loss of generality, that this element

is in the (1,2) position. We compute $\gcd\{b_{11}, b_{12}\} = d$ using Euclid's algorithm. We can translate the operations involved in the computation of d to elementary operations performed by multiplying our matrix by matrices of the form $C_{1\leftarrow 1+z2}$ and eventually by $C_{1\leftrightarrow 2}$. With this, we get a matrix equivalent to A so that the entry in the (1,1) position divides the entry in the (1,2) position. We perform this process for the rest of the elements of the first row of the resulting matrix and get a matrix C equivalent to A such that c_{11} divides c_{1i} for all i. Then we multiply the first column by suitable integers and add the result to the other columns ($C_{j\leftarrow j+z1}$) getting in this way a matrix whose first row has all its entries equal to zero but the first one. We can repeat an analogous procedure for the first column. Eventually, in this process the first row may be altered, in which case, the procedure must be repeated from the beginning. Observe that every time we repeat this procedure, the (1,1) entry may only be replaced by one of its divisors, and this stops when this element is also a divisor of all the elements in the first column and row. After a finite number of steps, we get a matrix of the form

$$\left(\begin{array}{c|ccc} f_{11} & 0 & \cdots & 0 \\ \hline 0 & f_{22} & \cdots & f_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & f_{s2} & \cdots & f_{st} \end{array}\right).$$

If there exist i, j such that f_{11} does not divide f_{ij}, then we add the i-th row to the first row (multiplying by $R_{1\leftarrow 1+1i}$ on the left) and we restart the process from the beginning. After a finite number of steps, we get in the (1,1) position the greatest common divisor of all the entries of A. Hence, our matrix becomes equivalent to one of the form

$$\left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & g_{22} & \cdots & g_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & g_{s2} & \cdots & g_{st} \end{array}\right),$$

with d_1 a divisor of g_{ij} for all i, j. We now repeat this procedure on the submatrix

$$\begin{pmatrix} g_{22} & \cdots & g_{2t} \\ \vdots & \ddots & \vdots \\ g_{s2} & \cdots & g_{st} \end{pmatrix}.$$

After a finite number of steps, we get the desired result. □

The elements $d_1, \ldots, d_r$ are called the **invariant factors** of A. We shall prove that they are unique.

A k-**minor** of a matrix A is the determinant of a submatrix of A with k rows and k columns. We denote by $\mathrm{D}_k(A)$ the greatest common divisor of all the k-minors of A. It is easy to show the following properties of D_k.

PROPOSITION 2.8. *Let A be a matrix with integer coefficients.*

1. $\mathrm{D}_k(R_{i\leftrightarrow j}A) = \mathrm{D}_k(A) = \mathrm{D}_k(AC_{i\leftrightarrow j})$.

2. $\mathrm{D}_k(R_{i\leftarrow -i}A) = \mathrm{D}_k(A) = \mathrm{D}_k(AC_{i\leftarrow -i})$.
3. $\mathrm{D}_k(R_{j\leftarrow j+zi}A) = \mathrm{D}_k(A) = \mathrm{D}_k(AC_{j\leftarrow j+zi})$.

As a consequence of this result we get that if A and B are equivalent then $\mathrm{D}_k(A) = \mathrm{D}_k(B)$ for all k. With this, we are ready to show that the invariant factors are unique and even more.

PROPOSITION 2.9. *Let A and B be two matrices with integer entries. Then A is equivalent to B if and only if they have the same invariant factors.*

PROOF. Since the binary relation $\sim$ is an equivalence relation, using Proposition 2.7, we get that it is enough to show that the matrices

$$\delta_1 = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$\delta_2 = \begin{pmatrix} d'_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d'_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d'_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

with $\{d_1, \dots, d_r, d'_1, \dots, d'_s\} \subset \mathbb{N} \setminus \{0\}$, d_i dividing d_{i+1} and d'_i dividing d'_{i+1} for all i, are equivalent if and only if $r = s$ and $d_i = d'_i$ for all i. Clearly, if $r = s$ and $d_i = d'_i$ then δ_1 and δ_2 are equivalent. The converse is a direct consequence of the fact that if δ_1 and δ_2 are equivalent, then $d_1 \cdots d_k = \mathrm{D}_k(\delta_1) = \mathrm{D}_k(\delta_2) = d'_1 \cdots d'_k$. □

We are ready to translate all these results to subgroups of $\mathbb{Z}^n$. The proof of the following result is left as an exercise to the reader.

PROPOSITION 2.10. *Let $\{m_1, \dots, m_i, \dots, m_j, \dots, m_r\}$ be a basis of a subgroup M of $\mathbb{Z}^n$. Then,*

1. *$\{m_1, \dots, m_j, \dots, m_i, \dots, m_r\}$ is a basis of M.*
2. *$\{m_1, \dots, -m_i, \dots, m_j, \dots, m_r\}$ is a basis of M.*
3. *$\{m_1, \dots, m_i, \dots, m_j + zm_i, \dots, m_r\}$ is a basis of M.*

These changes of a basis are known as **elementary changes of basis**. It is straightforward to show that this result is also true for systems of generators.

PROPOSITION 2.11. *Let*

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

be a matrix with integer entries and let $b_i = (b_{i1}, \dots, b_{in}) \in \mathbb{Z}^n$. *The set* $\{b_1, \dots, b_n\}$ *is a basis of* $\mathbb{Z}^n$ *if and only if* $\det(B) \in \{-1, 1\}$.

PROOF. *Necessity.* For each $i \in \{1, \dots, n\}$, there must exist $z_{i1}, \dots, z_{in} \in \mathbb{Z}$ such that $\sum_{j=1}^{n} z_{ij} b_j = e_i$. Hence,

$$\begin{pmatrix} z_{11} & \cdots & z_{1n} \\ \vdots & \ddots & \vdots \\ z_{n1} & \cdots & z_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

and therefore $\det((z_{ij}))\det(B) = 1$, which implies that $\det(B) \in \{-1, 1\}$.

Sufficiency. The matrix B is invertible and therefore the system of equations

$$(x_1, \dots, x_n)B = z,$$

has an unique solution, zB^{-1} for all $z \in \mathbb{Z}^n$ and this is the same as to say that every element has unique coordinates with respect to $\{b_1, \dots, b_n\}$ and consequently this set is a basis. □

We are now ready to prove one of the key results of this chapter.

THEOREM 2.12. *Let* M *be a subgroup of* $\mathbb{Z}^n$ *such that* $\operatorname{rank}(M) = r$. *Then there exists a basis* $\{f_1, \dots, f_r, \dots, f_n\}$ *of* $\mathbb{Z}^n$ *and* $\{d_1, \dots, d_r\} \subset \mathbb{N} \setminus \{0\}$, *such that* d_i *divides* d_{i+1} *for all* i, *and* $\{d_1 f_1, \dots, d_r f_r\}$ *is a basis of* M.

PROOF. Let $\{m_1, \dots, m_r\}$ be a basis of M with $m_i = (m_{i1}, \dots, m_{in})$ for all i. Using Proposition 2.7, we know that there exist matrices P and Q such that

$$P \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix} Q = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

for some $0 \le s \le \min\{r, n\}$ and $\{d_1, \dots, d_s\} \subset \mathbb{N} \setminus \{0\}$ such that d_i divides d_{i+1} for all i. First of all observe that since the matrices P and Q are invertible, the rank of the

matrix

$$\begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix}$$

and the rank of the matrix

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

are the same and therefore $s = r$. In addition let

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rn} \end{pmatrix} = P \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix}$$

and set $c_i = (c_{i1}, \dots, c_{in})$. The set $\{c_1, \dots, c_r\}$ was obtained from $\{m_1, \dots, m_r\}$ after a finite set of elementary changes of basis (the ones "stored" in P) and therefore $\{c_1, \dots, c_r\}$ is a basis of M.

Finally, observe that if we compute Q^{-1} and denote it by

$$Q^{-1} = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix},$$

we get that the set $\{f_1, \dots, f_n\}$, with $f_i = (f_{i1}, \dots, f_{in})$, is a basis of $\mathbb{Z}^n$ (Proposition 2.11) and

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rn} \end{pmatrix} = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix},$$

which means that $c_i = d_i f_i$ for all $i \in \{1, \dots, r\}$. □

As expected, the numbers $d_1, \dots, d_r$ are known as **invariant factors** of the subgroup M. Since $\{f_1, \dots, f_r, \dots, f_n\}$ is a basis of $\mathbb{Z}^n$ and $\{d_1 f_1, \dots, d_r f_r\}$ is a basis of M, an element $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$ belongs to M if and only if its coordinates $(z_1, \dots, z_n)$

with respect to the basis $\{f_1, \dots, f_n\}$ satisfy the following conditions:

$$\begin{aligned} z_1 &\equiv 0 \pmod{d_1}, \\ &\vdots \\ z_r &\equiv 0 \pmod{d_r}, \\ z_{r+1} &= 0, \\ &\vdots \\ z_n &= 0. \end{aligned}$$

Assume now that, as in the proof of Theorem 2.12, $f_i = (f_{i1}, \dots, f_{in})$ for all i. The fact that $(z_1, \dots, z_n)$ are the coordinates of x with respect to $\{f_1, \dots, f_n\}$ means that $x = (x_1, \dots, x_n) = \sum_{i=1}^n z_i f_i$, and therefore

$$(x_1, \dots, x_n) = (z_1, \dots, z_n) \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix},$$

which implies that

$$(z_1, \dots, z_n) = (x_1, \dots, x_n) \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix},$$

where the matrix with entries b_{ij} is the inverse of the matrix with entries f_{ij} (the matrix Q in the proof of Theorem 2.12). Hence, the element $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$ is in M if and only if

$$\begin{aligned} b_{11}x_1 + \cdots + b_{n1}x_n &\equiv 0 \pmod{d_1}, \\ &\vdots \\ b_{1r}x_1 + \cdots + b_{nr}x_n &\equiv 0 \pmod{d_r}, \\ b_{1(r+1)}x_1 + \cdots + b_{n(r+1)}x_n &= 0, \\ &\vdots \\ b_{1n}x_1 + \cdots + b_{nn}x_n &= 0. \end{aligned}$$

These equations are generally known as the **equations of M with respect to the basis** $\{e_1, \dots, e_n\}$ or simply **equations of M**. If $d_i = 1$, then the corresponding equation can be eliminated. The subgroup M is **homogeneous** if among its equations there are no equations in congruences, that is to say, its invariant factors are all equal to one.

EXAMPLE 2.13. Let $M = \mathbf{G}(\{(2,-1,1),(3,2,-1)\}) \subseteq \mathbb{Z}^3$. In order to keep track of the changes performed to the corresponding matrix, we will store them in matrices at both sides of the original matrix. The one on the left will store the changes on the rows and the one on the right the changes performed to the columns. In the last step, these two matrices become the matrices we must use to obtain the diagonal matrix

from the original matrix.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & -1 & 1 \\ 3 & 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 & 2 \\ -1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 5 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 5 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & -2 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -5 \\ 1 & 1 & -7 \end{pmatrix}$$

Hence

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & -1 & 1 \\ 3 & 2 & -11 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -5 \\ 1 & 1 & -7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

and therefore the equations of M are

$$\begin{aligned} x_3 &\equiv 0 \pmod 1, \\ x_2 + x_3 &\equiv 0 \pmod 1, \\ x_1 - 5x_2 - 7x_3 &= 0. \end{aligned}$$

Since the first two equations are redundant, we get that $(x_1, x_2, x_3) \in M$ if and only if $x_1 - 5x_2 - 7x_3 = 0$. ◇

The following theorem provides the last ingredient for demonstrating the structure theorem for finitely generated commutative groups.

THEOREM 2.14. *Let M be a subgroup of $\mathbb{Z}^n$ with invariant factors $d_1, \dots, d_r$. Then $\mathbb{Z}^n/M$ is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$.*

PROOF. We already know, by Theorem 2.12, that there exists a basis of M of the form $\{d_1 f_1, \dots, d_r f_r\}$ with $\{f_1, \dots, f_r, \dots, f_n\}$ a basis of $\mathbb{Z}^n$. Consider the map

$$\varphi : \mathbb{Z}^n/M \to \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$
$$\varphi([\textstyle\sum_{i=1}^n z_i f_i]_{\equiv_M}) = ([z_1]_{d_1}, \dots, [z_r]_{d_r}, z_{r+1}, \dots, z_n),$$

where, in order to simplify notation, $[z_i]_{d_i}$ denotes the element $[z_i]_{\equiv_{\mathbf{G}(\{d_1\})}}$ in $\mathbb{Z}_{d_i} = \mathbb{Z}/\mathbf{G}(\{d_i\})$. We leave to the reader the proof that φ is well defined and that it is an isomorphism of groups. □

3. Some practical results concerning the computation of a basis

We already know how to compute the defining equations of a subgroup of $\mathbb{Z}^n$ provided that we know one of its bases. The method explained in the preceding section is suitable also if we are given a system of generators instead of a basis of M. However, it may happen that we are interested in knowing a basis of M and only a system of generators of M or a set of defining equations of M is given.

3.1. Computing a basis of a subgroup of $\mathbb{Z}^n$ from one of its systems of generators. Before describing the procedure to compute a basis from a system of generators, observe that if Q is a matrix with integer entries whose determinant is not equal to zero and $f : \mathbb{Z}^n \to \mathbb{Z}^n$ is the map defined by $f(x_1,\dots,x_1) = (x_1,\dots,x_n)Q$, then the elements $m_1,\dots,m_r$ are linearly independent if and only if the elements $f(m_1),\dots,f(m_r)$ are linearly independent. The map $g : \mathbb{Q}^n \to \mathbb{Q}^n, g(x) = xQ$ is an isomorphism of vector spaces and hence it preserves linear independency of sets of vectors.

Let M be a subgroup of $\mathbb{Z}^n$ generated by $\{m_1,\dots,m_s\}$ with $m_i = (m_{i1},\dots,m_{in})$ for all $i \in \{1,\dots,s\}$. Let A be the matrix whose rows are $m_1,\dots,m_s$. We know that the matrix A is equivalent to a diagonal matrix of the form

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

with $d_1,\dots,d_r \in \mathbb{N}\setminus\{0\}$, and that there exist P and Q such that $PAQ = D$. Furthermore, we know that P and Q are the product of row and column elementary matrices, respectively. Observe that $PA = DQ^{-1}$ and thus the following statements hold.

1. The last $s-r$ rows of PA have all their entries equal to zero, since $PA = DQ^{-1}$ and Q performs only elementary operations on the columns of D and D has the last $s-r$ rows equal to zero.
2. The rows of PA are a system of generators of M, since P is a matrix that performs only elementary operations on the rows of A. Hence, the first r rows of PA are a system of generators of M.
3. The first r rows of PA are linearly independent, since the first r rows of D are linearly independent and $\det(Q) \neq 0$.

Hence a basis of M can be obtained by computing PA and extracting its first r rows.

3.2. Computing a basis of a subgroup of $\mathbb{Z}^n$ from its defining equations. We study first the homogeneous case (all the invariant factors are equal to one) and then the general case which, as we are going to see, can be reduced to the homogeneous case.

Let M be a homogeneous subgroup of $\mathbb{Z}^n$ and assume that $x \in M$ if and only if $Ax = 0$, where A is a given matrix with integer entries. We can compute P and Q such that $PAQ = D$, where P and Q are products of row and column elementary matrices, respectively, and D is a diagonal matrix of the form

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

with $d_1, \dots, d_r \in \mathbb{N} \setminus \{0\}$. Hence $AQ = P^{-1}D$ and therefore AQ is a matrix whose last $n-r$ columns are equal to 0. This implies that the last $n-r$ columns of Q verify the equation $Ax = 0$, and consequently they are elements of M. Observe also that these elements are linearly independent since they are part of a matrix whose determinant is not equal to zero. With this, we have that the last $n-r$ columns of Q are linearly independent elements of M. Next we show that they form a system of generators of M. Take $x \in M$. Hence $Ax = 0$ and this means that $P^{-1}DQ^{-1}x = 0$. Since $\det(P) \neq 0$, this leads to $D(Q^{-1}x) = 0$, which implies that $Q^{-1}x$ has its first r coordinates equal to zero. Thus $Q^{-1}x$ is of the form

$$Q^{-1}x = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ y_{r+1} \\ \vdots \\ y_n \end{pmatrix}$$

and therefore

$$x = Q \begin{pmatrix} 0 \\ \vdots \\ 0 \\ y_{r+1} \\ \vdots \\ y_n \end{pmatrix},$$

which implies that x can be written as a linear combination of the last $n-r$ columns of Q. Summarizing, we get that the last $n-r$ columns of Q are a basis of M.

We now proceed with the general case. Let M be the set of elements of $\mathbb{Z}^n$ satisfying the equations:

$$\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n &\equiv 0 \pmod{b_1},\\
&\vdots\\
a_{k1}x_1 + \cdots + a_{kn}x_n &\equiv 0 \pmod{b_k},\\
a_{(k+1)1}x_1 + \cdots + a_{(k+1)n}x_n &= 0,\\
&\vdots\\
a_{s1}x_1 + \cdots + a_{sn}x_n &= 0.
\end{aligned}$$

We define M' as the set of elements $(x_1, \dots, x_{n+k}) \in \mathbb{Z}^{n+k}$ such that

$$\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n - b_1x_{n+1} &= 0,\\
&\vdots\\
a_{k1}x_1 + \cdots + a_{kn}x_n - b_kx_{n+k} &= 0,\\
a_{(k+1)1}x_1 + \cdots + a_{(k+1)n}x_n &= 0,\\
&\vdots\\
a_{s1}x_1 + \cdots + a_{sn}x_n &= 0.
\end{aligned}$$

Since M' is homogeneous, we can compute a basis $B' = \{m'_1, \dots, m'_r\}$ for it. Let us assume that $m'_i = (m_{i1}, \dots, m_{i(n+k)})$ and take $m_i = (m_{i1}, \dots, m_{in})$. We show next that $B = \{m_1, \dots, m_r\}$ is a basis of M.

- Take $x = (x_1, \dots, x_n) \in M$. For all $i \in \{1, \dots, k\}$, we have that
$$a_{i1}x_1 + \cdots + a_{in}x_n \equiv 0 \pmod{b_i}.$$
Hence there exists $x_{n+i} \in \mathbb{Z}$ such that
$$a_{i1}x_1 + \cdots + a_{in}x_n = b_ix_{n+i}.$$
This implies that $x' = (x_1, \dots, x_n, x_{n+1}, \dots, x_{n+k}) \in M'$. Thus $x' = \sum_{i=1}^r a_im'_i$ for some $a_1, \dots, a_r \in \mathbb{Z}$. Clearly, $x = \sum_{i=1}^r a_im_i$. This implies that B is a system of generators of M.
- Assume that $a_1, \dots, a_r \in \mathbb{Z}$ are such that $\sum_{i=1}^r a_im_i = 0$. In order to show that $a_1 = \cdots = a_r = 0$, since B' is a basis, it suffices to show that $\sum_{i=1} ra_im'_i = 0$. As $\sum_{i=1}^r a_im_i = 0$, we only have to prove that $\sum_{i=1}^r a_im_{i(n+j)} = 0$ for all $j \in \{1, \dots, k\}$. Since $m'_1, \dots, m'_r \in M'$, they all satisfy the j-th equation of M' and for this reason
$$b_jm_{i(n+j)} = a_{j1}m_{i1} + \cdots + a_{jn}m_{in}.$$
This implies that
$$m_{i(n+j)} = (a_{j1}m_{i1} + \cdots + a_{jn}m_{in})/b_j.$$
Using this we get that
$$\sum_{i=1}^r a_im_{i(n+j)} = \sum_{i=1}^r a_i(\sum_{l=1}^n a_{jl}m_{il})/b_j =$$

$$= (\sum_{l=1}^{n} a_{jl}(\sum_{i=1}^{r} a_i m_{il}))/b_j = (\sum_{l=1}^{n} a_{jl}0)/b_j = 0.$$

Therefore the vectors in B are linearly independent.

Remarks

The substitution of fields by rings in vector spaces leads to the theory of modules. Abelian groups are $\mathbb{Z}$-modules and for this reason in many books the structure theorem for finitely generated Abelian groups appears in a more general scope. Usually this theorem is stated for finitely generated modules over a principal ideal domain (see for instance **[58]**, **[27]**, **[10]**), and finitely generated Abelian groups are a particular example of this kind of module. We have avoided the general version of this structure theorem for practical reasons: we shall only make use of this result and all its supporting background over the integers. The contents of this chapter shall be used repeatedly and over in the rest of the book.

Exercises

1. Let $n_1, \dots, n_k \in \mathbb{N} \setminus \{0\}$. Prove that $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ and $A = \{(x_1, \dots, x_k) \in \mathbb{N}^k \mid x_i < n_i \text{ for all } i\}$ have the same number of elements. Show that the set A together with the operation

   $$(x_1, \dots, x_k) \oplus (y_1, \dots, y_k) = ((x_1 + y_1) \pmod{n_1}, \dots, (x_k + y_k) \pmod{n_k})$$

   is a group isomorphic to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.
2. Compute the invariant factors of the matrix

   $$\begin{pmatrix} 2 & -6 & 8 \\ -4 & -6 & -10 \end{pmatrix}.$$

3. Compute a set of defining equations of $\mathbf{G}(\{(2,1,-1),(2,3,-2)\})$.
4. Find a basis of the subgroup M of $\mathbb{Z}^3$ where

   $$M = \left\{ (x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{array}{lcl} x+y & \equiv & 0 \pmod 2 \\ x+y+z & = & 0 \end{array} \right\}.$$

5. Find a basis of $\mathbf{G}(\{(2,4,-2,1),(1,0,-1,1),(2,2,-2,1)\}) \subset \mathbb{Z}^4$.
6. Let H a subgroup of a group G. We define the binary relation on G

   $$a \equiv_H b \text{ if and only if } a - b \in H.$$

   Show that
   (a) $\equiv_H$ is a congruence,
   (b) $G/\equiv_H$ is a group with the operation $[a] + [b] = [a+b]$.
   The group $G/\equiv_H$ is usually denoted as G/H and known as the quotient group of G over H.
7. Let $\varphi : G \to G'$ be a morphism of groups. Prove the following statements.
   (a) $\mathrm{Ker}(\varphi) = \{a \in G \mid \varphi(a) = 0\}$ is a subgroup of G.

(b) $\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\}$ is a subgroup of G'.

(c) The groups $G/\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$ are isomorphic.

This result is known as the First Isomorphism Theorem for Groups.

8. Let M be the subgroup of $\mathbb{Z}^n$ given by the equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &\equiv 0 \pmod{b_1}, \\ &\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n &\equiv 0 \pmod{b_k}, \\ a_{(k+1)1}x_1 + \cdots + a_{(k+1)n}x_n &= 0, \\ &\vdots \\ a_{s1}x_1 + \cdots + a_{sn}x_n &= 0. \end{aligned}$$

Prove that $\mathrm{rank}(M) \geq n - (s-k)$.

9. Let M be a subgroup of $\mathbb{Z}^n$. Show that $\mathbb{Z}^n/M$ is finite if and only if $\mathrm{rank}(M) = n$.
10. Find M and M' subgroups of $\mathbb{Z}^4$ such that M and M' are isomorphic, but so that $\mathbb{Z}^4/M$ and $\mathbb{Z}^4/M'$ are not isomorphic.
11. Prove that $\mathbb{Z}$ has only two bases.
12. Prove that $\mathbb{Z}^2$ has infinitely many bases.
13. Let H be a subgroup of $\mathbb{Z}^n$ and let A be a subgroup of $\mathbb{Z}^n/H$. Show that there exists a subgroup M of $\mathbb{Z}^n$ containing H such that $A = M/H$.
14. Prove that every subgroup of a finitely generated group is finitely generated.
15. Let

$$M_1 = \left\{(x,y,z) \in \mathbb{Z}^3 \mid x+y+z=0\right\},$$

$$M_2 = \left\{(x,y,z,t) \in \mathbb{Z}^4 \mid \begin{array}{c} x+2y-z+t=0 \\ x-y+z-t=0 \end{array}\right\}.$$

Show that M_1 and M_2 are isomorphic.

16. Find a subgroup M of $\mathbb{Z}^n$ and a system of generators of M not containing a basis of M.

CHAPTER 3

Finitely generated cancellative monoids

From the results exposed in Chapter 1 we know that a finitely generated cancellative monoid is isomorphic to a submonoid of a finitely generated group. Using the structure theorem for finitely generated Abelian groups proved in the last chapter, we can ensure that every finitely generated cancellative monoid is a submonoid of $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ for some $d_1, \ldots, d_r, k \in \mathbb{N} \setminus \{0\}$.

Among the finitely generated cancellative monoids we distinguish three classes: those being torsion free, those being reduced and those being finite. The main results proved in this chapter state that

1. every finitely generated cancellative torsion free monoid is isomorphic to a submonoid of $\mathbb{Z}^n$ for some positive integer n,
2. every finitely generated cancellative torsion free reduced monoid is isomorphic to a submonoid of $\mathbb{N}^n$ for some positive integer n,
3. every finite cancellative monoid is a group.

A finitely generated cancellative monoid S is isomorphic to $\mathbb{N}^n / \sim_M$, for some subgroup M of $\mathbb{Z}^n$ (see Theorem 1.2 and Proposition 1.4). The next result tells us that the submonoid of $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ isomorphic to S is the one generated by the "columns" of the equations of M. We will show later that, depending on the properties of S, these equations have special forms which will yield the abovementioned results.

PROPOSITION 3.1. *Let M be a subgroup of $\mathbb{Z}^n$ such that $(x_1, \ldots, x_n) \in M$ if and only if*

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

Then $\mathbb{N}^n / \sim_M$ is isomorphic to the submonoid S of $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ generated by

$$\{([a_{11}]_{d_1}, \ldots, [a_{r1}]_{d_r}, a_{(r+1)1}, \ldots, a_{(r+k)1}), \ldots,$$

$$([a_{1n}]_{d_1}, \ldots, [a_{rn}]_{d_r}, a_{(r+1)n}, \ldots, a_{(r+k)n})\}$$

where $[a]_d$ denotes the equivalence class of a in $\mathbb{Z}_d$.

PROOF. Define the map

$$\varphi : \mathbb{N}^n / \sim_M \to \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k,$$

$$\varphi([(a_1,\dots,a_n)]_{\sim_M}) = ([\sum_{i=1}^n a_i a_{1i}]_{d_1},\dots,[\sum_{i=1}^n a_i a_{ri}]_{d_r}, \sum_{i=1}^n a_i a_{(r+1)i},\dots \sum_{i=1}^n a_i a_{(r+k)i}).$$

We leave to the reader the checking that this map is well defined and that it is a monomorphism of monoids with $\mathrm{Im}(\varphi) = S$. Consequently S is isomorphic to $\mathbb{N}^n / \sim_M$. □

EXAMPLE 3.2. Let $M = \mathbf{G}(\{(2,0,0),(0,1,-1)\}) \subseteq \mathbb{Z}^3$. Let us compute the invariant factors of M.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

And this means that the equations of M are

$$\begin{aligned} y &\equiv 0 \pmod 1, \\ x &\equiv 0 \pmod 2, \\ y+z &= 0. \end{aligned}$$

Since the first one is trivial, we get that $(x,y,z) \in M$ if and only if

$$\begin{aligned} x &\equiv 0 \pmod 2, \\ y+z &= 0. \end{aligned}$$

Therefore $\mathbb{N}^3 / \sim_M$ is isomorphic to the submonoid of $\mathbb{Z}_2 \times \mathbb{Z}$ generated by $\{([1]_2,0),([0]_2,1),([0]_2,1)\}$. ◇

1. Finitely generated cancellative torsion free monoids

A monoid S is **torsion free** if for every $a,b \in S$ and $k \in \mathbb{N} \setminus \{0\}$, the equality $ka = kb$ implies that $a = b$. It is easy to show that the property of being torsion free is preserved under isomorphisms and that a submonoid of a torsion free monoid is again torsion free. Hence, in particular, every submonoid of $\mathbb{Z}^n$ is torsion free. We shall demonstrate that up to isomorphisms, these are all the possible finitely generated cancellative and torsion free monoids. In order to do that, we first have to prove that if a monoid of the form $\mathbb{N}^n / \sim_M$ is torsion free, then M must be homogeneous.

PROPOSITION 3.3. *Let M be a subgroup of $\mathbb{Z}^n$. The following statements are equivalent.*

(i) *M is homogeneous.*
(ii) *$\mathbb{N}^n / \sim_M$ is isomorphic to a submonoid of $\mathbb{Z}^k$ for some positive integer k.*
(iii) *$\mathbb{N}^n / \sim_M$ is torsion free.*

PROOF. *(i) implies (ii)* By definition, the equations of M must be of the form

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0, \end{aligned}$$

and by Proposition 3.1, this implies that $\mathbb{N}^n / \sim_M$ is isomorphic to

$$\langle (a_{11}, \dots, a_{m1}), \dots, (a_{1n}, \dots, a_{mn}) \rangle \subseteq \mathbb{Z}^m.$$

(ii) implies (iii) Since every submonoid of $\mathbb{Z}^n$ is torsion free and this property is preserved under isomorphisms, we get that $\mathbb{N}^n / \sim_M$ is torsion free.

(iii) implies (i) We show that the invariant factors of M are all equal to one, and consequently M is homogeneous. Let $d_1, \dots, d_r$ be the invariant factors of M. Using Theorem 2.12, we know that there exists a basis $\{f_1, \dots, f_r, \dots, f_n\}$ of $\mathbb{Z}^n$ such that $\{d_1 f_1, \dots, d_r f_r\}$ is a basis of M. Assume that there exist $i \in \{1, \dots, r\}$ with $d_i > 1$ and let $f_i = (f_{i1}, \dots, f_{in})$. Take

$$f_i^+ = (\max\{f_{i1}, 0\}, \dots, \max\{f_{in}, 0\}), f_i^- = (\max\{-f_{i1}, 0\}, \dots, \max\{-f_{in}, 0\}).$$

Observe that $f_i = f_i^+ - f_i^-$ and that $f_i^+, f_i^- \in \mathbb{N}^n$. Since $d_i > 1$, we get that $f_i^+ - f_i^- = f_i \notin M$ and therefore $[f_i^+]_{\sim_M} \neq [f_i^-]_{\sim_M}$. However, $d_i f_i = d_i f_i^+ - d_i f_i^- \in M$ which implies that $d_i[f_i^+] = d_i[f_i^-]$ and this is in contradiction with the hypothesis that $\mathbb{N}^n / \sim_M$ is torsion free. □

Using this proposition the abovementioned result for finitely generated cancellative torsion free monoids follows easily.

COROLLARY 3.4. *Let S be a finitely generated monoid. Then S is cancellative and torsion free if and only if it is isomorphic to a submonoid of $\mathbb{Z}^k$ for some positive integer k.*

PROOF. *Necessity.* Since S is finitely generated, it is isomorphic to $\mathbb{N}^n/\sigma$ for some positive integer n and some congruence σ on $\mathbb{N}^n$ (Theorem 1.2). In addition, since S is cancellative, by Proposition 1.4, we know that $\sigma = \sim_{M_\sigma}$. Moreover S is torsion free which by Proposition 3.3 implies that the $\mathbb{N}^n/\sim_{M_\sigma}$ is a submonoid of $\mathbb{Z}^k$ for some positive integer k.

Sufficiency. Trivial. □

EXAMPLE 3.5. Let $M = \mathbf{G}(\{(4,1,-3),(1,-2,1)\}) \subseteq \mathbb{Z}^3$. Computing the invariant factors of M we get that

$$\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 4 & 1 & -3 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 & 5 \\ 0 & -3 & 7 \\ 0 & -4 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Hence the equation of M is $5x+7y+9z=0$, which implies that $\mathbb{N}^3/\sim_M$ is isomorphic to the submonoid of $\mathbb{Z}$ generated by $\{5,7,9\}$. ◇

2. Finitely generated cancellative reduced monoids

Let S be a monoid. The element $a \in S$ is a **unit** if there exists $b \in S$ such that $a+b=0$. The set of units of S is denoted by $\mathrm{U}(S)$. Clearly, $\mathrm{U}(S)$ is a submonoid of S and it is also a group. We say that S is **reduced** if $\mathrm{U}(S) = \{0\}$. As for the property of being torsion free, being reduced is preserved under isomorphisms. It is also clear that every submonoid of a reduced monoid is again reduced. In particular, all submonoids of $\mathbb{N}^n$ for n a positive integer are reduced. Our aim in this section is to prove that every finitely generated cancellative torsion free reduced monoid is isomorphic to a finitely generated submonoid of $\mathbb{N}^n$ for some positive integer n.

The following result is a characterization of the property of being reduced for finitely generated cancellative monoids.

PROPOSITION 3.6. *Let M be a subgroup of $\mathbb{Z}^n$ such that $\{e_1,\dots,e_n\} \cap M = \emptyset$. The monoid $\mathbb{N}^n/\sim_M$ is reduced if and only if $M \cap \mathbb{N}^n = \{0\}$.*

PROOF. *Necessity.* Take $(a_1,\dots,a_n) \in M \cap \mathbb{N}^n$. If $a_i > 0$ for some i, then, since $(a_1,\dots,a_n) \in M$, we have that

$$[(a_1,\dots,a_n)] = [0] = [e_i] + [(a_1,\dots,a_i-1,\dots,a_n)].$$

But $e_i \notin M$, which implies that $[e_i] \neq [0]$, and this is in contradiction with the hypothesis that $\mathbb{N}^n/\sim_M$ is reduced.

Sufficiency. Assume that $\mathbb{N}^n/\sim_M$ is not reduced. Then there exist $[a],[b] \in \mathbb{N}^n/\sim_M \setminus \{[0]\}$ such that $[a+b] = [a]+[b] = [0]$. Since $a,b \in \mathbb{N}^n \setminus \{0\}$, we have that $0 \neq a+b \in M$ which is impossible, since we have assumed that $M \cap \mathbb{N}^n = \{0\}$. □

Therefore, if S is finitely generated and cancellative, then it is of the form $\mathbb{N}^n/\sim_M$. If we want to know whether S is reduced, we only must verify whether $M \cap \mathbb{N}^n = \{0\}$, provided that $M \cap \{e_1,\dots,e_n\} = \emptyset$. In the next chapter we give a procedure to check

this. Though the condition $M \cap \{e_1, \dots, e_n\} = \emptyset$ seems to be an odd one, it has a meaning in terms of the generators of S. The fact that $e_i \in M$ for some i tells us that the generator $[e_i]$ of $\mathbb{N}^n / \sim_M = \langle [e_1], \dots, [e_n] \rangle$ is equal to zero, and therefore we can suppress it. This idea is expressed in the following result, which indicates that the condition $M \cap \{e_1, \dots, e_n\} = \emptyset$ is irrelevant.

PROPOSITION 3.7. *Let M be a subgroup of $\mathbb{Z}^n$ such that $M \cap \{e_1, \dots, e_n\} = \{e_{r+1}, \dots, e_n\}$. Let*

$$M' = \{(x_1, \dots, x_r) \in \mathbb{Z}^r \mid (x_1, \dots, x_r, x_{r+1}, \dots, x_n) \in M \text{ for some } x_{r+1}, \dots, x_n\}.$$

Then

1. *M' is a subgroup of $\mathbb{Z}^r$,*
2. *$\mathbb{N}^n / \sim_M$ is isomorphic to $\mathbb{N}^r / \sim_{M'}$,*
3. *if*
$$M = \mathbf{G}(\{(m_{11}, \dots, m_{1n}), \dots, (m_{k1}, \dots, m_{kn})\}),$$
then
$$M' = \mathbf{G}(\{(m_{11}, \dots, m_{1r}), \dots, (m_{k1}, \dots, m_{kr})\}).$$

PROOF. The proof is easy and is left to the reader. We only wish to point out that the second statement follows when one shows that the map

$$\varphi : \mathbb{N}^n / \sim_M \to \mathbb{N}^r / \sim_{M'}$$
$$\varphi([(a_1, \dots, a_n)]_{\sim_M}) = [(a_1, \dots, a_r)]_{\sim_{M'}},$$

is an isomorphism of monoids. □

In order to illustrate this characterization, we give the following example.

EXAMPLE 3.8. Let

$$M = \mathbf{G}(\{(1,-1,1,1), (0,1,-1,-1), (-1,1,0,-1)\}) \subseteq \mathbb{Z}^4.$$

Computing the invariant factors of M, we get that they are all equal to 1 and that M has a single equation $x_2 + x_4 = 0$. From this equation, we deduce that $M \cap \{e_1, e_2, e_3, e_4\} = \{e_1, e_3\}$. Hence M' is the subgroup of $\mathbb{Z}^2$ generated by $\{(-1,1), (1,-1), (1,-1)\}$. Thus $M' = \mathbf{G}(\{(1,-1)\})$, since $(-1,1) = -(1,-1)$. One can easily check that the defining equation of M' is $x_1 + x_2 = 0$. By Proposition 3.1, we get that $\mathbb{N}^2 / \sim_{M'}$ is isomorphic to the submonoid of $\mathbb{Z}$ generated by $\{1,1\}$ (the columns of the defining equation of M are equal to 1) and therefore it is isomorphic to $\mathbb{N}$. We conclude that $\mathbb{N}^4 / \sim_M$ is isomorphic to $\mathbb{N}$. ◇

We now concentrate on the "shape" of the equations of M when $\mathbb{N}^n / \sim_M$ is reduced. As we shall see, in this case, we can always get an equation all of whose coefficients are greater than zero. This shall be the key result that will enable us to ensure that every finitely generated cancellative torsion free reduced monoid is isomorphic to a finitely generated submonoid of $\mathbb{N}^k$ for some positive integer k.

Recall that the **orthogonal space** $V^\perp$ of a subspace V of $\mathbb{Q}^n$ is the set of vectors $(x_1, \dots, x_n) \in \mathbb{Q}^n$ such that $\sum_{i=1}^n x_i y_i = 0$ for all $(y_1, \dots, y_n) \in V$ and that a nonnegative

element of $\mathbb{Q}^n$ is an element whose coordinates are greater than or equal to zero. Recall also that a strongly positive element of $\mathbb{Q}^n$ (as defined earlier on $\mathbb{Z}^n$) is an element whose coordinates are all greater than zero.

LEMMA 3.9. *Let V be a subspace of $\mathbb{Q}^n$. The space $V^\perp$ has a strongly positive element if and only if the only nonnegative element of V is* 0.

PROOF. Take $(a_1,\dots,a_n) \in V^\perp$ such that $a_i > 0$ for all i and suppose that $(b_1,\dots,b_n)$ is an element in V verifying that $b_i \geq 0$ for all i. Since $\sum_{i=1}^n a_i b_i = 0$, and $a_i b_i \geq 0$ for all i, we get $a_i b_i = 0$ for all i and as $a_i \neq 0$, we conclude that b_i is zero for $1 \leq i \leq n$.

The converse is a consequence of Minkowski-Farkas' lemma which will be shown in the next chapter (Theorem 4.2). □

The meaning of this result in terms of the equations of M is explained in the following result.

PROPOSITION 3.10. *Let M be a subgroup of $\mathbb{Z}^n$ such that $M \cap \mathbb{N}^n = \{0\}$. Then there exists a strongly positive element $(a_1,\dots,a_n) \in \mathbb{N}^n$ such that for every $(x_1,\dots,x_n) \in M$ the equality*

$$a_1x_1 + \cdots + a_nx_n = 0$$

holds.

PROOF. Let V be the subspace of $\mathbb{Q}^n$ spanned by M. Observe that since $M \cap \mathbb{N}^n = \{0\}$, the only nonnegative element of V is 0. Using Lemma 3.9, we get that there exists a strongly positive element $(a_1,\dots,a_n)$ in $V^\perp$, which we can assume to be in $\mathbb{N}^n$ (as we can eliminate the denominators). Hence for every element $(x_1,\dots,x_n) \in M \subset V$, we have that $a_1x_1 + \cdots + a_nx_n = 0$. □

With this last result we have collected the components needed to prove the main result of this section.

THEOREM 3.11 (Grillet). *Let S be a finitely generated monoid. The monoid S is cancellative, torsion free and reduced if and only if it is isomorphic to a submonoid of $\mathbb{N}^k$ for some positive integer k.*

PROOF. *Necessity.* Since S is cancellative, we have that S is of the form $\mathbb{N}^n/\sim_M$ for some subgroup M of $\mathbb{Z}^n$. By Proposition 3.3, we get that M is homogeneous. Using Proposition 3.1, we see that S is isomorphic to the submonoid of $\mathbb{Z}^k$ generated by $\{(a_{11},\dots,a_{k1}),\dots,(a_{1n},\dots,a_{kn})\}$, where

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0, \\ &\vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n &= 0, \end{aligned}$$

are the defining equations of M. Moreover, since S is reduced, by Propositions 3.6 and 3.10 we get that there exists $a_1,\dots,a_n \in \mathbb{N} \setminus \{0\}$ such that if $(x_1,\dots,x_n) \in M$, then

$a_1x_1+\cdots+a_nx_n=0$. Hence $(x_1,\dots,x_n)\in M$ if and only if

$$\begin{aligned} a_{11}x_1+\cdots+a_{1n}x_n &= 0,\\ &\vdots\\ a_{k1}x_1+\cdots+a_{kn}x_n &= 0,\\ a_1x_1+\cdots+a_nx_n &= 0. \end{aligned}$$

This is equivalent to saying that $(x_1,\dots,x_n)\in M$ if and only if

$$\begin{aligned} (a_{11}+ta_1)x_1+\cdots+(a_{1n}+ta_n)x_n &= 0,\\ &\vdots\\ (a_{k1}+ta_1)x_1+\cdots+(a_{kn}+ta_n)x_n &= 0,\\ a_1x_1+\cdots+a_nx_n &= 0, \end{aligned}$$

for all $t\in\mathbb{N}$. Since $a_i>0$, for t large enough we get that for all i,j the element $a_{ij}+ta_j$ is a positive integer. Proposition 3.1 ensures that the monoid $\mathbb{N}^n/\sim_M$, and consequently S, is isomorphic to the submonoid of $\mathbb{Z}^{k+1}$ generated by

$$\{(a_{11}+ta_1,\dots,a_{k1}+ta_1,a_1),\dots,(a_{1n}+ta_n,\dots,a_{kn}+ta_n,a_n)\}.$$

As all the elements $a_{ij}+ta_j$ are positive, this is a submonoid of $\mathbb{N}^{k+1}$.

Sufficiency. Clearly, every submonoid of $\mathbb{N}^k$ is cancellative, reduced and torsion free, and so are the monoids isomorphic to them. □

Finitely generated monoids isomorphic to a submonoid of $\mathbb{N}^k$ are known as **affine semigroups**. Thus Theorem 3.11 can be restated as: a monoid is an affine semigroup if and only if it is finitely generated, cancellative, torsion free and reduced.

EXAMPLE 3.12. Let $M=\mathbf{G}(\{(1,-2,2,-1),(-3,1,1,1)\})\subseteq\mathbb{Z}^4$. We can compute, as usual, its invariant factors and equations getting that

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

Therefore $(x_1,x_2,x_3,x_4)\in M$ if and only if

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

By multiplying the first equation by 2 and adding the result to the second equation, we obtain that $(x_1,x_2,x_3,x_4)\in M$ if and only if

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

Thus $\mathbb{N}^4/\sim_M$ is isomorphic to the submonoid $\langle(1,3),(1,0),(1,2),(1,7)\rangle$ of $\mathbb{N}^2$. ◇

3. Finite cancellative monoids

We finish this chapter with a study of finite cancellative monoids, which are naturally finitely generated and, as we next, they are groups as well.

PROPOSITION 3.13. *Let S be a finite monoid. Then S is a group if and only if S is cancellative.*

PROOF. Clearly, if S is a group, then it is cancellative.

Assume that S is cancellative and take s to be an element in $S\setminus\{0\}$. Since S is finite, the set $\{ns \mid n \in \mathbb{N}\setminus\{0\}\} \subseteq S$ must be finite too. Hence there exists $m,n \in \mathbb{N}\setminus\{0\}$, with $m < n$, such that $ms = ns$. By hypothesis, S is cancellative, and this leads to $(n-m)s = 0$, and since $n-m > 0$, we have that $(n-m-1)s + s = 0$, which means that s has an inverse. This can be done for each $s \in S\setminus\{0\}$. Thus S is a group. □

We know that if S is cancellative, then S is of the form $\mathbb{N}^n/\sim_M$ for some positive integer n and some subgroup M of $\mathbb{Z}^n$. We have shown that the equations of M have special form if S is torsion free and/or reduced. The same stands for the property of being finite.

THEOREM 3.14. *Let M be a subgroup of $\mathbb{Z}^n$. The following statements are equivalent.*

(i) *$\mathbb{N}^n/\sim_M$ is finite.*
(ii) $\operatorname{rank}(M) = n$.
(iii) *M has no homogeneous equations, that is to say, among its defining equations there is no equation of the form $a_1x_1 + \cdots + a_nx_n = 0$.*

PROOF. *(i) implies (ii)* Using the argument employed in the proof of Proposition 3.13, we can obtain $k_1,\dots,k_n \in \mathbb{N}\setminus\{0\}$ such that $k_i[e_i] = 0$ for all i. This means that $k_ie_i \in M$ for all i and this implies that $\operatorname{rank}(M) = n$.

(ii) implies (iii) In this setting, the subspace $V = \mathbf{L}_{\mathbb{Q}}(M)$ coincides with $\mathbb{Q}^n$. If M admits an homogeneous equation, say $a_1x_1 + \cdots + a_nx_n = 0$, then $(a_1,\dots,a_n) \in V^{\perp} = \mathbb{Q}^n = \{0\}$, and therefore $a_i = 0$ for all i.

(iii) implies (i) If we compute the equations of M as shown in Chapter 2, they must be of the form

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \pmod{d_1} \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0 \pmod{d_r}, \end{aligned}$$

with d_i dividing d_{i+1} for all i. Note that this implies that $d_re_i \in M$ for all i, and therefore $d_r[e_i] = [0]$ in $\mathbb{N}^n/\sim_M$. Hence the number of elements of $\mathbb{N}^n/\sim_M$ is less than or equal to $(d_r)^n$, since all elements of $\mathbb{N}^n/\sim_M$ must be of the form $\sum_{i=1}^n a_i[e_i]$, with $a_i \in \{0,\dots,d_r-1\}$. □

As a consequence we obtain the following corollary, whose proof is left to the reader.

COROLLARY 3.15. *Let M be a subgroup of $\mathbb{Z}^n$ with rank n and with invariant factors $d_1, \dots, d_n$.*

1. *$\mathbb{N}^n / \sim_M$ is a finite group.*
2. *M contains a strongly positive element.*
3. *$\mathbb{N}^n / \sim_M$ is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$.*

EXAMPLE 3.16. Computing the invariant factors of the subgroup

$$M = \mathbf{G}(\{(2,-4,2),(-6,2,2),(-2,2,4)\})$$

of rank three, we obtain that $d_1 = d_2 = 2$, and $d_3 = 22$. Hence, $\mathbb{N}^3 / \sim_M$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{22}$. ◇

Remarks

In [**9**] and [**39**] the idea of group of quotients (see the exercises of this chapter) is used to prove that every cancellative monoid can be embedded in a group. In this way, every cancellative monoid is a submonoid of a group. Particularly interesting are the submonoids of $\mathbb{Z}^n$ and $\mathbb{N}^n$ since they represent the submonoids of free groups and free monoids, respectively. In this chapter we have dealt with finitely generated monoids. Some of the results exposed here fail to be true for the non-finitely generated case. Thus for instance Theorem 3.11 is not true for non finitely generated monoids (see exercises below). Theorem 3.11 was proved independently in [**21**] and in [**41**]. The proof presented here follows the line of [**41**].

Exercises

1. Prove that if S is a finite cancellative torsion free monoid, then $S = \{0\}$.
2. Give an example of a reduced cancellative monoid which is not torsion free.
3. Let $M = \mathbf{G}(\{(1,1,-1)\}) \subseteq \mathbb{Z}^3$. Show that $\mathbb{N}^3 / \sim_M$ is an affine semigroup.
4. Let $M = \mathbf{G}(\{(2,1,-1),(2,-1,1)\}) \subseteq \mathbb{Z}^3$. Determine whether $\mathbb{N}^3 / \sim_M$ is cancellative, torsion free and/or reduced.
5. Show that $\mathbb{N}^3 / \sim_M$, with $M = \mathbf{G}(\{(2,-2,0),(4,-2,-2)\})$, is isomorphic to a submonoid of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}$.
6. Let $S \neq \{0\}$ be a finitely generated submonoid of $\mathbb{N}^r$. Prove that $S^* \setminus (S^* + S^*)$ is a system of generators of S, where $S^* = S \setminus \{0\}$, and that, every system of generators of S contains $S^* \setminus (S^* + S^*)$. Thus $S^* \setminus (S^* + S^*)$ is the unique minimal (with respect to inclusion) system of generators of S. Conclude that every affine semigroup has a unique minimal system of generators.
7. Find a finite monoid not being a group.
8. Let S be a cancellative monoid. Define on S the following binary relation:

$$(a,b)\ \tau\ (c,d) \text{ if and only if } a+d = b+c.$$

Prove that

(a) τ is a congruence,

(b) $(S \times S)/\tau$ is a group,

(c) S is isomorphic to a submonoid of $(S \times S)/\tau$.

The group $(S \times S)/\tau$ is known as the **group of quotients** of S. As a consequence of this exercise, every cancellative monoid is isomorphic to a submonoid of a group.

9. Prove that a submonoid of $\mathbb{Z}$ is reduced if and only if it is not a nontrivial subgroup of $\mathbb{Z}$ (equivalently: if a nontrivial submonoid of $\mathbb{Z}$ has a unit, then it is a group). Show that this result does not hold on $\mathbb{Z}^2$.
10. Find a torsion free monoid with two elements.
11. Prove that every subgroup of $\mathbb{Z}^n$ is finitely generated as a monoid.
12. Let S be the monoid
$$\{(x,y) \in \mathbb{Z}^2 \mid x > 0\} \cup \{(0,y) \in \mathbb{Z}^2 \mid y \geq 0\}.$$
Prove that S is cancellative, torsion free and reduced. Show that there exists no $k \in \mathbb{N}$ such that S is isomorphic to a submonoid of $\mathbb{N}^k$.
13. Let S_1 and S_2 be two monoids. Prove that:
    (a) $S_1 \times S_2$ is torsion free if and only if S_1 and S_2 are torsion free.
    (b) $S_1 \times S_2$ is reduced if and only if S_1 and S_2 are reduced.
14. Let S be a monoid. Define on S the following binary relation: $a \,\sigma\, b$ if and only if $ka = kb$ for some $k \in \mathbb{N} \setminus \{0\}$. Prove that:
    (a) σ is a congruence on S,
    (b) S/σ is torsion free.
15. Let S be a monoid and let $\mathrm{U}(S)$ be its group of units. Define on S the following binary relation: $a \,\sigma\, b$ if and only if $a + x = b + y$ for some $x, y \in \mathrm{U}(S)$. Prove that:
    (a) σ is a congruence on S,
    (b) S/σ is reduced.
16. Find a torsion free monoid S and a congruence σ on S such that S/σ is not torsion free.
17. Find a reduced monoid S and a congruence σ on S such that S/σ is not reduced.

CHAPTER 4

Minkowski-Farkas' lemma and its applications to monoids

In Chapter 3, we already mentioned one of the possible applications of Minkowski-Farkas' lemma: if the only nonnegative element in a vector subspace V of $\mathbb{Q}^n$ is the zero element, then $V^{\perp}$ has a strongly positive element. In this chapter, we prove Minkowski-Farkas' lemma and show how to use it to obtain the cited result. In addition, we present a series of algorithms that are used to determine whether a subspace of $\mathbb{Q}^n$ has nontrivial nonnegative elements. We also provide several applications of the algorithms presented which can be resumed in the following list.

1. Check whether a monoid of the form $\mathbb{N}^n / \sim_M$ is a group.
2. Detect whether a monoid of the form $\mathbb{N}^n / \sim_M$ is affine, and if so, determine an element $k \in \mathbb{N} \setminus \{0\}$ and a finitely generated submonoid S of $\mathbb{N}^k$ such that $\mathbb{N}^n / \sim_M$ is isomorphic to it.
3. Compute the group of units of $\mathbb{N}^n / \sim_M$ and a submonoid C of $\mathbb{N}^n / \sim_M$ such that $\mathbb{N}^n / \sim_M = \mathrm{U}(\mathbb{N}^n / \sim_M) + C$ and $\mathrm{U}(\mathbb{N}^n / \sim_M) \cap C = \{0\}$.
4. Determine whether a homogeneous linear system of equations with rational coefficients has a nontrivial solution all of whose coordinates are nonnegative integers.
5. Decide whether the intersection of two finitely generated submonoids of $\mathbb{N}^n$ is not trivial, and if so, find a nonzero element in this intersection.

1. Main result and algorithms

Throughout this chapter for a given $x \in \mathbb{Q}^n$ we shall denote by $x \geq 0$ the fact that x is nonnegative, that is to say, all its coordinates are greater than or equal to zero. We write $x > 0$ when x is strongly positive. Likewise, $x \leq 0$ and $x < 0$ have the corresponding meaning.

THEOREM 4.1 (Minkowski-Farkas' lemma). *Let A and b be $m \times n$ and $m \times 1$ matrices with rational entries, respectively. Let x and y be $n \times 1$ and $1 \times m$ matrices of unknowns, respectively. The following statements are equivalent.*

(i) *The system*

$$\begin{aligned} Ax &= b, \\ x &\geq 0, \end{aligned}$$

has a solution over the rationals.

(ii) *The system*

$$yA \geq 0,$$
$$yb < 0,$$

has no solution over the rationals.

PROOF. *(i) implies (ii)* For every $y \in \mathbb{Q}^n$, we have that $yb = yAx$. If $yA \geq 0$, then $yb \geq 0$, which implies that the system $yA \geq 0, yb < 0$ has no solution over the rationals.

(ii) implies (i) If the system $Ax = b, x \geq 0$ has no solution,

1. either $Ax = b$ has no solution over the rationals
2. or every solution of $Ax = b$ has at least a negative coordinate.

Denote the i-th column of A by A_i. We analyze both cases and show that the system $yA \geq 0, yb < 0$ has a solution over the rationals.

Case 1. If $Ax = b$ has no solution over the rationals, then there is no element $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ such that $\sum_{i=1}^n x_i A_i = b$, which means that b does not belong to the vector subspace V of $\mathbb{Q}^m$ generated by $\{A_1, \ldots, A_n\}$. We can choose an element $y \in V^\perp$ such that $yb \neq 0$, since $b \notin V$. It may happen that $yb < 0$, and for this reason y is a solution of the system $yA = 0$ and $yb < 0$. If $yb > 0$, we only have to take $-y$ instead of y. In any case, the system

$$yA \geq 0$$
$$yb < 0$$

has a solution over the rationals.

Case 2. Assume now that $Ax = b$ has a solution but every solution has at least a negative coordinate. We use induction on the number of columns of A in order to show that the system $yA \geq 0, yb < 0$ has a solution.

For $n = 1$, the hypothesis is that $Ax = xA_1 = b$ has at least one solution whose only coordinate must be less than zero, that is to say $x < 0$. Taking $y = -b$, we obtain $yA = -bA_1 = (-1/x)b^2 \geq 0$ and $yb = -b^2 < 0$ (b^2 denotes the dot product bb).

Suppose that the result is true for $n-1$ columns. If the system of equations $\sum_{i=1}^n x_i A_i = Ax = b$ has no solutions with $x \geq 0$, then the system of equations $\sum_{i=1}^{n-1} x_i A_i = b$ cannot have a solution with all its coordinates greater than or equal to zero. This implies (even if it has no solutions as we have seen in Case 1) that there exists an element y in $\mathbb{Q}^m$ such that $yA_i \geq 0$ for all $1 \leq i \leq n-1$ and $yb < 0$. Note that if $yA_n \geq 0$, then $yA \geq 0$ and $yb < 0$, which concludes the search. However if $yA_n < 0$, then some extra effort is needed. In this case, define

1. $a_0 = -(yb)/(yA_n) < 0$ and $a_i = -(yA_i)/(yA_n) \geq 0$ for all $1 \leq i \leq n-1$,
2. $A'_i = A_i + a_i A_n$ for every $1 \leq i \leq n-1$,
3. $b' = b + a_0 A_n$.

Observe that the system of equations $\sum_{i=1}^{n-1} x'_i A'_i = b'$ is equivalent to

$$\sum_{i=1}^{n-1} x'_i A_i + (\sum_{i=1}^{n-1} a_i x'_i - a_0) A_n = b.$$

Since $a_0 < 0$ and $a_i \geq 0$ for all $1 \leq i \leq n-1$, the fact that $Ax = b$ admits no solution of the form $x \geq 0$ implies that the system $\sum_{i=1}^{n-1} x_i' A_i' = b'$ has no solution with $x_i' \geq 0$ for every $1 \leq i \leq n-1$. Hence using once more the hypothesis of induction, but now for $\sum_{i=1}^{n-1} x_i' A_i' = b'$, we get that there exists $y' \in \mathbb{Q}^m$ such that $y'A_i' \geq 0$ for all $i \in \{1, \ldots, n-1\}$ and $y'b' < 0$. The reader can verify that for $\overline{y} = y' - ((y'A_n)/(yA_n))y$, we have that $\overline{y}A \geq 0$ and $\overline{y}b < 0$. □

Recall that we mentioned in Chapter 3 that Minkowski-Farkas' lemma was required to prove the following result.

THEOREM 4.2. *Let V be a subspace of $\mathbb{Q}^n$ such that its only nonnegative element is the zero element. Then $V^\perp$ has a strongly positive element.*

PROOF. Let $B = \{m_1, \ldots, m_r\}$ be a basis of V with $m_i = (m_{i1}, \ldots, m_{in})$. Let

$$A = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{r1} & m_{r2} & \cdots & m_{rn} \\ 1 & 0 & \cdots & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

We show that the system $yA \geq 0$ and $yb < 0$ has no solution over the rationals. If $y = (y_1, \ldots, y_{r+1})$ is a solution of this system of inequalities, then $y_{r+1} < 0$, since $yb < 0$. Moreover, as $yA \geq 0$, we get

$$(\sum_{i=1}^{r} y_i m_{i1} + y_{r+1}, \sum_{i=1}^{r} y_i m_{i2}, \ldots, \sum_{i=1}^{r} y_i m_{in}) \geq 0$$

which leads to

$$(\sum_{i=1}^{r} y_i m_{i1}, \sum_{i=1}^{r} y_i m_{i2}, \ldots, \sum_{i=1}^{r} y_i m_{in}) \geq (-y_{r+1}, 0, \ldots, 0)$$

and this implies that $\sum_{i=1}^{r} y_i m_i$ has its first coordinate greater than zero and the rest greater than or equal to zero. However this is impossible, since V has no nonnegative elements different from $(0, \ldots, 0)$. Thus Minkowski-Farkas' lemma tells us that the system $Ax = b, x \geq 0$ has a solution with rational coefficients. Let us assume that $a_1 = (a_{11}, \ldots, a_{1n})$ is a solution of this system. Hence $a_1 \geq 0$, $a_1 \in V^\perp$ and $a_{11} = 1$.

