Spring 3-5-2020

Groups of Divisibility

Seth J. Gerberding
University of South Dakota

Groups of Divisibility

by

Seth Gerberding

A thesis submitted in partial fulfillment
of the requirements for the
University Honors Program

Department of Mathematical Sciences
The University of South Dakota
May 2020

The members of the Honors Thesis Committee appointed
to examine the thesis of Seth Gerberding
find it satisfactory and recommend that it be accepted.

Dr. Ramiro Lafuente-Rodriguez
Department of Mathematical Sciences
Director of the Committee

Dr. Gabriel Picioroaga
Department of Mathematical Sciences

Dr. Dan Van Peursem
Department of Mathematical Sciences

ABSTRACT

Groups of Divisibility

Seth Gerberding

Director: Ramiro Lafuente-Rodriguez, Ph.D.

In this thesis, we examine a part of abstract algebra known as Groups of Divisibility. We construct these special groups from basic concepts. We begin with partially-ordered sets, then build our way into groups, rings, and even structures akin to rings of polynomials. In particular, we explore how elementary algebra evolves when an ordering is included with the operations. Our results follow the work done by Anderson and Feil [1], however we include more explicit proofs and constructions. Our primary results include proving that a group of divisibility can be provided with an order to make it a partially-ordered group; that every Bezout domain is a pseudo-Bezout domain; and that an integral domain is a pseudo-Bezout domain if and only if the partial order on its group of divisibility is a lattice.

KEYWORDS: Lattice, Divisibility, Order, Abstract algebra

Contents

1 Introduction

In this thesis, we explore a part of abstract algebra called *groups of divisibility*. These groups clearly have to do with divisibility, but what divisibility is in an algebraic sense is unclear. As it turns out, there is a rich way to conceptualize divisibility. It involves order. To help fuel intuition, consider a classic concept that addresses divisibility: the greatest common divisor (or greatest common factor).

For two numbers $a, b \in \mathbb{N}$, the greatest common divisor is a number d such that d divides both a and b, and if there is another number c that also divides a and b, then it also divides d. Of course, it follows that d is also greater than c.

But notice how the greatest common divisor is not defined using order. Order may intuitively be there, but it is not in the formal definition. But there still appears to be some kind of relationship between divisibility and order, at least with the greatest common divisor (and the least common multiple). In this thesis, we formalize this relationship by using algebraic structures with the inclusion of order. But to do so, we have to understand order.

Algebra, historically, has endeavoured to build up definitions and concepts that were intuitively used in prior mathematics. For example, we have groups, which are sets with an operation. Groups are fascinating structures, but have limitations with more complicated structures like the Real Numbers. With the Real Numbers we have more than one operation. Thus, to better understand the Real Numbers algebraically, we created rings, integral domains, and fields. But if we think about the Real Numbers a bit more, we find that order has still not been analyzed in an algebraic way. Some numbers are considered greater than or less than other numbers. The same can be said about functions: some functions are greater than others, either point wise or with respect to degree. This thesis explores the way ordering has been introduced into algebra, and specifically how it relates to divisibility.

Just like many other components of algebra, we will begin with groups and then move on to higher structures. However, before we begin with groups, we address order

more formally by discussing partially ordered sets and lattices. These special sets are in a way similar to groups and other algebraic structure: they include a set, but instead of an operation, they are equipped with a binary relation that has certain proprieties. Once partially-ordered sets are properly understood, then we can equip operations.

The concepts we cover, while deeply theoretical, actually have a wide range of applications. These applications extend well beyond merely enhancing already established uses. Lattices, for example, are useful for understanding circuit switches [9]. The work done, therefore, is more than theoretical: there is a great potential for powerful applications.

Section 2 goes over some background, including what is meant for something to be an order and what joins and meets are. Section 3 discusses lattices, section 4 addresses *l-groups* and proves some properties thereof. Section 5 extends the notions of homomorphisms and subgroups to l-groups. Section 6 addresses groups of divisibility. Finally, section 7 provides an example of our concepts at work. We follow the work done by Krull [8], Jaffard [6] and Ohm [10] to explore groups of divisibility.

We refer the reader, regarding basic algebraic concepts and notation, to Dummit and Foot [4], Hernstein [5], and Rotman [11], and for concepts and notation in lattice-ordered groups and rings: Anderson and Feil [1], Darnell [3] and Medvedev and Kopytov[7].

2 Partially Ordered Sets

A partial order consists of two things: a set and an ordering, denoted by "$\leq$". [1] This ordering *must be defined* because it is not obvious what is means to be less than or equal in all instances. However, whatever the definition of "$\leq$" is, in order to be a partial order it must fulfill three properties.

Definition 2.1. *A partial order, denoted by "$\leq$", is a binary relation between two elements a and b such that the ordering is:*

[1] Similarly, we may use $''\geq''$.

1. *Reflexive:* $a \leq a$

2. *Transitive: if* $a \leq b$ *and* $b \leq c$*, then* $a \leq c$*, and*

3. *Antisymmetric: if* $a \leq b$ *and* $b \leq a$*, then* $a = b$*.*

When we include this ordering on a set, we arrive at a *partially ordered set.*

Example 2.2. *Consider the power set on the set* $A = \{1, 2\}$*. Define the ordering as follows:* $X \leq Y$ *if and only if* $X \subseteq Y$*. Clearly, this relation defines a partial order.*

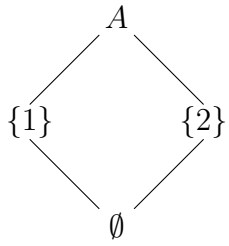

Figure 1

For example, as shown in Figure 1, by the ordering, $\{1\} \leq A$ *and* $\{2\} \leq A$*. Similarly,* $\emptyset \leq \{1\}$ *and* $\emptyset \leq \{2\}$*. However,* $\{1\} \not\leq \{2\}$ *and* $\{2\} \not\leq \{1\}$ *because* $\{1\}$ *and* $\{2\}$ *are "incomparable."*

One thing to note is that two elements may not be related in any way, just as $\{1\}$ and $\{2\}$ were in the last example. The only requirement for a partially ordered set is that every element be related to at least one other element, i.e., that they are "in the structure."

Next, we add more conditions onto a partially ordered set to create what we call a *lattice.*

3 Lattices

With a lattice, we introduce two new concepts called the *"meet"* and *"join"*, denoted by $\wedge$ and $\vee$ respectively, which are defined below.

