ABELIAN MONOIDS

ABELIAN MONOIDS

By

DALE STEPHEN COOPER, B.SC.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfilment of the Requirements

for the Degree

Master of Science

McMaster University

October 1970

MASTER OF SCIENCE (1970) McMASTER UNIVERSITY
(Mathematics) Hamilton, Ontario

TITLE: Abelian Monoids

AUTHOR: Dale Stephen Cooper, B.Sc. (McMaster University)

SUPERVISOR: Dr. T. M. K. Davison

NUMBER OF PAGES: vi, 74

SCOPE AND CONTENTS: This thesis makes a small study of various kinds of submonoids of abelian monoids, of the lattice of submonoids of an abelian monoid, and of the concept of unique factorization in abelian monoids. Also, the main concepts in category theory are examined in the special case of the category of abelian monoids and some of its subcategories.

PREFACE

In this century, a great deal of work has been done in the theory of groups and in the theory of semigroups. To the extent that monoids are special semigroups and groups are special monoids, we also know something about monoids. Moreover, there have appeared some papers dealing exclusively with monoids, usually abelian monoids. As far as the author can determine however, these have been relatively few in number; also, no really systematic treatment of monoids by themselves has yet appeared.

This paper attempts to provide an elementary introduction to the theory of abelian monoids. Most of the results are quite standard, or at least routine. As far as the author can determine, however, most of the results found in Chapter 1, § 3, Chapters II and III, and Chapter IV, §§ 6, 7 are new.

ACKNOWLEDGMENTS

The author expresses his deep gratitude to his supervisor, Dr. T. M. K. Davison, whose patience and guidance were of inestimable value in the preparation and review of this thesis.

The author also acknowledges the financial support of the National Research Council and McMaster University. Thanks go also to Mrs. Claudia McCarty for her prompt and efficient typing of the manuscript.

TABLE OF CONTENTS

NOTATIONS

Any notations that are not standard are introduced as the need arises. A partial summary of the notations used is included here for the reader's convenience.

$\exists$	there exist (s)
$\ni$	such that
$\forall$	for any
$\cong$	is isomorphic to
$<$	is a submonoid of
$\not<$	is a connected submonoid of
Δ	is a normally connected submonoid of
$\downarrow$	covers
$\vee$	join
$\wedge$	meet
ε	belongs to
$f_*(A)$	$\{ f(a) \mid a \varepsilon A \}$
$\Rightarrow$	implies
$\Leftrightarrow$	if and only if
$f: A \longrightarrow B$	f is a function (or morphism) from A into B
$a \longmapsto x$	a is mapped into x.

CHAPTER I

PRELIMINARY NOTIONS

§ 1: Introduction

Definition 1: A monoid is an ordered triple $(M, \cdot, i)$, where M is a set, $\cdot$ is an associative binary operation on M, $i \in M$, and $m \cdot i = m = i \cdot m$, for any $m \in M$. We call i the identity element of the monoid. If moreover $a \cdot b = b \cdot a$ for any $a, b \in M$, then we call $(M, \cdot, i)$ an abelian monoid. //

Remarks: 1. We shall observe the usual convention of referring to a monoid in terms of its underlying set only, unless there is ambiguity.

2. When the monoid's operation is denoted multiplicatively, we shall usually denote its identity by 1.

3. When the monoid's operation is denoted additively, we shall usually denote its identity by 0.

4. Unless indicated otherwise, we shall normally write monoids multiplicatively. //

Notations: 1. The class of all abelian monoids will be denoted $\mathcal{AM}$.

2. The class of all abelian groups will be denoted $\mathcal{Ab}$. //

Definition 2: Let M, N be monoids. Let $f: M \longrightarrow N$. We say

f is a <u>morphism of monoids</u> (or monoid homomorphism) if and only if $f(1) = 1$ and $f(xy) = f(x)\,f(y)$ for any $x, y \in M$. //

<u>Definition 3</u>: Let M be a monoid, and let $N \subseteq M$. We say N is a <u>submonoid</u> of M, denoted $N < M$, if and only if $1 \in N$ and, $x, y \in N$ implies $xy \in N$. //

If $(N_i)_{i \in I}$ is a family of submonoids of a monoid M, then it is easily seen that $\bigcap_{i \in I} N_i < M$. Thus, it makes sense to talk about the submonoid of M generated by some subset S of M; namely $\bigcap \mathcal{N}$, where $\mathcal{N} = \{ N < M \mid S \subseteq N \}$.

Notationally, if $a \in M$, then we will denote the submonoid generated by a, by $< a >$. Of course, $< a > = \{1, a, a^2, a^3, \ldots\}$. Also, we will have occasion to refer to $\{1, a^2, a^3, \ldots\}$, and this will be denoted $< a >'$. It should be noted that $< a >'$ and $< a > \setminus \{a\}$ are not necessarily the same.

<u>Definition 4</u>: Let M be a monoid, and let $N < M$. Then we say N is <u>finitely generated</u> if and only if there exists $S \subseteq N$ such that N is the submonoid generated by S, and S is finite. //

Two monoids which come to mind most readily are the set $\{0, 1, 2, \ldots\}$ under addition, and the set $\{1, 2, 3, \ldots\}$ under multiplication. The former set will be denoted $\mathbb{N}_0$, while the latter will be written $\mathbb{N}$. When considered as monoids, the operations will be as above unless otherwise stated.

Notationally, we will use $\mathbb{Z}$ to denote the set of rational integers, and when considered as a monoid, the operation will be assumed to be addition.

Occasionally we will refer to $\mathbb{R}$, and this will be understood to be the set of real numbers.

It is assumed that the reader is familiar with the concept of congruence relation - in our case an equivalence relation θ in an abelian monoid M such that $a \theta b$, $x \theta y$ implies $ax \theta by$, for all $a, b, x, y \in M$. The set of congruence classes will be denoted M/θ, and of course this is also an abelian monoid under the induced operation.

One particular congruence relation is introduced below - one which at first glance may seen somewhat unnatural. The main reason for introducing it is that it results in a quite satisfactory theory of factor monoids with respect to a submonoid.

Definition 5: Let $N < M \in \mathcal{M}$. Then $\sim(N)$ is the binary relation in M defined by $x \sim y\ (N)$ if and only if there exist $n, n' \in N$ such that $xn = yn'$. //

Proposition 1: Let $N < M \in \mathcal{M}$.

Then $\sim(N)$ is a congruence relation. //

Proof: That the relation is reflexive and symmetric is clear. Also, $x \sim y\ (N)$, $y \sim z\ (N)$ implies there exist $n, n', q, q' \in N$ such that $xn = yn'$, $yq = zq'$, and so $xnq = yn'q$, $yqn' = zq'n'$, $n,q,n',q' \in N$. Thus, $x(nq) = z(q'n')$, $nq, q'n' \in N$, whence $x \sim z(N)$. It follows that $\sim(N)$ is an equivalence relation.

Moreover, $x \sim y\ (N)$, $a \sim b\ (N)$ implies there exist $n, n', q, q' \in N$ such that $xn = yn'$, $aq = bq'$. Thus $(xa)(nq) = (yb)(n'q')$, $nq, n'q' \in N$, and so $xa \sim yb\ (N)$. //

Corollary: Let $N < M \in \mathcal{A}$.

Then $M/\sim(N) \in \mathcal{A}$, whose identity is the congruence class containing 1.

Proof: Clear. //

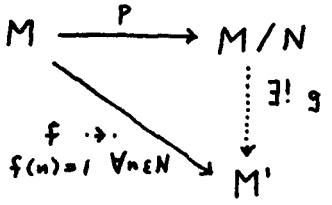
Notation: Let $N < M \in \mathcal{A}$. Then $M/\sim(N)$ is denoted M/N. //

Theorem 1: Let $N < M \in \mathcal{A}$.

Let $p: M \longrightarrow M/N$ by $m \longmapsto \bar{m}$, where $\bar{m}$ is the congruence class containing m. Let $M' \in \mathcal{A}$. Let $f: M \longrightarrow M'$ be a morphism of monoids such that $f(n) = 1$ for any $n \in N$.

Then there exists a unique $g: M/N \longrightarrow M'$ such that $f = g \circ p$.

(Illustration:



)

Proof: The uniqueness of g is clear, as p is onto.

Indeed, the only possible candidate for g is given by $p(m) \longmapsto f(m)$ for any $m \in M$. All we have to do is check that this is well-defined. Now, $p(x) = p(y)$ implies there exist $n, n' \in N$ such that $xn = yn'$, whence $f(x)\,f(n) = f(y)\,f(n')$, $f(n) = f(n') = 1$, and so $f(x) = f(y)$. //

Proposition 2: Let $M \in \mathcal{A}$. Let N be a subgroup of M (i.e. $N < M$, $N \in \mathcal{A}$ b). Let $x, y \in M$.

Then $x \sim y\ (N)$ if and only if $xN = yN$.

Proof: $\Rightarrow$): $x \sim y$ (N) implies there exist $n, n' \in N$ such that $xn = yn'$, whence $xnN = yn'N$, $n, n' \in N$, and so $xN = yN$.

$\Leftarrow$): $xN = yN$ implies $x \cdot 1 = y \cdot n$, $1, n \in N$. Then $x \sim y$ (N) follows, and we are done. //

§ 2: Connected Submonoids

Definition 6: Let $N < M \in \mathcal{M}$. We say that N is a connected submonoid of M, denoted $N \not\subset M$, if and only if $n, nx \in N$ implies $x \in N$. //

We note that this concept goes by at least two other designations in the literature. In [9], N is called closed; while in [10], N is said to have the isolation property. The fact that the nomenclature has yet to be standardized is what prompts us not to hesitate in using our own. It was felt that the condition $n, nx \in N$ implies $x \in N$ suggested connectedness more than isolation, as an intuitive concept; while "closed" seemed somehow too strong.

Perhaps the most immediate motivation for considering connected submonoids is the following observation.

Proposition 3: Let $N < M \in \mathcal{M}$.

Then $N \not\subset M$ if and only if there exists $f: M \longrightarrow M'$ a morphism of monoids such that $N = \text{Ker } f = \{ m \in M \mid f(m) = 1 \}$.

Proof: $\Leftarrow$): Let $f: M \longrightarrow M'$ be a monoid homomorphism such that $N = \text{Ker } f$. Then $n, nx \in N$ implies $f(n) = f(nx) = 1$; that is,

$f(n) = 1$, $f(n)\,f(x) = 1$, whence $f(x) = 1$, and so $x \in N$. Thus, $N \not< M$.

$\Longrightarrow$): Let $N \not< M$. Let $f: M \longrightarrow M/N$ be the natural map. Now, $n \in N$ implies $n \cdot 1 = 1 \cdot n$, $1, n \in N$, and so $n \sim 1\ (N)$. Then $n \in \operatorname{Ker} f$ is clear. Also, $n \in \operatorname{Ker} f$ implies $f(n) = 1$, whence there exist $x, y \in N$ such that $nx = 1y$. Then $x, nx \in N$, and $n \in N$ follows. Thus, $N = \operatorname{Ker} f$. //

Corollary: Let $N < M \in \mathcal{M}$.

Let $f: M \longrightarrow M/N$ be the natural map.

Then $N \not< M$ if and only if $N = \operatorname{Ker} f$.

Proof: Clear. //

Theorem 2: Let $N \not< M \in \mathcal{M}$.

Then the following are equivalent:

1. M/N is a group.
2. For each $x \in M$, there exists $y \in M$ such that $xy \in N$.

Proof: Let $p: M \longrightarrow M/N$ be the natural map.

1 $\Longrightarrow$ 2): Let $x \in M$. As M/N is a group, we know there exists $y \in M$ such that $p(x)\,p(y) = 1$. Then we have $p(xy) = p(1)$; and so there exist $n, n' \in N$ such that $xyn = n'$, which implies $n, nxy \in N$, whence $xy \in N$.

2 $\Longrightarrow$ 1): Let $p(x) \in M/N$. Then there exists $y \in M$ such that $xy \in N$. It follows that $p(xy) = p(1)$; thus $p(y)$ is the inverse of $p(x)$. //

Example: Let $n \in \mathbb{N}$. Then $\mathbb{N}_0 / \langle n \rangle$ is a cyclic group of order n. //

Example: Let $n \in \mathbb{N}$, $n > 1$. Let $P = \{ x^n \mid x \in \mathbb{N} \}$. Then $\mathbb{N}/P$ is an infinite group such that every element has order a factor of n. //

Proposition 4: Let $M \in \mathcal{M}$. Let N be a subgroup of M. Then $N \not\subset M$.

Proof: Let $n, nx \in N$. Then $n^{-1}, nx \in N$, and so $n^{-1}nx \in N$; thus $x \in N$. //

Proposition 5: Let $M \in \mathcal{M}b$. Then $N \not\subset M$ if and only if N is a subgroup of M.

Proof: $\Rightarrow$): $x \in N$ implies $x, xx^{-1} \in N$, which implies $x^{-1} \in N$.

$\Leftarrow$): Proposition 4. //

Definition 7: Let $M \in \mathcal{M}$. Then $M^* = \{ x \in M \mid \exists\, y \in M \cdot\cdot\cdot xy = 1 \}$. The elements of M^* are called the units of M. If $M^* = \{1\}$, then we say that M is rigid. //

Remarks: 1. M^* is a subgroup of M, and contains every subgroup of M.

2. M/M^* is rigid. //

Lemma 1: Let $1 \neq a \in M \in \mathcal{M}$ such that $1, a, a^2, a^3, \ldots$ are not all distinct. Then there exist $r, m \in \mathbb{N}$ such that $1, a, a^2, \ldots a^{r+m-1}$ are distinct but $a^{r+m} = a^r$. Moreover, there exists a unique $n \in \mathbb{N}$ such that $r \leq n \leq r + m - 1$, m divides n and a^n is an idempotent.

Proof: See Clifford and Preston [3; Theorem 1.9, p. 20]. //

Theorem 3: Let $M \in \mathcal{O}$.

Then the following are equivalent:

1. $N \not\subset M \Longrightarrow N = M$ or $N = \{1\}$.
2. M satisfies one of the following:
   - i $M = \{1\}$.
   - ii M is a cyclic group of prime order.
   - iii There exists $\theta \in M$ such that $\theta \neq 1$, $x\theta = \theta$ for any $x \in M$; and for each $a \in M$ such that $a \neq 1$, there exists $n(a) \in \mathbb{N}$ such that $a^{n(a)} = \theta$.

Proof: $2 \Rightarrow 1$): i Trivial

ii $N \not\subset M$ implies N is a subgroup of M, and so $N = \{1\}$ or $N = M$.

iii Let $\{1\} \neq N \not\subset M$. Then, there exists $a \in N$ such that $a \neq 1$, and so $\theta = a^{n(a)} \in N$. Thus, θ, $\theta x \in N$ for any $x \in M$, which implies $x \in N$ for any $x \in M$. Hence $N = M$.

$1 \Rightarrow 2$): Assume $M \neq \{1\}$.

As $M^* \not\subset M$, we know $M^* = \{1\}$ or $M^* = M$. If $M^* = M$, then $N \not\subset M$ if and only if N is a subgroup of M. It follows that M has no non-trivial subgroups, and so M is a cyclic group of prime order.

Assume $M^* \neq M$; i.e. $M^* = \{1\}$.

For each $u \in M$, define

$$T(u) = \{ x \in M \mid \exists\ p, q \in \mathbb{N}_0 \cdot\ u^p x = u^q \}.$$

Clearly $1 \in T(u)$. Also, $x, y \in T(u)$ implies there exist $p, q, r, s \in \mathbb{N}_0$ such that $u^p x = u^q$, $u^r y = u^s$; whence $u^{p+r}xy = u^{q+s}$, $p+r, q+s \in \mathbb{N}_0$; it follows that $xy \in T(u)$. Moreover, $x, xy \in T(u)$ implies there exist

$p, q, r, s \in \mathbb{N}_0$ such that $u^p x = u^q$, $u^r xy = u^s$. We then see that $u^{p+r}x = u^{q+r}$, $u^{p+r}xy = u^{p+s}$, and so $u^{q+r}y = u^{p+s}$; hence $y \in T(u)$. Thus, $T(u) \supset M$ for any $u \in M$. So we have that $1 \neq u \in M$ implies $T(u) = M$ (as $u \in T(u)$).

Let $1 \neq a \in M$. Now $M^* = \{1\}$; so $a^2 \neq 1$. Thus, $T(a^2) = M$ and hence $a \in T(a^2)$. It follows that there exist $p, q \in \mathbb{N}_0$ such that $a^{2p}a = a^{2q}$; that is, $a^{2p+1} = a^{2q}$, $p, q \in \mathbb{N}_0$. Thus, $1, a, a^2, \ldots$ are not all distinct and $a \neq 1$. Hence, there exists $n(a) \in \mathbb{N}$ such that $a^{n(a)}$ is an idempotent, (Lemma 1). Moreover, $a^{n(a)} \neq 1$.

Thus, $M = T(a^{n(a)})$

$$= \{x \in M \mid \exists\ p, q \in \mathbb{N}_0 \ni a^{n(a)p}x = a^{n(a)q}\}$$

$$= \{x \in M \mid a^{n(a)}x = a^{n(a)}\};$$

i.e. $a^{n(a)}x = a^{n(a)}$ for any $x \in M$.

Now this is true for any $1 \neq a \in M$. As $a, b \in M \setminus \{1\}$ implies $a^{n(a)} = a^{n(a)}b^{n(b)} = b^{n(b)}$, define $\theta = x^{n(x)}\ \forall\ x \in M \setminus \{1\}$. It is then readily seen that θ has all the desired properties. //

Corollary: Let $M \in \mathcal{A}$.

Then the following are equivalent:

1. $N < M$ implies $N = \{1\}$ or $N = M$.
2. M satisfies one of the following:
   - i $M = \{1\}$.
   - ii M is a cyclic group of prime order.
   - iii $M = \{1, e\}$, $e^2 = e \neq 1$.

Proof: $2 \Rightarrow 1$): Clear.