We proceed in the same way on the matrix

$$A = \begin{pmatrix} m_{11} & \cdots & m_{1i} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{ri} & \cdots & m_{rn} \\ 0 & \cdots & 1 & \cdots & 0 \end{pmatrix}$$

obtaining an element $a_i = (a_{i1}, \ldots, a_{in})$ such that $a_i \in V^\perp$, $a_{ii} = 1$ and $a_i \geq 0$. Then $a = \sum_{i=1}^{n} a_i$ is a strongly positive element in $V^\perp$. □

We now use the idea involved in the proof of Minkowski-Farkas' lemma in order to give a procedure for finding a nonnegative element of a subspace V of $\mathbb{Q}^n$ whose first coordinate is greater than zero (provided that this element exists). Observe that if $B = \{m_1, \dots, m_r\}$ with $m_i = (m_{i1}, \dots, m_{in})$ is a basis of V, the element $x = (x_1, \dots, x_n)$ belongs to V if and only if there exists $y = (y_1, \dots, y_r) \in \mathbb{Q}^r$ such that $x = \sum_{i=1}^r y_i m_i$. Using matrix notation, this can be expressed as $yA = x$, where

$$A = \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{r1} & \cdots & m_{rn} \end{pmatrix}.$$

Denote by A_i the i-th column of A. Since $x_i = yA_i$, if x is a nonnegative element whose first coordinate if greater than zero, then $yA_i \geq 0$ for all i and $yA_1 > 0$. Hence V contains a nonnegative element whose first coordinate is greater than zero if and only if there exists $y \in \mathbb{Q}^r$ such that $yA_1 > 0$ and $yA_i \geq 0$ for all $i \in \{2, \dots, n\}$. Thus we may focus our attention on finding $y \in \mathbb{Q}^r$ such that $yA_1 > 0$ and $yA_i \geq 0$ for all i. Note that

1. if our problem has no solution for the matrix $(A_1 \dots A_{n-1})$, then it cannot have a solution for A;
2. if our problem has a solution, say z, for $(A_1 \dots A_{n-1})$ and $zA_n \geq 0$, then zA is a nonnegative element of V with its first coordinate greater than zero;
3. if, as in the preceding case, z is a solution for $(A_1 \dots A_{n-1})$ but $zA_n < 0$, take a_i and A'_i, $1 \leq i \leq n-1$, to be as in the proof of Minkowski-Farkas' lemma. We distinguish two subcases (we leave the details to the reader):
   (a) If there exists $z' \in \mathbb{Q}^r$ such that $z'A'_1 > 0$ and $z'A'_i \geq 0$ for all $2 \leq i \leq n-1$, defining $y = z' - ((z'A_n)/(zA_n))z$, we obtain $yA_1 > 0$ and $yA_i \geq 0$ for all $i \in \{2, \dots, n\}$.
   (b) If there is no $z' \in \mathbb{Q}^r$ such that $z'A'_1 > 0$ and $z'A'_i \geq 0$ for all $2 \leq i \leq n-1$, then there is no $y \in \mathbb{Q}^r$ with $yA_1 > 0$ and $yA_i \geq 0$ for $i \in \{2, \dots, n\}$.

This ensures that the following algorithm will produce a nonnegative element x of V whose first coordinate is greater than zero, provided that such an element exists.

ALGORITHM 4.3 (FP). The input of the algorithm is a matrix A whose rows form a basis of a subspace V of $\mathbb{Q}^n$. The output is a nonnegative element in V whose first coordinate is greater than zero. If this element does not exist, then the algorithm returns false.

1. If $n = 1$, take $y = (0, \dots, 0, a_{i1}, 0, \dots, 0)$, where $i = \min\{k \mid a_{k1} \neq 0\}$, and return $x = yA = yA_1$. Observe that if A_1 has all its entries equal to zero, the problem has no solution. Return false.
2. If $n > 1$, solve the problem for the matrix $(A_1 \dots A_{n-1})$. If there is no solution for $(A_1 \dots A_{n-1})$, then there is no solution for A. Otherwise, let z be an element in $\mathbb{Q}^r$ such that $zA_1 > 0$ and $zA_i \geq 0$ for all $i \in \{2, \dots, n-1\}$.
   (a) If $zA_n \geq 0$, then zA is a nonnegative element in V whose first coordinate is greater than zero. Return zA.

(b) If $zA_n < 0$, let $A_i' = A_i - ((zA_i)/(zA_n))A_n$ and solve the problem for $(A_1' \dots A_{n-1}')$.

(i) If there is no solution for $(A_1' \dots A_{n-1}')$, then the original problem has no solution. Return false.

(ii) If z' is a solution for $(A_1' \dots A_{n-1}')$, define $y = z' - ((z'A_n)/(zA_n))z$ and return $x = yA$. ◇

We illustrate this algorithm with an example.

EXAMPLE 4.4. Let

$$V = \mathbf{L}_{\mathbb{Q}}(\{(1,-1,1,1),(0,1,-1,-1),(-1,1,0,-1)\}).$$

Then

$$A = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & -1 \end{pmatrix}.$$

We are looking for a nonnegative element in V such that its first coordinate is greater than zero. This is equivalent to finding $y \in \mathbb{Q}^3$ such that $yA_1 > 0, yA_2 \geq 0, yA_3 \geq 0$ and $yA_4 \geq 0$. Following the algorithm, we must solve the problem for $(A_1A_2A_3)$ and therefore for (A_1A_2) which finally reduces to solving the problem for A_1. Since $a_{11} \neq 0$, we get that $z = (1,0,0)$ verifies that $zA_1 = 1 > 0$. Unfortunately, $zA_2 = -1 < 0$, and for this reason z is not a solution of the problem for (A_1A_2). Hence we must construct

$$A_1' = A_1 - ((zA_1)/(zA_2))A_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

The element $z' = (0,1,0)$ is a solution for A_1'. Thus we must define

$$y = z' - ((z'A_2)/(zA_2))z = (1,1,0).$$

Observe that $yA_1 = 1 > 0$ and $yA_2 = 0 \geq 0$. We check whether this element fits for $(A_1A_2A_3)$. Since $yA_3 = 0 \geq 0$, y is a solution of the problem for the matrix $(A_1A_2A_3)$. Finally, $yA_4 = 0 \geq 0$ and therefore $yA = (1,0,0,0)$ is a nonnegative element of V whose first coordinate is greater than zero. ◇

If we are interested in finding a nonnegative element of V with i-th coordinate greater than zero, then we only have to apply the above described algorithm to the matrix $(A_i\, A_{i+1} \dots A_n\, A_1 \dots A_{i-1})$. For each i, we can find a nonnegative element with its i-th coordinate greater than zero (provided that it exists). If there exists such an element for every i, adding them altogether we obtain a strongly positive element belonging to V. However, if there exists an i such that the Algorithm FP fails to find a nonnegative element with its i-th coordinate positive, then V has no strongly positive elements. Note also that this process can be refined. We start looking for a nonnegative element whose first coordinate is greater than zero. If the result is a strongly positive element, we stop. Otherwise, we look for the first zero among its coordinates and then repeat the algorithm for this position. We add this new element to the preceding one

and repeat the process. We stop when we find a strongly positive element or when Algorithm FP fails to find a nonnegative element with the required coordinate greater than zero. Thus the algorithm could be described as follows.

ALGORITHM 4.5 (SP). The input of the algorithm is a matrix A whose rows form a basis of a subspace V of $\mathbb{Q}^n$. The output is a strongly positive element x belonging to V, provided that this element exists, and false otherwise.

1. Apply Algorithm FP to the matrix A. If the algorithm fails, then return false. Otherwise, if y is the output of FP, let $x = yA$.
2. If all the coordinates of x are greater than zero, then return x. Otherwise, find the first zero coordinate of x. Let i be the position of this coordinate. Apply FP to the matrix $(A_i \dots A_n A_1 \dots A_{i-1})$. If the output of FP is false, then return false. If the output is z, then redefine x as $x + (zA_1, \dots, zA_n)$, and repeat this step. ◇

EXAMPLE 4.6. In Example 4.4, we computed $(1,0,0,0) \in V$. Since the second coordinate is zero, we apply once more the algorithm to $(A_2A_3A_4A_1)$ and get the following.

For A_2, $z = (-1,0,0)$ verifies $zA_2 = 1 > 0$. However, $zA_3 = -1 < 0$ and for this reason z is not a solution for the problem stated for the matrix (A_2A_3). Hence we must compute

$$A_2' = A_2 - ((zA_2)/(zA_3))A_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

and z' such that $z'A_2' > 0$. Taking $z' = (0,0,1)$, we get that $y = z' - ((z'A_3)/(zA_3))z = z' = (0,0,1)$ verifies that $yA_2 = 1 > 0$ and $yA_3 \geq 0$. Unfortunately, $yA_4 = -1 < 0$. We must go one step back,

$$A_2' = A_2 - ((zA_2)/(zA_4))A_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

$$A_3' = A_3 - ((zA_3)/(zA_4))A_4 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}.$$

Since A_2' has all its entries equal to zero, the algorithm fails to find z' such that $z'A_2' > 0$.

Thus there is no nonnegative element in V with its second coordinate greater that zero and this implies that V has no strongly positive elements. ◇

Note that if we do not stop in the preceding algorithm when Algorithm FP returns false, then the resulting element is a positive element of V with the maximum of coordinates greater than zero.

ALGORITHM 4.7 (MCP). The input of the algorithm is a matrix A whose rows form a basis of a subspace V of $\mathbb{Q}^n$. The output is a nonnegative element x belonging to V with the maximum of coordinates greater than zero.

1. Let $x = 0$.
2. For all i apply Algorithm FP to the matrix $(A_i \dots A_n A_1 \dots A_{i-1})$. If the output of FP is false, do nothing. If the output is z, redefine x as $x + (zA_1, \dots, zA_n)$. ◇

Note that in the preceding algorithm, the second step does not have to be repeated for each i. It only has to be executed for each zero coordinate of the element x.

EXAMPLE 4.8. Let us return to Example 4.4. As we already know, for $(A_1A_2A_3A_4)$ we obtain $x = (1,0,0,0)$ and for $(A_2A_3A_4A_1)$, Algorithm FP returns false. We apply FP to $(A_3A_4A_1A_2)$ and get $y = (1,0,1)$. Hence $x = (1,0,0,0) + (0,0,1,0) = (1,0,1,0)$. The output of FP for $(A_4A_1A_2A_3)$ yields false. Therefore the resulting element is $x = (1,0,1,0)$. ◇

2. Applications to monoids

In this section we apply the algorithms appearing in this chapter to cancellative monoids.

2.1. Check whether a monoid of the form $\mathbb{N}^n / \sim_M$ is a group.

Let $M = \mathbf{G}(\{m_1, \dots, m_r\}) \subseteq \mathbb{Z}^n$. We wish to know whether $\mathbb{N}^n / \sim_M$ is a group. By Proposition 1.7, this occurs if and only if M has a strongly positive element. Define the subspace $V = \mathbf{L}_{\mathbb{Q}}(\{m_1, \dots, m_r\})$ of $\mathbb{Q}^n$. It is clear that V has a strongly positive element if and only if M has a strongly positive element. We can use Algorithm SP to determine whether V has a strongly positive element.

2.2. Detect whether a monoid of the form $\mathbb{N}^n / \sim_M$ is affine, and if so, determine an element $k \in \mathbb{N} \setminus \{0\}$ and a finitely generated submonoid S of $\mathbb{N}^k$ such that $\mathbb{N}^n / \sim_M$ is isomorphic to S.

Let M be as before. We want to know whether $\mathbb{N}^n / \sim_M$ is an affine semigroup. For this reason we must determine whether it is cancellative, torsion free and reduced (see Theorem 3.11).

1. Clearly, $\mathbb{N}^n / \sim_M$ is cancellative.
2. We may assume that $M \cap \{e_1, \dots, e_n\} = \emptyset$ (see Proposition 3.7). Compute the invariant factors and defining equations of M. If M is not homogeneous, then $\mathbb{N}^n / \sim_M$ is not torsion free and therefore it cannot be isomorphic to a submonoid of $\mathbb{N}^k$. Otherwise, let

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= 0, \\ &\vdots \\ a_{r1}x_1 + \dots + a_{rn}x_n &= 0, \end{aligned}$$

be the defining equations of M.
3. If $\mathbb{N}^n / \sim_M$ is reduced, then M must admit an equation of the form

$$a_1x_1 + \dots + a_nx_n = 0, \ a_i > 0 \text{ for all } i$$

(see Propositions 3.6 and 3.10). This holds if and only if the subspace

$$V = \mathbf{L}_{\mathbb{Q}}(\{(a_{11},\dots,a_{1n}),\dots,(a_{r1},\dots,a_{rn})\})$$

of $\mathbb{Q}^n$ has a strongly positive element. Apply Algorithm SP to V. If the answer is false, then our semigroup is not affine. Otherwise, let $(a_1,\dots,a_n)$ be a strongly positive element in V. We can eliminate the denominators and assume that $a_i \in \mathbb{N}\setminus\{0\}$ for all i. Multiplying this equation by large enough positive integers and adding it to the rest of the equations, we obtain new equations

$$\begin{aligned} b_{11}x_1+\cdots+b_{1n}x_n &= 0,\\ &\vdots\\ b_{s1}x_1+\cdots+b_{sn}x_n &= 0, \end{aligned}$$

of M such that $b_{ij} \in \mathbb{N}$ for all i,j. The submonoid of $\mathbb{N}^s$ generated by

$$\{(b_{11},\dots,b_{s1}),\dots(b_{1n},\dots,b_{sn})\}$$

is a monoid isomorphic to $\mathbb{N}^n/\sim_M$.

EXAMPLE 4.9. Let

$$M = \mathbf{G}(\{(1,-1,1,-1),(3,2,0,-2),(2,3,-1,-1),(1,4,-2,0)\}).$$

Computing its invariant factors, we obtain $d_1 = d_2 = 1$. The equations of M are

$$\begin{aligned} 2x_1+x_3+3x_4 &= 0,\\ -4x_1+x_2-5x_4 &= 0. \end{aligned}$$

If we add the second equation to the first one multiplied by two, we get that $(x_1,x_2,x_3,x_4) \in M$ if and only if

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

In this case, there is no need to apply Algorithm SP. The monoid $\mathbb{N}^4/\sim_M$ is isomorphic to the submonoid $S = \langle(2,0),(0,1),(1,2),(3,1)\rangle$ of $\mathbb{N}^2$. ◇

EXAMPLE 4.10. Consider the group

$$M = \mathbf{G}(\{(2,-1,-1),(1,1,-3),(1,-2,-1)\}).$$

The invariant factors of M are $d_1 = d_2 = 1$ and $d_3 = 9$. Thus $\mathbb{N}^3/\sim_M$ is not torsion free and therefore it is not an affine semigroup. In this case, the defining equation of M is $x_1 - x_2 + 3x_3 \equiv 0 \pmod 9$ and therefore the monoid $\mathbb{N}^3/\sim_M$ is isomorphic to $\langle[1]_9,[8]_9,[3]_9\rangle = \mathbb{Z}_9$. ◇

EXAMPLE 4.11. Let

$$M = \mathbf{G}(\{(2,-3,1),(-1,1,-4)\}).$$

Its invariant factors are $d_1 = d_2 = 1$ and its defining equation is $11x_1 + 7x_2 - x_3 = 0$. The subspace $V = \mathbf{L}_{\mathbb{Q}}(\{(11,7,-1)\})$ of $\mathbb{Q}^3$ has no positive elements. This means that $\mathbb{N}^3/\sim_M$ is not reduced and therefore it is not an affine semigroup. Note that $\mathbb{N}^3/\sim_M$

is isomorphic to the submonoid of $\mathbb{Z}$ generated by $\{11,7,-1\}$ and therefore $\mathbb{N}^3/\sim_M$ is isomorphic to $\mathbb{Z}$. ◇

2.3. Compute the set of units of $\mathbb{N}^n/\sim_M$ and a submonoid C of $\mathbb{N}^n/\sim_M$ such that $\mathbb{N}^n/\sim_M = \mathrm{U}(\mathbb{N}^n/\sim_M)+C$ and $\mathrm{U}(\mathbb{N}^n/\sim_M)\cap C=\{0\}$.

If $x,y\in S$ and if $x+y\in \mathrm{U}(S)$, then there exists $z\in S$ such that

$$z+(x+y)=(z+x)+y=y+(z+x)=0$$

and for this reason both x and y are units of S. Using this idea it is straightforward to show the following result.

PROPOSITION 4.12. *Let S be a monoid finitely generated by $\{s_1,\dots,s_n\}$ such that $\mathrm{U}(S)\cap\{s_1,\dots,s_n\}=\{s_1,\dots,s_r\}$. Then*

1. $\mathrm{U}(S)=\langle s_1,\dots,s_r\rangle$,
2. *the monoid $\langle s_{r+1},\dots,s_n\rangle$ is reduced,*
3. $S=\langle s_1,\dots,s_r\rangle+\langle s_{r+1},\dots,s_n\rangle$, *with* $\langle s_1,\dots,s_r\rangle\cap\langle s_{r+1},\dots,s_n\rangle=\{0\}$.

The proof is left as an easy exercise for the reader. The submonoid $\mathrm{U}(S)$ is uniquely determined, but this is not so for $\langle s_{r+1},\dots,s_n\rangle$, which depends on the choice of the system of generators of S. Therefore we will refer to this submonoid as a **complement** of $\mathrm{U}(S)$.

For the particular case of monoids of the form $\mathbb{N}^n/\sim_M$ we get the following result.

PROPOSITION 4.13. *Let M be a subgroup of $\mathbb{Z}^n$. Then*

$$\mathrm{U}(\mathbb{N}^n/\sim_M)\cap\{[e_1],\dots,[e_n]\}=\{[e_{i_1}],\dots,[e_{i_r}]\}$$

if and only if

(i) *if $(y_1,\dots,y_n)\in M\cap\mathbb{N}^n$ then $y_i=0$ for all $i\notin\{i_1,\dots,i_r\}$,*
(ii) *there exists $(x_1,\dots,x_n)\in M$ such that $x_i>0$ if $i\in\{i_1,\dots,i_r\}$ and $x_i=0$ otherwise.*

PROOF. *Necessity.* Take $(a_1,\dots,a_n)\in M\cap\mathbb{N}^n$. If $a_i>0$, we have

$$[e_i]+(a_1[e_1]+\cdots+(a_i-1)[e_i]+\cdots+a_n[e_n])=[(a_1,\dots,a_n)]=[0]$$

which implies that $[e_i]\in\mathrm{U}(\mathbb{N}^n/\sim_M)$. This proofs the first condition.

Since $[e_{i_1}],\dots,[e_{ir}]\in\mathrm{U}(\mathbb{N}^n/\sim_M)$, we have that $\sum_{j=1}^r[e_{i_j}]\in\mathrm{U}(\mathbb{N}^n/\sim_M)$. Hence there exists $\sum_{i=1}^n a_i[e_i]\in\mathbb{N}^n/\sim_M$ such that $\sum_{j=1}^r[e_{i_j}]+\sum_{i=1}^n a_i[e_i]=[0]$. The element

$$(x_1,\dots,x_n)=(a_1,\dots,a_{i_1}+1,\dots,a_{i_r}+1,\dots,a_n)$$

fulfills the second condition.

Sufficiency. Let $(x_1,\dots,x_n)\in M$ be such that $x_i>0$ for all $i\in\{i_1,\dots,i_r\}$ and the rest of its coordinates are zero. As before, this leads to $\{[e_{i_1}],\dots,[e_{ir}]\}\subseteq\mathrm{U}(\mathbb{N}^n/\sim_M)$. If $[e_i]$ is a unit, there must exist $[(a_1,\dots,a_n)]\in\mathbb{N}^n/\sim_M$ such that $[e_i]+[(a_1,\dots,a_n)]=[0]$ which means that $(a_1,\dots,a_i+1,\dots,a_n)\in M\cap\mathbb{N}^n$. By the first of our hypothesis, this implies that $i\in\{i_{i1},\dots,i_{ir}\}$. □

With these two results we can compute the group of units of a monoid of the form $\mathbb{N}^n/\sim_M$ and one of its complements. Denote by V the subspace of $\mathbb{Q}^n$ spanned by M. Let x be the element resulting from the application of Algorithm MCP to V.

- If $x = (0,\dots,0)$, the monoid $\mathrm{U}(\mathbb{N}^n/\sim_M) = \{0\}$ and consequently $\mathbb{N}^n/\sim_M$ is reduced.
- If $\{i_1,\dots,i_r\} = \{i \mid x_i \neq 0\}$, then $\mathrm{U}(\mathbb{N}^n/\sim_M) = \langle [e_{i_1}],\dots,[e_{i_r}]\rangle$ and a complement for $\mathrm{U}(\mathbb{N}^n/\sim_M)$ is $\langle \{[e_i] \mid i \notin \{i_1,\dots,i_r\}\}\rangle$.

EXAMPLE 4.14. Let

$$M = \mathbf{G}(\{(1,1,1,-1),(1,2,2,-1)\}).$$

A basis of V is $\{(1,1,1,-1),(1,2,2,-1)\}$. The output of Algorithm MCP applied to V is $(0,1,1,0)$. Thus $\mathrm{U}(\mathbb{N}^4/\sim_M) = \langle [e_2],[e_3]\rangle$ and a complement for $\mathrm{U}(\mathbb{N}^4/\sim_M)$ is $\langle [e_1],[e_4]\rangle$. ◇

It can be shown (see the exercises at the end of this chapter) that the monoid appearing in Example 4.14 is isomorphic to the direct product of two monoids, one isomorphic to its group of units and the other to a complement of it. In general, this need not be the case.

PROPOSITION 4.15. *Let S be a finitely generated monoid such that C is a complement of* $\mathrm{U}(S)$. *Let τ be congruence defined on* $\mathrm{U}(S)\times C$ *as*

$$(x,y)\ \tau\ (x',y') \text{ if and only if } x+y = x'+y'.$$

Then S is isomorphic to $(\mathrm{U}(S)\times C)/\tau$.

PROOF. The proof follows easily by defining $\varphi : \mathrm{U}(S)\times C \to S$ as $\varphi(x,y) = x+y$ and taking $\tau = \mathrm{Ker}(\varphi)$. □

2.4. Determine whether a homogeneous linear system of equations with rational coefficients has a nontrivial solution with all its coordinates being nonnegative integers.

Assume we are given a system of homogeneous linear equations with rational coefficients as follows

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0,\\ &\vdots\\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0. \end{aligned}$$

We wish to know whether there exists an element $(x_1,\dots,x_n) \in \mathbb{N}^n \setminus \{0\}$ which is a solution of this system of equations. This is equivalent to knowing whether there exists a nonnegative element different from zero belonging to the subspace of $\mathbb{Q}^n$ defined by the given equations. Hence we only have to compute a basis B for V using linear algebra methods and then apply Algorithm MCP to the matrix whose rows are the elements of B. The output of the algorithm is the element we are looking for, after eliminating the denominators.

EXAMPLE 4.16. Let us see if the system of equations

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

has a nonnegative integer solution. The subspace V defined by this set of equations is $V = \mathbf{L}_{\mathbb{Q}}(\{(1,1,1,-1),(1,2,2,-1)\})$. We already know that the output of Algorithm MCP applied to V is $(0,1,1,0)$ and therefore this is a nontrivial solution of the given system of equations having all its coordinates greater than or equal to zero. ◇

If the given system has a nonnegative integer solution, the method just described will find one. However, we still do not have tools to compute the monoid of all nonnegative integer solutions of a system of homogeneous linear equations. This will be accomplished in a forthcoming chapter.

2.5. Decide whether the intersection of two finitely generated submonoids of $\mathbb{N}^n$ is not trivial, and if so, find an element in this intersection.

Let S_1 and S_2 be two submonoids of $\mathbb{N}^n$ generated by $\{a_1,\dots,a_r\}$ and $\{b_1,\dots,b_s\}$, respectively. We want to know whether S_1 and S_2 have nontrivial elements in common. If $a_i = (a_{i1},\dots,a_{in})$ and $b_j = (b_{j1},\dots,b_{jn})$ for all $1 \le i \le r$ and $1 \le j \le s$, then this problem is equivalent to determining whether the system of equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{r1}x_r - b_{11}x_{r+1} - \cdots - b_{s1}x_{r+s} &= 0, \\ &\vdots \\ a_{1n}x_1 + \cdots + a_{rn}x_r - b_{1n}x_{r+1} - \cdots - b_{sn}x_{r+s} &= 0, \end{aligned}$$

has a nonnegative integer solution with at least two nonzero coordinates, one ranging from 1 to r and the other from 1 to s.

Thus we can use the Algorithm MCP to check whether $S_1 \cap S_2 \neq \{0\}$ and if so determine an element in this intersection.

Remarks

Minkowski-Farkas' lemma is a classical result appearing frequently in the books of linear programming. The applications given in this chapter for finitely generated monoids, together with some other applications appear in **[18]**, **[41]** and **[46]**.

Exercises

1. Let

$$M = \left\{ (x_1,x_2,x_3,x_4) \in \mathbb{Z}^4 \;\middle|\; \begin{aligned} 2x_1 - x_2 - 2x_3 + 2x_4 &= 0 \\ x_1 - 2x_2 - 3x_3 + x_4 &= 0 \\ x_1 - x_2 - x_3 - x_4 &= 0 \end{aligned} \right\}.$$

Show that $\mathbb{N}^4 / \sim_M$ is an affine semigroup.

2. Compute a nonnegative solution with the greatest possible number of positive coordinates of the system of equations

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

3. Let

$$M = \mathbf{G}(\{(1,2,-1,3),(2,1,-2,4),(3,2,-3,1)\}).$$

Prove that $\mathrm{U}(\mathbb{N}^4/\sim_M)$ is the submonoid of $\mathbb{N}^4/\sim_M$ generated by $\{[e_2],[e_4]\}$.

4. Let M be a subgroup of $\mathbb{Z}^n$ and

$$M' = \{(x_1,\dots,x_r) \in \mathbb{Z}^r \mid (x_1,\dots,x_r,0,\dots,0) \in M\}.$$

Prove the following assertions:
   (a) M' is a subgroup of $\mathbb{Z}^r$,
   (b) $\mathbb{N}^r/\sim_{M'}$ is isomorphic to the submonoid of $\mathbb{N}^n/\sim_M$ generated by $\{[e_1],\dots,[e_r]\}$.

5. Let M be a subgroup of $\mathbb{Z}^n$ such that $\mathrm{U}(\mathbb{N}^n/\sim_M) = \langle [e_1],\dots,[e_r]\rangle$. Define

$$M_1 = \{(x_1,\dots,x_r) \in \mathbb{Z}^r \mid (x_1,\dots,x_r,0,\dots,0) \in M\},$$

$$M_2 = \{(x_1,\dots,x_{n-r}) \in \mathbb{Z}^{n-r} \mid (0,\dots,0,x_1,\dots,x_{n-r}) \in M\}.$$

Prove the following assertions:
   (a) $\mathrm{U}(\mathbb{N}^n/\sim_M)$ is isomorphic to $\mathbb{N}^r/\sim_{M_1}$,
   (b) there exists a complement for $\mathrm{U}(\mathbb{N}^n/\sim_M)$ isomorphic to $\mathbb{N}^{n-r}/\sim_{M_2}$.

   Apply this result to the monoid occurring in the Example 4.14 and show that its group of units is isomorphic to $\mathbb{Z}$ and its complement is isomorphic to $\mathbb{N}$.

6. Let G be a group and H_1, H_2 be two of its subgroups such that $G = H_1 + H_2$ and $H_1 \cap H_2 = \{0\}$. Prove that G is isomorphic to $H_1 \times H_2$.

7. Let S be the submonoid of $\mathbb{N}^2$ generated by

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

Let S_1 and S_2 be the submonoids of S generated by $\{(1,0)\}$ and $\{(1,1),(1,2)\}$, respectively. Prove that $S = S_1 + S_2$, $S_1 \cap S_2 = \{(0,0)\}$ and that S is not isomorphic to $S_1 \times S_2$.

8. Let S be the submonoid of $\mathbb{Z}^2$ spanned by

$$\{(1,-1),(4,1),(-2,-3),(-1,-2)\}.$$

Prove that S is reduced.

9. Prove that the submonoids of $\mathbb{N}^3$ generated by

$$\{(1,2,3),(1,1,2)\} \text{ and } \{(2,4,7),(3,1,2)\},$$

respectively, have nontrivial intersection.

10. Let S be a monoid and let $\mathrm{U}(S)$ be its group of units. Prove that:
   (a) $(S \setminus \mathrm{U}(S)) \cup \{0\}$ is a reduced monoid,
   (b) $\mathbb{Z} \times \mathbb{N}$ is a finitely generated monoid,
   (c) the monoid $(\mathbb{Z} \times \mathbb{N} \setminus \mathrm{U}(\mathbb{Z} \times \mathbb{N})) \cup \{(0,0)\}$ is not finitely generated.

CHAPTER 5

Finitely generated monoids are finitely presented

Let S be a finitely generated monoid. Theorem 1.2 states that there exists a congruence σ on $\mathbb{N}^n$ such that S is isomorphic to $\mathbb{N}^n/\sigma$, where n is the number of elements in a system of generators for S. We can think of $\mathbb{N}^n/\sigma$ as a monoid generated by n elements whose elements are related according to a set of rules which are the elements of σ. We shall show that these infinitely many rules can be derived from a finite set of rules. In order to prove this assertion, we need to study some results and concepts related to orderings on $\mathbb{N}^n$. At the end of this chapter we describe the special case n equal to one (cyclic monoids).

1. Linear admissible orders

The binary relation $\Delta(X) = \{(x,x) \mid x \in X\}$ is known as the **diagonal** of X. For a binary relation ω on a set X its **inverse relation** is the set

$$\omega^{-1} = \{(b,a) \mid (a,b) \in \omega\}.$$

In this setting ω is **antisymmetric** whenever $\omega \cap \omega^{-1} \subseteq \Delta(X)$. The binary relation ω is a **partial order** on X if it is reflexive, transitive and antisymmetric. A partial order ω on X is **linear** if for any $a, b \in X$ either $a\ \omega\ b$ or $b\ \omega\ a$. Note that a partial order ω is a linear order if and only if $\omega \cup \omega^{-1} = X \times X$.

Given a subset Y of X and ω a partial order on X, we say that y is a **ω-minimal** element of Y (or simply minimal when there is no possible misunderstanding) if there is no other element $z \in Y \setminus \{y\}$ such that $z\ \omega\ y$. The set of minimal elements of Y is denoted by $\mathrm{Minimals}_\omega(Y)$. If there exists an element y in Y such that $y\ \omega\ z$ for all $z \in Y$, then y is called a **ω-minimum** of Y and it is denoted by $\min_\omega(Y)$. Dually, we can define the concept of **ω-maximal** element, the set $\mathrm{Maximals}_\omega(Y)$ of maximal elements of Y and if it exists, the **ω-maximum** of Y. If ω is a linear order on X, then for every pair of elements $x, y \in X$, there exist the ω-minimum of $\{x,y\}$. Observe that the same holds for any finite subset of X.

The partial order ω is a **well order** on X if every nonempty subset of X has a ω-minimum. If ω is a well order, then every set formed by two elements a and b has a minimum, and this means that either $a\ \omega\ b$ or $b\ \omega\ a$. Therefore well orders are linear. The converse is not true. Take $X = \mathbb{Z}$ and $\omega = \leq$; then ω is linear but it is not a well order. Note that $\leq$ is a well order on $\mathbb{N}$.

Let $\{X_1,\dots,X_n\}$ be a family of sets and let ω_i be a partial order on X_i for each $i \in \{1,\dots,n\}$. On $X_1 \times \cdots \times X_n$ we define the following binary relation

$$(x_1,\dots,x_n)\ \omega\ (y_1,\dots,y_n) \text{ if and only if } x_i\ \omega_i\ y_i \text{ for all } i \in \{1,\dots,n\}.$$

The reader can check that ω is a partial order. This partial order is called the **product order** of $\omega_1,\dots,\omega_n$. For the particular case $X_i = \mathbb{N}$ and $\omega_i = \leq$ for all i, we obtain the usual partial order on $\mathbb{N}^n$, which we also denote by $\leq$. Thus $(x_1,\dots,x_n) \leq (y_1,\dots,y_n)$ if and only if $x_i \leq y_i$ for all $i \in \{1,\dots,n\}$. We write $x < y$ whenever $x \leq y$ and $x \neq y$. Note that the product order on $\mathbb{N}^n$ is not linear for $n \geq 2$. One can find subsets of $\mathbb{N}^n, n \geq 2$ with more than one minimal element. The question is, how many minimal elements can a subset of $\mathbb{N}^n$ have?

THEOREM 5.1 (Dickson's Lemma). *Let N be a nonempty subset of $\mathbb{N}^n$. The set $M = \text{Minimals}_{\leq}(N)$ has finitely many elements.*

PROOF. We use induction on n. For $n = 1$, the result follows easily from the fact that $\leq$ is a well order on $\mathbb{N}$.

Assume that the statement is true for $n-1$ and let us show it for n. Choose an element $(a_1,\dots,a_n) \in M$. For each $1 \leq i \leq n$ and each $0 \leq j \leq a_i$ define

$$M_{ij} = \{(x_1,\dots,x_n) \in M \mid x_i = j\}$$

and

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

Observe that $\text{Minimals}_{\leq}(M) = M$ and for this reason $\text{Minimals}_{\leq}(M_{ij}) = M_{ij}$ and $\text{Minimals}_{\leq}(B_{ij}) = B_{ij}$. By the hypothesis of induction B_{ij} must be finite. Hence, M_{ij} is finite as well. Since there are finitely many sets M_{ij}, the set $\bigcup M_{ij}$ is again finite and nonempty. Hence it is enough to show that $M \subseteq \bigcup M_{ij}$. Take $(x_1,\dots,x_n)$ to be an element in M. There exists $i \in \{1,\dots,n\}$ such that $x_i \leq a_i$ (if this were not the case, $(a_1,\dots,a_n) < (x_1,\dots,x_n)$ and this is impossible, since $(x_1,\dots,x_n)$ is a minimal element of N). Hence $(x_1,\dots,x_n) \in M_{ix_i}$. □

The set of elements that are less than or equal to a fixed element in $\mathbb{N}^n$ with respect to the usual partial order is finite as the following result shows.

PROPOSITION 5.2. *Let $x \in \mathbb{N}^n$. The set*

$$A = \{y \in \mathbb{N}^n \mid y \leq x\}$$

is finite and nonempty.

PROOF. Clearly $0 \in A$, which means that A is not empty. By the definition of $\leq$, if $x = (x_1,\dots,x_n)$, then the cardinality of A is exactly $\prod_{i=1}^{n}(x_i+1)$. □

From this result we can derive some useful conclusions.

COROLLARY 5.3. *Let $\{x_i \mid i \in I\}$, $I \subseteq \mathbb{N}$, be a nonempty subset of $\mathbb{N}^n$ such that $x_j < x_i$ whenever $i < j$. Then I has finitely many elements.*

PROOF. By Proposition 5.2, the set

$$A = \{y \mid y \leq x_1\}$$

is finite and nonempty. Observe that $\{x_i \mid i \in I\} \subseteq A$. Thus I is finite, since all elements in $\{x_i \mid i \in I\}$ are different. □

If σ is a well order and $\{x_i \mid i \in I\}, I \subseteq \mathbb{N}$, is a sequence such that $x_j \,\sigma\, x_i$ and $x_j \neq x_i$ whenever $i < j$, the existence of a minimum of $\{x_i \mid i \in I\}$ forces I to be finite.

COROLLARY 5.4. *Let N be a nonempty subset of $\mathbb{N}^n$ and let $M = \text{Minimals}_{\leq}(N)$. Then for every $x \in N$ there exists $m \in M$ such that $m \leq x$.*

PROOF. Let $x \in N$. If $x \in M$, the proof is trivial since $x \leq x$. Thus assume that $x \in N \setminus M$. By the definition of minimal element, there exists an element $x_1 \in N$ such that $x_1 < x$. If $x_1 \in M$, then we conclude the proof. Otherwise, there exists $x_2 \in N$ such that $x_2 < x_1 < x$. By Corollary 5.3, this process stops, and it does so when there is an i such that $x_i \in M$. Since by transitivity $x_i < x$, we obtain the desired result. □

A partial order ω on $\mathbb{N}^n$ is **admissible** if the following conditions hold:

1. $0 \,\omega\, a$ for all $a \in \mathbb{N}^n$,
2. for every $a, b \in \mathbb{N}^n$, if $a \,\omega\, b$, then $a + c \,\omega\, b + c$ for all $c \in \mathbb{N}^n$.

If ω is admissible and $a \leq b$, then $b - a \in \mathbb{N}^n$ and for this reason $0 \,\omega\, (b - a)$. Adding a to both sides we obtain $a \,\omega\, b$. This implies that ω contains the partial order $\leq$. In other words, admissible orders are "extensions" of the product order on $\mathbb{N}^n$. From now on, we denote by $\preceq$ a linear admissible order on $\mathbb{N}^n$. The fact $a \preceq b$ and $a \neq b$ is denoted by $a \prec b$.

LEMMA 5.5. *Let $\preceq$ be a linear admissible order on $\mathbb{N}^n$ and let $a, b, c \in \mathbb{N}^n$ such that $a - c, b - c \in \mathbb{N}^n$ and $a \prec b$. Then $a - c \prec b - c$.*

PROOF. Since $\preceq$ is linear, $a - c \preceq b - c$ or $b - c \preceq a - c$. In the latter case, adding c to both sides, we obtain $b \preceq a$ which is in contradiction with $a \prec b$. Thus $a - c \preceq b - c$ and $a - c \neq b - c$, since $a \neq b$. □

LEMMA 5.6. *Let $\preceq$ be a linear admissible order on $\mathbb{N}^n$, let N be a nonempty subset of $\mathbb{N}^n$ and let $M = \text{Minimals}_{\leq}(N)$. Then $\min_{\preceq}(M) = \min_{\preceq}(N)$.*

PROOF. Since M is finite (Dickson's lemma) and $\preceq$ is linear, there exists $m = \min_{\preceq}(M)$. Take $x \in N$. By Corollary 5.4, there exists $y \in M$ such that $y \leq x$. Since $\preceq$ is admissible, $y \preceq x$. Hence $m \preceq y \preceq x$ and therefore $m \preceq x$. This proves that m is the $\preceq$-minimum of N. □

As a direct consequence of this statement we have the following consequence.

COROLLARY 5.7. *Every linear admissible order on $\mathbb{N}^n$ is a well order.*

2. Rédei's theorem

In this section we prove Rédei's theorem, which states that every finitely generated monoid is finitely presented. Although we have not defined the concept of presentation, the underlying idea is that every congruence on $\mathbb{N}^n$ can be "determined" by a finite set of its elements.

Let $\preceq$ be a linear admissible order and σ a congruence on $\mathbb{N}^n$. We define the map

$$\mu_{\preceq} : \mathbb{N}^n/\sigma \to \mathbb{N}^n,\ \mu_{\preceq}([x]_\sigma) = \min_{\preceq}([x]_\sigma).$$

Note that this map is well defined since $[x]_\sigma$ is a nonempty subset of $\mathbb{N}^n$ and by Corollary 5.7, $\preceq$ is a well order. The map $\mu_{\preceq}$ is called the **minimum function** associated to σ. As we did in the preceding chapters, if there is no possible misunderstanding, we shall write $[x]$ instead of $[x]_\sigma$. We do the same for $\mu_{\preceq}$ and write μ instead.

The next three results characterize the elements of $\mathrm{Im}(\mu)$. We shall see that this set plays an important role in the proof of Rédei's theorem.

LEMMA 5.8. *Let σ be a congruence on $\mathbb{N}^n$ and μ its minimum function. If $\mu([x]) - e_i \in \mathbb{N}^n$ for some $1 \le i \le n$, then $\mu([x]) - e_i = \mu([\mu([x]) - e_i])$.*

PROOF. Since $\mu([x]) - e_i \in [\mu([x]) - e_i]$, we have $\mu([\mu([x]) - e_i]) \preceq \mu([x]) - e_i$. Moreover,

$$(\mu([\mu([x]) - e_i]))\ \sigma\ (\mu([x] - e_i))$$

and since σ is a congruence,

$$(\mu([\mu([x]) - e_i]) + e_i)\ \sigma\ (\mu([x])).$$

Hence $(\mu([\mu([x]) - e_i]) + e_i)\ \sigma\, x$ which leads to $\mu([\mu([x]) - e_i]) + e_i \in [x]$. By the definition of μ, we have

$$\mu([x]) \preceq \mu([\mu([x]) - e_i]) + e_i.$$

By hypothesis $\mu([x]) - e_i \in \mathbb{N}^n$, which implies

$$\mu([x]) - e_i \preceq \mu([\mu([x]) - e_i]).$$

Therefore

$$\mu([x]) - e_i = \mu([\mu([x]) - e_i]).$$

□

LEMMA 5.9. *Let σ be a congruence on $\mathbb{N}^n$ and μ its minimum function. Let $b \in \mathrm{Im}(\mu)$ be such that $b - e_i \in \mathbb{N}^n$. Then $b - e_i \in \mathrm{Im}(\mu)$.*

PROOF. Since $b \in \mathrm{Im}(\mu)$, we have $\mu([b]) = b$. Applying Lemma 5.8, we obtain that

$$b - e_i = \mu([\mu([b]) - e_i]) = \mu([b - e_i]),$$

whence $b - e_i \in \mathrm{Im}(\mu)$. □

Given a cancellative monoid S and $a \in S$, we define the **Apéry set** of a in S as the set

$$\mathrm{Ap}(S,a) = \{x \in S \mid x - a \notin S\}.$$

We denote by $\mathrm{Ap}(S,a_1,\dots,a_r)$ the set $\bigcap_{i=1}^{r} \mathrm{Ap}(S,a_i)$. The assertion $x-a \notin S$ means that there is no $b \in S$ such that $x = a+b$. If there exists $b \in S$ such that $x = a+b$, then it is unique, since S is cancellative and therefore it makes sense to denote it by $x-a$.

PROPOSITION 5.10. *Let σ be a congruence on $\mathbb{N}^n$ and μ its minimum function with $\preceq$ a linear admissible order on $\mathbb{N}^n$. Let*

$$A = \{a_1,\dots,a_r\} = \mathrm{Minimals}_{\preceq}(\mathbb{N}^n \setminus \mathrm{Im}(\mu)).$$

Then

$$\mathrm{Im}(\mu) = \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_r).$$

PROOF. Take $b \in \mathrm{Im}(\mu)$. If $b - a_i \in \mathbb{N}^n$ for some $1 \le i \le n$, there exists $c \in \mathbb{N}^n$ such that $b = a_i + c$. Applying Lemma 5.9 on $b = a_i + c$ as many times as required, we obtain that $a_i \in \mathrm{Im}(\mu)$. But this is in contradiction with the hypothesis $a_i \in \mathbb{N}^n \setminus \mathrm{Im}(\mu)$. Thus $b - a_i \notin \mathbb{N}^n$ for all i and this implies that $b \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_r)$.

For the opposite inclusion, observe that if $b \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_r)$, then there exists no $a_i \in A$ such that $a_i \le b$. By Corollary 5.4, this implies that $b \notin \mathbb{N}^n \setminus \mathrm{Im}(\mu)$. □

Let ρ be a subset of $\mathbb{N}^n \times \mathbb{N}^n$. The **congruence generated** by ρ, denoted by $\langle\rho\rangle$, is the least (with respect to inclusion) congruence on $\mathbb{N}^n$ containing ρ. The next result shows that $\langle\rho\rangle$ always exists.

PROPOSITION 5.11. *Let ρ be a subset of $\mathbb{N}^n \times \mathbb{N}^n$. Define*

$$\rho_0 = \rho \cup \rho^{-1} \cup \Delta(\mathbb{N}^n),\ \rho_1 = \{(v+u, w+u) \mid (v,w) \in \rho_0, u \in \mathbb{N}^n\}.$$

Then $\langle\rho\rangle$ is the set of pairs $(v,w) \in \mathbb{N}^n \times \mathbb{N}^n$ such that there exist $k \in \mathbb{N}$ and $v_0,\dots,v_k \in \mathbb{N}^n$ with $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in \rho_1$ for all $0 \le i \le k-1$.

PROOF. We first show that $\langle\rho\rangle$ constructed in this way is a congruence.

1. Since $\Delta(\mathbb{N}^n) \subseteq \langle\rho\rangle$, the binary relation $\langle\rho\rangle$ is reflexive.
2. If $(v,w) \in \langle\rho\rangle$, there must exist $k \in \mathbb{N}$ and $v_0,\dots,v_k \in \mathbb{N}^n$ such that $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in \rho_1$ for all $0 \le i \le k-1$. Since $(v_i, v_{i+1}) \in \rho_1$ implies that $(v_{i+1}, v_i) \in \rho_1$, defining $w_i = v_{k-i}$ for every $0 \le i \le k$, we obtain that $(w,v) \in \langle\rho\rangle$. Hence $\langle\rho\rangle$ is symmetric.
3. If (u,v) and (v,w) are in $\langle\rho\rangle$, then there exists $k,l \in \mathbb{N}$ and $v_0,\dots,v_k,w_0,\dots,w_l \in \mathbb{N}^n$ such that $v_0 = u$, $v_k = w_0 = v$, $w_l = w$ and $(v_i, v_{i+1}), (w_j, w_{j+1}) \in \rho_1$ for all suitable i, j. Concatenating the sequences $\{v_i\}_i$ and $\{w_j\}_j$ we obtain $(u,w) \in \langle\rho\rangle$. Thus $\langle\rho\rangle$ is transitive.
4. Finally, let $(v,w) \in \langle\rho\rangle$ and $u \in \mathbb{N}^n$. There exists $k \in \mathbb{N}$ and $v_0,\dots,v_k \in \mathbb{N}^n$ such that $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in \rho_1$ for all $0 \le i \le k-1$. Defining $w_i = v_i + u$ for all $0 \le i \le k$ we have $(w_i, w_{i+1}) \in \rho_1$ and thus $(v+u, w+u) \in \langle\rho\rangle$.

It is clear that every congruence containing ρ must contain $\langle\rho\rangle$ and this means that $\langle\rho\rangle$ is the least congruence on $\mathbb{N}^n$ which contains ρ. $\square$

A congruence σ is **generated** by ρ if $\sigma = \langle\rho\rangle$. In this setting, we also say that ρ is a **system of generators** of σ. A congruence σ is **finitely generated** if there exists a finite set of generators of σ. A **presentation** of a finitely generated monoid S is a subset ρ of $\mathbb{N}^n \times \mathbb{N}^n$, for some nonnegative integer n, such that S is isomorphic to $\mathbb{N}^n/\langle\rho\rangle$. If the set ρ is finite, we say that S is **finitely presented**.

THEOREM 5.12 (Rédei). *Every finitely generated monoid is finitely presented.*

PROOF. Let S be a finitely generated monoid. Theorem 1.2 states that there exists a congruence on $\mathbb{N}^n$ such that S is isomorphic to $\mathbb{N}^n/\sigma$. Hence it is enough to show that every congruence on $\mathbb{N}^n$ is finitely generated.

Let σ be a congruence on $\mathbb{N}^n$ and let μ be its minimum function (with respect to a linear admissible order $\preceq$). Let

$$\{a_1,\dots,a_r\} = \mathrm{Minimals}_{\preceq}(\mathbb{N}^n \setminus \mathrm{Im}(\mu))$$

and $b_i = \mu([a_i])$ for all $1 \le i \le r$. We show that $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ is a system of generators of σ. Since $\rho \subseteq \sigma$, it is clear that $\langle\rho\rangle \subseteq \sigma$.

For the opposite inclusion take $(x,y) \in \sigma$. Note that if $x \in \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_r) = \mathrm{Im}(\mu)$, then $\mu([x]) = x$. Otherwise, there exists $i \in \{1,\dots,r\}$ such that $x - a_i \in \mathbb{N}^n$. Since $(a_i,b_i) \in \rho_0$,

$$(a_i + (x-a_i), b_i + (x-a_i)) = (x, x-a_i+b_i) \in \rho_1.$$

In addition, $b_i \prec a_i$ and this implies that $x_1 = x - a_i + b_i \prec x$. If $x_1 \in \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_r)$, then $x_1 = \mu([x])$. Otherwise, take $j \in \{1,\dots,r\}$ such that $x_1 - a_j \in \mathbb{N}^n$. As before, defining $x_2 = x_1 - a_j + b_j$ we obtain $(x_2,x_1) \in \rho_1$ and for this reason $x_2 \in [x]$. Observe that since $\preceq$ is a well order, after a finite number of steps, we obtain an element $x_k \in \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_r) = \mathrm{Im}(\mu)$ such that $x_k \in [x]$ and consequently $x_k = \mu([x])$. This method enables us to obtain $\mu([x])$ once we know $a_1,\dots,a_r$ and $b_1,\dots,b_r$. Furthermore, since $(x_i,x_{i+1}) \in \rho_1$, we obtain that $(x,\mu([x])) \in \langle\rho\rangle$. Note also that $x\sigma y$ if and only if $\mu([x]) = \mu([y])$. By transitivity, we conclude that $(x,y) \in \langle\rho\rangle$. $\square$

3. The word problem for monoids

By virtue of Theorem 1.2, every finitely generated monoid is isomorphic to a quotient of $\mathbb{N}^n$ over a congruence σ on $\mathbb{N}^n$ for some positive integer n. Rédei's theorem states that σ is fully determined by a finite set ρ of elements of $\mathbb{N}^n \times \mathbb{N}^n$. Therefore giving a finitely generated monoid is equivalent, up to isomorphisms, to giving a finite subset ρ of $\mathbb{N}^n \times \mathbb{N}^n$ for some positive integer n. From a theoretical point of view, $\sigma = \langle\rho\rangle$ is fully determined by ρ and consequently so is $\mathbb{N}^n/\sigma$. However, in practice, the construction of $\langle\rho\rangle$ given in Proposition 5.11 does not provide an effective method to decide whether $(a,b) \in \rho$ and for this reason we do not have a method for deciding

whether two elements are in the same σ-class. The problem of determining whether $(a,b) \in \langle \rho \rangle$, for a given finite set ρ, is known as the **word problem for monoids**.

If we look carefully at the system of generators ρ of σ given in the proof of Rédei's theorem, we deduce that this system of generators is "special", since it enables us to solve the word problem. In the next chapter we shall give a procedure for finding, from a given presentation of a monoid, a new presentation that solves the word problem for this monoid.

4. Cyclic monoids

We end this chapter with a study of **cyclic** monoids, the monoids generated by one element.

PROPOSITION 5.13. *Let S be a cyclic monoid. Then S is either isomorphic to $\mathbb{N}$ or to $\mathbb{N}/\langle (a,b) \rangle$ for some $(a,b) \in \mathbb{N} \times \mathbb{N}$.*

PROOF. Since S is cyclic, it is generated by a single element, say s. By Theorem 1.2, S is isomorphic to $\mathbb{N}/\sigma$ for some congruence σ on $\mathbb{N}$. Note that the least possible congruence on $\mathbb{N}$ is $\Delta(\mathbb{N})$ and that this congruence is generated by the empty set. If $\sigma \neq \Delta(\mathbb{N})$, then we can take

$$a = \min\{x \in \mathbb{N} \setminus \{0\} \mid xs = ys \text{ with } y < x\}.$$

Assume that $b < a$ verifies that $as = bs$. Take $x, y \in \mathbb{N}$ to be such that $xs = ys$, that is to say $x \,\sigma\, y$. We shall use induction on $x+y$ to prove that $(x,y) \in \langle \{(a,b)\} \rangle$. If $x+y = 0$, then both x and y are zero and clearly $(0,0) \in \langle \{(a,b)\} \rangle$. Assume that $(x,y) \in \langle \{(a,b)\} \rangle$ for all $(x,y) \in \sigma$ satisfying $x+y < n$. We must show that whenever $x \,\sigma\, y$ and $x+y = n$, $(x,y) \in \langle \{(a,b)\} \rangle$. Without loss of generality suppose that $x > y$. Then $a \leq x$ and there exists $z \in \mathbb{N}$ such that $x = a+z$. Hence

$$ys = xs = (a+z)s = as + zs = bs + zs = (b+z)s.$$

In addition, $b+z+y < x+y$ and by the induction hypothesis, $(b+z,y) \in \langle \{(a,b)\} \rangle$. Since $(a+z, b+z) \in \langle \{(a,b)\} \rangle$ and $a+z = x$, we have $(x, b+z) \in \langle \{(a,b)\} \rangle$ and therefore $(x,y) \in \langle \{(a,b)\} \rangle$.

We have shown that either $\sigma = \Delta(\mathbb{N}) = \langle \emptyset \rangle$ or $\sigma = \langle \{(a,b)\} \rangle$. □

Denote by $\mathbb{N}_{(a,b)}$ the monoid $\mathbb{N}/\langle \{(a,b)\} \rangle$. From the proof of Proposition 5.13 we have that if $[x] \in \mathbb{N}/\langle \{(a,b)\} \rangle$ and $x = a+z$ for some $z \in \mathbb{N}$, then $[x] = [b+z]$. Again, if $b+z = a+z_1$ for some $z_1 \in \mathbb{N}$, we repeat the reasoning and get that $[x] = [b+z_1]$. This process ends when $x < a$ and consequently

$$\mathbb{N}_{(a,b)} = \{[0], \ldots, [a-1]\}.$$

Note that if μ is the minimum function associated to $\langle (a,b) \rangle$, then

$$\mu([x]) = \begin{cases} x & if x < a, \\ b + ((x-b) \pmod{a-b}) & otherwise. \end{cases}$$

Remarks

Linear admissible orders play a fundamental role in Computer Algebra. Gröbner bases are tightly related with linear admissible orders. The reader interested in learning more about these topics should consult [**4**].

Rédei was the first to prove that every finitely generated (commutative) monoid is finitely presented. Its demonstration appears in [**39**]. In the literature there are other proofs of Rédei's theorem. Grillet gives in [**22**] and [**23**] a different approach to the problem, though the shortest proof of Rédei's theorem is due to Freyd ([**15**]). This chapter follows the line introduced in [**42**].

If S is a monoid and K a field, then we can construct the **semigroup ring** $K[S] = \bigoplus_{s\in S} Ky^s$, where addition is performed componentwise and multiplication follows the rule $y^s y^{s'} = y^{s+s'}$ (for a detailed description of $K[S]$, please refer to [**19**]). If S is generated by

$$\{n_1, \dots, n_p\},$$

then we know that S is isomorphic to $\mathbb{N}^p/\sigma$, where σ is the kernel congruence of the monoid morphism

$$\varphi : \mathbb{N}^p \to S,\ \varphi(a_1, \dots, a_p) = \sum_{i=1}^{p} a_i n_i.$$

Associated to φ we define the ring morphism

$$\psi : K[x_1, \dots, x_p] \to K[S],\ \psi(x_i) = y^{n_i}.$$

The kernel of ψ is usually denoted by I_S (note that $K[x_1, \dots, x_p]/I_S$ is isomorphic to $K[S]$). From the papers by Herzog ([**24**]) and Preston ([**37**]), the set

$$\{(a_1, b_1), \dots, (a_t, b_t)\}$$

is a system of generators of σ (and therefore a presentation of S) if and only if the set

$$\{X^{a_1} - X^{b_1}, \dots, X^{a_t} - X^{b_t}\}$$

is a system of generators of I_S, where X^c denotes $x_1^{c_1} \cdots x_p^{c_p}$ for $c = (c_1, \dots, c_p) \in \mathbb{N}^p$. In this way, Rédei's theorem turns out to be an easy consequence of Hilbert basis theorem.

The concept of Apéry set appears for the first time in [**1**] and it is sometimes referred to as Apéry basis. It has special importance in the characterization of minimal presentations of numerical semigroups (see [**44**]), and in the characterization of certain properties of simplicial affine semigroups (see [**49**]).

Exercises

1. Let $\preceq_{lex}$ be the binary relation on $\mathbb{N}^n$ defined by the rule $a \preceq_{lex} b$ if and only if the first nonzero coordinate of $a - b$ is negative. Prove that $\preceq_{lex}$ is a linear admissible order on $\mathbb{N}^n$. This order is called the **lexicographical** order on $\mathbb{N}^n$.

2. Let $\preceq_{rlex}$ be the binary relation on $\mathbb{N}^n$ defined by the rule $a \preceq_{rlex} b$ if and only if the last nonzero coordinate of $a-b$ is negative. Prove that $\preceq_{rlex}$ is a linear admissible order on $\mathbb{N}^n$. This order is called the **reverse lexicographical** order on $\mathbb{N}^n$.
3. Let $\preceq_{tdeg}$ be the binary relation on $\mathbb{N}^n$ defined as follows:

$$(a_1,\dots,a_n) \preceq_{tdeg} (b_1,\dots,b_n) \text{ if and only if } \sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i, \text{ or}$$

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i \text{ and } (a_1,\dots,a_n) \preceq_{lex} (b_1,\dots,b_n).$$

Show that $\preceq_{tdeg}$ is a linear admissible order on $\mathbb{N}^n$. The order $\preceq_{tdeg}$ is known as **total degree** order on $\mathbb{N}^n$.
4. Let $f : \mathbb{N}^n \to \mathbb{N}$ be a map. Define the binary relation $\leq_f$ on $\mathbb{N}^n$ as follows: $a \leq_f b$ if and only if $f(a) \leq f(b)$.
   (a) Which property must f fulfill so that $\preceq_f$ becomes a linear admissible order?
   (b) Take $p_1,\dots,p_n$ to be the first n prime numbers in $\mathbb{N}$. Show that if

$$f(a_1,\dots,a_n) = p_1^{a_1} \cdots p_n^{a_n},$$

   then $\preceq_f$ is a linear admissible order. For this particular definition of f, the linear admissible order $\preceq_f$ is known as **prime** order on $\mathbb{N}^n$ and it is denoted by $\preceq_p$.
5. Let $\rho = \{((2,1),(1,1)),((3,0),(2,0))\}$. Show that $((6,2),(4,2)) \in \langle\rho\rangle$.
6. Let $\rho = \{((3,2),(2,1))\}$. Prove that $\mathbb{N}^2/\langle\rho\rangle$ is neither cancellative nor torsion free but it is reduced.
7. Show that

$$\{[b],[b+1],\dots,[a-1]\} \subseteq \mathbb{N}_{(a,b)}$$

is a group isomorphic to $\mathbb{Z}_{a-b}$.
8. Find a torsion free monoid which is not cancellative.
9. Let M be a subgroup of $\mathbb{Z}^n$. Prove that:
   (a) $S = M \cap \mathbb{N}^n$ is a monoid,
   (b) the set $\text{Minimals}_{\leq}(S \setminus \{0\})$ is a system of generators of S,
   (c) S is an affine semigroup.
10. Prove that the intersection of two finitely generated submonoids of $\mathbb{Z}^n$ is again a finitely generated submonoid of $\mathbb{Z}^n$.
11. Show that $\mathbb{N}_{(a,b)}$ is a group if and only if $b = 0$.
12. Prove that two cyclic groups with the same cardinality are isomorphic.
13. Find two cyclic monoids with the same cardinality not being isomorphic.
14. Prove that every subgroup of a cyclic group is cyclic.
15. Find a submonoid of a cyclic monoid which is not cyclic.
16. For every $n \in \mathbb{N}$ find a reduced monoid with n elements.
17. Find a non admissible well order on $\mathbb{N}$.

