Distributive Lattices

by

Taqseer Khan

Submitted to

Central European University

Department of Mathematics and its Applications

In partial fulfulment of the requirements for the degree of

Master of Science

Supervisor: Prof. Pál Hegedűs

Budapest, Hungary

2011

I, the undersigned [Taqseer Khan], candidate for the degree of Master of Science at the Central European University Department of Mathematics and its Applications, declare herewith that the present thesis is exclusively my own work, based on my research and only such external informaion as properly credited in notes and bibliography. I declare that no unidentified and illegitimate use was made of work of others, and no part of the thesis infrignes on any person's or institution's copyright. I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Budapest, 19 May 2011

_____

Signature

Acknowledgments

I owe my profound gratitude to my supervisor Professor Pál Hegedűs for his valuable guidance, support and encouragement from the initial to the final level that enabled me to write this thesis.

My thanks are also due to Professor Ervin Győri who made me possible to use the books and collect articles from the library of the Renyi Institute of Mathematics.

I wish to thank to the department of Mathematics and its Applications and the head Professor Gheorghe Morosanu for all his generosity and encouragement to me.

I utter my special thanks to my senior Ivan Andrus who helped me in typing this thesis.

Lastly, I would like to thank Elvira Kadvány for her kindness, support and encouragement throughout.

Preface

This thesis is being submitted in partial fulfilment of the requirements for a Master's Degree in Mathematics for me. My supervisor for the thesis has been Professor Pál Hegedűs. The thesis has been made solely by me; most of the text, however, is based on the research of others, and I have done my best to provide references to these sources. Writing this thesis has been hard but in the process of writing I feel I have learnt a lot. In this preface I give a brief account of the thesis.

This thesis consists of six chapters. In the first chapter we have given a short introduction of the subject. We have mentioned almost chronological development of lattice theory starting from Georege Boole's attempt for formalising logics to the current main research. In this chapter we have described some areas in which lattices have found their applications in practical life.

Chapter two consists of the basic concepts of lattice theory. Several examples and counter example have been given here. As pictures speak better than texts, we have tried to give diagrams of most of the lattices included. We have given the lattice-as-an-algebraic-structure definition of a lattice and have stated a theorem showing the equivalence of the two versions of the definition . Then we have mentioned the concept of ideals in lattices and some results related to them.

Chapter three discusses special elements in lattices with examples.

In chapter four we have discussed distributive lattices in detail. Here we have mentioned the characterisation of distributive lattices in terms of lattices of sets. Two prototypical examples of non-distributive lattices have been given with their diagrams and a theorem has been stated which shows how the presence of these two lattices in any lattice matters for the distributive character of that lattice. We have introduced the concepts of Boolean lattices, Boolean algebras and Boolean rings and have shown the equivalence of Boolean algebras and Boolean rings. Then modularrity of lattices has been introduced. We have ended this chapter with the discussion of morphisms in lattices.

Chapter five introduces the concept of congruences in lattices. Some examples have been given to have a feel of this concept. Then we have discussed the connection between congruence lattices and distributive lattices. The concepts of factor lattice and kernels have been introduced. We close this chapter with the definitions of three important lattices; regular lattice, uniform lattice and isoform lattice.

In chapter six we have discussed representations of distributive lattices as congruence lattices. We have defined some more notions like atoms and atomisticity in lattices. We have given an example of a non-atomistic lattice with illustration. The chopped lattice concept has been introduced with example. Then we have stated and proved a result throwing light on the importance of chopped lattices. Finally, we have stated and illustrated two representation theorems of finite distributive lattices: one involves congruences of a chopped lattice and the other involves the join-irreducible elements of the distributive lattice.

Table of Contents

Chapter 1

Introduction

The origin of the lattice concept dates back to the nineteenth-century attempts to formalise logic. In the first half of the nineteenth century, George Boole discovered Boolean algebras. While investigating the axiomatics of Boolean algebras, Charles S. Pierce and Ernst Schröder introduced the concept of lattice in the late nineteenth century. Lattices, especially distributive lattices and Boolean algebras, arise naturally in logic, and thus some of the elementary theory of lattices had been worked out earlier by Ernst Schröder in his book *Die Algebra der Logik*. Richard Dedekind also independantly discovered lattices. In the early 1890's, Richard Dedekind was working on a revised and enlarged edition of Dirichlet's *Vorlesungen über Zahlentheorie*, and asked himself the following question: Given three subgroups A, B, C of an abelian group G, how many different subgroups can you get by taking intersections and sums, e.g., $A+B$, $(A+B)\cap C$, etc. The answer is 28. In looking at this and related questions, Dedekind was led to develop the basic theory of lattices, which he called *Dualgruppen*. The publication of the two fundamental papers *über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler* (1897) and *über die von drei Moduln erzeugte Dualgruppe* (1900), on the subject of R. Dedekind brought the theory to life well

over one hundred years ago. These two pappers are classical and have inspired many later mathematicians.

Richard Dedekind defined modular lattices which are weakend form of distributive lattices. He recognised the connection between modern algebra and lattice theory which provided the impetus for the development of lattice theory as a subject. Later Jónsson, Kurosh, Malcev, Ore, von Neumann, Tarski, and Garrett Birkhoff contributed prominently to the development of lattice theory. It was Garett Birkhoff's work in the mid thirties that started the general development of the subject. In a series of papers he demonstrated the importance of lattice theory and showed that it provides a unifying framework for unrelated developments in many mathematical disciplines. After that Valere Glivenko, Karl Menger, John Von Neumann, Oystein Ore and others developed this field. In the development of lattice theory, distributive lattices have played a vital role. These lattices have provided the motivation for many results in general lattice theory. Many conditions on lattices are weakened forms of distributivity. In many applications the condition of distributivity is imposed on lattices arising in various areas of Mathematics, especially algebras.

In bibliography, there are two quite different mathematical structures that are usually called lattices. The first one has to do with partially ordered sets while the other has to do with regular arrangements of points in space. In the thesis in hand, we exclusively consider the first case. In the 19th century, important results due to Minkowski motivated the use of lattice theory in the theory and geometry of numbers. The evolution of computer science in the 20th century led to lattice applications in various theoretical areas such as factorization of integer polynomials, integer programming and Public-Key Cryptography. In the latter area, lattice theory has played a significant role in the definition of new cryptosystems, in the study of cryptographic primitives and in cryptanalysis. The main goal of a cryptosystem is to ensure the safe exchange of information between the legitimate senders and the legitimate receivers, guaranteeing at the same time, that no unauthorized

party is able to recover any part of the information.

The important current research on lattice theory has been initiated by G. Birkhoff, R. P. Dilworth and G. Grätzer. They are primarily concerned with the systematic development of results which lie at the heart of the subject.

Chapter 2

Background Definitions

Partially Ordered Set (poset): A partially ordered set, or more briefly just ordered set, is a system $P = (P, \leq)$ where P is a nonempty set and $\leq$ is a binary relation on P satisfying, for all $x, y, z \in P$,

(i) $x \leq x$, (reflexivity)

(ii) if $x \leq y$ and $y \leq x$, then $x = y$, (antisymmetricity)

(iii) if $x \leq y$ and $y \leq z$ then $x \leq z$ (transitivity)

Examples of posets abound. The most natural example of an ordered set is $P(S)$, the collection of all subsets of a non empty set S ordered by $\subseteq$. Another familiar example is $Sub(G)$, the collection of all subgroups of a group G, again ordered by set containment.

Covering relations: let $(P, \leq)$ be a poset. Given two elements a, b of P, one says that b covers a if $a<b$ and there does not exist any element $c \in P$ such that $a<c<b$.

Atoms: Let $(P, \leq)$ be a poset. An element $a \in P$ is called an *atom* if it covers some minimal element of P. Consequently, an atom is never minimal. P is called *atomic* if for every non-minmal element $p \in P$ there is an atom a such that $a \leq p$.

Bounds: Let $(P, \leq)$ be a poset and Q be a subset of P. An element $a \in P$ is said to be a lower bound of Q if $a \leq x$, for all $x \in Q$. The greatest member of the set of all lower bounds of Q is called its greatest lower bound (glb) or infimum (inf) of Q. Dually, $b \in P$ is said to be an upper bound of Q if $y \leq b$, for all $y \in Q$. The smallest member of the set of all upper bounds of Q is called its least upper bound (lub) or supremum (sup).

Now we give the chief definition of the chapter

Lattice: A poset $\langle L, \leq \rangle$ is a lattice if $\sup\{a, b\}$ and $\inf\{a, b\}$ exist for all $a, b \in L$.

Examples :

1) The power set $P(S)$ of S above is a poset under inclusion. Let us define $\sup\{A, B\}$ as union of A, B and $\inf\{A, B\}$ as intersection of A, B. Then $P(S)$ becomes a lattice.

2) The set of all natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$ with the ususal order of $\leq$ is a poset. By defining $\sup\{a, b\}$ as the bigger of the two elements and $\inf\{a, b\}$ as the smaller of the two elements, it forms a lattice.

3) For a positive integer n, let L_n be the set of all positive divisors of n. Let us define a relation $\leq$ as

$$a \leq b \iff a \mid b$$

Definie $\sup\{a, b\}$ as lcm of a, b and $\inf\{a, b\}$ as gcd of a, b. Then L_n becomes a lattice. The lattice L_6 is the following

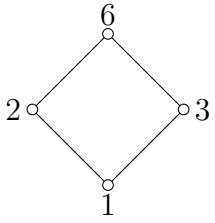

Figure 2.1: Lattice L_6

Examples of lattices in Group theory

A lattice diagram of a group is a diagram which lists all the subgroups of the group such that the larger subgroups occure above the smaller ones in the plane and there is a line joining the smaller subgroups to those containing them. If H, K are two subgroups of a group G, $H \vee K = \langle H, K \rangle$, the subgroup generated by H, K and $H \wedge K = H \cap K$, the set-theoretic intersection of H, K, then its lattice diagram is given by figure 2.2.