1 $\Longrightarrow$ 2): Now, $N \not\subset M$ implies $N < M$ which implies $N = \{1\}$ or $N = M$. Thus, by the theorem, $M = \{1\}$, or M is a cyclic group of prime order, or there exists $\theta \in M$ such that $\theta \neq 1$, $x\theta = \theta$ for any $x \in M$, and for each $1 \neq a \in M$ there exists $n(a) \in \mathbb{N}$ such that $a^{n(a)} = \theta$.

Assume $M \neq \{1\}$ and M is not a cyclic group of prime order. Then $\{1, \theta\} < M$. Hence, $M = \{1, \theta\}$. //

Let $M \in \mathcal{M}$. Let $(N_i)_{i \in I}$ be a family of connected submonoids of M. It is easily seen that $\bigcap_{i \in I} N_i \not\subset M$. Thus, we can make the following definition.

Definition 8: Let $N \subseteq M \in \mathcal{M}$. Then the connected cover of N, denoted con N, is given by $\bigcap \gamma$, where $\gamma = \{S \not\subset M \mid N \subseteq S\}$. //

Proposition 6: Let $N < M \in \mathcal{M}$.

Then con $N = \{y \in M \mid \exists\, x \in N \cdot\!\!\rightarrow\!\cdot\, xy \in N\}$.

Proof: Let $A = \{y \in M \mid \exists\, x \in N \cdot\!\!\rightarrow\!\cdot\, xy \in N\}$. Clearly, $A \subseteq$ con N. Now, $1 \in A$ is clear. Let $y, y' \in A$. Then there exist $x, x' \in N$ such that $xy, x'y' \in N$, which implies $(xx')(yy') \in N$, $xx' \in N$; thus $yy' \in A$.

Also, let $y, yy' \in A$. Then there exist $x, x' \in N$ such that $xy, x'yy' \in N$; that is, $x(x'yy'), xy \in N$. It follows that $[x'(xy)]y' \in N$, $x'(xy) \in N$, whence $y' \in A$. Thus, $A \not\subset M$. Also, $n \in N$ implies $1n, 1 \in N$, which implies $n \in A$. Hence, $N \subseteq A \not\subset M$.

Thus, con $N = A$. //

§ 3: Normally Connected Submonoids

Notation: The class of all abelian monoids M such that $x^2 = x$ implies $x = 1$, is denoted $\mathcal{J}$. //

Clearly, $\mathcal{A}b \subseteq \mathcal{J} \subseteq \mathcal{A}$.

Definition 9: Let $N < M \in \mathcal{A}$. We say that N is a normally connected submonoid of M, denoted $N \Delta M$, if and only if $a, b \in N$, $ax^2 = bx$ implies $x \in N$. //

The motivation for considering normally connected submonoids is contained in the following.

Proposition 7: Let $N < M \in \mathcal{A}$.

Then $N \Delta M$ if and only if there exists $f: M \longrightarrow M'$, $M' \in \mathcal{J}$, such that f is a monoid homomorphism and $N = \operatorname{Ker} f$.

Proof: $\Longleftarrow$): It is clear that $\operatorname{Ker} f < M$.

Let $a, b \in \operatorname{Ker} f$, $x \in M$ such that $ax^2 = bx$. Then $f(a) f(x)^2 = f(b) f(x)$, $a, b \in \operatorname{Ker} f$. Clearly, $f(x)^2 = f(x) \in M' \in \mathcal{J}$, whence $f(x) = 1$, which implies $x \in \operatorname{Ker} f$.

Thus, $\operatorname{Ker} f \Delta M$.

$\Longrightarrow$): Let $N \Delta M$. Let $f: M \longrightarrow M/N$ be the natural map. Then $N \Delta M$ implies that $n, nx \in N \Rightarrow nx^2 = (nx)x$, $n, nx \in N \Rightarrow x \in N$. Thus $N \not< M$, and so $\operatorname{Ker} f = N$. //

Corollary: Let $N \Delta M \in \mathcal{A}$.

Then $N \not< M$.

Proof: Contained in the proof of the proposition. //

Let $M \in \mathcal{A}$. Let $(N_i)_{i \in I}$ be a family of normally connected submonoids of M. Then it is easily seen that $\bigcap_{i \in I} N_i \Delta M$.

Definition 10: Let $N \subseteq M \in \mathcal{A}$. Then the normally connected cover of N, denoted $\overline{\text{con}}\ N$, is given by $\bigcap \gamma$, where $\gamma = \{ S \Delta M \mid N \subseteq S \}$. //

Proposition 8: Let $N < M \in \mathcal{A}$.

Let $D = \{ d \in M \mid \exists\ n \in N \cdot\ni\cdot d^2 = nd \}$.

Then $\overline{\text{con}}\ N = \text{con}\ D$.

Proof: It is clear that $N < D < \text{con}\ D < \overline{\text{con}}\ N$. Thus, it remains only to show that $\text{con}\ D \Delta M$.

Let $k_1, k_2 \in \text{con}\ D$, $x \in M$ such that $k_1 x^2 = k_2 x$. Since $k_1, k_2 \in \text{con}\ D$, we have there exist $d_1, d_2 \in D$ such that $k_1 d_1, k_2 d_2 \in D$. Therefore $d_1 d_2 k_1 x^2 = d_1 d_2 k_2 x$ which implies $[(d_1 k_1)\ d_2]\ x^2 = [(d_2 k_2)\ d_1]\ x$. That is, there exist $d_3, d_4 \in D$ such that $d_3 x^2 = d_4 x$.

Now there exist $n_3, n_4 \in N$ such that $d_3^2 = n_3 d_3$, $d_4^2 = n_4 d_4$. Thus, $d_3 x^2 = d_4 x$

$$\Rightarrow d_4^2 d_3^2 x^2 = d_4^2 d_3 d_4 x$$

$$\Rightarrow (d_4 d_3 x)^2 = n_4 d_4 d_3 d_4 x$$

$$= n_4 d_4^2 d_3 x$$

$$\Rightarrow (d_4 d_3 x)^2 = n_4^2 (d_4 d_3 x),\ n_4^2 \in N$$

$\Rightarrow d_4 d_3 x \in D,\ d_4 d_3 \in D$

$\Rightarrow x \in \text{con } D.$

Hence, $\text{con } D \Delta M.$ //

Theorem 4: Let $M \in \mathcal{J}$.

Then the following are equivalent:

1. $N \Delta M$ implies $N = \{1\}$ or $N = M$
2. $N \not\subset M$ implies $N = \{1\}$ or $N = M$
3. $N < M$ implies $N = \{1\}$ or $N = M$
4. Either $M = \{1\}$ or M is a cyclic group of prime order.

Proof: $4 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1)$: Clear.

$1 \Rightarrow 4)$: Let $a \in M$ and assume $a^2 \neq 1$. Then $\overline{\text{con}} < a^2 > = M$, and so $M = \text{con } D$, where $D = \{d \in M \mid \exists\ r \in \mathbb{N}_o \cdot\cdot d^2 = a^{2r} d\}$. In particular, $a \in \text{con } D$ and so there exists $d \in D$ such that $ad \in D$, whence there exist $r, s \in \mathbb{N}_o$ with $d^2 = a^{2r} d$, $(ad)^2 = a^{2s} (ad)$. It follows easily that $a^{2r+2} d = a^{2s+1} d$.

Let $m = |(2r + 2) - (2s + 1)|$, and note that $m \neq 0$. It is not difficult to show that $a^u d = a^{u+mx} d$ for any $x \in \mathbb{N}_o$ and for any $u \in \mathbb{N}_o$ with $u \geq \min\{2r + 2, 2s + 1\}$.

Now, let $t \in \mathbb{N}_o$ such that $t \geq \min\{2r + 2, 2s + 1\}$ and $t \equiv -2r \pmod m$. Then $t \equiv 2t + 2r \pmod m$, and so $2t + 2r = t + mx$, for some $x \in \mathbb{N}_o$. We can then argue that $(a^t d)^2 = a^{2t} d^2 = a^{2t} a^{2r} d = a^{2t+2r} d = a^{t+mx} d = a^t d$. It follows that $a^t d = 1$, and so $a \in M^*$.

Thus, $a^2 \neq 1 \Rightarrow a \in M^*$ and hence M is a group. Now it is

easy to see that every subgroup of an abelian group is normally connected, and so M is a group with no non-trivial subgroups. The result follows. //

Lemma 2: Let M be an abelian monoid such that for any $a, b, x \in M$, $ax^2 = bx$ implies there exists $n \in \mathbb{N}$ such that $(ax)^n = b^n$.

Then every connected submonoid of M is normally connected.

Proof: Let $N \not< M$. Let $x \in M$, $a, b \in N$ such that $ax^2 = bx$. Then there exists $n \in \mathbb{N}$ such that $(ax)^n = b^n$, whence $a^n x^n = b^n$ $(a^n, b^n \in N)$, and so $x^n \in N$.

If $n = 1$, we are done. If $n \neq 1$, then $n \geq 2$ and so $ax^n = ax^2x^{n-2} = bxx^{n-2} = bx^{n-1}$ $(ax^n, b \in N)$, whence $x^{n-1} \in N$. By repeating this, we see that $x \in N$. //

Proposition 9: Let $M \in \mathcal{O}$.

Then the following are equivalent:

1. $N \not< M$ implies $N \Delta M$.
2. $y^2 = cy$ implies there exists $n \in \mathbb{N}$ such that $y^n = c^n$, $\forall\ y, c \in M$.
3. $ax^2 = bx$ implies there exists $n \in \mathbb{N}$ such that $(ax)^n = b^n$, $\forall\ a, b, x \in M$.

Proof: 1 $\Rightarrow$ 2): Let $y, c \in M$ such that $y^2 = cy$. Then $y \in \overline{\text{con}}$ $< c > = \text{con} < c >$ and so there exist $s, u \in \mathbb{N}_o$ such that $c^s y = c^u$. Using induction and the fact that $y^2 = cy$, it is easy to show that $y^{r+1} = c^r y$ for any $r \in \mathbb{N}_o$. It follows that

$c^u = y^{s+1}$, and hence that $c^{2u} = (c^u)^2 = (y^{s+1})^2 = (y^2)^{s+1} = c^{u+s+1}$.

If $2u = u + s + 1$, then $u = s + 1$, and so $c^{s+1} = y^{s+1}$, $s + 1 \in \mathbb{N}_0$. If $2u \neq u + s + 1$, then $1, c, c^2, c^3, \ldots$ are not all distinct, and so $c^u \in M^*$. It follows that $y^{s+1} \in M^*$, and then $y \in M^*$, whence $y = c$. In either case, the implication is established.

2 $\Rightarrow$ 3): Let $a, b, x \in M$ such that $ax^2 = bx$. Then $b^2a^2x^2 = b^2abx$, and so $(abx)^2 = b^2(abx)$. By (2), there exists $u \in \mathbb{N}$ with $(abx)^u = (b^2)^u$, whence $(b^u)^2 = (a^ux^u)b^u$. Again, there exists $v \in \mathbb{N}$ with $(b^u)^v = (a^ux^u)^v$; hence, the result follows by taking $n = uv$.

3 $\Rightarrow$ 1): Lemma 2. //

<u>Proposition 10</u>: Let $M \in \mathcal{J}$. Then the following are equivalent:

1. $N < M \Rightarrow N \not\cong M$.
2. M is a torsion group.

<u>Proof</u>: 2 $\Rightarrow$ 1): Assume M is a torsion group. Let $N < M$. Let $n \in N$. Now there exists $x \in \mathbb{N}$ such that $n^x = 1$. If $x = 1$, then $n = 1$ which implies $n^{-1} \in N$. If $x > 1$, then $n\,n^{x-1} = 1$ which implies $n^{-1} = n^{x-1} \in N$. Thus N is a subgroup of M, and so $N \not\cong M$.

$1 \Longrightarrow 2)$: Let $a \in M$.

Suppose $1, a, a^2, a^3 \ldots$ are all distinct. As $\{1, a^2, a^3, a^4 \ldots\} < 1$, we have $\{1, a^2, a^3, \ldots\} \not\ni M$. But $a^2, a^2 a \in \{1, a^2 a^3, \ldots\}$, which implies $a \in \{1, a^2, a^3, a^4, \ldots\}$: -- contradiction.

Thus, $1, a, a^2, a^3, \ldots$ are not all distinct, whence there exists $n \in \mathbb{N}$ such that a^n is an idempotent, and so there exists $n \in \mathbb{N}$ such that $a^n = 1$.

It follows that M is a torsion group. //

Corollary: Let $M \in \mathcal{A}b$.

Then the following are equivalent:

1. Every submonoid of M is a subgroup of M.
2. M is a torsion group.

Proof: Clear. //

§ 4: Saturated Submonoids, and Localization

Definition 11: Let $N < M \in \mathcal{M}$. We say N is a saturated submonoid of M if and only if $xy \in N$ implies $x, y \in N$, for any $x, y \in M$. //

Let $M \in \mathcal{M}$. Let $(N_i)_{i \in I}$ be a family of saturated submonoids of M. Then $\bigcap_{i \in I} N_i$ is a saturated submonoid of M.

Definition 12: Let $N \subseteq M \in \mathcal{A}$. Then the saturated cover (or saturation) of N, denoted sat S, is given by $\bigcap \mathcal{S}$, where $\mathcal{S} = \{ S < M \mid N \subseteq S, \ S \text{ a saturated submonoid of } M \}$. //

Proposition 11: Let $S < M \in \mathcal{A}$.

Then $\text{sat } S = \{ x \in M \mid \exists\, y \in M \cdot\!\!\cdot\, xy \in S \}$.

Proof: Let $T = \{ x \in M \mid \exists\, y \in M \cdot\!\!\cdot\, xy \in S \}$. Clearly $T \subseteq \text{sat } S$.

Now, $x \in S$ implies $x1 \in S$, and so $x \in T$. Thus, $S \subseteq T$.

Also, $x, x' \in T$ implies there exist $y, y' \in M$ such that $xy, x'y' \in S$, whence $(xx')(yy') \in S$, and so $xx' \in T$. Moreover, $xy \in T$ implies there exists $z \in M$ such that $xyz \in S$, and so $x, y \in T$. Hence, T is a saturated submonoid of M.

Thus, $\text{sat } S = T$. //

Definition 13: Let $\emptyset \neq I \subseteq M \in \mathcal{A}$. Then I is called an ideal of M if and only if $IM \subseteq I$. If, moreover, $ab \in I$ implies $a \in I$ or $b \in I$ for any $a, b \in M$, then I is called a prime ideal. //

Proposition 12: Let $\emptyset \neq S \subsetneq M \in \mathcal{A}$.

Then the following are equivalent:

1. S is a saturated submonoid of M.
2. M\S is a prime ideal of M.

Proof: 1 $\Longrightarrow$ 2): Let $i \in M\backslash S$, $m \in M$. Suppose $im \in S$. Then $i \in S$, -- contradiction. Thus, $(M\backslash S)M \subseteq M\backslash S$.

Also, $ab \in M\backslash S$ implies $a \in M\backslash S$ or

$b \in M\backslash S$, for $a, b \notin M\backslash S$ implies $ab \in S$.

Hence, $M\backslash S$ is a prime ideal of M.

2 $\Longrightarrow$ 1): It is easily seen that $1 \in S$. Let $a, b \in S$. If $ab \notin S$, then $a \in M\backslash S$ or $b \in M\backslash S$; --contradiction. Thus, $a, b \in S$ implies $ab \in S$. Also, let $xy \in S$. Suppose $x \notin S$ or $y \notin S$. Then $xy \in M\backslash S$; -- contradiction. Hence, $\text{sat } S = S < M$. //

Definition 14: Let $M \in \mathcal{O}$. Then the cancellative part of M, denoted $C(M)$, is $\{c \in M \mid cx = cy \Rightarrow x = y\}$. If $C(M) = M$, then we say M is cancellative. The class of all cancellative monoids is denoted $\mathcal{L}$. //

It is clear that $\mathcal{A}b \subseteq \mathcal{L} \subseteq \mathcal{J} \subseteq \mathcal{O}$. //

Proposition 13: Let $M \in \mathcal{O}$.

Then:

1. $C(M)$ is a saturated submonoid of M.
2. M^* is a saturated submonoid of M.
3. If S is a saturated submonoid of M, then $M^* < S \not< M$.

Proof: 1. Clearly $1 \in C(M)$.

Now, $c, c' \in C(M) \Rightarrow (cx = cy \Rightarrow x = y;\ c'x = c'y \Rightarrow x = y)$

$\Rightarrow (cc'x = cc'y \Rightarrow c'x = c'y \Rightarrow x = y)$

$\Rightarrow cc' \in C(M)$.

Also, let $cc' \in C(M)$. Then $c'x = c'y \Rightarrow cc'x = cc'y \Rightarrow x = y$, and so $c' \in C(M)$. Hence, $C(M)$ is a saturated submonoid of M.

2. Clearly, $M^* < M$. Also, $ab \in M^*$ implies there exists $u \in M$ such that $abu = 1$, which implies $a, b \in M^*$. Thus M^* is a saturated submonoid of M.

3. Let S be a saturated submonoid of M. Now, $1 \in S$. Thus, $u \in M^*$ implies there exists $v \in M$ such that $u \cdot v = 1$, whence $u \in S$. Hence, $M^* < S$. Also, $n, nx \in S \Rightarrow nx \in S \Rightarrow x \in S$. //

The concept of localization in commutative rings with unit is well established, as, for example, in Lang [6; II, § 3].

The purpose of the remainder of this section is to parallel this development in abelian monoids. It will be seen that a more natural setting for a theory of localization is that of abelian monoids.

Definition 15: Let $S < M \in \mathcal{A}$. Let $M \oplus S = \{(m, s) \mid m \in M, S \in S\}$ be considered as a monoid under componentwise multiplication. Then $\equiv (S)$ is a binary relation on $M \oplus S$ given by $(a, b) \equiv (x, y)\ (S)$ if and only if there exists $s \in S$ such that $ays = bxs$. //

Proposition 14: Let $S < M \in \mathcal{A}$.

Then $\equiv (S)$ is a congruence relation.

