Partially Ordered Sets

And Applications

Pallavi

A dissertation submitted for the partial fulfilment of
BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali

April 2015

Certificate of Examination

This is to certify that the dissertation titled "Partially Ordered Sets and Applications" submitted by Ms.Pallavi (Reg.No.MS10062) for the partial fulfilment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Lingaraj Sahu	Dr. Amit Kulshrestha	Dr. Chanchal Kumar
		(Supervisor)

Dated: April 24, 2015

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Chanchal Kumar at Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Pallavi

(Candidate)

Dated: April 24, 2015

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Chanchal Kumar

(Supervisor)

Acknowledgement

First and foremost, I would like to thank my thesis supervisor Dr. Chanchal Kumar for his invaluable guidance and support. I feel extremely fortunate to work under his supervision. Without his supervision and constant help this dissertation would not have been possible. I am sincerely grateful to him for introducing me to this area of mathematics.

I also use this opportunity to express my gratitude to Dr. Amit Kulshrestha for his help and advice whenever I needed.

A special thanks to my family, my friends who always supported me and finally, I would like to thank IISER Mohali for providing me with the facilities being required and conducive conditions for my thesis work.

Pallavi

Abstract

This thesis provides a systematic exposition of the theory of incidence algebras and Möbius functions. So, for the initial preliminary work, partially ordered sets, lattices and their types are studied. The central theme revolves around the fundamental work of Gian-Carlo Rota on Möbius function of partially ordered sets. We see that the Möbius function can be expressed as reduced Euler characteristic of the order complex of a partially ordered set and since Euler characteristic is a topological invariant, so turns out the Möbius function on a poset. Furthermore, this Möbius function on a poset is just the classical number-theoretic Möbius function whose inverse is the zeta (ζ) function in incidence algebra. Möbius inversion theory also setups a generalization of the Principle of Inclusion-Exclusion and establishes an analogue of the "fundamental theorem of calculus." Finally, applications of Möbius functions have been examined, starting with the result by Rota that expresses the chromatic polynomial of a graph in terms of Möbius function of a poset and closing by zeta polynomial of a partially ordered set.

Contents

Chapter 1

Introduction

The fundamental work of Gian-carlo Rota on the theory of Möbius functions [Rot64] had a far reaching impact on Combinatorics, in particular and Mathematics, in general. In this thesis, one of our primary aims is to study properties of Möbius functions of a partially ordered set (poset) and present applications of Möbius functions in various counting problems. The basic concepts of ordered structures, such as posets, lattices and Boolean algebras, are introduced with examples to make the thesis self-contained.

George Boole introduced Boolean algebras, which proved to be a suitable set up to carry out calculus of logic. A number of mathematicians, such as George Boole, C. S. Peirce, E. Schröder and R. Dedekind, have studied ordered structures, but the credit of developing theory of posets and lattices as a branch of mathematical studies goes to G. Birkhoff. The pioneering work of Birkhoff done in 1930's appeared in his book [Bir67] that paved a way for further development. An extensive book on "General Lattice Theory" by G. Grätzer [Grä78] appeared in 1978.

The *principle of inclusion-exclusion* is an important result in combinatorics and it has provided solutions to many counting problems. The Möbius inversion formula is a far reaching generalization of the principle of inclusion-exclusion. The idea of incidence algebra was implicit in the work of R. Dedekind but the Möbius inversion formula for posets was proved by L. Weisner in 1935 and independently by P. Hall shortly thereafter. However, in words of Rota, "Weisner and Hall did not pursue the combinatorial implications of their work; nor was an attempt made to systematically investigate the properties of Möbius functions." Only in the seminal work of Rota [Rot64], it has been established that the Möbius inversion formula on a poset is a fundamental principle of enumeration.

The homology theory for posets was developed by many mathematicians [Far79], but combinatorial implications of such homology theory was perceived for first time only in the seminal work of Rota. It has been demonstrated that just like the (reduced) Euler characteristic is a fundamental invariant of a topological space, so is the Möbius function of a partially ordered set. Rota showed that Möbius function of a finite semimodular lattice (or a geometric lattice) alternates in sign. The Möbius function of $L_n(q)$ is obtained by P. Hall [Hal36], while the Möbius function of Π_n is obtained independently by Schützenberger and Rota. The zeta polynomial of a finite poset appeared in the work of R. Stanley [Sta74].

In order to understand the relevance of Möbius function of a poset, we recall the classical Möbius function. The number theoretic function $\mu : \mathbb{P} \to \mathbb{Z}$ defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^t, & n = p_1 p_2 .... p_t, \text{ (distinct primes } p_i) \\ 0, & \text{otherwise.} \end{cases}$$

is called the classical Möbius function. Möbius in 1832 proved an inversion formula for numerical functions $f, g : \mathbb{P} \to \mathbb{Z}$:

$$g(n) = \sum_{k|n} f(k) \quad \Leftrightarrow \quad f(n) = \sum_{k|n} g(k)\mu(\tfrac{n}{k}).$$

This inversion formula is used to obtain formula for well known arithmetic functions in elementary number theory. For example, it can be easily shown that

$$n = \sum_{k|n} \phi(k),$$

where ϕ is the Euler phi-function. Thus, by classical Möbius inversion formula, we obtain an expression

$$\phi(n) = \sum_{k|n} k \ \mu(\frac{n}{k}) = \sum_{k|n} \frac{n}{k} \ \mu(k).$$

If $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}.....{p_t}^{\alpha_t}$; $\alpha_i \geq 1$, then

$$\phi(n) = \sum_{S \subseteq [t]} \frac{n}{\big(\prod\limits_{i \in S} p_i\big)} (-1)^{|S|} = n \prod_{i=1}^{t} \Big(1 - \frac{1}{p_i}\Big).$$

In an another application of classical Möbius inversion formula, we obtain a formula for the number U_d of irreducible monic polynomial of degree d over a finite field $\mathbb{F}_q$ (with q elements). It can be shown that

$$x^{q^n} - x = \prod p(x),$$

where product runs over all irreducible monic polynomials $p(x)$ over $\mathbb{F}_q$ of degree d dividing n. On comparing degrees, we get

$$q^n = \sum_{d|n} d\, U_d.$$

Hence, the classical Möbius inversion formula gives

$$nU_n = \sum_{d|n} q^{\frac{n}{d}}\ \mu(d) \quad \text{or} \quad U_n = \frac{1}{n} \sum_{d|n} q^{\frac{n}{d}}\ \mu(d).$$

If $F, G : \mathbb{P} \to \mathbb{Z}$ are numerical functions, then we associate a *formal Dirichlet series*

$$\hat{F}(s) = \sum_{n=1}^{\infty} \frac{F(n)}{n^s} \quad \text{and} \quad \hat{G}(s) = \sum_{n=1}^{\infty} \frac{G(n)}{n^s}.$$

Now, consider the product $\hat{H}(s) = \hat{F}(s)\hat{G}(s)$ of two formal Dirichlet series as a function of s. We have

$$\hat{H}(s) = \Big(\sum_{n=1}^{\infty} \frac{F(n)}{n^s}\Big)\Big(\sum_{m=1}^{\infty} \frac{G(m)}{m^s}\Big) = \sum_{n=1}^{\infty} \frac{\big(\sum\limits_{ij=n} F(i)G(j)\big)}{n^s}.$$

This shows that $\hat{H}$ is the formal Dirichlet series of a numerical function $H : \mathbb{P} \to \mathbb{Z}$ given by

$$H(n) = \sum_{k|n} F(k)G(\frac{n}{k}).$$

We say that H is obtained by convolution product $H = F * G$ of F and G.

Now, consider the numerical function $E : \mathbb{P} \to \mathbb{Z}$ given by $E(n) = 1$ for all $n \in \mathbb{P}$. Then,

$$\hat{E}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the *Riemann zeta function* $\zeta(s)$. The inverse of Riemann zeta function $\zeta^{-1}(s)$ is given by

$$\zeta^{-1}(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

We see that for numerical functions $F, G : \mathbb{P} \to \mathbb{Z}$,

$$F * E = G \Leftrightarrow G * \mu = F.$$

This is a motivation for defining Möbius function as the inverse of zeta function in Chapter 6.

Now, we give a brief overview of the thesis.

The first chapter is a formal introduction. In Chapter 2, basic notions of posets along with examples are introduced. Hasse diagrams of various finite posets are illustrated. A poset is said to be graded if all maximal chains have the same length. There exists a unique rank function for a graded poset. Also, the rank-generating functions of certain posets are calculated. Further, new ways of constructing posets such as direct sum, ordinal sum, cartesian product and ordinal product of two posets are also given. If both posets are graded, then the rank-generating function of the new poset is given in terms of rank-generating functions of the individual posets.

Chapter 3 is a brief introduction to the theory of lattices. Modular and Distributive lattices are studied in Chapter 4. Birkhoff's representation theorem for finite distributive lattices is proved in this chapter.

Chapter 5 is an introduction to Boolean lattices and Boolean algebras. It is proved that the concept of a Boolean lattice, a Boolean algebra and a Boolean ring are equivalent. Stone's representation theorem for a finite Boolean algebra is proved in this chapter.

Chapter 6 is the most important chapter of this thesis. Incidence algebra, zeta function and Möbius function of a poset is introduced. Combinatorial interpretation of values of power of the zeta function ζ is given. If ζ is the zeta function of a poset P, then for $x \leq y$ in P, we have

- $\zeta^k(x, y) =$ number of k-multichains from x to y in P.
- $(\zeta - 1)^k(x, y) =$ number of k-chains from x to y in P.
- $(2 - \zeta)^{-1}(x, y) =$ total number of chains from x to y in P.

Möbius inversion formula along with the dual version is derived in this chapter. Product theorem for Möbius function is proved and using the product theorem, Möbius function for B_n and D_n are obtained.

For a poset P, $\Delta(P)$ denotes its order complex and $\widehat{P}$ is the poset obtained by adjoining the least element $\hat{0}$ and the greatest element $\hat{1}$ to P. Then,

$$\mu_{\widehat{P}}(\hat{0}, \hat{1}) = \widetilde{\chi}(\Delta(P)),$$

where $\widetilde{\chi}(\Delta(P))$ is the reduced Euler characteristic of $\Delta(P)$.

For a lattice or a semimodular lattice, a simpler recurrence formula for the Möbius function is given. Using these results, Möbius functions of $L_n(q)$ and Π_n are obtained. Some applications of Möbius functions in certain counting problems is given in the last chapter.

Chapter 2

Partially Ordered Sets

2.1 Basic Notions

Definition 2.1.1. A *partially ordered set* P or a *poset* is a set equipped with a binary relation $\leq$ which satisfies the following axioms:

1. Reflexivity: For all $x \in P$, $x \leq x$.
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$.
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$.

The nomenclature "partially ordered set" suggests that not every pair of elements in it are related. Consequently, it leads to the notion of comparable and incomparable elements in a poset.

Before discussing examples of posets, we shall describe some relevant terms used in the setting of partial ordered structures.

Definition 2.1.2. Two elements x and y of a poset P are said to be *comparable* if $x \leq y$ or $y \leq x$, otherwise they are termed as *incomparable*.

Definition 2.1.3. By a *chain* in a poset, we mean a subset in which any two elements are comparable. A chain in a poset is also called a *totally* or a *linearly ordered set*. Unlike a chain in a poset, in which any two elements are comparable, a subset of a poset in which no two elements are comparable is called an *antichain*.

There is an elegant pictorial way to represent (finite) posets called Hasse diagrams of posets.

Definition 2.1.4. Let P be a poset.

1. For given $x, y \in P$, we say y *covers* x if $x < y$ and there is no element z satisfying $x < z < y$. In other words, y is an immediate successor of x and x is an immediate predecessor of y.

2. The *Hasse diagram* of a finite poset P can be defined as the graph whose vertices are the elements of P and there is an edge between two vertices $x, y \in P$, if either x covers y or y covers x. As a convention in the Hasse diagram of a poset, bigger elements are placed above the smaller elements.

Remark 2.1.5. A finite poset is completely determined by its Hasse diagram. Diagrams are very useful in understanding abstract mathematical concepts. For example: If the Hasse diagram of a poset $P = \{a, b, c, d\}$ is as follows,

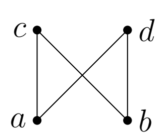


Figure 2.1

then it is clear that a and c are comparable whereas a and b are incomparable elements.

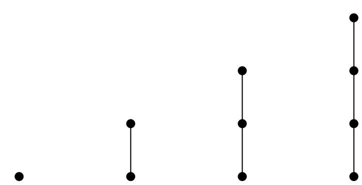
Examples 2.1.6. (Finite Posets)

1. Let $\mathbb{P}$ be the set of positive integers and $[n] = \{1, 2, ..., n\}$ for $n \in \mathbb{P}$. Then the set $[n]$ with its usual order forms an n-element poset in which any two elements are comparable. This poset is denoted by $\mathbf{n}$ and it is clearly a totally ordered set.

2. Let $\mathbb{N}$ be the set of non-negative integers and $n \in \mathbb{N}$. Then $[n] = \{1, 2, ..., n\}$ if $n \geq 1$ and $[0] = \emptyset$, the empty set. Let B_n be the power set of $[n]$, then B_n is a poset under the order induced by inclusion.

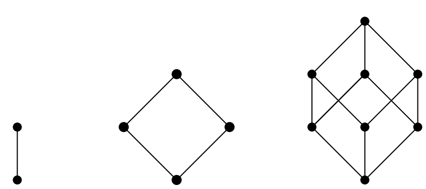
3. Let $n \in \mathbb{P}$ and D_n be the set of all positive integral divisors of n. Then D_n is a poset in which $i \leq j$ if i divides j (i.e. $i \mid j$).

Corresponding Hasse diagrams:



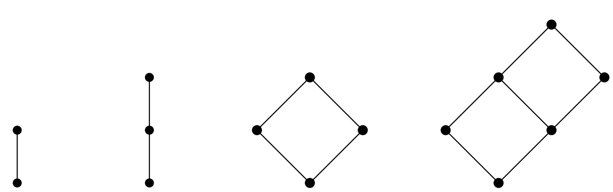
1 **2** **3** **4**

Figure 2.2: $[n]$



B_1 B_2 B_3

Figure 2.3: B_n



D_2 D_4 D_6 D_{12}

Figure 2.4: D_n

Definition 2.1.7. Two posets P and Q are said to be *isomorphic* if there exists an order-preserving bijection $\phi : P \to Q$ whose inverse is also order preserving. The mapping ϕ is called an *order isomorphism.*

Isomorphic posets have the same order structures and they are considered equivalent. The Hasse diagrams of isomorphic posets are isomorphic as graphs and they look the same. From Figure 2.3, 2.4 and 2.5, we see that $B_1 \simeq D_2 \simeq \mathbf{2}$, $D_4 \simeq \mathbf{3}$ and $D_6 \simeq B_2$. We also notice that $D_p \simeq \mathbf{2}$ for any prime p.

Some more examples:

We will give a few more interesting examples of finite posets but first we need to introduce related notions.

(1) Let $[n] = \{1, 2, ..., n\}$ where $n \in \mathbb{P}$. By *partition of* $[n]$, we mean a mutually exclusive and exhaustive family of subsets. In other words, a family of disjoint subsets of $[n]$ is a partition if their union is the entire set $[n]$. A partition π is said to be a $refinement$ of a partition σ if every block of π is contained in a block of σ. And for a given $n \in \mathbb{P}$, let Π_n to be the set of partitions of $[n]$ ordered by refinement. For example: if $[n] = 3$, then $\pi = \{1|2|3\}$ is a refinement of $\sigma = \{12|3\}$ in Π_3. The Hasse diagrams of Π_n for small values of $n = 1, 2, 3, 4$ are as follows:

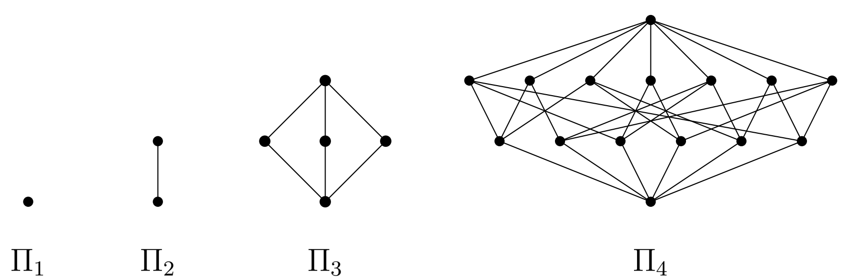
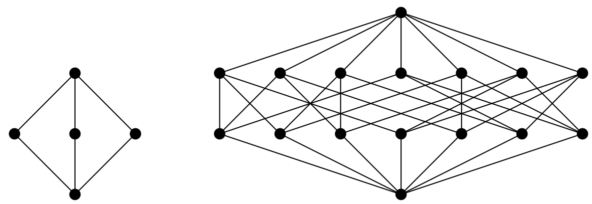


Figure 2.5

(2) Another example of finite poset consists of subspaces of a finite dimensional vector space. We shall see later that these form an interesting class of posets called *modular* posets.

Consider an n-dimensional vector space $V_n(q)$ over the q-element field $\mathbb{F}_q$ and let $L_n(q)$ be the set of all possible subspaces of $V_n(q)$. Then, $L_n(q)$ is certainly a finite poset ordered by inclusion. For $n = 2, 3$ and $q = 2$; the Hasse diagram of $L_n(q)$ is described as follows:

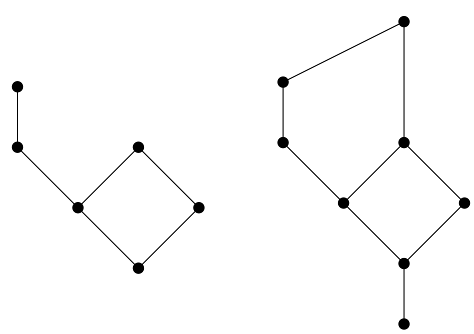


$L_2(2)$ $L_3(2)$

Figure 2.6

Definition 2.1.8. A poset P is said to have a *least element* (denoted $\hat{0}$) if there exists an element $\hat{0} \in P$ satisfying $x \geq \hat{0}$ for all $x \in P$. Similarly, a poset P is said to have a *greatest element* (denoted $\hat{1}$) if there exists an element $\hat{1} \in P$ satisfying $x \leq \hat{1}$ for all $x \in P$.