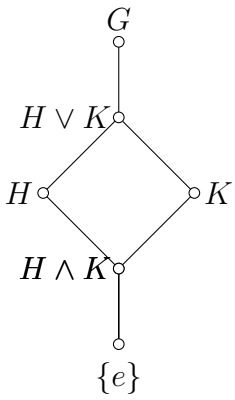

Figure 2.2: Lattice of Subgroups

Examples:

If $G = V_4$, the Klein-four group, then the lattice diagram of G is given by the figure 2.3.

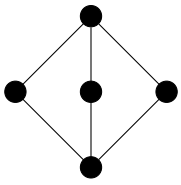

Figure 2.3: Lattice of V_4

Consider the symmetric group $S_3 = \{identity, (12), (13), (23), (123), (213)\}$ on three symbols $\{1, 2, 3\}$. Then the non-trivial subgroups of S_3 are $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$ and $\langle(123)\rangle$. The lattice diagram of S_3 is given by the figure 2.4.

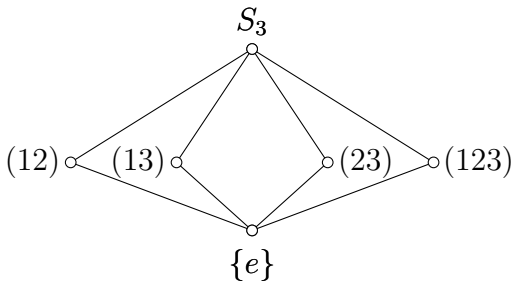

Figure 2.4: Lattice of S_3

Lattice diagrams of cyclic groups:

Lattice diagrams for cyclic groups of fnite orders are easy to draw. We know that if $G = \langle x \rangle$ is a cyclic group of order n, then any subgroup is of the form $H = \langle x^d \rangle$ where d is a divisor of n. In particular, when $G = \mathbb{Z}_n$ is the cyclic group generated by 1, we write $H = \langle d \rangle = d\mathbb{Z}_n$ as the cyclic subgroup generated by d.1.

(i) $G = \mathbb{Z}_{p^m}$ has the lattice

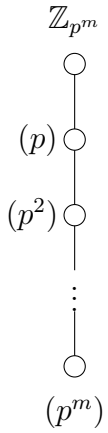

Figure 2.5: Lattice of $\mathbb{Z}_{p^m}$

(ii) $G = \mathbb{Z}_6$ has the lattice

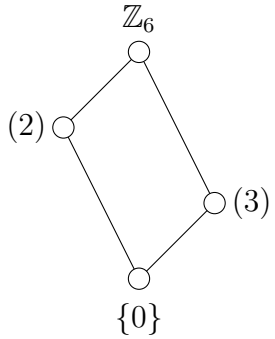

Figure 2.6: Lattice of $\mathbb{Z}_6$

(iii) $G = \mathbb{Z}_{12}$ has the lattice

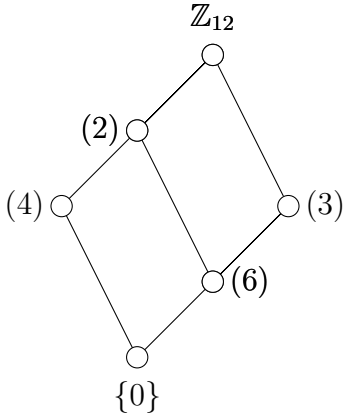

Figure 2.7: Lattice of $\mathbb{Z}_{12}$

Not every poset is a lattice:

Consider $S = \{2, 3, 4, \dots\}$, the set of natural numbers deleted 1. Let us define the partial order and sup and inf as in example 3 above, then S is not a lattice as, for example, the gcd of 2,3 does not belong to S.

Lattice as an algebraic structure:

Richard Dedekind discovered the algebraic characterisation of lattices. A lattice as an algebraic structure is a set on which two binary operations are defined, called *join* and *meet*, denoted by $\vee$ and $\wedge$, satisfying the following axioms:

i) Commutative law :

$$a \vee b = b \vee a$$

$$a \wedge b = b \wedge a$$

ii) Associative law :

$$a \vee (b \vee c) = (a \vee b) \vee c$$

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

iii) Absorption law :

$$a \vee (a \wedge b) = a$$

$$a \wedge (a \vee b) = a$$

iv) Idempotent law :

$$a \vee a = a$$

$$a \wedge a = a$$

for all $a, b, c \in L$.

Hungarian mathematician G. Grätzer (1971) proved that

Theorem 1. *A non-empty set L is a lattice $\Longleftrightarrow$ there are two binary operations $\vee$ and $\wedge$ satisfying the above axioms $(i) - (iv)$.*

Substructures of Lattices

Let L be any lattice. Then a non-empty subset $S \subseteq L$ is called a sublattice if S is closed under the meet $\wedge$ and join $\vee$.

Examples :

i) Consider $(I^+, \leq)$, where I^+ is the set of positive integers and $a \leq b \iff a \mid b$. Then for any positive integer n, $(L_n, \leq)$ is a sublattice of I^+.

ii) For any a in L,

$$L_a = \{x \in L \mid a \leq x\}$$

forms a sublattice of L.

Remark : If L, L^* are two lattices such that $L^* \subseteq L$, then L^* need not be a sublattice of L :

Let S be a group. Consider two families out of S - the power set $P(S)$ of S and $G(S)$, the collection of all subgroups of S. Then $P(S)$ is a lattice with the operations defined by $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. $G(S)$ also forms a lattice under the operations defined by $G_1 \wedge G_2 = G_1 \cap G_2$ and $G_1 \vee G_2 =$ the subgroup generated by $G_1 \cup G_2$. Then it is obvious that $G(S) \subseteq P(S)$. But $G(S)$ is not a sublattice of $P(S)$ as it is not closed under union, the operation of $P(S)$.

Ideal: A sublattice I of L is called an ideal iff $i \in I$ and $a \in L$ imply that $a \wedge i \in I$. An ideal I of L is called proper iff $I \neq L$. A proper ideal I of L is prime iff $a, b \in L$ and $a \wedge b \in I$ impy that either $a \in I$ or $b \in I$. In the following lattice, $I = \{0\}$ is an ideal and

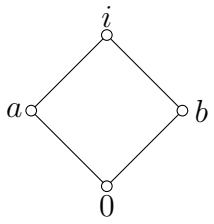

Figure 2.8: figure

$P = \{0,a\}$ is a prime ideal, while I is not prime.

Like other algebraic structures, we can also define the sublattice and the ideal generated by a subset of a lattice.

Let H be a subset of L. Then the smallest sublattice of L containg H is called the sublattice of L generated by H, denoted by [H]. It is the intersection of all sublattices of L containing H. Similarly an ideal generated by a subset H of L is the intersection of all ideals containing H, denoted by (H]. If $H = a$ then $(H] = (a]$ is called a principal ideal.

Meet and Join of ideals: The *meet* of two ideals I, J of L is defined to be the intersection $I \cap J$. The *join* is bit tricky defined as follows: Define

$$U_0(I, J) = I \cup J$$

$$U_1(I, J) = \{x | x \leq u \vee v; u, v \in U_0(I, J)\}$$

$$U_2(I, J) = \{x | x \leq u \vee v; u, v \in U_1(I, J)\}$$

etc. Then

$$I \vee J = \cup(U_i(I, J) | i<\omega)$$

Meet and join of two ideals are also ideals.

A characterisation theorem of an ideal is as follows:

Theorem 2. *Let L be a lattice and let H and I be nonvoid subsets of L.*

(i) *I is an ideal iff $a, b \in I$ implies that $a \vee b \in I$, and $a \in I, x \in L, x \leq a$ imply that $x \in I$.*

(ii) *$I = (H]$ iff I is an ideal, $H \subseteq I$ and for all $i \in I$ there exists an integer $n \geq 1$ and there exist $h_0, h_1, \ldots, h_{n-1} \in H$ such that $i \leq h_0 \vee \ldots \vee h_{n-1}$.*

(iii) *For $a \in L$, $(a] = \{x \in L : x \leq a\} = \{x \wedge a : x \in L\}$*

As an example, in the following lattice the principal ideal generated by the elements a, d can be written as

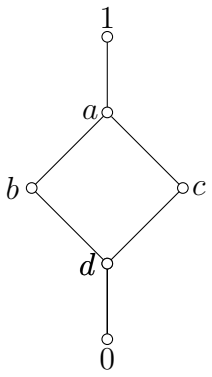

Figure 2.9: figure

$$(a] = \{0, a, b, c, d\}$$

$$(d] = \{0, d\}$$

Chapter 3

Special Notions in Lattices

Here we define some special types of elements in lattices.

Zero Element: In a lattice L an element 0 is called the zero element of L if $0 \leq a$, for every $a \in L$. Dually

Unit Element: An element 1 is called the unit element or the all element of L if $a \leq 1$, for every $a \in L$.

Bounded lattice: A lattice L with 0, 1 is called a bounded lattice.

Examples:

i) In chapter 2, the lattice of example 1 has the empty set ϕ and the set S as its zero element and the unit element respectively. Therefore $P(S)$ is a bounded lattice.

ii) The natural number 1 is the zero element in the lattice of example 2. This lattice does not possess the unit element. This lattice is not bounded.

iii) The lattice L_6 of example 3, chapter 2 has 1 as its zero element and 6 as its unit element. Hence, L_6 is bounded.

Join irreducible: An element a in a lattice L is said to be *join irreducible* iff a is not a zero element and whenever $a = b \vee c$, then either $a = b$ or $a = c$. Dually

Meet irreducible: An element a in a lattice L is *meet irreducible* iff a is not a unit element and whenever $a = b \vee c$, then either $a = b$ or $a = c$. If a is both join and meet irreducible, then a is said to be irreducible.