Definition 3.1. *Let A be a partially ordered set with $a, b \in A$. Then, $a \wedge b$ is an element $c \in A$ such that:*

- *$c \leq a$ and $c \leq b$ and*
- *For $c' \in A$, if $c' \leq a$ and $c' \leq b$, then $c' \leq c$*

Similarly, $a \vee b$ is an element c in A such that:

- *$a \leq c$ and $b \leq c$ and*
- *For $c' \in A$ such that $a \leq c'$ and $b \leq c'$, then $c \leq c'$.*

Definition 3.2. *Let A be a lattice, where $a_i \in A$, for $1 \leq i \leq n$. Then, $\bigvee a_i = a_1 \vee a_2 \vee ... \vee a_n$. Similar notation applies for meets.*

The join is commonly called the *least upper bound*, and the meet is the *greatest lower bound*. That is, the join is the smallest element that is greater than both a and b. Similarly, the meet is the greatest element that is smaller than both a and b.

An analogous concept is the supremum and infimum. The supremum is also considered the least upper bound and the infimum the greatest lower bound. However, the supremum and infimum can be take over an *entire set*, such as $(0, 1]$, whereas the join and meet can be defined over only two elements.

We define a lattice.

Definition 3.3. *$(A, \leq)$ is a lattice if, for every $a, b \in A$, there exists $a \vee b \in A$ and $a \wedge b \in A$.*

An example of a lattice would be the real numbers, $(\mathbb{R}, \leq)$, where the ordering $\leq$ is the usual order defined below.

Definition 3.4. *For $x, y \in \mathbb{R}$, $x \leq y$ if there exists a nonnegative $z \in \mathbb{R}$ such that $x + z = y$.*

Take any two elements of $\mathbb{R}$. For reflexivity, $x \leq x$ is certainly true: simply let $z = 0$. Certainly the relation is transitive: if $x \leq y$, and $y \leq z$, then there exist positive $a, b \in \mathbb{R}$ such that $x + a = y$ and $y + b = z$. Then, $y + b = x + a + b = z$. Since a, b are positive, $a + b$ is positive, and thus $x \leq z$.

For antisymmetry, there are two ways to approach it, the formal way and the intuitive way. We shall address the intuitive way first. A binary relation, $*$, is *symmetric* if $x * y$, implies $y * x$. But a relation could be *antisymmetric*, where, if the two elements are related to each other, then they are equal. In $\mathbb{R}$, it certainly is the case that $\leq$ is antisymmetric: $3 \leq 5$, but $5 \not\leq 3$. Formally, a relation is antisymmetric if:

$$x * y \text{ and } y * x \text{ implies } x = y.$$

For $\mathbb{R}$, say $x \leq y$ and $y \leq x$. Then, as before, there exist positive $a, b \in \mathbb{R}$ such that $x + a = y$ and $y + b = x$. Then, $y + b + a = y$, and $b = -a$. However, if $a \neq 0$, we have a contradiction since b would be negative. Thus, $a = b = 0$, and $x = y$. Thus, we have a partial order on $\mathbb{R}$, and since for any two real numbers, one is always greater or equal to another, it constitutes a lattice.

This understanding of "$\leq$" is the classical sense. However, $\leq$ can be defined in many different ways. For example, in the set of positive integers we could say that $a \leq b$ iff $a|b$. It is not obvious that this definition constitutes a partial order, but this is just an example of a new way to define an ordering.

Finally, we are ready to extend orderings to groups.

4 Lattice-Ordered Groups

To reach lattice-ordered groups, we begin with a standard group from abstract algebra, $(G, +)$, where $+$ is not necessarily commutative. All the properties of groups, including inverses, identities, etc. are included. Now, we attach an ordering "$\leq$" such that $(G, \leq)$ is a partially ordered set. However, now we also require that this relation must be compatible with the group operation. This forms an l-group defined below.

Definition 4.1. *An* l-group*, denoted by* $(G, +, \leq)$ *is a set quipped with an operation and ordering such that:*

1. $(G, +)$ *is a group*
2. $(G, \leq)$ *is a lattice*
3. *The operation is compatible with the ordering. That is,* $a \leq b$ *implies* $a + c \leq b + c$ *and* $c + a \leq c + b$

We call these special groups *lattice-ordered groups*, or l-groups. To briefly pause and summarize: A group G, with an operation $+$, and an ordering $\leq$ is called partially ordered when the order is reflexive, transitive, and antisymmetric, and is denoted by $(G, +, \leq)$. This group is "upgraded" to a lattice-order group, or l-group, when, for any two elements in G, both their least upper bound and greatest lower bound are also in G. If we add the following condition, we get a *total order group.*

Definition 4.2. *Let* $(G, +, \leq)$ *be an l-group. Then,* $(G, +, \leq)$ *is a total order group if for every* $g, h \in G$*, either* $g \leq h$ *or* $h \leq g$*.*

Next, we prove an important property between the operation of the group and the order, namely that the group operation distributes over both join and meet.

Theorem 4.3. *Let* $(G, +, \leq)$ *be an l-group, and* $a, b, c, d \in G$*. Then:*

$$a + b \vee c + d = (a + b + d) \vee (a + c + d) \tag{4.0.1}$$

$$a + b \wedge c + d = (a + b + d) \wedge (a + c + d). \tag{4.0.2}$$

Proof. To prove these equalities, we shall show that that the left hand side is less than or equal to right hand side, then show the right hand is less than or equal to the left. Then, the two must be equal.

We start with the first equality. By join properties, $b \leq b \vee c$ and $c \leq b \vee c$. Then, we add a and d to both sides of the inequality:

$$a + b + d \leq a + (b \vee c) + d$$
$$a + c + d \leq a + (b \vee c) + d.$$

Since $a + (b \vee c) + d$ is greater than both $a + b + d$ and $a + c + d$, it must be either greater than the join of the two, or equal to it. So:

$$(a + b + d) \vee (a + c + d) \leq a + (b \vee c) + d. \tag{4.0.3}$$

Now we shall develop the inequality the other way. We begin with

$$a + b + d \leq (a + b + d) \vee (a + c + d)$$
$$a + c + d \leq (a + b + d) \vee (a + c + d).$$

In this case, we subtract a and d from both sides, so we have:

$$b \leq -a + (a + b + d) \vee (a + c + d) - d$$
$$c \leq -a + (a + b + d) \vee (a + c + d) - d.$$

Since the right hand side is greater than both b and c, it must either be greater than or equal to the join of b and c. That is:

$$b \vee c \leq -a + (a + b + d) \vee (a + c + d) - d.$$

Bringing a and d back to the left hand side, we have our result:

$$a + (b \vee c) + d \leq (a + b + d) \vee (a + c + d). \tag{4.0.4}$$

Inequalities (4.0.3) and (4.0.4) complete (1). The proof for (2) is nearly identical. □

Next, we prove De Morgan's laws for joins and meets.