Clearly, least and/or greatest elements of a poset P, if exists, must be unique. A poset need not have a least/greatest element. In any case, given a poset P, we form a new poset $\widehat{P}$ obtained by adjoining a least element $\hat{0}$ and greatest element $\hat{1}$ to the poset P ($\hat{0}$ and $\hat{1}$ are not elements of P). The construction of $\widehat{P}$ from P is illustrated in the following Hasse diagram.



P $\widehat{P}$

Figure 2.7

We now define subposets, intervals and other relevant terms in context of a poset.

Definition 2.1.9. Let P be a poset.

1. A subset Q of P under the induced ordering is called a *subposet* of P. For $x, y \in Q$, we say that $x \leq y$ in the induced order in Q if and only if $x \leq y$ in P. Therefore, number of subposets of a finite poset P is exactly $2^{|P|}$.

2. For $x \leq y$ in P, the special subposet $[x, y] = \{z \in P : x \leq z \leq y\}$, is called a *closed interval* determined by x and y. Similarly, *open interval* (x, y) is defined as $(x, y) = \{z \in P : x < z < y\}$.

3. A subposet Q of P is defined to be *convex* if $y \in Q$ whenever $x < y < z$ in P and $x, z \in Q$. Thus, an interval can be regarded as convex.

We have mainly studied properties of a finite poset, but sometimes one can prove similar results in case the poset is locally finite.

Definition 2.1.10. A poset P is called a *locally finite poset* if every interval of P is finite.

Examples: (1) $\mathbb{Z}$ is not a finite poset with the usual order but it is locally finite; $\mathbb{Z}^n$ with coordinate wise order ($(x_1, x_2, ..., x_n) \leq (y_1, y_2, ..., y_n)$ if $x_i \leq y_i$ $\forall$ i) is also locally finite.
(2) The set $\mathbb{Q}$ is neither finite nor locally finite.

Now, we introduce various terminologies associated with chains in a poset.

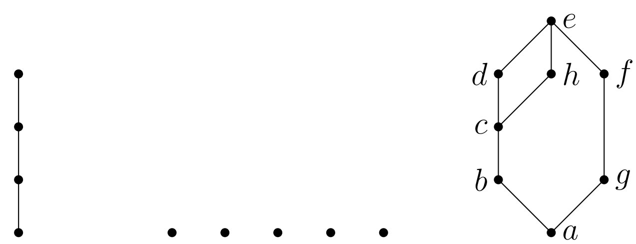
Definition 2.1.11. Let P be a poset.

1. A chain C is called a *maximal chain* in P if there does not exist a chain D in P such that $C \subsetneq D$.

2. A chain C is called a *saturated chain* in P if there does not exist $z \in P - C$ with $x < z < y$ for some $x, y \in C$ and such that $C \cup \{z\}$ is a chain. Clearly, every maximal chain is saturated but a saturated chain need not be maximal.

3. A *multichain* in a poset P is a multiset whose underlying set is a chain. A multichain of length n in a poset P is just a sequence $x_0 \leq x_1 \leq ..... \leq x_n$ of elements of P. On the other hand, a chain of length n in a poset P is a sequence $x_0 < x_1 < ..... < x_n$ of elements of P.

4. The *length* $\ell(C)$ of a finite chain C in a poset P is defined as $\ell(C) = |C| - 1$. In other words, length of a chain C counts the number of edges (rather than vertices) of C in the Hasse diagram of P.



(a) Chain (b) Antichain (c)

Figure 2.8

Examples 2.1.12. A chain and an antichain are depicted in Figure 2.8 (a) and (b). We can see that $a < b < c < d < e$ and $a < g < f < e$ are two maximal chains of different length in the poset shown in Figure 2.8 (c). It also shows $b < c < h < e$ and $b < c < e$ as saturated and non-saturated chains respectively whereas $b < c < h < f$ corresponds neither to a chain nor to an antichain.

Definition 2.1.13. An *order ideal* of a poset P is a subset I of P such that if $x \in I$ and $y \leq x$, then $y \in I$. Similarly, a *filter* is defined as a subset I of P such that if $x \in I$ and $y \geq x$, then $y \in I$.

Definition 2.1.14. The collection of all order ideals of P, ordered by inclusion forms a poset. This poset is denoted by $\mathcal{J}(P)$.

Proposition 2.1.15. *Let P be a finite poset. Then there is a one to one correspondence between order ideals I of P and antichains A of P.*

Proof. Given an order ideal I of P, let A be the set of maximal elements in I. Clearly, A is an antichain in P. On the other hand, for an antichain A in P, an order ideal I of P is given by $I = \{x \in P : x \leq y \text{ for some } y \in A\}$. □

Remark 2.1.16. Let P be a finite poset.

1. If $A = \{x_1, ..., x_k\}$ is a subset of P, then we denote the associated order ideal $I = \langle x_1, ..., x_k \rangle = \{x \in P : x \leq x_i \text{ for some } i\}$.

2. If $A = \{x\}$, then the associated order ideal $\langle x \rangle = \Lambda_x$ is called the *principal order ideal* generated by x. Similarly, $V_x = \{y \in P : y \geq x\}$ denotes the *principal filter* generated by x.

2.2 Graded Posets

A graded poset in simple terms has a well defined level assigned to each element which in turn facilitates the systematic study of posets.

Definition 2.2.1. The *rank of a finite poset* P is defined as

$$Rank(P) = max\{\ell(C) : C \text{ is a chain of } P\},$$

where $\ell(C)$ denotes the length of chain C. The length of an interval $[x, y]$ of P is denoted by $\ell(x, y)$.

Definition 2.2.2. A poset P is said to be *graded of rank* n if every maximal chain of P has the same length n.

Definition 2.2.3. The *rank function* of a poset P is a function $\rho : P \to \{0, 1, .., n\}$, $n \in \mathbb{N}$ which satisfy the following:

1. If x is a minimal element of P, then $\rho(x) = 0$.

2. $\rho(y) = \rho(x) + 1$, if y covers x in P.

If $\rho(x) = i$, then we say that the element x has *rank* i.

Theorem 2.2.4. *If a poset is graded of rank n, then there exists a unique rank function for a poset.*

Proof. Let P be a graded poset of rank n. Let $x \in P$. Then $\{x\}$ is a chain in P and hence $\{x\}$ is contained in a maximal chain $C = x_0 < x_1 < ..... < x_n$ of length n with $x_i = x$. Define $\rho(x) = i$. We need to show that if for any other maximal chain $C' = x'_0 < x'_1 < ..... < x'_n$ with $x = x'_j$, then we must have $i = j$. Otherwise, either $i > j$ or $i < j$. For $i > j$, we see that

$$x_0 < x_1 < ..... < x_i = x = x'_j < x'_{j+1} < ..... < x'_n$$

is a chain of length $n + (i - j) > n$, a contradiction. Similarly, for $i < j$, we see that

$$x'_0 < x'_1 < ..... < x'_j = x = x_i < x_{i+1} < ..... < x_n$$

is a chain of length $n + (j - i) > n$, again a contradiction. Therefore, the rank function ρ is well defined. Clearly, ρ has the properties as in Definition 2.2.3 and it is unique. □

Examples 2.2.5.

Table 2.1: Graded Posets

Poset P	Rank of $x \in P$	Rank of P
n	$x - 1$	$n - 1$
B_n	card x	n
D_n	number of prime divisors of x (counting multiplicity)	number of prime divisors of n
Π_n	$n - \|x\|$	$n - 1$
$L_n(q)$	dim x	n

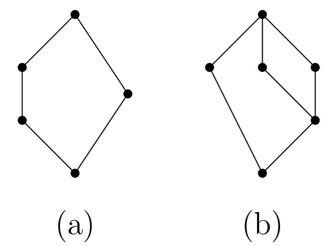


Figure 2.9: Hasse diagram of some non-graded posets

Definition 2.2.6. If P(assuming finite) is graded of rank n and it has p_i elements of rank i, then the polynomial (in variable q)

$$F(P,q) = \sum_{i=0}^{n} p_i q^i,$$

is called the *rank-generating function* of P.

Examples:

1. $F(\mathbf{n}, q)$

   Here, $p_i = 1$ for $0 \leq i \leq n-1$.

   So, $F(\mathbf{n}, q) = 1 + q + ... + q^{n-1} = \frac{q^n - 1}{q-1}$.

2. $F(B_n, q)$

   Here, $p_i = \big|\{A \subseteq [n] : |A| = i\}\big| = \binom{n}{i}$ for $0 \leq i \leq n$.

   Thus, $F(B_n, q) = \sum\limits_{i=0}^{n} \binom{n}{i} q^i = (1+q)^n$.

2.3 Construction of New Posets

We perform various operations on posets to obtain new posets from the old ones.

Definition 2.3.1. (Disjoint union or Direct sum)

Assume that P and Q are posets on disjoint sets. The (disjoint) union $P \cup Q$ under the ordering $\leq$ given by $x \leq y$ in P (both $x, y \in P$) or $x \leq y$ in Q (both $x, y \in Q$) is a poset. This poset is called the *disjoint union or direct sum* of P and Q and it is denoted by $P + Q$. The Hasse diagram of $P + Q$ consists of placing Hasse diagrams of P and Q side by side.

Definition 2.3.2. (Ordinal sum)

Assume that P and Q are posets on disjoint sets. The (disjoint) union $P \cup Q$ under the ordering $\leq$ given by $x \leq y$ in P (both $x, y \in P$) or $x \leq y$ in Q (both $x, y \in Q$) or $x \leq y$ if $x \in P$ and $y \in Q$ is a poset. This poset is called the *ordinal sum* of P and Q and it is denoted by $P \oplus Q$.

Examples 2.3.3.

1. If $P = (\mathbf{1} + \mathbf{1}) \oplus \mathbf{1}$ and $Q = \mathbf{1} \oplus \mathbf{1}$, then the Hasse diagram of P, Q and $P + Q$ are as follows:

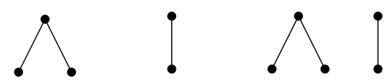


Figure 2.10

2. We denote by nP, the disjoint union of P with itself n times, hence an n-element antichain is isomorphic to $n\mathbf{1}$.

3. An n-element chain is given by $\mathbf{n} = \mathbf{1} \oplus \mathbf{1} \oplus ...... \oplus \mathbf{1}$ (n-times).

4. Let $P = (\mathbf{1} \oplus (\mathbf{1} + \mathbf{1}))$ and $Q = \mathbf{1} \oplus \mathbf{1}$, then we can clearly see from Figure 2.11 that $P \oplus Q \ncong P \oplus Q$.

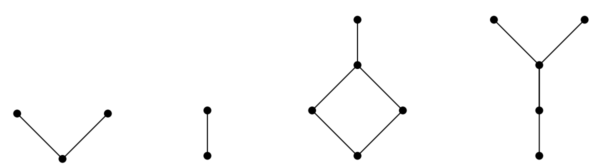


Figure 2.11

Remark 2.3.4. (1) Posets that can be built up using above mentioned operations are known as *series-parallel* posets.

(2) On a four-element set, there are exactly 16 partially ordered structures possible. All these posets with one exception are built from the poset $\mathbf{1}$ using the operations of disjoint union and/or ordinal sum. In the following Figure 2.12, Hasse diagram (a) represents the poset $(\mathbf{1} \oplus \mathbf{1}) + \mathbf{1}$, while the Hasse diagram (b) cannot be expressed as direct and/or ordinal sum of the poset $\mathbf{1}$.

(a) (b)

Figure 2.12

Definition 2.3.5. (Direct or cartesian product)
For posets P and Q, their *direct product* is the poset $P \times Q$ on the set $\{(x, y) : x \in P$ and $y \in Q\}$ such that $(x, y) \leq (x', y')$ in $P \times Q$ if $x \leq x'$ in P and $y \leq y'$ in Q. We denote by P^n, the direct product of P with itself n-times.

The product $P \times Q$ of finite posets can be illustrated with the help of Hasse diagrams. In the Hasse diagram of P, we replace each vertex x of P by a copy Q_x of Hasse diagram of Q. Further, corresponding vertices of Q_x and Q_y are connected if x and y are connected in the Hasse diagram of P. This construction gives us the Hasse diagram of $P \times Q$. For example: If $P = (\mathbf{1} + \mathbf{1}) \oplus \mathbf{1}$ and $Q = \mathbf{1} \oplus \mathbf{1}$, then the Hasse diagram of $P \times Q$ is

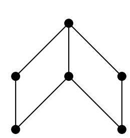


Figure 2.13

Remark 2.3.6. Clearly, $P \times Q \simeq Q \times P$. In fact, $f : P \times Q \to Q \times P$ given by $f(x, y) = (y, x)$ is an ordered isomorphism.

Theorem 2.3.7. *If P and Q are graded posets with rank-generating functions $F(P,q)$ and $F(Q,q)$ respectively, then $P \times Q$ is graded of*

$$Rank(P \times Q) = RankP + RankQ,$$

and with rank-generating function

$$F(P \times Q, q) = F(P,q)F(Q,q).$$

Proof. Let Rank(P) $= r$ and Rank(Q) $= s$. Then (all) maximal chains in P and Q are of length r and s respectively. Let $x_0 < x_1 < ..... < x_r$ be a maximal chain in P and $y_0 < y_1 < ..... < y_s$ be a maximal chain in Q. Then from the direct product construction of $P \times Q$ ($i.e.(x,y) \leq (x',y') \Leftrightarrow x \leq x'$ and $y \leq y'$), we see that the chain

$$(x_0, y_0) < (x_1, y_0) < ..... < (x_r, y_0) < (x_r, y_1) < ..... < (x_r, y_s)$$

is maximal in $P \times Q$, whose length is clearly $r + s$. All maximal chains are obtained in the similar manner. Then $P \times Q$ is graded and Rank($P \times Q$) $= r + s$.

Let $x \in P$ and $y \in Q$ such that rank(x) $= i$ and rank(y) $= j$. As above rank(x, y) $= i+j$. Let $n = i + j$. Then the number of elements of $P \times Q$ of length n is given by $\{(x,y) \in P \times Q :$ rank$(x)+$ rank$(y) = n\}$.
Let $F(P,q) = \sum\limits_{\alpha=0}^{r} a_\alpha q^\alpha$ and $F(Q,q) = \sum\limits_{\beta=0}^{s} b_\beta q^\beta$, where $a_\alpha =$ number of elements in P of rank α, and $b_\beta =$ number of elements in Q of rank β.
Clearly, number of elements in $(P \times Q)$ of rank $n = \sum\limits_{\alpha+\beta=n} a_\alpha b_\beta$. Therefore,

$$\begin{aligned} F(P \times Q, q) &= \sum_{n=0}^{r+s} \Big(\sum_{\alpha+\beta=n} a_\alpha b_\beta \Big) q^n = \Big(\sum_{\alpha=0}^{r} a_\alpha q^\alpha \Big) \Big(\sum_{\beta=0}^{s} b_\beta q^\beta \Big) \\ &= F(P,q)F(Q,q). \end{aligned}$$

□

Definition 2.3.8. (Ordinal product)

For posets P and Q, their *ordinal product* $P \otimes Q$ is the partial ordering defined on the set $\{(x,y) : x \in P$ and $y \in Q\}$ by setting $(x,y) \leq (x',y')$ if

(a) $x = x'$ and $y \leq y'$, or

(b) $x < x'$

The way to construct the Hasse diagram of $P \otimes Q$ is as follows: In the Hasse diagram of P, replace each element x of P by a copy Q_x of Hasse diagram of Q and then connect every maximal element of Q_x with every minimal element of Q_y whenever y covers x in P.

Remark 2.3.9. In general, $P \otimes Q$ and $Q \otimes P$ are not isomorphic and they do not have the same rank-generating function.

Theorem 2.3.10. *In case P and Q are graded, Q has rank s and their rank-generating functions are $F(P, q)$ and $F(Q, q)$ respectively, then we obtain,*

$$Rank(P \otimes Q) = RankP + RankQ + (RankP)(RankQ),$$

and rank-generating function of $P \otimes Q$ is

$$F(P \otimes Q, q) = F(P, q^{s+1})F(Q, q).$$

Proof. Let $\text{Rank}(P) = r$ and $\text{Rank}(Q) = s$. Consider a maximal chain $x_0 < x_1 < ..... < x_r$ in P and a maximal chain $y_0 < y_1 < ..... < y_s$ in Q. Since the ordering in $P \otimes Q$ is given by $((x, y) \leq (x', y') \Leftrightarrow x < x'$ or $x = x'$ & $y \leq y')$, we see that

$$(x_0, y_0) < ..... < (x_0, y_s) < (x_1, y_0) < ..... < (x_1, y_s) < (x_2, y_0) < .....$$

$$...... < (x_r, y_0) < (x_r, y_1) < ..... < (x_r, y_s)$$

is a maximal chain in $P \otimes Q$. Clearly, then the length of this chain is $(s+1)(r+1)-1 = rs + r + s$. So, $\text{Rank}(P \otimes Q)$ is $rs + r + s$.

Similarly, if $x \in P$ and $y \in Q$ such that $\text{rank}(x) = i$ and $\text{rank}(y) = j$, then the $\text{rank}(x, y)$ in $P \otimes Q$ can be calculated as above and $\text{rank}(x, y) = [(s+1)i+j+1]-1$. Thus, the number of elements of $P \otimes Q$ of rank n is given by $\{(x, y) \in P \otimes Q : (s+1)\text{rank}(x)+\text{rank}(y) = n\}$. Let $F(P, q) = \sum\limits_{\alpha=0}^{r} a_\alpha q^\alpha$ and $F(Q, q) = \sum\limits_{\beta=0}^{s} b_\beta q^\beta$, where a_α = number of elements in P of rank α, and b_β = number of elements in Q of rank β.

Then, the number of elements in $P \otimes Q$ of rank $n = \sum\limits_{(s+1)\alpha+\beta=n} a_\alpha b_\beta$.