Example: In the lattice diagram below

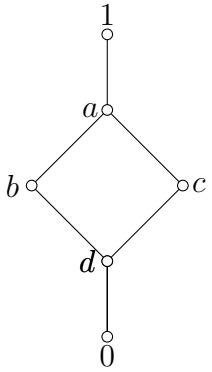

Figure 3.1: figure

a is meet irreducible but not join irreducible, d is join irreducible but not meet irreducible, while b, c are irreducibles.

Complement of an element: Let L be a bounded lattice and $a \in L$. Then a complement of a is defined to be an element $b \in L$, if such an element exists, such that

$$a \wedge b = 0, a \vee b = 1$$

For example, in the above lattice, the complement of b is c and vice-versa.

Remark: If a complement of an element exists, it may not be unique. For example, in the middle row of the diamond of figure 4.2 any two of the three elements are complements of the third.

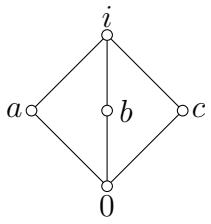

Figure 3.2: Lattice $\mathfrak{M}_3$

To get around the non-uniquness issue, an alternative to a complement is defined as

Pseudocomplement: An element $b \in L$ with 0 is called the pseudocomplement of $a \in L$ if

(i) $b \wedge a = 0$

(ii) for any c such that $c \wedge a = 0$, $c \leq b$.

In other words, b is the maximal element in the set $\{c \in L : c \wedge a = 0\}$ and, if it exists, it is unique.

Example: In the lattice of figure 4.3 (called Benzene) the pseudocomplement of a is y.

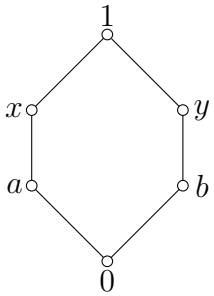

Figure 3.3: figure

It is noteworthy that the pseudocomplement of y is not a (it is in fact x)

Pseudocomplemented Lattice: L is called pseudocomplemented lattice if every element in L has a pseudocomplemnt.

Example: The Benzene is the pseudocomplemented lattice.

Complemented lattice: L is called complemented if every element in L has a complement.

Examples

(i) The lattice $\mathfrak{M}_3$ above is complemented lattice.

(ii) Let X be a topological space. Then the collection $L(X)$ of all open subsets of X is a pseudocomplemented lattice.

The pseudocomplement of an open set U of X is $(U^c)^o$, the interior of the complement of U.

Sectionally Complemented Lattice: L is called sectionally complemented lattice if for any $a \leq b$ in L, there is an element c in L such that $a \wedge c = 0$, and $a \vee c = b$.

Example: The lattice of figure 4.4 is sectionally complemented.

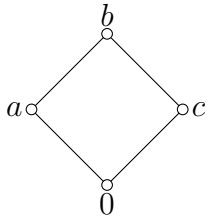

Figure 3.4: figure

Compact Elements : An element a of L is called compact if $a \in L$ is such that $a \leqslant \vee S$ for an arbitrary subset S of L then there exists a finite subset $S_1 \subseteq S$ such that $a \leqslant \vee S_1$.

Complete Lattices : L is complete if *sup* and *inf* exist for any arbitrary subset of L and every element of L can be written as a join of *compact elements*.

Chapter 4

Distributive Lattices

A distributive lattice is a lattice L satisfying the law (called the distributive identity)

$$c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) \tag{4.1}$$

for all $a, b, c \in L$. A distributive lattice of fundamental importance is the two-element chain $(2, \wedge, \vee)$. It is the only two-element lattice. This lattice features prominently in logic as the lattice of truth values. Later the Hungarian mathematician Andras Huhn introduced the concept of $n - distributivity$:

L is called $n - distributive$ if in L the following identity holds:

$$x \wedge (\bigvee_{i=0}^{n} y_i) = \bigvee_{i=0}^{n} (x \wedge (\bigvee_{j(\neq i)=0}^{n} y_j))$$

Remark: In the equlity (3.1), it is trivial that

$$(c \wedge a) \vee (c \wedge b) \leq c \wedge (a \vee b)$$

so to prove a lattice to be distributive, we only need to prove that

$$(c \wedge a) \vee (c \wedge b) \geq \wedge(a \vee b)$$

Examples:

i) Distributive lattices are ubiquitous. The prototypical examples of such structures are collections of sets for which the lattice operations can be given by set union and intersection. Indeed, these lattices of sets describe the scenery completely as stated in the following theorem

Theorem 3. *(G. Birkhoff and M. H. Stone) A lattice is distributive iff it is isomorphic to a ring of sets.*

ii) The lattice $(I^+, \leq)$ mentioned above is distributive.

Non-distributive lattices : The two protoype non-distributive lattices are the $\mathfrak{M}_3$ and $\mathfrak{N}_5$.

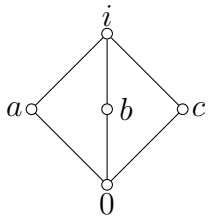

Figure 4.1: Lattice $\mathfrak{M}_3$

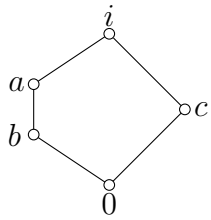

Figure 4.2: Lattice $\mathfrak{N}_5$

We shall call a subset A of a lattice L *diamond* or *pentagon* iff A is a sublattice isomorphic to $\mathfrak{M}_3$ or $\mathfrak{N}_5$ respectively.

Now we state a theorem without proof which reveals that the sublattices isomorphic to $\mathfrak{M}_3$ and $\mathfrak{N}_5$ play an important role.

Theorem 4. *A lattice L is distributive iff L does not contain a pentagon or a diamond.*

Lemma 5. *A lattice L is distributive iff for any two ideals I, J of L:*

$$I \vee J = \{i \vee j : i \in I, j \in J\}$$

Proof: Suppose L is distributive and let us take $t \in I \vee J$. Then by theorem 2 (ii), $t \leq i \vee j$, with $i \in I$, $j \in J$. Then by distributivity, $t = t \wedge (i \vee j) = (t \wedge i) \vee (t \wedge j) = i_1 \vee j_1$ where $i_1 = t \wedge i \in I$, $j_1 = t \wedge j \in J$, since I, J are ideals of L. Thus $t = i_1 \vee j_1$ for $i_1 \in I$, $j_1 \in J$. This implies that $I \vee J = \{i \vee j : i \in I, j \in J\}$.

For converse, suppose that $I \vee J = \{i \vee j : i \in I, j \in J\}$ and suppose, if possible, L is non-distributive. Then there exist three elements a, b, c (as in the lattice $\mathfrak{M}_3$). Now let us consider the principal ideals $I = (b], J = (c]$. (Keeping in mind the figure $\mathfrak{M}_3$), $a \leq b \vee c$ and so $a \in I \vee J$. But we claim that a can not be written as $a = i \vee j$ because if it is so then $i \leq a$, $j \leq a$. Then as $j \in J = (c]$, $j \leq c$. Now combining $j \leq a$, $j \leq c$ gives us $j \leq a \wedge c = 0 < b \in (b] = I$. Thus $a = i \vee j \in I = (b] = \{0, b\}$, a contradiction. Hence L is distributive.

We have seen in chapter 3 that comlement of an element in a lattice, if exists, is not unique in general. But it is not the case when the lattice is distributive. We have a lemma

Lemma 6. *In a bounded distributive lattice an element can have only one complement.*

Proof: Let L be a distributive lattice and suppose, if possible, an element $x \in L$ has two complements y_1 and y_2. Then using distributivity, $y_1 = 1 \wedge y_1 = (x \vee y_2) \wedge y_1 = (x \wedge y_1) \vee (y_2 \wedge y_1) = 0 \vee (y_2 \wedge y_1) = y_2 \wedge y_1 = y_1 \wedge y_2$. Similarly, $y_2 = 1 \wedge y_2 = (x \vee y_1) \wedge y_2 = (x \wedge y_2) \vee (y_1 \wedge y_2) = 0 \vee (y_1 \wedge y_2) = y_1 \wedge y_2$. These two give us $y_1 = y_2$. Hence the complement is unique.

Here we mention a nice characterisation of distributive lattice due to Oystein Ore (1938). Consider the lattice of all subgroups of a group G. Oystein Ore proved that the group G is locally cyclic iff the lattice of subgroups of G is distributive.

Boolean Lattice: A complemented distributive lattice is called a Boolean lattice.

Thus in a Boolean lattice every element has a unique complement.

Next we have some definitions and theorem(s) which investigate the structure of finite distributive lattices:

Definition: Let D be a distributive lattice and $J(D)$ denote the collection of all nonzero join-irreducible elements of D. Then $J(D)$ is a poset under the partial ordering inherited

from D. For $a \in D$, let us define

$$r(a) = \{x | x \leq a, x \in J(D)\} = (a] \cap J(D)$$

i.e. $r(a)$ is the set of join-irreducible elements below a.

Definition: Let P be a poset and $A \subseteq P$. We call A *hereditary* iff $x \in A$ and $y \leq x$ imply that $y \in A$. Let $H(P)$ denote the set of all hereditary subsets of P partially ordered by set inclusion. The $H(P)$ is a lattice in which meet and join are intersection and union respectively and hence $H(P)$ is a distributive lattice.

We have the following theorem

Theorem 7. *Let D be a finite distributive lattice. Then D is isomorphic to $H(J(D))$.*

Proof: Let us define the map $\Phi : D \longrightarrow H(J(D))$ by $a\Phi = r(a)$. The we prove that Φ is an isomorphism.