Proof: $(a, b) \equiv (a, b)\ (S)$, as $abl = bal$, $1 \in S$. That $(a, b) \equiv (x, y)\ (S)$ implies $(x, y) \equiv (a, b)\ (S)$, is clear.

Also $(a, b) \equiv (x, y)\ (S)$, $(x, y) \equiv (u, v)\ (S)$ implies there exist $s, t \in S$ such that $ays = bxs$, $xvt = yut$. We then have $aysvt = bxsvt = bsyut$, $b, y, v, s, t \in S$, whence $(av)(yst) = (bu)(yst)$, $yst \in S$, and so $(a, b) \equiv (u, v)\ (S)$. Thus, $\equiv (S)$ is an equivalence relation.

Moreover, $(a, b) \equiv (x, y)\ (S)$, $(a', b') \equiv (x', y')\ (S)$ implies there exist $s, s' \in S$ such that $ays = bxs$, $a'y's' = b'x's'$. Then we have $(aa')(yy')(ss') = (bb')(xx')(ss')$, $ss' \in S$, whence $(aa', bb') \equiv (xx', yy')\ (S)$, and finally $(a, b)(a', b') \equiv (x, y)(x', y')\ (S)$. //

Definition 16: Let $S < M \in \mathcal{A}$. Then $(M \oplus S) / \equiv (S)$ is called the localization of M at S, and is denoted $S^{-1}M$. Also, the congruence class containing (m, s) is denoted m/s. //

Proposition 15: Let $S < M \in \mathcal{A}$.

Let $\varphi : M \longrightarrow S^{-1}M$ by $m \longmapsto m/1$.

Then φ is 1 - 1 if and only if $S < C(M)$.

Proof: $\Longrightarrow$): Assume φ is 1 - 1. Let $s \in S$, $x, y \in M$ such that $sx = sy$. Then $xs/s = ys/s$, $s \in S$, which implies $x/1 = y/1$. It follows that $\varphi(x) = \varphi(y)$, and so $x = y$.

$\Longleftarrow$): Assume $S < C(M)$. Then $\varphi(x) = \varphi(y)$ implies $x/1 = y/1$, which implies there exists $s \in S$ such that $sx = sy$; so $x = y$. //

Proposition 16: Let $S < M \in \mathcal{A}$.

Let $a/b \in S^{-1}M$.

Then $a/b \in (S^{-1}M)^*$ if and only if $a \in \text{sat } S$.

Proof: $\Rightarrow$): $a/b \in (S^{-1}M)^* \Rightarrow \exists\ c/d \in S^{-1}M$ such that $ac/bd = 1/1$

$\Rightarrow \exists\ s \in S$ such that $acs = bds$

$\Rightarrow acs \in S$

$\Rightarrow a \in \text{sat } S$.

$\Leftarrow$): $a \in \text{sat } S \Rightarrow \exists\, x \in M$ such that $ax \in S$

$\Rightarrow (a/b)(bx/ax) = 1/1,\ bx/ax \in S^{-1}M$

$\Rightarrow a/b \in (S^{-1}M)^*$. //

Corollary: Let $S < M \in \mathcal{O}$ such that $S^{-1}M = \{1\}$.

Then sat $S = M$.

Proof: $m \in M \Rightarrow m/1 \in S^{-1}M \Rightarrow m/1 \in (S^{-1}M)^* \Rightarrow m \in \text{sat } S$. //

Proposition 17: Let $S < M \in \mathcal{O}$.

Then $S^{-1}M = (\text{sat } S)^{-1} M$.

Proof: Let $(a, b), (x, y) \in M \oplus S$.

Now, $(a, b) \equiv (x, y)\ (S)$ implies there exists $s \in S \subseteq \text{sat } S$ such that $ays = bxs$ which implies $(a, b) \equiv (x, y)\ (\text{sat } S)$.

Also, $(a,b) \equiv (x, y)\ (\text{sat } S)$ implies there exists $s \in \text{sat } S$ such that $ays = bxs$ which implies there exist $s, t \in M$ such that $ayst = bxst$, $st \in S$, and so $(a, b) \equiv (x, y)\ (S)$.

Thus, $\equiv (S)$ and $\equiv (\text{sat } S)$ are the same relation. Hence, $S^{-1}M = (\text{sat } S)^{-1}M$. //

Proposition 18: Let $S < M \in \mathcal{O}$.

Then there is a biunique correspondence between the set of all prime ideals of $S^{-1}M$ and the set of all those prime ideals of M which are disjoint from S.

Proof: See Maury [7: p. 54-57]. //

Notation: Let $f: A \longrightarrow B$. Then $f_*(A) = \{f(a) \in B \mid a \in A\}$. //

Proposition 19: Let $S < M \in \mathcal{M}$.

Let $\varphi : M \longrightarrow S^{-1}M$ by $m \longmapsto m/1$.

Then: 1. $\varphi_*(S) \subseteq (S^{-1}M)^*$

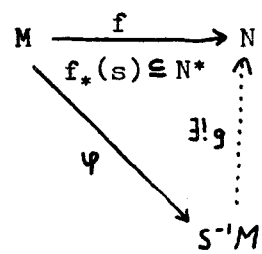
2. If $f: M \longrightarrow N$ is a monoid homomorphism such that $f_*(S) \subseteq N^*$, then there exists a unique $g: S^{-1}M \longrightarrow N$ such that $f = g \circ \varphi$.

Proof: 1. $s \in S \Rightarrow 1/s \in S^{-1}M$

$\Rightarrow (1/s)\,\varphi(s) = 1$

$\Rightarrow \varphi(s) \in (S^{-1}M)^*$

2. Let $g: S^{-1}M \longrightarrow N$ by $m/s \longmapsto f(m)f(s)^{-1}$.



To check that g is well-defined, we note that $m/s = n/t$ implies there exists $u \in S$ such that $mtu = snu$ which implies $f(m)f(t)f(u) = f(s)f(n)f(u)$, $f(s), f(t), f(u) \in N^*$ and so $f(m)f(s)^{-1} = f(n)f(t)^{-1}$.

Then $(g \circ \varphi)(m) = g(m/1) = f(m)$, for any $m \in M$ which implies $g \circ \varphi = f$.

Thus, we need only show that g is unique. Let $g': S^{-1}M \longrightarrow N$ such that $g' \circ \varphi = f$. Then $g'(m/1) = f(m) = g(m/1)$ for any $m \in M$. For each $s \in S$, $1 = g'\left(\frac{s}{1} \cdot \frac{1}{s}\right) = f(s)\, g'(1/s)$ which implies $g'(1/s) = f(s)^{-1}$. Thus, $g'(m/s) = g'(m/1)\, g'(1/s) = f(m)\, f(s)^{-1} = g(m/s)$. Hence, $g' = g$. //

CHAPTER II

LATTICE CONSIDERATIONS

Throughout this chapter, the lattice of submonoids of an abelian monoid M will be denoted $\mathfrak{L}(M)$.

Definition 1: An abelian group G is called locally cyclic if and only if for any finite subset S of G, the subgroup of G generated by S is cyclic. //

Definition 2: Let L be a lattice.

Then: 1. Let $x, y \in L$. We say x covers y, denoted $x \downarrow y$, if and only if $x > y$ and $x \geq a \geq y$ implies $a = x$ or $a = y$.

2. We say L is semi-modular if and only if for each $x, y \in L$, $x \downarrow x \wedge y$, $y \downarrow x \wedge y$ implies $x \vee y \downarrow x$, $x \vee y \downarrow y$. //

The reader is assumed to be familiar with the concepts of modular lattice and distributive lattice.

Lemma 1: Let G be an abelian group.

Then the lattice of subgroups of G is modular.

Proof: See Birkhoff [1; p. 65]. //

Lemma 2: Let G be an abelian group.

Then the following are equivalent:

1. the lattice of subgroups of G is distributive.
2. G is locally cyclic.

Proof: See Birkhoff [1; p. 96]. //

Theorem 1: Let $M \in \mathcal{S}$.

Then the following are equivalent:

1. $\mathbb{L}(M)$ is modular.
2. $\mathbb{L}(M)$ is semi-modular.
3. M is a torsion group.

Proof: 1 $\Longrightarrow$ 2): True for any lattice.

2 $\Longrightarrow$ 3): Let $a \in M$.

Suppose $1, a, a^2, a^3, \ldots$ are all distinct. Let $X = \{1, a^2, a^4, a^6, a^7, a^8, a^9, \ldots\}$ and $Y = \{1, a^3, a^4, a^6, a^7, a^8, a^9, \ldots\}$. Clearly $X, Y \in \mathbb{L}(M)$. Now, $X \wedge Y = \{1, a^4, a^6, a^7, a^8, a^9, \ldots\}$ and $X \vee Y = \{1, a^2, a^3, a^4, a^5, \ldots\}$. It is then evident that X covers $X \wedge Y$ and that Y covers $X \wedge Y$. However, $X \vee Y$ does not cover X, for $X \lneq \{1, a^2, a^4, a^5, a^6, \ldots\} \lneq X \vee Y$. Hence, $\mathbb{L}(M)$ is not semi-modular and we have a contradiction.

Since $1, a, a^2, \ldots$ are not all distinct, and $M \in \mathcal{S}$, it follows that there exists $n \in \mathbb{N}$ such that $a^n = 1$ (Chapter 1, Lemma 1, page 7). Hence, M is a torsion group.

3 $\Longrightarrow$ 1): Since M is a torsion group, it follows that $\mathbb{L}(M)$ is the lattice of subgroups of M (Chapter 1, Proposition 10, Corollary) and hence must be modular (Lemma 1). //

Corollary: Let $M \in \mathcal{J}$.

The the following are equivalent:

1. $\mathbb{L}(M)$ is distributive.
2. M is a locally cyclic torsion group.

Proof: 1 $\Rightarrow$ 2): $\mathbb{L}(M)$ distributive implies $\mathbb{L}(M)$ modular, and so, by the theorem, M is a torsion group. Thus M is a group whose lattice of subgroups is distributive, and hence M is locally cyclic.

2 $\Rightarrow$ 1): Clear from Lemma 2 and Chapter 1, Proposition 10, Corollary, page 15. //

Definition 3: Let $K < M \in \mathcal{A}$. Then K is called a modular cover in M if and only if $L \subseteq K$ implies $L(N \cap K) = (LN) \cap K$, for any $L, N \in \mathbb{L}(M)$. //

Remark: M and $\{1\}$ are always modular covers in M. //

Theorem 2: Let $K < M \in \mathcal{A}$.

Then the following are equivalent:

1. K is a modular cover.
2. $x, xy \in K$ implies there exist $\alpha, \beta \in \mathbb{N}_0$ such that $xy = x^{\alpha} y^{\beta}$ and $y^{\beta} \in K$.

Proof: 1 $\Rightarrow$ 2): Let $x, xy \in K$. Now $\langle x \rangle \subseteq K$. So $\langle x \rangle (\langle y \rangle \cap K) = (\langle x \rangle \langle y \rangle) \cap K$. But $xy \in (\langle x \rangle \langle y \rangle) \cap K$ implies $xy \in \langle x \rangle (\langle y \rangle \cap K)$ and so there exist $\alpha, \beta \in \mathbb{N}_0$ such that $xy = x^{\alpha} y^{\beta}$, $y^{\beta} \in K$.

2 $\Rightarrow$ 1): Let $L, N \in \mathbb{L}(M)$ such that $L \subseteq K$. That $L(N \cap K) \subseteq (LN) \cap K$ is well-known.

Let $xy \in (LN) \cap K$, $x \in L$, $y \in N$. Then $x, xy \in K$, whence there exist $\alpha, \beta \in \mathbb{N}_o$ such that $xy = x^{\alpha}y^{\beta}$, $y^{\beta} \in K$. We then have that $xy = x^{\alpha}y^{\beta}$, $x^{\alpha} \in L$, $y^{\beta} \in N \cap K$, and so $xy \in L(N \cap K)$.

Thus, $L(N \cap K) = (LN) \cap K$. //

Corollary: Let $K \not\subset M \in \mathcal{A}$.

Then K is a modular cover.

Proof: $x, xy \in K$ implies $xy = x^1y^1$, $y^1 \in K$. //

Proposition 1: Let $K < M \in \mathcal{A}b$.

Then the following are equivalent:

1. K is a modular cover in M.
2. K is a subgroup of M.
3. $K \not\subset M$.

Proof: 1 $\Rightarrow$ 2): Let $x \in K$. To establish the implication, we need only show that $x^{-1} \in K$. Now, $x, xx^{-1} \in K$ which implies there exist $\alpha, \beta \in \mathbb{N}_o$ such that $xx^{-1} = x^{\alpha}x^{-\beta}$, $x^{-\beta} \in K$. We distinguish two cases.

Case one: Assume we can choose $\alpha \neq 0$. Then $xx^{-1} = x^{\alpha}x^{-\beta}$, $x^{-\beta} \in K$ implies $x^{-1} = x^{\alpha-1}x^{-\beta}$, $x^{\alpha-1}, x^{-\beta} \in K$ whence $x^{-1} \in K$.

Case two: Assume we must have $\alpha = 0$. Now, $x^2, x^2x^{-1} \in K$, and so there exist $\gamma, \delta \in \mathbb{N}_o$ such that $x^2x^{-1} = x^{2\gamma}x^{-\delta}$, $x^{-\delta} \in K$. Thus, $xx^{-1} = x^{2\gamma-1}x^{-\delta}$, $x^{-\delta} \in K$. Suppose $\gamma \neq 0$. Then $2\gamma-1, \delta \in \mathbb{N}_o$, which implies $2\gamma-1 = 0$ (By assumption of case two); but then $\gamma \notin \mathbb{N}_o$, -- a

contradiction. So $\gamma = 0$. Thus, $x = x^{-\delta}$, which implies $x^{-\delta} \in K$ for some $\delta \in \mathbb{N}_0$. If $\delta = 0$, then $x = 1$, and $x^{-1} \in K$ is clear. If $\delta \neq 0$, then $x^{\delta-1} \in K$; it follows that $x^{-\delta}, x^{\delta-1} \in K$, and so $x^{-1} = x^{-\delta} x^{\delta-1} \in K$.

2 $\Rightarrow$ 3): Chapter 1, Proposition 4, page 7.

3 $\Rightarrow$ 1): Theorem 2, Corollary. //

Proposition 2: Let $M \in \mathfrak{L}$.

Let K be a modular cover in M.

Let $y \in \operatorname{con} K$.

Then $y \in M^*$ or there exists $n \in \mathbb{N}_0$ such that $y^n, y^{n+1} \in K$.

Proof: $y \in \operatorname{con} K$ implies there exists $x \in K$ such that $xy \in K$, which implies there exist $\alpha, \beta \in \mathbb{N}_0$ such that $xy = x^\alpha y^\beta$, $y^\beta \in K$. If $\alpha = 0$, $\beta = 0$, then $xy = 1$ which implies $y \in M^*$. If $\alpha = 0$, $\beta \neq 0$, then $xy = y^\beta$ which implies $x = y^{\beta-1}$, and so $y^{\beta-1}, y^\beta \in K$, $\beta - 1 \in \mathbb{N}_0$. If $\alpha \neq 0$, then $xy = x^\alpha y^\beta$ which implies $y = x^{\alpha-1} y^\beta$, and so $y^0, y^1 \in K$. //

Proposition 3: Let $M^* < K < M \in \mathfrak{L}$, where K is a modular cover.

Let $y \in \operatorname{con} K$.

Then $\langle y \rangle' \subseteq K$.

Proof: The proposition is clear if $y \in M^*$, so we assume $y \notin M^*$. Then there exists $n \in \mathbb{N}_0$ such that $y^n, y^{n+1} \in K$, and we choose n minimally. The proposition is clear if $n = 0$ or $n = 1$, so we assume $n \geq 2$.

Now $y^n, y^{n+1} \in K$ implies $y^{2n}, y^{n+1} \in K$, and so we have $y^{n+1}, y^{n+1} y^{n-1} \in K$. It follows that there exist $\alpha, \beta \in \mathbb{N}_0$ such that

$y^{n+1}y^{n-1} = y^{\alpha(n+1)}y^{\beta(n-1)}$, where $y^{\beta(n-1)} \in K$.

Suppose $\beta = 0$, $\alpha = 0$. Then $y^{n+1}y^{n-1} = 1$, and so $y \in M^*$; -- a contradiction.

Suppose $\beta = 0$, $\alpha \neq 0$. Then $y^{n-1} = y^{(\alpha-1)(n+1)}$, $\alpha - 1 \in \mathbb{N}_0$, whence $y^{n-1} \in K$. But this contradicts the minimality of n.

Suppose $\beta = 1$. Then $y^{1(n-1)} \in K$, which also contradicts the minimality of n.

Thus, $\beta \geq 2$.

Now, $y^{n+1}y^{n-1} = y^{\alpha(n+1)\ \beta(n-1)}$, $y \in M \in \mathcal{L}$, $\beta \geq 2$

$\Rightarrow \quad 2n = \alpha(n+1) + \beta(n-1)$, $\beta \geq 2$

$\Rightarrow \quad \frac{2n - \alpha(n+1)}{n - 1} \geq 2$

$\Rightarrow \quad \alpha \leq \frac{2}{n + 1}$

$\Rightarrow \quad \alpha \leq 2/3 \quad$ (as $n \geq 2$)

$\Rightarrow \quad \alpha = 0$.

So $2n = \beta(n-1)$, $\beta \geq 2$. Then $2(n-1) + 2 = \beta(n-1)$, $\beta \geq 2$, whence $(n-1)(\beta-2) = 2$, $\beta \geq 2$. It follows that $n-1$ divides 2, and so $n = 2$ or $n = 3$.