Therefore,

$$\begin{aligned}
F(P \otimes Q, q) &= \sum_{n=0}^{r+s} \Bigg(\sum_{(s+1)\alpha+\beta=n} a_\alpha b_\beta \Bigg) q^n = \sum_{n=0}^{r+s} \sum_{\alpha,\beta} a_\alpha (q^{s+1})^\alpha b_\beta q^\beta \\
&= \Bigg(\sum_\alpha a_\alpha (q^{s+1})^\alpha \Bigg) \Bigg(\sum_\beta b_\beta q^\beta \Bigg) \\
&= F(P, q^{s+1}) F(Q, q).
\end{aligned}$$

□

Definition 2.3.11. (Dual of a Poset)

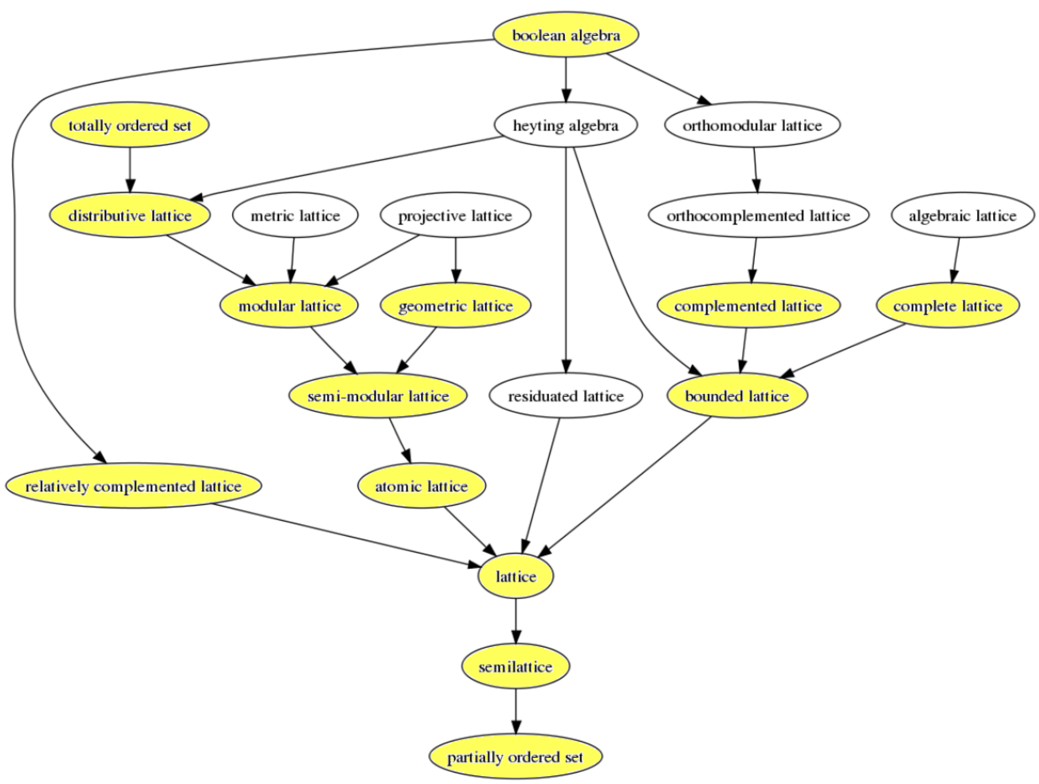
Dual of a poset P is the poset P^* with the same underlying set as P, but with $x \leq y$ in P^* if and only if $y \leq x$ in P. P is called *self-dual* if P and P^* are isomorphic.

Remark 2.3.12. We see that filter and order ideal are dual notions. If I is an order ideal in the poset P, then I is a filter in the dual poset P^* and vice-versa.

Definition 2.3.13. For the given posets P and Q, Q^P denotes the set of all order-preserving maps $f : P \to Q$ i.e. $x \leq y$ in P implies $f(x) \leq f(y)$ in Q. Q^P is given the structure of a poset by defining $f \leq g$ if $f(x) \leq g(x)$ for all $x \in P$.

Chapter 3

Lattices



Source: http://en.wikipedia.org/wiki/Map_of_lattices

3.1 Basics of Lattice Theory

Definition 3.1.1. Let P be a poset. An *upper bound* of elements x and y in P, is an element $z \in P$ which satisfies $z \geq x$ and $z \geq y$. A *least upper bound* or *supremum* z of x and y is the minimum of all possible upper bounds of x and y i.e. every upper bound w of x and y satisfies $w \geq z$. A least upper bound of elements x and y is denoted by $x \vee y$ (x join y).

Dually, we define lower bound and greatest lower bound of x and y in P by reversing the order as follows: An element $u \in P$ is said to be a *lower bound* of x and y if $u \leq x$ and $u \leq y$. A lower bound u of x and y is called the *greatest lower bound* or $infimum$ of x and y if $u \geq v$ for every lower bound v of x and y. The greatest lower bound of x and y, if exists, is denoted by $x \wedge y$ (x meet y).

Definition 3.1.2. A *lattice* is a partially ordered set L for which every pair of elements has a least upper bound and a greatest lower bound in L.

Properties of meet and join:

1. The join($\vee$) and meet($\wedge$) operations are commutative, associative and satisfies idempotent laws. Since $x \vee y = \sup\{x, y\}$ and $x \wedge y = \inf\{x, y\}$, we clearly have $x \vee y = y \vee x$ as well as $x \wedge y = y \wedge x$ for all $x, y \in L$. Also, $x \vee (y \vee z) = \sup \{x, y, z\} = (x \vee y) \vee z$ and it's dual i.e. $x \wedge (y \wedge z) = \inf \{x, y, z\} = (x \wedge y) \wedge z$ for $x, y, z \in L$. Furthermore, $x \vee x = x = x \wedge x$ for all $x \in L$.

2. The join($\vee$) and meet($\wedge$) operations satisfy absorption laws i.e. $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$ for $x, y \in L$. Since $x \leq \sup\{x, y\} = x \vee y$, so then $x \wedge (x \vee y) = \inf\{x, x \vee y\} = x$. Also, $x \wedge y = \inf\{x, y\} \leq x$ gives us that $x \vee (x \wedge y) = \sup\{x, x \wedge y\} = x$.

3. For $x, y \in L$, the following conditions are equivalent $x \wedge y = x \Leftrightarrow x \vee y = y \Leftrightarrow x \leq y$. Assume $x \wedge y = x = \inf\{x, y\}$, this implies that $x \leq y$ which in turn is equivalent to $x \vee y = y$. And if $x \vee y = y = \sup\{x, y\}$, then $x \leq \sup\{x, y\}$ i.e. $x \leq y$ which also means that $x \wedge y = x$.

It turns out that the properties (1) and (2) of join($\vee$) and meet($\wedge$) defines a lattice structure.

Examples 3.1.3. The posets $\mathbf{n}$, B_n, D_n and $L_n(q)$ are all lattices.

Table 3.1: Lattices

Lattice L	$\sup\{a,b\} = a \vee b$	$\inf\{a,b\} = a \wedge b$	$\hat{0}$	$\hat{1}$
$\mathbf{n}$	max{a,b}	min{a,b}	1	n
B_n	$A \cup B$	$A \cap B$	$\emptyset$	$\{1, 2, ..., n\}$
D_n	lcm{a,b}	gcd{a,b}	1	n
$L_n(q)$	$A + B$	$A \cap B$	$\{0\}$	$V_n(q)$

Proposition 3.1.4. *Suppose L be a set with two binary operations $+$ and $\cdot$ such that both $+$ and $\cdot$ satisfy the following properties:*
(1) $+$ and $\cdot$ both are commutative, associative and satisfies idempotent laws. (2) $+$ and $\cdot$ obeys absorption laws, i.e. $x + (x \cdot y) = x$ and $x \cdot (x + y) = x$ for all $x, y \in L$.

We define order relation $\leq$ on L given by $x \leq y$ if $x + y = y$ or equivalently $x.y = x$. Then, there is a unique lattice structure on $(L, \leq)$ such that $x + y = x \vee y = sup\{x, y\}$ and $x.y = x \wedge y = inf\{x, y\}$.

Proof. Observe that $\leq$ is a partial order. The idempotent law $x.x = x$ implies that $x \leq x$. If $x \leq y$, and $y \leq x$, then $x = x.y = y$. For transitivity, if $x \leq y$, and $y \leq z$, then $x.z = (x.y).z = x.(y.z) = x.y = x$ which implies $x \leq z$. Thus, L is a poset and laws of absorption ensure that $x.y = x$ is equivalent to $x + y = y$ for $x \leq y$.

Next, we see that $x.y$ is a lower bound for x and y, since $(x.y).x = (y.x).x = y.(x.x) = y.x = x.y$, so $(x.y) \leq x$ and $(x.y).y = x.(y.y) = x.y$, so $(x.y) \leq y$. Also, if $u \leq x$ and $u \leq y$, then $u.x = u = u.y$. Hence, $u.(x.y) = (u.x).y = u.y = u$, i.e., $u \leq (x.y)$. Consequently, $x.y$ is the infimum of x and y. Dually, we get the characterization for supremum following which we obtain a lattice L. $\square$

Remark 3.1.5. All finite lattices have the least element $\hat{0}$ and the greatest element $\hat{1}$.

Definition 3.1.6. If every pair of elements of a poset P possess a meet (or a join), then P is said to be a *meet-semilattice* (or a *join-semilattice*). A lattice is a both i.e. a meet-semilattice as well as a join-semilattice.

Proposition 3.1.7. *If P is a finite meet-semilattice with $\hat{1}$, then P is a lattice. And, dually a finite join-semilattice with $\hat{0}$ is a lattice.*

Proof. For given $x, y \in P$, let S be the set containing all possible upper bounds of x and y i.e. $S = \{z \in P : z \geq x \text{ and } z \geq y\}$. Then S is finite since P is finite and is non-empty since $\hat{1} \in S$. But then, it is also a meet-semilattice, so for all $w, z \in S$, $w \wedge z$ exists and $w \wedge z \geq x$ and $w \wedge z \geq y$. Thus, by induction meet of finitely many elements of a meet-semilattice exists and therefore, we have $x \vee y = \inf\{S\}$.

□

Remark 3.1.8. The above stated proposition may fail for an infinite lattice L because an arbitrary subset of L need not have a supremum or a infimum.

Definition 3.1.9. If every subset of a lattice L has a meet and a join, then L is called a *complete lattice*.

Clearly, a complete lattice has a $\hat{0} = \inf L$ and $\hat{1} = \sup L$. We can easily see that B_n, D_n are complete lattices.

Definition 3.1.10. Let L be a lattice.

1. A lattice L is said to be a *bounded lattice* if it has the least element $\hat{0}$ and the greatest element $\hat{1}$.

2. A lattice L is said to be *complemented* if for every $x \in L$, there exists $y \in L$ such that $x \wedge y = \hat{0}$ and $x \vee y = \hat{1}$.

3. A lattice L in which for every $x \in L$, the complement y is unique, then L is categorized as *uniquely complemented*.

4. A *relatively complemented lattice* is a lattice L in which every interval of L is itself complemented i.e. whenever $x \in [w, z]$, there exists $y \in [w, z]$ such that $x \wedge y = w$ and $x \vee y = z$.

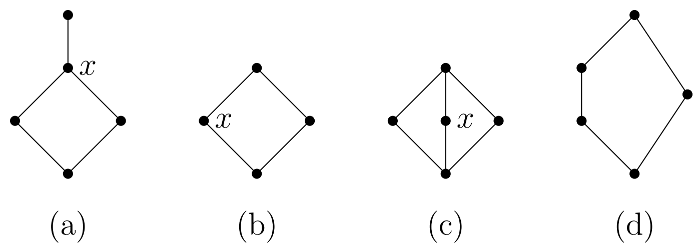


Figure 3.1: Lattices depicting x with no complement (a), a unique complement (b) and more than one complement (c) whereas lattice in (d) is complemented but not relatively complemented

Definition 3.1.11. An *atom* of a finite lattice L is an element which covers $\hat{0}$ and L is called an *atomic* or a *point lattice* if every element of L can be expressed as the join of atoms.

Dually, a *coatom* is an element covered by $\hat{1}$ and L is said to be a *coatomic lattice* if every element of L is the meet of coatoms.

Example: B_n is atomic while $\mathbf{n}$ $(n \geq 3)$ is not.

3.2 Construction of New Lattices

Proposition 3.2.1. *If L and M are lattices, then L^*, $L \times M$, $\widehat{L+M}$ and $L \oplus M$ are also lattices.*

Proof. In case of L^* supremum and infimum will be reverse of as that for L. For $L \times M$, take coordinate wise join (or meet) to obtain the supremum (or infimum) i.e. for all $(x, y)(x', y') \in L \times M$, $(x, y) \vee (x', y') = (x \vee x', y \vee y')$ and $(x, y) \wedge (x', y') = (x \wedge x', y \wedge y')$. $\widehat{L+M}$ is a lattice because by definition it contains $\hat{0}$ and $\hat{1}$. And finally, for $L \oplus M$ supremum is supremum of M and infimum is infimum of L.

□

Remark 3.2.2. $L + M$ is never a lattice unless one of them is void(empty).

Chapter 4

Modular and Distributive Lattices

In this chapter, we study modular and distributive lattices. A representation theorem for finite distributive lattice is also given.

4.1 Semimodularity and Modularity

Proposition 4.1.1. *Let L be a finite lattice. Then the following conditions are equivalent:*

1. *L is graded and for all $x, y \in L$, the rank function ρ of L satisfies $\rho(x) + \rho(y) \geq \rho(x \wedge y) + \rho(x \vee y)$.*

2. *If x and y both cover $x \wedge y$, then $x \vee y$ covers both x and y for all $x, y \in L$.*

Proof. (1) $\Rightarrow$ (2) Assume that both x and y cover $x \wedge y$ but $x \vee y$ does not cover x(or y). Then, $\rho(x) = \rho(y) = \rho(x \wedge y) + 1$ since x and y cover $x \wedge y$. Also, $\rho(x \vee y) > \rho(x) + 1$ if $x \vee y$ does not cover x. Similarly, $\rho(x \vee y) > \rho(y) + 1$ if $x \vee y$ does not cover y. Therefore, in either case, $\rho(x \vee y) + \rho(x \wedge y) > \rho(x) + \rho(y)$, which is a contradiction.

(2) $\Rightarrow$ (1) Assume that L is not graded, so there exists an interval $[u, v]$ of L of minimal length, which is not graded. Then, there must exist at least two elements x_1, x_2 of $[u, v]$ that cover u, along with the condition that all maximal chains of each interval $[x_i, v]$ have the same length l_i, where $l_1 \neq l_2$. Using (2), there exists saturated chains in

$[x_i, v]$ of the form $x_i < x_1 \vee x_2 < y_1 < y_2 < ..... < y_k = v$, which in turn contradicts that $l_1 \neq l_2$. Hence, L is graded.

Now, suppose that there exists a pair $x, y \in L$ such that

$$\rho(x) + \rho(y) < \rho(x \vee y) + \rho(x \wedge y)$$

and choose such a pair for which $l(x \wedge y, x \vee y)$ is minimal. We put further restriction on the pair x, y so that $\rho(x) + \rho(y)$ is minimal. Now, we can not have both x and y covering $x \wedge y$, because in that case by (2) we'll obtain that $\rho(x) = \rho(y) = \rho(x \wedge y) + 1 = \rho(x \vee y) - 1$ which implies that $\rho(x) + \rho(y) = \rho(x \wedge y) + \rho(x \vee y)$, contradicting our assumption. Therefore, assume that $x \wedge y < x' < x$. Then, by the minimality of $l(x \wedge y, x \vee y)$ and $\rho(x) + \rho(y)$, we obtain that

$$\rho(x') + \rho(y) \geq \rho(x' \wedge y) + \rho(x' \vee y).$$

Now, since $\rho(x' \wedge y) = \rho(x \wedge y)$, so from the last two inequalities, we get

$$\rho(x) + \rho(x' \vee y) < \rho(x') + \rho(x \vee y).$$

We also have that $x' \leq x \wedge (x' \vee y)$ and $x \vee (x' \vee y) = x \vee y$. Hence, by setting $X = x$ and $Y = x' \vee y$, we have found a pair $X, Y \in L$ satisfying $\rho(X) + \rho(Y) < \rho(X \wedge Y) + \rho(X \vee Y)$ and with $l(X \wedge Y, X \vee Y) < l(x \wedge y, x \vee y)$, again a contradiction. □

Remark 4.1.2.

1. A *finite upper semimodular lattice* is a lattice which satisfies any one of the equivalent conditions of the Proposition 4.1.1. Dually, we can obtain a *finite lower semimodular lattice.*

2. A finite lattice is said to be a *finite modular lattice* if it is both upper and lower semimodular. As in Proposition 4.1.1, it can be shown that a finite lattice L is modular if and only if L is graded and its rank function ρ satisfies

$$\rho(x) + \rho(y) = \rho(x \vee y) + \rho(x \wedge y) \text{ for all } x, y \in L.$$

Proposition 4.1.3. *A finite lattice L is modular if and only if for all $x, y, z \in L$ with $x \leq z$, we have*

$$x \vee (y \wedge z) = (x \vee y) \wedge z.$$

Proof. ($\Rightarrow$) Let L be modular and assume that for some $x, y, z \in L$ with $x \leq z$, $x \vee (y \wedge z) \neq (x \vee y) \wedge z$. Observe that, $y \notin [x, z]$, otherwise $x \vee (y \wedge z) = x \vee y = y = y \wedge z = (x \vee y) \wedge z$. Therefore, all these elements y, $x \vee y$, $y \wedge z$, $x \vee (y \wedge z)$ and $(x \vee y) \wedge z$ form a sublattice of L isomorphic to $\widehat{\mathbf{2+1}}$, whose Hasse diagram is as in Figure 4.1.

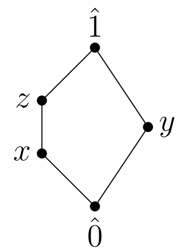


Figure 4.1

As $\widehat{\mathbf{2+1}}$ is not modular, the lattice L is not modular.

($\Leftarrow$) Assume that for all $x, y, z \in L$ with $x \leq z$, $x \vee (y \wedge z) = (x \vee y) \wedge z$. Choose $x, y \in L$ such that x and y both cover $x \wedge y$. This indicates that x and y are incomparable. Hence, any chain of $(x \wedge y, x \vee y)$ containing x is disjoint from any other chain of $(x \wedge y, x \vee y)$ containing y.