1-1ness: Take $a, b \in D$ such that $a\Phi = b\Phi$. Then we have $r(a) = r(b)$. This means the two sets

$$r(a) = \{x | x \leq a, x \in J(D)\}$$

and

$$r(b) = \{y | y \leq b, y \in J(D)\}$$

are equal. This is possible only when $a = b$. This proves Φ is one-to-one.

Ontoness: we have to show that for every $A \in H(J(D))$, there exists an $a \in D$ such that $a\Phi = A$. Let us set $a = \bigvee A$ (which exists because A is finite). Then as $A's$ elements are join-irreducible and $a \leq a$, for every $a \in A$, we get by definition $r(a) \supseteq A$. For reverse inclusion, we take any $x \in r(a)$. Then by definition $x \leq a$. Then we can write $x = x \wedge a = x \wedge \bigvee A = \bigvee\{x \wedge y | y \in A\}$. Now since x is join-irreducible so we will have $x = x \wedge y$, for some $y \in A$. This means $x \leq y$. But since A is hereditary, so it follows that

$x \in A$. Therefore $r(a) \subseteq A$. The two containments together give us $r(a) = A$. Thus the pre-image of $A \in H(J(D))$ is the join of A. Hence Φ is onto.

Φ is a homomorphism: By definition $(a \wedge b)\Phi = r(a \wedge b)$. Now we show that $r(a \wedge b) = r(a) \cap r(b)$. We note that $x \in r(a \wedge b) \Leftrightarrow x \leq a \wedge b \Leftrightarrow x \leq a$ and $x \leq b$ $\Leftrightarrow x \in r(a)$ and $x \in r(b) \Leftrightarrow x \in r(a) \cap r(b)$. Hence we get $r(a \wedge b) = r(a) \cap r(b)$. Therefore $(a \wedge b)\Phi = r(a \wedge b) = r(a) \cap r(b) = a\Phi \wedge b\Phi$.

Next, by definition $(a \vee b)\Phi = r(a \vee b)$. We prove that $r(a \vee b) = r(a) \cup r(b)$. It is trivial that $r(a) \cup r(b) \subseteq r(a \vee b)$. For reverse containment, let us take any $x \in r(a \vee b)$. Then by definition, $x \leq a \vee b$. From this we can write $x = x \wedge (a \vee b)$. Applying distributivity, this can be written as $x = (x \wedge a) \vee (x \wedge b)$. Now since x is join-irreducible, we shall get $x = x \wedge a$ or $x = x \wedge b$ and this implies that $x \leq a$ or $x \leq b$. Then $x \in r(a)$ or $x \in r(b)$ which means $x \in r(a) \cup r(b)$, proving that $r(a \vee b) \subseteq r(a) \cup r(b)$. Thus the two containments together imply that $r(a \vee b) = r(a) \cup r(b)$. So we have $(a \vee b)\Phi = r(a \vee b) = r(a) \cup r(b) = a\Phi \vee b\Phi$.

Therefore, Φ is a homomorphism.

Hence Φ is an isomorphism.

This proves the theorem.

Boolean Algebra: A Boolean algebra is a Bollean lattice in which $0, 1$ and $'$ (complementation) are also regarded as operations. Thus a Boolean algebra is a system: $\langle B; \wedge, \vee, ', 0, 1\rangle$, where $\wedge$, $\vee$ are binary operations; $0, 1$ are nullary operations (which just pick out an element of B)and $'$ is a $1 - ary$ operation.

Example: The $(P(S), \cap, \cup)$ is a Boolean Algebra.

Next we define

Boolean Ring: A ring R with multiplicative identity in which every element is idempotent, that is, $a^2 = a$, for all $a \in R$, is called a Boolean ring.

Boolean rings are Boolean algebras in disguise as stated in the following theorem.

Theorem 8. *Every Boolean algebra is equivalent to a Boolean ring.*

Proof: We will not give the entire proof, rather we shall give sketch of the proof. Let B be a Boolean algebra, then we define addition $+$ and multiplication . by

$$a + b = (a \wedge b') \vee (a' \wedge b)$$

$$a.b = a \wedge b$$

Then it is easy to check that these addition and multiplication satisfy all the axioms of a ring. Further, $a^2 = a.a = a \wedge a = a$, for all $a \in R$ and hence $(B, +, .)$ is a Boolean ring. Conversely, if B is Boolean ring with identity, then let's define the *join* and *meet* by

$$a \vee b = a + b - ab$$

and

$$a \wedge b = ab$$

Its again an easy calculation to verify that these $\vee$ and $\wedge$ satisfy all the algebraic axioms of a lattice. Moreover, the additive and multiplicative identities 0, 1 of the Boolean ring B act as the zero and unit element for this lattice. So B is bounded lattice. Further, for any $a \in B$, The $1 - a$ is its complement. Also the distributive identity is easily verifiable. Hence $(B, \vee, \wedge)$ is a Boolean lattice.

Modular Lattices : Modular lattices are lattices that satisfy the following identity (called the modular identity), discovered by Richard Dedekind: if $a \leqslant c, b \in L$

$$c \wedge (a \vee b) = a \vee (b \wedge c) \tag{4.2}$$

Remark: In the equality (3.2), it is trivial that

$$c \wedge (a \vee b) \geq a \vee (b \wedge c)$$

so to prove a lattice to be modular, it is sufficient to show that

$$c \wedge (a \vee b) \leq a \vee (b \wedge c)$$

Examples:

i) By taking $a \leqslant c$ in the distributive identity, we get the modular identity. Thus it implies that every distributive lattice is modular.

ii) The lattice of all ideals of a ring is a modular lattice but not distributive, in general.

Counterexample : The lattice of subgroups of a group is not modular in general.

For example, the subgroups of the group A_4 of all even permutaions on four symbols do not form a modular lattice.

But in the case of normal subgroups it is true as the following theorem states

Theorem 9. *The lattice of normal subgroups $\mathcal{N}$-sub(G) of a group G is modular.*

Proof : It is trivial to show that $\mathcal{N}$-sub(G) is a poset under set containment. Now for subgroups G_1, G_2 in $\mathcal{N}$-sub(G), let ue define $G_1 \wedge G_2 = G_1 \cap G_2$ and $G_1 \vee G_2 = \{g_1 g_2 \mid g_1 \in G_1, g_2 \in G_2\}$ = subgroup generated by G_1, G_2 which we shall denote by $G_1 G_2$. Then it is easy to check that $G_1 \cap G_2$ and $G_1 G_2$ are members of $\mathcal{N}$-sub(G). To prove $\mathcal{N}$-sub(G) to be a modular lattice, we shall show that for G_1, G_2 in $\mathcal{N}$-sub(G) such that $G_2 \subseteq G_1$, $G_1 \cap (G_2 G_3) = G_2(G_1 \cap G_3)$. For this take $x \in G_1 \cap (G_2 G_3)$. Then $x \in G_1$ and $x \in G_2 G_3$.Thus $x = g_1$ and $x = g_2 g_3$, for some $g_1 \in G_1, g_2 \in G_2, g_3 \in G_3$. From these we

can write $g_3 = g_2^{-1} g_1 \in G_1$. Thus $g_3 \in G_1 \cap G_2$ and then $g_2 g_3 \in G_2(G_1 \cap G_3)$ which implies that $x \in G_2(G_1 \cap G_3)$.Therefore we get

$$G_1 \cap (G_2 G_3) \subseteq G_2(G_1 \cap G_3)$$

Now as the reverse containment holds by the remark after the definition above, these together yield the modular identity.

This proves that $\mathcal{N}$-sub(G) is indeed a modular lattice.

Now we have a nice result characterising modular lattices:

Theorem 10. *A lattice L is modular iff it does not contain a pentagon.*

The proof of this theorem is similar to the proof of theorem 3.

Thus a modular lattice L is distributive iff it does not contain a diamond.

Next we define *intervals* in a lattice.

Interval: Let L be a lattice and $a, b \in L$. Then the interval $[a, b]$ with a and b as extremes is defined as follows

$$[a, b] = \{x \in L : a \leq x \leq b\}$$

Notion of Morphisms in Lattices:

In algebra *morphism* means *preserving the operation.* In lattice theory there are distinct operations, hence we have the following definitions.

Definition: Let L and M be two lattices and $f : L \longrightarrow M$ be a function. Then f is *isotone* if $x \leq y$ implies $f(x) \leq f(y)$. f is *join morphism* if

$$f(x \vee y) = f(x) \vee f(y))$$

for all $x, y \in L$.

f is called *meet morphism* if

$$f(x \wedge y) = f(x) \wedge f(y)$$

for all $x, y \in L$.

When f is both *join morphism* and *meet morphism* then f is called a *morphism* (or lattice-morphism).

Like in the case of other algebraic structures, a morphism f is called a *monomorphism* if it is $1-1$, an *epimorphism* if it is onto, an *isomorphism* if it is both $1-1$ and onto. f is called an *endomorphism* if $L = M$ and an *automorphism* if $L = M$ and it is an *isomorphism*.

In a modular lattice two intervals of specific form are isomorphic. We have the following theorem

Theorem 11. *Let L be a modular lattice and $a, b \in L$. Then the intervals $I[a \vee b, a]$ and $I[b, a \wedge b]$ are isomorphic.*

Sketch of Proof: Let us define the function $f : I[a \vee b, a] \longrightarrow I[b, a \wedge b]$ by $f(x) = x \wedge b$, for all x in the domain interval. Then it is easily seen that f is a lattice homomorphism. To prove that it is a bijection, we define another function $g : I[b, a \wedge b] \longrightarrow I[a \vee b, a]$ by $g(y) = y \vee a$, for all y in the domain interval. Then we easily see (using the *modularity* of L) that the compositions $f \circ g$ and $g \circ f$ are identity morphisms on the intervals $I[b, a \wedge b]$ and $I[a \vee b, a]$ respectively. This establishes that the two intervals are isomorphic.