18. Let S be a monoid and let

$$\{\sigma_i \mid i \in I\}$$

be a family of congruences on S. Prove that:

(a) $\bigcap_{i \in I} \sigma_i$ is a congruence;

(b) given $\rho \subseteq S \times S$, there exists the least congruence on S containing ρ.

CHAPTER 6

The word problem for monoids

In this chapter we introduce the concept of a canonical system of generators of a congruence. One of its main features is that it provides a method for determining when a pair of elements belongs to a congruence and consequently it is used to solve the word problem for finitely generated monoids. We present an algorithm based on critical pair completion for computing canonical systems of generators from any system of generators of a congruence. Since canonical systems of generators are unique for a fixed linear admissible order, we are able to decide whether two subsets of $\mathbb{N}^n \times \mathbb{N}^n$ generate the same congruence. As another application of canonical systems of generators, we give a procedure for computing the group of units of a finitely generated monoid given by a presentation.

1. Reduced systems of generators of a congruence

Let $\preceq$ be a linear admissible order on $\mathbb{N}^n$. A subset $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ of $\mathbb{N}^n \times \mathbb{N}^n$ is **reduced** with respect to $\preceq$ if

1. $b_i \prec a_i$,
2. $a_i \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_{i-1},a_{i+1},\dots,a_r)$,
3. $b_i \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_r)$,

for every $1 \le i \le n$. (Recall that the set $\mathrm{Ap}(\mathbb{N}^n, a)$ is the Apéry set of a in S and was defined in Chapter 5.)

The following result is straightforward to prove.

PROPOSITION 6.1. *Let $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ be a subset of $\mathbb{N}^n \times \mathbb{N}^n$.*

1. *Take ρ' to be the set obtained from ρ by suppressing the elements (a_i,b_i) such that $a_i = b_i$.*
2. *Let ρ'' be the set obtained from ρ by replacing the elements (a_i,b_i) satisfying that $a_i \prec b_i$ by (b_i,a_i).*
3. *Assume that $a_i - a_j \in \mathbb{N}^n$ for some $i \neq j$. Let ρ''' be the set obtained from ρ by replacing the element (a_i,b_i) by $(a_i - a_j + b_j, b_i)$.*
4. *Assume that $b_i - a_j \in \mathbb{N}^n$ for some i,j. Let ρ^{iv} be the set obtained from ρ by replacing the element (a_i,b_i) by $(a_i, b_i - a_j + b_j)$.*

Then $\langle\rho\rangle = \langle\rho'\rangle = \langle\rho''\rangle = \langle\rho'''\rangle = \langle\rho^{iv}\rangle$.

When applying the different reductions described in Proposition 6.1, the cardinality of the resulting set does not increase and, eventually, the coordinates of the pairs

appearing in this new set are less than or equal to the original ones (with respect to $\preceq$). This implies that after a finite set of transformations there will be no reduction applicable to the resulting set. When this occurs, the set is reduced and it generates the same congruence on $\mathbb{N}^n$ generated by the original set. This procedure is described in the following algorithm.

ALGORITHM 6.2 (Reduce). The input is a subset $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ of $\mathbb{N}^n \times \mathbb{N}^n$. The output is a reduced set ρ' such that $\langle\rho'\rangle = \langle\rho\rangle$.

1. Construct ρ' from ρ in the following way:
   (a) eliminate the elements (a_i,b_i) such that $a_i = b_i$,
   (b) replace the elements (a_i,b_i) such that $a_i \prec b_i$ by (b_i,a_i).
2. Let $\rho' = \{(a_1,b_1),\dots,(a_k,b_k)\}$. If there exists $1 \le i \ne j \le k$ such that $a_i \notin \mathrm{Ap}(\mathbb{N}^n,a_j)$, then replace in ρ' the element (a_i,b_i) by $(a_i - a_j + b_j, b_i)$. Set $\rho = \rho'$ and go to Step 1.
3. If there exists $1 \le i,j \le k$ such that $b_i \notin \mathrm{Ap}(\mathbb{N}^n,a_j)$, then in ρ' replace the element (a_i,b_i) by $(a_i, b_i - a_j + b_j)$. Set $\rho = \rho'$ and go to Step 1.
4. Return ρ'. ◇

EXAMPLE 6.3. Let

$$\rho = \{((2,0,0),(1,1,1)),((0,2,0),(1,1,0)),((0,2,1),(1,1,0))\}$$

and let $\preceq$ be $\preceq_{tdeg}$ (see the exercises at the end of Chapter 5 for the definition of $\preceq_{tdeg}$). The transformations of ρ are

$$\begin{aligned}
&\{((2,0,0),(1,1,1)),((0,2,0),(1,1,0)),((0,2,1),(1,1,0))\} \to \\
&\to \{((1,1,1),(2,0,0)),((1,1,0),(0,2,0)),((0,2,1),(1,1,0))\} \to \\
&\to \{((0,2,1),(2,0,0)),((1,1,0),(0,2,0)),((0,2,1),(1,1,0))\} \to \\
&\to \{((1,1,0),(2,0,0)),((1,1,0),(0,2,0)),((0,2,1),(1,1,0))\} \to \\
&\to \{((2,0,0),(1,1,0)),((1,1,0),(0,2,0)),((0,2,1),(1,1,0))\} \to \\
&\to \{((2,0,0),(0,2,0)),((1,1,0),(0,2,0)),((0,2,1),(1,1,0))\} \to \\
&\to \{((2,0,0),(0,2,0)),((1,1,0),(0,2,0)),((0,2,1),(0,2,0))\}
\end{aligned}$$

and this set is reduced. ◇

Let $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ be a reduced subset of $\mathbb{N}^n \times \mathbb{N}^n$. We define the map $\mathrm{NF}_\rho : \mathbb{N}^n \to \mathbb{N}^n$ recurrently by

1. if $x \in \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_r)$, then $\mathrm{NF}_\rho(x) = x$,
2. if $x \in \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_i)$ and $x \notin \mathrm{Ap}(\mathbb{N}^n,a_{i+1})$, then $\mathrm{NF}_\rho(x) = \mathrm{NF}_\rho(x - a_{i+1} + b_{i+1})$.

Since $b_{i+1} \prec a_{i+1}$, we obtain that $x - a_{i+1} + b_{i+1} \prec x$. After a finite number of steps the computation of the output of NF_ρ reduces to the first condition. Thus NF_ρ is a well defined map, called the **normal form** associated to ρ. When there is no danger of misunderstanding, we shall write NF instead of NF_ρ.

If $\mathrm{NF}(a) = \mathrm{NF}(b)$, then $(a,b) \in \langle\rho\rangle$ ($(a_i,b_i) \in \rho$ and $x - a_i \in \mathbb{N}^n$ implies that $(a_i + x - a_i, b_i + x - a_i) = (x, x - a_i + b_i) \in \langle\rho\rangle$). Unfortunately, the converse is not true.

EXAMPLE 6.4. Let

$$\rho = \{((2,1),(1,0)),((1,2),(1,0))\}$$

which is reduced with respect to $\preceq_{lex}$, and let σ be the congruence generated by ρ. Then

$$(2,0) = ((1,0)+(1,0))\ \sigma\ ((1,2)+(1,0)) = (2,2) =$$
$$= (2,2) = ((2,1)+(0,1))\ \sigma\ ((1,0)+(0,1)) = (1,1),$$

but $\mathrm{NF}((1,1)) = (1,1) \neq (2,0) = \mathrm{NF}((2,0))$. ◇

This means that NF does not solve the word problem for $\mathbb{N}^n/\langle\rho\rangle$. In the next section, we show that if we want NF to solve the word problem for $\mathbb{N}^n/\langle\rho\rangle$, then we must impose stronger conditions on ρ.

2. Canonical systems of generators of a congruence

Let σ be a congruence on $\mathbb{N}^n$ and μ its associated function minimum with respect to a fixed linear admissible order $\preceq$ (see Chapter 5). A finite reduced subset ρ of $\mathbb{N}^n \times \mathbb{N}^n$ is a **canonical system of generators** of σ with respect to $\preceq$ if

1. $\langle\rho\rangle = \sigma$,
2. for all $x \in \mathbb{N}^n$, we have that $\mathrm{NF}_\rho(x) = \mu([x])$.

Recall that $x\ \sigma\ y$ if and only if $\mu([x]) = \mu([y])$. Hence if ρ is a canonical system of generators of σ, then $x\ \sigma\ y$ if and only if $\mathrm{NF}(x) = \mathrm{NF}(y)$. Thus once we know a canonical system of generators of σ, we can solve the word problem for $\mathbb{N}^n/\sigma$. A natural question arises: is it possible to find a canonical system for an arbitrary congruence on $\mathbb{N}^n$? And if so, how can it be constructed from a system of generators? The following sequence of technical results lead to a solution to both problems.

LEMMA 6.5. *Let $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ be a reduced subset of $\mathbb{N}^n \times \mathbb{N}^n$. Assume that there exists $t \in \mathbb{N}^n$ satisfying that $\mathrm{NF}(a_i+s) = \mathrm{NF}(b_i+s)$ for all $1 \le i \le r$ and for all $s \in \mathbb{N}^n$ such that $a_i+s \prec t$. Then for all $a,b \in \mathbb{N}^n$ satisfying $a+b \prec t$, we have $\mathrm{NF}(a+b) = \mathrm{NF}(\mathrm{NF}(a)+b)$.*

PROOF. Since $\preceq$ is a well order, we can use induction on t. If $t = 0$, the result follows trivially. Assume that the lemma is true for values less than t and let us show it for t.

1. If $a \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_r)$, then $\mathrm{NF}(a) = a$. Hence $\mathrm{NF}(a+b) = \mathrm{NF}(\mathrm{NF}(a)+b)$.
2. If $a \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_i)$ and $a \notin \mathrm{Ap}(\mathbb{N}^n, a_{i+1})$, then $a = a_{i+1}+s$ for some $s \in \mathbb{N}^n$. Hence

$$\mathrm{NF}(a) = \mathrm{NF}(a - a_{i+1} + b_{i+1}) = \mathrm{NF}(b_{i+1}+s).$$

Thus

$$\mathrm{NF}(\mathrm{NF}(a)+b) = \mathrm{NF}(\mathrm{NF}(b_{i+1}+s)+b).$$

In addition, $b_{i+1}+s+b \prec a_{i+1}+s+b = a+b \prec t$. Applying the hypothesis of induction we obtain

$$\mathrm{NF}(b_{i+1}+s+b) = \mathrm{NF}(\mathrm{NF}(b_{i+1}+s)+b).$$

Therefore

$$\mathrm{NF}(\mathrm{NF}(a)+b) = \mathrm{NF}(\mathrm{NF}(b_{i+1}+s)+b) = \mathrm{NF}(b_{i+1}+s+b)$$

and by hypothesis, this means that $\mathrm{NF}(a_{i+1}+s+b) = \mathrm{NF}(a+b)$.

In both cases we have that $\mathrm{NF}(a+b) = \mathrm{NF}(\mathrm{NF}(a)+b)$. □

Let $(x_1,\dots,x_n),(y_1,\dots,y_n) \in \mathbb{N}^n$. Define

$$(x_1,\dots,x_n) \vee (y_1,\dots,y_n) = (\max(\{x_1,y_1\}),\dots,\max(\{x_n,y_n\})).$$

LEMMA 6.6. *Let* $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ *be a reduced subset of* $\mathbb{N}^n \times \mathbb{N}^n$ *and let* $s_{ij}, s_{ji} \in \mathbb{N}^n$ *be elements such that*

$$a_i \vee a_j = a_i + s_{ij} = a_j + s_{ji} \text{ for all } i,j \in \{1,\dots,r\}, i \neq j.$$

Assume that $\mathrm{NF}(b_i+s_{ij}) = \mathrm{NF}(b_j+s_{ji})$ *for all* $i,j \in \{1,\dots,r\}$, $i \neq j$. *Then* $\mathrm{NF}(a_i+s) = \mathrm{NF}(b_i+s)$ *for all* $s \in \mathbb{N}^n$.

PROOF. It suffices to show that for all $t \in \mathbb{N}^n$ we have that $a_i+s \preceq t$ implies that $\mathrm{NF}(a_i+s) = \mathrm{NF}(b_i+s)$. We show this by induction on t. If $t=0$, the result is trivial. Assume that the result is true for the elements less than t and let us prove it for t.

1. If $a_i+s \in \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_{i-1})$, then

$$\mathrm{NF}(a_i+s) = \mathrm{NF}(a_i+s-a_i+b_i) = \mathrm{NF}(b_i+s).$$

2. If $a_i+s \notin \mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_{i-1})$, then let j be the least index such that $a_i+s \notin \mathrm{Ap}(\mathbb{N}^n, a_j)$. Hence $a_i+s = a_j+s'$ for some $s' \in \mathbb{N}^n$. Since j is the minimum verifying this condition, we have that $\mathrm{NF}(a_i+s) = \mathrm{NF}(a_j+s') = \mathrm{NF}(b_j+s')$. Moreover, $a_i+s = a_j+s'$ implies the existence of $c \in \mathbb{N}^n$ such that $s = s_{ij}+c$ and $s' = s_{ji}+c$.

   Our induction hypothesis implies the hypothesis of Lemma 6.5. Hence

$$\mathrm{NF}((b_i+s_{ij})+c) = \mathrm{NF}(\mathrm{NF}(b_i+s_{ij})+c)$$

   and

$$\mathrm{NF}((b_j+s_{ji})+c) = \mathrm{NF}(\mathrm{NF}(b_j+s_{ji})+c),$$

   since

$$(b_i+s_{ij})+c = b_i+s \prec a_i+s \preceq t$$

   and

$$(b_j+s_{ji})+c = b_j+s' \prec a_j+s' = a_i+s \preceq t.$$

   The assumption $\mathrm{NF}(b_i+s_{ij}) = \mathrm{NF}(b_j+s_{ji})$ leads to

$$\begin{aligned}\mathrm{NF}(b_i+s) &= \mathrm{NF}(b_i+s_{ij}+c) = \mathrm{NF}(\mathrm{NF}(b_i+s_{ij})+c) = \\ &= \mathrm{NF}(\mathrm{NF}(b_j+s_{ji})+c) = \mathrm{NF}(b_j+s_{ji}+c) = \\ &= \mathrm{NF}(b_j+s') = \mathrm{NF}(a_j+s') = \mathrm{NF}(a_i+s).\end{aligned}$$

□

THEOREM 6.7. *Let σ be a congruence on $\mathbb{N}^n$ and let $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ be a reduced system of generators of σ with respect to a fixed linear admissible order $\preceq$. The following statements are equivalent.*

(i) *ρ is a canonical system of generators of σ.*
(ii) *For all $i,j \in \{1,\dots,r\}$ we have that $\mathrm{NF}(b_i+s_{ij}) = \mathrm{NF}(b_j+s_{ji})$, where $s_{ij} = (a_i \vee a_j) - a_i$.*
(iii) *For all $a,b \in \mathbb{N}^n$ we have that $\mathrm{NF}(a+b) = \mathrm{NF}(\mathrm{NF}(a)+b)$.*
(iv) *For every $a,b \in \mathbb{N}^n$ if $a \,\sigma\, b$, then $\mathrm{NF}(a) = \mathrm{NF}(b)$.*

PROOF. *(i) implies (ii)* By the definition of a canonical system of generators, for all $x \in \mathbb{N}^n$ we have $\mathrm{NF}(x) = \mu([x])$, where μ denotes the function minimum associated to σ with respect to $\preceq$. Since $a_i+s_{ij} = a_j+s_{ji}$, we obtain $(b_i+s_{ij}) \,\sigma\, (b_j+s_{ji})$ and for this reason $\mu([b_i+s_{ij}]) = \mu([b_j+s_{ji}])$. Therefore $\mathrm{NF}(b_i+s_{ij}) = \mathrm{NF}(b_j+s_{ji})$.

(ii) implies (iii) This implication is a direct consequence of Lemmas 6.5 and 6.6.

(iii) implies (iv) If $a \,\sigma\, b$, then by Proposition 5.11 there exist $v_0,\dots,v_k$ such that $a = v_0$, $b = v_k$ and $(v_i,v_{i+1}) \in \rho_1$ for all $i \in \{0,\dots,k-1\}$. Thus it suffices to prove that $\mathrm{NF}(v_i) = \mathrm{NF}(v_{i+1})$ for all i. Since $(v_i,v_{i+1}) \in \rho_1$, the pair (v_i,v_{i+1}) is of the form $(u+s,v+s)$ with $(u,v) \in \rho \cup \rho^{-1} \cup \Delta(\mathbb{N}^n)$ and $s \in \mathbb{N}^n$.

1. If $(u,v) \in \rho$, then there exists $1 \le j \le n$ such that $(u,v) = (a_j,b_j)$. Hence
$$\mathrm{NF}(u) = \mathrm{NF}(a_j) = b_j = \mathrm{NF}(b_j) = \mathrm{NF}(v).$$
2. If $(u,v) \in \rho^{-1}$, then there exists $1 \le j \le n$ such that $(u,v) = (b_j,a_j)$. Thus
$$\mathrm{NF}(u) = \mathrm{NF}(b_j) = b_j = \mathrm{NF}(a_j) = \mathrm{NF}(v).$$
3. If $(u,v) \in \Delta(\mathbb{N}^n)$, then $u = v$ and $\mathrm{NF}(u) = \mathrm{NF}(v)$.

In any case, $\mathrm{NF}(u) = \mathrm{NF}(v)$ and therefore
$$\mathrm{NF}(v_i) = \mathrm{NF}(u+s) = \mathrm{NF}(\mathrm{NF}(u)+s) = \mathrm{NF}(\mathrm{NF}(v)+s) = \mathrm{NF}(v+s) = \mathrm{NF}(v_{i+1}).$$

(iv) implies (i) Take $x \in \mathbb{N}^n$. Since $x \,\sigma\, \mu([x])$, we obtain $\mathrm{NF}(x) = \mathrm{NF}(\mu([x]))$. In addition, $\mu([x]) \in \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_r)$ and consequently $\mathrm{NF}(\mu([x])) = \mu([x])$. Thus $\mathrm{NF}(x) = \mu([x])$ for all $x \in \mathbb{N}^n$ and this implies that ρ is a canonical system of generators of σ. □

This result motivates the following algorithm.

ALGORITHM 6.8 (CPC). The input is a system of generators of σ. The output is a canonical system of generators of σ.

1. Let ρ' be the result of applying Algorithm Reduce to ρ. Set $\rho = \rho'$.
2. Compute s_{ij} for all $(a_i,b_i),(a_j,b_j) \in \rho$, $i \neq j$.
3. If there exist i,j such that $\mathrm{NF}(b_i+s_{ij}) \neq \mathrm{NF}(b_j+s_{ji})$, then add to ρ' the pair $(\mathrm{NF}(b_i+s_{ij}),\mathrm{NF}(b_j+s_{ji}))$ (if $\mathrm{NF}(b_i+s_{ij}) \prec \mathrm{NF}(b_j+s_{ji})$, we add $(\mathrm{NF}(b_j+s_{ji}),\mathrm{NF}(b_i+s_{ij}))$ instead). Go to Step 1.
4. Return ρ. ◇

It is clear that when the algorithm stops, the resulting set is a canonical system of generators of some congruence. We must show that

1. the resulting set is a system of generators of σ,
2. the algorithm stops after a finite number of steps.

When we apply Algorithm Reduce to ρ, the resulting set ρ' is again a system of generators of σ. Hence the congruence may only become larger when we add elements of the form $(\mathrm{NF}(b_i+s_{ij}),\mathrm{NF}(b_j+s_{ji}))$. Thus it is sufficient to prove that

$$\langle\rho\rangle = \langle\rho\cup\{(\mathrm{NF}(b_i+s_{ij}),\mathrm{NF}(b_j+s_{ji}))\}\rangle.$$

But this follows easily from the fact that both $(b_i+s_{ij},\mathrm{NF}(b_i+s_{ij}))$ and $(b_j+s_{ji},\mathrm{NF}(b_j+s_{ji}))$ belong to $\langle\rho\rangle$.

Before proving that Algorithm CPC ends after a finite number of steps, we need some results related to ascending chains of ideals of $\mathbb{N}^n$.

A subset I of $\mathbb{N}^n$ is an **ideal** if for every $a\in\mathbb{N}^n$ and $b\in I$ we have that $a+b$ lies again in I. From this definition it is easily derived that if $0\in I$, then $I=\mathbb{N}^n$. An ideal I is **principal** if there exists $a\in\mathbb{N}^n$ such that $x\in I$ if and only if $a\leq x$. In this setting, we write $I=a+\mathbb{N}^n$. Let $\{a_1,\dots,a_t\}\subset\mathbb{N}^n$. The **ideal generated** by $\{a_1,\dots,a_t\}$ is the ideal $\bigcup_{i=1}^t(a_i+\mathbb{N}^n)$.

LEMMA 6.9. *Let $\{I_i\mid i\in\mathbb{N}\}$ be a family of ideals of $\mathbb{N}^n$ such that $I_i\subseteq I_{i+1}$. Then there exists $k\in\mathbb{N}$ such that $I_j=I_k$ for all $j>k$.*

PROOF. For every $i\in\mathbb{N}\setminus\{0\}$ if I_{i-1} is strictly contained in I_i, choose $a_i\in I_i\setminus I_{i-1}$. Let A be the set of all the elements obtained in this way. If $a_i\leq a_j$, then there exists $s\in\mathbb{N}^n$ such that $a_j=a_i+s$ and this leads to $a_j\in I_i$ which means that $j<i$. Hence defining

$$B=A\setminus\{a_i\mid a_i\leq a_j \text{ for some } j<i\}$$

we obtain a set of incomparable elements of $\mathbb{N}^n$. Thus $\mathrm{Minimals}_{\leq}(B)=B$ and by Dickson's Lemma (Theorem 5.1), B must be finite. In addition, we have that

$$A\subseteq\bigcup_{b\in B}\{x\in\mathbb{N}^n\mid x\leq b\}.$$

Since the sets $\{x\in\mathbb{N}^n\mid x\leq b\}$ are finite, A has finitely many elements. Clearly, this implies that there exists $k\in\mathbb{N}$ such that for every $j>k$, we have $I_k=I_j$. □

The connection between this result and the finiteness of the number of steps performed in Algorithm CPC is illustrated in the following results.

LEMMA 6.10. *Let $\rho=\{(a_1,b_1),\dots,(a_r,b_r)\}$ be a subset of $\mathbb{N}^n\times\mathbb{N}^n$ such that $b_i\prec a_i$ for all $1\leq i\leq r$. Take $\rho'=\{(a'_1,b'_1),\dots,(a'_t,b'_t)\}$ to be the output of Algorithm Reduce applied to ρ. Then the ideal generated by $\{a_1,\dots,a_r\}$ is contained in the ideal generated by $\{a'_1,\dots,a'_t\}$.*

PROOF. Denote by I_k the ideal of $\mathbb{N}^n$ generated by the first coordinates of the elements of the set

$$\rho'=\{(a_1^k,b_1^k),\dots,(a_{r_k}^k,b_{r_k}^k))\}$$

resulting by executing k times the first step of Algorithm Reduce. Since $b_i^k \prec a_i^k$ for all i, the possible changes occurring when the first step of Algorithm Reduce is executed are of one of the following forms.

1. The element (a_i^k, b_i^k) is replaced by $(a_i^k - a_j^k + b_j^k, b_i^k)$, with $a_i^k - a_j^k \in \mathbb{N}^n$. In this case, $a_i^k = a_j^k + x$ for some $x \in \mathbb{N}^n$ and this implies that $a_i^k + \mathbb{N}^n \subseteq a_j^k + \mathbb{N}^n$. Hence
$$I_k = \bigcup_{s=1}^{r_k} (a_s^k + \mathbb{N}^n) \subseteq (\bigcup_{s=1, s\neq i}^{r_k} (a_s^k + \mathbb{N}^n)) \cup ((a_i^k - a_j^k + b_j^k) + \mathbb{N}^n) = I_{k+1}.$$
2. The element (a_i^k, b_i^k) is replaced by $(b_i^k, a_i^k - a_j^k + b_j^k)$, with $a_i^k - a_j^k \in \mathbb{N}^n$. As before, $a_i^k = a_j^k + x$ for some $x \in \mathbb{N}^n$ and $a_i^k + \mathbb{N}^n \subseteq a_j^k + \mathbb{N}^n$. Thus
$$I_k = \bigcup_{s=1}^{r_k} (a_s^k + \mathbb{N}^n) \subseteq (\bigcup_{s=1, s\neq i}^{r_k} (a_s^k + \mathbb{N}^n)) \cup (b_i^k + \mathbb{N}^n) = I_{k+1}.$$
3. The element (a_i^k, b_i^k) disappears. This may only happen when there exists j such that $a_i^k - a_j^k \in \mathbb{N}^n$ and $a_i^k - a_j^k + b_j^k = b_i^k$. Once more $a_i^k = a_j^k + x$ for some $x \in \mathbb{N}^n$ and $a_i^k + \mathbb{N}^n \subseteq a_j^k + \mathbb{N}^n$. Then
$$I_k = \bigcup_{s=1}^{r_k} (a_s^k + \mathbb{N}^n) \subseteq \bigcup_{s=1, s\neq i}^{r_k} (a_s^k + \mathbb{N}^n) = I_{k+1}.$$
4. The element (a_i^k, b_i^k) is replaced by $(a_i^k, b_i^k - a_j^k + b_j^k)$, with $a_i^k - a_j^k \in \mathbb{N}^n$. In this case,
$$I_k = \bigcup_{s=1}^{k} (a_s^k + \mathbb{N}^n) = I_{k+1}.$$
(Observe that the element (a_i^k, b_i^k) will never be replaced by $(b_i^k - a_j^k + b_j^k, a_i^k)$, since $b_i^k - a_j^k + b_j^k \preceq b_i^k \prec a_i^k$.)

□

PROPOSITION 6.11. *The algorithm CPC ends after a finite number of steps.*

PROOF. Let ρ_k be the system of generators resulting by executing the first step of Algorithm CPC k times, say
$$\rho_k = \{(a_1^k, b_1^k), \dots, (a_{r_k}^k, b_{r_k}^k)\}.$$
Define I_k to be the ideal generated by $\{a_1^k, \dots, a_{r_k}^k\}$. Since $\mathrm{NF}(b_i + s_{ij})$ and $\mathrm{NF}(b_j + s_{ji})$ belong to $\mathrm{Ap}(\mathbb{N}^n, a_1^k, \dots, a_{r_k}^k)$, these elements are not in I_k. Hence every time we add to ρ an element of the form $(\mathrm{NF}(b_i + s_{ij}), \mathrm{NF}(b_j + s_{ji}))$, the resulting ideal becomes larger. By Lemma 6.10, when we apply Algorithm Reduce to
$$\rho_k \cup \{(\mathrm{NF}(b_i + s_{ij}), \mathrm{NF}(b_j + s_{ji}))\}$$

we may get an even greater ideal (observe that the hypothesis $b_i \prec a_i$ of Lemma 6.10 is fulfilled). Thus $I_k \subset I_{k+1}$. Lemma 6.9 states that this sequence cannot be infinite, and this implies that there exists an integer k such that no new elements are added to ρ_k and at this point the algorithm stops, yielding a canonical system of generators. □

EXAMPLE 6.12. Let σ be the congruence on $\mathbb{N}^2$ generated by

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

If we apply Algorithm Reduce to ρ for the order $\preceq_{tdeg}$, we obtain

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

Computing s_{ij} we get $s_{12} = (3,1)-(3,0) = (0,1)$ and $s_{21} = (3,1)-(2,1) = (1,0)$. Since

$$\mathrm{NF}((1,2)+(0,1)) = \mathrm{NF}((1,3)) = (1,3),\ \mathrm{NF}((0,2)+(1,0)) = \mathrm{NF}(1,2) = (1,2),$$

we add $((1,3),(1,2))$ to ρ so that

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

This set is reduced and the elements s_{ij} are

	$s_{12} = (0,1)$	$s_{13} = (0,3)$
$s_{21} = (1,0)$		$s_{23} = (0,2)$
$s_{31} = (2,0)$	$s_{32} = (1,0)$	

Since

$$\mathrm{NF}((1,2)+(0,3)) = \mathrm{NF}((1,5)) = (1,2),\ \mathrm{NF}((1,3)+(2,0)) = \mathrm{NF}((3,3)) = (1,2)$$

and

$$\mathrm{NF}((0,2)+(0,2)) = \mathrm{NF}(0,4) = (0,4),\ \mathrm{NF}((1,2)+(1,0)) = \mathrm{NF}((2,2)) = (0,3),$$

we obtain a new element for our system of generators, say $((0,4),(0,3))$. Thus

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

which is a reduced set.

Now

	$s_{12} = (0,1)$	$s_{13} = (0,3)$	$s_{14} = (0,4)$
$s_{21} = (1,0)$		$s_{23} = (0,2)$	$s_{24} = (0,3)$
$s_{31} = (2,0)$	$s_{32} = (1,0)$		$s_{34} = (0,1)$
$s_{41} = (3,0)$	$s_{42} = (2,0)$	$s_{43} = (1,0)$	

Computing $\mathrm{NF}(b_i + s_{ij})$ we have

$$\mathrm{NF}((1,2)+(0,4)) = (1,2) = \mathrm{NF}((0,3)+(3,0)),$$
$$\mathrm{NF}((0,2)+(0,3)) = (0,3) = \mathrm{NF}((0,3)+(2,0)),$$
$$\mathrm{NF}((1,2)+(0,1)) = (1,2) = \mathrm{NF}((0,3)+(1,0)).$$

Therefore

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

is a canonical system of generators of σ. $\diamond$

We have seen that canonical systems of generators solve the word problem for finitely generated monoids. They can also be used to solve some other problems. Here is an example.

PROPOSITION 6.13. *Let ρ_1 and ρ_2 be two finite subsets of $\mathbb{N}^n \times \mathbb{N}^n$. Assume that ρ_1' and ρ_2' are the sets obtained when applying Algorithm CPC to ρ_1 and ρ_2, respectively (with respect to the same linear admissible order). Then $\langle \rho_1 \rangle = \langle \rho_2 \rangle$ if and only if $\rho_1' = \rho_2'$.*

PROOF. Since $\langle \rho_i \rangle = \langle \rho_i' \rangle$ for $1 \leq i \leq 2$, if $\rho_1' = \rho_2'$, we have that $\langle \rho_1 \rangle = \langle \rho_2 \rangle$.
Assume now that $\sigma = \langle \rho_1 \rangle = \langle \rho_2 \rangle$ and that

$$\rho_1' = \{(a_1, b_1), \dots, (a_r, b_r)\}.$$

Since $\mathrm{NF}_{\rho_1'}(x) = \mu([x])$ for all $x \in \mathbb{N}^n$ (where μ is the minimum function associated to σ), it can be easily proven that

1. $\mathrm{Minimals}_{\leq}(\mathbb{N}^n \setminus \mathrm{Im}(\mu)) = \{a_1, \dots, a_r\}$,
2. for all $i \in \{1, \dots, r\}$, we have that $b_i = \mu([a_i])$.

This implies that a canonical system is uniquely determined. Thus $\rho_1' = \rho_2'$. $\square$

3. The group of units of a monoid

Recall that, as an application of Minkowski-Farkas' lemma, we gave a procedure to compute the set of units of a monoid of the form $\mathbb{N}^n / \sim_M$. In this section, we generalize this result for finitely generated monoids not necessarily cancellative. First of all, we must eliminate of the elements in the presentation of our monoid which are of the form $(e_i, 0)$. As we pointed out in Chapter 3 (Proposition 3.7) for the cancellative case, these elements can be "removed" from the presentation together with the corresponding generators, since they indicate that the i-th generator is equal to zero. The following result enables us to to detect whether the congruence generated by the presentation of a monoid has elements of the form $(e_i, 0)$.

PROPOSITION 6.14. *Let ρ be a canonical system of generators of the congruence σ on $\mathbb{N}^n$. Then $[e_i]_\sigma = [0]_\sigma$ if and only if $(e_i, 0) \in \rho$.*

PROOF. Let $\rho = \{(a_1, b_1), \dots, (a_t, b_t)\}$. If $(e_i, 0) \in \rho$, then $[e_i]_\sigma = [0]_\sigma$. Assume that $[e_i]_\sigma = [0]_\sigma$, that is to say, $e_i \, \sigma \, 0$. Since ρ is a canonical system of generators of σ, by Theorem 6.7, we have that $\mathrm{NF}(e_i) = \mathrm{NF}(0) = 0$. Thus $\mathrm{NF}(e_i) \neq e_i$, which implies that $e_i \notin \mathrm{Ap}(\mathbb{N}^n, a_1, \dots, a_t)$. Hence there exists $j \in \{1, \dots, t\}$ such that $e_i - a_j \in \mathbb{N}^n$ and this forces a_j to be e_i. Therefore $b_j = \mathrm{NF}(a_j) = \mathrm{NF}(e_i) = 0$ and $(e_i, 0) \in \rho$. $\square$

Let us show that we can eliminate the elements $(e_i, 0)$ from σ.

PROPOSITION 6.15. *Let*

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

be a canonical system of generators of the congruence σ *on* $\mathbb{N}^n$ *such that* $(e_n,0) = (a_t,b_t) \in \rho$. *Define*

$$\rho' = \{(a'_1,b'_1),\dots,(a'_{t-1},b'_{t-1})\},$$

where a'_i, b'_i *are the projections onto the first* $n-1$ *coordinates of* a_i *and* b_i, *respectively. Let* σ' *be the binary relation on* $\mathbb{N}^{n-1}$ *defined by*

$$(x_1,\dots,x_{n-1})\ \sigma'\ (y_1,\dots,y_{n-1}) \text{ if and only if } (x_1,\dots,x_{n-1},0)\ \sigma\ (y_1,\dots,y_{n-1},0).$$

Then

1. σ' *is a congruence on* $\mathbb{N}^{n-1}$,
2. $\mathbb{N}^{n-1}/\sigma'$ *is isomorphic to* $\mathbb{N}^n/\sigma$,
3. ρ' *is a canonical system of generators of* σ'.

PROOF. First of all, observe that since ρ is reduced and $(a_t,b_t) = (e_n,0)$, the last coordinate of a_k and b_k is zero for every $k < t$.

The binary relation σ' is a congruence on $\mathbb{N}^{n-1}$, since σ is a congruence on $\mathbb{N}^n$. Define the map

$$\varphi : \mathbb{N}^{n-1}/\sigma' \to \mathbb{N}^n/\sigma,\ \varphi([(x_1,\dots,x_{n-1})]_{\sigma'}) = [(x_1,\dots,x_{n-1},0)]_\sigma.$$

The map φ is a morphism of monoids which, by the definition of σ', is clearly injective. Take $[(x_1,\dots,x_n)]_\sigma \in \mathbb{N}^n/\sigma$. Since $(e_n,0) \in \rho$, we have that $\mathrm{NF}_\rho(x_1,\dots,x_n)$ has its last coordinate equal to zero. Let $(y_1,\dots,y_{n-1},0) = \mathrm{NF}_\rho(x_1,\dots,x_n)$. Then

$$\varphi([(y_1,\dots,y_{n-1})]_{\sigma'}) = [(y_1,\dots,y_{n-1},0)]_\sigma = [(x_1,\dots,x_n)]_\sigma.$$

Thus φ is an isomorphism of monoids.

Finally, note that ρ' is reduced and that if $\mathrm{NF}_\rho((x_1,\dots,x_n)) = (y_1,\dots,y_{n-1},0)$, then $\mathrm{NF}_{\rho'}((x_1,\dots,x_{n-1})) = (y_1,\dots,y_{n-1})$. Using the definition of σ' and Theorem 6.7 (equivalence between (i) and (iv)), we conclude that ρ' is a canonical system of generators of σ' (with respect to the restriction of $\preceq$ to $\mathbb{N}^{n-1}$). □

Thus, from now on, we can assume without loss of generality that σ does not contain any element of the form $(e_i,0)$.

THEOREM 6.16. *Let* σ *be a congruence on* $\mathbb{N}^n$ *such that* $(e_i,0) \notin \sigma$, *for every* $1 \le i \le n$, *and let*

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

be a canonical system of generators of σ. *The following statements are equivalent:*

(i) $\mathbb{N}^n/\sigma$ *is reduced,*
(ii) *the element* b_i *is not zero for all* $i \in \{1,\dots,n\}$.

PROOF. *(i) implies (ii)* Assume that $b_i = 0$ for some i. Since $(e_j,0) \notin \sigma$ for all j and $a_i \neq 0$, we have that $0 \neq a_i - e_k \in \mathbb{N}^n$ for some $k \in \{1,\dots,n\}$. Thus $[a_i - e_k]_\sigma + [e_k]_\sigma = [0]_\sigma$ and $\mathbb{N}^n/\sigma$ is not reduced.

(ii) implies (i) Suppose that there exists $[a]_\sigma, [b]_\sigma \in (\mathbb{N}^n/\sigma) \setminus \{[0]_\sigma\}$ such that

$$[a]_\sigma + [b]_\sigma = [a+b]_\sigma = [0]_\sigma.$$

Since ρ is a canonical system of generators of σ, by Theorem 6.7, we have that $\mathrm{NF}_\rho(a+b) = \mathrm{NF}_\rho(0) = 0$. But this is not be possible, since $b_i \neq 0$ for all $i \in \{1,\dots,n\}$. □

This result enables us to determine whether a monoid given by a presentation is or is not reduced, that is to say, we can decide whether its group of units is or is not trivial. We illustrate with an example that we can obtain more information related to the group of units of a monoid from a canonical system of generators associated to a presentation of the given monoid.

EXAMPLE 6.17. Let S be the monoid given by the presentation

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

A canonical system of generators of $\sigma = \langle\rho\rangle$ with respect to $\preceq_{tdeg}$ (see exercises at the end of Chapter 5) is

$$\kappa = \rho \cup \{((0,1,3,0),(2,1,0,0))\}.$$

Since $((3,0,0,0),(0,0,0,0)) \in \kappa$, we have that $3[e_1]_\sigma = [0]_\sigma$ which implies that $[e_1]_\sigma \in \mathrm{U}(S)$ (denote by $-[e_1]_\sigma$ the inverse of $[e_1]_\sigma$). In addition $((0,0,3,0),(2,0,0,0)) \in \sigma$ and this leads to $3[e_3]_\sigma = 2[e_1]_\sigma$. Then $[e_3]_\sigma + (2[e_3]_\sigma - 2[e_1]_\sigma) = [0]_\sigma$ which means that $[e_3]_\sigma$ is also a unit. ◇

The underlying idea in this example is that if $x+y$ is a unit, then so are both x and y. (Hence $x+y$ is a unit if and only if x and y are units.) Let us work with this idea a little more.

Let S be a monoid given by a presentation ρ, that is to say, S is isomorphic to $\mathbb{N}^n/\sigma$ with $\sigma = \langle\rho\rangle$. Take

$$\kappa = \{(a_1,b_1),\dots,(a_t,b_t)\}$$

to be a canonical system of generators of σ with respect to a given linear admissible order. Recall that, by Proposition 4.12, if we want to compute $\mathrm{U}(\mathbb{N}^n/\sigma)$, we only have to determine for which $i \in \{1,\dots,n\}$ the element $[e_i]_\sigma$ belongs to $\mathrm{U}(\mathbb{N}^n/\sigma)$. By definition, the element $[e_i]_\sigma$ is a unit if there exists $(x_1,\dots,x_n) \in \mathbb{N}^n$ such that

$$[(x_1,\dots,x_n)]_\sigma + [e_i]_\sigma = [(x_1,\dots,x_{i-1},x_i+1,x_{i+1},\dots,x_n)]_\sigma = [0]_\sigma.$$

By Theorem 6.7 this occurs if and only if

$$\mathrm{NF}_\kappa((x_1,\dots,x_{i-1},x_i+1,x_{i+1},\dots,x_n)) = 0.$$

This happens if and only if there is a sequence

$$(a_{i_1},b_{i_1}),\dots,(a_{i_s},b_{i_s})$$

of elements of κ such that

$$(x_1,\dots,x_{i-1},x_i+1,x_{i+1},\dots,x_n)+\sum_{j=1}^{s}(-a_{i_j}+b_{i_j})=0$$

and

$$((x_1,\dots,x_{i-1},x_i+1,x_{i+1},\dots,x_n)+\sum_{j=1}^{k}(-a_{i_j}+b_{i_j}))-a_{i_{k+1}}\in\mathbb{N}^n$$

for all $k<s$. (Observe that, in particular, there must exist $j\in\{1,\dots,s\}$ such that $e_i<a_{i_j}$, since the i-th coordinate of $(x_1,\dots,x_{i-1},x_i+1,x_{i+1},\dots,x_n)$ is greater than zero.)

In order to simplify the notation, let $y=(x_1,\dots,x_n)+e_i$. Since

$$y-\sum_{j=1}^{s-1}(-a_{i_j}+b_{i_j})-a_{i_s}\in\mathbb{N}^n,\ b_{i_s}\in\mathbb{N}^n$$

and

$$y-\sum_{j=1}^{s-1}(-a_{i_j}+b_{i_j})-a_{i_s}+b_{i_s}=0,$$

we obtain that $b_{i_s}=0$. Thus $[a_{i_s}]_\sigma=[b_{i_s}]_\sigma=[0]_\sigma$ and this implies that for every k such that $e_k<a_{i_s}$, we have that $[e_k]_\sigma$ is a unit. Furthermore

$$y-\sum_{j=1}^{s-2}(-a_{i_j}+b_{i_j})-a_{i_{s-1}}+b_{i_{s-1}}=a_{i_s}$$

and as $[a_{i_s}]_\sigma$ is a unit, so is $[b_{i_{s-1}}]_\sigma=[a_{i_{s-1}}]_\sigma$. Hence for every k such that $e_k<a_{i_{s-1}}$ we have that $[e_k]_\sigma$ is a unit. The next step is to consider the equality

$$y-\sum_{j=1}^{s-3}(-a_{i_j}+b_{i_j})-a_{i_{s-2}}+b_{i_{s-2}}=a_{i_{s-1}}-b_{i_{s-1}}+a_{i_s},$$

and since $[a_{i_{s-1}}]_\sigma$, $[b_{i_{s-1}}]_\sigma$ and $[a_{i_s}]_\sigma$ are units, so is $[b_{i_{s-2}}]_\sigma=[a_{i_{s-2}}]_\sigma$. Once more, for every k with $e_k<a_{i_{s-2}}$, we have that $[e_k]_\sigma$ is a unit. If we continue this process, we obtain that for every j and for every k such that $e_k<a_{i_j}$ the element $[e_k]_\sigma$ is a unit of $\mathbb{N}^n/\sigma$. From this remark, the reader can easily prove that the following algorithm computes the set

$$\{\ i\in\{1,\dots,n\}\mid [e_i]_\sigma\in \mathrm{U}(\mathbb{N}^n/\sigma)\ \}.$$

ALGORITHM 6.18. The input is a canonical system of generators

$$\kappa=\{(a_1,b_1),\dots,(a_t,b_t)\}$$

of σ. The output is the set

$$A=\{\ i\in\{1,\dots,n\}\mid [e_i]_\sigma\in \mathrm{U}(\mathbb{N}^n/\sigma)\ \}.$$

1. Set $A=\emptyset$.

2. Let B be the set of elements j in $\{1,\dots,n\}$ such that there exists $k \in \{1,\dots,t\}$ such that a_k has its j-th coordinate nonzero ($e_j < a_k$) and that for every $i \notin A$, the element b_k has its i-th coordinate equal to zero.
3. If $A = B$, then return A.
4. Otherwise, set $A = B$ and go to Step 2. ◇

Observe that this algorithm also enables us to determine whether a monoid given by a presentation is a group; we only have to check whether $A = \{1,\dots,n\}$.

EXAMPLE 6.19. Let S be the monoid given by the presentation

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

A canonical system of generators with respect to $\preceq_{tdeg}$ is

$$\kappa = \{((1,2,0),(0,0,3)),((2,1,0),(0,0,0)),((1,0,3),(0,1,0)),((0,0,6),(0,3,0))\}.$$

Let us trace the execution of Algorithm 6.18 applied to this set.

- $A = \emptyset$ (Step 1).
- $B = \{1,2\}$ (Step 2, $k = 2$ for $j = 1$ and $j = 2$).
- $A = \{1,2\}$ (Step 4).
- $B = \{1,2,3\}$ (Step 2, $k = 3$ for $j = 3$).
- $A = \{1,2,3\}$ (Step 4).
- $B = \{1,2,3\}$ (Step 4, since $A = \{1,2,3\}$).
- The output is $\{1,2,3\}$.

Hence S is a group.

Remarks

The core of this chapter is Algorithm CPC which computes a canonical system of generators with respect to a given linear admissible order from a system of generators of a congruence on $\mathbb{N}^n$. This algorithm is inspired in Knuth-Bendix's critical pair completion algorithm for rewriting rules (see **[28]**). The description of Algorithm CPC presented in this chapter follows the line exposed in **[42]**. Buchberger's algorithm for the computation of a Gröbner basis of an ideal is also based on critical pair completion. Thus from the equivalence between systems of generators of a congruence and systems of generators of the ideal associated to the congruence (see the remarks section of Chapter 5) it is easy to show that a canonical system of generators with respect to a given linear admissible order corresponds exactly to a reduced Gröbner basis of the ideal associated to the congruence with respect to the same linear admissible order. More precisely, if S is isomorphic to $\mathbb{N}^n/\sigma$, then

$$\{(a_1,b_1),\dots,(a_t,b_t)\}$$

is a canonical system of generators of σ with respect to the linear admissible order $\preceq$ if and only if

$$\{X^{a_1} - X^{b_1},\dots,X^{a_t} - X^{b_t}\}$$

is a reduced Gröbner basis of I_S with respect to $\preceq$.

Exercises

1. Give an example of a subset of $\mathbb{N}^2 \times \mathbb{N}^2$ reduced with respect to $\preceq_p$ and not reduced with respect to $\preceq_{lex}$ (for the definition of $\preceq_p$ and $\preceq_{lex}$ see the exercises of Chapter 5).
2. Prove that the number of elements in a canonical system of generators of a congruence depends on the linear admissible order used to compute it.
3. Show that
$$\rho_1 = \{((3,0,0),(2,0,0)),((0,0,2),(1,3,0))\}$$
and
$$\rho_2 = \{((3,0,0),(2,0,0)),((0,0,2),(4,1,0))\}$$
generate the same congruence.
4. Let σ be the congruence generated by
$$\{((2,2),(1,1)),((3,0),(1,2))\}.$$
   (a) Compute a canonical system of generators for σ with respect to $\preceq_{lex}$.
   (b) Show that $(6,7)\ \sigma\ (1,2)$.
5. Let
$$\rho = \{((0,3,0),(3,1,0)),((0,0,2),(2,1,0)),((0,2,1),(3,0,1))\}.$$
Prove that ρ is a canonical system of generators for $\langle\rho\rangle$ with respect to $\preceq_p$.
6. Let $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\} \subseteq \mathbb{N}^n \times \mathbb{N}^n$ be a canonical system of generators of σ for some linear admissible order $\preceq$. Show that $\mathbb{N}^n/\sigma$ is finite if and only if $\mathrm{Ap}(\mathbb{N}^n, a_1,\dots,a_p)$ is finite.
7. Let σ be the congruence on $\mathbb{N}^4$ generated by
$$\{((3,0,0,0),(0,0,0,0)),((0,0,3,0),(2,0,0,0)),((0,1,0,1),(0,1,1,0))\}.$$
Show that $\mathrm{U}(\mathbb{N}^4/\sigma)$ is isomorphic to $\mathbb{N}^2/\sigma'$, where σ' is the congruence generated by
$$\{((3,0),(0,0)),((2,0),(0,3)).$$
Prove that this monoid is isomorphic to $\mathbb{Z}_9$ (hint: $\mathbb{N}^2/\sigma'$ is a group and therefore it is cancellative, which means that $\sigma' = \sim_{M_{\sigma'}}$).
8. Let σ be the congruence on $\mathbb{N}^3$ generated by
$$\{((2,1,0),(0,0,0)),((0,0,2),(1,1,0))\}.$$
Prove that $\mathbb{N}^3/\sigma$ is cancellative.
9. Find a noncyclic monoid with five elements.
10. Let (a,b,c) and (x,y,z) be two non-comparable elements of $\mathbb{N}^3$ (with respect to $\leq$). Prove that there exists a linear admissible order $\preceq$ such that $\{((a,b,c),(x,y,z))\}$ is a canonical system of generators, with respect to $\preceq$, of the congruence $\langle\{((a,b,c),(x,y,z))\}\rangle$.

11. Find a monoid S with eight elements such that for every $x \in S$, we have that $2x = x$.
12. Find a congruence σ on $\mathbb{N}^2$ and a system of generators ρ of σ which is a canonical system of generators with respect to any linear admissible order on $\mathbb{N}^2$.
13. Let $\preceq_1$ be a linear and admissible order on $\mathbb{N}^n$. Define on $\mathbb{N}^{n-1}$ the following relation:

    $$(x_1,\dots,x_{n-1}) \preceq_2 (y_1,\dots,y_{n-1}) \text{ if } (x_1,\dots,x_{n-1},0) \preceq_1 (y_1,\dots,y_{n-1},0).$$

    Prove that $\preceq_2$ is a linear admissible order on $\mathbb{N}^{n-1}$.
14. Prove that if σ is a congruence on $\mathbb{N}^n$ such that $\mathbb{N}^n/\sigma$ is cancellative and

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

    is a canonical system of generators of σ, then a_ib_i (the **dot product** of a_i and b_i, which is defined as: $(x_1,\dots,x_n)(y_1,\dots,y_n) = \sum_{i=1}^n x_iy_i$) is zero for all $i \in \{1,\dots,t\}$. Find a counterexample showing that the converse of this statement is not true.

CHAPTER 7

Nonnegative integer solutions of systems of linear equations

Let A be a $m \times n$ matrix with integer entries. Define

$$S = \{x \in \mathbb{N}^n \mid Ax = 0\}.$$

Observe that $0 \in S$ and that if $x, y \in S$, then so is $x + y$. Thus S is a submonoid of $\mathbb{N}^k$. This monoid has some interesting properties:

1. If $x, y \in S$ and $x - y \geq 0$, then $A(x-y) = Ax - Ay = 0$, which means that $x - y \in S$. This can be stated as $\mathbf{G}(S) \cap \mathbb{N}^n = S$.
2. By Dickson's Lemma, the set $\text{Minimals}_{\leq}(S \setminus \{0\})$ is finite. Let

   $$M = \text{Minimals}_{\leq}(S \setminus \{0\}) = \{s_1, \ldots, s_t\}.$$

   Take x to be an element of $S \setminus \{0\}$. If $x \notin M$, then by Corollary 5.4 there exists $s_{i_1} \in M$ such that $s_{i_1} < x$. Define $x_1 = s - s_{i_1}$, which belongs to $\mathbf{G}(S) \cap \mathbb{N}^n = S$. Once more, we check whether $x_1 \in M$. If not, there must be an element $s_{i_2} \in M$ such that $s_{i_2} < x_1$. Set $x_2 = x_1 - s_{i_2}$. By Corollary 5.3 this process must stop in a finite number of steps. In other words, there exists $k \in \mathbb{N}$ such that $x_k = s_{i_k} \in M$ and this leads to $x = \sum_{i=1}^{k} s_{i_j}$. Therefore S is an affine semigroup (that is to say, a finitely generated submonoid of $\mathbb{N}^n$).

This chapter is devoted to the study of this kind of semigroup. Our main goal is to provide an algorithm for computing the set $\text{Minimals}_{\leq}(S \setminus \{0\})$ (and therefore a system of generators of S).

1. Nonnegative integer solutions of a system of linear homogeneous Diophantine equations

We shall use $\leq$ to refer to two "different" partial orders: the first one is the product order on $\mathbb{N}^n$ and the second is the product order on $\mathbb{Q}^n$. Since we can think of the latter as an "extension" of the first one, this abuse of notation is not too severe. Throughout this section, for an element $y \in \mathbb{Q}^n$, we denote its i-th coordinate by y_i.

Given $y \in \mathbb{Q}^n$, define

$$\mathrm{B}(y) = \{z \in \mathbb{Q}^n \mid y \leq z \leq y + (1, \ldots, 1)\}$$

and

$$\overline{0y} = \{qy \mid q \in \mathbb{Q} \text{ and } 0 \leq q \leq 1\}.$$

The set $\mathrm{B}(y)$ is the translation of the cube whose vertices are the elements $\sum_{i=1}^n b_i e_i$, with $b_i \in \{0,1\}$, and the set $\overline{0y}$ is the segment joining 0 and y. Trivially

$$\mathrm{B}(y) \cap \overline{0z} = \{qz \mid q \in \mathbb{Q} \text{ and } y \leq qz \leq y + (1,\dots,1),\ 0 \leq q \leq 1\}.$$

Let x be an element in $\mathbb{N}^n \setminus \{0\}$ and set $p = \sum_{i=1}^n x_i = \|x\|_1$. We are going to define a sequence

$$\mathrm{T}(x) = \{(y^0, z^0), \dots, (y^p, z^p)\} \subseteq \mathbb{N}^n \times \mathbb{Q}^n$$

verifying the following properties.

1. $y^k < y^{k+1}$,
2. $z^k \in \mathrm{B}(y^k) \cap \overline{0x}$,
3. $\sum_{i=1}^n y_i^k = k$,
4. $y^p = x$.

This sequence is defined recurrently as follows:

- Set $(y^0, z^0) = (0,0) \in \mathbb{Q}^n \times \mathbb{Q}^n$.
- Assume that (y^k, z^k) has been defined for $k < p-1$. Since $z^k \in \mathrm{B}(y^k) \cap \overline{0x}$, the set

$$\left\{q \in \mathbb{Q} \mid qx \in \mathrm{B}(y^k) \cap \overline{0x}\right\}$$

is not empty and it is a segment in $\mathbb{Q}$. Its maximum (right end) w_k must verify that for every i such that $x_i \neq 0$, the inequality $w_k x_i \leq y_i^k + 1$ holds. Take $i_k \in \{1,\dots,n\}$ satisfying

$$\frac{y_{i_k}^k + 1}{x_{i_k}} = \min\left\{ \frac{y_i^k+1}{x_i} \,\middle|\, x_i \neq 0 \right\}.$$

Clearly $w_k = (y_{i_k}^k + 1)/x_{i_k}$. Define $(y^{k+1}, z^{k+1}) = (y^k + e_{i_k}, w_k x)$. (Roughly speaking, z^{k+1} belongs to the face of $\mathrm{B}(y^k)$ perpendicular to e_{i_k} and that is why we define $y^{k+1} = y^k + e_{i_k}$, since $\mathrm{B}(y^k)$ and $\mathrm{B}(y^{k+1})$ have this face in common.) Observe that:

1. $y^k < y^{k+1}$.
2. By the definition of w_k, we have that $y^k \leq w_k x \leq y^k + (1,\dots,1)$. Hence for all $i \neq i_k$, we get $y_i^{k+1} \leq w_k x_i = z_i^{k+1} \leq y_i^{k+1} + 1$. In addition, $w_k x_{i_k} = y_{i_k}^k + 1$ and for this reason $y_{i_k}^{k+1} = y_{i_k}^k + 1 \leq w_k x_{i_k} \leq y_{i_k}^{k+1} + 1$. Hence

$$y^{k+1} \leq w_k x = z^{k+1} \leq y^{k+1} + (1,\dots,1),$$

which means that $z^{k+1} \in \mathrm{B}(y^{k+1}) \cap \overline{0x}$.

3. $\sum_{i=1}^n y_i^{k+1} = \sum_{i=1}^n y_i^k + 1 = k+1$.

- For $k = p-1$, we have that $\sum_{i=1}^n y_i^{p-1} = p-1$ and that $\mathrm{B}(y^{p-1}) \cap \overline{0x}$ is not empty. Hence $x \in \mathrm{B}(y^{p-1})$. Define $y^p = x = z^p$.

EXAMPLE 7.1. Let $x = (3,2) \in \mathbb{N}^2$.

- $(y^0, z^0) = ((0,0),(0,0))$.

- $B((0,0)) = \{(r,s) \in \mathbb{Q}^2 \mid 0 \le r \le 1, 0 \le s \le 1\}$,

$$\begin{aligned} y_1^0 &= 0 \le 3w \le 1 = y_1^0 + 1, \\ y_2^0 &= 0 \le 2w \le 1 = y_2^0 + 1. \end{aligned}$$

  Then $w_1 = 1/3$, $z^1 = (1/3)x = (1,2/3)$ and $y^1 = (0,0) + (1,0) = (1,0)$.
- $B((1,0)) = \{(r,s) \in \mathbb{Q}^2 \mid 1 \le r \le 2, 0 \le s \le 1\}$,

$$\begin{aligned} y_1^1 &= 1 \le 3w \le 2 = y_1^1 + 1, \\ y_2^1 &= 0 \le 2w \le 1 = y_2^1 + 1. \end{aligned}$$

  Then $w_2 = 1/2$, $z^2 = (1/2)x = (3/2,1)$ and $y^2 = (1,0) + (0,1) = (1,1)$.
- $B((1,1)) = \{(r,s) \in \mathbb{Q}^2 \mid 1 \le r \le 2, 1 \le s \le 2\}$,

$$\begin{aligned} y_1^2 &= 1 \le 3w \le 2 = y_1^2 + 1, \\ y_2^2 &= 1 \le 2w \le 2 = y_2^2 + 1. \end{aligned}$$

  Then $w_3 = 2/3$, $z^3 = (2/3)x = (2,4/3)$ and $y^3 = (1,1) + (1,0) = (2,1)$.
- $B((2,1)) = \{(r,s) \in \mathbb{Q}^2 \mid 2 \le r \le 3, 1 \le s \le 2\}$,

$$\begin{aligned} y_1^3 &= 2 \le 3w \le 3 = y_1^3 + 1, \\ y_2^3 &= 1 \le 2w \le 2 = y_2^3 + 1. \end{aligned}$$

  Then $w_4 = 1$, $z^4 = 1x = (3,2)$ and $y^4 = (2,1) + (1,0) = (3,1)$ (or $y^4 = (2,1) + (0,1)$, the final result is the same).
- $B((3,1)) = \{(r,s) \in \mathbb{Q}^2 \mid 3 \le r \le 4, 1 \le s \le 2\}$.

$$\begin{aligned} y_1^4 &= 3 \le 3w \le 4 = y_1^4 + 1 \\ y_2^4 &= 1 \le 2w \le 2 = y_2^4 + 1 \end{aligned}$$

  Then $w_5 = 1$, $z^5 = 1x = (3,2)$ and $y^5 = (3,1) + (0,1) = (3,2) = x$. ◇

With this notation, it is easy to prove the following key result.