Theorem 4.4. *Let $(G, +, \leq)$ be an l-group such that $a, b \in G$. Then:*

$$-(a \vee b) = -a \wedge -b, \tag{4.0.5}$$

and

$$-(a \wedge b) = -a \vee -b. \tag{4.0.6}$$

Proof. We are going to prove (1), and the proof of (2) is nearly identical. We begin with two inequalities stemming from joins: $a \leq a \vee b$ and $b \leq a \vee b$. Then, $-(a \vee b) \leq -a$ and $-(a \vee b) \leq -b$. Since $-(a \vee b)$ is less than both $-a$ and $-b$, it must be less than or equal to the meet of $-a$ and $-b$. That is:

$$-(a \vee b) \leq -a \wedge -b. \tag{4.0.7}$$

Next we prove the opposite inequality. We need to be a little creative, and begin with something different: $-a \wedge -b \leq -a$ and $-a \wedge -b \leq -b$. Then, taking inverses yields $a \leq -(-a \wedge -b)$ and $b \leq -(-a \wedge -b)$. By proprieties of joins, since $-(-a \wedge -b)$ is greater than both a and b, it must be greater than or equal to the join of a and b. Therefore, $a \vee b \leq -(-a \wedge -b)$. Finally, by taking inverses again, we arrive at:

$$-a \wedge -b \leq -(a \vee b). \tag{4.0.8}$$

□

Next we prove an useful proposition.

Proposition 4.5. *Let a, b be in an l-group. Then,*

$$a - (a \wedge b) + b = a \vee b.$$

Proof. The proof is straight forward, using Theorem 4.4 and distributive properties.

$$\begin{aligned} a - (a \wedge b) + b &= a + (-a \vee -b) + b \\ &= (0 \vee a - b) + b \\ &= b \vee a \\ &= a \vee b. \end{aligned}$$

□

Corollary 4.6. $a - (a \vee b) + b = a \wedge b$

Proof. Follows immediately from Proposition 4.5. □

Next, we give a few definitions.

Definition 4.7. *Let $g \in G$, where $(G, +, \leq)$ is an l-group.*

- *The positive part of g is $g \vee 0$, denoted by g^+;*
- *The negative part of g is $-g \vee 0$, denoted by g^-.*

Observe that $g + g^- = g + (-g \vee 0) = (0 \vee g) = g^+$. Similarly, $-g^- = -(-g \vee 0) = (g \wedge 0)$. Thus we arrive at the following equality:

$$g^+ \wedge g^- = (g + g^-) \wedge g^- = (g \wedge 0) + g^- = -g^- + g^- = 0. \tag{4.0.9}$$

We say two elements of an l-group are *disjoint* if $a \wedge b = 0$. Therefore, g^+ and g^- are disjoint. Quickly, we want to prove an important property about disjoint elements.

Proposition 4.8. *Let $(G, +, \leq)$ be an l-group such that $a \wedge b = 0$ for $a, b \in G$. Then, $a + b = a \vee b$.*

Proof. From Proposition 4.5, we have that $a - (a \wedge b) + b = a \vee b$. Since $a \wedge b = 0$, we arrive at $a + b = a \vee b$. □

Corollary 4.9. *Let g be an element of an l-group. Then $g^+ + g^- = g^+ \vee g^-$.*

Proof. By Equation (4.0.9), g^+ and g^- are disjoint. Then, by Proposition 4.8, $g^+ + g^- = g^+ \vee g^-$. □

With this proposition in hand, we can prove a version of the triangle inequality for l-groups. Absolute value, in this context, means $|g| = g^+ + g^-$.

Theorem 4.10. *Let $(G, +, \leq)$ be an l-group and $a, b \in G$. Then, $|a+b| \leq |a| + |b| + |a|$.*

Proof. We begin with $|a + b| = (a + b)^+ + (a + b)^- = (a + b) \vee 0 + (-b - a) \vee 0$. Next, observe that $a \leq a \vee 0$ and $b \leq b \vee 0$ yields $a + b \leq a \vee 0 + b \vee 0$. Similarly, we arrive at $0 \leq a \vee 0 + b \vee 0$. Therefore, $(a + b) \vee 0 \leq a \vee 0 + b \vee 0$. The same argument will hold for $(a + b)^-$. Thus, we can deduce:

$$\begin{aligned}(a + b) \vee 0 + (-b - a) \vee 0 &\leq a \vee 0 + b \vee 0 + -b \vee 0 + -a \vee 0 \\ &= a^+ + |b| + a^-.\end{aligned}$$

Since $|a| = a^+ \vee a^-$, we can conclude that $a^+ \leq |a|$ and $a^- \leq |a|$. Therefore:

$$a^+ + |b| + a^- \leq |a| + |b| + |a|.$$

□

Now we prove a new distributive property for l-groups. Earlier, we proved that the operation distributes over joins and meets in Theorem 4.3. This new distributive property is about joins over meets and vice versa.

Lemma 4.11. *If $a \leq (a \vee b)$, then $c \wedge a \leq c \wedge (a \vee b)$.*

Proof. Since $a \leq a \vee b$ and $c \wedge a \leq a$, we conclude that $c \wedge a \leq a \vee b$. Finally, since $c \wedge a \leq a$, we deduce that $c \wedge a \leq c \wedge (a \vee b)$. □

Theorem 4.12. *The lattice of an l-group is torsion free.*

Torsion free means that, for an element a in a set, there does not exist a positive integer n such that $na = 0$. An element has torsion if there does exist such an n. For example, $\mathbb{Z}_6$ has torsion because $2(3) = 0$. Before we prove this theorem, we prove a lemma pertaining to joins.