Chapter 5

Congruences in Lattices

An equivalence relation $\ominus$ (that is, a reflexive, symmetric and transitive binary relation) on a lattice L is called a *congruence relation* iff $a_0 \equiv b_0(\ominus)$ and $a_1 \equiv b_1(\ominus)$ imply that $a_0 \wedge a_1 \equiv b_0 \wedge b_1(\ominus)$ and $a_0 \vee a_1 \equiv b_0 \vee b_1(\ominus)$.

Examples:

(1) In the integers $\mathbb{Z}$, a congruence relation is the same as congruence mod n, for some n. The case $n = 0$ gives the equality relation.

(2) In a group, a congruence relation is the same thing as the coset decomposition for some normal subgroup and in a commutative ring it is the same thing as the coset decomposition for an ideal.

(3) In a finite chain C, a congruence relation is any decomposition into intervals as depicted in figure (5.1).

(4) A congruence relation of a lattice is shown in figure (5.2).

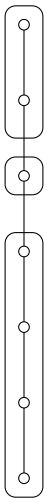

Figure 5.1: A congruence of a finite chain C_7

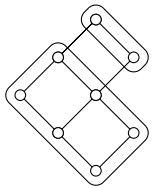

Figure 5.2: Congruence of a lattice

Now we state (without proof) a very important lemma which helps us to determine congruences of lattices.

Lemma 12. *A non-empty binary relation $\ominus$ on a lattice L is a congruence relation iff $\ominus$ satisfies the following* (1) *through* (4)*:*

(1) if $a \equiv b(mod \ominus)$, then $a \wedge b \equiv a \vee b(mod \ominus)$.

(2) if $a \leq t \leq b$ and $a \equiv b(mod \ominus)$, then $t \equiv a \equiv b(mod \ominus)$.

(3) if $a \wedge b \equiv a(mod \ominus)$, then $b \equiv a \vee b(mod \ominus)$, and dually.

(4) if $a \equiv b(mod \ominus)$ and $b \equiv c(mod \ominus)$, then $a \equiv c(mod \ominus)$.

Remark: If a_0, b_0 are two elements of a lattice L, then the smallest congruence relation $\ominus(a_0, b_0)$ on L that identifies a_0 and b_0 can be constructed by applying (1) above (unless

a_0 and b_0 are already comparable), then we apply (2) and (3) repeatedly and then (4) repeatedly. This congruence $\ominus(a_0, b_0)$ is called the principal congruence.

Congruence relations on an arbitrary lattice have an interesting connection with the distributive lattices:

Definiton: Let L be an arbitrary lattice. Then the collection $Con(L)$of all congruence relations of L form a lattice [5] with the meet and join defined as: for $\ominus_1, \ominus_2 \in L$, $\ominus_1 \wedge \ominus_2 = \ominus_1 \cap \ominus_2$, that is,

$$a \equiv b(\ominus_1 \wedge \ominus_2)$$

iff $a \equiv b(\ominus_1)$ and $a \equiv b(\ominus_2)$.

The join $\ominus_1 \vee \ominus_2$ is defined as: $a \equiv b(\ominus_1 \vee \ominus_2)$ iff there is a sequence $c_0 = a \wedge b, c_1, ..., c_{n-1} = a \vee b$ of elements of L such that $c_0 \leqslant c_1 \leqslant, ..., \leqslant c_{n-1}$ and for each i, $0 \leqslant \text{i} \lesssim n-1$, $c_i \equiv c_{i+1}(\ominus_1)$ or $c_i \equiv c_{i+1}(\ominus_2)$.

Theorem 13. *(N. Funayama and T. Nakayama) $Con(L)$ is distributive lattice.*

Proof: Let us take three congruences $\Theta, \Phi, \Psi \in con(L)$. By the first remark of chapter 4, we trivially have

$$\Theta \wedge (\Phi \vee \Psi) \geq (\Theta \wedge \Phi) \vee (\Theta \wedge \Psi)$$

so we show the reverse inequality i.e.

$$(\Theta \wedge \Phi) \vee (\Theta \wedge \Psi) \geq \Theta \wedge (\Phi \vee \Psi)$$

Taking $a \equiv b(\Theta \wedge (\Phi \vee \Psi))$, we have $a \equiv b(\Theta)$ and $a \equiv b(\Phi \vee \Psi))$. Then by above lemma $a \equiv b(\Theta)$ implies that $a \wedge b \equiv a \vee b(\Theta)$. Now consider $a \equiv b(\Phi \vee \Psi))$. By the definition of join of congruences, $a \equiv b(\Phi \vee \Psi))$ implies that there exist $z_0, z_1, \ldots, z_{n-1}$ such that $a \wedge b = z_0, z_1, \ldots, z_{n-1} = a \vee b$ such that for all $0 \leq i \leq n-2$, $z_i \equiv z_{i+1}(\Phi)$ or $z_i \equiv z_{i+1}(\Psi)$

and so $z_i \equiv z_{i+1}(\Theta)$ for each $0 \leq i \leq n-2$. Therefore we have

$$(z_i \equiv z_{i+1}(\Theta))and(z_i \equiv z_{i+1}(\Phi)orz_i \equiv z_{i+1}(\Psi))$$

$$(z_i \equiv z_{i+1}(\Theta))and(z_i \equiv z_{i+1}(\Phi)or(z_i \equiv z_{i+1}(\Theta))and(z_i \equiv z_{i+1}(\Psi)$$

$$(z_i \equiv z_{i+1}(\Theta \wedge \Phi))or(z_i \equiv z_{i+1}(\Theta \wedge \Psi)$$

for all $0 \leq i \leq n-2$. So by definition of the join $a \equiv b(\Theta \wedge \Phi) \vee (\Theta \wedge \Psi)$ and therefore

$$(\Theta \wedge \Phi) \vee (\Theta \wedge \Psi) \geq \Theta \wedge (\Phi \vee \Psi)$$

Hence the two inequalities together yield

$$(\Theta \wedge \Phi) \vee (\Theta \wedge \Psi) = \Theta \wedge (\Phi \vee \Psi)$$

This proves that $Con(L)$ is distributive lattice.

Homomorphisms and congruence relations express two different sides of the same phenomenon. To get a feel of this fact, first we need to define the factor (quotient)lattices.

Factor Lattice: Let L be a lattice and Θ be a congruence on L. Let L/Θ denote the collection of all congruence classes induced by the congruence Θ, that is,

$$L/\Theta = \{[a]\Theta : a \in L\}$$

Then it forms a lattice under

$$[a]\Theta \wedge [b]\Theta = [a \wedge b]\Theta$$

and

$$[a]\Theta \vee [b]\Theta = [a \vee b]\Theta$$

It is easy to verify the well-definedness of the two operations.

This lattice is called the factor lattice of L modulo Θ. The following lemma says that any factor lattice is a homomorphic image of a lattice:

Lemma 14. *For the congruence Θ of a lattice L, the map $\varphi : L \longrightarrow L/\Theta$ defined by $x \longmapsto [x]\Theta$ is a homomorphism of L onto L/Θ.*

Kernel of a homomorphism: Unlike the group theory or ring theory, there are three kernel concepts in lattice theory. They are defined as follows:

Let $\varphi : L \longrightarrow L_1$ be a homomorphism of L onto L_1. Define a congruence relation Θ as $x \equiv y(\Theta)$ iff $x\varphi = y\varphi$. Then this relation Θ is called the *congruence kernel of the homomorphism* φ. If L_1 has a zero, 0, the set of preimages of 0 forms and ideal of L. This ideal is called *ideal kernel of the homomorphism* φ.

If for a congruence Θ of L, L/Θ has a zero, $[a]\Theta$, then $[a]\Theta$ is an ideal of L, called the *ideal kernel of the congruence relation* Θ.

Based on the nature of the congruence classes of a congruence Θ, we define some special types of lattices:

Regular Lattices: Let L be a lattice. A congruence relation Θ of L is called *regular*, if any congruence class of Θ determines the congruence. The lattice L is called *regular* if all congruences of L are regular.

Example:

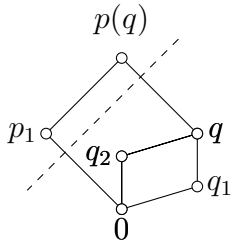

Figure 5.3: Regular Lattice $N_6 = N(p, q)$

Remark: The lattice N_6 has three congruence relations: the identity congruence relation ω, the universal congruence relation ι and a non-trivial congruence relation ψ, with the congruence classes $\{0, q_1, q_2, q\}$ and $\{p_1, p(q)\}$.

Claim: Every non-trivial congruence relation of N_6 coincides with the congruence relation ψ with the above congruence classes.

Proof of the claim: For example, let us determine the congruence relation $\Theta = con(q_1, q_2)$ generated by the pair (q_1, q_2). Then by definition the elements $(q_1, q_2), (q_2, q_1), (q_1, q_1), (q_2, q_2)$ belong to $con(q_1, q_2)$. Now as (q_1, q_2), belong to Θ, so by the lemma 12(1), $q_1 \wedge q_2 \equiv q_1 \vee q_2(\Theta)$ i.e. $(0, q)$ belong to Θ. So the elements $(q, 0), (0, 0), (q, q)$ should also be in Θ. Next we note that q_2 is such that $0 \leq q_2 \leq q$ so on applying part (2) of the lemma, we find that $(q_2, 0), (q_2, q), (q_1, 0), (q_1, q)$ are elements of Θ. Then we should also have $(0, q_2), (q, q_2), (0, q_1), (q, q_1)$ in Θ. Next we note that $q_1 \wedge p_1 = 0 \equiv q_1$ under Θ and $p(q)$ is the *join* of p_1 and q_1, so applying part (3) of the lemma, we get $p_1 \equiv p(q)(\Theta)$. Then it follows that $(p(q), p_1)$ also belong to Θ, and $(p_1, p_1), (p(q), p(q))$ should also belong to Θ. Applying part (4) of the lemma produces the pairs which have already been obtained. Thus we get $con(q_1, q_2) = \{(0, 0), (p_1, p_1), (p(q), p(q)), (q, q), (q_2, q_2), (q_1, q_1), (q_1, q_2), (q_2, q_1), (0, q), (q, 0), (q, q_1), (q_1, q), (q, q_2), (q_2, q), (p_1, p(q)), (p(q), p_1), (q_1, 0), (0, q_1), (q_2, 0), (0, q_2)\}$, containing 20 elements and its congruence classes are $\{0, q_1, q_2, q\}$ and $\{p_1, p(q)\}$.