Suppose that $x \vee y$ does not cover x. Then, there exists $z \in (x, x \vee y)$ and hence, $x \wedge y < x < z < x \vee y$ and $x \wedge y < y < x \vee y$ are two disjoint chains, i.e.,

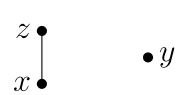


Figure 4.2

Therefore, $y \wedge z = x \wedge y$ and $y \vee z = x \vee y$ and consequently $x \vee (y \wedge z) = x \vee (x \wedge y) = x < z = (y \vee z) \wedge z = (x \vee y) \wedge z$. This contradicts our assumption. Thus, $x \vee y$ covers x

and y and hence, L is modular.

□

Examples 4.1.4. (Modular and Non-Modular lattices)

1. $\mathbf{n}$: For $x, y \in \mathbf{n}$, we have

$$\begin{aligned}\rho(x \vee y) + \rho(x \wedge y) &= \rho(max\{x, y\}) + \rho(min\{x, y\}) \\ &= \rho(x) + \rho(y).\end{aligned}$$

Thus, $\mathbf{n}$ is a modular lattice.

2. B_n : Let $X, Y, Z \in B_n$ with $X \leq Z$, then

$$\begin{aligned}X \vee (Y \wedge Z) = X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) &= (X \cup Y) \cap (Z) \\ &= (X \vee Y) \wedge Z.\end{aligned}$$

Hence, B_n is a modular lattice.

3. $L_n(q)$: For $X, Y \in L_n(q)$, we have

$$\begin{aligned}\rho(X \vee Y) + \rho(X \wedge Y) = dim(X + Y) + dim(X \cap Y) &= dimX + dimY \\ &= \rho(x) + \rho(y).\end{aligned}$$

This shows that $L_n(q)$ is a modular lattice.

4. A seven element non-modular, semimodular lattice is depicted in the figure below:

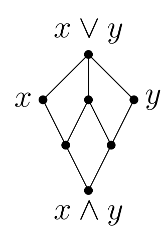


Figure 4.3

Here, $x \vee y$ covers x and y, but x and y do not cover $x \wedge y$.

Proposition 4.1.5. *Let L be a finite semimodular lattice. Then the following conditions are equivalent:*

(1) L is relatively complemented.

(2) L is atomic.

Proof. (1) $\Rightarrow$ (2) Assume that L is relatively complemented. Let $x \in L$, we need to show that x can be expressed as the join of atoms. If $x = \hat{0}$, then there is nothing to prove, so let $x \neq \hat{0}$ and consider the interval $[\hat{0}, x]$. Let $a_1 \leq x$ be an atom and x_1 be its complement in $[\hat{0}, x]$. Then $x = a_1 \vee x_1$ since L is relatively complemented. Replacing x by x_1 and on repeating the entire process we will obtain

$$x = a_1 \vee x_1 = a_1 \vee (a_2 \vee x_2) = (a_1 \vee a_2) \vee x_2 = ... = (a_1 \vee a_2 \vee ..... \vee a_n) \vee x_n = ...$$

Now, since $x > x_1 > x_2 > ....$, so x_n is eventually $\hat{0}$ and therefore, $x = a_1 \vee a_2 \vee ..... \vee a_n$.

(2) $\Rightarrow$ (1) Assume that L is atomic. Consider the interval $[x, y]$ in L. Then, x can be written as $x = a_1 \vee ..... \vee a_r$ and $y = a_1 \vee ..... \vee a_r \vee b_1 \vee ..... \vee b_s$. Here, a_i and b_j denote the set of atoms of L. Let $z \in [x, y]$, so then $z = x(\bigvee_{i \in S} b_i)$ where $S \subseteq [s]$. Take $z' = x(\bigvee_{i \in S'} b_i)$ where $S' = \{r+1, ..., s\} - S$. Clearly, $z \vee z' = y$ and $z \wedge z' = x$. Thus, L is relatively complemented.

□

Definition 4.1.6. A *finite geometric lattice* is one which is both semimodular as well as atomic.

Examples 4.1.7. (Geometric Lattices)

Consider a vector space V over a field k and take some finite set of points, say S in it. Now, intersect S with W, where W is a vector subspace of V. Then, the resultant subsets of S obtained via this construction and ordered by inclusion forms a geometric lattice $L(S)$. One such instance, with $S \subset \mathbb{R}^2$ and its corresponding $L(S)$ is shown in Figure 4.4.

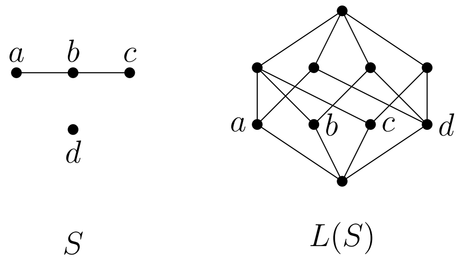


Figure 4.4

Another important example is that of B_n.

4.2 Distributive Lattice

A distributive lattice can be represented as subsets of a finite set, wherein lattice operations correspond to set-theoretic union and intersection.

Definition 4.2.1. *Distributive lattices* are those lattices L that satisfy the following distributive axioms,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z),$$

for all $x, y, z \in L$. These two conditions are equivalent. (By taking the dual of one, we obtain the other.)

Examples 4.2.2.

1. **n** (or every linearly ordered set) is a distributive lattice. We know that $x \wedge y$ is the lesser of x and y whereas $x \vee y$ is the greater of x and y. Using this, we obtain that $x \wedge (y \vee z)$ and $(x \wedge y) \vee (x \wedge z)$, both equals x in case x is smaller than y or z and $y \vee z$ if x is bigger than y and z.

2. B_n is a distributive lattice since union and intersection distribute over each other.

Proposition 4.2.3. *Every distributive lattice L is modular.*

Proof. Assume $x \leq z$. This implies $x \vee z = z$ and then, for any $y \in L$, we have $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z$. □

Remark 4.2.4.

1. Π_3, $L_2(2)$ are both modular but not distributive.

2. $\widehat{\mathbf{2}+\mathbf{1}}$ is not modular and hence, not distributive.

For a poset P, the set $\mathcal{J}(P)$ of all order ideals in P, is a poset w.r.t the order induced by inclusion.

Proposition 4.2.5. *For a finite poset P, $\mathcal{J}(P)$ is a distributive lattice.*

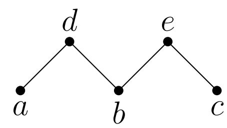
Proof. We define the lattice operations of join and meet to be the set union and intersection on order ideals. Firstly, we'll show that for $I, K \in \mathcal{J}(P)$, $I \cup K$ and $I \cap K$ also lies in $\mathcal{J}(P)$. Let $x \in I \cup K$ i.e. $x \in I$ or $x \in K$. Thus, for any $y \leq x$, $y \in I$ or $y \in K$ depending on x. Hence, $y \in I \cup K$ whereas in case of $I \cap K$, down set of any element in intersection will also lie in the intersection. Therefore, it shows that union and intersection of order ideals again turns out to be an order ideal. Secondly, set union and intersection are distributive over each other. So, it follows that $\mathcal{J}(P)$ is a distributive lattice. □

Examples 4.2.6.

1. If $P = \mathbf{n}$, an n-element chain, then $\mathcal{J}(P) \cong \mathbf{n}+\mathbf{1}$.

2. If $P = n\mathbf{1}$, an n-element antichain, then $\mathcal{J}(P) \cong B_n$.

Now, we move on to investigate the combinatorial properties of $\mathcal{J}(P)$, how to draw its Hasse diagram and study the relationship between P and $\mathcal{J}(P)$ for a finite poset P. For an arbitrary poset $P = \{a, b, c, d, e\}$, the Hasse diagram of corresponding $\mathcal{J}(P)$ is shown in Figure 4.5.



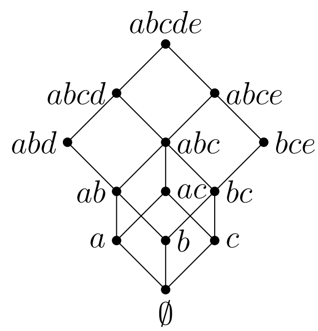


Figure 4.5

We describe here a series of steps for drawing the Hasse diagram of $\mathcal{J}(P)$, given P. Firstly, draw B_n where n is the number of minimal elements of P. Call the set of minimal elements to be I, so that $B_n \cong \mathcal{J}(I)$. Now, pick a minimal element of $P - I$, say x. Adjoin this to $\mathcal{J}(I)$ covering the order ideal $I_x - \{x\}$. The elements covering $I_x - \{x\}$ may not have joins, so draw in any new joins necessary to form boolean algebras. Next, pick a minimal element of $P - I - \{x\}$ and repeat the process until $\mathcal{J}(P)$ is reached.

Proposition 4.2.7. *Let I be an arbitrary order ideal of P. Then, the elements of $\mathcal{J}(P)$ that cover I are just the order ideals $I \cup \{x\}$, where x is a minimal element of $P - I$.*

Proof. We are given that $I \in \mathcal{J}(P)$ i.e. I is an order ideal of P. We need to prove that if x is a minimal element of $P - I$, then $I' = I \cup \{x\}$ is also an order ideal of P that covers I. Let $z \in I'$ and $y \leq z$. First possibility is that $z \in I$ which implies that $y \in I$. Thus, $y \in I'$. Second case is when $z = x$; but $y \leq z$, therefore either $y = z = x$ or $y < z = x$. Hence $y \in I \subseteq I'$. □

Proposition 4.2.8. *Let P be an n-element poset, then in that case $\mathcal{J}(P)$ is graded of rank n. Moreover, the rank $\rho(I)$ of $I \in \mathcal{J}(P)$ is the cardinality $|I|$ of I.*

Proof. Given $|P| = n$. From Proposition 4.2.5, $\mathcal{J}(P)$ is a distributive lattice and hence modular. Therefore, it is graded. By convention, $\emptyset \in \mathcal{J}(P)$. So, $\rho(\emptyset) = 0$. Now, pick a minimal element x from P. Then, by Proposition 4.2.7 x covers $\emptyset$ and thus, $\rho(x) = 1$.

Also, $|I_x| = 1$ in P. So, we can construct any maximal chain this way by adding one element from P and moving up in the Hasse diagram of $\mathcal{J}(P)$. And, since there are n elements available, therefore $\mathcal{J}(P)$ is graded of rank n. Similarly, maximal chain can be formed for any order ideal of P; i.e., start with a minimal element and then, leave the first one and look for others; go on iterating this process and move up until all the elements of the order ideal are exhausted. This shows that $\rho(I)$ of $I \in \mathcal{J}(P)$ is $|I|$. $\square$

Definition 4.2.9. A *finitary* distributive lattice L is a locally finite distributive lattice with $\hat{0}$.

Likewise in case of posets, L also has a unique rank function $\rho : L \to \mathbb{N}$ given by $\rho(x)$ to be the length of any saturated chain from $\hat{0}$ to x. *Rank-generating function* of L is also defined on similar lines as before and is given by the expression

$$F(L, q) = \sum_{i \geq 0} p_i q^i$$

provided p_i is finite.

4.3 Representation theorems

Now, we state one of the most important characterizations for finite distributive lattices which also accommodates the trueness of the converse of Proposition 4.2.5. It is known as *Birkhoff's representation theorem* or *fundamental theorem for finite distributive lattices* (FTFDL). But, before this we need some prerequisites for building up the main result.

Definition 4.3.1. An element x of a lattice L is defined to be *join-irreducible* if whenever $x = y \vee z$, then either $x = y$ or $x = z$. Another equivalent way of saying this is that an element is a join-irreducible if and only if it covers a unique element. Dually, one can define *meet-irreducibles.*

Remark 4.3.2.

1. The very first appearance of join-irreducibles in a lattice is marked by atoms.

2. The set comprising of join-irreducibles of a lattice L, call it $J(L)$ derives its partial order from L.

3. Every element in a finite lattice L is expressible as a join of join-irreducibles i.e. $x = \bigvee\{y : y \in J(L) \text{ and } y \leq x\}$.

Proposition 4.3.3. *Let P be a finite poset. An order ideal I is* join-irreducible *in $\mathcal{J}(P)$ if and only if it is a principal order ideal of P.*

Proof. ($\Rightarrow$) Assume that I is join-irreducible in $\mathcal{J}(P)$ but not a principal order ideal which means that there exists more than one maximal element in I. Since P is given to be finite, we obtain that I is finitely generated. Let $I = \langle x_1, ..., x_n \rangle$ and $I' = \langle x_n \rangle$. Then, we can write $I = (I - \langle x_n \rangle) \cup I'$ which contradicts our assumption that I is join-irreducible. Hence, I is a principal order ideal of P.

($\Leftarrow$) Suppose that I is a principal order ideal i.e. $I = \Lambda_x$ for some $x \in L$. Let $I = I_1 \cup I_2$ for $I_1, I_2 \in \mathcal{J}(P)$ and both are non-empty. Thus, $\langle x \rangle = I_1 \cup I_2$.

$\Rightarrow x \in I_1$ or $x \in I_2$

$\Rightarrow \langle x \rangle \subset I_1$ or $\langle x \rangle \subset I_2$

$\Rightarrow \langle x \rangle = I_1$ or $\langle x \rangle = I_2$ (since, it is principal)

i.e. I is join-irreducible. □

Proposition 4.3.4. *For a finite poset P, the set of join-irreducibles of $\mathcal{J}(P)$ is isomorphic to P. Hence, $\mathcal{J}(P) \cong \mathcal{J}(Q)$ if and only if $P \cong Q$.*

Proof. From Proposition 4.3.3, we obtain that there exists a bijection $\phi : P \to$ (join-irreducibles of $\mathcal{J}(P)$) defined by $\phi(x) = \Lambda_x$. Observe that ϕ is also order-preserving because $x \leq y$ if and only if $\Lambda_x \subseteq \Lambda_y$. Hence, we conclude that ϕ is an isomorphism.

Let $\mathcal{J}(P) \cong \mathcal{J}(Q)$. Then, we get that join-irreducibles of $\mathcal{J}(P)$ and $\mathcal{J}(Q)$ are isomorphic as induced subposets of $\mathcal{J}(P)$ and $\mathcal{J}(Q)$ respectively. Now, by using first part of the proposition, we conclude that $P \cong Q$. On the other hand, if we assume that $P \cong Q$, then we obtain that join-irreducibles of $\mathcal{J}(P)$ and $\mathcal{J}(Q)$ are isomorphic. This in turn implies that $\mathcal{J}(P) \cong \mathcal{J}(Q)$ since every order ideal can be generated by taking joins of some specific set of join-irreducibes. $\square$

Now, we'll state analogous version of arithmetic properties of primes and prime factorizations in lattice theory that are satisfied by distributive lattices.

Lemma 4.3.5. *For a join-irreducible j in a distributive lattice; $j \leq x \vee y$ implies $j \leq x$ or $j \leq y$.*

Proof. Since $j \leq x \vee y$, we have $j = j \wedge (x \vee y)$. Using distributivity, $j = (j \wedge x) \vee (j \wedge y)$. And, now because j is join-irreducible, therefore $j = j \wedge x$ or $j \wedge y$. Hence, the assertion follows. $\square$

Lemma 4.3.6. *Every element x in a finite distributive lattice is the join of a unique antichain of join-irreducibles.*

Proof. Assume that there exists two antichains of join-irreducibles $\{j_i\}$ and $\{h_i\}$ both representing x i.e.

$$j_1 \vee j_2 \vee .... \vee j_k = x = h_1 \vee h_2 \vee .... \vee h_n,$$

where $n \geq k$. By distributivity, we write

$$\begin{aligned} j_i = j_i \wedge x = j_i \wedge (h_1 \vee h_2 \vee .... \vee h_n) \\ = (j_i \wedge h_1) \vee (j_i \wedge h_2) \vee ..... \vee (j_i \wedge h_n). \end{aligned}$$

Now, by Lemma 4.3.5, for every index i, there exists an index $\pi(i)$ for which $j_i = j_i \wedge h_{\pi(i)}$. On reversing the argument, we obtain that for each i, there exists an index $\sigma(i)$ such that $h_i = h_i \wedge j_{\sigma(i)}$. After combining the above, we conclude that $j_i \leq h_{\pi(i)} \leq j_{\sigma(\pi(i))}$ for every index i. But then, since $\{j_i\}$ forms an antichain, therefore $j_i = j_{\sigma(\pi(i))}$ and hence $i = \sigma(\pi(i))$. So, it implies that $n = k$ and π is a permutation. $\square$

Theorem 4.3.7 (Birkhoff)**.** *Let L be a finite distributive lattice. Then there exists a unique finite poset P (upto isomorphism) for which $L \cong \mathcal{J}(P)$.*

Proof. In view of Proposition 4.3.4, we just need to consider P as the subposet of join-irreducibles of L and show that $L \cong \mathcal{J}(P)$. If $x \in L$, let $I_x = \{j \in P : j \leq x\}$. We define $\phi : L \to \mathcal{J}(P)$ to be given by $\phi(x) = I_x$. First, we will show that ϕ is a lattice homomorphism i.e. it preserves both meet and join. Now, since

$$\begin{aligned}\phi(x \wedge y) = I_{(x\wedge y)} &= \{j : j \in P,\ j \leq x \text{ and } j \leq y\}\\ &= I_x \cap I_y\\ &= \phi(x) \cap \phi(y)\end{aligned}$$

therefore, it respects the meet operation. Next, we see that if $j \leq x$ or $j \leq y$, then $j \leq x \vee y$. Hence, $I_x \cup I_y \subseteq I_{(x\vee y)}$. On the other side, if we suppose $j \in I_{(x\vee y)}$ meaning that $j \in P$ and $j \leq x \vee y$, then $j = j \wedge (x \vee y) = (j \wedge x) \vee (j \wedge y)$. And, since j is join-irreducible , so $j \leq x$ or $j \leq y$. Thus, $j \in I_x \cup I_y$ and then, we can conclude that $I_{(x\vee y)} = I_x \cup I_y$ i.e. joins are preserved.

Now, from Proposition 2.1.15 and Lemma 4.3.6, we know that the set of maximal elements of I_x equals an antichain of join-irreducibles and x is determined by a unique antichain of join-irreducibles. Hence, it proves the injectivity of ϕ.