Lemma 4.13. *Let n be a positive natural number and g be an element of an l-group. Then, $n(g \vee 0) = ng \vee (n-1) \vee ... \vee g \vee 0$.*

Proof. We proceed by induction on n. The first case, $n = 1$, is obvious: $1(g \vee 0) = (g \vee 0)$. Now assume $k(g \vee 0) = kg \vee (k-1)g \vee .... \vee g \vee 0$. Then, for $k+1$, we get the following:

$$\begin{aligned}(k+1)(g \vee 0) &= k(g \vee 0) + (g \vee 0) \\ &= (kg \vee (k-1)g \vee .... \vee g \vee 0) + (g \vee 0) \\ &= (kg + (g \vee 0)) \vee (k-1)g + (g \vee 0) \vee ... \vee g + (g \vee 0) \vee 0 + (g \vee 0) \\ &= (k+1)g \vee kg \vee kg \vee ... \vee g \vee g \vee 0 \\ &= (k+1)g \vee kg \vee ... \vee 2g \vee g \vee 0.\end{aligned}$$

□

Proof of Theorem 4.12. Assume that $ng = 0$ for an element of G. Then, by Lemma 4.13:

$$\begin{aligned}n(g \vee 0) &= ng \vee (n-1)g \vee ... \vee g \vee 0 \\ &= (n-1)g \vee ... \vee g \vee 0.\end{aligned}$$

By applying Lemma 4.13 to the right hand side again, we arrive at:

$$n(g \vee 0) = (n-1)(g \vee 0) = n(g \vee 0) - (g \vee 0).$$

Thus $0 = -(g \vee 0)$, and $0 = g \vee 0$. We can apply the same argument to $-g$, and arrive

at $0 = -g \vee 0$. Therefore, $-g \leq 0$ and $g \leq 0$, so $g = 0$. $\square$

Lastly, we prove an important property pertaining to l-groups. We switch from additive to multiplicative notation for simplicity's sake in these longer computations.

Theorem 4.14. *The lattice of an l-group is distributive.*

Proof. We prove both distribution equalities, beginning with $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. First, by Lemma 4.11, $a \wedge (b \vee c) \geq a \wedge b$ and $a \wedge (b \vee c) \geq a \wedge c$. Therefore, $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$. Now we need only show that any other upper bound is greater than $a \wedge (b \vee c)$.

Say $m \geq (a \wedge b)$ and $m \geq (a \wedge c)$. Since $b \leq b \vee c$ and $c \leq b \vee c$, we deduce that $e \leq (b \vee c)b^{-1}$ and $e \leq (b \vee c)c^{-1}$. Then, $a \leq (b \vee c)b^{-1}a$, and $a \wedge (b \vee c) \leq (b \vee c)b^{-1}a \wedge (b \vee c)$. Then,

$$\begin{aligned}(b \vee c)b^{-1}a \wedge (b \vee c) &= (b \vee c)(b^{-1}a \wedge e) \\ &= (b \vee c)(b^{-1}a \wedge b^{-1}b) \\ &= (b \vee c)b^{-1}(a \wedge b)\end{aligned}$$

Similarly, we arrive at $(b \vee c)b^{-1}a \wedge (b \vee c) \leq (b \vee c)c^{-1}(a \wedge c)$.

Since $(a \wedge b) \leq b$, we conclude $a \wedge (b \vee c) \leq (b \vee c)b^{-1}m$ and similarly $a \wedge (b \vee c) \leq (b \vee c)c^{-1}m$. Therefore, $a \wedge (b \vee c) \leq (b \vee c)b^{-1}m \wedge (b \vee c)c^{-1}m$. Also, note that

$$\begin{aligned}(b \vee c)b^{-1}m \wedge (b \vee c)c^{-1}m &= (b \vee c)(b^{-1} \wedge c^{-1})m \\ &= (b \vee c)(b \vee c)^{-1}m \\ &= m,\end{aligned}$$

and thus $a \wedge (b \vee c) \leq m$.

For the other distribution, the proof is similar: $(b \wedge c) \leq b$ implies that $a \vee (b \wedge c) \leq a \vee b$ (similarly for c). Then, assume $n \leq a \vee b$ and $n \leq a \vee c$. For $b \wedge c \leq b$, observe that

$(b \wedge c)b^{-1}a \leq a$ (again, similarly for c). Therefore:

$$\begin{aligned} a \vee (b \wedge c) &\geq (b \wedge c)b^{-1}a \\ &= (b \wedge c)(b^{-1}a \vee e) \\ &= (b \wedge c)(b^{-1}a \vee b^{-1}b) \\ &= (b \wedge c)b^{-1}(a \vee c) \end{aligned}$$

Thus, $(b \wedge c)b^{-1}(a \vee c) \leq a \vee (b \wedge c)$ and $(b \wedge c)c^{-1}(a \vee c) \leq a \vee (b \wedge c)$. Therefore, $(b \wedge c)c^{-1}n \vee (b \wedge c)c^{-1}n \leq a \vee (b \wedge c)$, and thus $n \leq a \vee (b \wedge c)$. □

This theorem shows that an l-group is distributive. However, it is *not* the case that all lattices are distributive.

Example 4.15. *Consider the following set,* $A = \{a, b, c, d, e\}$. *The diagram below signifies the ordering.*

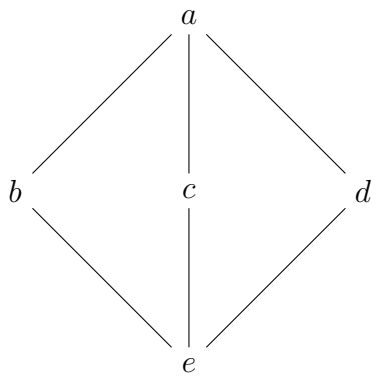

Figure 2

Now consider $b \wedge (d \vee c)$ *and* $(b \wedge d) \vee (b \wedge c)$. *The first term goes to* $b \wedge a$, *which is* b. *The second terms goes to* $e \vee e$, *which is just* e. *Thus the lattice is not distributive.*

Example 4.16. *Let* $A = \{a, b, c, d, e\}$. *The diagram below signifies the ordering.*

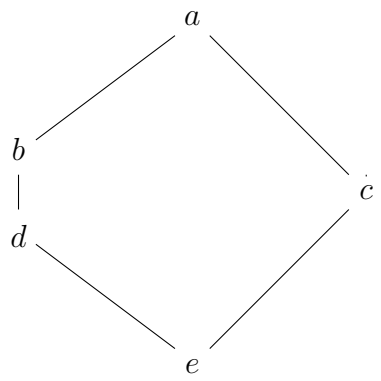

Figure 3

Again, we consider $b \wedge (d \vee c)$ *and* $(b \wedge d) \vee (b \wedge c)$*. The first term goes to* $b \wedge a$*, which is* b*. For the second term, it goes to* $d \vee e$*, which is* d*. Therefore this lattice is not distributive either. In fact, it can be shown the only nondistributive lattices are the lattices in which one of the these two are embedded [2].*

Now we are ready to develop some higher theory regarding homomorphisms, ideals, and kernels. First, we need to offer some new definitions which "update" traditional notions of these concepts to include order.