Similarly, if we consider any other non-trivial congruence relation of the lattice N_6, we shall get the same congruence classes. Thus the claim is proved.

Hence, $Con(p_1, 0) = \iota$. In other words, $p_1 \equiv 0$ *implies* that $q_1 \equiv 0$, but $q_1 \equiv 0$ *does not imply* that $p_1 \equiv 0$.

We shall utilise the lattice N_6 to construct a chopped lattice in a representation theorem in chapter 6.

Uniform Lattices: Let L be a lattice. A congruence relation Θ of L is called *uniform*, if any two congruence classes of Θ are of the same size (cardinality). The lattice L is called *uniform* if all congruences of L are uniform.

Isoform Lattices : Let L be a lattice. We call a congruence relation $\ominus$ of L *isoform*, if any two congruence classes of $\ominus$ are isomorphic (as lattices). Lattice L is called *isoform* if all congruences of L are isoform.

Chapter 6

Representation of Distributive Lattices

In this chapter we shall study the representation of finite distributive lattices and some related results. According to theorem 13, the congruence lattice, $Con(L)$, of a finite lattice L is a distributive lattice, a result by N. Funayama and T. Nakayama [12]. Its converse is a result of R. P. Dilworth from 1944 ([6]): *Every finite distributive lattice D can be represented as the congruence lattice, $Con(L)$, of a finite lattice L.*

From application point of view, it is interesting to know the size of the lattice whose congruence lattice is isomorphic to the lattice of Dilworth's theorem. It was worked out by Grätzer, Schmidt and Lakser: The lattice constructed by Dilworth ([6]) and Grätzer, Schmidt ([7]) showed that if D is a distributive lattice having n join-irreducible elements then there exists a lattice L with $O(2^{2n})$ elements such that $D \cong Con(L)$. Grätzer and Lakser ([8]) improved the size of the lattice L by showing that there exists a lattice L with $O(n^3)$ elements such that $D \cong Con(L)$.

Further improving the size of the lattice Grätzer, Lakser and Schmidt ([9]) constructed

a lattice L with $O(n^2)$ elements such that $D \cong Con(L)$ and this is the best known.

This gives the theorem:

Theorem 15. *Let $\alpha \geq 2$. If D is a distributive lattice with n join-irreducible elements, then D can be represented by the congruence lattice of a lattice L with $O(n^\alpha)$ elements.*

The representation of distributive lattices has been studied extensively. Many results have been obtained to make the lattice L *nicer* to represent D. Many properties (P) have been obtained together with which L represents the finite distributive lattice D. For example, if (P) is sectionally complemented or isoform, then L with (P) represents a finite distributive lattice.

In chapter 1 we have defined atoms in a poset. Here we talk of the this and some related notions in lattices.

Atoms in a Lattice: Let L be a lattice with underlying poset P. An element $a \in L$ is called an *atom* of L if it is an atom in P. L is called *atomic* if its underlying poset is atomic. An atomic lattice L is called *atomistic* lattice if it is atomic and every non-minimal element can be expressed as a join of atoms.

Example of atomistic lattice: Let S be any set and $P(S)$ be its power set. It is a lattice with the usual union and intersection as the lattice operations join and meet. The empty set ϕ is the unique minimal element. As each singleton in $P(S)$ covers ϕ, the singletons are atoms of this lattice. Also, every non-empty set in $P(S)$ has an atom below it, so $P(S)$ is atomic lattice. Moreover, every non-empty subset of $P(S)$ can be written as a union of singletons, it follows that $P(S)$ is an atomistic lattice.

Example of non-atomistic lattice: For another example, we can consider $\mathbb{Z}^+$ ordered by $a \leq b$ iff $a|b$. Then 1 is the minimal element and every prime p is an atom. Let us define the lattice binary operations by $a \wedge b = gcd(a, b)$, and $a \vee b = lcm(a, b)$. Then it is

an atomic lattice. But it is not atomistic since, for example, 4 is not join of $2's$:

$$4 \neq 2 \vee 2 = lcm\{2, 2\} = 1$$

36 is not join of $2's$ and 3's:

$$36 \neq 2 \vee 2 \vee 3 \vee 3 = lcm\{2, 2, 3, 3\} = 6$$

Before mentioning the results describing the representation of finite distributive lattices, we introduce the concept of chopped lattices which are important in representing the finite distributive lattices.

Chopped Lattice: Let M be a poset satisfying the following two condition:

(1) $inf\{a, b\}$ exists in M, for every $a, b \in M$:

(2) $sup\{a, b\}$ exists for those pairs $a, b \in M$ having a common upper bound in M.

We define in M:

$$a \wedge b = inf\{a, b\}$$

and

$$a \vee b = sup\{a, b\}$$

whenever $sup\{a, b\}$ exists in M. These make M into a partial lattice, called a chopped lattice.

The congruences and ideals of chopped lattices are defined in the similar way as done for lattices. So here we have the results similar to those stated for the lattices.

Lemma 16. *The set $Con(M)$ of all congruences of a finite chopped lattice M partially ordered by set inclusion is a lattice.*

Example:

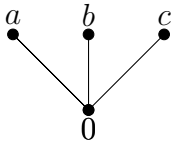

Figure 6.1: Chopped Lattice M_0

Remark: One can obtain a chopped lattice M by taking a finite lattice L with unit element 1 and defining $M = L - 1$ i.e. chopping off the unit element of a finite lattice produces a chopped lattice. The converse also holds: by adding a unit element 1 to a chopped lattice M, one obtains a finite lattice L.

Lemma 17. *The set $Id(M)$ of all ideals of a finite chopped lattice M partially ordered by set inclusion is a lattice.*

The importance of chopped lattices is revealed in the following lemma due to G. Grätzer and H Lakser [11]:

Lemma 18. *Let M be a finite chopped lattice. Then, for every congruence relation Θ of M, there exists one and only one congruence relation $\bar{\Theta}$ of $Id(M)$ such that, for $a, b \in M$, $id(a) \equiv id(b)(\bar{\Theta})$ iff $a \equiv b(\Theta)$*

Proof: We shall use the notation $id(a) = (a]$, for the principal ideal generated by a. Let Θ be a congruence relation on M. For $Y \subseteq M$, let us set $[Y]\Theta = \cup([y]\Theta | y \in Y)$, which is same as writing $[Y]\Theta = \{x | x \equiv y(\Theta), \text{for some } y \in Y\}$. Now we define a binary relation $\bar{\Theta}$ on $Id(M)$ by $I \equiv J(\bar{\Theta})$ iff $[I]\Theta = [J]\Theta$.

Claim: $\bar{\Theta}$ is a congruence relation on $Id(M)$.

(i) **Reflexivity**: As $[I]\Theta = [I]\Theta$, it follows by definition that $I \equiv I(\bar{\Theta})$. So $\bar{\Theta}$ is reflexive.

(ii) **Symmetricity**: Let $I \equiv J(\bar{\Theta})$. Then by definition, $[I]\Theta = [J]\Theta$, which can also be written as $[J]\Theta = [I]\Theta$ and then by the definition we get $J \equiv I(\bar{\Theta})$. So $\bar{\Theta}$ is symmetric.

(iii) **Transitivity**: For three ideals I, J, K in $Id(M)$, let us take $I \equiv J(\bar{\Theta})$ and $J \equiv K(\bar{\Theta})$. Then by definition we shall get $[I]\Theta = [J]\Theta$ and $[J]\Theta = [K]\Theta$ which gives us the equality $[I]\Theta = [K]\Theta$ and then by definition it follows that $I \equiv K(\bar{\Theta})$. So $\bar{\Theta}$ is transitive.

Thus upto here $\bar{\Theta}$ is a an equivalance relation.

Next we show that $\bar{\Theta}$ is compatible for the *meet* and *join*. To prove it we shall show that if

$$I \equiv J(\bar{\Theta})$$

and so

$$[I]\Theta = [J]\Theta \tag{6.1}$$

then for any ideal $T \in Id(M)$,

$$I \cap T \equiv J \cap T(\bar{\Theta}) \tag{6.2}$$

and

$$I \vee T \equiv J \vee T(\bar{\Theta}) \tag{6.3}$$

To establish (6.2), let us take an $x \in I \cap T$. Then $x \in I$. Now by definition of $[I]\Theta$, we have $[I] \subseteq [I]\Theta$ and by equation (6.1) we have $[I]\Theta \subseteq [J]\Theta$, so $x \in I$ implies that $x \in [J]\Theta$. Then by definition of $[J]\Theta$, we shall have $x \equiv y(\Theta)$, for some $y \in J$. Now since Θ is a congruence relation on M, so by $x \equiv y(\Theta)$ we can have $x \wedge x \equiv x \wedge y(\Theta)$ which means that

$$x \equiv x \wedge y(\Theta) \tag{6.4}$$

Now $y \in J$ and J is an ideal so by closure propert for *meet*, we shall have $x \wedge y \in J$. Similarly, as $x \in T$ and T is an ideal so we shall have $x \wedge y \in T$. These two together with (6.4) imply that $x \in J \cap T$. Thus we have $I \cap T \subseteq J \cap T$, which implies that $[I \cap T]\Theta \subseteq$

$[J \cap T]\Theta$. Similarly, we can show that $[J \cap T]\Theta \subseteq [I \cap T]\Theta$. These two containments yield $[I \cap T]\Theta = [J \cap T]\Theta$. Therefore by definition of $\bar{\Theta}$, we get $I \cap T \equiv J \cap T(\bar{\Theta})$. This establishes equation (6.2).