Suppose $n \neq 2$. Then y^3, $y^4 \in K$ and also $y^8 \in K$. Now, y^3, $y^3y^5 \in K$ implies there exist γ, $\delta \in \mathbb{N}_0$ such that $y^3y^5 = y^{3\gamma}y^{5\delta}$, $y^{5\delta} \in K$, which implies $8 = 3\gamma + 5\delta$. As $\delta = 0$ implies 3 divides 8 (contradiction), and $\delta \geq 2$ implies $8 \geq 10$ (contradiction), we must have $\delta = 1$. Thus, $y^5 \in K$. Then, y^3, $y^3y^2 \in K$, which implies there exist λ, $\pi \in \mathbb{N}_0$ such that $y^3y^2 = y^{3\lambda}y^{2\pi}$, $y^{2\pi} \in K$. Now, $5 = 3\lambda + 2\pi$. Since $\pi = 0$ implies 3 divides 5 (contradiction), and $\pi = 2$ implies 3 divides 1 (contradiction), and $\pi \geq 3$ implies $5 \geq 6$ (contradiction),

therefore $\pi = 1$, and so $y^2 \in K$. But this contradicts the minimality of n. Hence $n = 2$.

It follows readily that $\langle y \rangle' \subseteq K$. //

Theorem 3: Let M be a rigid cancellative monoid.

Let $K < M$.

Then the following are equivalent:

1. K is a modular cover.
2. K is connected or $K = \langle y \rangle'$ for any $y \in \text{con } K \backslash K$.
3. K is connected or there exists $y \in M$ such that $K = \langle y \rangle'$.

Proof: 1 $\Rightarrow$ 2): Assume K is a modular cover.

Assume K is not connected. Let $y \in \text{con } K \backslash K$. Then there exists $a \in K$ such that $ay \in K$.

Let $x \in K$ such that $xy \in K$, but otherwise arbitrary. Now there exist $\alpha, \beta \in \mathbb{N}_0$ such that $xy = x^{\alpha}y^{\beta}$, $y^{\beta} \in K$. Suppose $\beta = 0$, $\alpha = 0$. Then $xy = 1$ which implies $y \in M^*$, and so $y \in K$; -- a contradiction. Suppose $\beta = 0$, $\alpha \geq 1$. Then $xy = x^{\alpha}$, which implies $y = x^{\alpha-1} \in K$; -- a contradiction. Suppose $\beta = 1$. Then $y^1 \in K$; -- a contradiction. Thus, $\beta \geq 2$.

So $x = x^{\alpha}y^{\beta-1}$, $\beta - 1 \in \mathbb{N}$. Suppose $\alpha \neq 0$. Then $1 = x^{\alpha-1}y^{\beta-1}$, which implies $y \in M^*$, whence $y \in K$; -- a contradiction. Thus, $x = y^{\beta-1}$ and so $x \in \langle y \rangle$.

We have shown that $x, xy \in K \Rightarrow x \in \langle y \rangle$.

Let $k \in K$. Then $a, ay \in K$, $ka, kay \in K$ implies $a \in \langle y \rangle$, $ka \in \langle y \rangle$, from which it follows that there exist $n, m \in \mathbb{N}_0$ such that $ky^m = y^n$. If $m \leq n$, then $k = y^{n-m} \in \langle y \rangle$. If $n \leq m$, then $ky^{m-n} = 1$

which implies $k \in M^*$, whence $k \in \langle y \rangle$.

Hence, $K \subseteq \langle y \rangle$. Now, $\langle y \rangle' \subseteq K$. So $K = \langle y \rangle$ or $K = \langle y \rangle'$. But it is easily checked that $\langle y \rangle$ is connected. Thus, $K = \langle y \rangle'$.

$2 \Rightarrow 3$): Trivial.

$3 \Rightarrow 1$): The implication is known if K is connected.

Assume there exists $y \in M$ such that $K = \langle y \rangle'$. Let $a, ax \in K$. Then there exist $n, m \in \mathbb{N}_o$ such that $a = y^n$, $ax = y^m$, which implies $y^n x = y^m$. If $m \leq n$, then $y^{n-m}x = 1$, whence $x \in M^*$, and so $x^1 \in K$, $ax = a^1x^1$. If $n < m$, then $x = y^{m-n}$. If, moreover, $m-n \neq 1$, then $x \in \langle y \rangle' = K$, which implies $ax = a^1x^1$, $x^1 \in K$. If, on the other hand, $m - n = 1$, then $x = y$, and so $ax = a^0x^m$, $x^m \in K$.

Thus, $a, ax \in K$ implies there exist $\alpha, \beta \in \mathbb{N}_o$ such that $ax = a^\alpha x^\beta$, $x^\beta \in K$. Hence, K is a modular cover. //

Corollary: Let $K < \mathbb{N}_o$.

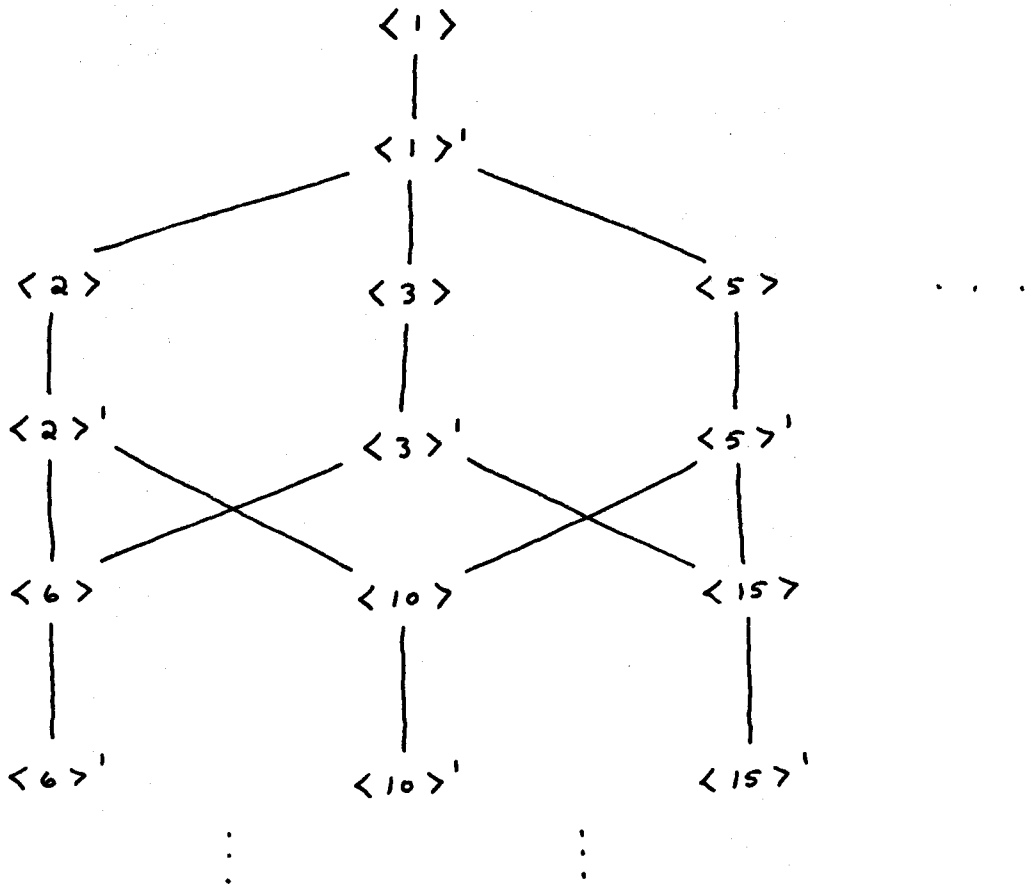
Then the following are equivalent:

1. K is a modular cover.
2. There exists $n \in \mathbb{N}_o$ such that $K = \langle n \rangle$ or $K = \langle n \rangle'$.

Proof: It is easily checked that $M \not\cong \mathbb{N}_o$ if and only if there exists $n \in \mathbb{N}_o$ such that $M = \langle n \rangle$. The result follows. //

It would seem reasonable to expect some sort of decent structure to appear in the lattice of modular covers in an abelian monoid M, although, of course, this lattice is usually not a sublattice of $\mathbb{L}(M)$. The example of $\mathbb{N}_o$ shows that not even semi-modularity can be expected, for it is not difficult to see that the lattice of modular covers in $\mathbb{N}_o$ is found by taking the lattice of natural numbers partially ordered by

divisibility and then splitting each point into two points. The illustration below should make clear what this means.



It is seen that $\langle 2\rangle' \downarrow \langle 2\rangle' \wedge \langle 3\rangle'$, $\langle 3\rangle' \downarrow \langle 2\rangle' \wedge \langle 3\rangle'$, but $\langle 2\rangle' \vee \langle 3\rangle' \not\downarrow \langle 2\rangle'$.

CHAPTER III

FORMAL GAUSS CONTENT

In the theory of rings, the concept of unique factorization domain, or factorial domain, is well known. One theorem of particular interest here is that the ring of polynomials over a factorial domain is again a factorial domain. This theorem is especially easy in the case that the original domain is a field; the general theorem, of course, is somewhat more involved.

The main point of this chapter is to provide a proof of this theorem based only upon the theory of abelian monoids, and a few selected axioms.

The concept of an irreducible element a of an abelian monoid A will be that $a = xy$, $x, y \in A$ implies $x \in A^*$ or $y \in A^*$. Of course, we could also insist that a be a non-unit, but we will find the statements in what follows to be more conveniently expressed if we do not impose this restriction. As would be expected, a factorial monoid will be an abelian monoid A with the property that every element is a product of irreducibles and moreover that the non-unit elements of such a product are unique except for order and multiplication by a unit. It is easily seen, as with rings, that in the presence of the first property, the second is equivalent to: if $p, a, b \in A$, p irreducible, and p divides ab, then p divides a or p divides b.

In what follows, we will assume throughout the following situation: D is an abelian cancellative monoid. The abelian group $D^{-1}D$ (see Chapter 1, § 4) will be denoted $q(D)$. Also, $p(D)$ and $p(q(D))$ are

abelian cancellative monoids. All of these objects are subject to the following axioms (referred to as "property 5", or "property 3", for example, in the text that follows):

1. $D < p(D) < p(q(D))$; $q(D) < p(q(D))$
2. $p(D) \cap q(D) = D$
3. $p(D)^* = D^*$, $p(q(D))^* = q(D)$
4. $p(q(D))$ is a factorial monoid.
5. $n \in p(q(D))$ implies there exists $d \in D$ such that $dn \in p(D)$.
6. $f: p(D) \longrightarrow D/D^*$ is a monoid homomorphism such that $p(D) = D \cdot \mathrm{Ker}\ f$ and when restricted to D, f is the natural map.

By taking D to be the multiplicative monoid of a domain, $p(D)$ to be the multiplicative monoid of the polynomial ring over D, and $p(q(D))$ to be the multiplicative monoid of the polynomial ring over the field $q(D) \cup \{0\}$, we see that the first four properties are clearly satisfied, that the fifth deals with the existence of common denominators, and that the sixth is the usual Gauss content function on the polynomial ring. In what follows, $p(D)$ will be denoted M, while $p(q(D))$ will be written N.

It should be noted that we could raise the status of p by making it a functor, and the same could be done for q. That is, let q be the functor from $\mathcal{L}$ to $\mathcal{A}b$ given by $A \longmapsto A^{-1}A$, and let p be a functor from $\mathcal{L}$ to $\mathcal{L}$ such that:

1. $A < p(A) < p(q(A))$, for any $A \in \mathcal{L}$
2. $p(A) \cap q(A) = A$, for any $A \in \mathcal{L}$
3. $p(A)^* = A^*$, for any $A \in \mathcal{L}$

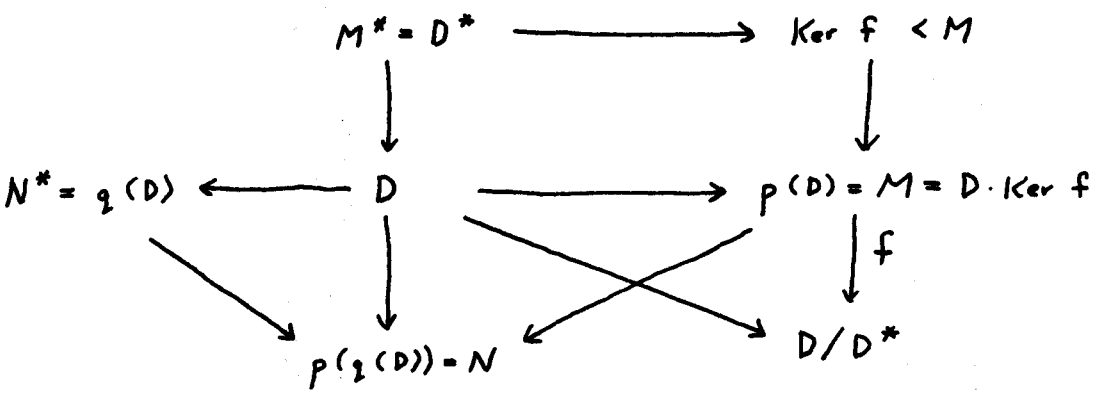
4. $G \in \mathcal{A}b$ implies $p(G)$ is a factorial monoid

5. $n \in p(q(A))$ implies there exists $a \in A$ such that $an \in p(A)$, for any $A \in \mathcal{L}$

6. for each $A \in \mathcal{L}$, there exists a monoid homomorphism $f_A: p(A) \longrightarrow A/A^*$ such that $A \cdot \mathrm{Ker}\ f = p(A)$, and when restricted to A, f is the natural map.

Now the case where $p(D)$ is taken from a polynomial ring is not the only situation in which the above axioms are satisfied -- although it is admittedly the most interesting. There are at least two other cases. The first, and most trivial case is that afforded by taking p to be the identity functor. A second case is given by taking p to be the functor defined by $A \longmapsto A \oplus \mathcal{N}_0$, where $A \oplus \mathcal{N}_0 = \{(a, n) \mid a \in A, n \in \mathcal{N}_0\}$ considered under componentwise operation, and with a and $(a, 0)$ being identified for each $a \in A$. That this functor satisfies the axioms is easily checked (take $f_A((a, n)) = a'$, where a' is the natural image of a).

We now proceed to establish the proof mentioned on page 32. In so doing, the situation we are assuming throughout the rest of this chapter (described above) can be partially summarized by the following diagram.



Lemma 1: Let $d \in D$, $m \in M$.

Then d divides m in M if and only if $f(d)$ divides $f(m)$ in D/D^*.

Proof: $\Rightarrow$): By assumption, $m = dx$ for some $x \in M$. It follows that $f(m) = f(d)\, f(x)$, and we are done.

$\Leftarrow$): It is clear that there exists $d'' \in D$ such that $f(m) = f(d)\, f(d'')$. Also, since $M = D \cdot \mathrm{Ker}\, f$, there exists $d' \in D$ such that $m = d'k$ for some $k \in \mathrm{Ker}\, f$. It is then easily seen that $f(d') = f(dd'')$. It follows readily that $d' = dx$ for some $x \in D$, whence $d'k = dxk$, and so d divides m in M. //

Lemma 2: Let $d \in D$, $m \in M$, $k \in \mathrm{Ker}\, f$ such that k divides dm.

Then k divides m.

Proof: By assumption, $dm = km'$ for some $m' \in M$. Looking at the image of each side under f, we see that $f(d)$ divides $f(m')$. By Lemma 1, there exists $m'' \in M$ such that $m' = dm''$, whence $km' = dm''k$, and so $dm = dm''k$. Using the fact that M is cancellative, we deduce $m = m''k$, and we are done. //

Lemma 3: Let $n \in N$.

Then there exists $n^* \in N^*$ such that $nn^* \in \mathrm{Ker}\, f$.

Proof: By property 5, there exists $d \in D$ such that $dn \in M$. Now, $M = D \cdot \mathrm{Ker}\, f$; so let $d' \in D$, $k \in \mathrm{Ker}\, f$ such that $dn = d'k$. But $q(D) = N^*$, and so d' has an inverse, say d''. Then $k = d''dn$, and, by taking $n^* = d''d$, we are done. //

Lemma 4: Let $k \in \text{Ker } f$ and let (n_i) be a finite family of elements of N such that $k = \prod_i n_i$.

Then there exists a corresponding family (n_i^*) in N^* such that $(n_i n_i^*)$ is a family in Ker f and $k = \prod_i n_i n_i^*$.

Proof: By Lemma 3, there exists a family (m_i^*) in N^* such that $(n_i m_i^*)$ is a family in Ker f. Now $N^* = q(D)$; so for each i, let $m_i^* = x_i/y_i$, $x_i, y_i \in D$. Set $x = \prod_i x_i$, $y = \prod_i y_i$. Clearly, $k = \prod_i \frac{y_i}{x_i} m_i^* n_i$. It follows that $xk = y \prod_i m_i^* n_i$, and so $\prod_i m_i^* n_i$ divides xk.

By Lemma 2, $\prod_i m_i^* n_i$ divides k in M. Thus, there exists $m \in M$ such that $k = m \prod_i m_i^* n_i$. We note that $f(m) = 1$ follows.

Define $n_1^* = mm_1^*$, and $n_i^* = m_i^*$ for all $i \neq 1$. Clearly, $k = \prod_i n_i n_i^*$. Also, for any $i \neq 1$, it is obvious that $n_i^* \in N^*$ and that $n_i n_i^* \in \text{Ker } f$. It remains to show that $n_1^* \in N^*$ and that $n_1 n_1^* \in \text{Ker } f$.

Now, $n_1 n_1^* = n_1 m_1^* m$, where we have already shown that $n_1 m_1^*$, $m \in \text{Ker } f$; and so $n_1 n_1^* \in \text{Ker } f$. Moreover, $k = m \prod_i m_i^* n_i$ implies $k = km \prod_i m_i^*$, whence $m \prod_i m_i^* = 1$. It follows that $m \in N^*$, and thus $mm_1^* \in N^*$. Hence, $n_1^* \in N^*$. //

Lemma 5: Let $m \in M$ be irreducible in M. Then m is irreducible in N.

Proof: Since $M = D \cdot \text{Ker } f$, there exist $d \in D$ and $k \in \text{Ker } f$ such that $m = dk$. But m is irreducible in M. Hence, $d \in M^*$ or $k \in M^*$. Now $M^* = D^*$. Thus, if $k \in M^*$, then $m \in D < q(D)$, and so $m \in N^*$.

We assume, therefore, that $d \in M^*$. It follows readily that $m \in \text{Ker } f$.