5 *l*-Homomorphisms and *l*-Subgroups

In this section, we extend homomorphisms and subgroups from elementary group theory to lattices and l-groups. We begin by defining the analogous terms, then prove results pertaining to these concepts.

Definition 5.1. *Let* $f : G \mapsto H$*, where* $(G, *, \leq)$ *and* $(H, *, \leq)$ *are l-groups, and* $a, b \in G$*. Then,* f *is an l-homomorphism if the following conditions hold:*

1. f *is a group homomorphism, i.e.,* $f(a * b) = f(a) * f(b)$
2. f *is a lattice homomorphism, i.e.,* $f(a \wedge b) = f(a) \wedge f(b)$ *and* $f(a \vee b) = f(a) \vee f(b)$*.*

Definition 5.2. *A function* f *between two partially ordered sets is order-preserving if* $a \leq b$ *implies* $f(a) \leq f(b)$*.*

Theorem 5.3. *If f is an l-homomorphism, then f is order-preserving.*

Proof. Let $f : G \to H$ be an l-homomorphism. For $a, b \in G$, let $a \leq b$. Then, $b = a \vee b$, and therefore $f(b) = f(a \vee b) = f(a) \vee f(b)$. Thus, $f(a) \leq f(b)$. □

However, the converse is not true: a function that is order-preserving does not imply that it is an l-homomorphism. Consider the following example.

Example 5.4. *Let $f : (D_6^+, |) \to (\{1, 2, 3, 6\}, \leq)$, such that f is the identity function, i.e., $f(x) = x$ for every x. The ordering on D_6^+ is as follows: (i.e., $a \leq b$ if and only if $a|b$).*

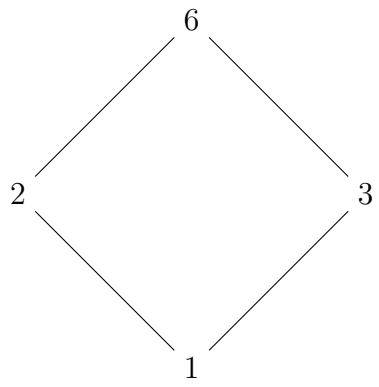

Figure 4

Computation reveals that f is order preserving. For example, $1 \leq 2$, and $f(1) \leq f(2)$. However, consider $f(2 \vee 3)$: $(2 \vee 3)$ is 6, and therefore $f(2 \vee 3) = 6$. However, $f(2) \vee f(3) = 2 \vee 3 = 3$. And thus, f is not an l-homormorphism, for it fails to preserve joins and meets.

We continue to extend classical algebra with more definitions.

Definition 5.5. *Let G be an l-group and H be a subgroup of G, with the further condition that for $a, b \in H$, then $a \vee b \in H$ and $a \wedge b \in H$. Then H is an l-subgroup of G.*

Definition 5.6. *Let H be an l-subgroup of l-group G. H is convex if, for $h, k \in H$ and $a \in G$, $h \leq a \leq k$ implies $a \in H$.*

Definition 5.7. *Let f be an l-homomorphism from G to H. If f is a bijection, then f is an l-isomorphism.*

Definition 5.8. *Let G be an l-group, and H an l-subgroup of G. If, for $h \in H$ and every $a, a^{-1} \in G$, we have $a^{-1}ha \in H$ then H is normal.*

Definition 5.9. *Let G be an l-group, and $H \subseteq G$. Then, H is an l-ideal if H is a subgroup of G, H is convex, and H is normal in G.*

Definition 5.10. *Let ϕ be a l-homomorphism from G to H, where G and H are l-groups. Then, $Ker(\phi) = \{a \in G | \phi(a) = e_h\}$, where e_h is the identity element in H.*

For Theorems 5.11, 5.12, and 5.13, assume the following:
Let ϕ be an l-homomorphism from $(G, *, \leq)$ to $(H, *, \leq)$, where G and H are l-groups, and ϕ is onto.

Theorem 5.11. *The kernel, Ker(ϕ), is an l-ideal.*

Proof. Three parts are required: $Ker(\phi)$ be an l-subgroup of G, convex, and normal. Let $a, b \in Ker(\phi)$. Then, $\phi(ab) = \phi(a)\phi(b) = e'e' = e'$ implies that $ab \in Ker(\phi)$. Since $Ker(\phi) \subseteq G$, $Ker(\phi)$ is associative by definition. It is well known that homomorphisms preserve the identity element. Lastly, observe that $\phi(aa^{-1}) = \phi(e) = e' = \phi(a)\phi(a^{-1})$. Then, $\phi(a^{-1}) = e'$. Therefore, $a^{-1} \in Ker(\phi)$. Finally, $\phi(a \wedge b) = \phi(a) \wedge \phi(b) = e' \wedge e' = e'$. Similarly, $a \vee b \in Ker(\phi)$. Thus, $Ker(\phi)$ is an l-subgroup of G.