Next we establish (6.3). To prove it, we shall use the definition of join of two ideals from chapter 2, where we have defined

$$I \vee J = \bigcup (U_i(I, J) | i < \omega)$$

Towards proving (6.3), we take an $x \in I \vee T$. Then we shall have $x \in U_i$, for some $i (i < \omega)$.

Claim: $U_i \subseteq [J \vee T]\Theta$, for all $i (i < \omega)$. We use induction on i. For $i = 0$, $U_0 = I \vee T$. Now as $[I]\Theta = [J]\Theta$ and $I \subseteq [I]\Theta$, so we have $I \subseteq [I]\Theta \subseteq [J]\Theta$ i.e. we get $I \subseteq [J]\Theta$. Therefore we have $U_0 = I \vee T \subseteq [J]\Theta \cup T \subseteq [J \vee T]\Theta$. So for $i = 0$, it is true. Suppose it holds for $i - 1$, that is $U_{i-1} \subseteq [J \vee T]\Theta$, then we shall show that $U_i \subseteq [J \vee T]\Theta$. From above we have $x \in U_i$, so by definition $x \leq t_0 \vee t_1$, for some $t_0, t_1 \in U_{i-1}$, and by induction hypothesis $U_{i-1} \subseteq [J \vee T]\Theta$, so $t_0, t_1 \in [J \vee T]\Theta$. Then by definition of $[J \vee T]\Theta$, we shall have $t_0 \equiv u_0(\Theta)$ and $t_1 \equiv u_1(\Theta)$, for some $u_0, u_1 \in J \vee T$. From which we can have

$$t_0 \equiv t_0 \wedge u_0(\Theta) \text{ and } t_1 \equiv t_1 \wedge u_1(\Theta) \tag{6.5}$$

Now we note that $t_0 \vee t_1$ is an upper bound for the two elements set $\{t_0 \wedge u_0, t_1 \wedge u_1\}$. So by definiton of chopped lattice this set must have a supremum. Thus $(t_0 \wedge u_0) \vee (t_1 \wedge u_1))$ does exist. Now by compatibility of Θ for join, we can write from eqns (6.5), $t_0 \vee t_1 \equiv ((t_0 \wedge u_0) \vee (t_1 \wedge u_1))(\Theta)$. Also from above we have $x \leq t_0 \vee t_1$, which gives us

$$x = x \wedge (t_0 \vee t_1) = x \wedge ((t_0 \wedge u_0) \vee (t_1 \wedge u_1))(\Theta) \tag{6.6}$$

Now as $u_0, u_1 \in J \vee T$ and it is an ideal so we shall have $t_0 \wedge u_0, t_1 \wedge u_1 \in J \vee T$ and so by

closure property for join, we will get

$$x \wedge ((t_0 \wedge u_0) \vee (t_1 \wedge u_1)) \in J \vee T \tag{6.7}$$

Let us write $x \wedge ((t_0 \wedge u_0) \vee (t_1 \wedge u_1)) = t^{'}$, then $t^{'} \in J \vee T$ and then by eqn (6.6), we can write $x \equiv t^{'}(\Theta)$, for $t^{'} \in J \vee T$. Then by definition of $[J \vee T]\Theta$, we shal have $x \in [J \vee T]\Theta$. Hence the claim is true for all $i(i<\omega)$. Therefore we have $U_i \subseteq [J \vee T]\Theta$, for all $i(i<\omega)$. Now since $I \vee T = \bigcup(U_i|i<\omega)$ and each $U_i \subseteq [J \vee T]\Theta$, therefore $\bigcup(U_i|i<\omega) \subseteq [J \vee T]\Theta$ i.e. $I \vee T \subseteq [J \vee T]\Theta$. Similarly, it can be shown that $J \vee T \subseteq [I \vee T]\Theta$. Then by definition of $\bar{\Theta}$, these two containments yield

$$I \vee T \equiv J \vee T(\bar{\Theta})$$

which establishes the compatibility for join.

This proves that $\bar{\Theta}$ is indeed a congruence relation on $Id(M)$.

Now we prove the *iff* of the lemma as follows.

($\Rightarrow$) Suppose $(a] \equiv (b](\bar{\Theta})$, then $a \equiv b_1(\Theta)$ and $a_1 \equiv b(\Theta)$, for some $a_1 \leq a$, $b_1 \leq b$. By compatibility, it follows that $a \vee a_1 \equiv b_1 \vee a_1(\Theta)$ and $a_1 \vee b_1 \equiv b \vee b_1(\Theta)$. By transitivity, these two together imply that $a \vee a_1 \equiv b \vee b_1(\Theta)$. But $a_1 \leq a$ implies that $a_1 \vee a = a$, and $b_1 \leq b$ implies that $b_1 \vee b = b$. Therefore $a \vee a_1 \equiv b \vee b_1(\Theta)$ implies that $a \equiv b(\Theta)$.

($\Leftarrow$) suppose that $a \equiv b(\Theta)$, then we show that $(a] \equiv (b](\bar{\Theta})$. Take any $x \in (a]$, then by definition of principal ideal generated by a, we have $x \leq a$. Then from $a \equiv b(\Theta)$, we get that $x \leq b(\Theta)$ and so $x \wedge b \equiv x(\Theta)$ or $x \equiv x \wedge b(\Theta)$. This implies that $(a] \subseteq [(b]]\Theta$. Similarly, we can get $(b] \subseteq [(a]]\Theta$. Therefore by definition of $\bar{\Theta}$, we get $(a] \equiv (b](\bar{\Theta})$.

The uniqueness of the congruence $\bar{\Theta}$ is easily verifiable.

This proves the lemma completely.

Remark: This result is very significant. It means that to construct a finite lattice L to

represent a finite distributive lattice D as a congruence lattice, it is sufficient to construct a finite chopped lattice M, since $Con(M) \cong Con(IdM) = Con(L)$, where $L = IdM$.

Now we state a representation theorem due to G. Grätzer and E. T. Schmidt [7]

Theorem 19. *Every finite distributive lattice D can be represented as the congruence lattice of a finite sectionally complemented lattice L.*

We shall illustrate the above theorem in the form of the following theorem:

Theorem 20. *Let P be a finite order. Then there exists a chopped lattice M such that $Con_J M$ is isomorphic to P, where $Con_J M$ is the lattice of join irreducible congruences of M.*

Illustration: We illustrate it by taking a chain D of four elements and condsidering the meet-semilattice M_0 of join irreducible elemets of D together with 0. We use the lattice N_6 of figure 5.1 to construct the finite chopped lattice M. We take two copies $N(a, b)$ and $N(b, c)$ of the gadget.

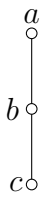

Figure 6.2: P

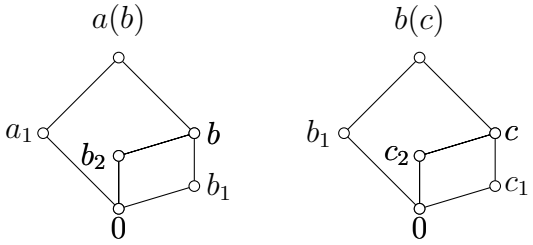

Figure 6.3: Lattices $N(a, b)$ and $N(b, c)$

They have a common ideal $I = \{0, b_1\}$ So we can merge them and form the chopped lattice

$$M = Merge(N(a, b), N(b, c))$$

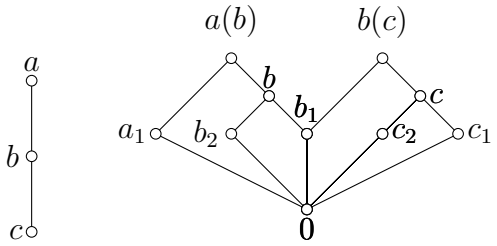

Figure 6.4: The merged lattice M

The proof of the fact that $L = IdM$ is sectionally complemented is not so easy. Towards proving this, G. Grätzer H. Lakser and M. Roody [7] have answered the following problem.

Problem: Let M be a finite sectionally complemented chopped lattice. Under what conditions is IdM sectionally complemented?

Solution: G. Grätzer H. Lakser and M. Roody proved that if M is finite sectionally complemented chopped lattice with exactly two maximal elements m_1, m_2 and $m_1 \wedge m_2$ is an atom of M, then IdM is sectionally complemented.

In continuation of the illustration for theorem 20, we need to find the join irreducible congruences of the chopped lattice M in figure (6.4). We assert that these are the principle congruences generated by the pairs $(0, a_1)$, $(0, b_1)$, $(0, c_1)$, where $Con(0, a_1)$, $Con(0, b_1)$, $Con(0, c_1)$ can be determined applying lemma 12 repeatedly as follows (similar to as we have done in claim in chapter 5): (We shall determine only one of these congruences, say, $Con(0, b_1)$) and shall list $Con(0, a_1)$ and $Con(0, c_1)$ directly).