THEOREM 7.2 (Pottier). *Let $A = (a_{ij})$ be a $m \times n$ matrix with integer entries and let S be the set of nonnegative solutions of $Ax = 0$. If $x \in \mathbb{N}^n$ belongs to* Minimals$_{\le}(S \setminus \{0\})$, *then*

$$\sum_{i=1}^{n} x_i \le \prod_{i=1}^{m} (1 + \sum_{j=1}^{n} |a_{ij}|).$$

PROOF. Let $p = \sum_{i=1}^{n} x_i$ and $\mathrm{T}(x) = \{(y^0, z^0), \dots, (y^p, z^p)\}$ as before. For all $k \in \{0, \dots, p\}$, define $y'^k = z^k - y^k$. From the definition of (y^k, z^k), we deduce that $0 \le y'^k \le (1, \dots, 1)$ and that

$$Ay^k = A(z^k - y'^k) = Az^k - Ay'^k = A(w_k x) - Ay'^k = -Ay'^k,$$

which leads to

$$|(Ay^k)_i| = |(Ay'^k)_i|.$$

Since $0 \leq y'^k \leq (1,\dots,1)$, the inequality $|(Ay'^k)_i| \leq \sum_{j=1}^n |a_{ij}|$ holds. In addition, $y^k \in \mathbb{N}^n$ and this leads to $|(Ay^k)_i| = |(Ay'^k)_i| \in \mathbb{N}$. Thus $(Ay^k)_i$ may have $1+\sum_{j=1}^n |a_{ij}|$ different values and thus there are $\prod_{i=1}^m (1+\sum_{j=1}^n |a_{ij}|)$ different possible values of Ay^k. From this remark the proof follows easily, since if $p > \prod_{i=1}^m (1+\sum_{j=1}^n |a_{ij}|)$, then there must exist $i,j \in \{0,\dots,p\}$, $i > j$ such that $Ay^i = Ay^j$ and consequently $A(y^i - y^j) = 0$. But $0 < y^i - y^j < x$ which contradicts with the fact that $x \in \text{Minimals}_{\leq}(S \setminus \{0\})$. □

This theorem yields a method for computing the set of generators of the monoid of nonnegative solutions of $Ax = 0$. It suffices to scan the region

$$\left\{ (x_1,\dots,x_n) \in \mathbb{N}^n \mid \sum_{i=1}^n x_i \leq \prod_{i=1}^m (1+\sum_{j=1}^n |a_{ij}|) \right\},$$

and choose from it the elements for which $Ax = 0$, discarding those that are not minimal.

EXAMPLE 7.3. Let S be the set of nonnegative solutions of the system of equations

$$\begin{aligned} x - y &= 0, \\ 3x - y - 2z &= 0. \end{aligned}$$

The bound of Theorem 7.2 is $3 \times 7 = 21$. Hence we must look for the elements in S belonging to

$$\{(x,y,z) \in \mathbb{N}^3 \mid x+y+z \leq 21\}.$$

The elements of $S \setminus \{0\}$ belonging to this set are $\{(1,1,1),(2,2,2),\dots,(7,7,7)\}$. Therefore

$$S = \langle (1,1,1) \rangle.$$

◇

Note that this testing may be tedious, even using a computer. In order to avoid scanning all the elements $x \in \mathbb{N}^n$ such that $\sum_{i=1}^n x_i$ is less than or equal to the bound appearing in Theorem 7.2, one should choose a strategy to move through this region avoiding to inspect parts of this set that yield no minimal solution. First we could eliminate, every time we find a solution x of $Ax = 0$, the elements y such that $x \leq y$ from the region to scan. A second hint is given in the construction of $\mathrm{T}(x)$ when x belongs to S. Observe that $\mathrm{T}(x)$ is a path that connects 0 with x by adding e_{i_k} at each step. The condition that fulfills y^k is that

$$|(Ay^k)_i| \leq \sum_{j=1}^n |a_{ij}| \text{ for all } i \in \{1,\dots,m\}.$$

Hence we can use a search tree with root 0 and for each node y, search in the subtree starting at $y + e_i$ if and only if this element fulfills the above condition. We also impose that every solution has no "sons", that is to say, do not explore the elements $x + e_i$ whenever x is an element in S. In this way the algorithm speeds up, but the implementation requires more work than simply scanning the whole region.

2. The monoid of nonnegative elements of a subgroup of $\mathbb{Z}^n$

Let M be a subgroup of $\mathbb{Z}^n$. We use the knowledge acquired in the last section to give a procedure for computing the elements of the monoid $M \cap \mathbb{N}^n$. Let

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

be the defining equations of M. We want to compute the set of nonnegative integer solutions of this system of equations. Since we know the solution to this problem for the homogeneous case, we transform this system of equations so that we can use what we have learned in the last section. Let M' be the subgroup of $\mathbb{Z}^{n+2r}$ with defining equations

$$\begin{array}{lcccl} a_{11}x_1 + \cdots + a_{1n}x_n & + & d_1x_{n+1} - d_1x_{n+r+1} & & = 0, \\ & & & \ddots & \vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n & + & & d_rx_{n+r} - d_rx_{n+2r} & = 0, \\ a_{(r+1)1}x_1 + \cdots + a_{(r+1)n}x_n & & & & = 0, \\ & & & & \vdots \\ a_{(r+k)1}x_1 + \cdots + a_{(r+k)n}x_n & & & & = 0. \end{array}$$

We can compute a minimal system of generators $\{s'_1, \ldots, s'_m\}$ of $M' \cap \mathbb{N}^{n+2r}$. Let π be the map defined as follows:

$$\pi : \mathbb{N}^{n+2r} \to \mathbb{N}^n, \ \pi(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+2r}) = (a_1, \ldots, a_n).$$

If $s = (a_1, \ldots, a_n) \in M \cap \mathbb{N}^n$, then for all $i \in \{1, \ldots, r\}$

$$a_{i1}a_1 + \cdots + a_{in}a_n = k_i d_i$$

for some $k_i \in \mathbb{Z}$. Define

$$b_i = \begin{cases} 0 & \text{if } k_i \geq 0, \\ -k_i & \text{otherwise}, \end{cases}, \quad c_i = \begin{cases} k_i & \text{if } k_i \geq 0, \\ 0 & \text{otherwise}. \end{cases}$$

If we take $s' = (a_1, \ldots, a_n, b_1, \ldots, b_r, c_1, \ldots, c_r)$, then $s' \in M' \cap \mathbb{N}^{n+2r}$ and $\pi(s') = s$. Since $s' \in M' \cap \mathbb{N}^{n+2r}$, there exist $l_1, \ldots, l_m \in \mathbb{N}$ such that $s' = \sum_{i=1}^m l_i s'_i$. Thus $s = \pi(s') = \sum_{i=1}^m l_i \pi(s'_i)$. This means that

$$M \cap \mathbb{N}^n = \langle \pi(s'_1), \ldots, \pi(s'_m) \rangle.$$

As a consequence of this, $M \cap \mathbb{N}^n$ is affine. The monoids of the form $M \cap \mathbb{N}^n$ are known as **full** affine semigroups.

EXAMPLE 7.4. Let M be the subgroup of $\mathbb{Z}^2$ given by the equation

$$x+y \equiv 0 \pmod 2.$$

If we want to compute $M \cap \mathbb{N}^2$, then we must first calculate the set $M' \cap \mathbb{N}^4$, where M' is the subgroup of $\mathbb{Z}^4$ with defining equation

$$x+y+2z-2t=0.$$

The bound of Theorem 7.2 is 7. Hence we must search for elements (x,y,z,t) in $\mathbb{N}^4$ such that $x+y+z+t \leq 7$. The set of elements of this region which are solutions of the equation $x+y+2z-2t=0$ are

$$\{(0,0,1,1),(0,2,0,1),(1,1,0,1),(2,0,0,1),(0,0,2,2),(0,2,1,2),$$

$$(1,1,1,2),(2,0,1,2),(0,0,3,3),(0,4,0,2),(1,3,0,2),(2,2,0,2),$$

$$(3,1,0,2),(4,0,0,2),(0,2,2,3),(1,1,2,3),(2,0,2,3)\}$$

and the minimal elements of this set (generators of $M' \cap \mathbb{N}^4$) are

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

Hence

$$M \cap \mathbb{N}^2 = \langle (0,0),(0,2),(1,1),(2,0)\rangle = \langle (0,2),(1,1),(2,0)\rangle.$$

◇

Next, we show that the procedure for finding a system of generators for $M \cap \mathbb{N}^n$ used in this example can be improved slightly. The reader can check that, as in the homogeneous case, $M \cap \mathbb{N}^n$ is generated by the set $\text{Minimals}_{\leq}(M \cap \mathbb{N}^n \setminus \{0\})$.

THEOREM 7.5. *Let M be the subgroup of $\mathbb{Z}^n$ with defining equations*

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

If $(x_1,\ldots,x_n) \in \text{Minimals}_{\leq}(M \cap \mathbb{N}^n \setminus \{0\})$, then

$$\sum_{i=1}^{n} x_i \leq \prod_{i=1}^{r}(1+|d_i|+\sum_{j=1}^{n}|a_{ij}|) \prod_{i=r+1}^{r+k}(1+\sum_{j=1}^{n}|a_{ij}|).$$

PROOF. Let M' be the homogeneous group associated to M as above. As we have shown before, the projections onto the first n coordinates of the elements in $\text{Minimals}_{\leq}(M' \cap \mathbb{N}^{n+2r} \setminus \{0\})$ form a system of generators of $M \cap \mathbb{N}^n$. Hence every

element in $\mathrm{Minimals}_{\leq}(M \cap \mathbb{N}^n \setminus \{0\})$ is one of these projections. Thus it suffices to show that

$$\sum_{i=1}^{n} x_i \leq \prod_{i=1}^{r}(1+|d_i|+\sum_{j=1}^{n}|a_{ij}|) \prod_{i=r+1}^{r+k}(1+\sum_{j=1}^{n}|a_{ij}|)$$

for the elements

$$x = (x_1, \dots, x_n, x_{n+1}, \dots, x_{n+2r}) \in \mathrm{Minimals}_{\leq}((M' \cap \mathbb{N}^{n+2r}) \setminus \{0\}),$$

such that $(x_1, \dots, x_n) \neq 0$. Since $(x_1, \dots, x_{n+2r})$ is minimal, the product $x_{n+i}x_{n+r+i} = 0$ for all $i \in \{1, \dots, r\}$ (if both x_{n+i} and x_{n+r+i} are nonzero, then the element $x - e_{n+i} - e_{n+r+i} \in M'$ and $x - e_{n+i} - e_{n+r+i} < x$). This motivates the definition of the subgroup $\overline{M}$ of $\mathbb{Z}^{n+r}$ whose defining equations are

$$\begin{array}{lcccl}
a_{11}x_1 + \cdots + a_{1n}x_n & + & \varepsilon_1 d_1 x_{n+1} & & = 0, \\
 & & & \ddots & \vdots \\
a_{r1}x_1 + \cdots + a_{rn}x_n & + & & \varepsilon_r d_r x_{n+r} & = 0, \\
a_{(r+1)1}x_1 + \cdots + a_{(r+1)n}x_n & & & & = 0, \\
 & & & & \vdots \\
a_{(r+k)1}x_1 + \cdots + a_{(r+k)n}x_n & & & & = 0,
\end{array}$$

where

$$\varepsilon_j = \begin{cases} 1 & \text{if } x_{n+r+j} = 0, \\ -1 & \text{otherwise.} \end{cases}$$

If we show that $(x_1, \dots, x_n, \max\{x_{n+1}, x_{n+r+1}\}, \dots, \max\{x_{n+r}, x_{n+r+r}\})$ is a minimal element of $\overline{M} \cap \mathbb{N}^{n+r} \setminus \{0\}$ then, using Theorem 7.2, we get the desired result, since

$$\sum_{i=1}^{n} x_i \leq \sum_{i=1}^{n} x_i + \sum_{i=n+1}^{n+r} \max\{x_{n+i}, x_{n+r+i}\} \leq \prod_{i=1}^{r}(1+|d_i|+\sum_{j=1}^{n}|a_{ij}|) \prod_{i=r+1}^{r+k}(1+\sum_{j=1}^{n}|a_{ij}|).$$

Assume that there exists $(y_1, \dots, y_{n+r}) \in \overline{M} \cap \mathbb{N}^{n+r} \setminus \{0\}$ such that

$$(y_1, \dots, y_n, y_{n+1}, \dots, y_{n+r}) < (x_1, \dots, x_n, \max\{x_{n+1}, x_{n+r+1}\}, \dots, \max\{x_{n+r}, x_{n+r+r}\}).$$

This means that either $y_i < x_i$ for some $i \in \{1, \dots, n\}$ or $y_{n+j} < \max\{x_{n+i}, x_{n+r+i}\}$ for some $j \in \{1, \dots, r\}$. In the latter case, $y_{n+j} < x_{n+j}$ or $y_{n+j} < x_{n+r+j}$. Take $(y_1, \dots, y_n, z_{n+1}, \dots, z_{n+2r})$ to be the element in $\mathbb{N}^{n+2r}$ such that

$$z_{n+j} = \begin{cases} y_{n+j} & \text{if } \varepsilon_j = 1, \\ 0 & \text{otherwise,} \end{cases} \qquad z_{n+r+j} = \begin{cases} y_{n+j} & \text{if } \varepsilon_j = -1, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $(y_1, \dots, y_n, z_{n+1}, \dots, z_{n+2r}) \in M' \cap \mathbb{N}^{n+2r}$ and by the definition of z_{n+j}, we have that

$$(y_1, \dots, y_n, z_{n+1}, \dots, z_{n+2r}) < (x_1, \dots, x_n, x_{n+1}, \dots, x_{n+2r}).$$

However, $(x_1, \dots, x_{n+2r}) \in \mathrm{Minimals}_{\leq}(M \cap \mathbb{N}^{n+2r} \setminus \{0\})$ and this leads to

$$(y_1, \dots, y_n, z_{n+1}, \dots, z_{n+2r}) = 0.$$

Therefore $(y_1,\dots,y_{n+r})=0$. We have shown that

$$(x_1,\dots,x_n,\max\{x_{n+1},x_{n+r+1}\},\dots,\max\{x_{n+r},x_{n+r+r}\})\in \mathrm{Minimals}_{\leq}(\overline{M}\cap\mathbb{N}^{n+r}\setminus\{0\}),$$

which concludes the proof. □

EXAMPLE 7.6. Let us go back to the subgroup M of $\mathbb{Z}^2$ given by the equation

$$x+y\equiv 0 \pmod 2.$$

The bound of Theorem 7.5 for the minimal elements of $(M\cap\mathbb{N}^2)\setminus\{0\}$ is 5. Hence we must search for elements (x,y) in $\mathbb{N}^2\setminus\{(0,0)\}$ such that $x+y\leq 5$. The set of elements of this region belonging to M are

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

Hence

$$M\cap\mathbb{N}^2=\langle(0,2),(1,1),(2,0)\rangle.$$

◇

3. Nonnegative integer solutions of systems of linear Diophantine equations

Let A and b be $m\times n$ and $m\times 1$ matrices with integer coefficients, respectively. Here we give a procedure for computing the set of nonnegative integer solutions of the system of equations of the form

$$Ax=b.$$

Let A_i be the i-th column of A. Take A' to be the $m\times(n+1)$ matrix $(A_1\dots A_n-b)$. We know how to compute the semigroup S' of nonnegative solutions of the homogeneous system of linear equations:

$$A'\begin{pmatrix} x_1\\ \vdots\\ x_n\\ x_{n+1}\end{pmatrix}=0.$$

Let $\{m_1,\dots,m_r\}$ be the minimal system of generators of S' ($\mathrm{Minimals}_{\leq}(S'\setminus\{0\})$). Rearranging this set, we can assume that $m_1,\dots,m_s$ are the elements in $\{m_1,\dots,m_r\}$ having the last coordinate equal to zero and that the elements $m_{s+1},\dots,m_t$ are the elements in $\{m_1,\dots,m_r\}$ with the last coordinate equal to one.

- If $t=s$, then there is no element in S' such that its last coordinate is one and therefore $Ax=b$ has no solution.
- If $s<t$, then the set of solutions is

$$\bigcup_{i=s+1}^{t}\overline{m}_i+S,$$

where $\overline{m}_i$ is the projection of m_i onto its first n coordinates and S is the affine semigroup generated by $\{\overline{m}_1,\dots,\overline{m}_s\}$. The elements of S are the solutions of the

homogeneous system $Ax = 0$ and the elements $\overline{m}_{s+1}, \dots, \overline{m}_t$ are the "particular" solutions of the system of equations $Ax = b$. If $S = \{0\}$ ($s = 0$), then the system of equations $Ax = b$ has finitely many nonnegative integer solutions.

EXAMPLE 7.7. Assume that we want to know in how many ways we can pay 19 dollars with 1 dollar and 5 dollars bank notes. We must compute the set of nonnegative integer solutions of the equation

$$x + 5y = 19.$$

First, we have to solve the homogeneous equation

$$x + 5y - 19z = 0.$$

Using the method outlined in the first section, we must look in the region

$$\{(x,y,z) \in \mathbb{N}^3 \mid x + y + z \leq 26\}.$$

The solutions of the equation $x + 5y - 19z = 0$ in this region are

$$\{(4,3,1),(3,7,2),(9,2,1),(2,11,3),(8,6,2),(14,1,1),(1,15,4),$$

$$(7,10,3),(13,5,2),(19,0,1),(0,19,5),(6,14,4),(12,9,3),(18,4,2)\}.$$

As expected, there are finitely many solutions and these are

$$\{(4,3),(9,2),(14,1),(19,0)\}.$$

Observe that if we have an equation with nonnegative coefficients, then a better bound is found if we divide the independent term by the least positive coefficient of the equation (in this case $19/1 = 19$). ◇

4. Normal affine semigroups

The monoid $S \subseteq \mathbb{N}^r$ is **normal** if for every $g \in \mathbf{G}(S)$, $kg \in S$ for some $k \in \mathbb{N} \setminus \{0\}$ implies that $g \in S$. Define

$$\mathbf{L}_{\mathbb{Q}_0^+}(S) = \left\{ \sum_{i=1}^{n} q_i s_i \mid n \in \mathbb{N},\ q_i \in \mathbb{Q},\ q_i \geq 0 \text{ and } s_i \in S \right\}.$$

It is easy to prove that S is normal if and only if $S = \mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S)$. In addition, if $S = \langle n_1, \dots, n_p \rangle$, then $\mathbf{G}(S) = \mathbf{G}(\{n_1, \dots, n_p\})$ and $\mathbf{L}_{\mathbb{Q}_0^+}(S) = \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1, \dots, n_p\})$. The question is, once we know $n_1, \dots, n_p$, how can we decide whether S is normal? The key to a solution of this problem is in the following result.

PROPOSITION 7.8. *Let $\{n_1, \dots, n_p\} \subseteq \mathbb{N}^r$. The monoid*

$$\mathbf{G}(\{n_1, \dots, n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1, \dots, n_p\})$$

has a system of generators contained in the set

$$\left\{ n \in \mathbb{N}^r \mid n \leq \sum_{i=1}^{p} n_i \right\}.$$

PROOF. Take $x \in \mathbf{G}(\{n_1,\dots,n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\})$. Then $x = \sum_{i=1}^p q_i n_i$ with $q_i \in \mathbb{Q}$ and $q_i \geq 0$ for all i. If there exists $i_1 \in \{1,\dots,p\}$ such that $q_{i_1} \geq 1$, define $x_1 = x - n_{i_1}$. Note that $x_1 < x$ and

$$x_1 = \sum_{i=1, i\neq i_1}^{p} q_i n_i + (q_{i_1} - 1) n_{i_1} \in \mathbf{G}(\{n_1,\dots,n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\}).$$

If $x_1 \notin \{n \in \mathbb{N}^r \mid n \leq \sum_{i=1}^p n_i\}$, then there exists $i_2 \in \{1,\dots,p\}$ such that

$$x_2 = x_1 - n_{i_2} \in \mathbf{G}(\{n_1,\dots,n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\}).$$

By Corollary 5.3, the process must stop, and when it does $x_k \in \{n \in \mathbb{N}^r \mid n \leq \sum_{i=1}^p n_i\}$. This sequence yields an expression of the form

$$x = \sum_{j=1}^{k-1} n_{i_j} + x_k$$

and therefore

$$x \in \left\langle \left\{ n \in \mathbb{N}^r \mid n \leq \sum_{i=1}^p n_i \right\} \cap \mathbf{G}(\{n_1,\dots,n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\}) \right\rangle.$$

□

As a consequence of this result, if S is finitely generated, then so is $\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S)$, since the set

$$\left\{ n \in \mathbb{N}^r \mid n \leq \sum_{i=1}^p n_i \right\} \cap \mathbf{G}(\{n_1,\dots,n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\})$$

is finite. This region is bounded by $\sum_{i=1}^p n_i$. Hence we can scan the region and look for the elements n such that $n \in \mathbf{G}(\{n_1,\dots,n_p\}) \cap \mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\})$. Clearly, $n \in \mathbf{G}(\{n_1,\dots,n_p\})$ if and only if n satisfies the equations of $\mathbf{G}(\{n_1,\dots,n_p\})$, and we know how to compute them (Chapter 2). The problem of determining whether n belongs to $\mathbf{L}_{\mathbb{Q}_0^+}(\{n_1,\dots,n_p\})$ is harder. There exist nonnegative elements $q_1,\dots,q_p \in \mathbb{Q}$ such that $n = \sum_{i=1}^p q_i n_i$ if and only if the system of equations

$$(n_1 \dots n_p - n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ x_{n+1} \end{pmatrix} = 0$$

has a nonnegative integer solution with $x_{n+1} \neq 0$. Hence we only have to compute a minimal system of generators of the monoid of nonnegative integer solutions of the above system of equations and see if there is some solution whose last coordinate is not zero (we can use Algorithm MCP as well). With this procedure, we can compute

a minimal system of generators of $\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S)$. After that, we only have to check whether this set is included in S in order to determine whether $S = \mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S)$.

EXAMPLE 7.9. Let

$$S = \langle (2,0),(1,1),(0,2) \rangle.$$

The elements $(1,0)$ and $(0,1)$ are in $\mathbf{L}_{\mathbb{Q}_0^+}(\{(2,0),(1,1),(0,2)\})$, which implies that

$$\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S) = \mathbf{G}(S) \cap \mathbb{N}^2.$$

Hence we must look in the set $\{(x,y) \in \mathbb{N}^2 \mid (x,y) \leq (3,3)\}$ for elements belonging to $\mathbf{G}(S)$. A defining equation of $\mathbf{G}(S)$ is $x - y \equiv 0 \pmod 2$. Thus the set

$$\{(0,0),(1,1),(2,2),(3,3),(2,0),(0,2),(3,1),(1,3)\} =$$

$$= \{(x,y) \in \mathbb{N}^2 \mid (x,y) \leq (3,3)\} \cap \mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S) =$$

$$= \{(x,y) \in \mathbb{N}^2 \mid (x,y) \leq (3,3)\} \cap \mathbf{G}(S)$$

is a system of generators of $\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S)$. Since this set is contained in S, we deduce that $\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S) \subseteq S$ and consequently $\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S) = S$. Therefore S is normal.

EXAMPLE 7.10. Let

$$S = \langle (2,0),(1,1),(0,3) \rangle.$$

In this case, $(1,0),(0,1) \in \mathbf{L}_{\mathbb{Q}_0^+}(S)$ and $\mathbf{G}(S) = \mathbb{Z}^2$. Since $(1,0) \in (\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S)) \setminus S$, the monoid S is not normal.

Remarks

Theorem 7.2 is due to Pottier (see **[36]**). The results presented here appear in **[18]**, **[47]** and in **[50]**, though the bound used there is not Pottier's bound but a bound that appears in **[59]** and **[60]** for the degree of the elements of a universal Gröbner basis of ideals associated to subsemigroups of $\mathbb{Z}^n$.

The method introduced here to solve systems of Diophantine equations is useful from the theoretical point of view. However, in practice, it turns out to be very inefficient. If the reader is looking for an efficient algorithm for finding the set of nonnegative integer solutions of systems of linear Diophantine equations, we strongly recomend the algorithm presented in **[11]**.

Hochster in **[26]** introduces the concept of full affine semigroup and proves that they characterize, up to isomorphism, normal affine semigroups. The concept of normal affine semigroup turns out to be the same as the concept of affine semigroup with divisor-theory (see **[33]**). It seems that the first clue of the idea of full and normal semigroup appears in the papers **[7]** and **[8]**. From the point of view of semigroup rings the importance of this kind of semigroup is the following. If S is a normal affine

semigroup, then $K[S]$ is normal (Noetherian and algebraically closed in its fraction field). Hochster proves in **[26]** that in this case $K[S]$ is also Cohen-Macaulay.

Exercises

1. Show that the submonoid of $\mathbb{N}^4$ spanned by $\{(0,1,0,1),(5,0,2,3)\}$ is full.
2. Compute a minimal system of generators of $S = M \cap \mathbb{N}^2$ where M is given by the equation
$$x+y \equiv 0 \pmod 3.$$
3. Find the set of nonnegative integer solutions of the system of equations
$$\begin{aligned} 2x+3y-4z &= 1, \\ x-3y+2z &= 0. \end{aligned}$$
4. Is the submonoid of $\mathbb{N}^3$ spanned by $\{(2,0,1),(3,0,1),(2,2,1)\}$ normal?
5. Compute a minimal system of generators of
$$\mathbf{L}_{\mathbb{Q}_0^+}(\{(2,1),(0,1)\}) \cap \mathbf{G}(\{(2,1),(0,1)\}).$$
6. Show that every full affine semigroup is normal.
7. Prove that the submonoid of $\mathbb{N}^2$ generated by
$$\{(0,1),(1,1)\}$$
is normal but not full.
8. Let
$$S_1 = \langle (0,3),(2,1)\rangle,\ S_2 = \langle (2,0),(1,2)\rangle.$$
Compute a minimal system of generators of $S_1 \cap S_2$.
9. Prove that the property of being normal is preserved under isomorphisms.
10. Find a full affine semigroup isomorphic to
$$\langle (0,1),(1,1)\rangle \subseteq \mathbb{N}^2.$$
Conclude that the property of being full is not preserved under isomorphisms.
11. Determine all full submonoids of $\mathbb{N}$.
12. Determine all normal submonoids of $\mathbb{N}$.
13. Let S be the monoid $((1,1)+\mathbb{N}^2) \cup \{(0,0)\}$. Prove that S is not finitely generated and that $\mathbf{G}(S) \cap \mathbf{L}_{\mathbb{Q}_0^+}(S) = S$.

CHAPTER 8

Computing presentations of finitely generated cancellative monoids

In this chapter we use the acquired knowledge for finding nonnegative integer solutions of systems of homogeneous equations in order to give a procedure for computing a presentation of a given finitely generated cancellative monoid. As a consequence of this procedure, we are able to decide whether a finitely generated monoid given by a presentation is cancellative.

1. Primitive elements of a congruence

The main result of this section is that a congruence on $\mathbb{N}^n$, associated to a cancellative monoid, is generated by its primitive elements. Before introducing the concept of primitive element of a congruence, we must familiarize ourselves with the irreducible elements of a congruence. An element (a,b) in a congruence σ on $\mathbb{N}^n$ is **irreducible** if it cannot be expressed as $(a,b) = (a_1,b_1) + (a_2,b_2)$, with $(a_1,b_1),(a_2,b_2) \in \sigma \setminus \{(0,0)\}$. Denote by $\mathfrak{I}_\sigma$ the set of irreducible elements of σ. Observe that σ can be considered as a submonoid of $\mathbb{N}^n \times \mathbb{N}^n$, since $(0,0) \in \sigma$ and if $(a,b),(c,d) \in \sigma$, then $(a+c,b+d) \in \sigma$. The set of irreducible elements of a congruence is the minimal system of generators of the congruence considered as a monoid.

PROPOSITION 8.1. *Let σ be a congruence on $\mathbb{N}^n$. Then σ is generated, as a submonoid of $\mathbb{N}^n \times \mathbb{N}^n$, by $\mathfrak{I}_\sigma$.*

PROOF. Take (a,b) to be an element in σ. Since $\mathbb{N}^n \times \mathbb{N}^n = \mathbb{N}^{2n}$, we can fix a linear admissible order $\preceq$ on $\mathbb{N}^n \times \mathbb{N}^n$ and use induction on (a,b).

- If $(a,b) = (0,0)$, then $(a,b) = (0,0) \in \langle \mathfrak{I}_\sigma \rangle$.
- Assume that for every $(a',b') \prec (a,b)$, we have that $(a',b') \in \langle \mathfrak{I}_\sigma \rangle$. If (a,b) is irreducible, then $(a,b) \in \mathfrak{I}_\sigma \subseteq \langle \mathfrak{I}_\sigma \rangle$. Otherwise, there exists (a_1,b_1), $(a_2,b_2) \in \sigma \setminus \{(0,0)\}$ such that $(a,b) = (a_1,b_1) + (a_2,b_2)$. Since $\preceq$ is admissible, we have that $(a_1,b_1) \prec (a,b)$ and $(a_2,b_2) \prec (a,b)$. Applying the induction hypothesis, we obtain $(a_1,b_1),(a_2,b_2) \in \langle \mathfrak{I}_\sigma \rangle$ and therefore $(a,b) = (a_1,b_1) + (a_2,b_2) \in \langle \mathfrak{I}_\sigma \rangle$.

□

The following result shows that if $\mathbb{N}^n/\sigma$ is cancellative, then σ is a finitely generated submonoid of $\mathbb{N}^n \times \mathbb{N}^n$.

PROPOSITION 8.2. *Let σ be a congruence on $\mathbb{N}^n$ such that $\mathbb{N}^n/\sigma$ is cancellative. Then $\mathfrak{I}_\sigma$ is finite.*

PROOF. If we prove that

$$\mathfrak{I}_\sigma \subseteq \text{Minimals}_{\leq}(\sigma \setminus \{0,0\}),$$

then using Dickson's Lemma the set $\mathfrak{I}_\sigma$ is finite. Let (a,b) be an element in $\mathfrak{I}_\sigma$. Assume that (a,b) is not a minimal element of $\sigma \setminus \{(0,0)\}$. By Corollary 5.4, there exists $(a_1,b_1) \in \text{Minimals}_{\leq}(\sigma \setminus \{0,0\})$ such that $(a_1,b_1) < (a,b)$. Hence $(a,b) = (a_1,b_1) + (a_2,b_2)$ with $(a_2,b_2) = (a-a_1, b-b_1) \in \mathbb{N}^n \times \mathbb{N}^n$. Since $(a,b) = (a_1+a_2, b_1+b_2) \in \sigma$ and $(b_1,a_1) \in \sigma$, we have that $(a_2+(a_1+b_1), b_2+(a_1+b_1)) \in \sigma$. By hypothesis, $\mathbb{N}^n/\sigma$ is cancellative and this implies that from the equality

$$[a_2+(a_1+b_1)]_\sigma = [a_2]_\sigma + [a_1+b_1]_\sigma = [b_2]_\sigma + [a_1+b_1]_\sigma = [b_2+(a_1+b_1)]_\sigma$$

we obtain that $[a_2]_\sigma = [b_2]_\sigma$. Thus $(a_2,b_2) \in \sigma$, which means that $(a,b) \notin \mathfrak{I}_\sigma$. The contradiction comes from the assumption $(a,b) \notin \text{Minimals}_{\leq}(\sigma \setminus \{0,0\})$. □

In the proof of Proposition 8.2, we do not need to show that the inclusion

$$\text{Minimals}_{\leq}(\sigma \setminus \{0,0\}) \subseteq \mathfrak{I}_\sigma$$

holds as well. The reader can prove this inclusion easily. Hence

$$\mathfrak{I}_\sigma = \text{Minimals}_{\leq}(\sigma \setminus \{0,0\}).$$

If the monoid $\mathbb{N}^n/\sigma$ is not cancellative, then the set $\mathfrak{I}_\sigma$ may have infinitely many elements. Take, for instance, $\sigma = \langle (2,1) \rangle \subseteq \mathbb{N} \times \mathbb{N}$; it is straightforward to show that the elements of the form $(n,1)$, with $n > 0$, are irreducible elements of σ.

Let σ be a congruence on $\mathbb{N}^n$ and τ be the congruence generated by $\mathfrak{I}_\sigma$. Since $\mathfrak{I}_\sigma \subseteq \sigma$, we have that $\tau \subseteq \sigma$. In addition, if $(a,b) \in \sigma$, by Proposition 8.2, we have that there exist $(a_1,b_1), \ldots, (a_s,b_s) \in \mathfrak{I}_\sigma$ such that

$$(a,b) = \sum_{i=1}^{s} (a_i,b_i).$$

Hence $(a,b) \in \tau$, since $(a_i,b_i) \in \tau$ and τ is a congruence on $\mathbb{N}^n$ (every congruence on $\mathbb{N}^n$ is a submonoid of $\mathbb{N}^n \times \mathbb{N}^n$). This means that the congruence σ is generated, as a congruence, by its irreducible elements. Observe that the elements of the form (a,a) are always in the congruence generated by any subset of σ and consequently, we can remove them from a system of generators. In this way, we say that the element $(a,b) \in \sigma$ is **primitive** if it is irreducible and $a \neq b$. The set of primitive elements of σ is denoted by $\mathfrak{P}_\sigma$. We have shown the following result.

PROPOSITION 8.3. *Let σ be a congruence on $\mathbb{N}^n$. Then σ is generated, as a congruence, by $\mathfrak{P}_\sigma$.*

For the cancellative case, the connection between $\mathfrak{I}_\sigma$ and $\mathfrak{P}_\sigma$ is the following.

PROPOSITION 8.4. *Let σ be a congruence on $\mathbb{N}^n$ such that $\mathbb{N}^n/\sigma$ is cancellative. Then*

1. *for every $(a,b) \in \mathfrak{P}_\sigma$, the dot product ab is zero,*
2. $\mathfrak{I}_\sigma \subseteq \mathfrak{P}_\sigma \cup \{(e_1,e_1), \ldots, (e_n,e_n)\}$.

PROOF. If (a,b) is a primitive element and $ab \neq 0$, then there exists $i \in \{1,\dots,n\}$ such that the i-th coordinates of a and b are nonzero. Hence $(a,b)-(e_i,e_i) = (c,d) \in \mathbb{N}^n \times \mathbb{N}^n \setminus \{(0,0)\}$. Since

$$[c]_\sigma + [e_i]_\sigma = [c+e_i]_\sigma = [a]_\sigma = [b]_\sigma = [d+e_i]_\sigma = [d]_\sigma + [e_i]_\sigma$$

and $\mathbb{N}^n/\sigma$ is cancellative, we have that $[c]_\sigma = [d]_\sigma$; in other words, $(c,d) \in \sigma$. Thus $(c,d) < (a,b)$, which is contradicts the fact that (a,b) is primitive (and consequently irreducible).

Now, take $(a,b) \in \mathfrak{I}_\sigma \setminus \mathfrak{P}_\sigma$. Then $a = b$ and since (a,b) is irreducible, $a = e_i$ for some $i \in \{1,\dots,n\}$. □

2. Computing presentations of finitely generated cancellative monoids

We know that a congruence is generated by its primitive elements. Thus for computing a presentation of a cancellative monoid, it suffices to find the set of primitive elements of its associated congruence. Assume that S is a cancellative monoid, that is to say, S is of the form $\mathbb{N}^n/\sim_M$ for some subgroup M of $\mathbb{Z}^n$. By Proposition 3.1, the monoid S is isomorphic to the monoid spanned by the columns of the equations of M.

First, we study the case when the equations of M are homogeneous. This is the case when S is isomorphic to a submonoid of $\mathbb{Z}^r$ for some positive integer r. Assume that the equations of M are

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0, \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0. \end{aligned}$$

An element $(a,b) \in \mathbb{N}^n \times \mathbb{N}^n$ belongs to $\sim_M$ if and only if $a-b \in M$, that is, the element $a-b$ satisfies the equations of M. If we want to compute a presentation of S, we must compute a system of generators of $\sim_M$. By Proposition 8.3, it is enough to compute the set of primitive elements of $\sim_M$. The following result tells us where to look for primitive elements of $\sim_M$.

THEOREM 8.5. *Let M be a homogeneous subgroup of $\mathbb{Z}^n$ with defining equations*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0, \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0. \end{aligned}$$

If $((a_1,\dots,a_n),(b_1,\dots,b_n)) \in \mathfrak{P}_{\sim_M}$, then

$$\sum_{i=1}^{n}(a_i+b_i) \leq \prod_{i=1}^{r}(1+\sum_{j=1}^{n}|a_{ij}|).$$

PROOF. Take $((a_1,\dots,a_n),(b_1,\dots,b_n)) \in \mathfrak{P}_{\sim_M}$. By Proposition 8.4, we have that $\sum_{i=1}^n a_ib_i = 0$. Hence

$$\{i \mid a_i \neq 0\} \cap \{i \mid b_i \neq 0\} = \emptyset.$$

We can assume, in order to simplify the notation, that

$$\{i \mid a_i \neq 0\} \subseteq \{1,\dots,k\} \text{ and } \{i \mid b_i \neq 0\} \subseteq \{k+1,\dots,n\}.$$

Since $(a,b) \in \sim_M$, $a-b \in M$ which means that the element $(a_1,\dots,a_k,b_{k+1},\dots,b_n) \in \mathbb{N}^n$ is a solution of the system of equations

$$\begin{array}{rcl} a_{11}x_1+\cdots+a_{1k}x_k \;+\; (-a_{1(k+1)})x_{k+1}+\cdots+(-a_{1n})x_n & = & 0, \\ & \vdots & \\ a_{r1}x_1+\cdots+a_{rk}x_k \;+\; (-a_{r(k+1)})x_{k+1}+\cdots+(-a_{rn})x_n & = & 0. \end{array}$$

Moreover, this solution is minimal, since otherwise (a,b) would not be a primitive element of $\sim_M$. The proof follows easily using Pottier's theorem (Theorem 7.2). □

If we want to compute a system of generators of $\sim_M$, we only have to search in the region

$$\left\{ ((a_1,\dots,a_n),(b_1,\dots,b_n)) \in \mathbb{N}^n \times \mathbb{N}^n \;\middle|\; \begin{array}{c} \sum_{i=1}^n a_ib_i = 0, \\ \sum_{i=1}^n (a_i+b_i) \leq \prod_{i=1}^r (1+\sum_{j=1}^n |a_{ij}|) \end{array} \right\}.$$

Note that this is the same as looking for elements $(x_1,\dots,x_n) \in M$ for which

$$\sum_{i=1}^n |x_i| \leq \prod_{i=1}^r (1+\sum_{j=1}^n |a_{ij}|)$$

and then take $(a,b) \in \sim_M$, where

$$a = (\max\{x_1,0\},\dots,\max\{x_n,0\}) \text{ and } b = (-\min\{x_1,0\},\dots,-\min\{x_n,0\}).$$

Unfortunately this region may be very large, so that computations are, in most cases, difficult to perform by hand.

EXAMPLE 8.6. Let M be the subgroup of $\mathbb{Z}^3$ with defining equations

$$\begin{array}{rcrcrcl} 2x & + & y & & & = & 0, \\ & & y & + & 2z & = & 0. \end{array}$$

Finding a system of generators for $\sim_M$ is equivalent to finding a presentation for the affine semigroup

$$\langle (2,0),(1,1),(0,2) \rangle.$$

The set of elements (x,y,z) in M such that $|x|+|y|+|z| \leq 16$ is

$$\{(1,-2,1),(2,-4,2),(3,-6,3),$$

$$(-1,2,-1),(-2,4,-2),(-3,6,-3)\}.$$

Hence the primitive elements of $\sim_M$ are

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

which means that $\sim_M = \langle ((1,0,1),(0,2,0)) \rangle$. ◇

Now assume that M is not necessarily homogeneous, that is to say, the defining equations of M are of the form

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

Let M' be the subgroup of $\mathbb{Z}^{n+r}$ with defining equations

$$\begin{array}{lcccl} a_{11}x_1+\cdots+a_{1n}x_n & + & d_1x_{n+1} & & = 0, \\ & & & \ddots & \vdots \\ a_{r1}x_1+\cdots+a_{rn}x_n & + & & d_rx_{n+r} & = 0, \\ a_{(r+1)1}x_1+\cdots+a_{(r+1)n}x_n & & & & = 0, \\ & & & & \vdots \\ a_{(r+k)1}x_1+\cdots+a_{(r+k)n}x_n & & & & = 0. \end{array}$$

We know how to compute the set of primitive elements of $\sim_{M'}$. Let us show how to obtain the primitive elements of $\sim_M$ from the set of primitive elements of $\sim_{M'}$.

PROPOSITION 8.7. *Let $\pi : \mathbb{N}^{n+r} \to \mathbb{N}^n$ be the projection onto the first n coordinates. If (a,b) is a primitive element of $\sim_M$, then there exists a primitive element (a',b') in $\sim_{M'}$ such that $(a,b) = (\pi(a'),\pi(b'))$.*

PROOF. Since $(a,b) \in \sim_M$, by the definition of M', there exists $(x,y) \in \sim_{M'}$ such that $(\pi(x),\pi(y)) = (a,b)$. Choose $(a',b') \in \sim_{M'}$ minimal (with respect to $\leq$) among the elements verifying that $(\pi(x),\pi(y)) = (a,b)$ (note that, by the minimality of (a',b'), $a'b' = 0$). We show that (a',b') is a primitive element in $\sim_{M'}$. Assume that $(a',b') = (x,y)+(z,t)$, with $(x,y),(z,t) \in \sim_{M'} \setminus \{(0,0)\}$. Then $(a,b) = (\pi(x),\pi(y))+(\pi(z),\pi(t))$. Since (a,b) is primitive, we get that $(\pi(x),\pi(y)) = (0,0)$ or $(\pi(z),\pi(t)) = (0,0)$. Suppose, without loss of generality, that $(\pi(x),\pi(y)) = (0,0)$. Thus (x,y) is of the form

$$((0,\ldots,0,x_{n+1},\ldots,x_{n+r}),(0,\ldots,0,y_{n+1},\ldots,y_{n+r})).$$

Since $(x,y) \neq (0,0)$, there exists j such that $x_{n+j} \neq 0$ or $y_{n+j} \neq 0$. Assume that $x_{n+j} \neq 0$. The fact that $a'b' = 0$ implies that $xy = 0$. Thus $y_{n+j} = 0$. In addition, $(x,y) \in \sim_{M'}$ and this implies that $x-y \in M'$, which yields $d_j(x_{n+j}-y_{n+j}) = 0$. Hence $d_jx_{n+j} = 0$, which leads to $x_{n+j} = 0$. But this contradicts the assumption $x_{n+j} \neq 0$. Assuming that $y_{n+j} \neq 0$, we again get a contradiction. Therefore (a',b') is primitive and $(a,b) = (\pi(a'),\pi(b'))$. □

Using this result together with Theorem 8.5 we obtain the following consequence.

COROLLARY 8.8. *Let M be a subgroup of $\mathbb{Z}^n$ with defining equations*

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

and let $((a_1,\dots,a_n),(b_1,\dots,b_n))$ be a primitive element of $\sim_M$. Then

$$\sum_{i=1}^{n}(a_i+b_i) \le \prod_{i=1}^{r}(1+|d_i|+\sum_{j=1}^{n}|a_{ij}|)\prod_{i=r+1}^{r+k}(1+\sum_{j=1}^{n}|a_{ij}|).$$

From the definition of a canonical system of generators of a congruence, each of its elements is primitive and consequently Corollary 8.8 provides a "bound" for them.

3. Deciding whether a monoid is cancellative

Let S be a monoid given by a presentation $\rho \subset \mathbb{N}^n \times \mathbb{N}^n$, that is to say, S is isomorphic to $\mathbb{N}^n/\langle\rho\rangle$. Let σ be the congruence generated by ρ. By Proposition 1.4, S is cancellative if and only if $\sigma = \sim_{M_\sigma}$. The only result we know so far that enables us to check whether two congruences are the same is Proposition 6.13, but if we want to use it, we need a system of generators of σ and a system of generators of $\sim_{M_\sigma}$. Thus the problem of deciding whether S is cancellative can be solved once we know a system of generators of $\sim_{M_\sigma}$. Assume that

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

Then

$$M_\sigma = \mathbf{G}(\{a_1-b_1,\dots,a_t-b_t\})$$

and consequently we can compute the equations of M_σ (see Chapter 2). Once we have the equations of M_σ, we can use the procedure presented in Section 2 for computing a system of generators of $\sim_{M_\sigma}$.

EXAMPLE 8.9. Let S be the monoid given by the presentation

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

The group M_σ ($\sigma = \langle\rho\rangle$ as usual) is generated by $(3,-2)$ and its defining equation is

$$2x_1+3x_2 = 0.$$

Hence $\mathbb{N}^2/\sim_{M_\sigma}$ is isomorphic to the submonoid of $\mathbb{N}$ generated by $\{2,3\}$. Computing a system of generators for $\sim_{M_\sigma}$, we obtain

$$\sim_{M_\sigma} = \langle((3,0),(0,2))\rangle = \langle\rho\rangle.$$

Therefore S is cancellative. ◇

EXAMPLE 8.10. Let S be the monoid $\mathbb{N}^3/\langle\rho\rangle$, where

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

The group M_σ ($\sigma = \langle\rho\rangle$) is generated by $\{(1,-1,1),(2,0,0)\}$ and its defining equations are

$$\begin{aligned} x_1 + x_2 &\equiv 0 \pmod 2, \\ x_2 + x_3 &= 0. \end{aligned}$$

The bound of Corollary 8.8 is $5 \times 3 = 15$. The primitive elements of $\sim_M$ are

$$\{((2,0,0),(0,0,0)),((0,0,0),(2,0,0)),((1,1,0),(0,0,1)),((0,0,1),(1,1,0)),$$

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

Hence a system of generators of $\sim_M$ is

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

Finally, we apply Proposition 6.13 for determining whether $\sigma = \sim_{M_\sigma}$. If we apply Algorithm CPC to ρ for the linear admissible order $\preceq_{tdeg}$ (see Chapter 6), we obtain

$$\{((2,1,2),(0,2,1)),((2,2,1),(0,2,3)),((3,1,1),((1,1,3)),$$

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

The set τ is already a canonical system of generators for $\sim_M$ with respect to the ordering $\preceq_{tdeg}$. Thus $\sigma \neq \sim_{M_\sigma}$ and consequently S is not cancellative. ◇

Once we know that a given monoid is cancellative, we can use the results presented in Chapter 3 for determining whether it is reduced, torsion free, affine, etc.

Remarks

Sturmfels gives in **[59]** and **[60]** a bound for the primitive elements of the kernel congruence associated to a finitely generated submonoid of $\mathbb{Z}^n$. Using this bound as starting point, in **[56]** we give an algorithm to compute a presentation of any finitely generated cancellative monoid, and therefore a procedure to determine whether a finitely generated monoid is or is not cancellative. The results/algorithms exposed in this chapter are fitted to use the bound that is derived from Theorem 7.2.

Exercises

1. Let M be the subgroup of $\mathbb{Z}^3$ with defining equation

$$x + y - z \equiv 0 \pmod 2.$$

   Compute a system of generators of $\sim_M$.

2. Let σ be the congruence on $\mathbb{N}^3$ generated by

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

   (a) Prove that $\mathbb{N}^3/\sigma$ is a cancellative monoid.
   (b) Show that $\mathbb{N}^3/\sigma$ is an affine monoid.

3. Let σ be the congruence on $\mathbb{N}^3$ generated by
$$\{((4,0,0),(0,1,2)),((0,2,0),(1,0,1))\}.$$
Show that $\mathbb{N}^3/\sigma$ is not cancellative.
4. Let M be a subgroup of $\mathbb{Z}^n$. Prove that if ρ is a canonical system of generators of $\sim_M$, then every element in ρ is primitive. (Thus, Corollary 8.8, gives a bound for the "total degree" of the elements belonging to any canonical system of generators of $\sim_M$.)
5. Let M be a subgroup of $\mathbb{Z}^n$. Prove that the union of all canonical systems of generators of $\sim_M$ has finitely many elements.
6. Let σ be the congruence generated by $\{(2,1)\}$. Show that
   (a) $\mathbb{N}^n/\sigma$ is a torsion free reduced monoid,
   (b) σ is not finitely generated as a submonoid of $\mathbb{N}\times\mathbb{N}$.
7. Let M be a subgroup of $\mathbb{Z}^n$ and let ρ be a system of generators of $\sim_M$. Prove that, in general, the inclusion $\mathfrak{P}_{\sim_M} \subseteq \rho \cup \rho^{-1}$ does not hold.
8. Prove that if σ_1 and σ_2 are congruences on $\mathbb{N}^n$ which are finitely generated as monoids, then $\sigma_1 \cap \sigma_2$ is a congruence on $\mathbb{N}^n$ finitely generated as a monoid.
9. Let σ_1 and σ_2 be congruences of $\mathbb{N}^n$. Show that, in general, $\sigma_1 + \sigma_2$ is not a congruence on $\mathbb{N}^n$.
10. Show that
$$\{((3,0,0),(0,1,1)),((0,2,0),(1,0,1)),((0,0,2),(2,1,0))\}$$
is a presentation of the submonoid of $\mathbb{N}$ spanned by $\{3,4,5\}$.
11. Compute a presentation of the submonoid of $\mathbb{Z}_3 \times \mathbb{N}$ generated by the set
$$\{([1],3),([2],4),([1],5)\}.$$

CHAPTER 9

Minimal presentations of finitely generated cancellative reduced monoids

We have already shown that every finitely generated monoid is finitely presented (Chapter 5). Moreover, using the results presented in Chapter 8, we can compute a presentation of a given finitely generated cancellative monoid. Here we are concerned with the problem of characterizing minimal presentations of finitely generated cancellative reduced monoids. Let S be the monoid generated by $\{s_1, \dots, s_p\}$ and ρ be a presentation of S (recall that this means that S is isomorphic to $\mathbb{N}^p/\langle\rho\rangle$). We could say that ρ is a **minimal presentation** (with respect to $\{s_1, \dots, s_p\}$) of S if no proper subset of ρ generates σ. But this is not the only possible choice; the meaning of minimal could be interpreted as the fact that ρ has the least possible number of elements among all the systems of generators of σ. Hence we can distinguish between minimal presentations with respect to inclusion and with respect to their cardinality. We shall prove that these two concepts coincide for cancellative reduced monoids and that there are monoids for which these two concepts are not the same. In the second part of this chapter we particularize the characterization of minimal presentations to affine semigroups. We show that there are affine semigroups with a fixed number of generators and with as many elements in its minimal presentations as we like.

1. Characterization of minimal presentations of finitely generated cancellative reduced monoids

Let S be a nontrivial finitely generated cancellative reduced monoid. Since S is cancellative, S is of the form $\mathbb{N}^n/\sim_M$ (see Chapter 3) and S is isomorphic to the submonoid spanned by the "columns" of the equations of M. Moreover, since S is reduced, M admits an equation with all its coefficients greater than zero, which allows us to obtain an equivalent system of equations of M with all its coefficients greater than or equal to zero. Hence we can suppose that, up to isomorphism, S is of the form,

$$S = \langle m_1, \dots, m_n\rangle \subseteq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{N}^k.$$

We define

$$\varphi : \mathbb{N}^n \to S,\ \varphi(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i m_i,$$

and denote, as usual, the congruence kernel of this morphism by σ. In this setting, the sets $\varphi^{-1}(x)$ are finite for all $x \in S$. This turns out to be the key result of this section.

LEMMA 9.1. *For every $x \in S$, the set $\varphi^{-1}(x)$ is finite.*

PROOF. The property is clearly true for every submonoid of $\mathbb{N}$ and, by extension, also for every submonoid of $\mathbb{N}^k$. If S is a reduced submonoid of $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{N}^k$, $x \in S$ and $\pi(x)$ represents the projection of x onto its last k coordinates (which is always nonzero, since S is reduced), then $\varphi^{-1}(x) \subseteq \varphi^{-1}(\pi(x))$, where the first φ map is referred to S and the second one to its affine component as a submonoid of $\mathbb{N}^k$. From these observations the lemma follows easily. □

Define the following binary relation on $\mathbb{N}^n$:

$$a \mathcal{R} b \text{ if } a = b = 0 \text{ or there exist } x \in S \text{ and } c_1, \dots, c_t \in \varphi^{-1}(x) \text{ such that } c_1 = a,\ c_t = b \text{ and } c_i c_{i+1} \neq 0 \text{ for every } i = 1, \dots, t-1$$

(here $c_i c_{i+1}$ denotes, as usual, the dot product on $\mathbb{N}^n$). Clearly $\mathcal{R}$ is an equivalence relation on $\mathbb{N}^n$ and $\mathcal{R} \subseteq \sigma$.

Let X be a set, $\mathcal{P} = \{B_1, \dots, B_t\}$ be a partition of X and ρ be a binary relation on X. We define the graph G_ρ associated to ρ with respect to the partition $\mathcal{P}$ as the graph whose vertices are $\mathcal{P}$ and the element $\overline{X_i X_j}$, with $i \neq j$, is an edge whenever there exist $x \in X_i$ and $y \in X_j$ such that $(x, y) \in \rho \cup \rho^{-1}$.

PROPOSITION 9.2. *Let $x \in S$ and let $\mathcal{P} = \{X_1, \dots, X_t\}$ be the set of $\mathcal{R}$-classes contained in $\varphi^{-1}(x)$. If ρ is a presentation of S, and $\rho_x = \rho \cap (\varphi^{-1}(x) \times \varphi^{-1}(x))$, then the graph G_{ρ_x} associated to ρ_x with respect to the partition $\mathcal{P}$ of $\varphi^{-1}(x)$ is a connected graph.*

PROOF. We must prove that for any two vertices in G_{ρ_x} there exists a path connecting them.

Assume that $X, Y \in \mathcal{P}$, with $X \neq Y$. Take $a \in X$ and $b \in Y$. Then $(a, b) \in \sigma = \langle \rho \rangle$. By Proposition 5.11, there exist $a_1, \dots, a_h \in \mathbb{N}^n$ such that $a_1 = a$, $a_h = b$ and $(a_i, a_{i+1}) \in \rho_1$ for every $i = 1, \dots, h-1$ (we can suppose that the elements a_i are all different, since $a \neq b$). Hence there exist $(b_i, c_i) \in \rho \cup \rho^{-1}$ and $d_i \in \mathbb{N}^n$ such that $(a_i, a_{i+1}) = (b_i + d_i, c_i + d_i)$. Observe that:

- If $d_i \neq 0$, we have that $b_i + d_i$ and $c_i + d_i$ are in the same $\mathcal{R}$-class, since $\varphi(b_i + d_i) = \varphi(c_i + d_i) = x$ and $(b_i + d_i)(c_i + d_i) \neq 0$.
- If $d_i = 0$, then $(a_i, a_{i+1}) = (b_i, c_i) \in \rho_x \cup \rho_x^{-1}$.

The elements a_i for which $d_i = 0$ determine a path in G_{ρ_x} from X to Y. □

Since every class $[a]_\sigma$ is finite, fixing a linear admissible order $\preceq$ on $\mathbb{N}^n$, we can define the following relation on $\mathbb{N}^n/\sigma$:

$$[a]_\sigma \leq_S [b]_\sigma \text{ if } \max([a]_\sigma) \preceq \max([b]_\sigma).$$

This relation is clearly reflexive and transitive. The antisymmetric property follows from the fact that if $[a]_\sigma \neq [b]_\sigma$, then $[a]_\sigma \cap [b]_\sigma = \emptyset$. Observe also that since $\preceq$ is a well order on $\mathbb{N}^n$, so is $\leq_S$ on $\mathbb{N}^n/\sigma$.

PROPOSITION 9.3. *Let ρ be a subset of σ such that G_{ρ_x} is connected for every $x \in S$. Then ρ is a presentation for S.*

PROOF. We must prove that $\langle\rho\rangle = \sigma$. It suffices to show that for every $a \in \mathbb{N}^n$, we have that $[a]_\sigma \times [a]_\sigma \subseteq \langle\rho\rangle$. Since $\leq_S$ is a well order on $\mathbb{N}^n/\sigma$, we can use induction on $[a]_\sigma$ for the proof.

- For $[a]_\sigma = [0]_\sigma$ the result is clear. Since S is reduced, $[0]_\sigma = \{0\}$ (see Proposition 3.6, we may assume that $(e_i, 0) \notin \sigma = \sim_M$ for all i) and therefore $[0]_\sigma \times [0]_\sigma = \{(0,0)\} \subseteq \langle\rho\rangle$.
- Assume the result is true for the classes in $\mathbb{N}^n/\sigma$ which are less than $[a]_\sigma$ and let us prove it for $[a]_\sigma$. Take $(f,g) \in [a]_\sigma \times [a]_\sigma$.
  1. If $f \mathcal{R} g$, then, by the definition of $\mathcal{R}$, there exist $a_1, \dots, a_t \in [a]_\sigma$ such that $f = a_1$, $g = a_t$ and $a_i a_{i+1} \neq 0$ for every $i = 1, \dots, t-1$. Hence if we want to show that $(f,g) \in \langle\rho\rangle$, it suffices to prove that $(a_i, a_{i+1}) \in \langle\rho\rangle$ for all i. Since $a_i a_{i+1} \neq 0$, there exist $k, \overline{k}, c \in \mathbb{N}^n$, with $c \neq 0$, such that $(a_i, a_{i+1}) = (k, \overline{k}) + (c, c)$. In addition, $S \cong \mathbb{N}^n/\sigma$ is a cancellative monoid, which means that $(k, \overline{k}) \in \sigma$. Since $\preceq$ is admissible, $\max[k]_\sigma \prec \max[k]_\sigma + c$. Moreover, $\max[k]_\sigma + c \in [k+c]_\sigma$, and this leads to $\max[k]_\sigma + c \preceq \max[k+c]_\sigma$. Hence $\max[k]_\sigma \prec \max[k+c]_\sigma = \max[a]_\sigma$, which implies that $[k]_\sigma <_S [a]_\sigma$. Applying the induction hypothesis to $[k]_\sigma$, we obtain that $(k, \overline{k}) \in \langle\rho\rangle$, and consequently $(k+c, \overline{k}+c) = (a_i, a_{i+1}) \in \langle\rho\rangle$.
  2. If $(f,g) \notin \mathcal{R}$, then $[a]_\sigma$ has at least two different $\mathcal{R}$-classes. Let X and Y be the $\mathcal{R}$-classes containing f and g, respectively. Since by hypothesis the graph $G_{\rho_{\varphi(a)}}$ is connected, there exists a path in $G_{\rho_{\varphi(a)}}$ from X to Y. Assume that such path is $X = X_1, X_2, \dots, X_t = Y$. It follows that for every $i = 1, \dots, t-1$ there exists $(a_i, b_i) \in \rho_{\varphi(a)} \cup \rho_{\varphi(a)}^{-1}$ with $a_i \in X_i$ and $b_i \in X_{i+1}$. As the pairs $(f, a_1), (b_t, g), (b_i, a_{i+1})$ belong to $\mathcal{R}$, we can apply the preceding case and deduce that $(f, a_1), (b_t, g), (b_i, a_{i+1}) \in \langle\rho\rangle$. Therefore, $(f,g) \in \langle\rho\rangle$ follows by transitivity.