For convexity, let $c \in G$ such that $a \leq c \leq b$. Then, $\phi(a) \leq \phi(c) \leq \phi(b)$ implies $e' \leq \phi(c) \leq e'$. Thus, $\phi(c) = e'$, and $c \in Ker(\phi)$. Finally, for normality, consider $c^{-1}ac$. Then, $\phi(c^{-1}ac) = \phi(c^{-1})\phi(a)\phi(c)$. Since $a \in Ker(\phi)$, $\phi(c^{-1})e\phi(c) = \phi(c^{-1})\phi(c)$. Since homormorphisms preserve inverses, our proof is complete. □

Theorem 5.12. *If N is an l-ideal of G, then the set of right cosets G/N can be provided with an order which makes it an l-group, so that the natural map $v : G \mapsto G/N$ is an l-homomorphism.*

Proof. It is well known, from classical group theory, that G/N is a group, and v is a group homomorphism. Therefore, we need to show that an order can be provided which makes G/N a lattice. We shall define that ordering, $Nb \leq Na$, to mean there exists an $n \in N$ such that $b \leq na$. We must show that this ordering is reflexive, transitive, and antisymmetric. For reflexivity, $Na \leq Na$ since $a \leq ea$. For transitivity, assume that $Nb \leq Na$ and $Nc \leq Nb$. That is, there exists n and n' such that $b \leq na$ and $c \leq n'b$. Then, $c \leq n'b \leq n'na$. Thus, $c \leq n'na$, and $Nc \leq Na$. Finally, for antisymmetry, assume that $Na \leq Nb$ and $Nb \leq Na$. Then, $a \leq nb$ and $b \leq n'a$ for $n, n' \in N$. Then, $n^{-1} \leq ba^{-1}$ and $ba^{-1} \leq n'$. Since N is an l-ideal, it is convex. Therefore, $ba^{-1} = k$, for some $k \in N$, and $b = ka$, and thus, $Nb = Na$. Thus, our ordering is valid, and G/N has partial order.

Next we show that our order is compatible with the group operation. Say $Nb \leq Na$, so $b \leq na$. Then, $bc \leq nac$, and $Nbc \leq Nac$. Thus, $NbNc \leq NaNc$. □

Theorem 5.13. *$G/Ker(\phi)$ is l-isomorphic to H.*

Proof. Define $\psi : G/Ker(\phi) \to G/N$. Observe that $(\psi(v))(g) = \phi(g)$. For one to one, assume that $\psi(na) = \psi(nb)$ for some $a, b \in G$. Then, $\phi(a) = \phi(b)$. Next, $\phi(b)^{-1}\phi(a) = e'$. Since ϕ is an l-homormorphism, it preserves inverses. Therefore, $\phi(b)^{-1}\phi(a) = \phi(b^{-1})\phi(a) = \phi(b^{-1}a) = e'$. Therefore, $b^{-1}a \in Ker(\phi)$, that is, $Ka = Kb$. For onto, take some $h \in H$. Since ϕ is onto, there exists $g \in G$ such that $\phi(g) = h$. Therefore, $\psi(Ng) = h$.

Finally, to show that ψ preserves lattices, suppose $Na \wedge Nb$ for Na and $Nb \in Ker(\phi)$. Then, $\psi(Na \wedge Nb) = \phi(a \wedge b)$, and since ϕ is an l-homomorphism, $\psi(Na \wedge Nb) = \phi(a) \wedge \phi(b)$, and thus $\psi(Na \wedge Nb) = \psi(Na) \wedge \psi(Nb)$. A similar argument can be made for joins. □

Notice that Theorem 5.12 is the classical First Isomorphism Theorem for groups.

6 Groups of Divisibility

We now turn to the topic of *Groups of Divisibility*. As the name suggests, we shall at some point arrive, at a group. But before we get to these special groups, we must start in *Rings*.

Definition 6.1. *A Ring $(G, +, \cdot)$ is a set G with two operations, denoted by "+" and "·", with the following properties:*

- *$(G, +)$ is an abelian group*
- *Multiplication is associative $a(bc) = (ab)c$, for $a, b, c \in G$.*
- *Multiplication is distributive over addition: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$*
- *If in addition, there exists an element denoted by 1 such that $1 \cdot a = a = a \cdot 1$ for every $a \in G$, then R is a ring with unity.*

Definition 6.2. *Let $(G, +, \cdot)$ be a ring. If $ab = ba$ for every $a, b \in G$, then $(G, +, \cdot)$ is a commutative ring.*

Definition 6.3. *An Integral Domain is a commutative ring with unity and the additional property: $ab = 0$ implies that $a = 0$ or $b = 0$.*

There is another way to characterize an integral domain, by using divisors of zero. Divisors of zero are elements that divide zero. That is, for a, b different than zero, $ab = 0$. With this new concept, we can create an equivalent meaning for integral domains.

Proposition 6.4. *Let G be an integral domain. Then G has no divisors of zero.*

Proof. Let $a, b \in G$ such that $ab = 0$. Then, $a0 = 0 = ab$, and so by the cancellation property, $b = 0$. Similarly, a may equal zero as well. □

The best example of an integral domain is $\mathbb{Z}$. However, not every ring is an integral domain. For example, take $\mathbb{Z}_6$: $2 \cdot 3 = 0$, but 2 and 3 are not zero, and so $\mathbb{Z}_6$ is *not* an integral domain. An integral domain can be further expanded to a *field*.

Definition 6.5. *A field is a commutative ring where every nonzero element is invertible.*

The best example of a field is $(\mathbb{R}, +, \cdot)$, which is certainly an abelian group; multiplication is commutative; 1 is the multiplicative identity; and every $a \neq 0$ has an inverse, namely $\frac{1}{a}$. For our purposes, fields are important because of their relationship with integral domains via *quotient fields.*

Once again, the best example of a quotient field is the rationals with respect to the integers. That is, the integral domain would be $(\mathbb{Z}, +, \cdot)$, and the rationals would be the quotient field because every rational number is the quotient of two integers.

Definition 6.6. *A Multiplicative Group is a group under multiplication of the invertible elements of a field or ring.*

With these definitions, we can now develop more theory.

Definition 6.7. *A unit of a ring is a nonzero element that has a multiplicative inverse. We denote the set of units of a ring by U.*

Definition 6.8. *Let R be a ring and I an ideal of R. I is principal if I is generated by a single element a, denoted as $\langle a \rangle$.*

Proposition 6.9. *$(U, \cdot)$ is a group, where U is the set of units in ring $(R, +, \cdot)$.*

Proof. Note that $1 \in U$, since $1 = 1 \cdot 1$. Then, let $a, b \in U$. Then, there exists a^{-1}, b^{-1} such that $aa^{-1} = 1$ and $bb^{-1} = 1$. Then, for ab, $(ab)b^{-1}a^{-1} = 1$. Thus, $ab \in U$. Furthermore, $a^{-1}, b^{-1} \in U$ as well, since they also divide 1. Multiplication is associative by definition of a ring. □

Definition 6.10. *Let D be an integral domain, K be the (unique) quotient field of D, and U the unit group. Let K^* be the multiplicative group of K. Then, the group of divisibility is defined as:*

$$G(D) = K^*/U$$

where $UaUb := Uab$.