We determine the congruence $Con(0, b_1) = \Psi$ by applying lemma 12 as follows:

By definition, the element $(0, b_1)$ belongs to Ψ.Then the elements $(b_1, 0)$, $(0, 0)$, (b_1, b_1) should also belong to Ψ. Now since $b_2 \wedge b_1 = 0 \equiv b_1(\Psi)$, so by lemma 12(3), $b_2 \equiv b_1 \vee b_2 =$

$b(\Psi)$ i.e. (b_2, b) should belong to Ψ. Then we should have the elements (b, b_2), $((b, b))$, (b_2, b_2) in Ψ too. Next pick the elements b_1, a_1 and see that $(0, b_1)$ belongs to Ψ so by part (3) of the lemma, we should have the element $(a_1, a(b))$ in Ψ and then must also have the elements (a_1, a_1), $(a(b), a_1)$, $(a(b), a(b))$ in Ψ. Now the elements b_1, c_2, are such that $(b_1, 0)$ is in Ψ so we shall have $(c_2, b(c))$ also in Ψ. This will force the elements (c_2, c_2), $(b(c), c_2)$ and $(b(c), b(c))$ to be in Ψ. Now we have $(c_2, b(c))$ in Ψ such that $c_2 \leq c \leq b(c)$, so the application of part (2) of the lemma gives that the elements $(b(c), c)$, $(c, b(c))$, (c, c_2), (c_2, c) are in Ψ, so by transitivity (c, c) should also be in Ψ. Looking at the elements b_1, c_1, we see that $(b_1, 0)$ belongs to Ψ so the elements $(c_1, b(c))$, (c_1, c_1), $(b(c), c_1)$ should also belong to Ψ. Lastly, we have $(b(c), c_1)$ such that $c_1 \leq c \leq b(c)$, so part (2) of the lemma yields that the pairs (c, c_1), (c_1, c) are also in Ψ. Finally, we get the congruence generated by $(0, b_1)$ as $Con(0, b_1) = \{(0,0), (a_1, a_1), (a(b), a(b)), (b, b), (b_2, b_2), (b_1, b_1), (b(c), b(c)), (c, c), (c_2, c_2), (c_1, c_1), (0, b_1), (b_1, 0), (b_2, b), (b, b_2), (a_1, a(b)), (a(b), a_1), (c_2, b(c)), (b(c), c_2), (b(c), c), (c, b(c)), (c, c_2), (c_2, c), (c_1, b(c)), (b(c), c_1), (c, c_1), (c_1, c), (0, c_1), (c_1, 0), (b_1, b(c)), (b(c), b_1), (b_1, c_1), (c_1, b_1), (0, b(c)), (b(c), 0), (b_1, c), (c, b_1), (b_1, c_2), (c_2, b_1), (c, 0), (0, c)\}$.

Similarly, we determine the congruences $Con(0, a_1)$ and $Con(0, c_1)$ generated by $(0, a_1)$, $(0, c_1)$ which turn out to be

$Con(0, a_1) = \{(0,0), (a_1, a_1), (a(b), a(b)), (b, b), (b_2, b_2), (b_1, b_1), (b(c), b(c)), (c, c), (c_2, c_2), (c_1, c_1), (0, a_1), (a_1, 0), (b_2, a(b)), (a(b), b_2), (a(b), b), (b, a(b)), (b, b_2), (b_2, b), (b_1, a(b)), (a(b), b_1), (b, a(b)), (b, b_1), (b_1, b), (0, b_1), (b_1, 0), (a_1, a(b)), (a(b), a_1), (c_2, b(c)), (b(c), c_2), (b(c), c), (c, b(c)), (c, c_2), (c_2, c), (c_1, b(c)), (b(c), c_1), (c, c_1), (c_1, c), (0, c_1), (c_1, 0), (b_1, b(c)), (b(c), b_1), (b_1, c_1), (c_1, b_1), (0, b(c)), (b(c), 0), (b_1, c), (c, b_1), (b_1, c_2), (c_2, b_1), (0, a(b)), (a(b), 0), (a_1, b_2), (b_2, a_1), (a_1, b), (b, a_1), (a_1, b_1), (b_1, a_1), (c_2, c_1), (c_1, c_2), (a(b), c_1), (c_1, a(b)), (a, a(b)), (c, 0), (o, c), (c_2, 0), (0, c_2)\}$

and

$Con(0, c_1) = \{(0,0), (a_1, a_1), (a(b), a(b)), (b, b), (b_2, b_2), (b_1, b_1), (b(c), b(c)), (c, c), (c_2, c_2), (c_1, c_1), (0, c_1), (c_1, 0), (c, c_2), (c_2, c), (b_1, b(c)), (b(c), b_1)\}$

respectively.

Next we need to show that P and $Con_J M$ are isomorphic. This isomorphism is established by sending $x \in P$ to the principal congruence generated by the pair $(0, x_1)$, that is, to $Con(0, x_1)$. Thus $P \cong Con_J M$.

This completes the illustration for the proof of theorem 20.

If we know the number of *join-irreducible* elements of a distributive lattice, then we can have a nice representation. Before stating that, we have a definition

Definition: A lattice diagram is said to be *planar* if no two lines in it intersect. A finite lattice is *planar* iff it has a planar diagram.

Theorem 21. *Let D be a finite distributive lattice with n join-irreducible elements. Then there exists a planar lattice L of $O(n^2)$ elements such that $Con(L) \cong D$.*

We shall illustrate the proof of theorem 21 on the following distributive lattice

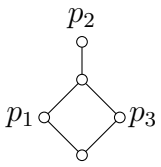

Figure 6.5: Distributive lattice D

The following figure shows the poset P of join-irreducible elements of D and the chain C formed from P. The length of the chain will be $2P = 6$ and the intervals of the chain are marked with the elements of P. This marking is called *coloring*. To illustrate the proof of

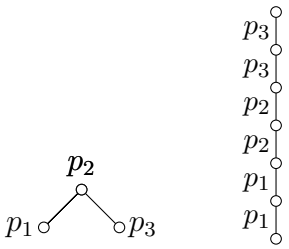

Figure 6.6: The poset P and the chain C

theorem 21, we use the following two building blocks M_3 and $N_{5,5}$ of figure 6.7 and figure 6.8 respectively.

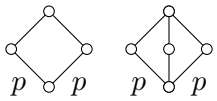

Figure 6.7: The first building block, for $p<q$

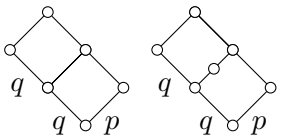

Figure 6.8: The second building block, for $p<q$

Now to construct the lattice L, we take $C^2(= C \times C)$, the direct product of the chain C of figure 6.6 with itself. We construct the lattice L by adding black-filled elements to this direct poduct as follows: if both the lower edges of a covering square in the direct product C^2 have the same color, then we add an element to it to make it a covering M_3. If in C^2 we have a covering $C_2 \times C_3$ (a rectangle in C^2 with length C_2 and breadth C_3), where the C_2 edge is colored by p, the C_3 edge is colored by q twice, where $p<q$ then we add an element to make it an $N_{5,5}$. We obtain the lattice of figure 6.9. The copies of $N_{5,5}$ in the diagram have been marked by black-filled elements.

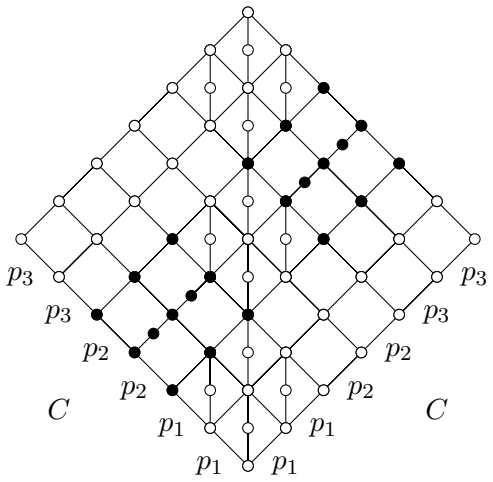

Figure 6.9: The lattice L constructed from C^2

It is easy to show that, in general, $|L| \leq kn^2$, for some constant k and that $D \cong Con(L)$. This isomorphism is established by assigning to $p \in P$ the congruence of L generated by collapsing any (all) prime intervals of color p.

Bibliography

[1] G. Birkhoff, *Lattice theory*, .

[2] P. Erdős, A. Hajnal, A. Mate, R. Rado, *Combinatorial set theory: Partion Relation for cardinals*, North-Holland, 1984, 282-285.

[3] C. Kuratowski, *Sur ene caraeterisation des alephs*, Fund. Mat. 38 (1951), 14-17.

[4] John C. Simms, *Sierpiński's theorem*, Simon Stevin 65 (1991), no. 1-2, 69163.

[5] G. Grätzer, *General lattice theory.*

[6] K. P. Bogart, R. Freese, and J. P. S. Kung (editors), *The Dilworth theorems. Selected papers of Robert P. Dilworth*, Birkhäuser Verlag, Basel-Boston, 1990, pp. 460-464.

[7] G. Grätzer and E. T. Schmidt, *On congruence lattices of lattices*, Acta Math. Acad. Sci. Hungar. **13** (1962), 179-185.

[8] G. Grätzer and H. Lakser, *Homomorphisms of distributive lattices as restrictions of congruences*, Con. J. Math.**38**(1986), 1122-1134.

[9] G. Grätzer, H. Lakser, and E. T. Schmidt,*Congruence lattices of small planar lattices, Proc. Amer. Math. Soc.***123** (1995), 2619-2623.

[10] E. T. Schmidt *Every finite distributive lattice is the congruence lattice of some modular lattice*, Algebra Universalis 4 (1974), 49-57.

[11] G. Grätzer and H. Lakser, *Extension theorems on congruences of partial lattices*, Notices Amer. Math. Soc. **15** (1968), 1122-1134.

[12] N. Funayama and T. Nakayama, *On the congruence relations on lattices*, Proc. Imp. Acad. Tokyo **18** (1942), 530-531