□

Putting these two results together, we obtain the following statement.

THEOREM 9.4. *Let ρ be a subset of σ. Then ρ is a presentation of S if and only if G_{ρ_x} is connected for each $x \in S$.*

If the number of $\mathcal{R}$-classes of $\varphi^{-1}(x)$ is greater than 1 and we are looking for the least possible (with respect to cardinality) ρ_x such that G_{ρ_x} is connected, then G_{ρ_x} has to be the least connected graph whose vertices are precisely the $\mathcal{R}$-classes in $\varphi^{-1}(x)$ and consequently, G_{ρ_x} must be a tree. Thus if ρ is a minimal (with respect to cardinality) presentation of S, then G_{ρ_x} is a tree for every $x \in S$ such that $\varphi^{-1}(x)$ has more than one $\mathcal{R}$-class.

Observe also that ρ is a minimal (with respect to inclusion) presentation if and only if every edge in the graphs G_{ρ_x}, with $x \in S$ verifying that $\varphi^{-1}(x)$ has more than one $\mathcal{R}$-class, is a bridge, and therefore G_{ρ_x} must be a tree as well.

These two remarks imply that the concepts of minimal presentation with respect to inclusion and cardinality coincide whenever the monoid is finitely generated, cancellative and reduced.

COROLLARY 9.5. *Let S be a finitely generated cancellative reduced monoid and let ρ be a presentation with respect to a given system of generators of S. Then ρ is a minimal presentation of S with respect to inclusion if and only if ρ is a minimal presentation of S with respect to cardinality. Furthermore, two minimal presentations have the same cardinality.*

Unfortunately, removing the condition of being reduced, these two concepts are not the same in general, as the following example shows.

EXAMPLE 9.6. Let

$$S = \langle (0,0,1),(2,1,1),(1,0,3),(-2,-1,3)\rangle \subset \mathbb{Z}\times\mathbb{Z}_2\times\mathbb{Z}_4.$$

Then,

$$\{((2,0,0,0),(0,0,4,2)),((0,1,0,0),(0,0,8,3)),((0,0,0,0),(0,0,8,4))\}$$

and

$$\{((0,0,0,0),(0,1,0,1)),((0,0,0,0),(4,0,0,0)),$$
$$((8,4,0,0),(0,0,8,0)),((10,6,0,0),(0,0,12,0))\}$$

are minimal presentations of S with respect to inclusion. (A system of generators ρ of σ is minimal with respect to inclusion if for every $(x,y)\in\rho$, we have that $\langle\rho\rangle \neq \langle\rho\setminus\{(x,y)\}\rangle$; we can determine whether $\langle\rho\rangle \neq \langle\rho\setminus\{(x,y)\}\rangle$ using Proposition 6.13.)$\diamond$

2. The affine case

As a particularization of the results presented in Section 1, we study minimal presentations of affine semigroups which are finitely generated cancellative reduced torsion free monoids. If S is an affine semigroup, then Theorem 3.11 asserts that we can assume, up to isomorphisms, that S is a finitely generated submonoid of $\mathbb{N}^r$ for some positive integer r. Let $\{n_1,\dots,n_p\}$ be the minimal system of generators of S (see exercises of Chapter 3). For every $n\in S\setminus\{0\}$, define the graph Δ_n whose vertices are

$$\mathrm{V}(\Delta_n) = \{n_i \mid n-n_i\in S\},$$

and whose edges are

$$\mathrm{E}(\Delta_n) = \{\overline{n_in_j} \mid n-(n_i+n_j)\in S\}.$$

The following result illustrates the connection between $\mathcal{R}$-classes and the graphs Δ_n.

PROPOSITION 9.7. *Let $0\neq n\in S$. There is a bijective map between the set of connected components of Δ_n and the set of $\mathcal{R}$-classes of $\varphi^{-1}(n)$.*

PROOF. Take $a \in \mathbb{N}^p$ such that $\varphi(a) = n$. The set of $\mathcal{R}$-classes of $\varphi^{-1}(n)$ is $[a]_\sigma/\mathcal{R}$. Denote by C_n the set of connected components of Δ_n. We define a bijective map $f : C_n \to [a]_\sigma/\mathcal{R}$. Given $C \in C_n$, take n_i to be a vertex in C (note that $\mathrm{V}(\Delta_n) \neq \emptyset$ because $n \neq 0$). Hence $n - n_i \in S$ and thus there exists an element a_i in $[a]_\sigma$ whose i-th coordinate is nonzero. Define $f(C) = [a_i]_\mathcal{R}$. Let us show that f is well defined, that is, it neither depends on the choice of n_i nor on the choice of a_i.

- Take $n_i \neq n_j \in \mathrm{V}(C)$. There must be an element a_j in $[a]_\sigma$ such that its j-th coordinate is nontrivial. Since n_i and n_j are both in C, there must be a path connecting them. Let $n_i = n_{i_0}, \dots, n_{i_t} = n_j$ be this path. As $n - (n_{i_k} + n_{i_{k+1}}) \in S$, for every $k \in \{0, \dots, t-1\}$, there is an element $b_k \in [a]_\sigma$ whose i_k-th and i_{k+1}-th coordinates are greater than zero. Hence

$$a_i, b_0, \dots, b_t, a_j \in \varphi^{-1}(n)$$

and

$$a_i b_i \neq 0,\ b_i b_{i+1} \neq 0,\ b_t a_j \neq 0.$$

Consequently a_i and a_j are in the same $\mathcal{R}$-class.
- Take $a_i' \neq a_i$, $a_i' \in [a]_\sigma$ verifying that its i-th coordinate is not zero. Then $(a_i, a_i') \in \mathcal{R}$, since $a_i a_i' \neq 0$.

Finally, we show that the map f is bijective.

- Injective: Assume that $f(C) = f(C') = [x]_\mathcal{R}$. Hence $\varphi(x) = n$ and since $n \neq 0$, we can choose i so that the i-th coordinate of x is not zero. By the definition of $f(C)$, we have that $n_i \in \mathrm{V}(C)$ and $n_i \in \mathrm{V}(C')$ and this leads to $C = C'$.
- Surjective: Take $[b]_\mathcal{R} \in [a]_\sigma/\mathcal{R}$. Since $a \neq 0$, we have that $b \neq 0$. Let $i \in \{1, \dots, p\}$ be such that the i-th coordinate of b is nonzero. This implies that $n_i \in \mathrm{V}(\Delta_n)$ and that if C is the connected component of Δ_n containing n_i, then clearly $f(C) = [b]_\mathcal{R}$.

□

Using the proof of Proposition 9.7 and Theorem 9.4, it is straightforward to show the following result.

COROLLARY 9.8. *For every $n \in S$, define ρ_n as follows:*

1. *if Δ_n is connected, then $\rho_n = \emptyset$;*
2. *if Δ_n is not connected and $\Delta_n^1, \dots, \Delta_n^t$ are the connected components of Δ_n, then choose a vertex $n_{j_i} \in \mathrm{V}(\Delta_n^i)$ and an element $\alpha_n^i = (a_1^i, \dots, a_p^i) \in \mathbb{N}^p$ such that $\varphi(\alpha_n^i) = n$ and $a_{j_i}^i \neq 0$; set*

$$\rho_n = \{(\alpha_n^2, \alpha_n^1), \dots, (\alpha_n^t, \alpha_n^1)\}.$$

Take $\rho = \bigcup_{n \in S} \rho_n$. Then G_{ρ_n} is a tree for all $n \in \mathbb{N}^p$ and therefore ρ is a minimal presentation for S.

The problem is, of course, that the set

$$\{n \in S \mid \Delta_n \text{ is not connected}\}$$

is not known (it is known to be finite, since any finitely generated monoid is finitely presented). Our next goal is to give a bound for its elements.

Assume that the generators of S can be written as $n_i = (a_{i1}, \dots, a_{ir}) \in \mathbb{N}^r$. By Proposition 3.1, S is isomorphic to $\mathbb{N}^p / \sim_M$, where M is the subgroup of $\mathbb{Z}^r$ with defining equations:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{p1}x_p &= 0, \\ &\vdots \\ a_{1r}x_1 + \ldots + a_{pr}x_p &= 0. \end{aligned}$$

Using Theorem 8.5, we know that if the pair $((a_1, \dots, a_p), (b_1, \dots, b_p))$ is a primitive element, then

$$\sum_{i=1}^{p}(a_i + b_i) \leq \prod_{i=1}^{r}(1 + \sum_{j=1}^{p} |a_{ji}|).$$

Thus either $\sum_{i=1}^{p} a_i \leq \frac{1}{2}\prod_{i=1}^{r}(1 + \sum_{j=1}^{p} |a_{ji}|)$ or $\sum_{i=1}^{p} b_i \leq \frac{1}{2}\prod_{i=1}^{r}(1 + \sum_{j=1}^{p} |a_{ji}|)$.

Clearly, a minimal set of generators of σ is contained in the set of primitive elements of σ. Hence the elements $a_1 n_1 + \cdots + a_p n_p \in S$ such that Δ_n is not connected must verify

$$\sum_{i=1}^{p} a_i \leq \frac{1}{2}\prod_{i=1}^{r}(1 + \sum_{j=1}^{p} |a_{ji}|).$$

The following remarks give rise to an algorithm for computing a minimal presentation of an affine semigroup.

1. As we have just shown, if Δ_n is not connected, then $n = \sum_{i=1}^{p} a_i n_i$, with

$$\sum_{i=1}^{p} a_i \leq \frac{1}{2}\prod_{i=1}^{r}(1 + \sum_{j=1}^{p} |a_{ji}|).$$

   Let

$$A = \{\sum_{i=1}^{p} a_i n_i \mid \sum_{i=1}^{p} a_i \leq \frac{1}{2}\prod_{i=1}^{r}(1 + \sum_{j=1}^{p} |a_{ji}|)\}$$

   and let

$$\Gamma = \{x \in \mathbb{N}^r \mid x \leq a \text{ for some } a \in A\}.$$

   This set contains the elements $n \in S$ such that Δ_n is not connected.
2. Once we have solved the membership (in S) problem for all the elements in this "box" which are smaller (with respect to the lexicographical order) than a certain n, the question of whether n belongs or not to S can be answered in the following way: if $n \in S$, then there exists $i \in \{1, \dots, p\}$ such that $n - n_i \in S$.

Note that $n - n_i \preceq_{lex} n$ and therefore we already know whether $n - n_i$ belongs to S or not.

3. In addition, using the idea exposed in the preceding remark, we get the elements of $\mathrm{V}(\Delta_n)$, because we can check whether $n - n_i \in S$, for any $i \in \{1, \dots, p\}$.
4. Assuming that we know the vertices of the graph associated to the elements of S smaller than $n \in S$ (with respect to the lexicographical order), it is easy to compute the graph Δ_n and its connected components, taking into account the following facts.
   (a) If $n - n_i \in S$, then $\mathrm{V}(\Delta_{n-n_i}) \subseteq \mathrm{V}(\Delta_n)$. Furthermore, $\mathrm{V}(\Delta_{n-n_i})$ is contained in a connected component of Δ_n (the connected component where n_i lies).
   (b) $\mathrm{V}(\Delta_n) = \bigcup_{n-n_i \in S}(\mathrm{V}(\Delta_{n-n_i}) \cup \{n_i\})$.
   (c) If $\mathrm{V}(\Delta_{n-n_i}) \cap \mathrm{V}(\Delta_{n-n_j}) \neq \emptyset$, then $\mathrm{V}(\Delta_{n-n_i})$ and $\mathrm{V}(\Delta_{n-n_j})$ are contained in the same connected component.
   (d) If $\mathrm{V}(\Delta_n) = \{n_{i_1}, \dots, n_{i_k}\}$, define
   $$B_j^0 = \mathrm{V}(\Delta_{n-n_{i_j}}) \cup \{n_{i_j}\},$$
   and
   $$P_n^0 = \{B_1^0, \dots, B_k^0\}.$$
   We construct P_n^l in the following way: if $P_n^{l-1} = \{B_1^{l-1}, \dots, B_{k_{l-1}}^{l-1}\}$ and there exist i, j such that B_i^{l-1}, B_j^{l-1} are not disjoint, then set
   $$P_n^l = \{B_h^{l-1} \mid h \neq i, j\} \cup \{B_i^{l-1} \cup B_j^{l-1}\}.$$
   This process ends when P_n^l is a partition of $\mathrm{V}(\Delta_n)$. It is easy to see that, in this case, the elements in P_n^l are the sets of vertices of the connected components of Δ_n.
5. Once we know the connected components of the graph associated to each element $n \in S \cap \Gamma$, we must construct ρ_n. For this purpose, we must find the tuples α_n^i described in the definition of ρ_n. Assume that $\Delta_n^1, \dots, \Delta_n^{t_n}$ are the connected components of Δ_n. Take $n_{i_1} \in \mathrm{V}(\Delta_n^i)$, then $n - n_{i_1} \in S$. Two cases may occur: $n - n_{i_1} = 0$ and therefore $\alpha_n^i = e_{i_1}$; or $n - n_{i_1} \neq 0$. In the latter case, there exists n_{i_2} such that $(n - n_{i_1}) - n_{i_2} \in S$ (hence $n_{i_2} \in \mathrm{V}(\Delta_n^i)$). This process must stop and when it does we have that $n - \sum_{j=1}^k n_{i_j} = 0$. Thus, $\alpha_n^i = \sum_{j=1}^k e_{i_j}$.

We illustrate this procedure by some examples.

EXAMPLE 9.9. Let
$$S = \langle 3,5,7 \rangle \subseteq \mathbb{N} = \{0,3,5,6,7,\dots\} = \mathbb{N} \setminus \{1,2,4\}.$$
The elements $n = 3a_1 + 5a_2 + 7a_3 \in S$ such that Δ_n is not connected must satisfy
$$a_1 + a_2 + a_3 \leq (1+3+5+7)/2 = 8.$$
The non connected graphs are:

Graph	Connected components	Relators
Δ_{10}	$\{3,7\},\{5\}$	$e_1+e_3=2e_2$
Δ_{12}	$\{3\},\{5,7\}$	$4e_1=e_2+e_3$
Δ_{14}	$\{3,5\},\{7\}$	$3e_1+e_2=2e_3$

Therefore

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

is a minimal presentation of S. In chapters to come, we shall deal again with the problem of computing a presentation of a submonoid of $\mathbb{N}$ and we shall prove that this procedure can be improved. ◇

EXAMPLE 9.10. Let

$$S=\langle(2,0),(0,1),(1,2),(3,1)\rangle\subseteq\mathbb{N}^2.$$

The elements

$$n=a_1(2,0)+a_2(0,1)+a_3(1,2)+a_4(3,1)\in S$$

such that Δ_n is not connected verify the inequality

$$\sum_{i=1}^{4}a_i\leq(7\times5)/2<18.$$

The non connected graphs are:

Graph	Connected components	Relators
$\Delta_{(3,2)}$	$\{(2,0),(1,2)\},\{(0,1),(3,1)\}$	$e_1+e_3=e_2+e_4$
$\Delta_{(6,2)}$	$\{(2,0),(0,1)\},\{(3,1)\}$	$3e_1+2e_2=2e_4$
$\Delta_{(4,3)}$	$\{(2,0),(0,1)\},\{(1,2),(3,1)\}$	$2e_1+3e_2=e_3+e_4$
$\Delta_{(2,4)}$	$\{(2,0),(0,1)\},\{(1,2)\}$	$e_1+4e_2=2e_3$

Hence

$$\begin{aligned}\rho=\ &\{((1,0,1,0),(0,1,0,1)),((3,2,0,0),(0,0,0,2)),\\ &((2,3,0,0),(0,0,1,1)),((1,4,0,0),(0,0,2,0))\}\end{aligned}$$

is a minimal presentation of S. ◇

It may happen that we are not given a minimal system of generators of an affine semigroup and we wish to compute a presentation for this system of generators. The procedure to follow in this case is easy and it is explained in the following example.

EXAMPLE 9.11. Let

$$S=\langle0,3,5,6,7\rangle$$

and assume that we are looking for a presentation for this set of generators of S. First of all, note that the pair $((1,0,0,0,0),(0,0,0,0,0))$ must be in this presentation. This pair is telling us that the first generator is zero. Secondly, since $6 = 2 \times 3$, the pair $((0,0,0,1,0),(0,2,0,0,0))$ must be also in the presentation. Finally, since a presentation of $\langle 3,5,7\rangle$ (which is now a minimal system of generators of S) is

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

we have that

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

is a presentation of S for the system of generators $\{0,3,5,6,7\}$. ◇

We finish this section showing that the cardinal of a minimal presentation for an affine semigroup can not be bounded as a function on the number of generators of the given monoid. Before proving this, we need a technical lemma.

LEMMA 9.12. *Let*

$$S = \langle (2,1),(2n+1,1),(2n+3,1),(0,1)\rangle,$$

with $0 \neq n \in \mathbb{N}$, *and let* $\lambda_1,\lambda_3 \in \mathbb{N}$ *be such that* $0 < \lambda_1+\lambda_3 < 2n+1$. *Then the element* $((\lambda_1,0,\lambda_3,0),(a_1,a_2,a_3,a_4)) \in \sigma$ *if and only if* $(\lambda_1,0,\lambda_3,0) = (a_1,a_2,a_3,a_4)$.

PROOF. Take (λ_1,λ_3) to be an element in $\mathbb{N}^2$ such that $\lambda_1+\lambda_3$ is minimum among the elements in σ of the form $((\lambda_1,0,\lambda_3,0),(a_1,a_2,a_3,a_4))$ with $(\lambda_1,0,\lambda_3,0) \neq (a_1,a_2,a_3,a_4)$. We show that $\lambda_1+\lambda_3 \geq 2n+1$, and to this end, we distinguish three different cases:

Case 1. $\lambda_1 \neq 0$ and $\lambda_3 \neq 0$. By the minimality of $\lambda_1+\lambda_3$ and since $((\lambda_1,0,\lambda_3,0),(a_1,a_2,a_3,a_4)) \in \sigma$, we deduce that $a_1 = a_3 = 0$. Hence

$$\lambda_1(2,1)+\lambda_3(2n+3,1) = a_2(2n+1,1)+a_4(0,1),$$

which implies that

$$2(\lambda_1+\lambda_3) = (2n+1)(a_2-\lambda_3).$$

Since $\gcd(2,2n+1) = 1$, we have that $\operatorname{lcm}(2,2n+1) = 2(2n+1)$. In addition $2(\lambda_1+\lambda_3)$ is a multiple of 2 and $2n+1$, which implies that the least common multiple of 2 and $2n+1$ must be less than or equal to $2(\lambda_1+\lambda_3)$. Therefore $\lambda_1+\lambda_3 \geq 2n+1$.

Case 2. $\lambda_1 \neq 0$ and $\lambda_3 = 0$. As in Case 1, from the minimality of $\lambda_1+\lambda_3 = \lambda_1$, we deduce that $a_1 = 0$ and

$$\lambda_1(2,1) = a_2(2n+1,1)+a_3(2n+3,1)+a_4(0,1).$$

It follows that $2\lambda_1 = a_2(2n+1)+a_3(2n+3)$, which leads to

$$2(\lambda_1-a_3) = (2n+1)(a_2+a_3).$$

If $a_2+a_3=0$, then $\lambda_1=0=a_3$, which is impossible. If $a_2+a_3=1$, then $2(\lambda_1-a_3)=2n+1$ which is in contradiction with the fact that $2(\lambda_1-a_3)$ is even and $2n+1$ is odd. Thus $a_2+a_3>1$, whence

$$2(\lambda_1-a_3)=(a_2+a_3)(2n+1)\geq 2(2n+1).$$

Hence $\lambda_1-a_3\geq 2n+1$ and therefore $\lambda_1=\lambda_1+\lambda_3\geq 2n+1$.

Case 3. $\lambda_1=0$ and $\lambda_3\neq 0$. In this case, using once more the minimality of $\lambda_1+\lambda_3=\lambda_3$, we obtain that $a_3=0$ and

$$\lambda_3(2n+3,1)=a_1(2,1)+a_2(2n+1,1)+a_4(0,1).$$

However, $(2n+3,1)$ cannot be expressed as a linear combination with nonnegative rational coefficients of $\{(2,1),(2n+1,1),(0,1)\}$. Hence this case cannot occur. □

With this strange result, we can prove that a minimal presentation for this particular affine semigroup has at least $2n$ elements, and consequently, there is no general bound for the number of elements in a minimal presentation of an affine semigroup in terms of the cardinality of a minimal system of generators.

PROPOSITION 9.13. *Let*

$$S=\langle(2,1),(2n+1,1),(2n+3,1),(0,1)\rangle,$$

with $0\neq n\in\mathbb{N}$. *Then the cardinality of every presentation of* S *is greater than or equal to* $2n$.

PROOF. Let $\rho=\{(n_1,m_1),\dots,(n_t,m_t)\}$ be a presentation of S. Since for every $k\in\{2,\dots,2n+1\}$ we have

$$k(2,1)+(2n+1-k)(2n+3,1)=(2n+3-k)(2n+1,1)+(k-2)(0,1),$$

the elements $((k,0,2n+1-k,0),(0,2n+3-k,0,k-2))$ are in σ. By Proposition 5.11, there exists a sequence $v_0,\dots,v_l\in\mathbb{N}^4$ such that $v_0=(k,0,2n+1-k,0)$, $v_l=(0,2n+3-k,0,k-2)$ and $(v_i,v_{i+i})\in\rho_1$ for every $i\in\{0,\dots,l-1\}$. Hence there exists $i\in\{1,\dots,t\}$ such that $(k,0,2n+1-k,0)-n_i\in\mathbb{N}^4$ or $(k,0,2n+1-k,0)-m_i\in\mathbb{N}^4$. Without loss of generality, assume that $(k,0,2n+1-k,0)-n_i\in\mathbb{N}^4$, and let $n_i=(a_{i_1},a_{i_2},a_{i_3},a_{i_4})$. Thus $a_{i_2}=a_{i_4}=0$, $a_{i_1}\leq k$ and $a_{i_3}\leq 2n+1-k$, which means that $a_{i_1}+a_{i_3}\leq 2n+1$. Since (n_i,m_i) belongs to a minimal system of generators for σ, we have that $n_i\neq m_i$ and by Lemma 9.12, we get that $a_{i_1}+a_{i_3}\geq 2n+1$, whence $n_i=(k,0,2n+1-k,0)$. Hence $t\geq 2n$, since k ranges from 2 to $2n+1$ in the elements $((k,0,2n+1-k,0),(0,2n+3-k,0,k-2))$. □

Remarks

The idea of characterizing minimal presentations in terms of the connectedness of certain graphs is due to Rosales. In **[40]** and **[44]** he gives a characterization of minimal presentations of numerical semigroups in terms of graphs associated to its elements. After that, the same idea is extended in **[18]** to affine semigroups. Following this line,

in [**6**], a characterization of minimal presentations for finitely generated reduced cancellative monoids is obtained. Finally, in [**55**] those characterizations are generalized for finitely generated monoids which are strongly reduced (they include the class of reduced cancellative monoids). Example 9.6 appears in [**35**].

Exercises

1. Show, by means of an example, that minimal presentations of monoids are not unique.
2. Let S be the submonoid of $\mathbb{N}^2$ spanned by
$$\{(4,0),(2,3),(0,4)\}.$$
Compute a minimal presentation of S.
3. Let S be the submonoid of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{N}$ generated by
$$\{([1]_2,[1]_2,1),([0]_2,[1]_2,1),([1]_2,[0]_2,1)\}.$$
Show that
$$\rho = \{((0,2,0),(2,0,0)),((0,0,2),(2,0,0))\}$$
is a minimal (with respect to cardinality) presentation of S.
4. Let
$$S = \langle (0,1),(2,1),(3,1),(4,1)\rangle \subseteq \mathbb{N}^2.$$
Prove that
$$\rho = \{((0,2,0,0),(1,0,0,1)),((0,0,2,0),(0,1,0,1))\}$$
is a minimal presentation of S.
5. Let $S \subseteq \mathbb{N}^k$ be an affine semigroup minimally generated by $\{n_1,\dots,n_p\}$. Prove that if ρ is a minimal presentation of S, then the cardinality of ρ is greater than or equal to $p-r$, where r is the rank of $\mathbf{G}(\{n_1,\dots,n_p\})$.
6. Let $a_1,b_1,\dots,a_r,b_r \in \mathbb{N}^n$ and let M be the subgroup of $\mathbb{Z}^n$ generated by
$$\{a_1-b_1,\dots,a_r-b_r\}.$$
Prove that $\rho = \{(a_1,b_1),\dots,(a_r,b_r)\}$ is a system of generators of $\sim_M$ if and only if $\mathbb{N}^n/\langle\rho\rangle$ is cancellative.
7. Let M be a subgroup of $\mathbb{Z}^n$ and let $\{m_1,\dots,m_r\}$ be a basis of M such that m_r is strongly positive. Prove that
$$\{(m_1^+,m_1^-),\dots,(m_r^+,m_r^-)\}$$
is a system of generators of $\sim_M$ (see the definition of m^+ and m^- in the proof of Proposition 3.3).
8. Find a basis $\{m_1,\dots,m_r\}$ of a subgroup M of $\mathbb{Z}^n$ such that
$$\{(m_1^+,m_1^-),\dots,(m_r^+,m_r^-)\}$$
is not a system of generators of $\sim_M$ (see the definition of m^+ and m^- in the proof of Proposition 3.3).

9. Let
$$M = \{(x,y,z) \in \mathbb{Z}^3 \mid 4x+6y+7z=0\}.$$
Prove that:
   (a) $\sim_M = \langle((3,0,0),(0,2,0)),((0,0,2),(2,1,0))\rangle$,
   (b) $\{(3,-2,0),(-2,-1,2)\}$ is a basis of M.
10. Let
$$M = \{(x,y,z) \in \mathbb{Z}^3 \mid 5x+6y+7z=0\}.$$
Prove that:
   (a) $\sim_M = \langle((4,0,0),(0,1,2)),((0,2,0),(1,0,1)),((0,0,3),(3,1,0))\rangle$,
   (b) $\{(4,-1,-2),(-1,2,-1),(-3,-1,3)\}$ is not a basis of M.
11. Let M be a subgroup of $\mathbb{Z}^n$ such that $M \cap \mathbb{N}^n = \{0\}$. Show that $\sim_M$ has finitely many minimal systems of generators.
12. Let M be a subgroup of $\mathbb{Z}^n$. Prove that the following statements are equivalent:
   (a) $M \cap \mathbb{N}^n = \{0\}$,
   (b) $[x]_{\sim_M}$ is finite for all $x \in \mathbb{N}^n$,
   (c) $[0]_{\sim_M} = \{0\}$.
13. Find a congruence σ on $\mathbb{N}$ such that $[0]_\sigma = \{0\}$ and such that $[a]_\sigma$ has infinitely many elements for some $a \in \mathbb{N}$.
14. Let M be a subgroup of $\mathbb{Z}^n$ with $M \cap \mathbb{N}^n = \{0\}$. Prove that $\mathbb{N}^n / \sim_M$ has a unique minimal system of generators.
15. Show that $\{1\}$ and $\{2,3\}$ are minimal systems of generators of the monoid $\mathbb{Z}_6$.

CHAPTER 10

Numerical semigroups

A **numerical semigroup** is a submonoid of $\mathbb{N}$ such that the greatest common divisor of its elements is equal to one. Every submonoid of $\mathbb{N}$ is, up to isomorphism, a numerical semigroup, as the next result illustrates.

PROPOSITION 10.1. *Every nontrivial submonoid of* $\mathbb{N}$ *is isomorphic to a numerical semigroup.*

PROOF. Let S be a nontrivial submonoid of $\mathbb{N}$ and let $0 \neq d$ be the greatest common divisor of the elements of S. Define

$$f : S \to \mathbb{N},\ f(s) = \frac{s}{d}.$$

Clearly, f is a monomorphism and therefore $\mathrm{Im}(f)$ is isomorphic to S. Observe that $\mathrm{Im}(f)$ is a numerical semigroup. □

The following result provides us with alternative ways of defining a numerical semigroup: as a "cofinite" submonoid of $\mathbb{N}$ or as a submonoid of $\mathbb{N}$ whose spanning group is $\mathbb{Z}$.

PROPOSITION 10.2. *Let S be a submonoid of* $\mathbb{N}$. *The following statements are equivalent:*

(i) *S is a numerical semigroup.*
(ii) $\mathbf{G}(S) = \mathbb{Z}$.
(iii) $\mathbb{N} \setminus S$ *is finite.*

PROOF. *(i) implies (ii)* By Proposition 2.1, $\mathbf{G}(S) = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Since $\gcd(S) = 1$, the element n must be equal to 1.

(ii) implies (iii) Since $\mathbf{G}(S) = \mathbb{Z}$, we have that $1 \in \mathbf{G}(S)$ and by the definition of $\mathbf{G}(S)$, there exist s and s' in S such that $s' - s = 1$. Hence $s' = s + 1$ which implies that

$$\{s, s+1, 2s+2, 3s+3, \ldots, (s-1)s + (s-1)\} \subseteq S.$$

We show that for every $n \in \mathbb{N}$ such that $n \geq (s-1)s + (s-1)$, the element n belongs to S. Let q and r be elements of $\mathbb{N}$ such that $n = qs + r$, with $0 \leq r < s$. Then $n = (rs + r) + (q - r)s \in S$ (observe that $q \geq s - 1 \geq r$, since $n \geq (s-1)s + (s-1)$).

(iii) implies (i) By the finiteness of $\mathbb{N} \setminus S$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have that $n \in S$. Hence N and $N + 1$ are both in S and this implies that $\gcd(S) = 1$. □

Thus if S is a numerical semigroup, then it makes sense to speak about a the greatest element of $\mathbb{Z}$ not belonging to S. We call this element the **conductor** of S, which is usually denoted by $\mathrm{C}(S)$.

Let $m \in \mathbb{N} \setminus \{0\}$ and $A = \{a_1, \dots, a_r\}$ be a subset of $\mathbb{N}$. We say that A is a **system of incongruent numbers modulo** m if for every $i \neq j$, we have that $a_i \not\equiv a_j \pmod{m}$. Note that this implies that $r \leq m$. If $r = m$, then A is a **complete system modulo** m.

PROPOSITION 10.3. *Let S be a numerical semigroup and let n be an element of $S \setminus \{0\}$. The set $\mathrm{Ap}(S,n)$ is a complete system modulo n.*

PROOF. Recall that

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

For every $i \in \{0, \dots, n-1\}$, define

$$w_i = \min\{s \in S \mid s \equiv i \pmod{n}\}.$$

The element w_i exists since for every $n \in \mathbb{N}$, $n > \mathrm{C}(S)$, we have that $n \in S$, which implies that the set $\{s \in S \mid s \equiv i \pmod{n}\}$ is not empty. The reader can check that

$$\mathrm{Ap}(S,n) = \{w_0, \dots, w_{n-1}\},$$

which concludes the proof. □

Let S be a numerical semigroup and $n \in S \setminus \{0\}$. By the definition of $\mathrm{Ap}(S,n)$, the element $\max(\mathrm{Ap}(S,n)) - n \notin S$. Take $s \in \mathbb{N}$ to be an element greater than $\max(\mathrm{Ap}(S,n)) - n$ and assume that $w \in \mathrm{Ap}(S,n)$ is such that $s \equiv w \pmod{n}$. Since $s + n > \max(\mathrm{Ap}(S,n))$, we have that $s + n > w$ and consequently $s + n = w + qn$ for some $q \in \mathbb{N} \setminus \{0\}$. Hence $s = w + (q-1)n \in S$. We have shown the following result.

PROPOSITION 10.4. *Let S be a numerical semigroup and $n \in S \setminus \{0\}$. Then*

$$\mathrm{C}(S) = \max(\mathrm{Ap}(S,n)) - n.$$

If $s \in S$ and $s \notin \mathrm{Ap}(S,n)$, then, by the definition of $\mathrm{Ap}(S,n)$, $s - n$ is again in S. Furthermore, there exists $k \in \mathbb{N}$ such that $s - kn = w \in \mathrm{Ap}(S,n)$ (observe that w is the element in $\mathrm{Ap}(S,n)$ verifying that $s \equiv w \pmod{n}$). Thus $s = w + kn$. Assume that $s = w' + k'n$ for some $w' \in \mathrm{Ap}(S,n)$ and $k' \in \mathbb{N}$. Hence $w \equiv w' \pmod{n}$ and since $\mathrm{Ap}(S,n)$ is a complete system modulo n, we deduce that $w = w'$, which leads to $k = k'$. Therefore every element $s \in S$ can be expressed in a unique way as $s = w + kn$ for some $w \in \mathrm{Ap}(S,n)$ and $k \in \mathbb{N}$. A clear consequence of this fact is that

$$S = \langle \{n\} \cup \mathrm{Ap}(S,n) \rangle$$

and therefore every numerical semigroup is finitely generated, since $\mathrm{Ap}(S,n)$ has n elements. We can state this remark as follows.

PROPOSITION 10.5. *Every numerical semigroup S is an affine semigroup. Furthermore, for a fixed $n \in S \setminus \{0\}$, we have that for every $s \in S$ there exist unique $k \in \mathbb{N}$ and $w \in \mathrm{Ap}(S,n)$ such that $s = kn + w$.*

If S is a numerical semigroup, then the set $S^* \setminus (S^* + S^*)$, with $S^* = S \setminus \{0\}$, is the minimal system of generators of S (see exercises at the end of Chapter 3). Assume that $\{n_0, \dots, n_p\}$ is the minimal system of generators of S. Since S is numerical, the greatest common divisor of $\{n_0, \dots, n_p\}$ is equal to 1 (clearly, the converse is also true). The elements of S can be computed taking into account the following remarks.

1. $0 \in S$.
2. For every $n \in \mathbb{N} \setminus \{0\}$, if we know which are the elements less that n belonging to S, then we can determine whether n belongs or not to S, since $n \in S$ if and only if $n - n_i$ for some $i \in \{0, \dots, p\}$.
3. If we are at at a stage when we know that $n, n+1, \dots, n+(n_0-1) \in S$, then, for every $i \in \{0, \dots, n_0 - 1\}$, we have computed at least one element congruent with i modulo n_0. Hence at this stage, we already know $\mathrm{Ap}(S, n_0)$ and, by Proposition 10.4, $\mathrm{C}(S)$ as well.

EXAMPLE 10.6. Let S be the monoid generated by $\{5,7,9\}$. Since $\gcd\{5,7,9\} = 1$, the monoid S is a numerical semigroup. Using the ideas exposed above, we obtain that

$$S = \{0,5,7,9,10,12,14,15,16,17,18,\dots\}.$$

Hence

$$S = \{0,5,7,9,10,12\} \cup \{n \in \mathbb{N} \mid n \geq 14\} \text{ and } \mathrm{C}(S) = 13.$$

For instance, if we want to compute $\mathrm{Ap}(S,7)$, we only must look for the first seven numbers in S such that subtracting 7 to them they lie outside S and such that they are less than or equal to $\mathrm{C}(S) + 7 = 20$. Thus

$$\mathrm{Ap}(S,7) = \{0,5,9,10,15,18,20\}.$$

◇

Let $S \neq \{0\}$ be a numerical semigroup with minimal system of generators $\{n_0, \dots, n_p\}$. Take n to be an element in S. By Proposition 10.5, we know that there exist $k_0 \in \mathbb{N}$ and $w_0 \in \mathrm{Ap}(S, n_0)$ such that $n = k_0 n_0 + w_0$. Again using Proposition 10.5, we see that there are unique $k_1 \in \mathbb{N}$ and $w_1 \in \mathrm{Ap}(S, n_1)$ such that $w_0 = k_1 n_1 + w_1$ and therefore $n = k_0 n_0 + k_1 n_1 + w_1$. Observe that $w_1 \in \mathrm{Ap}(S, n_0, n_1)$. Repeating this process we finally get that there exist unique $k_0, \dots, k_{p-1} \in \mathbb{N}$ and $w_{p-1} \in \mathrm{Ap}(S, n_0, \dots, n_{p-1})$ such that

$$n = k_0 n_0 + \cdots + k_{p-1} n_{p-1} + w_{p-1}.$$

Since $w_{p-1} \in \mathrm{Ap}(S, n_0, \dots, n_{p-1})$, there exists an element $k_p \in \mathbb{N}$ such that $w_{p-1} = k_p n_p$. The element k_p is unique fulfilling this condition, hence n can be expressed uniquely as

$$n = k_0 n_0 + \cdots + k_p n_p$$

with

$$k_{i+1} n_{i+1} + \cdots + k_p n_p \in \mathrm{Ap}(S, n_0, \dots, n_i), \text{ for all } i \in \{0, \dots, p-1\}.$$

The expression $n = k_0 n_0 + \cdots + k_p n_p$ is called the **primary representation** of n for the ordering of the generators $n_0, n_1, \ldots, n_p$.

EXAMPLE 10.7. Going back to the numerical semigroup $S = \langle 5,7,9 \rangle$, it is easy to compute

$$\mathrm{Ap}(S,5) = \{0,7,9,16,18\},$$

$$\mathrm{Ap}(S,5,7) = \{n \in \mathrm{Ap}(S,5) \mid n-7 \notin S\} = \{0,9,18\},$$

$$\mathrm{Ap}(S,5,7,9) = \{0\}.$$

Let us compute the primary representation of 26 for the ordering of generators 5,7,9. Since $26 \equiv 1 \pmod 5$, we must look in $\mathrm{Ap}(S,5)$ for an element w_0 such that $w_0 \equiv 1 \pmod 5$. We obtain that $26 = 2 \times 5 + 16$. Now, we search in $\mathrm{Ap}(S,5,7)$ for an element w_1 such that $16 \equiv w_1 \pmod 7$. We get that $26 = 2 \times 5 + 7 + 9$, which is already the primary representation of 26 for the ordering of generators 5,7,9. ◇

1. Minimal presentations of numerical semigroups

Let S be the numerical semigroup with minimal system of generators $\{n_0, \ldots, n_p\}$. Since S is an affine semigroup, we can use the results appearing in Chapter 9 for computing a minimal presentation of S. In this section we sharpen the method exposed there. Recall that the main idea of the procedure consists in finding the elements $n \in S$ such that the graph Δ_n is not connected. The improvement of the method is realized by refining the bound derived for the affine case from Theorem 8.5.

PROPOSITION 10.8. *Let S be the numerical semigroup with minimal system of generators $\{n_0, \ldots, n_p\}$. If Δ_n is not connected for some $n \in S$, then there exist $w \in \mathrm{Ap}(S,n_0) \setminus \{0\}$ and $j \in \{1, \ldots, p\}$ such that $n = w + n_j$.*

PROOF. Take $n \in S$ be such that Δ_n is not connected. We distinguish two cases.

1. The element n belongs to $\mathrm{Ap}(S,n_0)$. This means that $n_0 \notin \mathrm{V}(\Delta_n)$. Since Δ_n is not connected, the set $\mathrm{V}(\Delta_n)$ is not empty and therefore there exists $j \in \{1, \ldots, p\}$ such that $n - n_j \in S \setminus \{0\}$. Clearly, $n = (n - n_j) + n_j$ and $n - n_j \in \mathrm{Ap}(S,n_0) \setminus \{0\}$.
2. If $n \notin \mathrm{Ap}(S,n_0)$, then $n_0 \in \mathrm{V}(\Delta_n)$. Take n_j to be an element in $\mathrm{V}(\Delta_n)$ not belonging to the same connected component containing n_0. Then $n - (n_j + n_0) = (n - n_j) - n_0 \notin S$, which implies that $n - n_j \in \mathrm{Ap}(S,n_0) \setminus \{0\}$. Hence $n = (n - n_j) + n_j$, with $n - n_j \in \mathrm{Ap}(S,n_0) \setminus \{0\}$.

□

Assume that $n_0 < n_1 < \cdots < n_p$. Since $\max(\mathrm{Ap}(S,n_0)) = \mathrm{C}(S) + n_0$, the maximum of the elements of the form $w + n_j$ with $w \in \mathrm{Ap}(S,n_0)$ and $j \in \{1, \ldots, p\}$ is exactly $\mathrm{C}(S) + n_0 + n_p$. With this remark it is easy to prove the following statement.

COROLLARY 10.9. *Let S be a numerical semigroup with minimal system of generators $\{n_0 < \cdots < n_p\}$. If Δ_n is not connected for some $n \in S$, then*

$$n \leq \mathrm{C}(S) + n_0 + n_p.$$

The results presented so far ensure that the following algorithm computes a minimal presentation of a given numerical semigroup.

ALGORITHM 10.10 (MPNS). The input is the set of minimal generators

$$\{n_0 < \ldots < n_p\}$$

of a numerical semigroup S. The output is a minimal presentation of S.

1. Compute the set of elements n of S such that $n \leq \mathrm{C}(S) + n_0 + n_p$.
2. Compute $\mathrm{Ap}(S, n_0), \ldots, \mathrm{Ap}(S, n_p)$.
3. Compute $(\mathrm{Ap}(S, n_0) \setminus \{0\}) + \{n_1, \ldots, n_p\}$.
4. For every element $n \in (\mathrm{Ap}(S, n_0) \setminus \{0\}) + \{n_1, \ldots, n_p\}$ construct Δ_n.
5. For every resulting non-connected graph Δ_n and each connected component C_j^n of Δ_n, choose a vertex $n_{j_i} \in C_j^n$ and compute a primary representation

$$k_{j_i}^j n_{i_j} + k_0^j n_0 + \cdots + k_{j_i-1}^j n_{j_i-1} + k_{j_i+1}^j n_{j_i+1} + \cdots + k_p^j n_p$$

with respect to the ordering of generators

$$n_{j_i}, n_0, \ldots, n_{j_i-1}, n_{j_i+1}, \ldots, n_p.$$

(Observe that only the vertices of C_j^n may appear in this primary representation.)

6. Define

$$\rho_n = \{((k_0^1, \ldots, k_p^1), (k_0^2, \ldots, k_p^2)), \ldots, ((k_0^1, \ldots, k_p^1), (k_0^{t_n}, \ldots, k_p^{t_n}))\},$$

where t_n is the number of connected components of Δ_n.

7. Return

$$\rho = \bigcup \rho_n.$$

◇

EXAMPLE 10.11. In Chapter 9 we computed a minimal presentation for $S = \langle 3, 5, 7 \rangle$. Let us see that using Algorithm MPNS we save some computations. Recall that using the general algorithm obtained for affine semigroups we had to determine which graphs Δ_n, with $n = 3a_1 + 5a_2 + 7a_2$ and $a_1 + a_2 + a_3 \leq 8$, where not connected. This is, even in this case, a big region to deal with by hand.

Using Algorithm MPNS, we have to compute the elements n in S such that $n \leq \mathrm{C}(S) + 3 + 7 = 14$. Then we must determine for which elements n in

$$(\mathrm{Ap}(S, 3) \setminus \{0\}) + \{5, 7\} = \{10, 12, 14\}$$

the graph Δ_n is connected. This drives us directly to the non-connected graphs Δ_{10}, Δ_{12} and Δ_{14}. ◇

EXAMPLE 10.12. Let

$$S = \langle 5,7,9,11 \rangle.$$

We start computing S and notice that

$$S = \{0,5,7,9,10,11,12,14,15,16,17,18,\ldots\}$$

which means that $\mathrm{C}(S) = 13$. We already know the elements n in S such that $n \leq \mathrm{C}(S)+5+11 = 29$.

The Apéry sets of the generators in S are

$$\begin{aligned}
\mathrm{Ap}(S,5) &= \{0,7,9,11,18\},\\
\mathrm{Ap}(S,7) &= \{0,5,9,10,11,15,20\},\\
\mathrm{Ap}(S,9) &= \{0,5,7,10,11,12,15,17,22\},\\
\mathrm{Ap}(S,11) &= \{0,5,7,9,10,12,14,15,17,19,24\}.
\end{aligned}$$

Next we compute $(\mathrm{Ap}(S,5) \setminus \{0\}) + \{7,9,11\}$ obtaining

$$\{14,16,18,20,22,25,27,29\}.$$

Now, we study the graphs Δ_n, with n in the set $(\mathrm{Ap}(S,5) \setminus \{0\}) + \{7,9,11\}$.

Graph	Connected components	Relators
Δ_{14}	$\{5,9\},\{7\}$	$e_1+e_3=2e_2$
Δ_{16}	$\{5,11\},\{7,9\}$	$e_1+e_4=e_2+e_3$
Δ_{18}	$\{7,11\},\{9\}$	$e_2+e_4=2e_3$
Δ_{20}	$\{5\},\{9,11\}$	$4e_1=e_3+e_4$
Δ_{22}	$\{5,7\},\{11\}$	$3e_1+e_2=2e_4$
Δ_{25}	$\{5,7,9,11\}$	
Δ_{27}	$\{5,7,9,11\}$	
Δ_{29}	$\{5,7,9,11\}$	

Therefore a minimal presentation of S is

$$\begin{aligned}
\rho = \{&((1,0,1,0),(0,2,0,0)),((1,0,0,1),(0,1,1,0)),((0,1,0,1),(0,0,2,0)),\\
&((4,0,0,0),(0,0,1,1)),((3,1,0,0),(0,0,0,2))\}.
\end{aligned}$$

◇

2. A bound for the cardinality of minimal presentations of numerical semigroups

In order to give a bound for the cardinality of a minimal presentation of a numerical semigroup, we need first to refine Proposition 10.8.

LEMMA 10.13. *Let S be a numerical semigroup minimally generated by*

$$\{n_0 < n_1 < \cdots < n_p\}$$

and let $n \in S$ be such that Δ_n is not connected. Then there exists a number $0 < k \leq p$ and an element $s \in \mathrm{Ap}(S, n_0, \dots, n_{k-1})$ such that:

(i) $n = n_k + s$,

(ii) $n \notin \mathrm{Ap}(S, n_0, \dots, n_{k-1})$,

(iii) *for all $s' \in S \setminus \{s\}$, with $s \notin \mathrm{Ap}(S, s')$, we have that $s' + n_k \in \mathrm{Ap}(S, n_0, \dots, n_{k-1})$.*

PROOF. *(i)* Let n_i be such that $i = \min\{j \mid n_j \in \mathrm{V}(\Delta_n)\}$. Since Δ_n has more than one connected component, we can choose another vertex of Δ_n which is not in the connected component C_i that contains n_i. Choose n_k so that $k = \min\{j \mid n_j \in \mathrm{V}(\Delta_n) \setminus \mathrm{V}(C_i)\}$. Note that k is always greater than zero, since $k > i \geq 0$. In addition, by the definition of $\mathrm{V}(\Delta_n)$, $s = n - n_k \in S$. Moreover, from the way we have chosen k, for any $j < k$, $\overline{n_j n_k}$ is not an edge of Δ_n. Hence $s - n_j = n - (n_j + n_k) \notin S$ and therefore $s \in \mathrm{Ap}(S, n_0, \dots, n_{k-1})$.

(ii) Since $n - n_i \in S$ and $i < k$, we have that $n \notin \mathrm{Ap}(S, n_0, \dots, n_{k-1})$.

(iii) Assume that $s' \in S$ is such that $s \neq s'$ and $s \notin \mathrm{Ap}(S, s')$. Then $0 \neq s - s' \in S$ and thus there is a generator n_t such that $s - s' - n_t \in S$. Further, n_t is a vertex of Δ_n, since $n - n_t = (s - s' - n_t) + s' + n_k \in S$. Moreover $n - (n_t + n_k) = (s - s' - n_t) + s' \in S$. Hence n_t and n_k are in the same connected component of Δ_n. If there exists $j \leq k - 1$ such that $s' + n_k \notin \mathrm{Ap}(S, n_j)$, then we have

$$n - n_j = (s - s' - n_t) + n_t + (s' + n_k - n_j) \in S.$$

Thus n_j is a vertex of Δ_n which is in the connected component that contains n_t (notice that $n - (n_j + n_t) \in S$). We conclude that n_j and n_k are in the same connected component, but $j < k$, which is in contradiction with the choice of k. □

The following result will be used later for counting the elements of a minimal presentation of a given numerical semigroup.

LEMMA 10.14. *Let S be a numerical semigroup minimally generated by*

$$\{n_0 < n_1 < \cdots < n_p\}.$$

For every $1 \leq k \leq p$, let D_k be the set of elements s in $\mathrm{Ap}(S, n_0, \dots, n_{k-1})$ such that

(i) $s + n_k \notin \mathrm{Ap}(S, n_0, \dots, n_{k-1})$,

(ii) *for all $s' \in S \setminus \{s\}$ with $s \notin \mathrm{Ap}(S, s')$, we have that $s' + n_k \in \mathrm{Ap}(S, n_0, \dots, n_{k-1})$.*

Take $\dot{\bigcup}_{k=1}^{p} D_k$ to be the disjoint union of the sets D_k. If ρ is a minimal presentation of S, then there is an injective map

$$i : \rho \to \dot{\bigcup}_{k=1}^{p} D_k.$$

PROOF. Since every minimal presentation has the same cardinality (Corollary 9.5), it suffices to show the result for ρ being the output of Algorithm MPNS. For every $n \in S$, let $C_1^n, \dots, C_{t_n}^n$ be the connected components of Δ_n. We may assume that C_1^n contains the vertex of Δ_n with the lowest index. Recall that ρ_n, whenever $t_n \geq 2$, is of the form

$$\rho_n = \{(r_1^n, r_2^n), \dots, (r_1^n, r_{t_n}^n)\},$$

where each r_i^n is associated to a primary representation of n with respect to the vertices of C_i^n. For every $i \in \{2,\dots,t_n\}$, take $n_{j_i} \in \mathrm{V}(C_i^n)$ such that $j_i = \min\{k \mid n_k \in \mathrm{V}(C_i^n)\}$. From the assumption imposed on C_1^n, we obtain that $j_i > 0$. As in the proof of Lemma 10.13, it is not hard to show that $n - n_{j_i} \in D_{j_i}$. Define $i((r_1^n, r_i^n)) = n - n_{j_i}$.

Assume now that $i(a,b) = i(a',b')$. The element

$$i(a,b) = \varphi(b) - n_k = \varphi(a) - n_k \in D_k,$$

with k depending on b and φ being, as usual, the map

$$\varphi : \mathbb{N}^{p+1} \to S,\ \varphi(a_0,\dots,a_p) = \sum_{i=0}^{p} a_i n_i.$$

Observe that this leads to $i(a,b) = i(a',b') \in D_k$. It follows that $i(a',b') = \varphi(a') - n_k$, which yields $\varphi(a) = \varphi(a')$. Hence (a,b) and (a',b') are both in $\rho_{\varphi(a)}$. Thus

$$a = a' = r_1^{\varphi(a)}.$$

If $b \neq b'$, then their corresponding connected components are different and therefore $i(a,b)$ and $i(a',b')$ belong to different D_k's, which is a contradiction. □

Putting the above information together, we get a bound for the cardinality of a minimal presentation of a given numerical semigroup.

THEOREM 10.15. *Let S be a numerical semigroup with minimal system of generators $\{n_0 < n_1 < \cdots < n_p\}$. The cardinality of a minimal presentation of S is less than or equal to*

$$\frac{(2n_0 - p)(p-1)}{2} + 1.$$

PROOF. Using Lemma 10.14, we only have to compute the number of elements in D_k for $1 \le k \le p$. Let c be the least positive integer such that $cn_p \in \langle n_0,\dots,n_{p-1}\rangle$. It can be easily shown that

$$\mathrm{Ap}(S,n_0,\dots,n_{p-1}) = \{0,n_p,\dots,(c-1)n_p\}.$$

Hence the only element in D_p is $(c-1)n_p$.

For any $1 \le k \le p-1$,

$$D_k \subseteq \mathrm{Ap}(S,n_0,\dots,n_{k-1}) \setminus \{0\} \subseteq \mathrm{Ap}(S,n_0) \setminus \{0,n_1,\dots,n_{k-1}\}.$$

Since

$$\{0,n_1,\dots,n_{k-1}\} \subseteq \mathrm{Ap}(S,n_0),$$

the cardinality of D_k is less than or equal to $n_0 - k$. Therefore, by Lemma 10.14, the cardinality of any minimal presentation of S is less than or equal to

$$1 + \sum_{i=1}^{p-1} (n_0 - i) = \frac{(2n_0 - p)(p-1)}{2} + 1.$$

□

EXAMPLE 10.16. Let $S = \langle 3,5,7 \rangle$. Then $n_0 = 3$ and $p = 2$. If ρ is a minimal presentation of S, then it has, at most,

$$\frac{(2\times 3-2)(2-1)}{2}+1=3$$

elements. We already know that a minimal presentation of S is

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

◇

This example shows that the the bound given in Theorem 10.15 can be reached. As we are going to see in the next section, there is a wide class of numerical semigroups reaching this bound.

3. Numerical semigroups with maximal embedding dimension

The **embedding dimension** of a numerical semigroup is the cardinality of its minimal system of generators. The **multiplicity** of a numerical semigroup S is the least integer belonging to $S \setminus \{0\}$. If S is a numerical semigroup whose minimal system of generators is

$$\{n_0 < n_1 < \cdots < n_p\},$$

then $p+1$ is its embedding dimension and n_0 is its multiplicity. Since $\{n_0,\dots,n_p\}$ is a minimal system of generators of S, every element n_i, with $i > 0$, belongs to $\mathrm{Ap}(S,n_0)$. Hence the set $\{0,n_1,\dots,n_p\}$ is always contained in $\mathrm{Ap}(S,n_0)$. Recall that the cardinality of $\mathrm{Ap}(S,n_0)$ is exactly n_0 and this implies that $p+1 \leq n_0$, that is to say, the embedding dimension of a numerical semigroup is always less than or equal to its multiplicity. Therefore we say that S has **maximal embedding dimension** whenever $n_0 = p+1$. In this section we study the cardinality of minimal presentations for this kind of numerical semigroup. Thus assume that S is a semigroup with maximal embedding dimension, that is to say,

$$\mathrm{Ap}(S,n_0) = \{0,n_1,\dots,n_p\}.$$

By Proposition 10.8, we know that if Δ_n is not connected, then $n = w + n_j$ with

$$w \in \mathrm{Ap}(S,n_0) \setminus \{0\} = \{n_1,\dots,n_p\} \text{ and } 1 \leq j \leq p.$$

Thus whenever Δ_n is not connected, we have $n = n_i + n_j$ for some $i,j \in \{1,\dots,p\}$. The converse is also true. If $n = n_i + n_j$, then $n \notin \mathrm{Ap}(S,n_0)$, which means that $n_0 \in \mathrm{V}(\Delta_n)$. Observe that n_i and n_j are in the same connected component of Δ_n. If $n-(n_i+n_k) \in S$ with $k \notin \{i,j\}$, then $n_j - n_k \in S$ and this is impossible, since $\{n_0,\dots,n_p\}$ is a minimal system of generators of S. As a consequence of this fact, $\{n_i,n_j\}$ are the vertices of a connected component of Δ_n which clearly does not contain n_0. Therefore Δ_n is not connected. We have shown the following result.

LEMMA 10.17. *Let S be a numerical semigroup with maximal embedding dimension minimally generated by $\{n_0 < n_1 < \cdots < n_p\}$. The graph Δ_n is not connected if and only if $n = n_i + n_j$ for some $i, j \in \{1, \ldots, p\}$.*

Thus in every non connected graph $\Delta_{n_i+n_j}$ there is always a connected component containing n_0 and another whose vertices are $\{n_i, n_j\}$. From the construction of a minimal presentation ρ of S, if we fix C_1^n to be the connected component containing n_0, then we have as many elements in ρ as elements of the form $n_i + n_j$ with $i, j \in \{1, \ldots, p\}$. Hence we obtain $(p+1)p/2 = n_0(n_0-1)/2$ elements in ρ.

PROPOSITION 10.18. *Let S be a numerical semigroup with multiplicity n_0. Then S has maximal embedding dimension if and only if a (every) minimal presentation of S has exactly $n_0(n_0-1)/2$ elements.*

PROOF. *Necessity.* We have already shown that if S has maximal embedding dimension, then the cardinality of a minimal presentation of S is $n_0(n_0-1)/2$.

Sufficiency. By Theorem 10.15, we know that

$$\frac{n_0(n_0-1)}{2} \leq \frac{(2n_0-p)(p-1)}{2} + 1.$$

Hence

$$p^2 - (2n_0+1)p + n_0^2 + n_0 - 2 \leq 0.$$

This inequality on p has solution $n_0 - 1 \leq p \leq n_0 + 2$ and since $p + 1 \leq n_0$, we have that $p + 1 = n_0$, which means that S has maximal dimension. □

If we substitute p by $n_0 - 1$ in the bound obtained in Theorem 10.15, we get

$$\frac{(2n_0-p)(p-1)}{2} + 1 = \frac{(2n_0-(n_0-1))(n_0-1-1)}{2} + 1 = \frac{n_0(n_0-1)}{2}.$$

Thus for all maximal embedding dimension numerical semigroups the bound of Theorem 10.15 is reached.

Next, we give a procedure for constructing numerical semigroups with maximal embedding dimension.

PROPOSITION 10.19. *Let S be a numerical semigroup minimally generated by $\{n_0 < n_1 < \cdots < n_p\}$ such that*

$$\mathrm{Ap}(S, n_0) = \{w_1 < w_2 < \cdots < w_{n_0}\}.$$

Then

$$\overline{S} = \langle n_0 + w_1, n_0 + w_2, \ldots, n_0 + w_{n_0} \rangle$$

is a maximal embedding dimension numerical semigroup. Furthermore,

$$\mathrm{C}(\overline{S}) = \mathrm{C}(S) + n_0.$$

PROOF. Observe that $w_1 = 0$ and that it suffices to show that

$$\{n_0 + w_1, n_0 + w_2, \dots, n_0 + w_{n_0}\}$$

is a minimal system of generators of $\overline{S}$. Clearly,

$$n_0 \notin \langle n_0 + w_2, \dots, n_0 + w_{n_0} \rangle.$$

If there exists $i \in \{2, \dots, n_0\}$ such that

$$n_0 + w_i \in \langle \{n_0 + w_1, \dots, n_0 + w_{n_0}\} \setminus \{n_0 + w_i\} \rangle,$$

then there exists $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n_0} \in \mathbb{N}$ such that

$$n_0 + w_i = \sum_{j=1, j\neq i}^{n_0} a_j(n_0 + w_j) = \left(\sum_{j=1, j\neq i}^{n_0} a_j \right) n_0 + \sum_{j=1, j\neq i}^{n_0} a_j w_j.$$

Since $n_0 + w_i \neq 0$ and $w_i \neq w_j$ for $j \neq i$, we have that $\sum_{j=1, j\neq i}^{n_0} a_j \geq 2$, whence $w_i - n_0 \in S$ which contradicts $w_i \in \mathrm{Ap}(S, n_0)$. □

We can also prove a kind of converse of this result.