To show that ϕ is surjective, consider an order ideal I in $\mathcal{J}(P)$ and let x be the join of all the elements in I. We want to show that $I = I_x = \phi(x)$. Certainly, $I \subseteq I_x$. Suppose $j \in I_x$ and then use distributivity to obtain that

$$j = j \wedge x = j \wedge (\bigvee_{y\in I} y) = \bigvee_{y\in I}(j \wedge y).$$

Now, because j is a join-irreducible, therefore $j = j \wedge y$ or $j \leq y$ for some $y \in I$. Thus, $j \in I$ since I is an order ideal. Consequently, $I = I_x$.

Finally, we see that ϕ being a lattice homomorphism implies that it is an order-preserving map. But, since it is also bijective, so we conclude that both ϕ and ϕ^{-1} are order preserving. And hence, we obtain the desired isomorphism. □

On the similar lines, Representation theorem for finitary distributive lattices can be obtained. We state the result without proof.

Proposition 4.3.8. *(FTFDL for finitary distributive lattices)*
Let P be a poset for which every principal order ideal is finite. Then the poset $\mathcal{J}_f(P)$ of finite order ideals of P, (where ordering is given by inclusion), is a finitary distributive

lattice. Conversely, if L *is a finitary distributive lattice and* P *is the subposet of its join-irreducibles, then every principal order ideal of* P *is finite and* $L \cong \mathcal{J}_f(P)$.

Chapter 5

Boolean Algebras

5.1 Boolean Lattices

Definition 5.1.1. A lattice L is said to be a *Boolean lattice* if it is bounded, complemented and distributive.

These (uniquely) complemented distributive lattices have particularly nice properties and so they are considered very useful in various applications of lattice theory. In this chapter, we will write 0 for $\hat{0}$ and 1 for $\hat{1}$ just for notational convenience.

Lemma 5.1.2. *A Boolean lattice L is uniquely complemented for every $x \in L$.*

Proof. For $x \in L$, let there exist two complements y and z in L. Since y and z are complements of x, so we have the following:

$$x \wedge y = 0 \text{ and } x \vee y = 1,$$

$$x \wedge z = 0 \text{ and } x \vee z = 1.$$

$$\text{Now, } y = y \vee 0 = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z) = 1 \wedge (y \vee z) = (y \vee z) \text{ and}$$

$$z = z \vee 0 = z \vee (x \wedge y) = (z \vee x) \wedge (z \vee y) = 1 \wedge (z \vee y) = (z \vee y).$$

So, then since $(y \vee z) = (z \vee y)$, therefore $y = z$. □

The way a lattice was defined algebraically as a set with two operations that satisfy certain conditions, without any reference to the underlying partial order, in an analogous fashion, Boolean algebra gives us an equivalent algebraic interpretation of Boolean lattices as a set with certain operations.

Definition 5.1.3. $(B, \wedge, \vee, ', 0, 1)$ is a *Boolean algebra*, where B is a non-empty set together with two binary operations $\wedge$ and $\vee$ and a unary operation $'$. The operation $\vee$ is called *join*, $\wedge$ is called *meet* and $'$ is called *complementation*. These operations satisfy the following laws:

1. The two binary operations $\wedge$ and $\vee$ are commutative and associative.
2. Both the operations $\wedge$ and $\vee$ satisfy the distributive laws.
3. (Identity law) There exist an element $0 \in B$ called the *zero element* and an element $1 \in B$ called the *unit element* such that $x \vee 0 = x$ and $x \wedge 1 = x$ for all $x \in B$.
4. (Complementation law) $x \vee x' = 1$ and $x \wedge x' = 0$ for all $x \in B$.

Duality principle: If we interchange $\wedge$ with $\vee$ and 0 with 1 everywhere in an expression valid in a Boolean algebra, then the resulting expression is also valid there.

Properties in a Boolean algebra: Let B be a Boolean algebra, then following are some consequences of the defining laws:

1. $x \vee x = x, \quad x \wedge x = x$ for all $x \in B$. We see that

$$\begin{aligned} x \vee x &= (x \vee x) \wedge 1 = (x \vee x) \wedge (x \vee x') \\ &= x \vee (x \wedge x') \\ &= x \vee 0 \\ &= x. \end{aligned}$$

2. $x \vee 1 = 1, \quad x \wedge 0 = 0$ for all $x \in B$. Observe that

$$\begin{aligned} x \vee 1 &= x \vee (x \vee x') = (x \vee x) \vee x' \\ &= x \vee x' \\ &= 1. \end{aligned}$$

3. (Absorption laws) $(x \wedge y) \vee x = x$ and $(x \vee y) \wedge x = x$ for all $x, y \in B$. We have,

$$\begin{aligned}(x \wedge y) \vee x &= (x \wedge y) \vee (x \wedge 1) = x \wedge (y \vee 1) \\ &= x \wedge 1 \\ &= x.\end{aligned}$$

   Dually, we obtain other expressions.

4. $0' = 1, 1' = 0$ and $x'' = x$ for all $x \in B$. We begin by showing that if $x \vee y = 1$ and $x \wedge y = 0$, then $y = x'$.

$$\begin{aligned}y = y \vee 0 &= y \vee (x \wedge x') \\ &= (y \vee x) \wedge (y \vee x') \\ &= 1 \wedge (y \vee x') \\ &= (x \vee x') \wedge (y \vee x') \\ &= (x \wedge y) \vee x' = 0 \vee x' \\ &= x'.\end{aligned}$$

   This gives us the uniqueness of complement and clearly from above, we conclude that $0' = 1$ and $1' = 0$. We also obtain that $x = (x')'$ since $x \vee x' = 1$ and $x \wedge x' = 0$.

5. (De Morgan's laws) $(x \vee y)' = x' \wedge y'$ and $(x \wedge y)' = x' \vee y'$ for all $x, y \in B$. For $(x \vee y)' = x' \wedge y'$, we need to show that $(x \vee y) \vee (x' \wedge y') = 1$ or $(x \vee y) \wedge (x' \wedge y') = 0$. We see that

$$\begin{aligned}(x \vee y) \vee (x' \wedge y') &= \big[(x \vee y) \vee x'\big] \wedge \big[(x \vee y) \vee y'\big] \\ &= \big[(x \vee x') \vee y\big] \wedge \big[x \vee (y \vee y')\big] \\ &= \big[(1) \vee y\big] \wedge \big[x \vee (1)\big] \\ &= 1 \wedge 1 = 1.\end{aligned}$$

   The other law $(x \wedge y)' = x' \vee y'$ is established on similar lines.

We define $x \leq y \Leftrightarrow x \vee y = y$. Notice that $x \vee y = y \Leftrightarrow x \wedge y = x$ for all $x, y \in B$. Suppose that $x \wedge y = x$, then $(x \wedge y) \vee y = x \vee y$. So, we obtain $y = x \vee y$ by absorption law. Similarly, we obtain the other way implication.

Thus, a Boolean algebra $(B, \wedge, \vee, ', 0, 1)$ is a boolean lattice along with the unary operation of complementation, and where 0 and 1 corresponds to the least and the greatest element respectively. The relation defined by $x \leq y$ if and only if $x \vee y = y$ (or equivalently $x \wedge y = x$) is a partial order on B. The meet and the join of two elements corresponds to infimum and supremum respectively. Conversely, any Boolean lattice forms a Boolean algebra. (Assume $0 \neq 1$ in order to exclude the case of trivial Boolean algebra.)

Examples 5.1.4.

1. The power set $\mathcal{P}(S)$ of a set S is a Boolean algebra. It is called the *power set algebra*. The operations in this case correspond to a Boolean algebra like this: $(\mathcal{P}(S), \cap, \cup, ^c, \emptyset, S) \equiv (B, \wedge, \vee, ', 0, 1)$. Furthermore, we will also prove that every finite Boolean algebra is isomorphic to the power set $\mathcal{P}(S)$ for some finite set S.

2. Two element set $\mathbb{B} = \{0, 1\}$ is another simplest non-trivial Boolean algebra. It is defined by the following:

   - $0' = 1$ and $1' = 0$.
   - $x \vee y = \begin{cases} 0 & \text{if } x = y = 0, \\ 1 & \text{otherwise.} \end{cases}$
   - $x \wedge y = \begin{cases} 1 & \text{if } x = y = 1, \\ 0 & \text{otherwise.} \end{cases}$

Now, we move on to study an interesting connection between Boolean algebras and rings.

Definition 5.1.5. A commutative ring R with 1 is said to be a *Boolean ring* if every element in it is idempotent, i.e, $x^2 = x$ for all $x \in R$. For example: $\mathbb{Z}/2\mathbb{Z}$.

Theorem 5.1.6. *Suppose* $(B, \wedge, \vee, ', 0, 1)$ *be a Boolean algebra. We define a multiplication and an addition on* B *by setting* $x.y = x \wedge y$ *and* $x + y = (x \wedge y') \vee (x' \wedge y)$ *for all* $x, y \in B$*. Then* $(B, +, \cdot, 0, 1)$ *is a Boolean ring.*

Proof. First, we check that $(B, +)$ forms an abelian group. The commutative law of addition follows since $x+y = (x \wedge y') \vee (x' \wedge y) = (y \wedge x') \vee (y' \wedge x) = y+x$. The additive identity is 0 because $x+0 = (x \wedge 0') \vee (x' \wedge 0) = (x) \vee (0) = x$. Also, $x+x = (x \wedge x') \vee (x' \wedge x) = 0$, so every element is its own additive inverse. Furthermore, for given $x, y, z \in B$, we see that

$(x + y) + z$

$$= \big[(x \wedge y') \vee (x' \wedge y)\big] + z$$

$$= \Big(\big[(x \wedge y') \vee (x' \wedge y)\big] \wedge z'\Big) \vee \Big(\big[(x \wedge y') \vee (x' \wedge y)\big]' \wedge z\Big)$$

$$= \Big((x \wedge y' \wedge z') \vee (x' \wedge y \wedge z')\Big) \vee \Big(\big[(x' \vee y) \wedge (x \vee y')\big] \wedge z\Big)$$

$$= \Big((x \wedge y' \wedge z') \vee (x' \wedge y \wedge z')\Big) \vee \Big((x' \vee y) \wedge \big[(x \vee y') \wedge z\big]\Big)$$

$$= \Big((x \wedge y' \wedge z') \vee (x' \wedge y \wedge z')\Big) \vee \Big((x' \vee y) \wedge \big[(x \wedge z) \vee (y' \wedge z)\big]\Big)$$

$$= (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y \wedge z)$$

$= x + (y + z)$ since the above expression is symmetric in x, y, z. Thus, addition is associative.

Next, multiplication is commutative as well as associative since $x.y = x \wedge y = y \wedge x = y.x$ and $(x.y).z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x.(y.z)$ holds for all $x, y, z \in B$. The element 1 is the identity of B as $x.1 = 1.x = x$. For each $x \in B$, we see that $x^2 = x.x = x \wedge x = x$, therefore every element in B is an idempotent. Finally, for distributivity, let $x, y, z \in B$, then

$$\begin{aligned} x.y + x.z &= \big[(x.y) \wedge (x.z)'\big] \vee \big[(x.y)' \wedge (x.z)\big] \\ &= \big[(x \wedge y) \wedge (x \wedge z)'\big] \vee \big[(x \wedge y)' \wedge (x \wedge z)\big] \\ &= \big[x \wedge y \wedge (x' \vee z')\big] \vee \big[(x' \vee y') \wedge x \wedge z\big] \\ &= \big[x \wedge y \wedge z'\big] \vee \big[(x \wedge y' \wedge z\big] \\ &= x \wedge \big[(y \wedge z') \vee (y' \wedge z)\big] \\ &= x.(y + z). \end{aligned}$$

Therefore, $(B, +, \cdot, 0, 1)$ is a Boolean ring.

□

Theorem 5.1.7. *Let $(B, +, \cdot, 0, 1)$ be a Boolean ring. We define operations in B by $x \wedge y = x.y$, $x \vee y = x + y + x.y$ and $x' = 1 + x$ for all $x, y \in B$. Then, $(B, \wedge, \vee, ', 0, 1)$ is a Boolean algebra.*

Proof. Firstly, observe that for elements x, y in a Boolean ring B, we have

$$x + y = (x + y)^2 = x.x + x.y + y.x + y.y = x + x.y + y.x + y$$

which implies that $x.y + y.x = 0$ i.e. $x.y = -y.x$. Now, put $x = y$ and obtain that $x^2 + x^2 = 0$. Thus, $x + x = 0$. Hence, notice that a Boolean ring has characteristic 2. So, then using that $x = -x$ for each $x \in B$, we get $x.y = -x.y = y.x$ implying that a Boolean ring is commutative.

Clearly, then $\wedge$ operation is commutative and associative since $x \wedge y = x.y = y.x = y \wedge x$ and $(x \wedge y) \wedge z = (x.y).z = x.(y.z) = x \wedge (y \wedge z)$ for all $x, y, z \in B$. It also satisfy idempotent laws because $x \wedge x = x.x = x$ for all $x \in B$. Also, $\vee$ operation is commutative as $x \vee y = x + y + x.y = y + x + y.x = y \vee x$ and satisfy idempotent laws since $x \vee x = x + x + x.x = x.x = x$ for all $x \in B$. For associativity of $\vee$, observe that

$$\begin{aligned} (x \vee y) \vee z &= (x \vee y) + z + (x \vee y).z = (x + y + x.y) + z + (x + y + x.y).z \\ &= x + y + z + x.y + x.z + y.z + x.y.z \\ &= x \vee (y \vee z), \end{aligned}$$

because of being symmetric in x, y, z. Next, we verify absorption laws i.e.

$$x \wedge (x \vee y) = x.(x + y + x.y) = x + x.y + x.y = x + 0 = x \text{ and}$$

$$x \vee (x \wedge y) = x \vee (x.y) = x + x.y + x.(x.y) = x + x.y + x.y = x + 0 = x.$$

From above, we conclude that $(B, \vee, \wedge)$ forms a lattice where partial order is given by $x \leq y \Leftrightarrow x = x \wedge y = (x.y)$. This lattice also satisfies distributive laws as

$$\begin{aligned} x \wedge (y \vee z) = x.(y + z + y.z) &= x.y + x.z + x.(y.z) \\ &= x.y + x.z + x.x.(y.z) \\ &= x.y + x.z + (x.y).(x.z) \\ &= x.y \vee x.z \\ &= (x \wedge y) \vee (x \wedge z). \end{aligned}$$

Finally, for the complement of x, observe that $x \wedge x' = x.x' = x.(1 + x) = 0$ and $x \vee x' = x + x' + x.x' = x + x' = x + 1 + x = 1$. Thus, the lattice is complemented and bounded by 0 and 1. Hence, $(B, \wedge, \vee, ', 0, 1)$ forms a Boolean algebra. □

From the last two theorems, it is clear that Boolean algebras and Boolean rings are equivalent concepts.

5.2 Representation theorem for a finite Boolean Algebra

Definition 5.2.1. Suppose that $(B_1, \wedge, \vee, ', 0, 1)$ and $(B_2, \wedge, \vee, ', 0, 1)$ are Boolean algebras. A function $\phi : B_1 \to B_2$ is said to be a *Boolean algebra homomorphism* if

$$\phi(x \vee y) = \phi(x) \vee \phi(y),$$

$$\phi(x \wedge y) = \phi(x) \wedge \phi(y),$$

$$\phi(x') = \phi(x)',$$

for all $x, y \in B_1$. And, if ϕ is bijective, then ϕ is called a *Boolean algebra isomorphism.*

Theorem 5.2.2 (Stone)**.** *Let B be a finite Boolean algebra and let A be the set of its atoms. Then, the map $\phi : \mathcal{P}(A) \to B$ given by*

$$\phi(S) = \begin{cases} 0 & \text{if } S = \emptyset, \\ \bigvee_{a \in S} a & \text{if } S \neq \emptyset, \end{cases}$$

is a Boolean algebra isomorphism of $\mathcal{P}(A)$ onto B. In particular, if $|A| = n$, then $|B| = 2^n$.

Proof. Notice that $\phi(\{a\}) = a$ for all $a \in A$ and ϕ maps union of atoms $\{a\}$ in $\mathcal{P}(A)$ to the join of atoms a in B. By Lemma 4.3.6, we see that ϕ is onto and uniqueness part shows that ϕ is one-one. So, ϕ is a one-to-one correspondence between $\mathcal{P}(A)$ and B. Consequently, we have $|B| = |\mathcal{P}(A)| = 2^n$.

Now, we check that ϕ is a Boolean algebra isomorphism. First, we prove that ϕ preserves joins. Let $S = \{s_1, s_2, ..., s_m\}$ and $T = \{t_1, t_2, ..., t_n\}$ be subsets in $\mathcal{P}(A)$. Then, $\phi(S) = s_1 \vee s_2 \vee .... \vee s_m$ and $\phi(T) = t_1 \vee t_2 \vee .... \vee t_n$. So, $\phi(S) \vee \phi(T) = s_1 \vee s_2 \vee .... \vee s_m \vee t_1 \vee t_2 \vee .... \vee t_n$. If $s_i = t_j$ for some i and j, then $s_i \vee t_j = s_i$ in which case drop t_j in the expression $\phi(S) \vee \phi(T)$. After removing such duplicate copies, we obtain that $\phi(S \cup T) = \phi(S) \vee \phi(T)$.

Next, we show that ϕ preserves meets i.e.

$$\begin{aligned}
\phi(S \cap T) &= \phi(S) \wedge \phi(T) \\
&= (s_1 \vee s_2 \vee .... \vee s_m) \wedge (t_1 \vee t_2 \vee .... \vee t_n) \\
&= \left(\bigvee_{i=1}^{m} s_i \right) \wedge \left(\bigvee_{j=1}^{n} t_j \right) \\
&= \bigvee_{i=1}^{m} \left(s_i \wedge \left(\bigvee_{j=1}^{n} t_j \right) \right) \\
&= \bigvee_{i=1}^{m} \left(\bigvee_{j=1}^{n} (s_i \wedge t_j) \right) \text{ by distributive property.}
\end{aligned}$$

Now,

$$s_i \wedge t_j = \begin{cases} 0, & \text{if } s_i \neq t_j \\ s_i = t_j, & \text{if } s_i = t_j. \end{cases}$$

Thus, $(s_1 \vee s_2 \vee .... \vee s_m) \wedge (t_1 \vee t_2 \vee .... \vee t_n)$ is the join of all the atoms in $\{s_1, s_2, ..., s_m\} \cap \{t_1, t_2, ..., t_n\}$. Therefore, ϕ preserves meets.