Now, let $n_1, n_2 \in N$ such that $m = n_1 n_2$. By lemma 4, we may choose $n_1^*, n_2^* \in N^*$ such that $n_1 n_1^*, n_2 n_2^* \in \text{Ker } f$ and $m = n_1 n_1^* n_2 n_2^*$. By the irreducibility of m in M, either $n_1 n_1^* \in M^*$ or $n_2 n_2^* \in M^*$. But $M^* = D^* < N^*$. Thus, $n_i n_i^*, n_i^* \in N^*$ for either $i = 1$ or $i = 2$. Hence, $n_1 \in N^*$ or $n_2 \in N^*$. //

Lemma 6: Let $n \in N$ be irreducible in N.

Let $n^* \in N^*$ such that $nn^* \in \text{Ker } f$.

Then nn^* is irreducible in M.

Proof: Let $m_1, m_2 \in M$ such that $nn^* = m_1 m_2$. Now, $f(m_1)f(m_2) = f(nn^*) = 1$. Since D/D^* is rigid (see Chapter 1, Definition 7 page 7), it follows that $m_1, m_2 \in \text{Ker } f$.

It is easily seen, from the irreducibility of n, that $m_i \in N^*$ for either $i = 1$ or $i = 2$. Now, $N^* = q(D)$; so $m_i \in q(D) \cap p(D)$ for either $i = 1$ or $i = 2$. By property 2, we see that $m_1 \in D$ or $m_2 \in D$. But $m_1, m_2 \in \text{Ker } f$. It follows that $m_1 \in D^*$ or $m_2 \in D^*$. //

Lemma 7: Let $d \in D$ be irreducible in D.

Then d is irreducible in M.

Proof: Let $m_1, m_2 \in M$ such that $d = m_1 m_2$. Now, in N, $1 = d^{-1} m_1 m_2$, and so $m_1, m_2 \in N^*$. Thus, $m_1, m_2 \in q(D) \cap p(D)$. Hence, $m_1, m_2 \in D$. But d is irreducible in D. It follows that $m_1 \in D^*$ or $m_2 \in D^*$, and we are done. //

Theorem 1: Assume D is a factorial monoid. Then M is a factorial monoid, where $M = p(D)$.

Proof: Let $m \in M$.

Then there exist $d \in D$ and $k \in \text{Ker } f$ such that $m = dk$. Since D is a factorial monoid, we know that d is a product of irreducibles in D, and hence, by Lemma 7, a product of irreducibles in M. Now, $k \in N$, and N is a factorial monoid. Thus, $k = \prod_i n_i$, where each n_i is an irreducible in N. By Lemma 4, there exist $n_i^* \in N^*$ such that $n_i n_i^* \in \text{Ker } f$ for all i, and $k = \prod_i n_i n_i^*$. Moreover, by Lemma 6, $n_i n_i^*$ is irreducible in M for each i.

It follows that m is a product of irreducibles in M.

Now, let $m, m', m'' \in M$ such that m divides $m'm''$ (in M), and m is irreducible. It is easy to see that if we can show that m divides m' or m divides m'', then we are done.

Now, there exist $d' \in D$, $k' \in \text{Ker } f$ such that $m = d'k'$. By the irreducibility of m, and noting that $M^* = D^*$, it is readily seen that either $m \in D$ or $m \in \text{Ker } f$.

Assume first that $m \in D$. Since m divides $m'm''$, we have that $f(m)$ divides $f(m')f(m'')$ in D/D^*, where $f(m)$ is irreducible in D/D^*. But D/D^* is a factorial monoid. Hence, $f(m)$ divides $f(m')$ or $f(m)$ divides $f(m'')$. By Lemma 1, m divides m' or m divides m''.

If, on the other hand, we assume that $m \in \text{Ker } f$, then we can argue as follows. By Lemma 5, m is irreducible in N. Thus, in N, either m divides m' or m divides m''. Without loss of generality, we may assume m divides m', and so there exists $n \in N$ such that $m' = mn$. Now, by property 5, there exists $d \in D$ such that $dn \in M$. Also,

$m'd = mdn$, where $m'd, m, dn \in M$. Thus, m divides $m'd$ in M, where $m \in \text{Ker } f$, $d \in D$, and $m' \in M$. By Lemma 2, m divides m' in M. //

CHAPTER 4

CATEGORICAL CONSIDERATIONS

§ 1: Introduction; Coreflections and Reflections

In this chapter we will be considering the categories $\mathcal{A}$, $\mathcal{S}$, $\mathcal{L}$, and $\mathcal{A}b$. Our main purpose will be to identify some of the more important categorical objects of $\mathcal{A}$, and to a lesser extent those in $\mathcal{S}$ and $\mathcal{L}$ as well. $\mathcal{A}b$ is, of course, a well known category. Because our main attention will be directed to $\mathcal{A}$, any categorical concept mentioned in this chapter which does not refer explicitly to some category will be assumed to refer to $\mathcal{A}$. Normally, a concept considered strictly within some subcategory of $\mathcal{A}$, say $\mathcal{L}$ for example, will be prefixed with that category; for example, we would speak of a $\mathcal{L}$-epimorphism.

On the whole, definitions of standard categorical concepts are assumed to be known by the reader. Readers for whom this assumption is false are referred to Mitchell [8].

Notationally, given maps will be assumed to be monoid homomorphisms unless otherwise stated.

Proposition 1: Let $A, B \in \mathcal{A}$, $f: A \longrightarrow B$.

Then: 1. f is an isomorphism if and only if f is 1-1 and onto.

2. f is a monomorphism if and only if f is 1-1.

Proof: 1. $\Longrightarrow$): True in any concrete category.

$\Longleftarrow$): The only conceivable candidate for an inverse of f is both obvious and easily verified.

2. $\Leftarrow$): True in any concrete category.

$\Rightarrow$): Let $x, y \in A$ such that $f(x) = f(y)$. Let $M = \{(x^n, y^n) \mid n \in \mathbb{N}_o\}$ with componentwise multiplication. Clearly $M \in \mathcal{A}$. Let α: $M \longrightarrow A$ by $(x^n, y^n) \longmapsto x^n$, for any $n \in \mathbb{N}_o$. and β: $M \longrightarrow A$ by $(x^n, y^n) \longmapsto y^n$, for any $n \in \mathbb{N}_o$. It is easily seen that α and β are monoid homomorphisms, and readily checked that $f\alpha = f\beta$. Since f is a momomorphism, we have $\alpha = \beta$, which implies $\alpha((x, y)) = \beta((x, y))$, and so $x = y$. Hence, f is 1-1. //

Lemma 1: Let $S < M \in \mathcal{A}$.

Let φ : $M \longrightarrow S^{-1}M$ by $m \longmapsto m/1$

Then φ is a epimorphism.

Proof: Let $N \in \mathcal{A}$. Let α, β: $S^{-1}M \longrightarrow N$ such that $\alpha\varphi = \beta\varphi$ Then $\alpha(m/1) = \beta(m/1)$ for any $m \in M$. Let $s \in S$.

Then $\alpha(1/1) = \beta(1/1)$

$\Rightarrow \alpha(s/1)\,\alpha(1/s) = \beta(s/1)\,\beta(1/s)$

$\Rightarrow \alpha(s/1)\,\alpha(1/s) = \alpha(s/1)\,\beta(1/s)$, $\alpha(s/1) \in N^*$

$\Rightarrow \alpha(1/s) = \beta(1/s)$.

It follows that $\alpha(m/s) = \beta(m/s)$ for any $m/s \in S^{-1}M$. Hence, φ is an epimorphism. //

Corollary: Epimorphisms are not necessarily onto.

Proof: Take $S = M = \mathbb{N}_o$ in the lemma. //

Proposition 2: Let $M \in \mathcal{A}$.

Let φ : $M \longrightarrow M^{-1}M$ by $m \longmapsto m/1$.

Then φ is an epimorphic coreflection into $\mathcal{A}b$.

Proof: We know that φ is an epimorphism. Also, it is readily checked that $M^{-1}M$ is a group. Let $G \in \mathcal{A}b$ and $f: M \longrightarrow G$. Clearly $f(m) \in G^* = G$ for any $m \in M$. Hence, there exists a unique $g: M^{-1}M \longrightarrow G$ such that $f = g\varphi$ (Chapter 1, Proposition 19, page 22). //

Proposition 3: Let $M \in \mathcal{M}$.

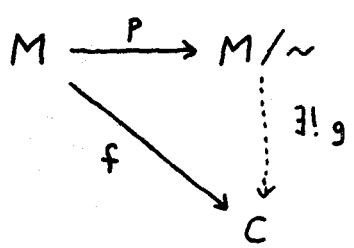
Let $\sim$ be the binary relation on M defined by $x \sim y$ if and only if there exists $m \in M$ such that $mx = my$.

Then $\sim$ is a congruence relation.

Moreover, let $p: M \longrightarrow M/\sim$ be the natural map.

Then p is an onto coreflection into $\mathcal{L}$.

Proof: It is readily checked that $\sim$ is a congruence relation and obvious that p is onto. Also, it is easily seen that $M/\sim \in \mathcal{L}$. Let $C \in \mathcal{L}$ and $f: M \longrightarrow C$. Now, $p(x) = p(y)$ implies there exists $m \in M$ such that $mx = my$, whence $f(m)f(x) = f(m)f(y)$, and so $f(x) = f(y)$. Thus, we may well define $g: M/\sim \longrightarrow C$ by $p(x) \longmapsto f(x)$. It is easily seen that g is a monoid homomorphism and that $gp = f$.



Moreover g is unique, for $g'p = f$ implies $g'p = gp$, p onto, and so $g' = g$. //

Proposition 4: Let $M \in \mathcal{M}$.

Let $N = \{ n \in M \mid n^2 = n \}$.

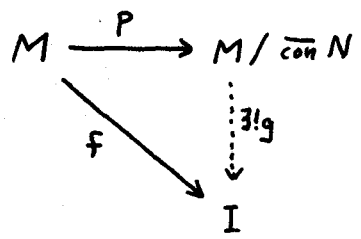
Let $p: M \longrightarrow M/\overline{\text{con}}\, N$ be the natural map.

Then p is an onto coreflection into $\mathcal{J}$.

Proof: It is clear that p is onto.

Now, $p(x)^2 = p(x)$ implies $x^2 \sim x$ $(\overline{\text{con}}\ N)$. It follows that there exist $a, b \in \overline{\text{con}}\ N$ such that $ax^2 = bx$. From this we get $x \in \overline{\text{con}}\ N$, and so $p(x) = 1$. Thus, $M/\overline{\text{con}}\ N \in \mathcal{J}$.

Let $D = \{ d \in M \mid \exists\ n \in N \cdot\ d^2 = nd \}$. Then $\overline{\text{con}}\ N = \text{con}\ D$. Let $f: M \longrightarrow I \in \mathcal{J}$. Now $n \in N$ implies $n^2 = n$, which in turn implies $f(n)^2 = f(n)$, whence $f(n) = 1$. Also, $d \in D$ implies there exists $n \in N$ such that $d^2 = nd$. From this we get $f(d)^2 = f(d)$, and so $f(d) = 1$.



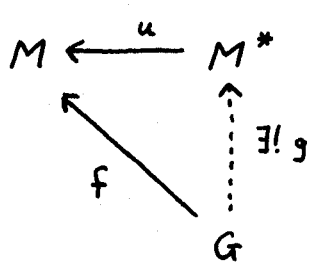
Finally, $x \in \overline{\text{con}}\ N$ implies $x \in \text{con}\ D$, which implies there exists $d \in D$ such that $dx \in D$; so $f(d) = 1$, $f(d)f(x) = 1$, and hence $f(x) = 1$.

Thus there exists a unique $g: M/\overline{\text{con}}\ N \longrightarrow I$ such that $f = gp$, (Chapter 1, Theorem 1, page 4). //

Proposition 5: Let $u: M^* \longrightarrow M \in \mathcal{A}$ be the natural injection. Then u is a monomorphic reflection out of $\mathbb{A}\,b$.

Proof: It is clear that u is a monomorphism and of course that $M^* \in \mathbb{A}\,b$.

Let $G \in \mathbb{A}\,b$ and $f: G \longrightarrow M$. Now, $G \in \mathbb{A}\,b$ implies $f_*(G) \in \mathbb{A}\,b$, which in turn implies $f_*(G) \subseteq M^*$. Thus we may define $g: G \longrightarrow M^*$ by $x \longmapsto f(x)$. Obviously, $f = ug$ and the fact u is a monomorphism ensures that g is unique. //



We have now that $\mathcal{A}b \subseteq \mathcal{L} \subseteq \mathcal{J} \subseteq \mathcal{M}$ is a chain of full coreflective subcategories of $\mathcal{M}$, and moreover that $\mathcal{A}b$ is a reflective one. In searching to determine whether or not $\mathcal{L}$ and $\mathcal{J}$ are also reflective in $\mathcal{M}$ we are first lead to consider whether or not we want to insist that the reflections be monomorphisms. Without this restriction, I suspect, but have failed to prove, that $\mathcal{L}$ and $\mathcal{J}$ are not reflective. It can be proved, however, that, in general, monomorphic reflections out of $\mathcal{L}$ and $\mathcal{J}$ do not exist.

Example: Let $M = \{1, e\} \in \mathcal{M}$, where $e^2 = e \neq 1$. Then M has no monomorphic reflection out of $\mathcal{J}$ or $\mathcal{L}$.

Proof: Suppose M does have a monomorphic reflection out of $\mathcal{J}$ or $\mathcal{L}$. Without loss of generality, we may assume that the domain of such a reflection is a submonoid of M. But $M \notin \mathcal{J}$ and $M \notin \mathcal{L}$. Thus, the domain of the reflection must be $\{1\}$. Define $f: \mathbb{N}_0 \longrightarrow M$ by $n \longmapsto e^n$. Clearly, there does not exist a morphism $g: \mathbb{N}_0 \longrightarrow \{1\}$ such that $ug = f$, where $u: \{1\} \longrightarrow M$. Noting that $\mathbb{N}_0, \{1\} \in \mathcal{J}$ and $\mathbb{N}_0, \{1\} \in \mathcal{L}$, we are done. //

§ 2: Various Identifications

It is clear that $\{1\}$ is the zero of all four of the categories we are considering. Consequently, we shall often denote $\{1\}$ by 0, even when considered as a submonoid of a multiplicatively written monoid. Similarly, if $f: A \longrightarrow B$ by $a \longmapsto 1$ for any $a \in A$, then f will usually be denoted 0, or 0_{AB} if the context is not clear.

If $f: A \longrightarrow A$ by $a \longmapsto a$ for any $a \in A$, then f is usually denoted id, or id_A.

Proposition 6: Let $(A_i)_{i \in I}$ be a family of abelian monoids.

Then:
1. the product of this family, denoted $\prod_{i \in I} A_i$, is $\{(a_i)_{i \in I} \mid a_i \in A_i \ \forall \ i \in I\}$;
2. the coproduct of this family, denoted $\bigoplus_{i \in I} A_i$, is $\{(a_i)_{i \in I} \in \prod_{i \in I} A_i \mid a_i = 1$ for all but finitely many $i \in I\}$. //

Proof: Routine. //

Proposition 7: Let $f, g: A \longrightarrow B$.

Let $E = \{x \in A \mid f(x) = g(x)\}$.

Let $u: E \longrightarrow A$ by $x \longmapsto x$.

Then u is an equalizer for f and g.

Proof: Routine. //

Corollary: Let $f: A \longrightarrow B$.

Let $K = \{x \in A \mid f(x) = 1\}$.

Let $u: K \longrightarrow A$ by $x \longmapsto x$.

Then u is a kernel of f.

Proof: We note that u is an equalizer for f and 0. //

Proposition 8: Let $f, g: A \longrightarrow B$.

Let $\mathcal{R} = \{R \subseteq B \times B \mid R$ is a congruence relation, $(f(a), g(a)) \in R$, $\forall\ a \in A\}$.

Let $\sim = \bigcap \mathcal{R}$.

Let $p: B \longrightarrow B/\sim$ be the natural map.

Then p is a coequalizer for f and g.

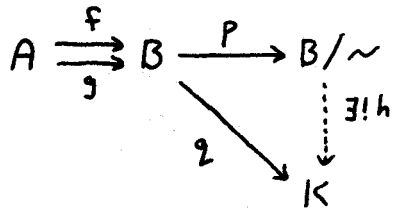
Proof: Since $(pf)(a) = p(f(a))$

$= p(g(a))$ (as $f(a) \sim g(a)$)

$= (pg)(a)$,

therefore $pf = pg$.

Let $q: B \longrightarrow K$ such that $qf = qg$



Let $\equiv$ be the binary relation in B defined by $x \equiv y$ if and only if $q(x) = q(y)$. It is then easily checked that $\equiv$ is a congruence relation. Moreover, $qf = qg$ implies $q(f(a)) = q(g(a))$ for any $a \in A$, whence $f(a) \equiv g(a)$ for any $a \in A$. Thus, $\sim \subseteq \equiv$; so $x \sim y$ implies $x \equiv y$. Hence we may well define $h: B/\sim \longrightarrow K$ by $p(b) \longmapsto q(b)$ for any $b \in B$. Now, $(hp)(a) = q(a)$ for any $a \in A$, is clear. Thus, $q = hp$. Moreover, as p is onto and thus an epimorphism, we are ensured that h is unique. //

Corollary: Let $f: A \longrightarrow B$.

Let p be the coequalizer for f and 0.

Then p is a cokernel for f.

Proof: Clear. //

Although the above description of cokernels is accurate, it is apparent that it is not as useful as it might be. For this reason we give below a different description, together with an independent proof.

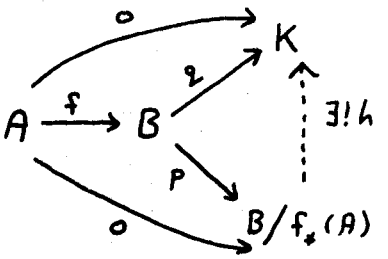
Proposition 9: Let $f: A \longrightarrow B$.