PROPOSITION 10.20. *Let S be a numerical semigroup with maximal embedding dimension minimally generated by $\{n_0 < n_1 < \cdots < n_{n_0-1}\}$. Then the numerical semigroup*

$$S' = \langle n_0, n_1 - n_0, \dots, n_{n_0-1} - n_0 \rangle$$

satisfies

$$\mathrm{Ap}(S', n_0) = \{0, n_1 - n_0, \dots, n_{n_0-1} - n_0\}.$$

Furthermore, $\mathrm{C}(S) = \mathrm{C}(S') + n_0$.

PROOF. It is clear that

$$\{0, n_1 - n_0, \dots, n_{n_0-1} - n_0\}$$

is a complete system modulo n_0 since

$$\mathrm{Ap}(S, n_0) = \{0, n_1, \dots, n_{n_0-1}\}.$$

Thus it suffices to show that, for every i, we have that $n_i - n_0$ is the least element in S' verifying $n_i - n_0 \equiv n_i \pmod{n_0}$. Assume that $n \in S'$ is such that $n \equiv n_i \pmod{n_0}$ and $n < n_i - n_0$. Hence $n_i - n_0 = kn_0 + n$ for some $k \in \mathbb{N} \setminus \{0\}$. Since n belongs to S', there exist $a_0, \dots, a_{n_0-1} \in \mathbb{N}$ such that

$$n = a_0 n_0 + \sum_{j=1}^{n_0-1} a_j(n_j - n_0).$$

Hence

$$n_i - n_0 = (a_0 + k)n_0 + \sum_{j=1}^{n_0-1} a_j(n_j - n_0).$$

By Proposition 10.5, for every i, j, there exists $k_{i_j} \in \mathbb{N}$ such that $n_i + n_j = k_{i_j} n_0$ or $n_i + n_j = k_{i_j} n_0 + n_{i_j}$ for some $i_j \in \{1, \dots, n_0 - 1\}$. Since $\{n_0, \dots, n_{n_0-1}\}$ is a minimal system of generators of S, we deduce that in the first case $k_{ij} \geq 2$ and in the second case $k_{i_j} \geq 1$. Thus

$$(n_i - n_0) + (n_j - n_0) = k_{i_j} n_0 - 2n_0 = (k_{i_j} - 2)n_0$$

or

$$(n_i - n_0) + (n_j - n_0) = k_{i_j} n_0 + n_{i_j} - 2n_0 = (k_{i_j} - 1)n_0 + (n_{i_j} - n_0),$$

for every $i, j \in \{1, \dots, n_{n_0-1}\}$. Applying this "rule" to $\sum_{j=1}^{n_0-1} a_j(n_j - n_0)$ as many times as necessary, we obtain that $\sum_{j=1}^{n_0-1} a_j(n_j - n_0) = mn_0$, for some $m \geq 0$, or $\sum_{j=1}^{n_0-1} a_j(n_j - n_0) = mn_0 + (n_l - n_0)$ for some $l \in \{1, \dots, n_0 - 1\}$. Combining, we get

$$n_i - n_0 = (a_0 + k)n_0 + mn_0 = (a_0 + k + m)n_0$$

or

$$n_i - n_0 = (a_0 + k)n_0 + mn_0 + (n_l - n_0) = (a_0 + k + m)n_0 + (n_l - n_0)$$

and thus $n_i = (a_0 + k + m + 1)n_0$ or $n_i = (a_0 + k + m)n_0 + n_l$. The first case is impossible. In the second case, again using Proposition 10.5, we conclude that $i = k$ and $a_0 + k + m = 0$, which leads to $k = 0$ contradicting that $k \in \mathbb{N} \setminus \{0\}$. □

As a consequence of the last two results we obtain the following statement.

COROLLARY 10.21. *There is a one-to-one correspondence between the class of numerical semigroups with multiplicity n_0 and conductor C and the class of numerical semigroups with maximal embedding dimension, multiplicity n_0, conductor $C + n_0$ and minimum generator different from n_0 greater than $2n_0$.*

Remarks

The problems related to numerical semigroups are classical. Sylvester in **[61]** solves the problem of computing the conductor of a numerical semigroup with embedding dimension equal to two. Sometimes the conductor of a numerical semigroup is called the Frobenius number. There is no general formula for the conductor of a numerical semigroup. However, for some special cases there exists an explicit formula for it (see **[3, 17, 16, 51]**).

As a consequence of the papers **[13, 24, 30, 34]** and many others, the study of numerical semigroups becomes more appealing for its applications to Algebraic Geometry. The relationship between numerical semigroups and Algebraic Geometry has been the reason why some of the terminology employed in numerical semigroups is inherited from classical Algebraic Geometry.

Most of the results presented in this chapter are part of **[40]**. The algorithm for computing a minimal presentation of a numerical semigroup appears in **[44]**. Bresisnky shows in **[5]** that there is no upper bound for the cardinality of a minimal presentation of a numerical semigroup in terms of the embedding dimension. The bound

given in this chapter for the cardinality of a minimal presentation of a numerical semigroup appears in [**43**] and in a more general context in [**49**]. In [**57**], the cardinality of a minimal presentation of a numerical semigroup with maximal embedding dimension is determined. This result and its converse appears in [**43**]. Algorithm MPNS has allowed us to determine the cardinality of numerical semigroups with high embedding dimension (see [**45**] and [**48**]).

Exercises

1. Let S be the numerical semigroup generated by $\{5,8,11,12\}$.
   (a) Compute $\mathrm{Ap}(S,5)$.
   (b) Compute $\mathrm{C}(S)$.
2. Let $S \neq \{0\}$ be a submonoid of $\mathbb{N}$ such that $\gcd(S) = d \neq 1$ and take $n \in S \setminus \{0\}$. Prove that the cardinality of $\mathrm{Ap}(S,n) = n/d$.
3. Compute a minimal presentation for $S = \langle 5,8,11,12 \rangle$.
4. Let $x \in \mathbb{N} \setminus \{0\}$. Find a numerical semigroup such that the cardinality of one of its minimal presentations is $x(x-1)/2$.
5. Let S be a numerical semigroup with minimal system of generators $\{n_0, n_1\}$.
   (a) Show that the conductor of S is $(n_0-1)n_1 - n_0$ (hint: construct $\mathrm{Ap}(S,n_0)$).
   (b) Prove that $\{((n_1,0),(0,n_0))\}$ is a minimal presentation of S.
6. Let S be the numerical semigroup minimally generated by $\{n_0,n_1,n_2\}$. Define

$$\begin{aligned} c_0 &= \min\{k \in \mathbb{N} \setminus \{0\} \mid kn_0 \in \langle n_1,n_2 \rangle\}, \\ c_1 &= \min\{k \in \mathbb{N} \setminus \{0\} \mid kn_1 \in \langle n_0,n_2 \rangle\}, \\ c_2 &= \min\{k \in \mathbb{N} \setminus \{0\} \mid kn_2 \in \langle n_0,n_1 \rangle\}. \end{aligned}$$

   (a) Prove that Δ_n is not connected if and only if $n \in \{c_0n_0, c_1n_1, c_2n_2\}$.
   (b) Let a be the number of elements in $\{c_0n_0, c_1n_1, c_2n_2\}$ and let b be the cardinality of a minimal presentation of S. Show:
      (i) For $a = 1$, we have that $b = 2$ (one non-connected graph with three connected components).
      (ii) If $a = 2$, then $b = 2$ (two non-connected graphs with two connected components each).
      (iii) Finally, if $a = 3$, then $b = 3$ (three non-connected graphs with two connected components each).

   Compute a presentation of S in each case.
7. Use last exercise to compute a minimal presentation of
   (a) $\langle 6,10,15 \rangle$,
   (b) $\langle 4,6,7 \rangle$,
   (c) $\langle 5,6,7 \rangle$.
8. Let $W = \{0 = w_1, w_2, \ldots, w_n\}$ be a complete system modulo n and let S be the numerical semigroup generated by $W \cup \{n\}$. Prove that $\mathrm{Ap}(S,n) = W$ if and only if for every $i,j \in \{1,\ldots,n\}$ there exists $k \in \{1,\ldots,n\}$ and $t \in \mathbb{N}$ such that $w_i + w_j = tn + w_k$.

9. Compute the conductor and the cardinality of a minimal presentation of the numerical semigroup generated by $\{8, 9, 10, 11\}$.
10. Let S be a numerical semigroup. Prove that if $n > 4\mathrm{C}(S) + 2$, then Δ_n is connected.
11. Show that every numerical semigroup with embedding dimension two reaches the bound of Theorem 10.15.
12. Let S be a numerical semigroup minimally generated by $\{n_0 < n_1 < \cdots < n_p\}$.
    (i) Prove that if S has maximal embedding dimension, then $C = n_p - n_0$.
    (ii) Give a counterexample for the converse of (i).
13. Prove that there are infinitely many numerical semigroups with maximal embedding dimension and multiplicity $m \geq 2$.
14. Find two different numerical semigroups with maximal embedding dimension having the same conductor and the same multiplicity.

CHAPTER 11

Projections of congruences

Given $\rho \subseteq \mathbb{N}^{n+1} \times \mathbb{N}^{n+1}$ and $\rho' \subseteq \mathbb{N}^n \times \mathbb{N}^n$, we say that ρ' is the **projection** of ρ if for every $(x,y) = ((x_1,\dots,x_n),(y_1,\dots,y_n)) \in \mathbb{N}^n \times \mathbb{N}^n$, we have that $(x,y) \in \rho'$ if and only if there exists $x_{n+1}, y_{n+1} \in \mathbb{N}$ such that $((x_1,\dots,x_n,x_{n+1}),(y_1,\dots,y_n,y_{n+1})) \in \rho$. Clearly, if σ is a congruence on $\mathbb{N}^{n+1}$ and σ' is its projection, then σ' is a congruence on $\mathbb{N}^n$. Moreover, provided that ρ is a system of generators of σ, it is easy to show that the projection of ρ is a system of generators of σ' (the reader can check this using Proposition 5.11). This simple idea shall be used to prove that every congruence σ on $\mathbb{N}^k$ such that $\mathbb{N}^k/\sigma$ is cancellative can be obtained after several projections from a congruence $\overline{\sigma}$ on $\mathbb{N}^n$, for some $n \in \mathbb{N}\setminus\{0\}$, for which $\mathbb{N}^n/\overline{\sigma}$ is an affine semigroup.

In some special cases, we shall prove that from a canonical system of generators of σ' we can construct a canonical system of generators of σ. The process has some applications. For instance, it provides an alternative way for computing a presentation of a numerical semigroup. We shall also use this construction to show that there is no bound for the cardinality of a canonical system of generators of a congruence in terms of the cardinality of a minimal system of generators of the given congruence.

1. Presentations of finitely generated cancellative monoids as projections of affine semigroups

Let S be a finitely generated cancellative monoid. We can assume, up to isomorphism, that S is generated by $\{m_1,\dots,m_n\} \subseteq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^k$ (see the beginning of Chapter 3). Furthermore, if

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

then S is isomorphic to $\mathbb{N}^n/\sim_M$, where M is the subgroup of $\mathbb{Z}^n$ with defining equations:

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

We are going to transform this system into a system fulfilling the conditions of the affine case and then show that we can go back by performing a finite number of projections.

PROPOSITION 11.1. *Let M be the subgroup of $\mathbb{Z}^n$ given by the system of equations*

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

and let $\overline{M}$ be the subgroup of $\mathbb{Z}^{n+1}$ given by the system of equations

$$\begin{array}{rcccrcrcl} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & & & \equiv & 0 \pmod{d_1}, \\ & & & & & & & \vdots & \\ a_{(r-1)1}x_1 & + & \cdots & + & a_{(r-1)n}x_n & & & \equiv & 0 \pmod{d_{r-1}}, \\ a_{r1}x_1 & + & \cdots & + & a_{rn}x_n & + & d_rx_{n+1} & = & 0, \\ a_{(r+1)1}x_1 & + & \cdots & + & a_{(r+1)n}x_n & & & = & 0, \\ & & & & & & & \vdots & \\ a_{(r+k)1}x_1 & + & \cdots & + & a_{(r+k)n}x_n & & & = & 0. \end{array}$$

Then $\sim_M$ is the projection of $\sim_{\overline{M}}$.

PROOF. Assume that $((x_1,\dots,x_n,x_{n+1}),(y_1,\dots,y_n,y_{n+1})) \in \sim_{\overline{M}}$, that is,

$$(x_1-y_1,\dots,x_n-y_n,x_{n+1}-y_{n+1}) \in \overline{M}.$$

Then $(x_1-y_1,\dots,x_n-y_n) \in M$, whence $((x_1,\dots,x_n),(y_1,\dots,y_n)) \in \sim_M$.

Now assume that $((x_1,\dots,x_n),(y_1,\dots,y_n) \in \sim_M$. Then $(x_1-y_1,\dots,x_n-y_n) \in M$, by the r-th equation of M we get the following identity

$$a_{r1}(x_1-y_1)+\cdots+a_{rn}(x_n-y_n) = d_rz,$$

for some $z \in \mathbb{Z}$, or equivalently,

$$a_{r1}(x_1-y_1)+\cdots+a_{rn}(x_n-y_n) - zd_r = 0.$$

Choose $x_{n+1},y_{n+1} \in \mathbb{N}$ such that $z = y_{n+1}-x_{n+1}$; the preceding identity yields

$$a_{r1}(x_1-y_1)+\cdots+a_{rn}(x_n-y_n)+d_r(x_{n+1}-y_{n+1}) = 0,$$

which means that $(x_1-y_1,\dots,x_n-y_n,x_{n+1}-y_{n+1}) \in \overline{M}$, and consequently $((x_1,\dots,x_n,x_{n+1}),(y_1,\dots,y_n,y_{n+1})) \in \sim_{\overline{M}}$. □

PROPOSITION 11.2. *Let M be the subgroup of $\mathbb{Z}^n$ given by the system of equations*

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

and let $\overline{M}$ be the subgroup of $\mathbb{Z}^{n+1}$ given by the system of equations

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

Then $\sim_M$ is the projection of $\sim_{\overline{M}}$.

PROOF. If

$$((x_1,\dots,x_n,x_{n+1}),(y_1,\dots,y_n,y_{n+1})) \in \sim_{\overline{M}},$$

then $((x_1,\dots,x_n),(y_1,\dots,y_n)) \in \sim_M$.

Take $((x_1,\dots,x_n),(y_1,\dots,y_n)) \in \sim_M$. Then $(x_1-y_1,\dots,x_n-y_n) \in M$. Let

$$z = (x_1-y_1)+\cdots+(x_n-y_n) \in \mathbb{Z}$$

and choose $x_{n+1}, y_{n+1} \in \mathbb{N}$ such that $z = y_{n+1}-x_{n+1}$. Trivially

$$(x_1-y_1,\dots,x_n-y_n,x_{n+1}-y_{n+1}) \in \overline{M}$$

and therefore

$$((x_1,\dots,x_n,x_{n+1}),(y_1,\dots,y_n,y_{n+1})) \in \sim_{\overline{M}}.$$

□

Recall that the equations of M where

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

and that finding a presentation for S is equivalent to finding a system of generators of $\sim_M$. Using Propositions 11.1 and 11.2 several times, we see that $\sim_M$ can be obtained

by performing a finite sequence of projections with starting point $\sim_{M'}$, where M' is the subgroup of $\mathbb{Z}^{n+r+1}$ given by the equations

$$\begin{array}{rcccccccccl}
x_1 & + & \cdots & + & x_n & + & x_{n+1} & & & & = 0, \\
a_{11}x_1 & + & \cdots & + & a_{1n}x_n & + & & d_1x_{n+2} & & & = 0, \\
 & & & & & & & & & & \vdots \\
a_{r1}x_1 & + & \cdots & + & a_{rn}x_n & + & & \cdots & & d_rx_{n+r+1} & = 0, \\
a_{(r+1)1}x_1 & + & \cdots & + & a_{(r+1)n}x_n & & & & & & = 0, \\
 & & & & & & & & & & \vdots \\
a_{(r+k)1}x_1 & + & \cdots & + & a_{(r+k)n}x_n & & & & & & = 0.
\end{array}$$

Multiplying the first equation by suitable positive integers and adding it to the rest of the equations, we can obtain an equivalent system of equations with all its coefficients greater than or equal to zero:

$$\begin{array}{rcccccccccccl}
x_1 & + & \cdots & + & x_n & + & x_{n+1} & & & & & & = 0, \\
b_{11}x_1 & + & \cdots & + & b_{1n}x_n & + & b_{1(n+1)}x_{n+1} & + & d_1x_{n+2} & & & & = 0, \\
 & & & & & & & & & & & & \vdots \\
b_{r1}x_1 & + & \cdots & + & b_{rn}x_n & + & b_{r(n+1)}x_{n+1} & + & \cdots & & & d_rx_{n+r+1} & = 0, \\
b_{(r+1)1}x_1 & + & \cdots & + & b_{(r+1)n}x_n & + & b_{(r+1)(n+1)}x_{n+1} & & & & & & = 0, \\
 & & & & & & & & & & & & \vdots \\
b_{(r+k)1}x_1 & + & \cdots & + & b_{(r+k)n}x_n & + & b_{(r+k)(n+1)}x_{n+1} & & & & & & = 0.
\end{array}$$

The set

$$A = \{(1, b_{11}, \ldots, b_{(r+k)1}), \ldots, (1, b_{1n}, \ldots, b_{(r+k)n}),$$
$$(1, b_{1(n+1)}, \ldots, b_{(r+k)(n+1)}), (0, d_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, d_r, 0, \ldots, 0)\}$$

is a subset of $\mathbb{N}^{r+k+1}$. (If the coefficients of the equations of M are already in $\mathbb{N}$ we do not have to introduce the equation $x_1 + \cdots + x_{n+1} = 0$ and in this way we save one projection.) By Proposition 3.1, the semigroup generated by A is isomorphic to $\mathbb{N}^{n+r+1} / \sim_{M'}$ and thus it is an affine semigroup. We have proved the following result.

THEOREM 11.3. *Let σ be a congruence on $\mathbb{N}^k$ such that $\mathbb{N}^k/\sigma$ is cancellative. Then σ can be obtained by a finite sequence of projections from a congruence $\overline{\sigma}$ on $\mathbb{N}^n$ for some n such that $\mathbb{N}^n/\overline{\sigma}$ is an affine semigroup.*

This procedure can be used as well to compute a presentation of a cancellative monoid.

EXAMPLE 11.4. Let

$$S = \langle ([2], -1), ([3], 3) \rangle \subset \mathbb{Z}_5 \times \mathbb{Z}.$$

The equations of M ($S \cong \mathbb{N}^2 / \sim_M$) are

$$\begin{array}{rcl}
2x + 3y & \equiv & 0 \pmod 5, \\
-x + 3y & = & 0.
\end{array}$$

The equations of M' are

$$\begin{aligned} x+y+z &= 0, \\ 2x+3y+5t &= 0, \\ -x+3y &= 0, \end{aligned}$$

and this system is equivalent to

$$\begin{aligned} x+y+z &= 0, \\ 2x+3y+5t &= 0, \\ 4y+z &= 0. \end{aligned}$$

Hence we must find a presentation for the affine semigroup

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

Using the procedure explained in Chapter 9, we obtain that

$$\{((15,5,0,0),(0,0,20,9))\}$$

is a presentation of T and therefore it generates $\sim_{M'}$. Projecting twice, we get that

$$\{((15,5),(0,0))\}$$

is a system of generators of $\sim_M$ and therefore a presentation of S. ◇

2. Lifting some projections

We have already pointed out that if σ' is the projection of σ, then the projection of a generating system for σ is a system of generators of σ'. In this section we are interested in the converse process, that is to say, try to construct a generating system of σ from a generating system of σ'. We provide certain conditions under which this can be done.

Assume that σ is a congruence on $\mathbb{N}^{n+1}$ and that $\sigma' \subseteq \mathbb{N}^n \times \mathbb{N}^n$ is its projection. Suppose that there exist $a_1,\dots,a_{n+1} \in \mathbb{N}\setminus\{0\}$ such that

$$(x_1,\dots,x_n,x_{n+1})\ \sigma\ (y_1,\dots,y_n,y_{n+1})$$

if and only if

$$\begin{gathered} (x_1,\dots,x_n)\ \sigma'\ (y_1,\dots,y_n), \\ a_1x_1+\cdots+a_nx_n+a_{n+1}x_{n+1} = a_1y_1+\cdots+a_ny_n+a_{n+1}y_{n+1}. \end{gathered}$$

Associated to $a_1,\dots,a_n,a_{n+1}$, we define the following binary relations (the reader should prove that they are linear admissible orders).

1. $(x_1,\dots,x_n) \preceq_1 (y_1,\dots,y_n)$ if and only if $a_1x_1+\cdots+a_nx_n < a_1y_1+\cdots+a_ny_n$, or $a_1x_1+\cdots+a_nx_n = a_1y_1+\cdots+a_ny_n$ and $(x_1,\dots,x_n) \preceq_{lex} (y_1,\dots,y_n)$, where $\preceq_{lex}$ represents the lexicographical order on $\mathbb{N}^n$ (see exercises of Chapter 5).
2. $(x_1,\dots,x_n,x_{n+1}) \preceq_2 (y_1,\dots,y_n,y_{n+1})$ if and only if $(x_1,\dots,x_n) \prec_1 (y_1,\dots,y_n)$, or $(x_1,\dots,x_n) = (y_1,\dots,y_n)$ and $x_{n+1} \leq y_{n+1}$.

Let μ and μ' be the functions minimum associated to σ and σ' with respect to the linear admissible orders $\preceq_2$ and $\preceq_1$, respectively (see Chapter 5 for details).

LEMMA 11.5. *With the notation introduced above,*

$$\mathrm{Im}(\mu) = \mathrm{Im}(\mu') \times \mathbb{N}.$$

PROOF. Let $(x_1, \dots, x_n, x_{n+1}) \in \mathbb{N}^{n+1}$ be such that

$$(x_1, \dots, x_n, x_{n+1}) \notin \mathrm{Im}(\mu') \times \mathbb{N}.$$

This means that $(x_1, \dots, x_n) \notin \mathrm{Im}(\mu')$. Thus there exists $(y_1, \dots, y_n) \in \mathbb{N}^n$ verifying

$$(x_1, \dots, x_n)\ \sigma'\ (y_1, \dots, y_n), (y_1, \dots, y_n) \prec_1 (x_1, \dots, x_n).$$

Hence there exist $u, v \in \mathbb{N}$ with

$$(x_1, \dots, x_n, u)\ \sigma\ (y_1, \dots, y_n, v)$$

and

$$a_1x_1 + \cdots + a_nx_n + a_{n+1}u = a_1y_1 + \cdots + a_ny_n + a_{n+1}v.$$

Since $(y_1, \dots, y_n) \prec_1 (x_1, \dots, x_n)$, we have that $t = v - u \geq 0$. Hence

$$a_1x_1 + \cdots + a_nx_n = a_1y_1 + \cdots + a_ny_n + a_{n+1}t.$$

Adding $x_{n+1}a_{n+1}$ to both sides of this equality, we get

$$a_1x_1 + \cdots + a_nx_n + a_{n+1}x_{n+1} = a_1y_1 + \cdots + a_ny_n + a_{n+1}y_{n+1},$$

where $y_{n+1} = t + x_{n+1} \in \mathbb{N}$. So we have that

$$(x_1, \dots, x_n, x_{n+1})\ \sigma\ (y_1, \dots, y_n, y_{n+1}) \text{ and } (y_1, \dots, y_n, y_{n+1}) \prec_2 (x_1, \dots, x_n, x_{n+1}).$$

It follows that $(x_1, \dots, x_n, x_{n+1})$ can not be in $\mathrm{Im}(\mu)$.

For the opposite inclusion, assume that $(x_1, \dots, x_n, x_{n+1}) \notin \mathrm{Im}(\mu)$. This means that there exists $(y_1, \dots, y_n, y_{n+1}) \in \mathbb{N}^{n+1}$ verifying

$$(x_1, \dots, x_n, x_{n+1})\ \sigma\ (y_1, \dots, y_n, y_{n+1}), (y_1 \dots, y_n, y_{n+1}) \prec_2 (x_1, \dots, x_n, x_{n+1}).$$

Hence $(y_1, \dots, y_n) \prec_1 (x_1, \dots, x_n)$, or $(y_1, \dots, y_n) = (x_1, \dots, x_n)$ and $y_{n+1} < x_{n+1}$. By the relationship between σ and σ',

$$a_1x_1 + \cdots + a_nx_n + a_{n+1}x_{n+1} = a_1y_1 + \cdots + a_ny_n + a_{n+1}y_{n+1},$$

and consequently the latter case can not hold. Therefore $(y_1, \dots, y_n) \prec_1 (x_1, \dots, x_n)$ and, in particular, $(x_1, \dots, x_n) \notin \mathrm{Im}(\mu')$ (note that $(y_1, \dots, y_n)\ \sigma'(x_1, \dots, x_n)$, since σ' is the projection of σ). □

As a clear consequence of this result, we have

$$\mathrm{Minimals}_{\leq}(\mathbb{N}^n \setminus \mathrm{Im}(\mu')) \times \{0\} = \mathrm{Minimals}_{\leq}(\mathbb{N}^{n+1} \setminus (\mathrm{Im}(\mu') \times \mathbb{N})) =$$

$$= \mathrm{Minimals}_{\leq}(\mathbb{N}^{n+1} \setminus \mathrm{Im}(\mu)).$$

This remark together with the connection between canonical systems of generators and functions minimum (see the proof Proposition 6.13), make it straightforward to prove the following statement.

THEOREM 11.6. *Let* $\{(u_1,v_1),(u_2,v_2),\dots,(u_r,v_r)\}$ *be the canonical system of generators of the congruence* σ' *with respect to the order* $\preceq_1$. *Then there exist* $z_1,\dots,z_r \in \mathbb{N}$ *such that*

$$\{((u_1,0),(v_1,z_1)),((u_2,0),(v_2,z_2)),\dots,((u_r,0),(v_r,z_r))\}$$

is the canonical system of generators of the congruence σ *with respect to the order* $\preceq_2$. *Moreover* z_i *is the only natural number such that* $a_1u_{i,1}+\dots+a_nu_{i,n} = a_1v_{i,1}+\dots+a_nv_{i,n}+a_{n+1}z_i$.

2.1. The cardinality of a canonical system of generators of a congruence may not to be bounded in terms of the cardinality of minimal system of generators. Here we prove that the cardinality of the output of Algorithm CPC is not bounded, in general, as a function of the cardinality of the input.

Let

$$S = \langle (2,1),(2n+1,1),(2n+3,1),(0,1)\rangle,$$

for $n \in \mathbb{N}\setminus\{0\}$. Recall that by Proposition 9.13, the cardinality of a minimal presentation of S is greater than or equal to $2n$. If we project S onto the first coordinate, we obtain the numerical semigroup

$$S' = \langle 2, 2n+1, 2n+3\rangle,$$

which is minimally presented by

$$\{((0,0,1),(1,1,0)),((2n+1,0,0),(0,2,0))\}.$$

The monoid S is isomorphic to $\mathbb{N}^4/\sim_M$, where M is the subgroup of $\mathbb{Z}^4$ whose defining equations are

$$\begin{aligned} 2x+(2n+1)y+(2n+3)z &= 0,\\ x+y+z+t &= 0, \end{aligned}$$

and S' is isomorphic to $\mathbb{N}^3/\sim_{M'}$, where M' is the subgroup of $\mathbb{Z}^3$ with defining equation

$$2x+(2n+1)y+(2n+3)z = 0.$$

Hence

$$(x_1,x_2,x_3,x_4) \sim_M (y_1,y_2,y_3,y_4)$$

if and only if

$$\begin{gathered} (x_1,x_2,x_3) \sim_{M'} (y_1,y_2,y_3),\\ x_1+x_2+x_3+x_4 = y_1+y_2+y_3+y_4. \end{gathered}$$

Thus $\sim_{M'}$ is the projection of $\sim_M$ and we can apply Theorem 11.6 (in this case, $a_i = 1$ for all i). This implies that applying Algorithm CPC to

$$\{((1,1,0),(0,0,1)),((2n+1,0,0),(0,2,0))\}$$

for the linear admissible order $\preceq_1$, the cardinality of the output ρ_1 equals the cardinality of the canonical system of generators ρ_2, with respect to $\preceq_2$, of the congruence associated to S. By Proposition 9.13, the cardinality of ρ_2 is greater than or equal to $2n$,

whence the same holds for ρ_1, in contrast with the fact that every minimal presentation of S' has only two elements.

2.2. Applications to numerical semigroups. We use Theorem 11.6 for determining an alternative way for constructing a presentation of a numerical semigroup. Let S be the numerical semigroup with minimal generating system $\{n_1,\dots,n_p,n_{p+1}\}$. By Proposition 3.1, S is isomorphic to $\mathbb{N}^{p+1}/\sigma$ where σ is the congruence associated to the subgroup

$$M=\{(x_1,\dots,x_{p+1}) \mid n_1x_1+\dots+n_{p+1}x_{p+1}=0\}$$

of $\mathbb{Z}^{p+1}$.

Let M' be the subgroup of $\mathbb{Z}^p$ defined by

$$M'=\{(x_1,\dots,x_p) \mid n_1x_1+\dots+n_px_p\equiv 0 \pmod{n_{p+1}}\},$$

and let σ' be the corresponding congruence on $\mathbb{N}^p$, that is $\sigma'=\sim_{M'}$.

Clearly, σ' is the projection of σ in the sense mentioned above, since

$$(x_1,\dots,x_{p+1})\ \sigma\ (y_1,\dots,y_{p+1})$$

if and only if

$$(x_1,\dots,x_p)\ \sigma'\ (y_1,\dots,y_p) \text{ and } n_1x_1+\dots+n_{p+1}x_{p+1}=n_1y_1+\dots+n_{p+1}y_{p+1}.$$

(In this case $a_i=n_i$ for all i.)

Hence we can reconstruct a system of generators of σ from a system of generators of σ'. Of course, first of all, we must give a procedure to obtain a system of generators of σ'.

Assume that $B'=\{u_1^+-u_1^-,\dots,u_p^+-u_p^-\}$ is a basis of M', where for every i, u_i^+ and u_i^- are nonnegative p–tuples. (The basis B' can be computed easily using the procedure presented in Chapter 2 for finding a basis of a subgroup of $\mathbb{Z}^n$ given by a system of equations.)

Define

$$\rho=\{((n_{p+1},0,\dots,0),(0,\dots,0)),((0,n_{p+1},\dots,0),(0,\dots,0)),\dots$$
$$\dots,((0,\dots,0,n_{p+1}),(0,0,\dots,0)),(u_1^+,u_1^-),\dots,(u_p^+,u_p^-)\}$$

and let τ be the congruence on $\mathbb{N}^p$ generated by ρ. Then $M_\tau=M'$ (the elements $(0,\dots,0,n_{p+1},0,\dots,0)$ satisfy the equations of M'). In addition, $\mathbb{N}^p/\tau$ is in fact a group, since for every $i=1,\dots,p$, $[e_i]_\tau+[(n_{p+1}-1)e_i]_\tau=[0]_\tau$, which implies that $[e_i]_\tau$ is a unit in $\mathbb{N}^p/\tau$. Hence $\mathbb{N}^p/\tau$ is a cancellative monoid, and consequently $\tau=\sim_{M_\tau}=\sim_{M'}=\sigma'$. Therefore ρ is a generating system for the congruence σ'. This enables us to compute a canonical system of generators of σ' with respect to $\preceq_1$ (Algorithm CPC) and then use Theorem 11.6 for obtaining a system of generators of σ and therefore a presentation of S.

We illustrate this procedure with an example.

EXAMPLE 11.7. Let S be the numerical semigroup generated by $\{5,7,9\}$. We want to compute a system of generators for the congruence σ such that S is isomorphic to $\mathbb{N}^3/\sigma$. The groups M and M' are

$$M = \{(x,y,z) \in \mathbb{Z}^3 \mid 5x+7y+9z = 0\},$$

$$M' = \{(x,y) \in \mathbb{Z}^2 \mid 5x+7y \equiv 0 \bmod 9\},$$

respectively. A basis for M' is $\{(1,-2),(4,1)\}$. This implies that

$$\rho = \{((9,0),(0,0)),((0,9),(0,0)),((1,0),(0,2)),((4,1),(0,0))\}$$

generates σ'. Next, we must compute a canonical system of generators of σ with respect to the ordering $(x,y) \preceq_1 (x',y')$ if and only if $5x+7y < 5x'+7y'$ or $5x+7y = 5x'+7y'$ and $(x,y) \preceq_{lex} (x',y')$. The resulting canonical system of generators is

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

Applying Theorem 11.6, we get that $2\times 7 = 1\times 5 + 1\times 9$, $5\times 5 = 1\times 7 + 2\times 9$ and $4\times 5 + 1\times 7 = 3\times 9$, which means that

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

is a canonical system of generators of σ with respect to the ordering $\preceq_2$ (and consequently a presentation of S). ◇

Remarks

In this chapter we have shown that every cancellative congruence is the projection of the congruence associated to an affine semigroup. This is one of the ideas used in [**56**] to give an algorithm for computing a presentation of a cancellative monoid and for determining whether a semigroup given in terms of a presentation is cancellative. In [**55**] the method is generalized to strongly reduced monoids and it is shown that the congruence associated to a finitely generated monoid is the projection of the congruence associated to a finitely generated strongly reduced monoid. As a consequence of this result, it is derived that we can "theoretically" compute a presentation of any finitely generated monoid. Some of these ideas where exposed in [**54**].

Exercises

1. Show that if σ is a congruence on $\mathbb{N}^{n+1}$ and σ' its projection in $\mathbb{N}^n$, then σ' is a congruence on $\mathbb{N}^n$. Prove also that if ρ is minimal system of generators of σ, then its projection is a system of generators for σ'.
2. Prove that σ' is the projection of σ if and only if the projection of a system of generators of σ is a system of generators of σ'.
3. Let M be the subgroup of $\mathbb{Z}^n$ with defining equation

$$a_1x_1 + \ldots + a_nx_n \equiv 0 \pmod{b}.$$

Show that $\sim_M$ has a system of generators with, at most, $2n$ elements.

4. Prove that for every congruence σ on $\mathbb{N}^n$, there exists a congruence $\overline{\sigma}$ on $\mathbb{N}^{n+1}$ such that σ is the projection of $\overline{\sigma}$ and $\mathbb{N}^{n+1}/\overline{\sigma}$ is reduced.
5. Prove that for every congruence σ on $\mathbb{N}^n$ there exists a congruence $\overline{\sigma}$ on $\mathbb{N}^{n+1}$ such that σ is the projection of $\overline{\sigma}$ and every $\overline{\sigma}$-class has finitely many elements.
6. Let σ be a congruence on $\mathbb{N}^{n+1}$ and let σ' be its projection in $\mathbb{N}^n$.
   (a) Prove that if $\mathbb{N}^{n+1}/\sigma$ is cancellative, then so is $\mathbb{N}^n/\sigma'$.
   (b) Prove that if $\mathbb{N}^{n+1}/\sigma$ is a group, then so is $\mathbb{N}^n/\sigma'$.
   (c) Find a congruence σ such that $\mathbb{N}^{n+1}/\sigma$ is torsion free but $\mathbb{N}^n/\sigma'$ is not torsion free.
   (d) Find a congruence σ such that $\mathbb{N}^{n+1}/\sigma$ is reduced but $\mathbb{N}^n/\sigma'$ is not reduced.
7. Let σ be a congruence on $\mathbb{N}^n$. Show that there exists a congruence σ' on $\mathbb{N}^{n+1}$ such that σ is the projection of σ' and such that $\mathbb{N}^{n+1}/\sigma'$ is isomorphic to $\mathbb{N}^n/\sigma$.
8. Let S be a numerical semigroup minimally generated by $\{n_0, \ldots, n_p\}$. Let σ be a congruence on $\mathbb{N}^{p+1}$ such that S is isomorphic to $\mathbb{N}^{p+1}/\sigma$. If σ' is the projection of σ, then $\mathbb{N}^p/\sigma'$ is a group. Show that this statement is not true for affine semigroups in general.

CHAPTER 12

Finite torsion free monoids

In this chapter we study the relationship between finite torsion free monoids and finite lattices. We shall prove that a finite torsion free monoid can be regarded as a finite lattice with respect to an appropriate order induced by $+$ and that any finite lattice has structure of a torsion free monoid with the operation $\vee$.

1. Presentations of finite torsion free monoids

We start by studying the form of the congruences associated to finite monoids and give a characterization of finite monoids in terms of a canonical system of generators of its associated congruence. This characterization will be adapted to the torsion free case.

PROPOSITION 12.1. *Let σ be a congruence on $\mathbb{N}^n$. The monoid $\mathbb{N}^n/\sigma$ is finite if and only if every canonical system of generators of σ is of the form*

$$\{(k_1e_1,b_1),\dots,(k_ne_n,b_n),(a_{n+1},b_{n+1}),\dots,(a_t,b_t)\}$$

for some $k_1,\dots,k_n \in \mathbb{N}\setminus\{0\}$.

PROOF. *Necessity.* Let

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

be a canonical system of generators of σ. Since $\mathbb{N}^n/\sigma$ is finite, the set

$$\mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_t)$$

is finite. Hence for every $1 \le i \le n$, we have that

$$\{ke_i \mid k \in \mathbb{N}\} \not\subseteq \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_t).$$

Therefore there exits $t_i \in \mathbb{N}$ such that $t_ie_i \notin \mathrm{Ap}(\mathbb{N}^n,a_1,\dots,a_t)$, which means that $a_j \le t_ie_i$ for some j and consequently $a_j = k_ie_i$, with $k_i \in \mathbb{N}\setminus\{0\}$.

Sufficiency. This implication is a straightforward consequence of the fact that

$$\mathrm{Ap}(\mathbb{N}^n,k_1e_1,\dots,k_ne_n,a_{n+1},\dots,a_t) \subseteq \mathrm{Ap}(\mathbb{N}^n,k_1e_1,\dots,k_ne_n)$$

and this latter set is finite (see exercises at the end of Chapter 6). □

Before studying the torsion free version of Proposition 12.1, we need a result which describes finite torsion free cyclic monoids.

LEMMA 12.2. *Up to isomorphisms, the monoid $\mathbb{N}/\langle\{(2,1)\}\rangle = \mathbb{N}_{(2,1)}$ is the only nontrivial finite torsion free cyclic monoid.*

PROOF. Assume that $S \neq \{0\}$ is a finite torsion free cyclic monoid. By Proposition 5.13, there exist $a, b \in \mathbb{N}$, $a > b$ such that S is isomorphic to $\mathbb{N}_{(a,b)}$. Assume that $a \geq 3$. Then $[1] \neq [2]$ and $(a(a-b), 2a(a-b)) \in \langle\{(a,b)\}\rangle$, since

$$\mu([a(a-b)]) = b + ((a(a-b) - b) \bmod (a-b)) = b + (-b \bmod (a-b)) =$$

$$= b + ((2a(a-b) - b) \bmod (a-b)) = \mu([2a(a-b)]),$$

where μ is the function minimum associated to $\langle\{(a,b)\}\rangle$ for a certain linear admissible order (see Chapter 5). Hence $a(a-b)[1] = a(a-b)[2]$ and $a(a-b) \neq 0$, which implies that S is not torsion free. Thus a must be less than three and since S is not trivial, we have only two choices: $(a,b) = (2,1)$ or $(a,b) = (2,0)$. The second choice yields a non torsion free monoid and for the first one we have that $\mathbb{N}/\langle\{(2,1)\}\rangle$ is torsion free, since $[k] = [1]$ for all $k \in \mathbb{N} \setminus \{0\}$. □

We use Lemma 12.2 in order to give a result for torsion free monoids similar to Proposition 12.1.

THEOREM 12.3. *Let σ be a congruence on $\mathbb{N}^n$. The monoid $\mathbb{N}^n/\sigma$ is finite and torsion free if and only if $(2e_i, e_i) \in \sigma$ for all $i \in \{1, \ldots, n\}$.*

PROOF. *Necessity.* Take $i \in \{1, \ldots, n\}$. Since $\mathbb{N}^n/\sigma$ is finite, the submonoid of $\mathbb{N}^n/\sigma$ generated by $[e_i]$ is cyclic, finite and torsion free. By Lemma 12.2, the monoid $\langle[e_i]\rangle$ is isomorphic to $\mathbb{N}_{(2,1)}$, which implies that $2[e_i] = [e_i]$, whence $(2e_i, e_i) \in \sigma$.

Sufficiency. Since $(2e_i, e_i) \in \rho$, we deduce that $(ke_i, e_i) \in \sigma$ for all $k \in \mathbb{N} \setminus \{0\}$, which implies that $(ka, a) \in \sigma$ for all $a \in \mathbb{N}^n$. If $k[a] = k[b]$, that is to say, $(ka, kb) \in \sigma$, then $(ka, a) \in \sigma$ and $(kb, b) \in \sigma$. By transitivity and symmetry, we have $(a, b) \in \sigma$, which means that $[a] = [b]$. Therefore $\mathbb{N}^n/\sigma$ is torsion free.

Another consequence of the fact that $(2e_i, e_i) \in \sigma$ for all i, is that every σ-class has an element whose coordinates are in $\{0, 1\}$. Thus there are at most 2^n different elements in $\mathbb{N}^n/\sigma$. □

2. Finite lattices

Here we give some classical results concerning finite lattices. We shall establish the connection between finite torsion free monoids and finite lattices.

Let X be a set and let $\leq$ be a partial order on X (that is, a binary relation on X which is reflexive, antisymmetric and transitive). Given two elements x and y in X, we say that $z \in X$ is the **supremum** of x and y, and denote it by $x \vee y$, if the following conditions hold:

1. $x \leq z$,
2. $y \leq z$,
3. for any $t \in X$ such that $x \leq t$ and $y \leq t$, we have that $z \leq t$.

Analogously, the element $z \in X$ is the **infimum** of x and y, and we denote it by $x \wedge y$, if the following conditions hold:

1. $z \leq x$,

2. $z \leq y$,
3. for any $t \in S$ such that $t \leq x$ and $t \leq y$, we have that $t \leq z$.

The element $x \vee y$ might not exist, but if it does, then it can be easily shown that it is unique. The same holds for $x \wedge y$.

The set X is an **upper semilattice** if for every two elements in X, their supremum exists. Dually, the set X is a **lower semilattice** if the infimum of any two elements exists. If both supremum and infimum exist for every pair of elements of X, then we say that X is a **lattice**.

If X is an upper semilattice, then we can think of X as a set with a binary operation $\vee$ fulfilling the associative, commutative and idempotent (for all $x \in X, x \vee x = x$) laws (which are straightforward to prove).

Conversely, we have the following result.

PROPOSITION 12.4. *Let S be a set with a binary operation $+$ verifying the associative, commutative and idempotent laws. Define on S the binary relation $a \leq b$ if $a+b=b$. Then $\leq$ is a partial order on S for which $(S, \leq)$ is an upper semilattice with $a \vee b = a+b$ for all $a, b \in S$.*

PROOF. First, we show that $\leq$ is a partial order on S.

1. Reflexive: $a+a=a$, since $+$ fulfills the idempotent property.
2. Antisymmetric: Assume that $a \leq b$ and $b \leq a$. Then $a+b=b$ and $b+a=a$, whence $a=b+a=a+b=b$.
3. Transitive: Let a, b, c be elements in S such that $a \leq b$ and $b \leq c$. Then $a+b=b$ and $b+c=c$. Hence
$$a+c=a+(b+c)=(a+b)+c=b+c=c$$
and thus $a \leq c$.

Finally, we show that $a+b=a \vee b$ and in this way we prove that for every two elements, its supremum exits.

1. $a+(a+b)=(a+a)+b=a+b$, which means that $a \leq a+b$.
2. $b+(a+b)=(b+a)+b=(a+b)+b=a+(b+b)=a+b$ and therefore $b \leq a+b$.
3. Assume that there exists $c \in S$ such that $a \leq c$ and $b \leq c$. Then $a+c=c=b+c$. Hence
$$(a+b)+c=a+(b+c)=a+c=c,$$
which implies that $a+b \leq c$.

□

If S is as in Proposition 12.4 and S has an identity element 0, then 0 is the minimum with respect to the order $\leq$, since $0+a=a$ for all $a \in S$ and this means that $0 \leq a$. This is exactly the condition we impose to a finite upper semilattice in order to make it a lattice.

LEMMA 12.5. *Every finite upper semilattice with minimum is a finite lattice.*

PROOF. Let L be a finite upper semilattice, with respect to the partial order $\leq$, for which there exists $\min_{\leq}(L)$. We must show that for every $a,b \in L$ there exists the element $x \wedge y$. Let

$$\{x_1, \dots, x_n\} = \{x \in L \mid x \leq a, x \leq b\}.$$

This set is not empty since $\min_{\leq}(L)$ is one of its elements. Since $\vee$ satisfies the associative law, it makes sense to write $x_1 \vee x_2 \vee \cdots \vee x_n$. We show that

$$x \wedge y = x_1 \vee x_2 \vee \cdots \vee x_n \in S.$$

1. Since $x_i \leq a$, it follows that $x_1 \vee \cdots \vee x_n \leq a$.
2. For the same reason, $x_1 \vee \cdots \vee x_n \leq b$.
3. If $c \leq a$ and $c \leq b$, then $c \in \{x_1, \dots x_n\}$ and consequently $c \leq x_1 \vee \cdots \vee x_n$.

□

We are now ready to prove the equivalence between finite torsion free monoids and finite lattices.

THEOREM 12.6. *Let S be a finite set with a binary operation $+$. The following conditions are equivalent:*

(i) *with the operation $+$, S is a torsion free monoid,*
(ii) *with the operation $+$, S is a monoid satisfying the idempotent law,*
(iii) *the set S together with the partial order defined by $a \leq b$ if $a+b=b$, is a lattice.*

PROOF. *(i) implies (ii)* Since S is finite, it is finitely generated and thus there exists a congruence σ on $\mathbb{N}^n$ such that S is isomorphic to $\mathbb{N}^n/\sigma$. By Theorem 12.3, we have that $2[e_i] = [e_i]$ for all $i \in \{1, \dots, n\}$. It follows easily that $2[a] = [a]$ for all $[a] \in \mathbb{N}^n/\sigma$.

(ii) implies (iii) By Proposition 12.4, we have that S is a finite upper semilattice with respect to the partial order $a \leq b$ if and only if $a+b=b$. Since $0 = \min_{\leq}(S)$, we can use Lemma 12.5 to assert that S is a lattice with respect to the partial order $\leq$.

(iii) implies (i) As we have seen before, $a \vee b = a+b$, so $+$ is associative, commutative and idempotent. Since S is a finite lattice, $\bigwedge_{s \in S} s$ is the minimum of S and consequently the identity element under $+$. Finally, since $+$ is idempotent $ka = a$ for any $k \in \mathbb{N} \setminus \{0\}$; whence if $ka = kb$, then $a = b$. □

Proposition 12.4 asserts that if S is a set with a binary operation $+$ satisfying the associative, commutative and idempotent laws, then S has the structure of an upper semilattice. If in addition S is finite and has a minimum (the identity element of $(S,+)$), then S becomes a lattice. Next we give a different approach to provide a characterization for lattices, but this time with two binary operations on the given set. The idea is the following. If X is a lattice, then it can be easily show that $\wedge$ and $\vee$ fulfill the associative, commutative, idempotent and absorption (for every $a,b \in X$, $x \vee (x \wedge y) = x$ and $x \wedge (x \vee y) = x$) laws.

The converse of this fact is also true, and therefore these four properties characterize the structure of lattice on a set.

PROPOSITION 12.7. *Let S be a set with two binary operations $+$ and $\cdot$ satisfying the associative, commutative, idempotent and absorption laws. Take $\leq$ to be the binary relation on S defined by $a \leq b$ if $a+b=b$. Then S, with this binary relation, is a lattice such that for all $a,b \in S$, $a \vee b = a+b$ and $a \wedge b = a \cdot b$.*

PROOF. By Proposition 12.4, we already know that S, with the partial order $\leq$, is an upper semilattice such that $a \vee b = a+b$ for all $a,b \in S$. The only thing left to prove is that $a \wedge b$ is equal to $a \cdot b$.

1. Since $(a \cdot b)+a = a+(a \cdot b) = a$ (commutative and absorption laws), we have that $a \cdot b \leq a$.
2. Likewise $a \cdot b \leq b$.
3. If $c \leq a$ and $c \leq b$, then $c+a=a$ and $c+b=b$. Since $c \cdot (c+a) = c$ (absorption law) and $c \cdot (c+a) = c \cdot a$, then $c = c \cdot a$. Similarly, we obtain that $c = c \cdot b$. Thus
$$c \cdot (a \cdot b) = (c \cdot a) \cdot b = c \cdot b = c,$$
whence
$$a \cdot b = (c \cdot (a \cdot b)) + (a \cdot b) = c + (a \cdot b).$$
Therefore $c \leq a \cdot b$.

□

Summarizing, we obtain the following statement.

THEOREM 12.8. *Let $(S,+,\cdot)$ be a set with two binary operations. The following conditions are equivalent.*

1. *The binary operations $+$ and $\cdot$ satisfy the commutative, associative, idempotent and absorption laws.*
2. *For every $a,b \in S$ the infimum and supremum of a and b (with respect to the partial order $a \leq b$ if and only if $a+b=b$) exists (and it can be computed as $a \wedge b = a \cdot b$ and $a \vee b = a+b$, respectively).*

In all this reasoning we could have defined $a \leq b$ if $a \cdot b = a$. As a matter of fact, the definitions of $a \leq b$ by $a+b=b$ and $ab=a$ are equivalent.

3. Finite Boolean algebras

We recall some classical results concerning Boolean algebras, including the structure theorem for finite Boolean algebras.

A **Boolean algebra** B is a set with two binary operations $+$ and $\cdot$ satisfying the following properties.

1. *Commutative*: for every $a,b \in B$,
$$a+b = b+a \text{ and } a \cdot b = b \cdot a.$$
2. *Associative*: for every $a,b,c \in B$,
$$(a+b)+c = a+(b+c) \text{ and } (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

3. *Identity element*: There exists $0, 1 \in B$ such that for every element $a \in B$
$$a+0=a \text{ and } a \cdot 1 = a.$$
4. *Complement*: for every $a \in B$, there exists $\overline{a}$ such that
$$a+\overline{a}=1 \text{ and } a \cdot \overline{a}=0.$$
5. *Distributive*: for every $a,b,c \in B$,
$$a \cdot (b+c) = (a \cdot b)+(a \cdot c) \text{ and } a+(b \cdot c) = (a+b) \cdot (a+c).$$

We refer to $\overline{a}$ as the **complement** of a. It can be easily shown that the complement is unique and thus it makes sense to think of it as a function of a.

In order to simplify notation, the element $a \cdot b$ is denoted by ab. We give precedence to the operation of product, which enables us to write $ab+c$ instead of $(ab)+c$.

A lattice L is a **distributive lattice** if for every $a,b,c \in L$,
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \text{ and } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

We say that the lattice L (with respect to the order $\leq$) is a **complemented lattice** if

1. there exists the minimum of L, say 0;
2. there exists the maximum of L, say 1;
3. for every $a \in L$, there exists $\overline{a} \in L$ such that
$$a \vee \overline{a} = 1 \text{ and } a \wedge \overline{a} = 0.$$

The following result is straightforward to prove just using these definitions.

PROPOSITION 12.9. *Every distributive complemented lattice is a Boolean algebra with the operations* $\vee$ *and* $\wedge$.

We show that the converse is also true.

PROPOSITION 12.10. *Let B be a Boolean algebra. Then for every $a \in B$, we have*
$$a+a=a=aa, \ a+1=1 \text{ and } a \cdot 0 = 0.$$
Furthermore, for every $a,b \in B$, we get
$$a+(ab)=a=a(a+b).$$

PROOF. Using Theorem 12.8, we only have to prove that $+$ and $\cdot$ satisfy the idempotent and absorption laws.

Let a be an element in B. Since $a\overline{a}=0$, we have
$$a=a+0=a+(a\overline{a})=(a+a)(a+\overline{a})=(a+a)1=a+a.$$
From $a+\overline{a}=1$, we obtain
$$a=a1=a(a+\overline{a})=aa+a\overline{a}=aa+0=aa.$$
It follows that
$$a+1=a+(a+\overline{a})=(a+a)+\overline{a}=a+\overline{a}=1,$$
$$a0=a(a\overline{a})=(aa)\overline{a}=a\overline{a}=0.$$

Finally,

$$a = a1 = a(1+b) = a1 + ab = a + (ab),$$

$$a = a + 0 = a + (0b) = (a+0)(a+b) = a(a+b).$$

□

As a consequence of this result and Theorem 12.8, we obtain the following assertion.

COROLLARY 12.11. *Let $(B,+,\cdot)$ be a set with two binary operations. The following conditions are equivalent:*

(i) *B is a Boolean algebra,*
(ii) *B is a distributive complemented lattice under the partial order $a \leq b$ if $a+b=b$ (equivalently $ab=a$), for which $a \vee b = a+b$ and $a \wedge b = ab$.*

3.1. Structure theorem for finite Boolean algebras. For every finite set X, the **power set** of X, denoted by $\mathcal{P}(X)$, is the set of all subsets of X. The reader can check that $\mathcal{P}(X)$, with the binary operations $\cup$ and $\cap$, is a Boolean algebra. From the lattice point of view, the partial order considered in $\mathcal{P}(X)$ is the order defined by the inclusion. With this order, $\cup$ becomes the supremum and $\cap$ the infimum of any two subsets of X. Our next goal is to show that every finite Boolean algebra is "isomorphic" to the power set of a finite set. In $\mathcal{P}(X)$ an element $A \in \mathcal{P}(X) \setminus \{\emptyset\}$ is equal to $\bigcup_{a \in A}\{a\}$. That is to say, every nonempty element in $\mathcal{P}(X)$ can be expressed as the supremum of elements of the form $\{a\}$, with $a \in X$. An element a belongs to $A \subseteq X$ if $\{a\} \cap A = \{a\}$ and it does not belong to A whenever $\{a\} \cap A = \emptyset$. This is the idea of the definition of an atom in a Boolean algebra.

Let B be a Boolean algebra. The element a in $B \setminus \{0\}$ is an **atom** if for every $b \in B$ we have that either $ab = a$ or $ab = 0$. As in $\mathcal{P}(X)$, the atoms are the minimal elements with respect to the order induced by $\cup$. This fact is pointed out in the next result. By Corollary 12.11, we know that "$+ = \vee$", "$\cdot = \wedge$" and $a \leq b$ if and only if $a+b=b$ or equivalently $ab = a$.

PROPOSITION 12.12. *Let B be a Boolean algebra. The element a is an atom of B if and only if it belongs to* $\mathrm{Minimals}_{\leq}(B \setminus \{0\})$.

PROOF. *Necessity.* Take $b \in B$ be such that $b \leq a$. Then $ba = b \wedge a = b$. However $ab = a$ or $ab = 0$, which leads to $b = a$ or $b = 0$.

Sufficiency. For every $b \in B$, we have that $ab = a \wedge b \leq a$. Hence either $ab = a$ or $ab = 0$. □

The fact that for every $a \neq b \in X$, we have that $\{a\} \cap \{b\} = \emptyset$, is expressed in terms of atoms as follows.

PROPOSITION 12.13. *Let a and b be two different atoms of a Boolean algebra B. Then $ab = 0$.*

PROOF. Assume that $ab \neq 0$. Since a is an atom this forces $ab = a$ and as b is also an atom, we have $ba = b$. Thus $a = b$. □

With these two results we are ready to prove that every nontrivial element in a finite Boolean algebra can be expressed as the supremum of a set of atoms.

THEOREM 12.14. *Let B be a finite Boolean algebra. For every element $a \in B \setminus \{0\}$ there exists a set of atoms $\{a_1, \dots, a_n\}$ such that $a = a_1 + \cdots + a_n$. Furthermore, the set $\{a_1, \dots, a_n\}$ is the only set of atoms satisfying this condition, that is, this expression of a is unique up to rearrangement of the elements $a_1, \dots, a_n$.*

PROOF. Let a be an element in $B \setminus \{0\}$. Take $\{a_1, \dots, a_n\}$ to be the set of atoms x of B such that $x \leq a$. Since

$$a_1 + \cdots + a_n = a_1 \vee \cdots \vee a_n,$$

and $a_i \leq a$ for all i, we obtain that $a_1 + \cdots + a_n \leq a$. Set $b = a_1 + \cdots + a_n$ and assume that $a\overline{b} \neq 0$. Since B is finite, it can be shown that there exists a minimal element of $B \setminus \{0\}$ such that $c \leq a\overline{b}$ (the argument is easier than the one used in Corollary 5.4). In addition, $a\overline{b} = a \wedge \overline{b}$, whence $c \leq a$ and $c \leq \overline{b}$. Thus there exists $i \in \{1, \dots, n\}$ such that $c = a_i$. Clearly $c = a_i \leq a_1 \vee \cdots \vee a_n = b$ and as $c \leq \overline{b}$, we deduce that $c \leq b \wedge \overline{b} = 0$, which leads to $c = 0$, contradicting the fact that $c \in B \setminus \{0\}$. Therefore $a\overline{b}$ must be equal to 0. Hence

$$b = b + 0 = b + (a\overline{b}) = (b + a)(b + \overline{b}) = (b + a)1 = b + a,$$

which means that $a \leq b$. Since we have already shown that $b \leq a$, we can assert that

$$a = b = a_1 + \cdots + a_n.$$

Now, assume that

$$a_1 + \cdots + a_n = a'_1 + \cdots + a'_m,$$

with $a'_1, \dots, a'_m$ atoms of B, and let us show that

$$\{a_1, \dots, a_n\} = \{a'_1, \dots, a'_m\}.$$

Trivially $a'_i \leq a'_1 + \cdots + a'_m = a_1 + \cdots + a_n = a$. Hence

$$a'_i = a'_i \wedge a = a'_i(a_1 + \cdots + a_n) = a'_i a_1 + \cdots + a'_i a_n.$$

By Proposition 12.13, we have that $a'_i a_j = 0$ whenever $a'_i \neq a_j$. Thus there exists $j \in \{1, \dots, n\}$ such that $a'_i = a_j$ and consequently $a'_i \in \{a_1, \dots, a_n\}$. The other inclusion is proven similarly. □

With this set of results, we have shown that a finite Boolean algebra "behaves" like the power set of a finite set. To make this precise, we need to introduce the concept of isomorphism of Boolean algebras. Given two Boolean algebras A and B, a **morphism of Boolean algebras** from A to B is a map $f : A \to B$ satisfying that for all $a, b \in A$,

1. $f(a + b) = f(a) + f(b)$,
2. $f(ab) = f(a)f(b)$.

As usual, if f is injective (respectively surjective, bijective), then we say that f is a **monomorphism** (respectively **epimorphism, isomorphism**). It is easy to prove that if f is an isomorphism, then so is f^{-1}. We say that A and B are isomorphic if there exists an isomorphism of Boolean algebras $f : A \to B$.