Finally, we need to show that $\phi(S') = \phi(S)'$ which is equivalent to showing that $\phi(S) \vee$

$\phi(S') = 1$ and $\phi(S) \wedge \phi(S') = 0$. Since ϕ preserves join and meet, so we have $\phi(S) \vee \phi(S') = \phi(S \vee S') = \phi(A) = 1$ and $\phi(S) \wedge \phi(S') = \phi(S \wedge S') = \phi(\emptyset) = 0$.

Therefore, ϕ is a Boolean algebra isomorphism. $\square$

Remark 5.2.3. The correspondence stated in Theorem 5.2.2 does not get carried over to infinite Boolean algebras.

Chapter 6

Möbius Functions

6.1 Incidence Algebra

We introduce here a notion of Incidence Algebra with the aim of associating an algebraic object to a partially ordered set which will then assist us in the further investigation of its structure and subobjects.

Let P be a locally finite poset, $Int(P)$ denote the set of (closed) intervals of P, and let K be a field. For a function $f : Int(P) \to K$, the value $f([x,y])$ is simply represented by $f(x,y)$.

Definition 6.1.1. The set $I(P,K) = \{f : Int(P) \to K\}$ of all functions has the usual structure of a vector space over K, i.e., with pointwise addition and scalar multiplication as given below:

$$(f+g)(x,y) = f(x,y) + g(x,y),$$

$$(kf)(x,y) = k.f(x,y),$$

where $f, g \in I(P,K)$ and $k \in K$. On $I(P,K)$, a pointwise multiplication can be defined, but a more useful product structure on $I(P,K)$ is given by a product called the *convolution product*, which is defined as

$$f * g(x,y) = \begin{cases} \sum\limits_{x \le z \le y} f(x,z)g(z,y) & \text{if } x \le y, \\ 0 & \text{if } x \nleq y. \end{cases}$$

The vector space $I(P,K)$ over K together with the convolution product is called the *incidence algebra* of the poset P with values in the field K. It is interesting to note that the multiplicative identity of the incidence algebra $I(P,K)$ is given by Kronecker delta function (denoted δ or 1) defined below:

$$\delta(x,y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

In fact, for any $f \in I(P,K)$, we have that

$$\begin{aligned} (f * \delta)(x,y) &= \sum_{x \le z \le y} f(x,z)\delta(z,y), \quad \text{for } \; x \le y \\ &= f(x,y) \quad (\because \delta(z,y) = 0 \text{ unless } z = y). \end{aligned}$$

Similarly, $(\delta * f)(x,y) = f(x,y)$.

We easily show that the convolution product is associative.

Proposition 6.1.2. *The incidence algebra $I(P,K)$ is an associative* K-algebra*.*

Proof. Let $f, g, h \in I(P,K)$ and $x \le y$ in P. Then, we have

$$\begin{aligned} ((f * g) * h)(x,y) &= \sum_{x \le z \le y} (f * g)(x,z)h(z,y) \\ &= \sum_{x \le z \le y} \left[\sum_{x \le w \le z} f(x,w)g(w,z) \right] h(z,y) \\ &= \sum_{x \le w \le z \le y} f(x,w)g(w,z)h(z,y) \\ &= \sum_{x \le w \le y} \left[\sum_{w \le z \le y} f(x,w)g(w,z)h(z,y) \right] \\ &= \sum_{x \le w \le y} f(x,w) \left[\sum_{w \le z \le y} g(w,z)h(z,y) \right] \\ &= \sum_{x \le w \le y} f(x,w)(g * h)(w,y) \\ &= (f * (g * h))(x,y). \end{aligned}$$

□

For a finite poset P, the *incidence algebra I(P,K)* can be identified with a certain subalgebra of matrices over K. Suppose P has n elements and elements of P are labelled by $x_1, x_2, ..., x_n$, where $x_i < x_j \Rightarrow i < j$. Then, for each $f \in I(P, K)$, we can associate an $n \times n$ matrix $M_f = (m_{ij})$ over K, where

$$m_{ij} = \begin{cases} f(x_i, x_j) & \text{if } x_i \leq x_j, \\ 0 & \text{if } x_i \nleq x_j. \end{cases}$$

Proposition 6.1.3. *The map $f \mapsto M_f$ from $I(P, K)$ into the algebra $M_n(K)$ of $n \times n$ matrices over K is an injective algebra homomorphism. Thus, the incidence algebra $I(P, K)$ can be identified with a subalgebra of an upper triangular $n \times n$ matrices over K.*

Proof. Since $P = \{x_1, x_2, ..., x_n\}$ has been labelled so that $x_i < x_j \Rightarrow i < j$, it is clear that for each $f \in I(P, K)$, the associated $n \times n$ matrix $M_f = (m_{ij})$ is an upper triangular matrix. Further, if $M_f = M_g$, then $f(x_i, x_j) = g(x_i, x_j)$ for all $i \leq j$. Hence, $f = g$.

Also, as addition and scalar multiplication in $I(P, K)$ are given by pointwise operations, we clearly have

$$M_{f+g} = M_f + M_g \text{ and } M_{kf} = kM_f$$

for $f, g \in I(P, K)$ and $k \in K$. Further, we claim that $M_{(f*g)} = M_f M_g$. In fact,

$$(i, j)^{th} \text{ entry of } M_{(f*g)} = \begin{cases} (f * g)(x_i, x_j) & \text{if } x_i \leq x_j, \\ 0 & \text{if } x_i \nleq x_j. \end{cases}$$

On the other hand, the $(i, j)^{th}$ entry of the product $M_f M_g$ of $n \times n$ matrices M_f and M_g can be easily calculated. If $x_i \nleq x_j$, then $j < i$. Since, both M_f and M_g are upper triangular matrices, the $(i, j)^{th}$ entry of $M_f M_g = 0$. But, if $x_i \leq x_j$, then $i \leq j$. Again, since both M_f and M_g are upper triangular matrices, we see that the $(i, j)^{th}$ entry of $M_f M_g = \sum_{x_i \leq x_k \leq x_j} f(x_i, x_k) g(x_k, x_j) = (f * g)(x_i, x_j)$. Thus, $M_{f*g} = M_f M_g$. □

Examples 6.1.4.

1. If $P = \mathbf{1}$, then $I(P, K)$ is isomorphic to the field K as K-algebra.

2. If $P = \mathbf{2}$, then $I(P, K)$ is isomorphic to the K-algebra of 2×2 upper triangular matrices $\left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in K \right\}$ over K.

3. Consider a poset $P = \{x_1, x_2, x_3, x_4\}$, whose Hasse diagram is described as in Figure 6.1.

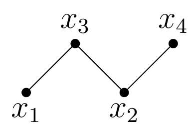


Figure 6.1

Then, the incidence algebra $I(P, K)$ is isomorphic to the algebra of all $n \times n$ matrices of the form,

$$\begin{bmatrix} * & 0 & * & 0 \\ 0 & * & * & * \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{bmatrix}$$

where $*$ denotes any arbitrary element of K.

For $n > 1$, the algebra $M_n(K)$ of matrices is non-commutative. Therefore, the incidence algebra $I(P, K)$ is very rarely commutative.

Proposition 6.1.5. *Let P be a finite poset. Then, the incidence algebra $I(P, K)$ is commutative if and only if P is an antichain.*

Proof. If $P = \{x_1, x_2, ..., x_n\}$ is an antichain, then $x_i \nleq x_j$ for $i \neq j$. Hence, for each $f \in I(P, K)$, the associated $n \times n$ matrix M_f (as in Proposition 6.1.3) is diagonal. Hence, $I(P, K)$ is isomorphic to the subalgebra of diagonal matrices, which is clearly commutative.

Conversely, if $I(P, K)$ is commutative, then we need to show that $x_i \nleq x_j$ for all $i \neq j$. Suppose, on contrary, we have that $x_i < x_j$ for some $i < j$. Consider $f, g \in I(P, K)$ such that $M_f = E_{ij}$ and $M_g = E_{jj}$. Now, $M_f M_g = E_{ij} E_{jj} = E_{ij}$ but $M_g M_f = E_{jj} E_{ij} = 0$.

Clearly, $M_{f*g} = M_f M_g \neq M_g M_f = M_{g*f}$. This implies $f * g \neq g * f$ which is a contradiction to commutativity of $I(P, K)$.

□

The next proposition characterizes when does an inverse exists for some $f \in I(P, K)$.

Proposition 6.1.6. *Let $f \in I(P, K)$. Then the following conditions are equivalent:*

(1) f has a left inverse,

(2) f has a right inverse,

(3) f has a two-sided inverse,

(4) $f(x, x) \neq 0$ for all $x \in P$.

Moreover, if f^{-1} exists, then $f^{-1}(x, y)$ depends only on the poset $[x, y]$.

Proof. Assume that g is the right inverse of f i.e. $f * g = \delta$. Now, the statement $f * g = \delta$ is equivalent to

$$\sum_{x \leq z \leq y} f(x, z) g(z, y) = \delta(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

So, we have $f(x, x) g(x, x) = 1$ if $x = y$ in P

and

$$f(x, x) g(x, y) + \sum_{x < z \leq y} f(x, z) g(z, y) = 0 \text{ if } x < y \text{ in } P$$

i.e.

$$g(x, y) = -f(x, x)^{-1} \sum_{x < z \leq y} f(x, z) g(z, y)$$

From above, it follows that g is the right inverse of f if and only if $f(x, x) \neq 0$ $\forall x \in P$. And, clearly then $f^{-1}(x, y)$ depends only on the poset $[x, y]$. Apply the similar reasoning to $h * f = \delta$ to obtain that f has a left inverse h if and only if $f(x, x) \neq 0$ $\forall x \in P$. Thus, f has the right inverse if and only if $f(x, x) \neq 0$ $\forall x \in P$ if and only if f has the left inverse. But from $f * g = \delta$ and $h * f = \delta$, we derive that $g = h$ and hence, the proof follows.

For a finite poset P, identifying $f \in I(P, K)$ with the matrix M_f (as in Proposition 6.1.3), one clearly sees that all the given conditions are equivalent because an upper triangular matrix M_f is invertible if and only if all the diagonal entries are non-zero. □

Now, we'll discuss some useful functions in $I(P,K)$ and carry out certain computations in $I(P,K)$ that will provide us some structural information about the poset.

Definition 6.1.7. The *zeta function* ζ of a poset P is defined by

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y, \\ 0 & \text{if } x \nleq y, \end{cases}$$

where $x, y \in P$.

Usefulness of zeta function ζ is reflected in the following proposition.

Proposition 6.1.8. *Let P be a poset and ζ be the zeta function of P.*

1. *For $k \in \mathbb{P}$, $\zeta^k(x,y)$ gives the number of multichains of length k from x to y in the poset P.*

2. *Similarly, $(\zeta - 1)^k(x,y)$ where $k \in \mathbb{P}$, gives the number of chains of length k from x to y in the poset P.*

Proof. We have $\zeta^2(x,y) = \sum_{x \leq z \leq y} \zeta(x,z)\zeta(z,y) = \sum_{x \leq z \leq y} 1 = card[x,y]$.

More generally, if $k \in \mathbb{P}$, then

$$\zeta^k(x,y) = \sum_{x = x_0 \leq x_1 \leq .... \leq x_k = y} 1,$$

where the summation runs over all the multichains $x = x_0 \leq .... \leq x_k = y$ of length k from x to y. Hence, $\zeta^k(x,y)$ gives the number of multichains of length k from x to y in the poset P.

Similarly,

$$(\zeta - 1)(x,y) = \begin{cases} 1 & \text{if } x < y, \\ 0 & \text{if } x = y. \end{cases}$$

Thus, for $k \in \mathbb{P}$, $(\zeta - 1)^k(x,y)$ is the number of chains $x = x_0 < x_1 < ..... < x_k = y$ of length k from x to y in P. $\square$

Total number of chains from x to y ($x \leq y$) in a poset can also be described with the help of zeta function.

Proposition 6.1.9. $(2-\zeta)^{-1}(x,y)$ *is equal to the total number of chains from* x *to* y.

Proof. Notice that

$$(2-\zeta)(x,y) = \begin{cases} 1 & \text{if } x = y, \\ \text{-1} & \text{if } x < y. \end{cases}$$

As $(2-\zeta)(x,x) \neq 0$, by Proposition 6.1.5, the function $(2-\zeta)$ is invertible in $I(P,K)$. Let ℓ be the length of the longest chain in the interval $[x,y]$. Then $(\zeta-1)^{\ell+1}(u,v) = 0$ for all $x \leq u \leq v \leq y$. Thus, for $x \leq u \leq v \leq y$, we have

$$\begin{aligned} &(2-\zeta)[1+(\zeta-1)+(\zeta-1)^2+.....+(\zeta-1)^\ell](u,v) \\ &\quad = (1-(\zeta-1)[1+(\zeta-1)+(\zeta-1)^2+.....+(\zeta-1)^\ell](u,v) \\ &\quad = [1-(\zeta-1)^{\ell+1}](u,v) \\ &\quad = \delta(u,v); \text{ where } \delta \text{ is Kronecker delta.} \end{aligned}$$

Hence, $(2-\zeta)^{-1} = 1+(\zeta-1)+(\zeta-1)^2+.....+(\zeta-1)^\ell$ when the poset is restricted to the interval $[x,y]$. Since all the chains from x to y are contained in the interval $[x,y]$, we conclude that $[1+(\zeta-1)+(\zeta-1)^2+.....+(\zeta-1)^\ell](x,y)$ is the total number of chains from x to y. □

Definition 6.1.10. The *eta function* η of a poset P is defined as

$$\eta(x,y) = \begin{cases} 1 & \text{if } y \text{ covers } x, \\ 0 & \text{otherwise,} \end{cases}$$

where $x, y \in P$.

Proposition 6.1.11. $(1-\eta)^{-1}(x,y)$ *is equal to the total number of maximal chains in* $[x,y]$.

Proof. First of all, observe that $\eta^k(x,y)$ gives us the number of maximal chains of length k from x to y. It is similar to $\zeta^k(x,y)$ except for the fact that we avoid repetitions in this case. So, then $(\zeta-1)^k(x,y)$ is equivalent to $\eta^k(x,y)$. Now, $(1-\eta)^{-1} = 1+\eta+\eta^2+....+\eta^\ell$ since $\eta^{\ell+1} = 0$ for some $\ell \in \mathbb{N}$ denoting the length of the interval $[x,y]$. □

6.2 Möbius Functions and Inversion formula

$\zeta(x,x) = 1$ for all x in a poset P ensures the existence of the inverse ζ^{-1} of ζ. Since multiplying by ζ is analogous to integration in calculus, so its inverse is expected to behave like that of a differential operator. And, it is called the *Möbius function* denoted by μ which is defined recursively.

Definition 6.2.1. Let $\mu \in I(P,K)$. We define μ by:

$\mu(x,x) = 1$ for all $x \in P$

$\mu(x,y) = -\sum\limits_{x \leq z < y} \mu(x,z)$ for all $x < y$ in P

This is derived from the relation $\mu * \zeta = \delta$.

Before moving on to compute Möbius functions of certain posets discussed so far, we'll give Möbius inversion formula and the product theorem that would be utilized thereupon in order to facilitate easier calculations.

Proposition 6.2.2 (Möbius inversion formula for posets)**.** *Let P be a poset in which every principal order ideal is finite. Let $f, g : P \to \mathbb{C}$. Then*

$$g(x) = \sum_{y \leq x} f(y) \text{ for all } x \in P$$

if and only if

$$f(x) = \sum_{y \leq x} g(y)\mu(y,x) \text{ for all } x \in P.$$

Proof. Observe that the set $\mathbb{C}^P = \{f \mid f : P \to \mathbb{C}\}$ forms a vector space with addition and scalar multiplication defined as usual.

$$(f+g)(x) = f(x) + g(x),$$

$$(kf)(x) = k.f(x).$$

Now, the incidence algebra $I(P)$ acts on $\mathbb{C}^P$ on the right i.e. $\mathbb{C}^P \times I(P) \to \mathbb{C}^P$ by $(f\xi)(x) = \sum\limits_{y \leq x} f(y)\xi(y,x)$, where $f \in \mathbb{C}^P$ and $\xi \in I(P)$. We verify that it is an action.

$$(f\delta)(x) = \sum_{y \leq x} f(y)\delta(y,x) = \sum_{y < x} f(y)\delta(y,x) + f(x)\delta(x,x) = f(x),$$

and

$$\begin{aligned}((f\xi)\chi)(x) &= \sum_{y\leq x}(f\xi)(y)\chi(y,x)\\ &= \sum_{y\leq x}\Bigg(\sum_{z\leq y} f(z)\xi(z,y)\Bigg)\chi(y,x)\\ &= \sum_{z\leq x} f(z)\Bigg(\sum_{z\leq y\leq x}\xi(z,y)\chi(y,x)\Bigg)\\ &= \sum_{z\leq x} f(z)\big(\xi\chi(z,x)\big)\\ &= (f(\xi\chi))(x).\end{aligned}$$

In terms of this action, Möbius inversion formula is then the statement that $f\zeta = g \Leftrightarrow f = g\mu$, which is indeed true since $g\mu = (f\zeta)\mu = f(\zeta\mu) = f\delta = f$. Therefore, $f(x) = (g\mu)(x) = \sum_{y\leq x} g(y)\mu(y,x)$. □

Proposition 6.2.3 (Dual form of Möbius inversion formula)**.** *Let P be a poset in which every principal dual order ideal is finite. Let $f, g : P \to \mathbb{C}$. Then*

$$g(x) = \sum_{y\geq x} f(y) \textit{ for all } x \in P$$

if and only if

$$f(x) = \sum_{y\geq x} \mu(x,y)g(y) \textit{ for all } x \in P.$$

Proof. The proof goes on similar lines as for Proposition 6.2.2, except that $I(P)$ in this case acts on the left by $(\xi f)(x) = \sum_{y\geq x}\xi(x,y)f(y)$. □

Proposition 6.2.4 (Product theorem)**.** *Let P and Q be locally finite posets with $P\times Q$ as their direct product. If $x, x' \in P$; $y, y' \in Q$ and $(x,y) \leq (x',y')$ in $P\times Q$, then*

$$\mu_{P\times Q}((x,y),(x',y')) = \mu_P(x,x')\mu_Q(y,y').$$

Proof. Let $(x,y) \leq (x',y')$ and $\mu_R((x,y),(x',y')) = \mu_P(x,x')\mu_Q(y,y')$. We will use $\delta_{P\times Q}((x,y),(x',y')) = \delta_P(x,x')\delta_Q(y,y')$, so we compute

$$(\zeta_{P\times Q} * \mu_R)((x,y),(x',y'))$$

$$= \sum_{(x,y)\leq(u,v)\leq(x',y')} \zeta_{P\times Q}((x,y)(u,v))\mu_R((u,v)(x',y'))$$

$$= \sum_{(x,y)\leq(u,v)\leq(x',y')} \mu_P(u,x')\mu_Q(v,y')$$

$$= \sum_{x\leq u\leq x'} \sum_{y\leq v\leq y'} \mu_P(u,x')\mu_Q(v,y')$$

$$= \left(\sum_{x\leq u\leq x'} \mu_P(u,x')\right)\left(\sum_{y\leq v\leq y'} \mu_Q(v,y')\right)$$

$$= \left(\sum_{x\leq u\leq x'} \zeta_P(x,u)\mu_P(u,x')\right)\left(\sum_{y\leq v\leq y'} \zeta_Q(y,v)\mu_Q(v,y')\right)$$

$$= \Big((\zeta_P * \mu_P)(x,x')\Big)\Big((\zeta_Q * \mu_Q)(y,y')\Big)$$

$$= \delta_P(x,x')\delta_Q(y,y')$$

$$= \delta_{P\times Q}((x,y),(x',y')).$$

Therefore, μ_R equals $\mu_{P\times Q}$ and hence, the result. □

Examples 6.2.5. (Applications of Möbius inversion formula)

1. For a chain $\mathbb{N}$, we have

$$\mu(x,y) = \begin{cases} 1, & \text{if } x = y \\ \text{-1}, & \text{if } x+1 = y \\ 0, & \text{otherwise.} \end{cases}$$

Using this, for $g(n) = \sum_{i\leq n} f(i)$, where $f, g : P \to K$, by Möbius inversion we have

$$f(n) = \sum_{i\leq n} g(i)\mu(i,n) = g(n) - g(n-1) = (\Delta g)(n).$$

These operations of $\sum$ and Δ give us the finite difference analogue of "fundamental theorem of calculus."