Let $p: B \longrightarrow B/f_*(a)$ be the natural map.

Then p is a cokernel for f.

Proof: It is readily checked that $pf = 0$.

Let $q: B \longrightarrow K$ such that $qf = 0$. Now, $qf = 0$ implies $q(f(a)) = 1$ for any $a \in A$, whence $q(n) = 1$ for any $n \in f_*(A)$. Thus, there exists a unique $h: B/f_*(A) \longrightarrow K$ such that $q = hp$, (Chapter 1, Theorem 1, page 4).



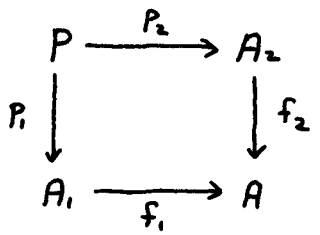
//

Proposition 10: Let $f_1: A_1 \longrightarrow A$, $f_2: A_2 \longrightarrow A$.

Let $P = \{(x, y) \mid x \in A_1, y \in A_2, f_1(x) = f_2(y)\}$.

Let $p_1: P \longrightarrow A_1$ by $(x, y) \longmapsto x$, and $p_2: P \longrightarrow A_2$ by $(x, y) \longmapsto y$.

Then



is a pullback.

Proof: Routine. //

Proposition 11: Let $f_1: A \longrightarrow A_1$, $f_2: A \longrightarrow A_2$.

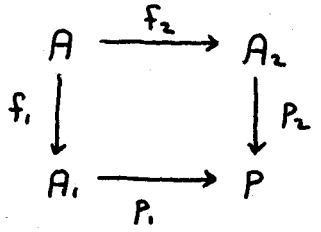
Let $\mathcal{R} = \{R \mid R$ is a congruence relation in $A_1 \times A_2$, $(f_1(a), 1)\ R\ (1, f_2(a))\ \forall\ a \in A\}$.

Let $\sim\ = \bigcap \mathcal{R}$

Let $P = (A_1 \times A_2) / \sim$.

Let $p_1: A_1 \longrightarrow P$, $p_2: A_2 \longrightarrow P$ be the natural maps.

Then



is a pushout.

Proof: Since $(p_1 f_1)(a) = p_1(f_1(a))$

$= [(f_1(a), 1)]$ (i.e. the congruence class containing $(f_1(a), 1)$)

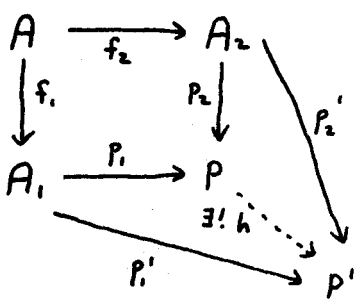
$= [(1, f_2(a))]$ (as $(f_1(a), 1) \sim (1, f_2(a))$)

$= (p_2 f_2)(a)$, for any $a \in A$,

therefore $p_1 f_1 = p_2 f_2$.

Let $p_1': A_1 \longrightarrow P'$, $p_2': A_2 \longrightarrow P'$ such that $p_1' f_1 = p_2' f_2$.

Let $\equiv$ be the binary relation on $A_1 \times A_2$ given by $(x,y) \equiv (a,b)$ if and only if $p_1'(x)\, p_2'(y) = p_1'(a)\, p_2'(b)$. It is readily checked that $\equiv$ is a congruence relation and that $\sim \subseteq \equiv$. Thus we may well define $h: P \longrightarrow P'$ by $[(x, y)] \longmapsto p_1'(x)\, p_2'(y)$. It is then easy to show that $p_1' = hp_1$, $p_2' = hp_2$, and that h is unique. //

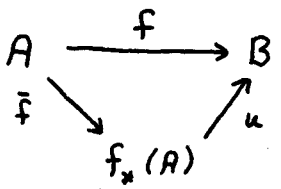


Proposition 12: Let $f: A \longrightarrow B$.

Let $\bar{f}: A \longrightarrow f_*(A)$ by $a \longmapsto f(a)$.

Let $u: f_*(A) \longrightarrow B$ by $x \longmapsto x$.

Then



is the image of f.

Proof: Easy. //

Lemma 2: Let $A < B \in \mathcal{M}$.

For each $N < B$ such that $A \subseteq N$, define i_N: $A \longrightarrow N$ by $a \longmapsto a$.

Then there exists $M < B$ such that $A \subseteq M$, i_M is an epimorphism, and $A < M' < B$, $i_{M'}$ an epimorphism implies $M' \subseteq M$.

Proof: Let $\mathcal{N} = \{ N \mid A < N < B, \ i_N \text{ is an epimorphism} \}$. It is clear that $\mathcal{N} \neq \emptyset$, for $A \in \mathcal{N}$. Let M be the submonoid of B generated by $\bigcup \mathcal{N}$. It is easily checked that $A < M < B$ and that $A < M' < B$, $i_{M'}$ an epimorphism $\Rightarrow M' \subseteq M$.

It remains to show that i_M is an epimorphism. Let f, g: $M \longrightarrow D$ such that $fi_M = gi_M$. Now it is easy to show that $b \in M$ if and only if b is a finite product of elements of $\bigcup \mathcal{N}$. Thus, it is sufficient to show that for each $N \in \mathcal{N}$, $f(x) = g(x)$ for any $x \in N$.

Let $N \in \mathcal{N}$. Define f': $N \longrightarrow D$ by $n \longmapsto f(n)$ and g': $N \longrightarrow D$ by $n \longmapsto g(n)$. Then, $fi_M = gi_M$ implies $f(x) = g(x)$ for any $x \in A$, whence $f'(x) = g'(x)$ for any $x \in A$, and so $f'i_N = g'i_N$. But i_N is an epimorphism. Hence $f' = g'$. //

Notation: In the above lemma, we denote M by $\text{epi}_B(A)$. //

Proposition 13: Let $f: A \longrightarrow B$.

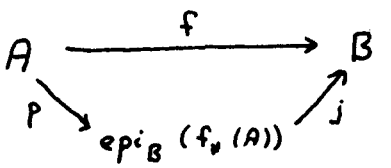
Let $\bar{f}: A \longrightarrow f_*(A)$ by $a \longmapsto f(a)$.

Let $i: f_*(A) \longrightarrow epi_B(f_*(A))$ by $f(a) \longmapsto f(a)$.

Let $j: epi_B(f_*(A)) \longrightarrow B$ by $x \longmapsto x$.

Let $p = if$.

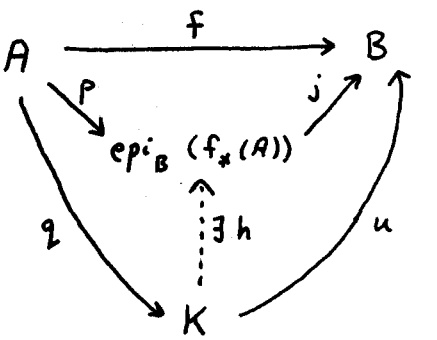
Then



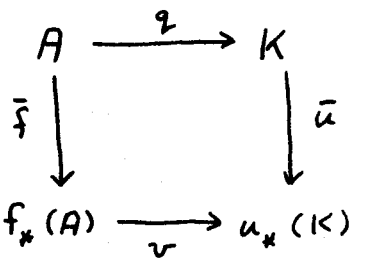
is a coimage for f.

Proof: It is clear that p is an epimorphism and that $jp = f$.

Let $q: A \longrightarrow K$ be an epimorphism,



and $u: K \longrightarrow B$ such that $uq = f$. Let $\bar{u}: K \longrightarrow u_*(K)$ by $k \longmapsto u(k)$. Now $uq = f$ implies $f_*(A) \subseteq u_*(K)$. Let $v: f_*(A) \longrightarrow u_*(K)$ by $x \longmapsto x$. It is easily checked that $v\bar{f} = \bar{u}q$. But q is an epimorphism (by assumption), as is $\bar{u}$ (since it is onto). Thus, $\bar{u}q$ is an epimorphism; hence $v\bar{f}$, and so v. It follows that $u_*(K) \subseteq epi_B(f_*(A))$. Hence, we may define $h: K \longrightarrow epi_B(f_*(A))$ by $k \longmapsto u(k)$, and it is seen that $hq = p$ and $jh = u$.



//

To conclude this section, we present below some examples of coimages. This is intended to serve three purposes: first, to give some

feeling for what coimages in $\mathcal{A}$ look like; second, to give some more varied examples of epimorphisms that are not onto (for $f'\colon A \longrightarrow \mathrm{epi}_B(f_*(A))$ by $a \longmapsto f(a)$ is such whenever $\mathrm{epi}_B(f_*(A)) \neq f_*(A)$); and third, to give some ground work for counterexamples to be given later.

Lemma 3: Let $M < G \in \mathcal{A}\mathrm{b}$.

Let H be the subgroup of G generated by M.

Let $i\colon M \longrightarrow H$ by $m \longmapsto m$.

Then i is an epimorphism.

Proof: H is just $M^{-1}M$. (See Lemma 1). //

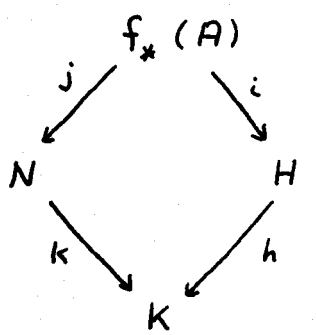
Proposition 14: Let $f\colon A \longrightarrow G$, where $A \in \mathcal{A}$, $G \in \mathcal{A}\mathrm{b}$.

Let H be the subgroup of G generated by $f_*(A)$.

Then $H = \mathrm{Coim}\, f$.

Proof: We must prove that $H = \mathrm{epi}_B(f_*(A))$.

Let $i\colon f_*(A) \longrightarrow H$ by $x \longmapsto x$.



Now we know that i is an epimorphism. So let $j\colon f_*(A) \longrightarrow N < G$ by $x \longmapsto x$, where $f_*(A) < N$ and j is an epimorphism. Clearly, if we can show that $N < H$, then we are done.

Let K be the subgroup of G generated by N. Evidently $H < K$. Let $k\colon N \longrightarrow K$ and $h\colon H \longrightarrow K$ be the natural injections. Now, $kj = hi$ is clear. Also, j is given to be an epimorphism and by Lemma 3, k is also; hence kj and so hi is. It follows that h is an epimorphism. In particular, h is an $\mathcal{A}\mathrm{b}$-epimorphism and is thus onto. Hence, $H = K$, and so $N < H$. //

Proposition 15: Let $f: A \longrightarrow B$.

Let B' be B with a zero adjoined. That is, $B' = B \cup \{e\}$, where $be = eb = e^2 = e$ for any $b \in B$.

Let $f': A \longrightarrow B'$ by $a \longmapsto f(a)$.

Then Coim f' = Coim f.

Proof: If $e \notin$ Coim f', then the proposition is clear.

Suppose $e \in$ Coim f'. Then define $D =$ Coim $f' \cup \{e'\}$ where $xe' = e'x = e'e' = e'$ for any $x \in$ Coim f'. Define $g:$ Coim $f' \longrightarrow D$ by $x \longmapsto x$ and $h:$ Coim $f' \longrightarrow D$ by $x \longmapsto \{x$, if $x \neq e, e'$, if $x = e.\}$ Let $i: f_*^!(A) \longrightarrow$ Coim f' by $x \longmapsto x$. Then it is easily seen that $gi = hi$ but $g \neq h$. But this contradicts the fact that i is an epimorphism. //

Proposition 16: Let $f: A \longrightarrow B$.

Let $A' = A \cup \{e_A\}$, where $ae_A = e_Aa = e_A^2 = e_A$ for any $a \in A$; and B' be defined similarly.

Let $f': A' \longrightarrow B'$ by $x \mapsto \{f(x)$, if $x \in A \setminus e_B$, if $x = e_A\}$.

Then Coim f' = Coim $f \cup \{e_B\}$.

Proof: It is not difficult to verify that $i: f_*^!(A') \longrightarrow$ Coim $f \cup \{e_B\}$ by $x \longmapsto x$ is an epimorphism, and hence that Coim $f \cup \{e_B\} \subseteq$ Coim f'. Suppose that equality does not hold; that is, that Coim $f \subsetneq$ Coim $f' \setminus \{e_B\} < B$. Then there exist $g, h:$ Coim $f' \setminus \{e_B\} \longrightarrow N$ such that $g \neq h$ but $gj = hj$, where $j: f_*(A) \longrightarrow$ Coim $f' \setminus \{e_B\}$. Let $N' = N \cup \{e_N\}$ as usual. Define $g':$ Coim $f' \longrightarrow N'$ and $h':$ Coim $f' \longrightarrow N'$ in the obvious way, and $k: f_*^!(A') \longrightarrow$ Coim f' by $x \longmapsto f'(x)$. Then it is seen that $g'k = h'k$. But k is an epimorphism, and so $g' = h'$, whence $g = h$. Contradiction. //

Proposition 17: Let $f: A \longrightarrow B$.

Let $M \in \mathcal{M}$.

Let $g: A \longrightarrow B \oplus M$ by $a \longmapsto (f(a), 1)$. Then

$\text{Coim } g = \{ (b, 1) \mid b \in \text{Coim } f \}$.

Proof: Let $K = \{ (b, 1) \mid b \in \text{Coim } f \}$. Clearly $K \subseteq \text{Coim } g$.

Now, let $i: g_*(A) \longrightarrow \text{Coim } g$ be the natural map. Define $u: \text{Coim } g \longrightarrow B \oplus M$ by $(x, y) \longmapsto (x, y)$ and $v: \text{Coim } g \longrightarrow B \oplus M$ by $(x, y) \longmapsto (x, 1)$. Then $ui = vi$ is clear, and, since i is an epimorphism, $u = v$. Thus, if $(x, y) \in \text{Coim } g$, then $y = 1$. It follows easily that $K = \text{Coim } g$. //

§ 3: Extremal Morphisms; Exactness

Definition 1: (See Herrlich [4; p. 61]). Let $f: A \longrightarrow B$.

Then: 1. f is called an extremal monomorphism if and only if

i f is a monomorphism.

ii $f = np$, p an epimorphism, implies p is an isomorphism.

2. f is called an extremal epimorphism if and only if

i f is an epimorphism

ii $f = un$, u a monomorphism, implies u is an isomorphism. //

We note that in a balanced category, f is an extremal monomorphism (extremal epimorphism) if and only if f is a monomorphism (epimorphism).

While it is well known that $\mathcal{A}b$ is a balanced category, we see from Lemma 1, Corollary, that $\mathcal{R}$, $\mathcal{J}$, and $\mathcal{L}$ are not balanced.

We recall below a few known facts concerning extremals.

Lemma 4: Let $\mathcal{X}$ be any category.

Let $A \in \mathcal{X}$

Then id_A is an extremal monomorphism and an extremal epimorphism.

Proof: Easy. //

Lemma 5: Let $\mathcal{X}$ be any category.

Let f be an extremal monomorphism (extremal epimorphism).

Let $f = pu$.

Then u is an extremal monomorphism (p is an extremal epimorphism).

Proof: Easy. //

Proposition 18: Let $\mathcal{X}$ be any category.

Let $u: E \longrightarrow A$ be an equalizer in $\mathcal{X}$.

Then u is an extremal monomorphism.

Proof: It is proved in Mitchell [8] that u is a monomorphism.

Let $u = fp$, p an epimorphism. Now, u is an equalizer; let it equalize $a, b: A \longrightarrow B$.

So, $au = bu$

$\Rightarrow afp = bfp$

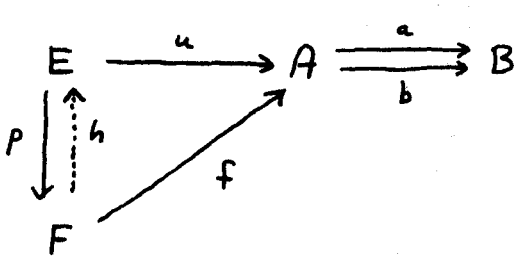
$\Rightarrow af = bf$

$\Rightarrow \exists\ h \cdot\ uh = f$

$\Rightarrow uhp = fp$

$\Rightarrow uhp = u$

$\Rightarrow hp = id$



But id is an extremal monomorphism and p is an epimorphism, hp = id. Thus, p is an isomorphism. //

Corollary: Let $\mathcal{X}$ be a category with zeroes.

Let f: $A \longrightarrow B$.

Then f is a kernel $\Rightarrow$ f an equalizer

$\Rightarrow$ f an extremal monomorphism.

$\Rightarrow$ f a monomorphism.

Proof: Clear. //

We turn now to the question of defining what we want to mean when we say a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ is exact. It seems perfectly natural to insist that the concept of exactness should at least contain the restriction that Im f = Ker g. The issue is whether or not this restriction by itself would lead to a worthwhile theory of exactness. In answering this, we note that any such theory would surely have the result that if $0 \xrightarrow{o} B \xrightarrow{g} C$ is exact, the g is a monomorphism, but we find that this would not be true in $\mathcal{A}$ if we took only the restriction indicated above. A counterexample is obtained by taking $B = \mathbb{N}_o$, $C = \{1, e\}$, (where $e^2 = e \neq 1$), and g to be defined by $n \longmapsto e^n$ for any $n \in \mathbb{N}_o$ ($e^0 = 1$); for we see then that Im 0 = Ker g and yet g is not 1 - 1.

For this reason then, we adopt the definition indicated below. Considering that the second restriction is redundant in $\mathcal{Ab}$, but not redundant in $\mathcal{A}$, $\mathcal{J}$, or $\mathcal{L}$ we feel that this definition is the next most natural one to adopt.

Definition 2: We say $A \xrightarrow{f} B \xrightarrow{g} C$ is exact at B if and only if 1. $\text{Im } f = \text{Ker } g$,

2. $\text{Coker } f = \text{Coim } g$. //

Theorem 1: Let $f: A \longrightarrow B$.

Then the following are equivalent:

1. $f: A \longrightarrow B$ is an extremal epimorphism.
2. $f: A \longrightarrow B$ is onto.
3. $A \xrightarrow{f} B \xrightarrow{0} 0$ is exact.