THEOREM 12.15. *Let B be a finite Boolean algebra and let* $\mathrm{At}(B)$ *be the set of atoms of B. Then B is isomorphic to the Boolean algebra $\mathcal{P}(\mathrm{At}(B))$, with the binary operations of union and intersection of sets.*

PROOF. Define

$$\varphi : \mathcal{P}(\mathrm{At}(B)) \to B,\ \varphi(\{a_1, \dots, a_n\}) = a_1 + \cdots + a_n \text{ and } \varphi(\emptyset) = 0.$$

The reader can check that this map is a morphism of Boolean algebras. Theorem 12.14 ensures that this map is bijective. □

As a consequence of this result, if B is a finite Boolean algebra with n atoms, then the cardinality of B is 2^n.

COROLLARY 12.16. *Let A and B be to finite Boolean algebras. Then A and B are isomorphic if and only if the have the same cardinality.*

PROOF. Clearly, if A and B are isomorphic, then they have the same amount of elements.

If A and B have n and m atoms, respectively, then the cardinalities of A and B are 2^n and 2^m, respectively. Thus $2^n = 2^m$ implies $n = m$ and that A and B are both isomorphic to $\mathcal{P}(\{1, \dots, n\})$. □

4. Boolean monoids

If S is a finite torsion free monoid, then Theorem 12.6 ensures that S is a lattice with respect to the partial order $a \leq b$ if and only if $a + b = b$. Furthermore, the supremum of a and b is $a + b$. It may happen that S is not only a lattice, but a Boolean algebra as well. In this case we say that S is a **Boolean monoid**. In other words, a finite torsion free monoid S is a Boolean monoid if and only if S as a lattice is distributive and complemented. An element a in a Boolean monoid S is an atom if a is an atom of S as a Boolean algebra. Theorem 12.14 can be translated to the language of Boolean monoids as follows. (Observe that the binary operation $+$ of the Boolean algebra S is the binary operation $+$ of the monoid S.)

THEOREM 12.17. *Let S be a Boolean monoid. The set of atoms of S is the only minimal system of generators of S.*

PROOF. Let $A = \{a_1, \dots, a_n\}$ be the set of atoms of S. By Theorem 12.14, every element $a \in S$ can be expressed as $a = a_{i_1} + \cdots + a_{i_k}$, with $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$. This implies that $S = \langle A \rangle$. In order to show that A is the only minimal system of generators of S, let us show that every system of generators must contain A. This follows from the fact that if $a \in A$ and $a = b + c$, then $b \leq a$ and $c \leq a$ and by Proposition 12.12, we have that either $b = a$ or $c = a$. □

The following theorem is the monoid counterpart of Theorem 12.15. Observe that if X is a finite set, then $\mathcal{P}(X)$ with the binary operation $\cup$ is a monoid.

THEOREM 12.18. *Let S be a Boolean monoid and let A be the set of atoms of S. Then S is isomorphic, as a monoid, to $(\mathcal{P}(A), \cup)$.*

Before studying the presentations of Boolean monoids we need a lemma that ensures that the structure of a Boolean monoid is preserved by monoid isomorphisms.

LEMMA 12.19. *Let $f : S \to T$ be an isomorphism of monoids. If S is a Boolean monoid, then so is T.*

PROOF. Since S is a Boolean monoid, it is finite and torsion free. Hence T is also finite and torsion free. By Theorem 12.6, we have that T is an upper semilattice with respect to the partial order $a \leq b$ if and only if $a+b=b$. Furthermore, $0 \in T$ satisfies that $0+t=t$ for all t in T and hence $0 = \min_{\leq} T$. This implies, using Lemma 12.5, that T is a lattice. Let us show that $f(a \wedge b) = f(a) \wedge f(b)$ (using Boolean algebra notation $f(ab) = f(a)f(b)$).

1. Since
$$f(a)+f(a\wedge b) = f(a+(a\wedge b)) = f(a\vee(a\wedge b)) = f(a),$$
we obtain $f(a\wedge b) \leq f(a)$.
2. Analogously $f(a\wedge b) \leq f(b)$.
3. Assume that $t \in T$ is such that $t \leq f(a)$ and $t \leq f(b)$. Since f is surjective, there exists $c \in S$ such that $f(c) = t$. Hence $f(c)+f(a) = f(a)$ and $f(c)+f(b) = f(b)$. Thus $f(c+a) = f(a)$ and $f(c+b) = f(b)$, which means that $c+a=a$ and $c+b=b$. It follows that $c \leq a$ and $c \leq b$, which leads to $c \leq a\wedge b$. Therefore $c+(a\wedge b) = a\wedge b$ and as f is a morphism of monoids, we have $f(c)+f(a\wedge b) = f(a\wedge b)$. Therefore $t = f(c) \leq f(a\wedge b)$.

So far we have shown that T is a lattice and that $f(a\wedge b) = f(a)\wedge f(b)$ (the fact $f(a\vee b) = f(a)\vee f(b)$ follows from the fact that f is a morphism of monoids and the supremum coincides with addition). The only thing left to prove is that T is distributive and complemented.

1. *T is distributive.* Take $x,y,z \in T$, we must prove that
$$x\vee(y\wedge z) = (x\vee y)\wedge(x\vee z), x\wedge(y\vee z) = (x\wedge y)\vee(x\wedge z).$$
Since f is surjective, there exist $a,b,c \in S$ such that $f(a) = x$, $f(b) = y$ and $f(c) = z$. The proof uses the fact that f preserves $\vee$ and $\wedge$, and that S is distributive.
2. *T is complemented.* We have already pointed out that 0 is the minimum of T (observe also that $f(0) = 0$, since $f(0+c) = f(0)+f(c) = f(c)$ and this leads to $f(0) \leq f(c)$ for all $c \in S$, which means that $f(0)$ is the minimum of T). Take $t \in T$. Then there exists $s \in S$ such that $f(s) = t$. Since $s \leq 1 \in S$, we have that $s+1 = 1$ and consequently $f(s)+f(1) = f(s+1) = f(1)$. Hence $f(1)$ is the maximum of T. We denote it by 1. In addition, since there exists

$\bar{s} \in S$ such that $s \vee \bar{s} = 1$ and $s \wedge \bar{s} = 0$, we have that $f(s) \vee f(\bar{s}) = f(1) = 1$ and $f(s) \wedge f(\bar{s}) = f(s \wedge \bar{s}) = f(0) = 0$. Thus $\bar{t} = f(\bar{s})$ and T is complemented.

We have shown that T is a distributive and complemented lattice, which, by Corollary 12.11, means that T is a boolean algebra and consequently a Boolean monoid. □

Finally, we describe the minimal presentations of Boolean monoids. This description turns out to be a characterization of Boolean monoids in terms of their presentations.

THEOREM 12.20. *Let $S = \mathbb{N}^n/\sigma$ be a finitely generated monoid. Then S is a Boolean monoid with n atoms if and only if for every admissible order $\preceq$ on $\mathbb{N}^n$ the set*

$$\{(2e_1, e_1), \dots, (2e_n, e_n)\}$$

is a canonical system of generators of σ with respect to $\preceq$.

PROOF. *Necessity.* Let ρ be a canonical system of generators of σ with respect to the linear admissible order $\preceq$. As usual, we denote the function minimum associated to $\preceq$ by μ (see Chapter 5). Using Theorem 12.3 and since S is finite and torsion free, we have that for all $i \in \{1, \dots, n\}$, the element $(2e_i, e_i)$ belongs to σ. Hence $\mathrm{Im}(\mu) \subseteq \{0,1\}^n$ and as the cardinality of S is equal to the cardinality of $\mathrm{Im}(\mu)$, we have that $\mathrm{Im}(\mu) = \{0,1\}^n$, which enforces ρ to be equal to

$$\{(2e_1, e_1), \dots, (2e_n, e_n)\}.$$

Sufficiency. Define

$$\varphi : \mathbb{N}^n/\sigma \to (\mathcal{P}(\{1, \dots, n\}), \cup), \ \varphi([(x_1, \dots, x_n)]) = \{i \mid x_i \neq 0\}.$$

It is easy to show that φ is a monoid isomorphism. Using Lemma 12.19, we get that $\mathbb{N}^n/\sigma$ is a Boolean monoid since $\mathcal{P}(\{1, \dots, n\})$ is a Boolean monoid. □

Remarks

The enumeration problem for finite lattices (and more generally for combinatorial objects involving transitivity) is a long standing open problem. No closed analytic formulae are known for it (see, for instance, [**2**] and [**29**]). Thus the most common way to enumerate this kind of object is to build up a procedure for constructing finite lattices in an inductive way. In this line, Kyuno obtained the number of finite lattices with up to nine elements (see [**31**]). Kyuno and Ito took one step further in [**32**]. Koda in [**38**] presented orderly algorithms to count the number of finite lattices with k elements, for $k \leq 13$.

k	Number of lattices with k elements
1	1
2	1
3	1
4	2
5	5
6	15
7	33
8	222
9	1078
10	5994
11	37622
12	262775
13	2018442

Exercises

1. Construct a monoid S with 12 elements such that S is neither cyclic nor torsion free.
2. Prove that if $\leq$ is a well order on the set X, then $(X, \leq)$ is a lattice.
3. Find a torsion free monoid with n elements for every $n \in \mathbb{N}$.
4. Show that the monoid $\mathbb{N}^3/\sigma$, with
$$\sigma = \langle (2e_1, e_1), (2e_2, e_2), (2e_3, e_3), (e_2 + e_3, e_1 + e_2), (e_1 + e_3, e_1 + e_2) \rangle,$$
is not distributive as a lattice.
5. Prove that there are torsion free monoids with 2^n elements which are not Boolean monoids.
6. Prove that if the complement of an element in a distributive lattice exists, then it is unique.
7. Give an example of a complemented lattice with elements having more than one complement.
8. Compute a presentation of the monoid $(\mathcal{P}(\{1,2,3\}), \cup)$.
9. Let $X = \{1,2,3\}$ with the restriction of the usual order on $\mathbb{N}$. Compute a presentation of $(X, \vee)$.
10. Prove that the cartesian product of two finite torsion free monoids is again a finite torsion free monoid.
11. Let $X = \{0,1\}^p$ with the operations
$$(x_1, \dots, x_p) + (y_1, \dots, y_p) = (\max\{x_1, y_1\}, \dots, \max\{x_p, y_p\}),$$
$$(x_1, \dots, x_p) \cdot (y_1, \dots, y_p) = (\min\{x_1, y_1\}, \dots, \min\{x_p, y_p\}).$$
Show that $(X, +, \cdot)$ is a Boolean algebra.

12. Prove that two finite Boolean monoids are isomorphic if and only if they have the same cardinality.
13. Prove that the cartesian product of two finite Boolean monoids is again a finite Boolean monoid.
14. Construct, up to isomorphisms, all torsion free monoids with five elements.
15. Prove that every finite torsion free monoid is reduced.

UNIVERSITAT DE BARCELONA

Biblioteca de Matemàtiques

Gran Via de les Corts Catalanes, 585
08007 Barcelona

CHAPTER 13

Archimedean Components

We show here how to compute the set of Archimedean components of a finitely generated monoid. As we shall see in the next chapter, this information is essential for determining whether a finitely generated monoid is separative and/or torsion free.

Since Archimedean components are semigroups but not monoids in general, we must transfer some of the concepts used so far to the language of semigroups. The definition of **congruence** on a semigroup is exactly the same as on monoids: an equivalence relation on S compatible with the addition. The **quotient semigroup** of a semigroup by a congruence is defined as for monoids. The idea of semigroup morphism is slightly different, since we do not have to impose that the image of the zero element is again the zero element. Thus a map f from the semigroup S to the semigroup S' is a **semigroup morphism** if for every $a,b \in S$ we have that $f(a+b) = f(a)+f(b)$. A **subsemigroup** T of a semigroup S is a subset of S such that $a+b \in T$ for all $a,b \in T$. The definition of **cancellative semigroup** is the same as the definition of cancellative monoid, that is, $a+c = b+c$ implies $a = b$. Note that in a cancellative monoid from $2a = a$, we can deduce that $a = 0$, since $2a = a+a = a = a+0$ and we can cancel a in the equality $a+a = a+0$. However, in general, we cannot do the same in cancellative semigroups, since we do not have an identity element. Given a semigroup S and a subset A of S, the **semigroup generated** by A is the smallest subsemigroup of S containing A. If there exists a finite subset A of S for which the semigroup S is the semigroup generated by A, then we say that S is **finitely generated.**

Given a monoid S we define the following binary relation over it:

$$a \leq_S b \text{ if } b = a+c \text{ for some } c \in S.$$

Clearly $\leq_S$ is reflexive and transitive. Moreover, if $a \leq_S b$, then $a+c \leq_S b+c$ for all $c \in S$. As usual, we write $a \geq_S b$ whenever $b \leq_S a$. We also define the binary relation $\mathcal{N}$ on S by

$$a\mathcal{N}b \text{ if there exists } k \text{ and } lin\mathbb{N}\setminus\{0\} \text{ such that } ka \geq_S b \text{ and } lb \geq_S a.$$

It is easy to check that $\mathcal{N}$ is a congruence. The elements of $S/\mathcal{N}$ are the **Archimedean components** of S.

PROPOSITION 13.1. *Let S be a monoid. The Archimedean components of S are subsemigroups of S.*

PROOF. Let C be an Archimedean component of S and let a,b be two elements of C. Then $a\mathcal{N}b$, whence there exist $k,l \in \mathbb{N}\setminus\{0\}$ such that $ka \geq_S b$ and $lb \geq_S a$.

Hence $(k+1)a = a+ka \geq_S a+b$ and trivially $1(a+b) = a+b \geq_S a$. This implies that $a\mathcal{N}(a+b)$ and consequently $a+b \in C$. □

Observe that 0 belongs only to one of the Archimedean components of S and for this reason an Archimedean component of S may not be a submonoid of S. The following example shows also that the Archimedean components do not have to be finitely generated (as semigroups), even in the case S is finitely generated.

EXAMPLE 13.2. It is easy to prove that the Archimedean components of $\mathbb{N}^2$ are

$$C_1 = \{0\},$$

$$C_2 = \{(a,0) \mid a \geq 1\},$$

$$C_3 = \{(0,a) \mid a \geq 1\},$$

$$C_4 = \{(a,b) \mid a \geq 1 \text{ and } b \geq 1\}.$$

Observe that C_4 is not finitely generated as a semigroup. The only Archimedean component of $\mathbb{N}^2$ which is a submonoid of $\mathbb{N}^2$ is C_1. ◇

Next we give an upper bound for the number of Archimedean components of a finitely generated monoid.

PROPOSITION 13.3. *Let S be a monoid generated by $\{n_1,\dots,n_p\}$. Then S has at most 2^p Archimedean components.*

PROOF. It suffices to show that for every $x \in S \setminus \{0\}$ there exists

$$\{i_1,\dots,i_t\} \subseteq \{1,\dots p\}$$

such that $x\mathcal{N}(n_{i_1}+\cdots+n_{i_t})$. Since $x \in S \setminus \{0\}$, there exist $a_1,\dots,a_p \in \mathbb{N}$ such that $x = \sum_{i=1}^{p} a_i n_i$. As $x \neq 0$, the set

$$\{i_1,\dots,i_t\} = \{i \mid a_i \neq 0\}$$

is not empty. Set $k = \max\{a_{i_1},\dots,a_{i_t}\}$. Then

$$1x \geq_S n_{i_1}+\cdots+n_{i_t},\ k(n_{i_1}+\cdots+n_{i_t}) \geq_S x.$$

Therefore $x\mathcal{N}(n_{i_1}+\cdots+n_{i_t})$, which implies that there are at most as many Archimedean components as elements of the form $n_{i_1}+\cdots+n_{i_t}$. □

As a consequence of Proposition 13.3, we have that if S is finitely generated, then $S/\mathcal{N}$ is finite.

COROLLARY 13.4. *Let S be a finitely generated monoid. Then $S/\mathcal{N}$ is a finite torsion free monoid.*

PROOF. Since $\mathcal{N}$ is a congruence, the set $S/\mathcal{N}$ is a monoid. By Proposition 13.3, we know that $S/\mathcal{N}$ is finite. Thus we only have to prove that $S/\mathcal{N}$ is torsion free. Take $x \in S$ and $k \in \mathbb{N}\setminus\{0\}$. Clearly $1(kx) \geq_S x$ and $kx \geq_S kx$, which means that $kx\mathcal{N}x$. This implies that $S/\mathcal{N}$ is torsion free. □

A semigroup T is an **Archimedean semigroup** if for every $(x,y) \in T \times T$, with $x \neq y$, there exist $k \in \mathbb{N} \setminus \{0\}$ and $z \in T$ such that $kx = y+z$. The following result uses the connection studied in Chapter 12 between finite torsion free monoids and finite lattices.

THEOREM 13.5. *Every finitely generated monoid is a finite lattice of Archimedean semigroups.*

PROOF. Let S be a finitely generated monoid. By Corollary 13.4, we know that $S/\mathcal{N}$ is a finite torsion free monoid. By Theorem 12.6, $S/\mathcal{N}$ is a finite lattice. Thus we only have to show that every element in $S/\mathcal{N}$ (every Archimedean component of S) is an Archimedean semigroup. Let C be an Archimedean component of S. By Proposition 13.1, C is a semigroup. Take $x \neq y$ in C. Since $x\mathcal{N}y$, there exists $k,l \in \mathbb{N} \setminus \{0\}$ verifying that $kx \geq_S y$ and $ly \geq_S x$. As $kx \geq_S y$, there exists $z \in S$ such that $kx = y+z$ (note that z does not have to be in C, and we are looking for an expression like this one but with $z \in C$). We already know (see proof of Corollary 13.4) that $(kx)\mathcal{N}x$, which implies that $y+z \in C$. In addition, $2(y+z) \geq_S y+2z$ and $1(y+2z) \geq_S y+z$, whence $y+2z$ belongs to C as well. Observe that $(2k)x = y+(y+2z)$ and $y+2z \in C$. □

1. Computing the Archimedean components of a finitely generated monoid

Let S be a monoid generated by $\{n_1,\dots,n_p\}$. Define, as usual,

$$\varphi : \mathbb{N}^p \to S,\ \varphi(a_1,\dots,a_p) = \sum_{i=1}^{p} a_i n_i$$

and let σ be its kernel congruence. Assume that

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

is a canonical system of generators of σ.

Let $\mathcal{A} = \{0,1\}^p$. This set is a Boolean algebra with the binary operations

$$(x_1,\dots,x_p)+(y_1,\dots,y_p) = (\max\{x_1,y_1\},\dots,\max\{x_p,y_p\}),$$

$$(x_1,\dots,x_p)\cdot(y_1,\dots,y_p) = (\min\{x_1,y_1\},\dots,\min\{x_p,y_p\}).$$

The partial order that makes $+$ and $\cdot$ to be supremum and infimum, respectively, is

$$(x_1,\dots,x_p) \leq (y_1,\dots,y_p) \text{ if and only if } x_i \leq y_i \text{ for all } i \in \{1,\dots,p\}.$$

Define the map

$$\pi : \mathbb{N}^p \to \mathcal{A},\ \pi(x) = (\pi_1(x),\dots,\pi_p(x)),$$

where

$$\pi_i(x_1,\dots,x_p) = \begin{cases} 1 & \text{if } x_i \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Associated to ρ we define the graph $G(\rho)$ as follows:

1. the vertices of $G(\rho)$ are the elements of $\mathcal{A}$,

2. an element $\overline{xy}$ is an edge of $G(\rho)$ if
   (a) $y = x + e_i$ for some $i \in \{1, \dots, p\}$,
   (b) there exists $(a, b) \in \pi(\rho) \cup \pi(\rho^{-1})$ such that $a \leq x$ and $e_i \leq b$.

EXAMPLE 13.6. Let S be the monoid $\mathbb{N}^3/\sigma$, where σ is the congruence generated by $\rho = \{(e_1 + e_2, 2e_3)\}$. In this case $\mathcal{A} = \{0,1\}^3 = \mathrm{V}(G(\rho))$. The set $\pi(\rho) \cup \pi(\rho^{-1})$ is $\{((1,1,0),(0,0,1)),((0,0,1),(1,1,0))\}$. Since there is no (a,b) in this set such that $a \leq c$ for $c \in \{(0,0,0),(1,0,0),(0,1,0)\}$, we have that these vertices are isolated. In addition, $(1,0,1) = e_1 + (0,0,1)$ and the pair $((0,0,1),(1,1,0))$ satisfies that $(0,0,1) \leq (0,0,1)$ and $e_1 \leq (1,1,0)$. Thus $\overline{(0,0,1)(1,0,1)}$ is an edge of $G(\rho)$. In the same way, the edges $\overline{(1,0,1)(1,1,1)}$ and $\overline{(0,1,1)(1,1,1)}$ are also in $\mathrm{E}(G(\rho))$. Hence the vertices $(0,0,1)$, $(1,0,1)$, $(0,1,1)$ and $(1,1,1)$ are in the same connected component of $G(\rho)$. Finally for the vertex $(1,1,0)$, we have that $(1,1,0) \leq (1,1,0)$ and $e_3 \leq (0,0,1)$, which implies that $\overline{(1,1,0)(1,1,1)}$ is also an edge of $G(\rho)$. We conclude that there are four connected components in $G(\rho)$ and their vertices are

$$\{(0,0,0)\},\ \{(1,0,0)\},\ \{(0,1,0)\},$$

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

◇

The motivation for the definition of $G(\rho)$ comes from the proof of Proposition 13.3 and the following results.

LEMMA 13.7. *Let x be an element of S. The following statements are equivalent.*

(i) *The elements x and $x + n_i$ are in the same Archimedean component of S.*
(ii) *There exists a positive integer k such that $kx \geq_S n_i$.*

PROOF. Assume that x and $x + n_i$ are in the same Archimedean component of S. This means that there exists some positive integer k such that $kx \geq_S x + n_i$. Since $x + n_i \geq_S n_i$ and $\leq_S$ is transitive, we conclude that $kx \geq_S n_i$.

Clearly $x + n_i \geq_S x$. If $kx \geq_S n_i$, then $(k+1)x \geq_S x + n_i$, which implies that x and $x + n_i$ are in the same Archimedean component of S. □

LEMMA 13.8. *Let C be an Archimedean component of S and*

$$\{i_1, \dots, i_t\} = \{\ i \in \{1, \dots, p\} \mid \textit{there exists } x \in C \textit{ with } x \geq_S n_i\ \}.$$

Then $n_{i_1} + \cdots + n_{i_t} \in C$.

PROOF. Since C is a semigroup, there must be an element x in C such that $x = \sum_{j=1}^{t} a_j n_{i_j}$ and $a_j \neq 0$ for all j. As in the proof of Proposition 13.3, it can be shown that $n_{i_1} + \cdots + n_{i_t} \in C$. □

LEMMA 13.9. *Let*

$$\{i_1, \dots, i_r, i_{r+1}, \dots, i_{r+t}\} \subseteq \{1, \dots, p\}.$$

If $n_{i_1}+\cdots+n_{i_r}$ *and* $n_{i_1}+\cdots+n_{i_r}+n_{i_{r+1}}+\cdots+n_{i_{r+t}}$ *are in the same Archimedean component* C *of* S*, then*

$$n_{i_1}+\cdots+n_{i_r}+n_{i_{r+1}}+\cdots+n_{i_{r+s}}\in C,$$

for all $s\in\{1,\dots,t\}$.

PROOF. It suffices to show that $n_{i_1}+\cdots+n_{i_{r+1}}$ is in C. Note that

$$n_{i_1}+\cdots+n_{i_{r+1}}\geq_S n_{i_1}+\cdots+n_{i_r}.$$

Since there exists $k\in\mathbb{N}\setminus\{0\}$ such that

$$k(n_{i_1}+\cdots+n_{i_r})\geq_S n_{i_1}+\cdots+n_{i_r}+n_{i_{r+1}}+\cdots+n_{i_{r+t}},$$

and

$$n_{i_1}+\cdots+n_{i_r}+n_{i_{r+1}}+\cdots+n_{i_{r+t}}\geq_S n_{i_1}+\cdots+n_{i_{r+1}},$$

we obtain that $k(n_{i_1}+\cdots+n_{i_r})\geq n_{i_1}+\cdots+n_{i_{r+1}}$. □

THEOREM 13.10. *Let* $a,b\in\mathcal{A}$. *The following statements are equivalent.*

(i) *The vertices* a *and* b *are in the same connected component of* $G(\rho)$.

(ii) *The elements* $\pi_1(a)n_1+\cdots+\pi_p(a)n_p$ *and* $\pi_1(b)n_1+\cdots+\pi_p(b)n_p$ *are in the same Archimedean component of* S.

PROOF. For the sake of simplicity, we set

$$\pi(a)N=\pi_1(a)n_1+\cdots+\pi_p(a)n_p$$

(that is, the "dot" product of $\pi(a)$ and $N=(n_1,\dots,n_p)$).

(i) implies (ii) It suffices to show that if $\overline{ab}$ is an edge $G(\rho)$, then $\pi(a)N$ and $\pi(b)N$ are in the same Archimedean component of S. Assume that $\overline{ab}$ is an edge of $G(\rho)$. Then $b=a+e_i$ for some i and there exists $(\alpha,\beta)\in\pi(\rho)\cup\pi(\rho)^{-1}$ such that $\alpha\leq a$ and $e_i\leq\beta$. Hence $\pi(b)N=\pi(a)N+n_i$. Take (x,y) in $\rho\cup\rho^{-1}$ such that $(\pi(x),\pi(y))=(\alpha,\beta)$. Since $\alpha\leq a$, there exists a positive integer k such that $x\leq ka$, that is, $ka=x+z$ for some $z\in\mathbb{N}^p$. Note also that the i-th coordinate of y must be nonzero, since $e_i\leq\beta$ and $\pi(y)=\beta$. As $\varphi(x)=\varphi(y)$, we obtain that

$$\varphi(ka)=\varphi(x)+\varphi(z)=\varphi(y)+\varphi(z)=\sum_{j=1}^{p}d_jn_j,$$

for some nonnegative integers d_j, such that $d_i\neq 0$. This means that $k(\pi(a)N)=k\varphi(a)\geq_S n_i$, which by Lemma 13.7 leads to the assertion that $\pi(a)N$ and $\pi(a)N+n_i=\pi(b)N$ are in the same Archimedean component of S (observe that $\pi(a)=a$, since $a\in\mathcal{A}$).

(ii) implies (i). Let C be the Archimedean component of S containing both $\pi(a)N$ and $\pi(b)N$. Define $m=(m_1,\dots,m_p)$ by

$$m_i=\begin{cases}1 & \text{if there exists } x\in C \text{ such that } n_i\leq_S x,\\ 0 & \text{otherwhise.}\end{cases}$$

We show that a and m are in the same connected component of $G(\rho)$. It is shown similarly that b and m belong to the same connected component of $G(\rho)$.

Observe that $a \leq m$. If $a = m$, then the proof is trivial, so we may assume that $a < m$. In order to show that a and m are in the same connected component, we show that if $a \leq g < m$, for some $g \in \mathcal{A}$, then there exists j such that $g < g + e_j \leq m$ and $\overline{g(g+e_j)}$ is an edge of $G(\rho)$. Since $g < m$, there exists q such that $\pi_q(g) = 0$ and $\pi_q(m) = 1$. From the definition of m, Lemma 13.8 ensures that $\pi(m)N \in C$. In addition, since $a \leq g < m$, by Lemma 13.9, we get that $\pi(g)N$ is also in C, whence there exists $0 \neq k \in \mathbb{N}$ such $k\pi(g)N \geq_S \pi(m)N$. Hence there exists $s \in S$ such that $k\pi(g)N = \pi(m)N + s$. This yields an equality in S of the form $k\pi(g)N = \sum_{i=1}^{p} d_i n_i$, with $d_q \neq 0$, since $d_q \geq \pi_q(m) \neq 0$. Thus the element $(k\pi(g), (d_1, \ldots, d_p))$ belongs to σ. Since ρ generates σ, we deduce that there exists $(\alpha, \beta) \in \rho \cup \rho^{-1}$ such that $\pi_i(\alpha) = 0$ whenever $\pi_i(g) = 0$ and such that $\pi_j(\beta) \neq 0$ for some j such that $\pi_j(g) = 0$. In this setting, $\pi(\alpha) \leq \pi(g)$ and $e_j \leq \pi(\beta)$, which means that $\overline{g(g+e_j)}$ is an edge of $G(\rho)$. The only thing left to prove is that $g + e_j \leq m$. For this, it suffices to show that there exist $x \in C$ such that $n_j \leq x$. Since $\pi(\alpha) \leq \pi(g)$, there exists $l \in \mathbb{N} \setminus \{0\}$ and $s \in S$ such that $l\pi(g)N = \varphi(\alpha) + s$. It follows that $l\pi(g)N = \varphi(\beta) + s$ and as $\pi_j(\beta) \neq 0$, we get that $l\pi(g)N \geq n_j$. By Proposition 13.1, since $\pi(g)N$ belongs to C, then so does $l\pi(g)N$. □

As an easy consequence of this fact, we have that the number of Archimedean components of S is equal to the number of connected components of $G(\rho)$.

We now focus our attention on the description of the Archimedean components of S. This description passes through a better understanding of the connected components of $G(\rho)$.

PROPOSITION 13.11. *Let D be a connected component of $G(\rho)$.*

1. *There exists the maximum γ of D (with respect to the partial order defined on $\mathcal{A}$).*
2. *If $\{\gamma_1, \ldots, \gamma_s\}$ are the minimal elements of D, then*

$$D = \{x \in \mathcal{A} \mid x \leq \gamma \text{ and } \gamma_i \leq x \text{ for some } 1 \leq i \leq s\}.$$

PROOF. Take γ to be the sum in $\mathcal{A}$ of all elements belonging to D. Then γ is the maximum of D. Clearly

$$D \subseteq \{x \in \mathcal{A} \mid x \leq \gamma \text{ and } \gamma_i \leq x \text{ for all } 1 \leq i \leq s\}.$$

Take $x \in \mathcal{A}$ such that $x \leq \gamma$ and $\gamma_i \leq x$ for some i. Since γ and γ_i are in D, Theorem 13.10, ensures that $\pi(\gamma)N$ and $\pi(\gamma_i)N$ are in the same Archimedean component of S. Using Lemma 13.9, we get that $\pi(x)N$ is in the Archimedean component containing $\pi(\gamma)N$ and $\pi(\gamma_i)N$. Using once more Theorem 13.10, we see that x, γ and γ_i are in the same connected component of $G(\rho)$. □

Let C be an Archimedean component of S and D be the corresponding connected component of $G(\rho)$. Let $\gamma = \max(D)$ and $\{\gamma_1, \ldots, \gamma_s\}$ be the set of minimal elements

of D. For the sake of simplicity, assume that, after possibly reordering the generators of S, we have that

$$\{n_1,\dots,n_r\} = \{n_i \mid \pi_i(\gamma) \neq 0\}.$$

Under this assumption we can make the following remarks.

1. If $\pi_i(\gamma_j) \neq 0$, then $i \in \{1,\dots,r\}$, since $\gamma_j \leq \gamma$. Hence we can consider the elements in D as r-tuples.
2. Define
$$I_C = \{x \in \mathbb{N}^r \mid \gamma_i \leq x \textit{ for some } i \in \{1,\dots,s\}\}.$$
Then I_C is an ideal of $\mathbb{N}^r$.
3. As a consequence of Proposition 13.1 and Theorem 13.10, C is a subsemigroup of $\langle n_1,\dots,n_r\rangle$.

With this information it is straightforward to prove the following result.

PROPOSITION 13.12. *The Archimedean component C is equal to*

$$\{x_1n_1 + \cdots + x_rn_r \mid (x_1,\dots,x_r) \in I_C\}.$$

EXAMPLE 13.13. Let us have another look at Example 13.6. Recall that the vertices of the connected components of $G(\rho)$ are

$$D_1 = \{(0,0,0)\},\ D_2 = \{(1,0,0)\},\ D_3 = \{(0,1,0)\},$$

$$D_4 = \{(0,0,1),(1,0,1),(1,1,0),(0,1,1),(1,1,1)\}.$$

The Archimedean components of $\mathbb{N}^3/\sigma$ are as follows.

1. The maximum of D_1 is $(0,0,0)$ and thus the set
$$\{n_i \mid \pi_i((0,0,0)) \neq 0\} = \emptyset.$$
Hence $I_{C_1} = \{0\} \subseteq \mathbb{N}^0 = \{0\}$ and $C_1 = \{(0,0,0)\}$.
2. The maximum of D_2 is $(1,0,0)$, which implies that the set
$$\{n_i \mid \pi((1,0,0)) \neq 0\} = \{n_1\}.$$
The ideal $I_{C_2} = \{x \in \mathbb{N} \mid x \geq 1\}$ and $C_2 = \{kn_1 \mid k \geq 1\}$.
3. The maximum of D_3 is $(0,1,0)$. In this case
$$\{n_i \mid \pi((0,1,0)) \neq 0\} = \{n_2\},$$
whence $I_{C_3} = I_{C_2}$ and $C_3 = \{kn_2 \mid k \geq 1\}$.
4. The maximum of D_4 is $(1,1,1)$ and its minimal elements are $(0,0,1)$ and $(1,1,0)$. Hence
$$\{n_i \mid \pi((1,1,1)) \neq 0\} = \{n_1,n_2,n_3\}$$
and $I_{C_4} = \{x \in \mathbb{N}^3 \mid x \geq (0,0,1) \text{ or } x \geq (1,1,0)\} = (0,0,1)+\mathbb{N}^3 \cup (1,1,0)+\mathbb{N}^3$. Therefore
$$C_4 = \{xn_1 + yn_2 + (z+1)n_3 \mid (x,y,z) \in \mathbb{N}^3\} \cup$$

$$\cup\{(x+1)n_1+(y+1)n_2+zn_3 \mid (x,y,z)\in\mathbb{N}^3\}.$$

◇

Another way to represent C is described in the following result. This representation shall be used in the next chapter.

PROPOSITION 13.14. *The Archimedean component C is isomorphic (as a semigroup) to I_C/σ_{I_C}, where σ_{I_C} is the restriction of σ to I_C, that is to say,*

$$(x_1,\dots,x_r)\sigma_{I_C}(y_1,\dots,y_r) \text{ if and only if } x_1n_1+\cdots+x_rn_r=y_1n_1+\cdots+y_rn_r.$$

PROOF. The map $f: I_C\to C$ defined by $f(x_1,\dots,x_r)=x_1n_1+\cdots+x_rn_r$ is a semigroup morphism. The rest of the proof follows easily. □

Remarks

Tamura and Kimura show in **[63]** that every commutative semigroup can be expressed uniquely as a semilattice of Archimedean semigroups. As we have seen in this chapter, for finitely generated monoids we obtain a lattice instead of a semilattice.

The algorithm described in this chapter for the computation of the Archimedean components of a finitely generated monoid appears in **[52]**.

Exercises

1. Let $\rho=\{((2,1,0),(0,0,3)),((1,0,1),(0,2,0))\}$. Compute the number of Archimedean components of the monoid $\mathbb{N}^3/\langle\rho\rangle$.
2. Prove that the semigroup $\{x\in\mathbb{N}^n \mid x\geq(1,\dots,1)\}$ is Archimedean.
3. Show that groups have only one Archimedean component.
4. Prove that a monoid with only one Archimedean component is a group.
5. Prove that every monoid has an Archimedean component which is a group.
6. Prove that every nontrivial submonoid of $\mathbb{N}$ has two Archimedean components.
7. Show that not all submonoids of $\mathbb{N}^2$ have the same number of Archimedean components.
8. Prove that a cancellative monoid generated by p elements and with 2^p Archimedean components is isomorphic to $\mathbb{N}^p$.
9. Give an example of a non-cancellative monoid generated by p elements, with 2^p Archimedean components.
10. Let S be an Archimedean semigroup and σ be a congruence on S. Prove that S/σ is Archimedean.
11. Show that a subsemigroup of an Archimedean semigroup does not have to be Archimedean.
12. Prove that if $C=\{x\}$ is an Archimedean component of a monoid S, then $2x=x$.
13. Find a monoid S and an element x in S such that $2x=x$ and so that $\{x\}$ is not an Archimedean component of S.
14. Prove that all Archimedean components of a finite torsion free monoid have cardinality one.

15. Let I be an ideal of $\mathbb{N}^n$ and σ be a congruence on $\mathbb{N}^n$. Prove that $\sigma \cap (I \times I)$ is a congruence on I.
16. Find an ideal I of $\mathbb{N}$ and a congruence σ on I such that $\sigma \neq \tau \cap (I \times I)$ for every congruence τ on $\mathbb{N}$.
17. Let S_1 and S_2 be two semigroups. Prove that $S_1 \times S_2$ is Archimedean if and only if both S_1 and S_2 are Archimedean.

CHAPTER 14

Separative monoids

Here we study separative monoids, $\mathcal{N}$-semigroups and torsion free monoids. We shall see that there is a close relationship between these concepts and some properties of their Archimedean components.

1. Separative monoids and their Archimedean components

A monoid S is **asymptotic free of torsion** if for every $x, y \in S$, the existence of $N \in \mathbb{N}$ such that $kx = ky$ for all $k \geq N$, implies that $x = y$.

PROPOSITION 14.1. *A monoid S is asymptotic free of torsion if and only if for every $x, y \in S$, $2x = 2y$ and $3x = 3y$ imply that $x = y$.*

PROOF. *Necessity.* If $2x = 2y$ and $3x = 3y$, then it can be easily derived that for every $k \geq 2$, we have that $kx = ky$. Since S is asymptotic free of torsion, $x = y$.

Sufficiency. Let $x, y \in S$ be such that $kx = ky$ for all $k \geq N$, with N the minimum positive integer satisfying this condition. Assume that $N \neq 1$. Then $2(N-1)$ and $3(N-1)$ are greater than or equal to N. Thus $2(N-1)x = 2(N-1)y$ and $3(N-1)x = 3(N-1)y$. By hypothesis, this implies that $(N-1)x = (N-1)y$, which contradicts the choice of N. Therefore N must be equal to one, which leads to $x = y$. □

We could have defined an asymptotic free of torsion monoid as a monoid verifying that whenever $2x = 2y$ and $3x = 3y$, then $x = y$. As we see next, there is still another way to "define" the concept asymptotic free of torsion monoid.

A monoid S is **separative** if for every $x, y \in S$, $2x = x + y = 2y$ implies $x = y$.

PROPOSITION 14.2. *The monoid S is separative if and only if S is asymptotic free of torsion.*

PROOF. *Necessity.* Let $N \in \mathbb{N} \setminus \{0\}$ be the minimum element such that $kx = ky$ for all $k \geq N$. Assume that $N \neq 1$. As above, $2(N-1)x = 2(N-1)y$, since $2(N-1) \geq N$. Let $z = (N-1)x + (N-1)y$. By hypothesis, if $z = 2(N-1)x$, then $(N-1)x = (N-1)y$. But this cannot occur, since we have chosen N minimal with respect to the condition $kx = ky$ for all $k \geq N$. Thus $z \neq 2(N-1)x$. In addition,

$$2z = 2(N-1)x + 2(N-1)y = 4(N-1)x$$

and

$$z + 2(N-1)x = 3(N-1)x + (N-1)y = 4(N-1)y = 4(N-1)x,$$

since $3(N-1) \geq N$ and $4(N-1) \geq N$. Hence $2z = z + 2(N-1)x = 2(2(N-1))x$ and since S is separative, we have that $z = 2(N-1)x$. But this is impossible, since we have shown that $z \neq 2(N-1)x$. This implies that N must be equal to 1 and therefore $x = y$.

Sufficiency. Assume that there exist $x, y \in S$ such that $2x = x + y = 2y$. Then $3x = 2x + y = 2y + y = 3y$ and by Proposition 14.1, we have that $x = y$. □

Next result indicates that the separative property (and therefore the asymptotic free of torsion property) of a monoid can be characterized in terms of the cancellativity of its Archimedean components.

PROPOSITION 14.3. *The monoid S is separative if and only if its Archimedean components are cancellative.*

PROOF. *Necessity.* Let x, y, z be elements in an Archimedean component C of S such that $x + z = y + z$. Since $x \mathcal{N} z$ and $y \mathcal{N} z$, there exist $k, k' \in \mathbb{N} \setminus \{0\}$ and $s, s' \in S$ such that $kx = z + s$ and $k'y = z + s'$. Assume, without loss of generality, that $k \geq k'$. Then $kx = z + s$ and $ky = z + s' + (k - k')y = z + t$, with $t = s' + (k - k')y \in S$. Hence

$$(k+1)x = x + z + s = z + y + s = kx + y,$$

$$(k+1)y = y + z + t = x + z + t = x + ky.$$

Using induction on k it is easy to show that

$$2kx = (k+1)x + (k-1)x = kx + y + (k-1)x = \cdots = kx + ky =$$

$$= (k-1)x + x + ky = (k-1)x + (k+1)y = \cdots = 2ky.$$

Since S is separative, we have that $kx = ky$. Furthermore,

$$(k+1)x = kx + x = ky + x = (k+1)y.$$

Using once more induction, but this time on n, it can be shown that $(k+n)x = (k+n)y$ for all $n \geq 0$. By Proposition 14.2, we deduce that $x = y$, since S is asymptotic free of torsion.

Sufficiency. Assume that $2x = x + y = 2y$. Then x and y are in the same Archimedean component C. Furthermore $2x + y = x + y + y = x + 2y = x + 2x$. Since C is cancellative, we conclude that $x = y$. □

As a consequence of Proposition 14.3 and Theorem 13.5, we have the following statement.

COROLLARY 14.4. *Every finitely generated separative monoid is a finite lattice of cancellative Archimedean semigroups.*

An element x of a semigroup S is **idempotent** if $2x = x$. Clearly if every element of a semigroup S is idempotent, then $+$ satisfies the idempotent law.

PROPOSITION 14.5. *Let S be a finitely generated separative monoid and let C be one of its Archimedean components. Then C is a group if and only if C contains an idempotent.*

PROOF. One of the implications is easy, since if C is a group then its identity element is an idempoten.

Assume that the element x in C verifies that $2x = x$. Then for every $c \in C$ we have that $c+x = c+2x$. By Proposition 14.3, the semigroup C is cancellative. From $c+x = c+2x$ we deduce that $c = c+x$. Thus x is the identity element of C (it does not have to be the identity element of S). Since C is an Archimedean semigroup (Theorem 13.5), we have that there exists $k \in \mathbb{N} \setminus \{0\}$ and $a \in C$ such that $kx = c+a$. Clearly $kx = x$, which implies that a is the inverse of c. Therefore every element in C has an inverse and this means that C is a group. □

2. Deciding whether the quotient of an ideal of $\mathbb{N}^n$ by a congruence is cancellative

As we have seen before (Proposition 14.3), a finitely generated monoid is separative if and only if its Archimedean components are cancellative. In Chapter 13 we gave a description of the Archimedean components of a finitely generated monoid by means of quotients of ideals of $\mathbb{N}^n$ for some nonnegative integer n (Proposition 13.14). Thus will have a method for deciding whether a finitely generated monoid is separative as soon as we know how to determine whether the quotient of a ideal by a congruence is cancellative. Recall that $\mathbb{N}^n/\sigma$ is cancellative if and only if $\sigma = \sim_{M_\sigma}$ (Proposition 1.4). A similar result can be obtained for ideals of $\mathbb{N}^n$.

PROPOSITION 14.6. *Let I be an ideal of $\mathbb{N}^n$ and σ be a congruence on $\mathbb{N}^n$. Then $I/(\sigma \cap (I \times I))$ is cancellative if and only if $\sim_{M_\sigma} \cap (I \times I) \subseteq \sigma$.*

PROOF. *Necessity.* Let $(a,b) \in \sim_{M_\sigma} \cap (I \times I)$. By Lemma 1.3, there exists $c \in \mathbb{N}^n$ such that $(a+c, b+c) \in \sigma$. Take $x \in \mathbb{N}^n$ such that $x+c \in I$. Clearly, $(a+c+x, b+c+x) \in \sigma$. Since $(a,b) \in I \times I$, $(c+x, c+x) \in I \times I$ and $I/(\sigma \cap (I \times I))$ is cancellative, we obtain that $(a,b) \in \sigma$.

Sufficiency. If there exist $(a,b) \in I \times I$ and $c \in I$ such that $(a+c, b+c) \in \sigma \cap (I \times I)$, then $a+c-(b+c) = a-b \in M_\sigma$, which implies that $(a,b) \in \sim_{M_\sigma} \cap (I \times I)$. By hypothesis, we have that $(a,b) \in \sigma \cap (I \times I)$. □

Unfortunately this result cannot be used directly in practice. Let

$$P = \{(a_1,b_1), \dots, (a_u,b_u)\}$$

be the set of primitive elements of $\sim_{M_\sigma}$ (see Chapter 8). For every $(a_i,b_i) \in P$, define the set

$$A_i = \text{Minimals}_{\leq}\{(x,y) \in \mathbb{N}^n \times \mathbb{N}^n \mid (a_i,b_i)+(x,y) \in \sim_{M_\sigma} \cap (I \times I)\}$$

($\leq$ denotes the usual product partial order on $\mathbb{N}^n \times \mathbb{N}^n$). If $I/(\sigma \cap (I \times I))$ is cancellative, by Proposition 14.6, we have that

1. $(a_i,b_i)+(x,y) \in \sigma$ for all $(x,y) \in A_i$,
2. $(a_i,b_i)+(x,y)+(a_j,b_j) \in \sigma$ for all $(x,y) \in A_i$ and every $j \in \{1,\dots,u\}$.

The converse is also true.

THEOREM 14.7. *Let I be an ideal of $\mathbb{N}^n$ and σ be a congruence on $\mathbb{N}^n$ such that for all $i \in \{1,\dots,u\}$,*

(i) $(a_i,b_i)+(x,y) \in \sigma$ *for all* $(x,y) \in A_i$,

(ii) $(a_i,b_i)+(x,y)+(a_j,b_j) \in \sigma$ *for all* $(x,y) \in A_i$ *and every* $j \in \{1,\dots,u\}$.

Then $I/(\sigma \cap (I \times I))$ is cancellative.

PROOF. Using Proposition 14.6, it suffices to prove that if $(a,b) \in \sim_{M_\sigma} \cap (I \times I)$, then $(a,b) \in \sigma$. If $a = b$, then clearly $(a,b) \in \sigma$. Thus we may assume that $a \neq b$. Since P is the set of primitive elements of $\sim_{M_\sigma}$, there exist $(a_{i_1},b_{i_1}) \in P$ and $(c_1,d_1) \in \mathbb{N}^n \times \mathbb{N}^n$ such that $(a,b) = (a_{i_1},b_{i_1})+(c_1,d_1)$. From the definition of A_i, there exists $(x,y) \in A_i$ and $(c_1',d_1') \in \mathbb{N}^n \times \mathbb{N}^n$ verifying that $(c_1,d_1) = (x,y)+(c_1',d_1')$. (Observe that if (a,b) is already in P, then $(c_1,d_1) = (x,y) = (0,0)$.) Hence $(a,b) = (a_{i_1},b_{i_1})+(x,y)+(c_1',d_1')$. As (a,b) and $(a_{i_1},b_{i_1})+(x,y)$ are in $\sim_{M_\sigma}$, we get that $(c_1',d_1') \in \sim_{M_\sigma}$, whence either $c_1' = d_1'$ or there exist $(a_{i_2},b_{i_2}) \in P$ and (c_2,d_2) such that $(c_1',d_1') = (a_{i_2},b_{i_2})+(c_2,d_2)$. We repeat the process for (c_2,d_2) and then obtain (c_3,d_3). Since the elements (c_i,d_i) yield a strictly decreasing chain in $\mathbb{N}^n \times \mathbb{N}^n$, we can ensure that at a certain stage of the process we get that $c_l = d_l$. Thus

$$(a,b) = (a_{i_1},b_{i_1})+(x,y)+(a_{i_2},b_{i_2})+(a_{i_3},b_{i_3})+\cdots+(a_{i_l},b_{i_l})+(c_l,c_l),$$

where $(a_{i_j},b_{i_j}) \in P$ for all $j \in \{1,\dots,l\}$. Using the hypothesis, we get that

(i) $(a_{i_1}+x)\ \sigma\ (b_{i_1}+y)$,

(ii) $(a_{i_1}+x+a_{i_j})\ \sigma\ (b_{i_1}+y+b_{i_j})$ for all $2 \leq j \leq l$.

Hence

$$(a_{i_1}+x+a_{i_2}+a_{i_3}+\cdots+a_{i_l})\ \sigma\ (b_{i_1}+y+b_{i_2}+a_{i_3}+\cdots+a_{i_l}),\ \text{(by } (ii))$$

$$(b_{i_1}+y+b_{i_2}+a_{i_3}+\cdots+a_{i_l})\ \sigma\ (a_{i_1}+x+b_{i_2}+a_{i_3}+\cdots+a_{i_l}),\ \text{(by } (i))$$

$$(a_{i_1}+x+b_{i_2}+a_{i_3}+\cdots+a_{i_l})\ \sigma\ (a_{i_1}+x+b_{i_2}+b_{i_3}+a_{i_4}\cdots+a_{i_l})\ \text{(by } (i)).$$

Repeating this procedure we obtain

$$(a_{i_1}+x+a_{i_2}+a_{i_3}+\cdots+a_{i_l})\ \sigma\ (b_{i_1}+y+b_{i_2}+b_{i_3}+\cdots+b_{i_l}),$$

whence

$$(a_{i_1}+x+a_{i_2}+a_{i_3}+\cdots+a_{i_l}+c_l)\ \sigma\ (b_{i_1}+y+b_{i_2}+b_{i_3}+\cdots+b_{i_l}+c_l),$$

which means that $(a,b) \in \sigma$. □

If we want to use this result in practice, we still must solve the problem of how to compute A_i for every $1 \leq i \leq u$.

Let M be a subgroup of $\mathbb{Z}^n$ and

$$I = \bigcup_{i=1}^{s} (\alpha_i + \mathbb{N}^n)$$

be an ideal of $\mathbb{N}^n$. Take $(a,b) \in \sim_M$ and define

$$A_{(a,b)} = \text{Minimals}_{\leq}\{(x,y) \in \mathbb{N}^n \times \mathbb{N}^n \mid (a,b)+(x,y) \in \sim_M \cap (I \times I)\}.$$

Assume that

$$\mathfrak{I}_{\sim_M} = \{(a_1,b_1),\dots,(a_t,b_t)\}$$

is the set of irreducible elements of $\sim_M$ (recall that this set is a system of generators of $\sim_M$ as a submonoid of $\mathbb{N}^n \times \mathbb{N}^n$). Define

$$\alpha = \max\{\alpha_{11},\dots,\alpha_{1n},\dots,\alpha_{s1},\dots,\alpha_{sn}\},$$

where $(\alpha_{i1},\dots,\alpha_{in}) = \alpha_i$. Take $(x,y) \in A_{(a,b)}$. Then $(a,b)+(x,y) \in \sim_M$. Since $(a,b) \in \sim_M$, we have that $x-y = ((x+a)-(y+b))-(a-b) \in M$, which means that $(x,y) \in \sim_M$. Hence there exist $\lambda_1,\dots,\lambda_t \in \mathbb{N}$ such that

$$(x,y) = \sum_{i=1}^{t} \lambda_i (a_i,b_i).$$

Since $(a,b)+(x,y) \in I \times I$, we have that

$$a+\sum_{i=1}^{t} \lambda_i a_i, b+\sum_{i=1}^{t} \lambda_i b_i \in I.$$

Thus there exist $i,j \in \{1,\dots,s\}$ such that

$$a+\sum_{i=1}^{t} \lambda_i a_i \geq \alpha_i, b+\sum_{i=1}^{t} \lambda_i b_i \geq \alpha_j.$$

Clearly, if $\lambda_k > \alpha$ for some k, then

$$a+\sum_{i=1,i\neq k}^{t} \lambda_i a_i + \alpha a_k \geq \alpha_i, b+\sum_{i=1,i\neq k}^{t} \lambda_i b_i + \alpha b_k \geq \alpha_j,$$

which contradicts the minimality of (x,y). Thus $\lambda_k \leq \alpha$ for all k, whence

$$(x,y) \leq \alpha((a_1,b_1)+\cdots+(a_t,b_t))$$

for all $(x,y) \in A_{(a,b)}$.

We know how to compute $\mathfrak{I}_{\sim_M}$ (note also that if I is the ideal associated to an Archimedean component, then $\alpha \in \{0,1\}$, since $\alpha_i \in \{0,1\}^n \times \{0,1\}^n$). Therefore we have a method for computing A_i and hence, by Theorem 14.7, a procedure for deciding whether $I/(\sigma \cap (I \times I))$ is cancellative.

3. Elimination

Assume that $S = \mathbb{N}^n/\sigma$ is a finitely generated monoid. Recall that the ideal I_C associated to an Archimedean component C of S may be defined over $\mathbb{N}^r$, with $r < n$, and that the congruence σ_{I_C} is the restriction of σ to I_C, that is to say, if we define σ_r to be the restriction of σ to $\mathbb{N}^r$, then $\sigma_{I_C} = \sigma_r \cap (I_C \times I_C)$. If we want to use Theorem 14.7, we must know how to compute σ_r.

Let σ be a congruence on $\mathbb{N}^n$ and σ' be the restriction of σ to the set

$$\{(x_1,\dots,x_r,0,\dots,0) \in \mathbb{N}^n \mid (x_1,\dots,x_r) \in \mathbb{N}^r\}.$$

We show how to construct a system of generators of σ' from a system of generators of σ (observe that σ' is not, in general, the result of applying a sequence of projections to σ and thus we cannot use the results obtained in Chapter 11). Assume that

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

is the canonical system of generators of σ with respect to $\preceq_{rlex}$, where

$$(a_i,b_i) = ((a_{i1},\dots,a_{in}),(b_{i1},\dots,b_{in}))$$

(see the exercises at the end of Chapter 5 for the definition of $\preceq_{rlex}$). Define

$$\rho' = \{(a_i,b_i) \in \rho \mid a_{i_{r+1}} = \cdots = a_{i_n} = b_{i_{r+1}} = \cdots = b_{i_n} = 0\}.$$

Clearly $\rho' \subseteq \sigma'$ and therefore $\langle \rho' \rangle \subseteq \sigma'$. Take (x,y) to be an element of σ'. Then $x \,\sigma\, y$, and this implies that $\mathrm{NF}_\rho(x) = \mathrm{NF}_\rho(y)$ (see Theorem 6.7). Since x and y are of the form

$$x = (x_1,\dots,x_r,0,\dots,0),\ y = (y_1,\dots,y_r,0,\dots,0),$$

we have that if $a_i \preceq_{rlex} x$, then the last $n-r$ coordinates of a_i must be zero and the same holds for b_i. It follows that in the process of computing $\mathrm{NF}_\rho(x)$ and $\mathrm{NF}_\rho(y)$, the elements $(a_i,b_i) \in \rho$ involved verify this condition. Hence they belong to ρ', which leads to $\mathrm{NF}_\rho(x) = \mathrm{NF}_{\rho'}(x)$ and $\mathrm{NF}_\rho(y) = \mathrm{NF}_{\rho'}(y)$. By Theorem 6.7, we can conclude that $(x,y) \in \sigma'$. Thus ρ' is a canonical system of generators of σ' with respect to $\preceq_{rlex}$.

If instead of the last $n-r$ coordinates, we need to eliminate another set $\{i_1,\dots,i_k\}$ of coordinates of the congruence, then we only have to interchange these coordinates with the last k coordinates and apply the method presented in this section. Once the computations are performed and the last k coordinates are removed, we only have to rearrange the rest of coordinates according to the initial order of coordinates.

4. Deciding whether a finitely generated monoid is separative

We have all the results needed to check whether a given finitely generated monoid is separative. Let $S = \mathbb{N}^n/\sigma$ be a finitely generated monoid and

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

be a system of generators of σ. The following procedure can be used for determining whether S is separative.

1. Compute the Archimedean components of S. This can be done using the results presented in Chapter 13.
2. For every Archimedean component C of S compute $r \in \mathbb{N}$ and $I_C \subseteq \mathbb{N}^r$ such that C is isomorphic to I_C over the restriction of σ to I_C (see Proposition 13.14).
3. Compute ρ_r, a canonical system of generators of the restriction σ_r of σ to the r coordinates of the preceding step. This can be performed by using the method described in Section 3.
4. Once we have calculated I_C and ρ_r, we compute the set of primitive elements P_r of $\sim_{M_{\sigma_r}}$ as explained in Chapter 8 and see whether the conditions of Theorem 14.7 hold. For every $(a_i,b_i),(a_j,b_j) \in P_r$ and $(x,y) \in A_i$, we have that (a_i+x,b_i+y) and (a_i+x+a_j,b_i+y+b_j) belong to σ_r if and only if

$$\mathrm{NF}_{\rho_r}(a_i+x) = \mathrm{NF}_{\rho_r}(b_i+x),\ \mathrm{NF}_{\rho_r}(a_i+x+a_j) = \mathrm{NF}_{\rho_r}(b_i+y+b_j).$$

EXAMPLE 14.8. Let us go back to Example 13.13, where

$$\rho = \{(e_1+e_2, 2e_3)\}$$

and the Archimedean components of S are

$$C_1 = \{0\},\ C_2 = \{kn_1 \mid k \geq 1\},\ C_3 = \{kn_2 \mid k \geq 1\},$$

$$C_4 = \{xn_1 + yn_2 + (z+1)n_3 \mid (x,y,z) \in \mathbb{N}^3\} \cup$$

$$\cup \{(x+1)n_1 + (y+1)n_2 + zn_3 \mid (x,y,z) \in \mathbb{N}^3\}.$$

First C_1 is cancellative. The same holds for C_2 and C_3, since they are isomorphic to $\mathbb{N}\setminus\{0\}$. The ideal associated to C_4 is $I_{C_4} = (0,0,1)+\mathbb{N}^3 \cup (1,1,0)+\mathbb{N}^3$. Hence $\sigma_r = \sigma$ and we have to compute the primitive elements of $\sim_{M_\sigma}$. The group M_σ is generated by $\{(1,1,-2)\}$. The equations of M_σ are

$$\begin{aligned} x-y &= 0, \\ 2x+z &= 0. \end{aligned}$$

The set of primitive elements of $\sim_{M_\sigma}$ is

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

Thus we only have to compute A_1:

$$A_1 = \mathrm{Minimals}_{\leq}\{(x,y) \in \mathbb{N}^3 \times \mathbb{N}^3 \mid (a_i,b_i)+(x,y) \in \sim_{M_\sigma} \cap (I_{C_4} \times I_{C_4})\} = \{(0,0)\},$$

since $((1,1,0),(0,0,2)) \in I_{C_4} \times I_{C_4}$. Clearly σ fulfills the conditions of Theorem 14.7 and hence C_4 is cancellative. Therefore $S = \mathbb{N}^3/\langle\rho\rangle$ is separative. $\diamond$

5. Deciding whether a finitely generated monoid is torsion free

Here we give a procedure for determining whether a finitely generated monoid is torsion free. Recall that if the given monoid is cancellative, then it is isomorphic to $\mathbb{N}^n/\sim_M$ for some nonnegative integer n and some subgroup M of $\mathbb{Z}^n$. Deciding whether $\mathbb{N}^n/\sim_M$ is torsion free is easy by Proposition 3.3. We only have to compute the invariant factors of M and see if they are all equal to one. For the non-cancellative case, we can sometimes use a similar criterium.