2. Let $P = B_n$, the boolean algebra of rank n. Then $B_n \cong \mathbf{2}^n$. Identify B_n with set of all subsets of an n-set i.e. a subset T represents $(a_1, a_2, ..., a_n) \in P$, where $a_i = 1$ if $i \in T$ and $a_i = 0$ if $i \notin T$. If S represents $(b_1, b_2, ..., b_n) \in P$ and $T \subset S$, then by the product theorem we have the following:
$$\begin{aligned}\mu(T, S) &= \mu((a_1, a_2, ..., a_n), (b_1, b_2, ..., b_n)) \\ &= \prod_{i=1}^{n} \mu_{\mathbf{2}}(a_i, b_i) = (-1)^{|S-T|}.\end{aligned}$$

3. Let $n_1, ..., n_k$ be non-negative integers and let $P = \mathbf{n_1} + \mathbf{1} \times .... \times \mathbf{n_k} + \mathbf{1}$.
Identify P with the set of all k-tuples $(a_1, a_2, ..., a_k) \in \mathbb{N}^k$ with $0 \leq a_i \leq n_i$, ordered componentwise.
If $a_i \leq b_i$ for all i, then the interval $[(a_1, ..., a_k), (b_1, ..., b_k)]$ in P is isomorphic to $\mathbf{b_1} - \mathbf{a_1} + \mathbf{1} \times .... \times \mathbf{b_k} - \mathbf{a_k} + \mathbf{1}$.
Hence, we have
$$\mu((a_1, ..., a_k), (b_1, ..., b_k)) = \begin{cases} (-1)^{\sum(b_i - a_i)}, & \text{if each } b_i - a_i = 0 \text{ or } 1 \\ 0, & \text{otherwise.} \end{cases}$$
If N is a positive integer of the form $p_1^{n_1} p_2^{n_2} .... p_k^{n_k}$, where the p_i's are distinct primes, then P is isomorphic to the poset D_N.

Further, if M divides N, then
$$\mu(M, N) = \begin{cases} (-1)^t, & \text{if } N/M \text{ is a product of } t \text{ distinct primes} \\ 0, & \text{otherwise.} \end{cases}$$
In other words, $\mu(M, N)$ is just the classical number-theoretic Möbius function $\mu(N/M)$. Then, the Möbius inversion formula becomes the classical one i.e.
$$g(n) = \sum_{d|n} f(d) \text{ for all } n|N$$
if and only if
$$f(n) = \sum_{d|n} g(d)\mu(n/d) \text{ for all } n|N.$$

4. Take a collection of n finite sets denoted $S_1, S_2, ..., S_n$. Form a poset P of all their possible intersections and order them via containment, including the void intersection i.e. $\bigcap_{i\in\emptyset} S_i = \bigcup_{i=1}^{n} S_i = \hat{1}$. For $T \in P$, let $f(T) = \Big|\{x \in T : x \notin T' \text{ for any } T' < T \text{ in } P\}\Big|$ and $g(T) = \big|T\big|$. We are looking for $g(\hat{1}) = \sum\limits_{T\leq\hat{1}} f(T)$ which also equals $\big|S_1 \cup S_2 .... \cup S_n\big|$. Now, $g(T) = \sum\limits_{T'\leq T} f(T')$, so apply Möbius inversion to obtain that $f(T) = \sum\limits_{T'\leq T} g(T')\mu(T',T)$ and consequently, we have

$$\hat{0} = f(\hat{1}) = \sum_{T'\leq\hat{1}} g(T')\mu(T',\hat{1}),$$

$$\Rightarrow g(\hat{1}) = -\sum_{T'\leq\hat{1}} g(T')\mu(T',\hat{1}) = -\sum_{T'<\hat{1}} \big|T'\big|\mu(T',\hat{1}).$$

This shows that the theory of Möbius inversion results in the generalization of the well known Principle of Inclusion-Exclusion when incorporated with some minor simplifications.

For instance, if we have four finite sets A, B, C, D with $D = A \cap B = A \cap C = B \cap C = A \cap B \cap C$, then by Inclusion-Exclusion principle

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$= |A| + |B| + |C| - 2|D|.$$

Here, P is given by the figure below, in which case $\mu(A,\hat{1}) = \mu(B,\hat{1}) = \mu(C,\hat{1}) = -1$ and $\mu(D,\hat{1}) = 2$ that are consistent with the coefficients in the expression above.

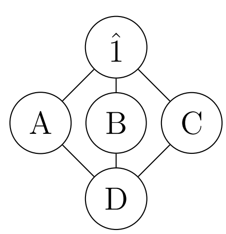


Figure 6.2

6.3 Simplicial Complexes

We begin by defining a simplex that provides a foundational structure for building Simplicial Complexes. In simple terms, simplices are glued together to form a simplicial complex and it's combinatorial counterpart is categorized as an abstract simplicial complex in which case simplex corresponds to any finite set of vertices.

Definition 6.3.1. A *k-simplex* is defined to be a k-dimensional polytope which is the convex hull of its $k+1$ vertices. For instance, 0-simplex is a point, 1-simplex is a line segment, 2-simplex is a triangle and 3-simplex is a tetrahedron.

Definition 6.3.2. Let V be a finite vertex set. An (*abstract*) *simplicial complex* Δ is a collection of subsets of V that satisfy the following:

(1) $\{v\} \in \Delta$ for all $v \in V$.

(2) If $T \in \Delta$ and $S \subset T$, then $S \in \Delta$.

If $T \in \Delta$, then we say that T is a $face$ of Δ and dimension of T is defined to be $|T| - 1$. The maximal dimensional faces are called the $facets$ of Δ and dimension of the complex i.e. $\dim\Delta$ equals the dimension the largest dimension of any of its faces.

Remark 6.3.3. Let Δ be a simplicial complex on a vertex set V. Then, $\emptyset \in \Delta$ always provided $\Delta \neq \emptyset$. $\Delta = \emptyset$ is called the *void* abstract simplicial complex and denoted by $\emptyset$ or $\{\}$ whereas an *empty* abstract simplicial complex is denoted by $\{\emptyset\}$.

The dimension of an empty abstract simplicial complex is -1, since cardinality of an empty set is zero.

We now define face posets for studying simplicial complexes from combinatorial perspective.

Definition 6.3.4. Given a poset P, we define a simplicial complex $\Delta(P)$, known as the *order complex* of P. $\Delta(P)$ has the underlying set of P as vertices and the finite chains of P as faces.

Examples 6.3.5.

1. Let $V = \{v_1, v_2, v_3, v_4\} = \mathbf{4}$. Then, Δ on V is given by

$$\begin{aligned}\Delta &= \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,4\}, \{3,4\}, \{1,2,3\}\Big\} \\ &= \Big\langle \{1,2,3\}, \{1,4\}, \{3,4\} \Big\rangle\end{aligned}$$

   for the figure shown below:

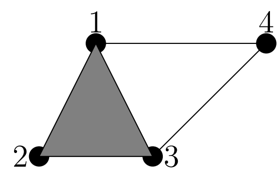


Figure 6.3

2. If $P = \mathbf{3}$, then $\Delta(P) = \Big\{\{1,2\}, \{1,3\}, \{2,3\}\Big\}$.

6.4 Möbius function and Euler characteristic

Proposition 6.4.1. *Let P be a finite poset. For the poset $\widehat{P}$, let c_i be the number of i-chains $(\hat{0} = x_0 < x_1 < .... < x_i = \hat{1})$ between $\hat{0}$ and $\hat{1}$. Then*

$\mu_{\widehat{P}}(\hat{0}, \hat{1}) = c_0 - c_1 + c_2 - c_3 + ...$

Proof. Notice that $c_0 = 0$ and $c_1 = 1$. Then by making simple computation, we obtain that

$$\begin{aligned}\mu_{\widehat{P}}(\hat{0}, \hat{1}) &= \big(1 + (\zeta - 1)\big)^{-1}(\hat{0}, \hat{1}) \\ &= \big(1 - (\zeta - 1) + (\zeta - 1)^2 - .....\big)(\hat{0}, \hat{1}) \\ &= \delta(\hat{0}, \hat{1}) - (\zeta - 1)(\hat{0}, \hat{1}) + (\zeta - 1)^2(\hat{0}, \hat{1}) - ..... \\ &= c_0 - c_1 + c_2 - c_3 + ...\end{aligned}$$

□

The aforementioned proposition sets up the background for interpreting Möbius function in topological context. $\mu_{\widehat{P}}(\hat{0}, \hat{1})$ actually turns out to be an Euler characteristic which is a well known topological invariant.

Definition 6.4.2. For a finite Δ, let f_i denote the number of i-dimensional faces of Δ. Then, the *Euler characteristic* of Δ is defined as

$$\chi(\Delta) = \sum_{i\geq 0}(-1)^i f_i = f_0 - f_1 + f_2 - ....$$

and, the *reduced* Euler characteristic by $\widetilde{\chi}(\Delta) = \chi(\Delta) - 1$.

Proposition 6.4.3. *Let P be a finite poset. Then, we have*

$$\mu_{\widehat{P}}(\hat{0},\hat{1}) = \widetilde{\chi}(\Delta(P)).$$

Proof. Follows from Proposition 6.4.1 and Definition 6.4.2 by which f_k corresponds to c_{k+2} for $k \geq -1$. $\square$

6.5 Möbius functions of Lattices

The theory of Möbius algebras is purposely designed to deal with Möbius functions of lattices in specific and not intended for any general partially ordered set.

Definition 6.5.1. Let L be a finite lattice and K be a field. The *Möbius algebra* $A(L,K)$ is defined to be the semigroup algebra of L with the meet operation, over K. To put in other words,

$$A(L,K) = \Big\{\sum_{v\in L}\alpha_v v : \alpha_v \in K\Big\}$$

where for $\alpha = \sum\limits_v \alpha_v v$ and $\beta = \sum\limits_w \beta_w w$, we have addition and multiplication defined as follows:

$$\alpha + \beta = \sum_{v\in L}(\alpha_v + \beta_v)v$$

$$\alpha\beta = \sum_{u\in L}\Big(\sum_{v\wedge w=u}\alpha_v\beta_w\Big)u$$

Remark 6.5.2. The Möbius algebra $A(L,K)$ is clearly a commutative algebra (as $\alpha\beta = \beta\alpha$) and $\{1v : v\in L\}$ is a K-basis of $A(L,K)$. Thus, $\dim_K\big(A(L,K)\big) = |L|$.

Proposition 6.5.3. *For a finite lattice L, $A(L,K)\cong K^{|L|}$ as K-algebras.*

Proof. For every $x \in L$, we define $\theta_x \in A(L,K)$ by $\theta_x = \sum\limits_{y \leq x} \mu(y,x)y$.

Then, apply Möbius inversion formula in order to obtain that $x = \sum\limits_{y \leq x} \theta_y$.

Since $\{1x : x \in L\}$ is a basis of $A(L,K)$, therefore the set $\{\theta_x : x \in L\}$ is also a generating set for $A(L,K)$. But, we also have $\big|\{\theta_x : x \in L\}\big| = |L| = \dim_K\big(A(L,K)\big)$. Hence, $\{\theta_x : x \in L\}$ also forms a basis for $A(L,K)$.

Now, compare $A(L,K)$ with the usual algebra $A'(L,K) = \underbrace{K \times K \times .... \times K}_{|L| \text{ -times}}$ $= K^{|L|}$ where we have addition and multiplication defined componentwise and for each $x \in L$, $e_x \in A'(L,K)$;

$$e_x(y) = \begin{cases} 0 & \text{if } y \neq x \\ 1 & \text{if } y = x \end{cases}$$

Thus, $\{e_x : x \in L\}$ is a standard basis of K-algebra $A'(L,K)$ where multiplication of basis elements is given by $e_x.e_y = \delta_{xy}e_x$.

Finally, we define $\phi : A(L,K) \to A'(L,K)$ by $\phi(\theta_x) = e_x$ for all $x \in L$. Certainly, ϕ is a K-vector space isomorphism. Let $x, y \in L$. Then

$$\begin{aligned} \phi\big((1x)(1y)\big) &= \phi(xy) = \phi(x \wedge y) \\ &= \phi\Big(\sum_{u \leq x \wedge y} \theta_u\Big) = \sum_{u \leq x \wedge y} \phi(\theta_u) = \sum_{u \leq x \wedge y} e_u, \end{aligned}$$

and

$$\begin{aligned} \phi(1x)\phi(1y) &= \phi\Big(\sum_{v \leq x} \theta_v\Big)\phi\Big(\sum_{w \leq y} \theta_w\Big) = \Big(\sum_{v \leq x} \phi(\theta_v)\Big)\Big(\sum_{w \leq y} \phi(\theta_w)\Big) \\ &= \Big(\sum_{v \leq x} e_v\Big)\Big(\sum_{w \leq y} e_w\Big) = \sum_{\substack{v \leq x \\ w \leq y}} e_v e_w \\ &= \sum_{u \leq x \wedge y} e_u. \end{aligned}$$

Therefore, ϕ is an isomorphism of K-algebras. $\square$

Corollary 6.5.4. *Let L be a finite lattice having at least two elements and with $\hat{1} \neq a \in L$. Then*

$$\sum_{x : x \wedge a = \hat{0}} \mu(x, \hat{1}) = 0.$$

Proof. Consider the Möbius algebra $A(L, \mathbb{C})$ in which

$$a\theta_{\hat{1}} = \Big(\sum_{y \leq a} \theta_y\Big)\theta_{\hat{1}} = \sum_{y \leq a} \theta_y \theta_{\hat{1}} = 0 \ \text{ if } \ a \neq \hat{1} \tag{6.1}$$

We may also write $\theta_{\hat{1}} = \sum_{y \leq \hat{1}} \mu(y, \hat{1}) y$, so then one obtains the expression

$$a\theta_{\hat{1}} = \sum_{y \leq \hat{1}} \mu(y, \hat{1})(a \wedge y). \tag{6.2}$$

We also have $a\theta_{\hat{1}} = \sum_{v \in L} \alpha_v v$. On equating the coefficients of $\hat{0}$, we see that $\alpha_{\hat{0}} = 0$ from (6.1) and $\alpha_{\hat{0}} = \sum_{x : x \wedge a = \hat{0}} \mu(x, \hat{1})$ from (6.2). Hence, the result follows. □

Corollary 6.5.5. *Let L be a finite lattice and $X \subseteq L$ such that (1) $\hat{1} \notin X$ and (2) If $y \in L$ and $y \neq \hat{1}$, then $y \leq x$ for some $x \in X$. Then*

$$\mu(\hat{0}, \hat{1}) = \sum_k (-1)^k N_k,$$

where N_k represents the number of k-subsets of X whose meet is $\hat{0}$.

Proof. We see that for any $x \in L$,

$$\hat{1} - x = \sum_{y \leq \hat{1}} \theta_y - \sum_{y \leq x} \theta_y = \sum_{y \not\leq x} \theta_y \text{ in } A(L, \mathbb{C}).$$

By Proposition 6.5.3, $\prod_{x \in X} (\hat{1} - x) = \prod_{x \in X} \Big(\sum_{y \not\leq x} \theta_y\Big) = \sum_{\substack{y \not\leq x \\ \forall x \in X}} \theta_y = \theta_{\hat{1}}$

$$= \sum_{y \leq \hat{1}} \mu(y, \hat{1}) y$$

Now, coefficient of $\hat{0}$ on RHS is $\mu(\hat{0}, \hat{1})$. However, coefficient of $\hat{0}$ on LHS turns out to be $\sum_k (-1)^k N_k$ since $\prod_{x \in X} (\hat{1} - x) = \sum_{T \subseteq X} \Big(\prod_{z \in T} z\Big)(-1)^{|T|} = \sum_k (-1)^k \sum_{\substack{|T| = k \\ T \subseteq X}} \Big(\prod_{z \in T} z\Big)$.