Proof: 1 $\Longrightarrow$ 2): Assume f is an extremal epimorphism. Let $f': A \longrightarrow f_*(A)$ by $a \longmapsto f(a)$. Let $u: f_*(A) \longrightarrow B$ by $f(a) \longmapsto f(a)$. Then $f = uf'$, u a monomorphism, implies u is an isomorphism, whence u is onto. Thus $f_*(A) = B$, and so f is onto.

2 $\Longrightarrow$ 3): Assume f is onto. Clearly, $\text{Im } f = B = \text{Ker } 0$. Also, $\text{Coker } f = B/B \cong 0 = \text{Coim } 0$. Thus, $A \xrightarrow{f} B \xrightarrow{0} 0$ is exact.

3 $\Longrightarrow$ 1): Assume $A \xrightarrow{f} B \xrightarrow{0} 0$ is exact. Then $\text{Im } f = \text{Ker } 0 = B$ implies f is onto, and so f is an epimorphism.

Let $f = un$, where u is a monomorphism. Now f is onto. Thus, u is onto, and so u is an isomorphism.

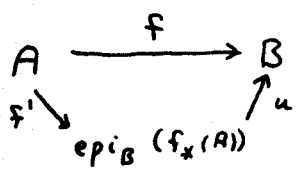
Hence, f is an extremal epimorphism. //

Theorem 2: Let $f: A \longrightarrow B$.

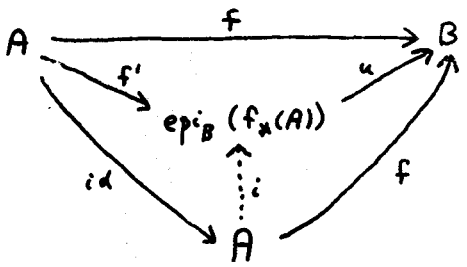
Then the following are equivalent:

1. $f: A \longrightarrow B$ is an extremal monomorphism.
2. $0 \xrightarrow{0} A \xrightarrow{f} B$ is exact.

Proof: 1 $\Rightarrow$ 2): Assume f is an extremal monomorphism. Since f is 1 - 1, it is clear that $\text{Im } 0 = \text{Ker } f = \{1\}$. Let $f': A \longrightarrow \text{epi}_B(f_*(A))$ by $a \longmapsto f(a)$ and $u: \text{epi}\ (f_*(A)) \longrightarrow B$ by $x \longmapsto x$. Then $f = uf'$, f' an epimorphism implies f' is an isomorphism, which in turn implies $\text{Coker } 0 = A/\{1\} \cong A \cong \text{epi}_B(f_*(A)) = \text{Coim } f$. Thus, $0 \xrightarrow{0} A \xrightarrow{f} B$ is exact.



2 $\Rightarrow$ 1): Assume $0 \xrightarrow{0} A \xrightarrow{f} B$ is exact. It is clear that we may take $id: A \longrightarrow A$ to be the cokernel of 0. Let $f': A \longrightarrow \text{epi}_B(f_*(A))$ by $a \longmapsto f(a)$ and $u: \text{epi}_B(f_*(A)) \longrightarrow B$ by $x \longmapsto x$.



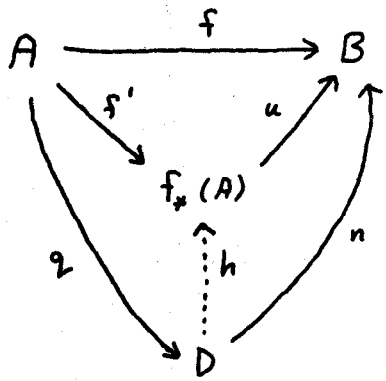
Since $\text{Coim } f = \text{epi}_B(f_*(A))$, it follows that there exists a unique $i: A \longrightarrow \text{epi}_B(f_*(A))$ such that $i\ id = f' \Rightarrow i = f'$. By the exactness at A, we see that i (i.e. f') is an isomorphism. It follows that f is a monomorphism and that $\text{epi}_B(f_*(A)) = f_*(A)$.

Let $f = nq$, q an epimorphism, $q: A \longrightarrow D$. Now, there exists a unique $h: D \longrightarrow f_*(A)$ such that

$hq = f'$, $uh = n$. We notice that

$qf'^{-1}hq = qf'^{-1}f' = q$, which implies

$qf'^{-1}h = id_D$, and thus h is 1-1.



Thus, $d \in D \Rightarrow h(d) \in f_*(A)$

$\Rightarrow \exists\ a \in A \cdot\!\!\cdot\ f(a) = h(d)$

$\Rightarrow f'(a) = h(d)$

$\Rightarrow (hq)(a) = h(d)$

$\Rightarrow h(q(a)) = h(d)$

$\Rightarrow q(a) = d$,

and so q is onto. It follows that q is an isomorphism. //

The observations below that conclude this section are designed to show that, in spite of the good behaviour of exact sequences as exhibited in the preceding, our concept of exactness is still capable of some rather strange behaviour.

<u>Proposition 19</u>: Let $A \xrightarrow{f} B \xrightarrow{0} 0$ be exact.

Let i: Ker $f \longrightarrow A$ by $x \longmapsto x$.

Then Ker $f \xrightarrow{i} A \xrightarrow{f} B \xrightarrow{0} 0$ is not necessarily exact at A.

<u>Proof</u>: Take $\mathbb{N}_0 \xrightarrow{f} \{1, e\} \xrightarrow{0} 0$, where $f: n \longmapsto e^n$, and $e^2 = e \neq 1$. Since f is onto, we know this is exact. However, Ker $f \xrightarrow{i} \mathbb{N}_0 \xrightarrow{f} \{1, e\} \xrightarrow{0} 0$ is not exact at $\mathbb{N}_0$, for Coker i is seen to be $\mathbb{N}_0$, while Coim $f = \{1, e\}$. //

Proposition 20: Let $0 \xrightarrow{0} A \xrightarrow{f} B$ be exact.

Let $p: B \longrightarrow \text{Coker } f$ be the natural map.

Then $0 \xrightarrow{0} A \xrightarrow{f} B \xrightarrow{p} \text{Coker } f$ is not necessarily exact at B.

Proof: Take $0 \xrightarrow{0} \langle 1 \rangle' \xrightarrow{f} \mathbb{N}_0$ where f is the natural injection. It will be shown in § 5, Theorem 4 that this is exact. Now it is easily checked that Coker f = 0 and thus Ker $p = \mathbb{N}_0 \neq \langle 1 \rangle' = \text{Im } f$. Thus, $0 \xrightarrow{0} \langle 1 \rangle' \xrightarrow{f} \mathbb{N}_0 \xrightarrow{p} \text{Coker } f$ is not exact at $\mathbb{N}_0$. //

Proposition 21: Coreflection into $\mathcal{Ab}$, $\mathcal{L}$, or $\mathcal{J}$ does not necessarily preserve exactness.

Proof: Let $M = \mathbb{N}_0 \cup \{e\}$, where $e + n = n + e = e + e = e$ for any $n \in \mathbb{N}_0$. Let $f: \mathbb{N}_0 \longrightarrow M$ by $n \longmapsto n$. Then $0 \xrightarrow{0} \mathbb{N}_0 \xrightarrow{f} M$ is exact (see Proposition 15).

It is easily checked that the sequence when coreflected into $\mathcal{J}$ or $\mathcal{L}$ becomes $0 \xrightarrow{0} \mathbb{N}_0 \xrightarrow{0} 0$, which is not exact; and when coreflected into $\mathcal{Ab}$ becomes $0 \xrightarrow{0} \mathbb{Z} \xrightarrow{0} 0$, which is not exact. //

§ 4: Hom (A, B)

Notation: As expected, for each $A, B \in \mathcal{A}$, the set of all monoid homomorphisms is denoted Hom (A, B). //

Proposition 22: Let $A, B \in \mathcal{A}$.

Define the binary operation $\circ$ in Hom (A, B) by $f \circ g : a \longmapsto f(a)g(a)$.

Define $0: A \longrightarrow B$ by $a \longmapsto 1$.

Then $(\mathrm{Hom}(A, B), \circ, 0) \in \mathcal{A}$.

Proof: Clear. //

Corollary: $\mathcal{A}$ is a semiadditive category. //

Proposition 23: Let $A \in \mathcal{A}$, $B \in \mathcal{L}$.

Let $\mathcal{L}(A)$ be the coreflection of A into $\mathcal{L}$.

Then $\mathrm{Hom}(A, B) \cong \mathrm{Hom}(\mathcal{L}(A), B)$.

Proof: For each $f \in \mathrm{Hom}(A, B)$, define $f': \mathcal{L}(A) \longrightarrow B$ by $[a] \longmapsto f(a)$, where $[a]$ is the congruence class containing a (see Proposition 3). It is easily checked that f' is well defined and that $f' \in \mathrm{Hom}(\mathcal{L}(A), B)$.

The mapping $f \longmapsto f'$ is routinely seen to be an isomorphism. //

Proposition 24: Let $f \in \mathrm{Hom}(A, B)$.

Then the following are equivalent:

1. $f \in \mathrm{Hom}(A, B)^*$.
2. $f_*(A) \subseteq B^*$.

Proof: Easy. //

Proposition 25: Let $M \in \mathcal{A}$.

Then the following are equivalent:

1. $\mathrm{id} \in \mathrm{Hom}(M, M)^*$.
2. M is a group.
3. $\mathrm{Hom}(M, M)$ is a group. //

Proof: Clear. //

Lemma 6: Let $B \in \mathcal{A}$

Then $B \cong \mathrm{Hom}(\mathcal{N}_o, B)$.

Proof: For each $b \in B$, define $f_b: \mathcal{N}_o \longrightarrow B$ by $n \longmapsto b^n$. Then it is routinely checked that the mapping $b \longmapsto f_b$ is an isomorphism from B into $\mathrm{Hom}(\mathcal{N}_o, B)$. //

Theorem 3: Let $A, B \in \mathcal{A}$.

Then: 1. $B \in \mathcal{A}b \Longrightarrow \mathrm{Hom}(A, B) \in \mathcal{A}b$.

2. $B \in \mathcal{L} \Longrightarrow \mathrm{Hom}(A, B) \in \mathcal{L}$.

3. $B \in \mathcal{J} \Longrightarrow \mathrm{Hom}(A, B) \in \mathcal{J}$.

4. $A \in \mathcal{A}b \Longrightarrow \mathrm{Hom}(A, B) \in \mathcal{A}b$.

5. $A \in \mathcal{L} \nRightarrow \mathrm{Hom}(A, B) \in \mathcal{L}$

6. $A \in \mathcal{J} \nRightarrow \mathrm{Hom}(A, B) \in \mathcal{J}$

7. $\mathrm{Hom}(A, B) \in \mathcal{A}b \nRightarrow A \in \mathcal{A}b$ or $B \in \mathcal{A}b$.

8. $\mathrm{Hom}(A, B) \in \mathcal{L} \nRightarrow B \in \mathcal{L}$.

9. $\mathrm{Hom}(A, B) \in \mathcal{J} \Longrightarrow A \in \mathcal{A}b$ or $B \in \mathcal{J}$.

Proof:

1. Clear from Proposition 24.
2. Easy.
3. Easy.
4. Clear from Proposition 24.
5. Let $M \in \mathcal{A} \setminus \mathcal{L}$. By Lemma 6, $\mathrm{Hom}(\mathcal{N}_o, M) \cong M \in \mathcal{L}$ even though $\mathcal{N}_o \in \mathcal{L}$.
6. Let $M \in \mathcal{A} \setminus \mathcal{J}$. By Lemma 6, $\mathrm{Hom}(\mathcal{N}_o, M) \cong M \notin \mathcal{J}$

7. Let $H = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$ be considered multiplicatively. Clearly, $H, \aleph_0 \in \mathcal{A} \setminus \mathcal{A}b$.

Let $f \in \mathrm{Hom}(H, \aleph_0)$. Suppose $f \neq 0$. Then there exists $a \in H$ such that $f(a) = n \neq 0$, $a \neq 1$. Then $n = f(a) = f((\sqrt[2n]{a})^{2n}) = 2n\, f(\sqrt[2n]{a})$, $\sqrt[2n]{a} \in H$, and so $f(\sqrt[2n]{a}) = \frac{1}{2} \notin \aleph_0$. Thus $f = 0$. Hence, $\mathrm{Hom}(H, \aleph_0) \in \mathcal{A}b$.

8. Take $A \in \mathcal{A}b$, $B \in \mathcal{A} \setminus \mathcal{L}$. Then the result is clear by Proposition 24.

9. Assume $A \notin \mathcal{A}b$.

Suppose $B \notin \mathcal{J}$. Then there exists $n \in B$ such that $n^2 = n \neq 1$. Define $f: A \longrightarrow B$ by $a \longmapsto 1$ if $a \in A^*$ and $a \longmapsto n$ if $a \notin A^*$. Then it is routinely checked that $f \in \mathrm{Hom}(A, B)$, $f^2 = f$, and thus $f = 0$. Hence $A = A^*$. But this contradicts our assumption. //

§ 5: Free Abelian Monoids

Proposition 26: Let I be a set.
Let $F = \bigoplus_{i \in I} \aleph_0^{(i)}$, where $\aleph_0^{(i)} = \aleph_0$ for any $i \in I$.
Then F is the free abelian monoid on $|I|$ generators.

Proof: See Chevalley [2; Chapter 1, § 6]. //

Corollary: The free objects of $\mathcal{A}$, $\mathcal{J}$, and $\mathcal{L}$ coincide. //

The remainder of this section will be devoted to a small study of the structure of submonoids of the free monoids.

Theorem 4: Let F be a free abelian monoid.

Let $N < F$ and $f: N \longrightarrow F$ be the natural map.

Then $0 \xrightarrow{0} N \xrightarrow{f} F$ is exact.

Proof: We must show that Coim $f = N$. We know that $N < \text{Coim } f < F$.

Suppose $N \neq \text{Coim } f$. Now, let $F = \bigoplus_{i\in I} \mathbb{N}_0^{(i)}$ and choose $(n_i)_{i\in I} \in \text{Coim } f \setminus N$ such that $\sum_{i\in I} n_i \leq \sum_{i\in I} m_i$ for any $(m_i)_{i\in I} \in \text{Coim } f \setminus N$. Let $M = \left\{ (a_i^{x_i})_{i\in I} \mid (x_i)_{i\in I} \in \text{Coim } f \right\} \cup \left\{ (b_i^{n_i})_{i\in I} \right\}$ with $(b_i^{x_i})^2_{i\in I} = (a_i^{2n_i})_{i\in I}$ and $(b_i^{n_i})_{i\in I} (a_i^{x_i})_{i\in I} = (a_i^{x_i + n_i})_{i\in I}$ for any $(x_i)_{i\in I} \in \text{Coim } f \setminus 0$. Clearly $M \in \mathcal{A}$.

Define g: Coim $f \longrightarrow M$ by $(x_i)_{i\in I} \longmapsto (a_i^{x_i})_{i\in I}$ and

h: Coim $f \longrightarrow M$ by $(x_i)_{i\in I} \mapsto \begin{cases} (a_i^{x_i})_{i\in I}, & \text{if } (x_i)_{i\in I} \neq (n_i)_{i\in I} \\ (b_i^{n_i})_{i\in I}, & \text{if } (x_i)_{i\in I} = (n_i)_{i\in I}. \end{cases}$

To ensure that $h \in \text{Hom}(\text{Coim } f, M)$, we need check only that $(x_i)_{i\in I}$, $(y_i)_{i\in I} \in \text{Coim } f$, $(x_i)_{i\in I} + (y_i)_{i\in I} = (n_i)_{i\in I} \Rightarrow x_i = 0$ for any i or $y_i = 0$ for any i. Now, $(x_i)_{i\in I}, (y_i)_{i\in I} \in N$ would imply $(n_i)_{i\in I} \in N$ -- a contradiction. So without loss of generality, we may assume $(x_i)_{i\in I} \notin N$. It follows that $\sum_{i\in I} n_i \leq \sum_{i\in I} x_i$. But $(x_i)_{i\in I} + (y_i)_{i\in I} = (n_i)_{i\in I}$ implies that $x_i \leq n_i$ for any i. Moreover, if $x_i < n_i$ for some i, then we get $\sum_{i\in I} x_i < \sum_{i\in I} n_i \leq \sum_{i\in I} x_i$, which is impossible. Hence, $x_i = n_i$ for any i and so $(y_i)_{i\in I} = 0$. Thus, h is a morphism of monoids. Define f': $N \longrightarrow$ Coim f to be the natural map. Then we have $gf' = hf'$, f' an epimorphism, and so $g = h$. In particular, $g((n_i)_{i\in I}) = h((n_i)_{i\in I})$ and we have our contradiction. //

Corollary 1: Let F be a free abelian monoid.

Let $F' = F \cup \{e\}$, where e is an adjoined zero.

Let $N < F'$ and $f: N \longrightarrow F'$ be the natural map.

Then $0 \xrightarrow{0} N \xrightarrow{f} F'$ is exact.

Proof: If $e \notin N$, then the result follows from Proposition 15.

If $e \in N$, then the result follows from Proposition 16. //

Corollary 2: Let $\mathbb{N}_0$ be considered multiplicatively.

Let $N < \mathbb{N}_0$ and let $f: N \longrightarrow \mathbb{N}_0$ be the natural map.

Then $0 \xrightarrow{0} N \xrightarrow{f} \mathbb{N}_0$ is exact.

Proof: We need only note that $\mathbb{N}_0 \cong (\bigoplus_{i \in \mathbb{N}} \mathbb{N}_0^{(i)}) \cup \{e\}$. //

It is well known that any subgroup of a free abelian group is free, while it is easy to find a non-free submonoid of a free abelian monoid. It would seem to be instructive therefore to look at the free submonoids of free abelian monoids. Many things can indeed be said on this topic, of which the following are perhaps the most noteworthy.

Proposition 27: Let $n \in \mathbb{N}$.

Let $N < \bigoplus_{i=1}^{n} \mathbb{N}_0^{(i)} = F$.