Now, $G(D)$ (referred to from here on out as G) is an abelian group because multiplication was said to be commutative.

Now, we are going to attached an ordering on G: let $Ua \leq Ub$ if $b/a \in D$. Notice that $b/a \in D$ is equivalent to $a|b$, where $a|b$ if $b = ak$ for some $k \in D$. Now we are going to prove that G with this partial order produces an l-group.

Theorem 6.11. *Let G be a group of divisibility. Then G is a partially ordered group.*

Proof. We must prove that the ordering satisfies the symmetric, reflexive, and transitive properties required for a lattice, and that it is compatible with the operation. Say, $Ua \leq Ub$ for $a, b \in K^*$. $Ua \leq Ua$ since $a = 1a$. Assume further that $Ub \leq Uc$. Then, there exist $k_1, k_2 \in D$ such that $k_1 a = b$ and $k_2 b = c$. Then, $k_2 k_1 a = c$. Since D is a domain, $k_2 k_1 \in D$. Thus, $a|c$ and $Ua \leq Uc$. Next, say $Ua \leq Ub$ and $Ub \leq Ua$. Then, $k_1 b = a$ and $k_2 a = b$. Therefore, $k_1 k_2 a = a$ and $k_1 k_2 = 1$. Thus, $k_1, k_2 \in U$. Then, for $x \in Ua$, there exists a $u \in U$ such that $x = ua$. Then $x = uk_1 b$. Since $u, k_1 \in U$, $x \in Ub$. Therefore, $Ua \subseteq Ub$. Similarly, $Ub \subseteq Ua$. Thus $Ua = Ub$. Finally, let $Ua \leq Ub$, so $k_1 b = a$. Then, $k_1 bc = ac$, and $Uac \leq Ubc$. Therefore, $UaUc \leq UbUc$. □

Before we proceed much further, we need to make one last note about rings. From elementary number theory we know that for two numbers a, b, the greatest common divisor, c is a number that divides both a and b, and any other number that also divides a and b also divides c. We extend (rather intuitively) this notion into the context of rings.

Definition 6.12. *For two elements of a ring, a, b, the greatest common divisor, or gcd, is an element c such that c divides both a and b and any other elements that divides a, b also divides c.*

With this new concept, we can define a new kind of domain: a *pseudo-Bezout* domain.

Definition 6.13. *A domain D is a pseudo-Bezout domain if every two elements of D has a greatest common divisor also in D.*[2]

[2]Also known as *GCD-Domains*.

We have the "psuedo" version of a Bezout domain, and now we introduce a regular Bezout domain.

Definition 6.14. *A domain D is a Bezout Domain if every finitely generated ideal is principal.*

At first glance, there appears to be no obvious connection between a Bezout Domain and a psuedo-Bezout Domain. However, there is one.

Theorem 6.15. *Every Bezout Domain is a psuedo-Bezout Domain.*

Proof. Let $a, b \in D$. Then, the ideal $\langle a, b\rangle$ is principal, and therefore $\langle a, b\rangle = \langle d\rangle$ for some $d \in D$. Clearly, $d|b$ and $d|a$, for $a0 + be = dk$ for some $k \in D$. Then, assume $d'|a$ and $d'|b$ for some $d' \in D$. Then, $d = sa + tb$ for $s, t \in D$, and thus $d = sd'k + td'k'$, and thus $d'|d$. □

Theorem 6.16. *A domain is a pseudo-Bezout domain if and only if the partial order on its group of divisibility is a lattice.*

Proof. Assume D is psuedo-Bezout. That is, for every $a, b \in D$, there exists a greatest common divisor, $c \in D$, such that $c|a$ and $c|b$, and for any c' that divides both a and b, c' also divides c. Therefore, $Uc \leq Ua$ and $Uc \leq Ub$, and thus $Uc \leq Ua \wedge Ub$. Since $Uc' \leq Uc$ for any c' that divides both a and b, we conclude $Uc = Ua \wedge Ub$. We must also find a join for every $a, b \in D$. We claim that $\frac{ab}{c}$ is the join (and the least common multiple). First, observe that $\frac{ab}{c} \in D$. Let $m = \frac{ab}{c}$. Now, $a|m$ and $b|m$, and therefore $Ua \leq Um$ and $Ub \leq Um$. Assume $a|m'$ and $b|m'$. Then, take $ak = m$ for some $k \in D$. Since $\frac{ab}{c} = m$, $\frac{cm}{b} = a$. Therefore, $\frac{cm}{b}k = m'$, and thus $m|m'$.

Now, assume the group of divisibility is a lattice. Then, for every $a, b \in G$, there exists a c such that $Uc = Ua \wedge Ub$. Therefore, $c|a$ and $c|b$, and for every c' that divides both a and b, $c'|c$, since if $c'|a$ and $c'|b$, then $Uc' \leq Ua$ and $Uc' \leq Ub$, and therefore is less than the meet. Therefore, a, b has a gcd, and the domain is therefore psuedo-Bezout. □

Before we turn to the main theorem of this thesis, we have to provide a final definition.

Definition 6.17. *Let K be a field. Then, a demivaluation on K is a group homomorphism ϕ from from the multiplication group of K, K^*, onto an abelian l-group G such that:*

$$\phi(x+y) \geq \phi(x) \wedge \phi(y).$$

Theorem 6.18. *Every abelian l-group is the group of divisibility of a Bezout Domain.*

Proof. Let G be an abelian l-group and K a field. Then, let $K[G]$ denote the group ring of G over K, where $K[G]$ is the vector space with a basis of aX^g, where $g \in G$ and $a \in K$. So, $r \in K[G]$ is of the form $r = \sum_{i=1}^{n} a_i X^{g_i}$. Let $I := \{g_i\} \bigcap \{h_i\}$, $\bar{g} := \{g_i\} - \{h_i\}$, and finally $\bar{h} := \{h_i\} - \{g_i\}$. Finally, we define the following operations:

$$\sum_{i=1}^{n} a_i X^{g_i} + \sum_{i=1}^{m} b_i X^{h_i} =: \sum_{i \in I} (a_i + b_i) X^g + \sum_{i \in \bar{g}} a_i X^{g_i} + \sum_{i \in \bar{h}} b_i X^{h_i}$$

$$aX^g \cdot bX^g =: abX^{g+h}.$$

These two operations behave exactly the same way addition and multiplication operate in any ring of polynomials. So $K[G]$ is a ring. Next we show it is an integral domain.