PROPOSITION 14.9. *Let σ be a congruence on $\mathbb{N}^n$. If $\mathbb{N}^n/\sigma$ is torsion free, then so is $\mathbb{N}^n/\sim_{M_\sigma}$.*

PROOF. Assume that $(ka,kb) \in \sim_{M_\sigma}$, with $k > 0$. By Lemma 1.3, there exists $c \in \mathbb{N}^n$ such that $(ka+c, kb+c) \in \sigma$. Since σ is a congruence,

$$(ka+kc, kb+kc) = (k(a+c), k(b+c)) \in \sigma,$$

which by hypothesis leads to $(a+c, b+c) \in \sigma$. Therefore $(a,b) \in \sim_{M_\sigma}$. □

Unfortunately this result does not completely solve the problem of deciding whether a finitely generated monoid is torsion free. However it sometimes gives a quick answer to our problem.

EXAMPLE 14.10. Let $S \cong \mathbb{N}^2/\langle\rho\rangle$, with

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

In this case, $M_\sigma = \langle(2,0)\rangle \subseteq \mathbb{Z}^2$ and $\sim_{M_\sigma} = \langle((2,0),(0,0))\rangle$. Note that $\sigma \neq \sim_{M_\sigma}$ and therefore S is not cancellative. Since $\mathbb{Z}^2/M_\sigma$ is not torsion free, S is not torsion free. ◇

If S is a finitely generated torsion free monoid, then S is separative. Thus the Archimedean components of S must be cancellative. We prove next that finitely generated torsion free monoids are separative monoids whose Archimedean components fulfill an additional condition.

Let $S = \mathbb{N}^n/\sigma$ be a finitely generated monoid and C be one of its Archimedean components. Take $\{i_1,\dots,i_r\}$ to be the set of $i \in \{1,\dots,n\}$ such that $x_i \neq 0$ for some $(x_1,\dots,x_n) \in \mathbb{N}^n$ with $[(x_1,\dots,x_n)] \in C$. Define

$$\mathbb{N}^C = \{(x_1,\dots,x_n) \in \mathbb{N}^n \mid x_i = 0 \text{ for all } i \notin \{i_1,\dots,i_r\}\}.$$

Clearly, $\mathbb{N}^C$ is a subsemigroup of $\mathbb{N}^n$ which is isomorphic to $\mathbb{N}^r$. Furthermore, if $[x] \in C$, then $x \in \mathbb{N}^C$. Denote by $\sigma_{\mathbb{N}^C}$ the restriction of σ to $\mathbb{N}^C$, that is, for every $a,b \in \mathbb{N}^C$, $a\sigma_{\mathbb{N}^C}b$ if and only if $a\sigma b$.

A system of generators for the congruence $\sigma_{\mathbb{N}^C}$ can be computed from ρ as shown in Section 3.

THEOREM 14.11. *Let σ be a congruence on $\mathbb{N}^n$. The monoid $S = \mathbb{N}^n/\sigma$ is torsion free if and only if every Archimedean component C of S satisfies the following conditions:*

1. *C is cancellative,*

2. $\mathbb{N}^C/\sim_{M_{\sigma_{\mathbb{N}^C}}}$ *is torsion free.*

PROOF. *Necessity.* If S is torsion free, then it is separative and by Proposition 14.3, its Archimedean components are cancellative. In addition $\mathbb{N}^C/\sigma_{\mathbb{N}^C}$ is a submonoid of $\mathbb{N}^n/\sigma$, which implies that it is torsion free. By Proposition 14.9, we get that $\mathbb{N}^C/\sim_{M_{\sigma_{\mathbb{N}^C}}}$ is torsion free.

Sufficiency. Take $(ka,kb) \in \sigma$, with $0 \neq k \in \mathbb{N}$. Since $k[a] = [ka] = [kb] = k[b]$, we have that $[a] \leq_S k[a] = k[b]$, and $[b] \leq_S k[b] = k[a]$. Thus $[a]$ and $[b]$ are in the same Archimedean component C of $\mathbb{N}^n/\sigma$. Hence $ka, kb \in \mathbb{N}^C$ and $(ka,kb) \in \sigma_{\mathbb{N}^C} \subseteq \sim_{M_{\sigma_{\mathbb{N}^C}}}$. By hypothesis, $\sim_{M_{\sigma_{\mathbb{N}^C}}}$ is torsion free, which leads to $(a,b) \in \sim_{M_{\sigma_{\mathbb{N}^C}}}$. Using Lemma 1.3, there exist $c \in \mathbb{N}^C$ such that $(a+c,b+c) \in \sigma_{\mathbb{N}^C}$. We show next that we can choose d such that $[d] \in C$ and $(a+d,b+d) \in \sigma_{\mathbb{N}^C}$. If we prove this, then $[a]+[d] = [b]+[d] \in C$, and by the hypothesis that C is cancellative, we get $[a] = [b]$, that is, $(a,b) \in \sigma$. The only thing left to demonstrate is that we can find d such that $[d] \in C$ and $(a+d,b+d) \in \sigma_{\mathbb{N}^C}$. As before, let $\{i_1,\dots,i_r\}$ be the set of $i \in \{1,\dots,n\}$ such that there exists $[(x_1,\dots,x_n)] \in C$ and $x_i \neq 0$. Set $d = c + e_{i_1} + \cdots + e_{i_r}$. Clearly, $(a+d,b+d) \in \sigma_{\mathbb{N}^C}$, since $\sigma_{\mathbb{N}^C}$ is a congruence and $(a+c,b+c) \in \sigma_{\mathbb{N}^C}$. By the definition of $\{i_1,\dots,i_r\}$, for every $j \in \{1,\dots,r\}$, there exists $x^j = (x_1^j,\dots,x_n^j)$ such that $[x^j] \in C$ and $x_{i_j}^j \neq 0$. Take $f = \sum_{j=1}^r x^j$. Since C is a semigroup, $[f] \in C$. Furthermore, $f = \sum_{j=1}^r \lambda_j e_{i_j}$ and $d = \sum_{j=1}^r \mu_j e_{i_j}$, for some $\lambda_i, \mu_j \in \mathbb{N}\setminus\{0\}$. It is straightforward to show that $[f]\mathcal{N}[d]$, which means that $[d] \in C$. □

EXAMPLE 14.12. We go back once more to Example 14.8, where S is the monoid with presentation

$$\rho = \{(e_1+e_2, 2e_3)\}.$$

As we have already shown, S is separative and its Archimedean components are

$$C_1 = \{0\},\ C_2 = \{kn_1 \mid k \geq 1\},\ C_3 = \{kn_2 \mid k \geq 1\},$$

$$C_4 = \{xn_1 + yn_2 + (z+1)n_3 \mid (x,y,z) \in \mathbb{N}^3\} \cup$$

$$\cup \{(x+1)n_1 + (y+1)n_2 + zn_3 \mid (x,y,z) \in \mathbb{N}^3\}.$$

We only have to check the second condition in Theorem 14.11. The Archimedean component C_1 is torsion free and so are C_2 and C_3. For C_4, the set $\mathbb{N}^{C_4} = \mathbb{N}^3$ and $\sigma_{\mathbb{N}^{C_4}} = \sigma$. Thus

$$\mathbb{N}^{C_4}/\sim_{M_{\sigma_{\mathbb{N}^{C_4}}}} = \mathbb{N}^3/\sim_{M_\sigma}.$$

Since the equations of M_σ are

$$x - y = 0,$$
$$2x + z = 0,$$

we have that M_σ is homogeneous and thus $\mathbb{N}^3/\sim_{M_\sigma}$ is torsion free. Therefore S is torsion free. $\diamond$

6. $\mathcal{N}$-semigroups

From the proof of Proposition 14.5, it can be derived that if S is an Archimedean cancellative semigroup with an idempotent element, then S turns out to be a group. Thus the existence of an identity element in an Archimedean cancellative semigroup spoils its structure, in the sense that it becomes a better known object. In this section, we focus our attention on the Archimedean cancellative semigroups not containing idempotent elements. These semigroups are known as **$\mathcal{N}$-semigroups**. The property of being $\mathcal{N}$-semigroup is preserved under isomorphisms of semigroups. Next, we show that every cancellative semigroup can be embedded in a group. In particular, every $\mathcal{N}$-semigroup is isomorphic to a subsemigroup of a group and this allows us to write expressions like $a-b$, $0a=0$, $a+0$, $a-0$, etc.

PROPOSITION 14.13. *Let S be a cancellative semigroup. On $S\times S$ define the following binary relation*

$$(a,b)\ \tau\ (c,d) \text{ if } a+d=b+c.$$

Then

(i) *the binary relation τ is a congruence on $S\times S$,*
(ii) *the quotient $(S\times S)/\tau$ is a group,*
(iii) *the map*

$$\psi : S \to \frac{S\times S}{\tau},\ \psi(s)=[(2s,s)]$$

is a semigroup monomorphism.

PROOF. The set $S\times S$ has the structure of a semigroup (addition is performed componentwise), thus it makes sense to talk about the semigroup quotient of $S\times S$ by τ.

(i) Since $a+b=b+a$, we have that $(a,b)\ \tau\ (a,b)$. If $a+d=b+c$, then $b+c=a+d$, which means that if $(a,b)\ \tau\ (c,d)$, then $(c,d)\ \tau\ (a,b)$. Assume that $(a,b)\ \tau\ (c,d)$ and $(c,d)\ \tau\ (e,f)$. Then $a+d=b+c$ and $c+f=d+e$. Thus

$$a+f+d=b+c+f=b+e+d$$

and since S is cancellative, we have that $a+f=b+e$, which leads to $(a,b)\ \tau\ (e,f)$. Hence τ is an equivalence relation on $S\times S$. Finally, suppose that $(a,b)\ \tau\ (c,d)$. Then $a+d=b+c$, which implies that $a+d+e+f=b+c+e+f$, which becomes $((a,b)+(e,f))\ \tau\ ((c,d)+(e,f))$.

(ii) We already know that $(S\times S)/\tau$ is a semigroup. Let c be an element in S. Since $a+c+b=b+c+a$, we have that $[(a,b)]+[(c,c)]=[(a,b)]$, which means that $[(c,c)]$ is the identity element of $(S\times S)/\tau$. In addition, $a+b+c=b+a+c$ and this is the same as $((a,b)+(b,a))\ \tau\ (c,c)$, whence $[(a,b)]+[(b,a)]=[(c,c)]$. Therefore the inverse of $[(a,b)]$ is $[(b,a)]$. Consequently $(S\times S)/\tau$ is a group.

(iii) Take $s, s' \in S$. Then

$$f(s)+f(s') = [(2s+2s', s+s')],\ f(s+s') = [(2(s+s'), s+s')].$$

Thus f is a semigroup morphism. Assume that $f(s) = f(s')$. Then $[(2s,s)] = [(2s',s')]$ and hence $2s+s' = s+2s'$. Since S is cancellative, we obtain $s = s'$. Therefore f is a monomorphism.

□

Let m be an element of a $\mathcal{N}$-semigroup S. Define the binary relation R_m on S as

$$xR_my \text{ if } x+km = y+k'm \text{ for some } k,k' \in \mathbb{N}.$$

The reader can check that R_m is a congruence on S.

PROPOSITION 14.14. *Let S be a $\mathcal{N}$-semigroup and m be an element of S. The semigroup S/R_m is a group.*

PROOF. For all $x \in S$ we have that $x\ R_m\ (x+m)$, since $x+2m = (x+m)+1m$. Thus

$$[x]+[m] = [x+m] = [x],$$

whence $[m]$ is the identity element of S/R_m.

Take $[x] \in S/R_m$. Since S is Archimedean, there exist $k \in \mathbb{N}\setminus\{0\}$ and $z \in S$ such that $km = x+z$. Hence

$$[x]+[z] = [km] = [m]$$

($km+m = m+km$ and thus $[km] = [m]$). It follows that every element in S/R_m has an inverse. □

Our aim is to prove that a $\mathcal{N}$-semigroup S is isomorphic to $\mathbb{N}\times S/R_m$ (but not with the standard addition defined componentwise).

LEMMA 14.15. *Let S be a $\mathcal{N}$-semigroup and m be an element in S.*

(i) *For every $x \in S$ there exists*

$$k_x = \max\{k \in \mathbb{N} \mid x-km \in S\}.$$

(ii) *For any $x,y \in S$, if $x\ R_m\ y$, then $x+k_ym = y+k_xm$.*

PROOF. *(i)* Let $x \in S$. Since S is Archimedean, there exists $a \in \mathbb{N}\setminus\{0\}$ and $z \in S$ for which $am = x+z$. If there exists $b > a$ such that $x-bm \in S$, then $(am-x)+(x-bm) \in S$. Thus $(a-b)m$ belongs to S. In addition, $b > a$, which implies that $(b-a)m \in S$. Therefore $0 = (a-b)m+(b-a)m \in S$, which is impossible since S has no idempotent elements ($2\cdot 0 = 0$). It follows that if $x-bm \in S$, then $b \leq a$ and consequently the set $\{k \in \mathbb{N} \mid x-km \in S\}$ has a maximum.

(ii) Take $x,y \in S$ to be such that $x\ R_m\ y$. Since $x\ R_m\ y$, it can be easily derived that

$$(x+k_ym)\ R_m\ (y+k_xm).$$

By the definition of R_m, there exist k and k' such that $x+k_ym+km=y+k_xm+k'm$. If $k'>k$, then $x-(k_x+k'-k)m=y-k_ym\in S$ and $k_x+k'-k>k_x$, which contradicts the maximality of k_x. Thus $k'\leq k$. Analogously, it is shown that $k\leq k'$. Therefore $k=k'$ and since S is cancellative, we obtain that $x+k_ym=y+k_xm$. □

Let S be a $\mathcal{N}$-semigroup and take m to be an element in S. By Lemma 14.15, the map

$$\mathrm{A}_S^m : S/R_m \to S,\ \mathrm{A}_S^m([x]) = x-k_xm$$

is well defined.

PROPOSITION 14.16. *Let S be a $\mathcal{N}$-semigroup and let $m\in S$. Then*

$$\mathrm{Im}(\mathrm{A}_S^m) = \mathrm{Ap}(S,m) = \{s\in S \mid s-m\notin S\}.$$

PROOF. If $s\in \mathrm{Im}(\mathrm{A}_S^m)$, then $s=x-k_xm$ for some $x\in S$. Thus $s-m\notin S$, since $s-m\in S$ contradicts the maximality of k_x (observe that $k_s=0$).

Take $s\in S$ such that $s-m\notin S$. Then $s-km$ is not in S for any $k\geq 1$. This implies that $k_s=0$ and $\mathrm{A}_S^m([s])=s\in \mathrm{Im}(\mathrm{A}_S^m)$. □

This result, together with the next one, are telling us that $\mathcal{N}$-semigroups are very similar to numerical semigroups (compare them with Proposition 10.5).

PROPOSITION 14.17. *Let S be a $\mathcal{N}$-semigroup and $m\in S$. For every $s\in S$ there exists a unique element $(k,x)\in \mathbb{N}\times \mathrm{Im}(\mathrm{A}_S^m)$ for which $s=km+x$.*

PROOF. Clearly $s=k_sm+(s-k_sm)$. Assume that $km+x=k'm+y$, with $x,y\in \mathrm{Im}(\mathrm{A}_S^m)$. If $k'>k$, then $x-(k'-k)m=y\in S$, but this is impossible since $k'-k>0=k_x$. Hence $k'\leq k$. Analogously, we see that $k\leq k'$, which implies that $k=k'$, whence $x=y$. □

Take S to be a $\mathcal{N}$-semigroup and $m\in S$. For every $x,y\in S$, the element $(x-k_xm)+(y-k_ym)\in S$. Hence $k_{x+y}\geq k_x+k_y$. Define

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

Lemma 14.15 and Proposition 14.17 ensure that this map is well defined.

PROPOSITION 14.18. *The map* I *has the following properties:*

(i) $\mathrm{I}([a],[b])=\mathrm{I}([b],[a])$,
(ii) $\mathrm{I}([m],[a])=1$,
(iii) $\mathrm{I}([a],[b])+\mathrm{I}([a]+[b],[c])=\mathrm{I}([b],[c])+\mathrm{I}([a],[b]+[c])$,
(iv) $\mathrm{I}([a],n[a])\geq 1$ *for some* $n\geq 1$.

PROOF. (i) Trivial.

(ii) Clearly $k_{a+m}=k_a+1$ and $k_m=0$ ($m-m=0\notin S$ since S has no idempotents). Thus

$$k_{a+m}-k_a-k_m = k_a+1-k_a-0=1.$$

(iii) Since

$$\mathrm{I}([a]+[b],[c]) = \mathrm{I}([a+b],[c]) = k_{a+b+c} - k_{a+b} - k_c$$

and

$$\mathrm{I}([a],[b]+[c]) = \mathrm{I}([a],[b+c]) = k_{a+b+c} - k_a - k_{b+c},$$

we have that

$$\mathrm{I}([a],[b]) + \mathrm{I}([a]+[b],[c]) = k_{a+b} - k_a - k_b + k_{a+b+c} - k_{a+b} - k_c =$$

$$= k_{a+b+c} - k_a - k_b - k_c =$$

$$= k_{b+c} - k_b - k_c + k_{a+b+c} - k_a - k_{b+c} = \mathrm{I}([b],[c]) + \mathrm{I}([a],[b]+[c]).$$

(iv) Since in every R_m-class there exists an element in $\mathrm{Im}(\mathrm{A}_S^m)$, it suffices to show that for every $a \in \mathrm{Im}(\mathrm{A}_S^m)$, there exists $n \geq 1$ such that $\mathrm{I}([a],n[a]) \geq 1$. Since $a \in \mathrm{Im}(\mathrm{A}_S^m)$, we have that $k_a = 0$. Hence we are looking for an element $n \geq 1$ such that $k_{na+a} - k_{na} > 0$. The semigroup S is Archimedean and thus there exist $t \in \mathbb{N} \setminus \{0\}$ and $z \in S$ such that $ta = m+z$. Note that t cannot be equal to 1, since this would mean that $k_a \geq 1$. Thus $k_{ta} \neq 0$ and the set

$$\{x \in \mathbb{N} \mid k_{xa} \neq 0\}$$

is not empty. Let n be the minimum of this set. Like t, the element n is not equal to 1. Therefore $k_{na} \neq 0$ and $k_{(n-1)a} = 0$. We conclude that

$$\mathrm{I}([a],(n-1)[a]) = k_{na} - k_a - k_{(n-1)a} = k_{na} \neq 0.$$

□

Properties (i) and (iii) of I allows us to define the following associative and commutative binary operation on $\mathbb{N} \times S/R_m$:

$$(a,[x]) + (b,[y]) = (a+b+\mathrm{I}([x],[y]),[x]+[y]).$$

Therefore $\mathbb{N} \times S/R_m$, with this binary operation, is a semigroup. This semigroup is isomorphic to S as the following result shows.

THEOREM 14.19. *Let S be a $\mathcal{N}$-semigroup and m be an element in S. The semigroup $\mathbb{N} \times S/R_m$, with the binary operation $+$ defined above, is isomorphic to S.*

PROOF. By Proposition 14.17, for every $s \in S$ there exists a unique pair $(k,x) \in \mathbb{N} \times \mathrm{Im}(\mathrm{A}_S^m)$ such that $s = km+x$. Define

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

Recall that $(k,x) = (k_s, s-k_s m)$. Hence $\theta(s) = (k_s,[s-k_s m]) = (k_s,[s])$. It is easy to show that the map θ is bijective. Take $a,b \in S$. Then

$$\theta(a)+\theta(b) = (k_a,[a]) + (k_b,[b]) = (k_a+k_b+\mathrm{I}([a],[b]),[a]+[b]) =$$

$$= (k_a+k_b+k_{a+b}-k_a-k_b,[a+b]) = (k_{a+b},[a+b]) = \theta([a+b]).$$

□

The converse of this result is also true. Let G be a group and let $\mathrm{I} : G \times G \to \mathbb{N}$ be a map verifying the properties:

(i) for all $g_1, g_2 \in G$, $\mathrm{I}(g_1, g_2) = \mathrm{I}(g_2, g_1)$,
(ii) for every $g \in G$, $\mathrm{I}(0, g) = 1$,
(iii) for all $g_1, g_2, g_3 \in G$, $\mathrm{I}(g_1, g_2) + \mathrm{I}(g_1 + g_2, g_3) = \mathrm{I}(g_2, g_3) + \mathrm{I}(g_1, g_2 + g_3)$,
(iv) for all $g \in G$, there exits $k \in \mathbb{N} \setminus \{0\}$ such that $\mathrm{I}(g, kg) \geq 1$.

Define on $\mathbb{N} \times G$ the binary operation

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

By (i) and (iii), this operation provides $\mathbb{N} \times G$ with the structure of a semigroup. Denote this semigroup by $\mathbb{N} \ltimes_{\mathrm{I}} G$.

THEOREM 14.20. *For every group G and every map I satisfying conditions (i) – (iv), the semigroup $\mathbb{N} \ltimes_{\mathrm{I}} G$ is a $\mathcal{N}$-semigroup.*

PROOF. Conditions (i) and (iii) ensure that $\mathbb{N} \ltimes_{\mathrm{I}} G$ is a commutative semigroup. Assume that $(a_1, g_1) + (a_3, g_3) = (a_2, g_2) + (a_3, g_3)$. Then

$$(a_1 + a_3 + \mathrm{I}(g_1, g_3), g_1 + g_3) = (a_2 + a_3 + \mathrm{I}(g_2, g_3), g_2 + g_3),$$

which leads to $a_1 + a_3 + \mathrm{I}(g_1, g_3) = a_2 + a_3 + \mathrm{I}(g_2, g_3)$ and $g_1 + g_3 = g_2 + g_3$. Since $\mathbb{N}$ and G are both cancellative, we obtain that $g_1 = g_2$ and $a_1 = a_2$. Hence $(a_1, g_1) = (a_2, g_2)$. Therefore $\mathbb{N} \ltimes_{\mathrm{I}} G$ is cancellative.

If $2(a, g) = (a, g)$ for some $(a, g) \in \mathbb{N} \times G$, then $(a + a + \mathrm{I}(g, g), 2g) = (a, g)$. Thus $a + \mathrm{I}(g, g) = 0$ and $g = 0$, which leads to $\mathrm{I}(0, 0) = 0$, contradicting (ii). Thus $\mathbb{N} \ltimes_{\mathrm{I}} G$ has no idempotent elements.

Finally, let us show that $\mathbb{N} \ltimes_{\mathrm{I}} G$ is Archimedean.

- We show first that for every $(a, g) \in \mathbb{N} \ltimes_{\mathrm{I}} G$, there exist $k \in \mathbb{N} \setminus \{0\}$ and $(a', g') \in \mathbb{N} \ltimes_{\mathrm{I}} G$ such that $k(0, 0) = (a, g) + (a', g')$. Using induction on k it can be easily shown that

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

Then

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

- Let us show now that for every $(a, g) \in \mathbb{N} \ltimes_{\mathrm{I}} G$, there exist $k \in \mathbb{N} \setminus \{0\}$ and $(a', g') \in \mathbb{N} \ltimes_{\mathrm{I}} G$ such that $k(a, g) = (0, 0) + (a', g')$. By property (ii) of I, we have that $(0, 0) + (b, h) = (b + 1, h)$ and by (iv), there exists $n \geq 1$ for which $\mathrm{I}(g, ng) \geq 1$. By induction on n, it is easy to show that

$$(n + 1)(a, g) = ((n + 1)a + \mathrm{I}(g, g) + \mathrm{I}(g, 2g) + \cdots + \mathrm{I}(g, ng), (n + 1)g).$$

Since $\mathrm{I}(g, ng) \geq 1$, we have that

$$(n + 1)(a, g) = (0, 0) + ((n + 1)a + \mathrm{I}(g, g) + \mathrm{I}(g, 2g) + \cdots + \mathrm{I}(g, ng) - 1, (n + 1)g).$$

- Let $(x,y) \in (\mathbb{N} \ltimes_{\mathrm{I}} G) \times (\mathbb{N} \ltimes_{\mathrm{I}} G)$ such that $x \neq y$. Then there exists $k, k' \in \mathbb{N} \setminus \{0\}$ and $s, s' \in \mathbb{N} \ltimes_{\mathrm{I}} G$ for which $kx = (0,0) + s$ and $k'(0,0) = y + s'$. Therefore
$$kk'x = k'(0,0) + k's = y + (s' + k's).$$
This shows that $\mathbb{N} \ltimes_{\mathrm{I}} G$ is Archimedean.

□

We have shown that $\mathcal{N}$-semigroups are, up to isomorphism, semigroups of the form $\mathbb{N} \ltimes_{\mathrm{I}} G$, with G a group and I a map fulfilling conditions (i) trough (iv).

Remarks

The concept of a separative semigroup comes from the theory of representation of semigroups. The results appearing in Section 1 are originally by Hewitt and Zuckerman (see **[9]** and **[25]** for further information). The definition of $\mathcal{N}$-semigroup and the results appearing in Section 6 are due to Tamura and appear in **[62]**. The algorithm for deciding whether a finitely generated monoid is separative appears in **[52]** and the one for determining whether a finitely generated monoid is torsion free is described in **[53]**. The relationship between the property of being separative and its counterpart in semigroup ring theory is explained in **[19]**. Finally, elimination can be performed using the equivalence between σ and the ideal I_S by means of the computation of a Gröbner basis (see **[4]** or **[12]**).

Exercises

1. Prove that every finite separative monoid is a finite lattice of finite groups.
2. Show that if $\mathbb{N}^n/\sigma$ is separative, then $(a,b) \in \sim_{M_\sigma}$ implies that
$$(a + e_1 + \cdots + e_n, b + e_1 + \cdots + e_n) \in \sigma.$$
3. Prove that $\mathbb{N}^4/\langle\{((2,1),(0,4))\}\rangle$ is torsion free but not cancellative.
4. Prove that $\mathbb{N}/\langle\{(3,1)\}\rangle$ is separative but not torsion free.
5. Let σ be the congruence on $\mathbb{N}^3$ generated by
$$\{((3,0,0),(0,0,2)),((0,2,0),(1,0,1))\}.$$
Compute a system of generators of σ restricted to the set
$$\{(0,x,y) \mid (x,y) \in \mathbb{N}^2\}.$$
6. Let σ be the congruence on $\mathbb{N}^2$ generated by $\{((3,2),(2,1))\}$. Prove that $\mathbb{N}^2/\sim_{M_\sigma}$ is torsion free but $\mathbb{N}^2/\sigma$ is not torsion free.
7. Let $S = (1,1) + \mathbb{N}^2$. Prove that S is a $\mathcal{N}$-semigroup.
8. Let $(a_1,\ldots,a_n),(b_1,\ldots,b_n) \in \mathbb{N}^n$ such that
   (a) $a_1b_1 + \cdots + a_nb_n = 0$,
   (b) $\gcd\{a_1 - b_1,\ldots,a_n - b_n\} = 1$.
   Then $\mathbb{N}^n/\langle\{((a_1,\ldots,a_n),(b_1,\ldots,b_n))\}\rangle$ is a torsion free cancellative monoid.

9. Prove that every $\mathcal{N}$-semigroup is isomorphic to a subsemigroup of a reduced monoid with two Archimedean components.
10. Show that if S is a separative monoid with n idempotent elements, then S has at least n Archimedean components.
11. Show that a finite torsion free monoid with n elements has n Archimedean components.
12. Prove that an Archimedean cancellative semigroup is a group if and only if it contains an idempotent element.
13. Prove that if S is an Archimedean semigroup without idempotent elements, then for all $x, y \in S$, we have that $x + y \neq x$.
14. Prove that a submonoid of a separative monoid is separative.
15. Let S be a semigroup and let A be the set of elements $s \in S$ such that $2s = s$. Prove that A is a subsemigroup of S.
16. Find a congruence σ on $\mathbb{N}$ such that $\mathbb{N}/\sigma$ is not separative.
17. Prove that every subsemigroup of $\mathbb{N} \setminus \{0\}$ is a $\mathcal{N}$-semigroup.
18. Find a subsemigroup of a $\mathcal{N}$-semigroup which is not a $\mathcal{N}$-semigroup.

APPENDIX A

Graphs

We give the definitions concerning graphs that have been used in the text.

A **graph** G is a pair (V,E) where V is a set whose elements are called **vertices** of G and E is a subset of $(V \times V) \setminus \Delta(V)$ whose elements are called **edges** of G (the element $(a,b) \in E$ is usually denoted by $\overline{ab}$).

A **walk** of length r connecting the vertices x and y of G is a sequence

$$\overline{v_0 v_1}, \overline{v_1 v_2}, \dots, \overline{v_{r-1} v_r}$$

of edges of G such that $v_0 = x$ and $v_r = y$. We denote this walk by $v_0, v_1, \dots, v_r$.

A **path** is a walk all of whose edges are different. It is easy to show that if there is a walk connecting two vertices of G, then there is also a path connecting them.

A graph G is **connected** if for every two vertices of G, there exists a path connecting them.

Given a graph $G = (V,E)$, a **subgraph** $G' = (V',E')$ of G is a graph verifying that $V' \subseteq V$ and $E' \subseteq E$. A **connected component** of a graph G is a maximal connected subgraph of G. Every graph is a disjoint union of its connected components.

A **tree** is a connected graph (V,E) such that the cardinality of V is equal to the cardinality of E plus 1. If G is a connected graph, then we say that a tree T is a **generating tree** of G whenever T is a subgraph of G and every vertex of G is a vertex of T. Every connected graph admits at least one generating tree.

UNIVERSITAT DE BARCELONA

Biblioteca de Matemàtiques

Gran Via de les Corts Catalanes, 585
08007 Barcelona

Bibliography

[1] R. Apéry. *Sur les branches superlinéaires des courbes algébriques.* C. R. Acad. Sci. Paris, **222** (1946).

[2] G. Birkhoff. *Lattice Theory.* Amer. Math. Soc., Providence, 1967.

[3] A. Brauer and J. E. Shockley. *On a problem of Frobenius.* J. Reine Angew. Math., **211** (1962), 215-220.

[4] T. Becker and W. Weispfenning. *Gröbner bases: a computational approach to commutative algebra.* Springer, 1993.

[5] H. Bresinsky. *On prime ideals with generic zero* $x_i = t^{n_i}$. Proc. Amer. Math. Soc., **47** (2) (1975) 329-332.

[6] E. Briales, A. Campillo, C. Marijuán and P. Pisón. *Minimal systems of generators for ideals of semigroups.* J. Pure Appl. Algebra, **124** (1998), 7-30.

[7] A. H. Clifford. *Arithmetic and ideal theory of commutative semigroups.* Ann. of Math., **39** (1938), 594-610.

[8] A. H. Clifford. *Partially ordered abelian groups.* Ann. of Math., **41** (1949), 465-473.

[9] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups.* Amer. Math. Soc., Providence, 1961.

[10] P. Cohn. *Algebra vol. I.* Wiley, 1974.

[11] E. Contejean and H. Devie. *An efficient incremental algorithm for solving systems of linear diophantine equations.* Inform. and Comput., **113** (1994), 143-172.

[12] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties and Algorithms.* Springer, New York 1992.

[13] C. Delorme. *Sous-monoïdes d'intersection complète de* $\mathbb{N}$. Ann. Scient. École Norm. Sup. (4), **9**, 1976, 145-154.

[14] D. Eisenbud and B. Sturmfels. *Binomial Ideals.* Duke Math. J., **84** (1996), 1-45.

[15] P. Freyd. *Rédei's finitness theorem for commutative semigroups.* Proc. Amer. Math. Soc., **19** (1968), 1003.

[16] R. Fröberg. *The Frobenius number of some semigroups.* Comm. Algebra, **22**(14) (1994), 6021-6024.

[17] R. Fröberg, C. Gottlieb and R. Häggkvist. *On numerical semigroups.* Semigroup Forum, **35** (1987), 63-83.

[18] P. A. García-Sánchez. *Semigrupos afines.* Tesis Doctoral, Universidad de Granada, 1996.

[19] R. Gilmer. *Commutative semigroup rings.* Chicago Lectures in Math., 1984.

[20] G. M. Greuel, G. Pfister and H. Schoenemann. *Singular Reference Manual.* In: Reports On Computer Algebra, **20**. Centre for Computer Algebra, University of Kaiserslautern, June 1998. http://www.mathematik.uni-kl.de/ zca/Singular

[21] P. A. Grillet. *The free envelope of a finitely generated commutative semigroup.* Trans. Amer. Math. Soc., **149** (1970), 665-682.

[22] P. A. Grillet. *A short proof of Redei's theorem.* Semigroup Forum, **46** (1993), 126-127.

[23] P. A. Grillet. *Semigroups. An introduction to the structure theory.* Dekker, 1995.

[24] J. Herzog. *Generators and relations of abelian semigroups and semigroup rings.* Manuscripta Math., **3** (1970), 175-193.

[25] E. Hewitt and H. S. Zuckerman. *The l_1-algebra of a commutative semigroup*. Trans. Amer. Math. Soc., **83** (1956), 70-97.

[26] M. Hochster. *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes*. Ann. of Math., **96** (1972), 318-337.

[27] N. Jacobson. *Basic Algebra I*. W.H. Freeman and company, 1994.

[28] 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.

[29] Y. Koda. *The numbers of finite lattices and finite topologies*. Bulletin of the ICA, **10** (1994), 83-89.

[30] E. Kunz. *The value-semigroup of a one-dimensional Gorenstein ring*. Proc. Amer. Math. Soc., **25** (1973), 748-751.

[31] S. Kyuno. *An inductive algorithm to construct finite lattices*. Math. of comp., **33** (145)(1970) 409-421.

[32] S. Kyuno and A. Ito. *The construction of finite lattices*. Tohoku-Gakuin University. Faculty of Engineering research report, **20**(2) (1986), 71-79.

[33] G. Lettl. *Subsemigroups of finitely generated groups with divisor-theory*. Monatsh. Math., **106**, 205-210 (1988).

[34] H. Pinkham. *Deformations of algebraic varieties with G_m action*. Asterisque, **20** (1974).

[35] P. Pisón and A. Vigneron Tenorio. *Ideales de semigrupos con torsión: cálculos mediante Maple V*. EACA'96, Universidad de Sevilla.

[36] L. Pottier. *Bornes et algorithme de calcul des générateurs des solutions de systèmes diophantiens linéaires*. C. R. Acad. Sci. Paris, **311** (1990), 813-816.

[37] G. B. Preston. *Rédei's characterization of congruences of finitely generated free commutative semigroups*. Acta Math. Acad. Sci. Hungar., **26** (1975), 337-342.

[38] R. C. Read. *A survey of graph generation techniques. Eighth Australian Combinatorics Conference, Deakin University 1980*. Lecture Notes in Math., **884**, Springer, 1981, 77-89.

[39] L. Rédei. *The theory of finitely generated commutative semigroups*. Pergamon, 1965.

[40] J. C. Rosales. *Semigrupos numéricos*. Tesis Doctoral, Universidad de Granada, 1991.

[41] J. C. Rosales. *On finitely generated submonoids of $\mathbb{N}^k$*. Semigroup Forum, **50** (1995) 251-262.

[42] J.C. Rosales. *Function minimum associated to a congruence on integral n-tuple space*. Semigroup Forum, **51** (1995), 87-95.

[43] J.C. Rosales. *On numerical semigroups*. Semigroup Forum, **52** (1996), 307-318.

[44] J.C. Rosales. *An algorithmic method to compute a minimal relation for any numerical semigroup*. Internat. J. Algebra Comput., **6**(4), (1996) 441-455.

[45] J.C. Rosales. *On symmetric numerical semigroups*. J. Algebra, **182** (1996) 422-434.

[46] J. C. Rosales and P. A. García-Sánchez. *On affine semigroups with divisor theory*. EACA'96, Universidad de Sevilla.

[47] J. C. Rosales and P. A. García-Sánchez. *Nonnegative elements of subgroups of $\mathbb{N}^n$*. Linear Algebra Appl., **270** (1998), 351-357.

[48] J. C. Rosales and P. A. García-Sánchez. *On numerical semigroups with high embedding dimension*. J. Algebra, **203** (1998), 567-578.

[49] J.C. Rosales and P. A. García-Sánchez. *On Cohen-Macaulay and Gorenstein simplicial affine semigroups*. To appear in the Proc. Edinburgh Math. Soc.

[50] J. C. Rosales and P. A. García-Sánchez. *On normal affine semigroups*. To appear in Linear Algebra Appl.

[51] J. C. Rosales and P. A. García-Sánchez. *Numerical semigroups generated by intervals*. To appear in Pacific J. Math.

[52] J. C. Rosales and P. A. García-Sánchez. *Archimedean components and finitely generated commutative separative monoids*. Manuscript.

[53] J. C. Rosales and P. A. García-Sánchez. *A deterministic algorithm to decide if a finitely presented monoid is torsion free*. Manuscript.

[54] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco. *Sobre un tipo de proyecciones para congruencias en* $\mathbb{N}^n$. EACA'97, Universidad de Granada.

[55] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco. *On presentations of commutative monoids*. To appear in Internat. J. Algebra Comput.

[56] 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.

[57] J. Sally. *Cohen-Macaulay local rings of maximal embedding dimension*. J. Algebra, **56** (1979), 168-183.

[58] L. E. Sigler. *Algebra*. Reverté, 1981.

[59] B. Sturmfels. *Gröbner bases of toric varieties*. Tôhoku Math. J., **43** (1991), 249-261.

[60] B. Sturmfels. *Gröbner bases and convex polytopes*. Amer. Math. Soc., Providence, RI, 1995.

[61] J. J. Sylvester. *Mathematical questions with their solutions*. Educational Times, **41** (1884), 21.

[62] T. Tamura. *Nonpotent Archimedean semigroups with cancellative law*. I. J. Gakugei Tokushima Univ., **8** (1957), 5-11.

[63] T. Tamura and N. Kimura. *On decompositions of a commutative semigroup*. Kodai Math. Sem. Rep., 1954, 109-112.

[64] N. V. Trung and L.T. Hoa. *Affine semigroups and Cohen-Macaulay rings generated by monomials*. Trans. Amer. Math. Soc., **298** (1986), 145-167.

[65] K. Watanabe. *Some examples of one dimensional Gorenstein domains*. Nagoya Math. J., **49** (1973), 101-109.

Index of notation

$\mathbb{N}$ - monoid of nonnegative integers
$\mathbb{Q}$ - field of rational numbers
$\mathbb{Q}_0^+$ - set of nonnegative rational numbers
$\mathbb{Z}$ - group of additive integers
$\mathbb{Z}_n$ - cyclic group with n elements
$n\mathbb{Z}$ - set of integer multiples of n
$\emptyset$ - empty set
$\subseteq$ - contained in or equal to
$\subset$ - contained in but not equal to
$\leq$ - usual (partial) order on $\mathbb{N}^n$, $\mathbb{Z}^n$, $\mathbb{Q}^n$
$\preceq_{lex}$ - lexicographical order
$\preceq_{rlex}$ - reverse lexicographical order
$\preceq_{tdeg}$ - total degree order
$A \setminus B = \{a \in A \mid a \notin B\}$
$A + B = \{a + b \mid a \in A,\ b \in B\}$
$A \times B = \{(a,b) \mid a \in A,\ b \in B\}$
$A^n = A \times \cdots \times A$, n times
$\mathcal{P}(A) = \{B \mid B \subseteq A\}$ - power set of A
$\langle A \rangle$ - monoid generated by A
$\mathbf{G}(A)$ - group generated by A
$\mathbf{L}_{\mathbb{Q}}(A)$ - $\mathbb{Q}$-vector space generated by A
$\mathbf{L}_{\mathbb{Q}_0^+}(A) = \{\sum_{i=1}^n q_i a_i \mid q_i \in \mathbb{Q}_0^+,\ a_i \in A,\ n \in \mathbb{N}\}$
$A^\perp$ - orthogonal subspace of the subspace A
$\Delta(A) = \{(a,a) \mid a \in A\}$ - diagonal of $A \times A$
$M_\sigma = \{a - b \in \mathbb{Z}^n \mid (a,b) \in \sigma\}$
$\sim_M = \{(a,b) \in \mathbb{N}^n \times \mathbb{N}^n \mid a - b \in M\}$
$\sigma_A = \sigma \cap (A \times A)$ - the restriction of σ to A
$\mathfrak{I}_\sigma$ - set of irreducible elements of σ
$\mathfrak{P}_\sigma$ - set of primitive elements of σ
$\{e_1, \ldots, e_n\}$ - "canonical" basis of $\mathbb{Z}^n$
$\gcd(a,b)$ - greatest common divisor of a and b
$\operatorname{lcm}(a,b)$ - least common multiple of a and b
$a \bmod b$ - remainder of the integer division of a by b
$a \operatorname{div} b$ - quotient of the integer division of a by b

$a \equiv b \pmod{m}$ - m divides $a-b$
$\max(a,b)$ - the maximum of a and b
$\min(a,b)$ - the minimum of a and b
$a \vee b$ - supremum of a and b
$a \wedge b$ - infimum of a and b
$\overline{a}$ - complement of a
$-a$ - inverse of a
$\mathrm{NF}_\rho(a)$ - normal form of a with respect to ρ
$|a|$ - absolute value of a
$(a_1,\dots,a_n)^+ = (\max(a_1,0),\dots,\max(a_n,0))$
$(a_1,\dots,a_n)^- = (-\min(a_1,0),\dots,-\min(a_n,0))$
$\det(A)$ - determinant of the matrix A
$\mathrm{Im}(f)$ - image of the map f
$\mathrm{Ker}(f)$ - kernel of the map f
$\mathrm{rank}(G)$ - rank of the group G
$\mathrm{C}(S)$ - the conductor of the numerical semigroup S
$\mathrm{U}(S)$ - units of the monoid S
$\mathrm{Ap}(S,a) = \{s \in S \mid s-a \notin S\}$
$\mathrm{Ap}(S,a_1,\dots,a_n) = \bigcap_{i=1}^n \mathrm{Ap}(S,a_i)$
$\Delta_n = (\mathrm{V}(\Delta_n),\mathrm{E}(\Delta_n))$ - the graph associated to n
$\rho^{-1} = \{(a,b) \mid (b,a) \in \rho\}$
$\langle\rho\rangle$ - the congruence generated by ρ
S/σ - quotient monoid of S modulo σ

Index of main results and algorithms

Chapter 1

If S is a monoid generated by n elements, then there exists a congruence σ on $\mathbb{N}^n$ such that S is isomorphic to $\mathbb{N}^n/\sigma$. — Theorem 1.2, page 3

$\mathbb{N}^n/\sigma$ is cancellative if and only if $\sigma = \sim_{M_\sigma}$. — Proposition 1.4, page 4

$\mathbb{N}^n/\sim_M$ is a group if and only if M contains a strongly positive element. — Proposition 1.7, page 5

Chapter 2

A subgroup of $\mathbb{Z}^n$ has a basis with at most n elements. — Proposition 2.2, page 10

All bases of a subgroup of $\mathbb{Z}^n$ have the same cardinality. — Proposition 2.3, page 11

If M is a subgroup of $\mathbb{Z}^n$ with $\operatorname{rank}(M) = r$, then there exists a basis $\{f_1, \dots, f_r, \dots, f_n\}$ of $\mathbb{Z}^n$ and $\{d_1, \dots, d_r\} \subset \mathbb{N} \setminus \{0\}$ such that d_i divides d_{i+1} and $\{d_1 f_1, \dots, d_r f_r\}$ is a basis of M. — Theorem 2.12, page 16

If M is a subgroup of $\mathbb{Z}^n$ with invariant factors $d_1, \dots, d_r$, then $\mathbb{Z}^n/M$ is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$. — Theorem 2.14, page 19

Computing a basis of a subgroup of $\mathbb{Z}^n$ from one of its systems of generators. — Section 3.1, page 20

Computing a basis of a subgroup of $\mathbb{Z}^n$ from its defining equations. — Section 3.2, page 21

Chapter 3

A finitely generated monoid is cancellative and torsion free if and only if it is isomorphic to a submonoid of $\mathbb{Z}^k$ for some nonnegative integer k.	Corollary 3.4, page 27
Let V be a subspace of $\mathbb{Q}^n$. The subspace $V^\perp$ has a strongly positive element if and only if the only nonnegative element of V is 0.	Lemma 3.9, page 30
Grillet's theorem: A finitely generated monoid is cancellative, torsion free and reduced if and only if it is isomorphic to a submonoid of $\mathbb{N}^k$ for some nonnegative integer k.	Theorem 3.11, page 30
A finite monoid is a group if and only if it is cancellative.	Proposition 3.13, page 32
Characterization of the subgroups M of $\mathbb{Z}^n$ such that $\mathbb{N}^n / \sim_M$ is finite.	Theorem 3.14, page 32

Chapter 4

Minkowski-Farkas' Lemma.	Theorem 4.1, page 35
Computes a nonnegative element of a subspace of $\mathbb{Q}^n$ with its first coordinate greater than zero (if such element exists).	Algorithm FP, page 38
Computes a strongly positive element of a subspace of $\mathbb{Q}^n$ (if such element exists).	Algorithm SP, page 40
Computes a nonnegative element of a subspace of $\mathbb{Q}^n$ with maximum number of positive coordinates.	Algorithm MCP, page 40
Algorithmic method for deciding whether $\mathbb{N}^n / \sim_M$ is or not a group.	Section 2.1, page 41
Algorithmic method for deciding whether $\mathbb{N}^n / \sim_M$ is or not an affine semigroup.	Section 2.2, page 41
Algorithm for computing $\mathrm{U}(\mathbb{N}^n / \sim_M)$.	Section 2.3, page 43

Algorithmic method for deciding whether a linear homogeneous system of equations has a nontrivial nonnegative solution. — Section 2.4, page 44

Algorithmic method for deciding whether two submonoids of $\mathbb{N}^n$ have nontrivial intersection. — Section 2.5, page 45

Chapter 5

Dickson's Lemma: The sets of incomparable elements (with respect to the usual partial order) of $\mathbb{N}^n$ are finite. — Theorem 5.1, page 48

Every linear admissible order on $\mathbb{N}^n$ is a well order. — Corollary 5.7, page 49

Rédei's Theorem: Every finitely generated monoid is finitely presented. — Theorem 5.12, page 52

Every cyclic monoid is isomorphic to either $\mathbb{N}$ or to $\mathbb{N}/\langle\{(a,b)\}\rangle$ for some $(a,b) \in \mathbb{N}\times\mathbb{N}$. — Proposition 5.13, page 53

Chapter 6

Computes a canonical system of generators of a congruence. — Algorithm CPC, page 61

Computes $\mathrm{U}(\mathbb{N}^n/\sigma)$. — Algorithm 6.18, page 68

Chapter 7

Pottier's theorem: Bound for the minimal nonnegative solutions of the system $Ax = 0$, with A a matrix with integer entries. — Theorem 7.2, page 75

Algorithmic method for computing a minimal system of generators of the monoid of nonnegative elements of a subgroup of $\mathbb{Z}^n$. — Section 2, page 77

Algorithmic method for computing the set of nonnegative integer solutions of a system of linear equations with integer coefficients. — Section 3, page 80

Algorithmic method for deciding whether an affine semigroup is normal. — Section 4, page 81

Chapter 8

If M is a subgroup of $\mathbb{Z}^n$, then $\sim_M$ is a finitely generated submonoid of $\mathbb{N}^n \times \mathbb{N}^n$.	Proposition 8.1+8.2, page 85
Bound for the elements of a minimal system of generators of $\sim_M$ as submonoid of $\mathbb{N}^n \times \mathbb{N}^n$. As a consequence yields an algorithmic method for computing a presentation of $\mathbb{N}^n / \sim_M$.	Corollary 8.8, page 90
Algorithmic method for deciding whether $\mathbb{N}^n / \sigma$ is cancellative from a system of generators of σ.	Section 3, page 90

Chapter 9

Characterization of minimal presentations of finitely generated reduced cancellative monoids.	Theorem 9.4, page 95
Algorithmic method for computing a minimal presentation of an affine semigroup.	Section 2, page 96
There is no upper bound for the cardinality of a minimal presentation of an affine semigroup in terms of the number of generators of the affine semigroup.	Proposition 9.13, page 102

Chapter 10

Computes a minimal presentation of a numerical semigroup.	Algorithm MPNS, page 109
Upper bound for the cardinality of a minimal presentation of a numerical semigroup.	Theorem 10.15, page 112
Characterization of numerical semigroups with maximal embedding dimension in terms of the cardinality of minimal presentations.	Proposition 10.18, page 114
Show how maximal embedding dimension numerical semigroups classify numerical semigroups.	Corollary 10.21, page 116

Chapter 11

If $\mathbb{N}^n/\sigma$ is cancellative, then σ can be obtained after a finite sequence of projections of a congruence σ' such that $\mathbb{N}^{n+k}/\sigma'$ is an affine semigroup.	Theorem 11.3, page 122
The cardinality of a canonical system of generators of a congruence is not bounded in terms of the cardinal of a minimal system of generators of the congruence.	Section 2.1, page 125

Chapter 12

Characterization of the presentations of finite monoids. This characterization can be used to check whether $\mathbb{N}^n/\sigma$ is finite.	Proposition 12.1, page 129
Gives a method for deciding whether $\mathbb{N}^n/\sigma$ is a finite torsion free monoid.	Theorem 12.3, page 130
The concepts of finite torsion free monoid and finite lattice are equivalent.	Theorem 12.6, page 132
Lattices are sets with two binary operations satisfying associative, commutative, idempotent and absorption laws.	Theorem 12.8, page 133
The concepts of Boolean algebra and distributive complemented lattice coincide.	Corollary 12.11, page 135
Finite Boolean algebras are, up to isomorphisms, power sets of finite sets with the binary operations $\cup$ and $\cap$.	Theorem 12.15, page 137
Finite Boolean monoids are, up to isomorphisms, power sets of finite sets with the binary operation $\cup$.	Theorem 12.18, page 138
Characterization of the presentations of finite Boolean monoids	Theorem 12.20, page 139

Chapter 13

Every finitely generated monoid is a finite lattice of Archimedean semigroups.	Theorem 13.5, page 145
Gives an algorithmic method for computing the Archimedean components of a finitely generated monoid.	Theorem 13.10, page 147

Chapter 14

A monoid is separative if and only if it is asymptotic free of torsion.	Proposition 14.2, page 153
A monoid is separative if and only if its Archimedean components are cancellative.	Proposition 14.3, page 154
Every finitely generated separative monoid is a finite lattice of cancellative Archimedean semigroups.	Corollary 14.4, page 154
Algorithmic method for determining whether the quotient of an ideal of $\mathbb{N}^n$ by the restriction of a congruence of $\mathbb{N}^n$ to the ideal is cancellative.	Section 2, page 155
Algorithmic method for computing a system of generators of $\sigma \cap (\mathbb{N}^r \times \mathbb{N}^r)$ from a system of generators of the congruence σ on $\mathbb{N}^{r+m}$.	Section 3, page 158
Algorithmic method for deciding whether a finitely generated monoid is separative.	Section 4, page 158
Algorithmic method for deciding whether a finitely generated monoid is torsion free.	Section 5, page 160
Structure theorem for $\mathcal{N}$-semigroups.	Theorem 14.19+14.20, page 165

Index

Apéry set, 51
Archimedean component, 143–150, 153–155
associative law, 1

binary relation, *see also* relation
Boolean algebra, 133
  atom of a Boolean algebra, 135
  finite Boolean algebra, 133–137

commutative law, 1
complement, 134
complement law, 134
complete system modulo m, 106
congruence, 2, 143
  canonical system of generators of a congruence, 59–65, 125–126
  congruence associated to a group, 4
  congruence generated by a set, 51, 52
  diagonal congruence, 47
  finitely generated congruence, 52
  irreducible elements of a congruence, 85
  kernel congruence, 3
  primitive elements of a congruence, 85–87
  projection of a congruence, 119
  reduced system of generators of a congruence, 57–59
  system of generators of a congruence, 52
CPC algorithm, 61

Dickson's Lemma, 48
distributive law, 134
dot product, 71

FP algorithm, 38

graph, 169
  connected component of a graph, 169
  graph Δ_n associated to an element of an affine semigroup, 96
  graph $G(\rho)$ associated to a presentation, 145
  graph G_ρ associated to a binary relation with respect to a partition, 94
  subgraph of a graph, 169
  tree, 169
    generating tree, 169
Grillet's theorem, 30
group, 1, 6, 41
  finitely generated group, 2, 9–23
  group associated to a congruence, 4
  group generated by a set, 2
  group of quotients, 34
  group of units of a cancellative monoid, 43–44
  group of units of a monoid, 65–69
  subgroup of a group, 2
    basis of a subgroup of $\mathbb{Z}^n$, 9, 20–23
    equations of a subgroup of $\mathbb{Z}^n$, 18
    homogeneous subgroup of $\mathbb{Z}^n$, 18
    invariant factors of a subgroup of $\mathbb{Z}^n$, 17
    rank of a subgroup of $\mathbb{Z}^n$, 11
    set of linear independent elements a subgroup of $\mathbb{Z}^n$, 9
  system of generators of a group, 2

idempotent law, 131
identity element, 1
infimum, 130

lattice, 131
  complemented lattice, 134
  distributive lattice, 134
  finite lattice, 130–133

matrix
  elementary matrices, 12
  equivalent matrices, 12
  invariant factors of a matrix, 14
  minor of a matrix, 14
maximum, 47
MCP algorithm, 40
minimal element, 47

minimum, 47
minimum function, 50
Minkowski-Farkas' Lemma, 36
monoid, 1
  asymptotic free of torsion monoid, 153
  Boolean monoid, 137–139
  cancellative monoid, 1, 4, 5, 25–33, 90–91
    finite monoid, 32–33
    group of units of a cancellative monoid, 43–44
    minimal presentation of a cancellative monoid, 93–96
    presentation of a cancellative monoid, 87–90, 119–123
  cyclic monoid, 53
  direct product of monoids, 2
  finite monoid, 32
    presentation of a finite monoid, 129–130
  finitely generated monoid, 2
  finitely presented monoid, 52
  group of units of a monoid, 65–69
  ideal of a monoid, 62
    ideal generated by a set, 62
  identity element of a monoid, 1
  intersection of submonoids of $\mathbb{N}^n$, 45
  isomorphic monoids, 3
  minimal presentation of a monoid, 93–102, 108–113
  monoid generated by a set, 2
  presentation of a monoid, 47–71, 87–90, 93–102, 108–113, 119–127, 129–130
  quotient monoid, 3
  reduced monoid, 28–31
  separative monoid, 153–155, 158–159
  submonoid of a monoid, 1
    complement of a submonoid, 43
  system of generators of a monoid, 2
  torsion free monoid, 27–28, 160–162
    presentation of a torsion free monoid, 129–130
  unit of a monoid, 28
morphism, 3
  epimorphism of monoids, 3
  isomorphism of monoids, 3
  monomorphism of monoids, 3
  morphism of Boolean algebras, 136
  morphism of monoids, 3
    image of a morphism of monoids, 3
    kernel of a morphism of monoids, 3
  morphism of semigroups, 143
MPNS algorithm, 109

nonnegative element, 5
normal form, 58

order, 47
  admissible order, 49
  lexicographical order, 54
  linear order, 47
    linear admissible order, 47–49
  prime order, 55
  product order, 48
  reverse lexicographical order, 55
  total degree order, 55
  well order, 47
orthogonal space, 29

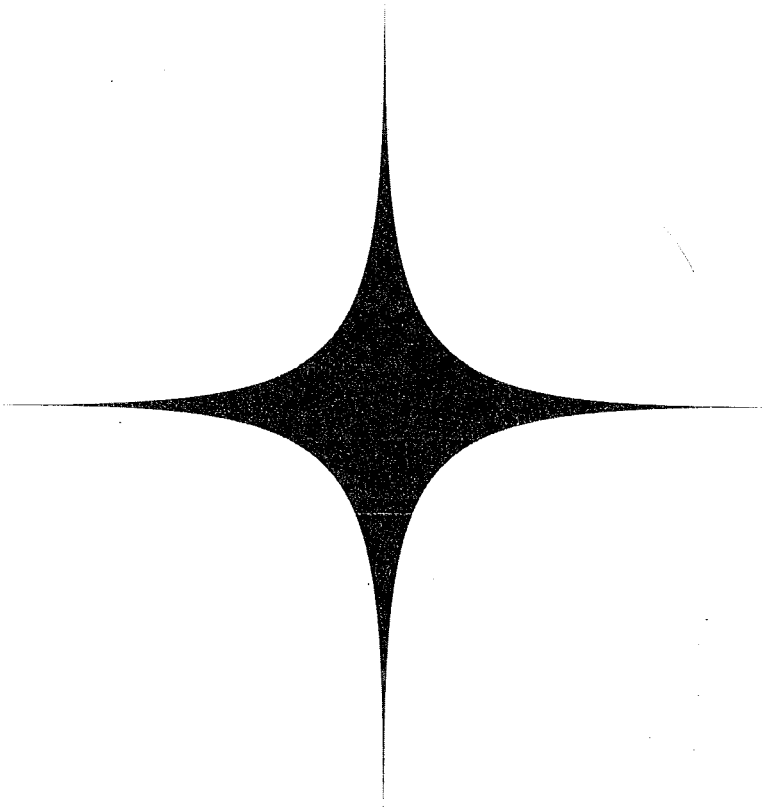
partial order, *see also* order
Pottier's theorem, 75
power set, 135
primary representation, 108

Redei's theorem, 52
Reduce algorithm, 58
relation, 2
  antisymmetric relation, 47
  congruence, *see also* congruence
  equivalence relation, 2
  inverse relation, 47
  partial order, *see also* order
  reflexive relation, 2
  symmetric relation, 2
  transitive relation, 2

semigroup, 1
  affine semigrou
    full affine semigroup, 77
  affine semigroup, 31
    minimal presentation of an affine semigroup, 96–102
    normal affine semigroup, 81–83
  Archimedean semigroup, 145, 162–167
  cancellative semigroup, 143, 162–167
  finitely generated semigroup, 143
  $\mathcal{N}$-semigroups, 162–167
  numerical semigroup, 105–118, 126–127
    conductor of a numerical semigroup, 106
    embedding dimension of a numerical semigroup, 113
    minimal presentation of a numerica semigroup, 108

minimal presentation of a numerical semigroup, 113
multiplicity of a numerical semigroup, 113
numerical semigroup with maximal embedding dimension, 113
presentation of a numerical semigroup, 126–127
quotient semigroup, 143
semigroup generated by a set, 143
semigroup ring, 54
semilattice
lower semilattice, 131
upper semilattice, 131
SP algorithm, 40
strongly positive element, 5
supremum, 130
system of incongruent integers modulo m, 106

word problem for monoids, 53, 57–71



Cover design:
Frank Grucci

ISBN 1-56072-670-9