Then the following are equivalent:

1. $N \cong F$.
2. There exist $a_{ij} \in \mathbb{N}_0$, $i, j = 1, \ldots, n$ such that

   i $N = \left\{ \left(\sum_{j=1}^{n} a_{1j}x_j, \ldots, \sum_{j=1}^{n} a_{nj}x_j \right) \;\middle|\; x_1, \ldots, x_n \in \mathbb{N}_0 \right\}$

   ii $\begin{vmatrix} a_{11}, & \ldots, & a_{1n} \\ \vdots & & \vdots \\ a_{n1}, & \ldots, & a_{nn} \end{vmatrix} \neq 0.$

Proof: 2 $\Rightarrow$ 1): Let such a_{ij} exist.

Define $f: F \longrightarrow N$ by $(x_1, \ldots, x_n) \longmapsto (\sum_{j=1}^{n} a_{ij}x_j, \ldots, \sum_{j=1}^{n} a_{nj}x_j)$.

It is clear that f is a well-defined onto monoid homomorphism. We thus need only show that f is 1 - 1. But the fact that the determinant is not zero is quickly seen to ensure this.

1 $\Rightarrow$ 2): Let $f: F \longrightarrow N$ be an isomorphism.

Let $(0, \ldots, 0, 1, 0, \ldots, 0) \longmapsto (a_{1j}, \ldots, a_{nj})$ where the 1 is in the j^{th} component. Then it is clear that N is as described in i.

Suppose the required determinant is zero. Then the system

$$\begin{aligned} a_{11} z_1 + \ldots + a_{1n} z_n &= 0 \\ &\vdots \\ a_{n1} z_1 + \ldots + a_{nn} z_n &= 0 \end{aligned}$$

has a non-trivial solution in $\mathbb{Q}$ and hence a non-trivial solution in $\mathbb{Z}$. Let $(z_1, \ldots, z_n)$ be a non-trivial solution in $\mathbb{Z}$. Define $x_i = z_i$ if $z_i \geq 0$, $x_i = 0$ if $z_i < 0$, $y_i = 0$ if $z_i \geq 0$ and $y_i = -z_i$ if $z_i < 0$. Then it is easily seen that $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$ are distinct elements of F whose images under f are the same. But this contradicts the fact that f is 1 - 1. //

Corollary: Let $N < \aleph_0$.

Then the following are equivalent:

1. $N \tilde{=} \aleph_0$.
2. There exists $n \in \aleph_0$ such that $N = \langle n \rangle$.
3. $N \not\cong \aleph_0$.

Proof: 1 $\Leftrightarrow$ 2): Clear.

2 $\Leftrightarrow$ 3): Easy. //

The fact that the free submonoids of $\mathbb{N}_o$ are exactly the connected submonoids is a situation not found in the free abelian monoids on more than one generator.

That connected submonoids are not necessarily free is seen by considering the submonoid N of $\mathbb{N}_o \oplus \mathbb{N}_o$, where $N = \{ (3a + c, 3b + c) \mid a, b, c \in \mathbb{N}_o \}$.

That free submonoids are not necessarily connected can be deduced from the proposition above and the one below.

Proposition 28: Let $\mathbb{N}_o \oplus \mathbb{N}_o \cong N < \mathbb{N}_o \oplus \mathbb{N}_o$.

Then the following are equivalent:

1. $N \not\leq \mathbb{N}_o \oplus \mathbb{N}_o$.
2. There exist $\alpha, \beta \in \mathbb{N}$ such that $N = \{ (\alpha x, \beta y) \mid x, y \in \mathbb{N}_o \}$.

Proof: 2 $\Rightarrow$ 1): Obvious

1 $\Rightarrow$ 2): Assume N is connected.

Now, we know that there exist $a, b, c, d \in \mathbb{N}_o$ such that $ad - bc \neq 0$ and $N = \{ (ax + by, cx + dy) \mid x, y \in \mathbb{N}_o \}$ (Proposition 27).

Suppose $a, b, c, d \neq 0$. Let $n \in \mathbb{N}$ such that $n \geq a/b$, $n \geq c/d$. Then $(bn - a, dn - c) \in \mathbb{N}_o \oplus \mathbb{N}_o$ and $(a, c) + (bn - a, dn - c) = (bn, dn)$, where $(a, c), (bn, dn) \in N$. Since N is connected, it follows that $(bn - a, dn - c) \in N$. This is easily shown to be impossible, and so one of a, b, c, d is zero.

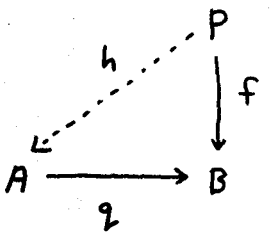
Without loss of generality, assume $d = 0$. Since $ad \neq bc$, we have $b \neq 0$, $c \neq 0$. It remains to show that $a = 0$.

Suppose $a \neq 0$. Then let $n \in \mathbb{N}$ such that $n \geq b/a$. It follows that $(an - b, cn) \in \mathbb{N}_o \oplus \mathbb{N}_o$, $(b, 0) + (an - b, cn) = (an, cn)$, $(b, 0), (an, cn) \in N$, and hence $(an - b, cn) \in N$. But this is easily

shown to be impossible. //

§ 6: Projectives

Definition 3: Let $P \in \mathcal{A}$.



Then we say that P is projective if and only if for each $f: P \longrightarrow B$ and for each epimorphism $q: A \longrightarrow B$, there exists $h: P \longrightarrow A$ such that $f = qh$.

We say that P is extremally projective if and only if for each $f: P \longrightarrow B$ and for each extremal epimorphism $q: A \longrightarrow B$, there exists $h: P \longrightarrow A$ such that $f = qh$. //

Lemma 7: Let $(P_i)_{i \in I}$ be a family of abelian monoids.

Then $\bigoplus_{i \in I} P_i$ is projective (extremally projective) if and only if P_i is projective (extremally projective) for any $i \in I$.

Proof: Routine. //

We introduce the definition below in order to facilitate the proof of the lemma that follows. It may as well be noted here that that lemma will be seen to be the main result which allows us to identify all the projectives and extremal projectives in $\mathcal{A}$, $\mathcal{S}$, and $\mathcal{L}$.

Definition 4: Let $x \in M \in \mathcal{A}$, where M is written additively.

Then the height of x in M, denoted M-ht (x), is given by $\sup \{ n \in \mathbb{N}_0 \mid \exists\, x_1, \ldots, x_n \in M \setminus \{0\} \cdot \ni \cdot x = x_1 + \ldots + x_n \}$. //

Example: $\mathbb{N}_0$ - ht (n) = n for any $n \in \mathbb{N}_0$.

$\mathbb{Z}$ - ht (x) = ∞ for any $x \in \mathbb{Z}$ //

Lemma 8: Let $P \in \mathcal{A}$ and let P be written additively.

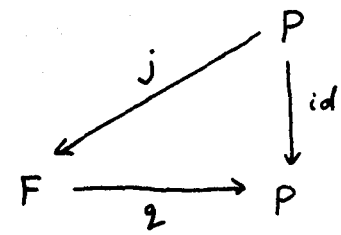
Let $F = \bigoplus_{i \in P} \mathbb{N}_0^{(i)}$, where $\mathbb{N}_0^{(i)} = \mathbb{N}_0$ for any $i \in P$.

Let $q: F \longrightarrow P$ by $(x_i)_{i \in P} \longmapsto \sum_{i \in P} x_i i$.

Let $j: P \longrightarrow F$ such that $id_P = pj$.

Then P is free.

Proof: Since $id = pj$, then it is clear that j is 1 - 1, and so P is isomorphic to a submonoid of F. It follows easily that every element of F and of P has finite height.



Let $x \in P \setminus \{0\}$. Then there exists $n \in \mathbb{N}$, $x_1, \ldots, x_n \in P \setminus \{0\}$ such that $x = x_1 + \ldots + x_n$, with n maximal. Now, $j(x) = j(x_1) + \ldots + j(x_n)$, and $j(x_i) = 0$ implies $x_i = 0$ (since j is 1 - 1), which is false. Thus F - ht (j(x)) $\geq$ P - ht (x). Let F - ht(x) = m. Then, there exist $y_1, \ldots, y_m \in F \setminus \{0\}$ such that $j(x) = y_1 + \ldots + y_m$, whence $x = q(y_1) + \ldots + q(y_m)$. Now we know that $m \geq n$. Suppose $m \neq n$. Then, without loss of generality, we may assume $q(y_m) = 0$. But we note that P is isomorphic to a submonoid of F, and this, together with the definition of q, is easily seen to imply that Ker $q = \{0\}$. Hence, $y_m = 0$ and we have our contradiction.

Thus, F - ht (j(x)) = P - ht (x), for any $x \in P$.

Now, every non-zero element of P is a sum of elements of height one, and so P is generated by its height one elements. Moreover, each such element has as its image under j a height one element which must

then be of the form $(u_i)_{i \in P}$, where $u_i = 0$ for all $i \in P$ except $i = i'$, and $u_{i'} = 1$. It follows easily that $j_*(P)$, and hence P, is free. //

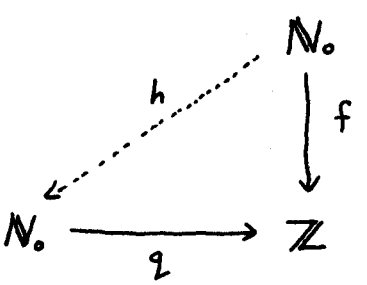
Theorem 5: Let $P \in \mathcal{P}$.

Then: 1. P is extremally projective if and only if P is free.

2. P is projective if and only if P is trivial.

Proof: 1. Assume P is extremally projective. Then P has the properties given in Lemma 8, and so P is free. On the other hand, it is easy to show that $\mathbb{N}_0$ is extremally projective and so, by Lemma 7, every free abelian monoid is extremally projective.

2. That the trivial monoid is projective is obvious. Assume P is projective. It is then again seen by Lemma 8 that P is free. Suppose P is not trivial. Then by Lemma 7, $\mathbb{N}_0$ is projective. Define $f: \mathbb{N}_0 \to \mathbb{Z}$ by $n \longmapsto -n$, and $q: \mathbb{N}_0 \to \mathbb{Z}$ by $n \longmapsto n$. By Lemma 3, q is an epimorphism. Since $\mathbb{N}_0$ is projective, there exists $h: \mathbb{N}_0 \to \mathbb{N}_0$ such that $f = qh$. In particular, $-1 = f(1) = q(h(1)) = h(1)$. Thus, $-1 \in \mathbb{N}_0$ which is clearly nonsense. //



Corollary 1: The theorem remains true when stated within $\mathcal{J}$ or within $\mathcal{L}$.

Proof: Clear. //

Corollary 2: A direct summand of a free abelian monoid is free.

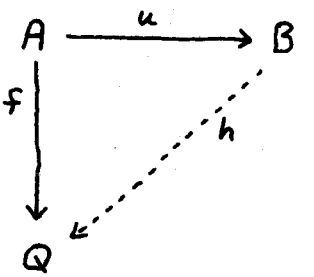
Proof: Let $F = A \oplus B$, F free.

Then F is extremally projective, whence A is extremally projective (Lemma 7), and so A is free. //

§ 7: Injectives

Definition 5: Let $Q \in \mathcal{A}$.

Then we say Q is injective if and only if for each $f: A \longrightarrow Q$ and for each monomorphism $u: A \longrightarrow B$, there exists $h: B \longrightarrow Q$ such that $f = hu$.



We say Q is extremally injective if and only if for each $f: A \longrightarrow Q$ and for each extremal monomorphism $u: A \longrightarrow B$, there exists $h: B \longrightarrow Q$ such that $f = hu$. //

Lemma 9. Let $Q \in \mathcal{A}b$.

Then the following are equivalent:

1. Q is a divisible group.
2. Q is $\mathcal{A}b$-injective.
3. Q is extremally injective in $\mathcal{A}b$.

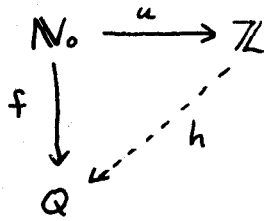
Proof: 1 $\Leftrightarrow$ 2): See Lambek [5; Chapter 4, § 4.2].

2 $\Leftrightarrow$ 3): It is well known that $u: A \longrightarrow B$ is an $\mathcal{A}b$-monomorphism if and only if it is an extremal monomorphism in $\mathcal{A}b$. //

Proposition 29: Let $Q \in \mathcal{A}$ ($\mathcal{J}$, $\mathcal{L}$) such that Q is injective ($\mathcal{J}$-injective, $\mathcal{L}$-injective).

Then Q is a divisible group.

Proof: Suppose Q is not a group.



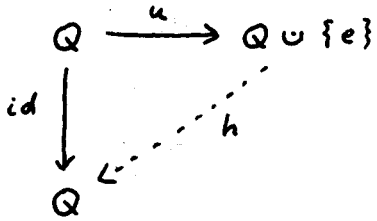
Then there exists $a \in Q \setminus Q^*$. Define $f: \mathbb{N}_0 \longrightarrow Q$ by $n \longmapsto a^n$. Define $u: \mathbb{N}_0 \longrightarrow \mathbb{Z}$ by $n \longmapsto n$. Then there exists $h: \mathbb{Z} \longrightarrow Q$ such that $f = hu$. In particular, $a = f(1) = (hu)(1) = h(1)$, and so $h(1) \notin Q^*$. But $\mathbb{Z}$ a group implies $h_*(\mathbb{Z}) \subseteq Q^*$. Thus we have a contradiction and so Q is a group.

Moreover, it follows that Q is $\mathcal{A}$b-injective. By Lemma 9, Q is a divisible group. //

Theorem 6: Let $Q \in \mathcal{A}$ such that Q is extremally injective.

Then $Q = \{1\}$ or Q contains a zero.

Proof: Let $u: Q \longrightarrow Q \cup \{e\}$ be the natural map, where e is an adjoined zero. Now u is an extremal monomorphism (Proposition 15). Thus, there exists $h: Q \cup \{e\} \longrightarrow Q$ such that $id = hu$. Also, $h(a) = a$ for any $a \in Q$ is clear.



Now, $h(e)a = h(e)h(a) = h(ea) = h(e)$ for any $a \in Q$. Thus either $h(e)$ is a zero of Q, or $h(e) = 1$ and so $a = 1 \; \forall \; a \in Q$. //

Theorem 7: Let $Q \in \mathcal{A}$.

Then Q is injective if and only if Q is trivial.

Proof: That $\{1\}$ is injective is clear.

Assume Q is injective. Then Q is extremally injective and so Q is trivial or contains a zero. (Theorem 6). But Q injective implies Q is a divisible group (Proposition 29). Hence, Q is trivial. //

Lemma 10: Let Q be a divisible group.

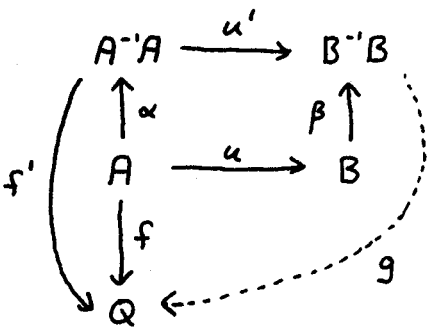
Let $f: A \longrightarrow Q$.

Let $u: A \longrightarrow B$ be a monomorphism such that its coreflection into $\mathcal{A}b$ is also a monomorphism.

Then there exists $h: B \longrightarrow Q$ such that $f = hu$.

Proof: Let $\alpha: A \longrightarrow A^{-1}A$ and $\beta: B \longrightarrow B^{-1}B$ be the natural maps, and $u': A^{-1}A \longrightarrow B^{-1}B$ be the induced map.

Let $f': A^{-1}A \longrightarrow Q$ by $x/y \longmapsto f(x)\, f(y)^{-1}$. It is easily seen that f' is well defined and that $f = f'\alpha$.



Now Q is $\mathcal{A}b$-injective (Lemma 9). Thus, there exists $g: B^{-1}B \longrightarrow Q$ such that $f' = gu'$, whence $f'\alpha = gu'\alpha$, $f = gu'\alpha$, and so $f = (g\beta)u$ (as $u'\alpha = \beta u$ is easily checked). //

Theorem 8: Let $Q \in \mathcal{I}$.

Then Q is $\mathcal{I}$-injective if and only if Q is a divisible group.

Proof: Assume Q is $\mathcal{I}$-injective. Then Proposition 29 ensures that Q is a divisible group.

Assume Q is a divisible group. Now, if $A, B \in \mathcal{I}$ and

u: $A \longrightarrow B$ is a monomorphism, then it is readily checked that its coreflection into $\mathcal{A}\, b$ is also a monomorphism. Hence, Lemma 10 applies and we are done. //

BIBLIOGRAPHY

1. Birkhoff, Garrett, Lattice Theory, Revised Edition, American Mathematical Society, Providence, (1948).

2. Chevalley, Claude, Fundamental Concepts of Algebra, Academic Press, New York, (1956).

3. Clifford and Preston, The Algebraic Theory of Semigroups, Volume 1, American Mathematical Society, Providence, (1961).

4. Herrlich, Horst, Topogolische Reflexionen und Coreflexionen, Lecture Notes in Mathematics, Volume 78, (1968), Springer-Verlag, Berlin.

5. Lambek, Joachim, Lectures on Rings and Modules, Blaisdell, Toronto, (1966).

6. Lang, Serge, Algebra, Addison-Wesley, Reading (1967).

7. Maury, M. Guy, La Condition "Intégralement Clos" dans Quelques Structures Algébriques, Ann. Scient. Ec. Norm. Sup., 3^{e} série, t. 78, 1961, p. 31 à 100.

8. Mitchell, Barry, Theory of Categories, Academic Press, New York, (1965).

9. Poyatos, Suarez Francisco, Formulas of Length for Commutative Semigroups, Rev. Mat. Hisp.-Amer. (4), 28, (1968), p. 95-127.

10. Shershin, Anthony C; Moore, John T., Direct Summands of Abelian Monoids, Math. Notae, 20, (1965), p. 109-116.