Say $r, s \in K[G]$. Let α be a compatible order on G (since G is an l-group). Let $E(r)$ denote the set of elements of G that appear as exponents in the linear expansion of r (similarly for $E(s)$). Then, for rs, there will be a unique term corresponding to the multiplication of the terms of degree g and h of the form $k_1 k_2 X^{g+h}$ for $k_1, k_2 \in K$. But then, since K is a field, $k_1 k_2 \neq 0$, and therefore $k_1 k_2 X^{g+h} \neq 0$.

Next, we are going to define a demivalution from the quotient field of $K[G]$, k, to G^+. Let $\psi : k \to G^+$ such that $\psi(r) = g_1 \wedge g_2 \wedge ... \wedge g_n$. Clearly, this map is injective. To show that ψ is a demivalution, take $r, s \in K[G]$. Then, $E(r+s) \subseteq E(r) \bigcup E(s)$, and therefore:

$$\psi(r+s) = \bigwedge E(r+s) \geq \bigwedge E(r) \bigwedge E(s) = \psi(w) \wedge \psi(s).$$

And thus ψ is a demivaluation. To see that it is a group homormorphism, observe

that since G is abelian, it is representable. Therefore, $\phi(r)$ is the smallest element of $E(r)$, and therefore $\psi(rs) = \psi(s) + \psi(r)$. Finally, we will show that the subring D_w, where $D_w = \{x \in k | \psi(x) \geq 0\}$, of k is a Bezout domain. Let $r, s \in D_w$, where $\psi(r) = g$, $\psi(s) = h$, so $r = tX^g$ and $s = uX^h$ where $\psi(t) = 0$ and $\psi(u) = 0$. Thus, $< r, s >=< X^g, X^h >$. But, since D_w is a pseudo-Bezout domain, g, h have a gcd, namely $g \wedge h$. Therefore $< X^g, X^h >=< X^{g \wedge h} >$. Thus, D_w is a Bezout domain. $\square$

7 Example

In our final section, we shall present an example of a integral domain and it's group of divisibility and show its partial ordering.

For our integral domain, we select $\mathbb{Z}$. The quotient field is $\mathbb{Q}$, and the group of units is $U = \{-1, 1\}$. The group of divisibility, therefore, is $\mathbb{Q}^*/U$. And so, the ordering is defined as:

$$Ua \leq Ub \text{ if and only if } \frac{b}{a} \in \mathbb{Z}.$$

Now we will show that the ordering is reflexive, antisymmetric, transitive, and is compatible with the operation. We begin with reflexivity. Since $a/a = 1 \in \mathbb{Z}$, $Ua \leq Ua$.

For antisymmetry, assume $Ua \leq Ub$ and $Ub \leq Ua$, so $b/a \in \mathbb{Z}$ and $a/b \in \mathbb{Z}$. Thus, $\frac{b}{a} = x \in \mathbb{Z}$ and $\frac{a}{b} = y \in \mathbb{Z}$. Then, $1 = yx$, and since $x, y \in \mathbb{Z}$, $x = y = 1$ or $x = y = -1$. Thus, $a = \pm b$. Since $U = \{1, -1\}$, $Ua = Ub$.

For transitivity, let $Ua \leq Ub$ and $Ub \leq Uc$ such that $c/b = y \in \mathbb{Z}$. Since $b/a \in \mathbb{Z}$, $b = ax$, and so $c/(ax) = y$. Therefore, $c/a = xy$, and since $x, y \in \mathbb{Z}$, xy is also in $\mathbb{Z}$. Thus, $Ua \leq Uc$.

Finally, let $Ua \leq Ub$, so $ak = b$ for $k \in \mathbb{Z}$. Then, $ack = bc$, and so $Uac \leq Ubc$, and finally $UaUc \leq UbUc$. Therefore the ordering is compatible with the operation. Since we have reflexivity, transitivity, antisymmetry, and compatibility, the group of divisibility is a partially ordered group.

8 Acknowledgements

I would like to extend a special thank to Dr. Ramiro Lafuente-Rodriguez for providing me with the opportunity to study this subject. It has opened my eyes to a part of mathematics that was foreign to me for many years, even as an undergraduate. His guidance, patience, and mentorship are not only qualities that have made it a pleasure to work with him, but are qualities I hope to emulate in the future.

I would also like to thank the other members of this committee, Dr. Dan Van Peursem and Dr. Gabriel Picioroaga. Their advice, insights, and instruction have proved invaluable, not just in the classroom, but in research, career decisions, and general intellectual endeavours.

Finally, I would like to thank the Department of Mathematical Sciences at USD. The entire department has been a source of endless support and inspiration.

References

[1] Marlow Anderson and Todd Feil. *Lattice-Ordered Groups: An Introduction*. D. Reidel, Dordrecht, Holland, 1988.

[2] Garret Birkoff. Lattice theory. *Colloquium Publications*, 25:8–12, 1967.

[3] Michael Darnell. *Theory of Lattice-Ordered Groups*. Marcel Dekker, 1995.

[4] David Dummit and Richard Foote. *Abstract Algebra*. John Wiley & Sons, 2004.

[5] I.N. Hernstein. *Abstract Algebra*. John Wiley & Sons, Inc., 1999.

[6] Paul Jaffard. *Les systemes d'ideaux*. Dunond, 1960.

[7] V.M. Kopytov and N. Ya. Medvedev. *The Theory of Lattice-Ordered Groups*. Springer, 1994.

[8] Wolfgang Krull. *Gesammelte Abhandlungen; Collected papers*. Walter de Gruyter, 1999.

[9] Rudolf Lidl and Gunter Pilz. *Applied Abstract Algebra*. Springer-Verlag, 1997.

[10] Jack Ohm. Semi-valuations and groups of divisbility. *Canadian Journal of Mathematics*, 21:576–591, 1969.

[11] Josesph Rotman. *A First Course in Abstract Algebra with Applications*. Prentice Hall, 2006.