□

Corollary 6.5.6. *Let L be a finite lattice and assume that $\hat{0}$ is not a meet of coatoms. Then, $\mu(\hat{0}, \hat{1}) = 0$. The dual version of this result states that, if $\hat{1}$ is not a join of atoms, then $\mu(\hat{0}, \hat{1}) = 0$.*

Proof. Firstly, observe that it will suffice if we take X to be the set comprising of just the coatoms in Corollary 6.5.5. Now, we are given that $\hat{0}$ is not a meet of coatoms, so then $N_k = 0$ for all $k \geq 1$. Hence, $\mu(\hat{0}, \hat{1}) = 0$. Dually, the other part follows. □

For a finite lattice L with at least two elements, it can be shown that

$$\sum_{x : x \wedge a = \hat{0}} \mu(x, \hat{1}) = 0,$$

where $\hat{1} \neq a \in L$ (Corollary 6.5.4). For a finite semimodular lattice L, this result has a dual version which is given by the following:

$$\sum_{x : x \vee a = \hat{1}} \mu(\hat{0}, x) = 0.$$

For an atom $a \in L$, where L is semimodular with $x \vee a = \hat{1}$, it can be shown that either $x = \hat{1}$ or x is a coatom with $x \ngeq a$. Thus, for a semimodular lattice,

$$\mu(\hat{0}, \hat{1}) = -\sum \mu(\hat{0}, x), \tag{6.3}$$

where summation runs over all coatoms x with $x \ngeq a$.

Corollary 6.5.7. *The Möbius function of a finite semimodular lattice alternates in sign.*

Proof. Since every interval in a finite semimodular lattice is again semimodular, on applying (6.3), we see that

$$(-1)^{\ell(x,y)} \mu_{[x,y]}(x, y) = (-1)^{\ell(x,y)} \Big[-\sum \mu(x, y') \Big],$$

where summation on the RHS is over all coatoms y' in $[x, y]$ such that $y' \ngeq x'$ for a fixed atom x' in $[x, y]$.

Clearly, $\mu(x, y') = \mu_{[x,y']}(x, y')$ and by induction hypothesis,

$$(-1)^{\ell(x,y')} \mu_{[x,y']}(x, y') \geq 0.$$

As $\ell(x, y) - 1 = \ell(x, y')$, we see that $(-1)^{\ell(x,y)} \mu(x, y) \geq 0$. □

We now turn to the most important examples of semimodular lattices.

Examples 6.5.8.

1. Consider an n-dimensional vector space $V_n = V_n(q)$ over a finite field $\mathbb{F}_q$ with q-elements. Let $L_n = L_n(q)$ be the poset of all subspaces of $V_n = V_n(q)$. Clearly, $L_n(q)$ is a finite geometric modular lattice. For $W_1 \subseteq W_2$, in $L_n(q)$, the interval $[W_1, W_2]$ is isomorphic to $L_m(q)$, where $m = \dim_{\mathbb{F}_q}\left(\dfrac{W_2}{W_1}\right)$.

   Let μ_m be the Möbius function of $L_m(q)$. Consider an atom a in $L_n(q)$. Then, a is an one-dimensional subspace of $V_n(q)$. Total number of coatoms in $L_n(q)$ is given by $\binom{\boldsymbol{n}}{\boldsymbol{n-1}} = q^{n-1} + q^{n-2} + ... + 1$. Also, the number of coatoms in $L_n(q)$ above a will be precisely the number of coatoms in $L_{n-1}(q)$, which is given by $\binom{\boldsymbol{n-1}}{\boldsymbol{n-2}}$ $= q^{n-2} + ... + 1$. Therefore,

$$\mu_n \equiv -\sum \mu_{n-1},$$

   where summation runs over all coatoms in $L_n(q)$ which are not above a. Hence, $\mu_n = -q^{n-1}\mu_{n-1}$. Since $\mu_0 = 1$, so we have

$$\mu_n = (-1)^2 q^{n-1} q^{n-2} \mu_{n-2} = ... = (-1)^n q^{\binom{n}{2}}.$$

   The Möbius function of $L_n(q)$ is due to P. Hall. Consider the following counting problem: What is the number of generating subsets of $V_n(q)$? We use Möbius inversion formula to solve this in the following example.

2. Let $f(W)$ be the number of subsets of $V_n(q)$ spanning $W \in L_n(q)$. Also, let $g(W)$ be the number of subsets of $V_n(q)$ whose span is contained in $W \in L_n(q)$. Thus, $g(W) = 2^{q dim W} - 1$ (Empty set $\emptyset$ do not span a subspace). Since

$$g(W) = \sum_{W' \leq W} f(W'),$$

   by Möbius inversion formula in $L_n(q)$, we get

$$f(W) = \sum_{W' \leq W} g(W')\mu(W', W).$$

Thus, on taking $W = V_n(q)$,

$$\begin{aligned}
f(V_n) &= \sum_{W'} g(W')\mu(W', V_n) \\
&= \sum_{k=0}^{n} \left(\sum_{\substack{W' \\ dim W'=k}} g(W')\mu(W', V_n) \right) \\
&= \sum_{k=0}^{n} \left(\sum_{\substack{W' \\ dim W'=k}} \big(2^{qk} - 1\big)\mu_{n-k} \right) \\
&= \sum_{k=0}^{n} \binom{\boldsymbol{n}}{\boldsymbol{k}} (-1)^{n-k} q^{\binom{n-k}{2}} \big(2^{qk} - 1\big).
\end{aligned}$$

Chapter 7

Applications

In this chapter, we shall present various illustrations of usefulness of the Möbius function of a poset.

1. Chromatic polynomial of a graph

Consider a simple graph $G = (V, E)$ with vertex set V and edge set E. We say that the graph G is *n-colourable* if it is possible to color each vertex of G using n colors so that adjacent vertices always have different colours. The smallest n for which the given graph G is n-colourable is called its *chromatic number* and it is denoted by $ch(G)$. For each $n \in \mathbb{N}$, counting the number of all possible n-colourings on G defines a function $ch_G : \mathbb{N} \to \mathbb{N}$ called the *chromatic function* of G. It can be shown that the numerical function ch_G is actually a polynomial and it is called the *chromatic polynomial* of the graph G.

Birkhoff introduced the concept of Graph colouring in an attempt to prove "Four colour problem." The chromatic number and chromatic polynomial of a graph are invariants associated with a graph.

Examples 7.1.1.

1. If G is a discrete graph, i.e., $E = \emptyset$, then chromatic number of G is $ch(G) = 1$.

Further, $ch_G(n) = n^{|V|}$.

2. Bipartite graph are precisely (simple) graphs with chromatic number 2.

3. If $|V| = m$ and $G = K_m$ is the complete graph, then $ch(K_m) = m$ and the chromatic polynomial is given by

$$ch_{K_m}(n) = n(n-1)....(n-m+1) = n^{\underline{m}}.$$

Remark 7.1.2.

1. An n-colouring on a graph $G = (V, E)$ corresponds to a function $f : V \to [n]$ such that $f(v) \neq f(v')$ if $\{v, v'\} \in E$. Thus,

$$ch_G(n) = \left|\left\{f : V \to [n] : f(v) \neq f(v') \text{ if } \{v, v'\} \in E\right\}\right|.$$

2. The chromatic number $ch(G)$ can be obtained from the chromatic polynomial $ch_G(n)$ of a graph $G = (V, E)$. We have $ch(G)$ =inf $k : ch_G(k) > 0$. Equivalently, $ch(G) = m$ if and only if $ch_G(k) = 0$ for $k < m$ and $ch_G(m) > 0$.

We now proceed to express the chromatic polynomial $ch_G(n)$ of a graph G in terms of Möbius function of a poset L_G associated with G. This result is due to Gian-Carlo Rota. For a graph $G = (V, E)$, let L_G be the set of all partitions π of V such that each block of π is connected. In other words, if $\pi = \{B_1, ..., B_s\}$ is a partition of V, then any two vertices in a block B_i are connected by a path in G. Then, L_G is a poset where the partial order is defined by refinement.

Theorem 7.1.3. [Rota] *For a graph $G = (V, E)$, the chromatic polynomial $ch_G(n)$ is given by*

$$ch_G(n) = \sum_{\pi \in L_G} \mu(\hat{0}, \pi) n^{|\pi|},$$

where $|\pi|$ is the number of blocks in π and $\mu = \mu_{L_G}$ is the Möbius function of G.

Proof. For a partition $\sigma = \{B_1, ..., B_s\}$ of V, consider the set C^n_σ of all functions $f : V \to [n]$ such that $f(a) = f(b)$ if $a, b \in B_i$ and $f(a) \neq f(b)$ if $a \in B_i, b \in B_j (i \neq j)$ with $\{a, b\} \in E$.

If $f : V \to [n]$ is any function, then there is a unique partition $\sigma \in L_G$ such that $f \in C^n_\sigma$. In fact, given a function f, consider a partition $\{B_1, ..., B_s\}$ of V such that $f(B_i)$ is singleton for all i. Now, σ can be taken to be the coarsest refinement of the partition $\{B_1, ..., B_s\}$ such that all blocks of σ are connected. Clearly, σ is unique and $f \in C^n_\sigma$. Now, for $\pi \in L_G$ consider the set S_π of all functions $f : V \to [n]$ such that f is constant on every block of π. Clearly, $|S_\pi| = n^{|\pi|}$. From the above remark,

$$S_\pi = \coprod_{\pi \leq \sigma} C^n_\sigma.$$

Thus, we obtain $n^{|\pi|} = \sum_{\pi \leq \sigma} |C^n_\sigma|$. Using Möbius Inversion formula (Proposition 6.2.2), we have

$$|C^n_\pi| = \sum_{\pi \leq \sigma} n^{|\sigma|} \mu(\pi, \sigma).$$

Specializing the last expression to $\pi = \hat{0}$, we obtain

$$|C^n_{\hat{0}}| = \sum_{\sigma \in L_G} \mu(\hat{0}, \sigma) n^{|\sigma|}.$$

Since $\hat{0}$ is the partition $\{\{1\}, \{2\}, ..., \{n\}\}$, we see that $C^n_{\hat{0}}$ is the set of all n-colourings of G. Hence, $|C^n_{\hat{0}}| = ch_G(n)$. □

Corollary 7.1.4. $\sum_{\pi \in \Pi_m} \mu(\hat{0}, \pi) n^{|\pi|} = n^{\underline{m}}$.

Proof. Consider $G = K_m$, then $L_G = \Pi_m$. Hence, this corollary follows from Theorem 7.3 in view of the fact that $ch_{K_m}(n) = n^{\underline{m}}$.

□

2. Möbius function of Π_n

The set Π_n of all partitions of $[n]$ is a poset w.r.t the partial order defined by refinement. Every maximal chain in Π_n is of length $n - 1$. For every $\pi \in \Pi_n$, the rank $\rho(\pi) = n-$(number of blocks of π)$= n - |\pi|$. Thus, Π_n is a graded poset of rank $n - 1$. Also, Π_n

is a geometric lattice. If $\pi = \{B_1, ..., B_s\} \in \Pi_n$, then the interval $[\pi, \hat{1}]$ is isomorphic to the partition lattice of the set $\{B_1, ..., B_s\} \cong [s]$. Thus, the interval $[\pi, \hat{1}] \cong \Pi_s$.

Consider $a = \big\{\{1, 2, ..., n-1\}, \{n\}\big\}$. Then, a is any coatom in Π_n. Also, $x \in \Pi_n$ satisfies $x \wedge a = \hat{0}$ if and only if $x = \hat{0}$ or x is an atom $\sigma_i = \big\{\{1\}, ..., \{i-1\}, \{i+1\}, ..., \{n-1\}, \{i, n\}\big\}$ for $1 \leq i \leq n-1$. Thus,

$$\sum_{x : x \wedge a = \hat{0}} \mu(x, \hat{1}) = 0,$$

implies that

$$\mu_n = \mu(\hat{0}, \hat{1}) = -\sum \mu(x, \hat{1}),$$

where summation runs over all atoms x of the form σ_i, $i \in [n-1]$. Also, $[x, \hat{1}] \cong \Pi_{n-1}$. Therefore, $\mu_n = -(n-1)\mu_{n-1}$. Since $\mu_0 = 1$, we get

$$\mu_n = (-1)^2(n-1)(n-2)\mu_{n-2} = ... = (-1)^{n-1}(n-1)!$$

The above equation can also be deduced from

$$\sum_{\pi \in \Pi_n} \mu(\hat{0}, \pi) q^{|\pi|} = q^{\underline{n}} = q(q-1)....(q-n+1),$$

by equating the coefficient of q, i.e.,

$$\mu(\hat{0}, \hat{1}) = \mu_n = (-1)^{n-1}(n-1)!.$$

Motivated by Theorem 7.3, we define *characteristic polynomial* of a finite graded poset P of rank n and with $\hat{0}$ as follows:

$$\chi(P, q) = \sum_{x \in P} \mu(\hat{0}, x) q^{n-\rho(x)},$$

where $\rho(x) =$ rank of x in P.

In view of Theorem 7.3, for a graph $G = (V, E)$,

$$\chi(L_G, q) = \sum_{\sigma \in L_G} \mu(\hat{0}, \sigma) q^{\mathrm{rank}(L_G) - \rho(\sigma)},$$

where $\rho(\sigma)$ = rank of σ in L_G. But, rank(L_G)$= n - c$, where $n = |V|$ and c is the number of connected components of G. So, then we have

$$\begin{aligned}\chi(L_G, q) &= \sum_{\sigma \in L_G} \mu(\hat{0}, \sigma) q^{(n-c)-(n-|\sigma|)} \\ &= q^{-c}\Big(\sum_{\sigma \in L_G} \mu(\hat{0}, \sigma) q^{|\sigma|}\Big) \\ &= q^{-c} \mathrm{ch}_G(q).\end{aligned}$$

On rearranging terms in the characteristic polynomial $\chi(P, q)$, we obtain

$$\begin{aligned}\chi(P, q) &= \sum_{k=0}^{n} \Big(\sum_{\substack{x \in P \\ \rho(x)=k}} \mu(\hat{0}, x)\Big) q^{n-k} \\ &= \sum_{k=0}^{n} w_k q^{n-k},\end{aligned}$$

where $w_k = \sum\limits_{\substack{x \in P \\ \rho(x)=k}} \mu(\hat{0}, x)$ is called the *k-th Whitney number of P of the first kind*. Similarly, from the rank generating function $F(P, q)$ of the graded poset P of rank n, we have

$$F(P, q) = \sum_{x \in P} q^{\rho(x)} = \sum_{k=0}^{n} W_k q^k,$$

where W_k is the number of elements of P of rank k. W_k is called the *k-th Whitney number of P of the second kind.*

For $P = \Pi_n$, we see that $F(P, q) = \sum\limits_{k=0}^{n-1} S(n, n-k) q^k$, where $S(n, n-k)$ is a Stirling number of the second kind. Thus, the k-th Whitney number of Π_n of the second kind $W_k = S(n, n-k)$. Also,

$$\begin{aligned}\chi(\Pi_n, q) &= (q-1)(q-2)......(q-n+1) \\ &= \chi(L_{K_n}, q) \\ &= q^{-1} \mathrm{ch}_{K_n}(q).\end{aligned}$$

Thus, it can be proved that the k-th Whitney number of Π_n of the first kind $w_k = s(n, n-k)$, is the Stirling number of the first kind.

3. Zeta Polynomials of a poset

Consider a finite poset P. Let $Z(P,n)$ be the number of multichains $x_1 \leq x_2 \leq ..... \leq x_{n-1}$ in P for $n \geq 2$. Then, we see that $Z(P,n)$ is actually a polynomial function in n.

Proposition 7.3.1. *Let P be a finite poset. If b_i is the number of chains $x_1 < x_2 < ..... < x_{i-1}$ in P, then for $n \geq 2$,*

$$Z(P,n) = \sum_{i \geq 2} b_i \binom{n-2}{i-2}.$$

Proof. Consider an $(n-1)$-multichain in P with support $x_1 < x_2 < ..... < x_{i-1}$. Such a multichain may be expressed as $\{{x_1}^{a_1}, {x_2}^{a_2}, ..., {x_{i-1}}^{a_{i-1}}\}$ with $a_j \geq 1$ and $\sum_{j=1}^{i-1} a_j = n-1$. The number of $(n-1)$-multichains in P with support $x_1 < x_2 < ..... < x_{i-1}$ is $\binom{n-2}{i-2}$. Then, for $n \geq 2$, we have

$$Z(P,n) = \sum_{i \geq 2} b_i \binom{n-2}{i-2}.$$

If d is the length of the longest chain in P, then $b_i = 0$ for $i > d+2$. This shows that $Z(P,n)$ is a polynomial function of n with leading coefficient $b_{d+2}/d!$. □

Remark 7.3.2. $Z(P,2) = b_2 = |P|$.

Proposition 7.3.3. *The zeta polynomial $Z(P,n)$ defined for $n \geq 2$ can be extended for all $n \in \mathbb{Z}$. In particular,*

1. $Z(P,1) = \chi(\Delta(P)) = 1 + \mu_{\widehat{P}}(\hat{0}, \hat{1})$.

2. *If P has a $\hat{0}$ and $\hat{1}$, then $Z(P,n) = \zeta^n(\hat{0}, \hat{1})$ for all $n \in \mathbb{Z}$. Also,* $Z(P,-1) = \mu(\hat{0}, \hat{1})$.

Proof. From Proposition 7.3.1, we have

$$Z(P,n) = \sum_{i \geq 2} b_i \binom{n-2}{i-2}$$

as polynomial in n. Putting $n = 1$, we get

$$Z(P,1) = \sum_{i \geq 2} b_i \binom{-1}{i-2} = \sum_{i \geq 2} (-1)^i b_i.$$

We know that $\chi(\Delta(P)) = \sum_{i \geq 0}(-1)^i f_i(\Delta(P))$; where $f_i(\Delta(P))$ is the number of i-dimensional faces of $(\Delta(P))$. Clearly, $f_i(\Delta(P)) = b_{i+2}$. Hence, $Z(P, 1) = (\Delta(P))$.

If P has a $\hat{0}$ and $\hat{1}$, then the number of multichains $x_1 \leq x_2 \leq ..... \leq x_{n-1}$ is same as the number of multichains $\hat{0} \leq x_1 \leq x_2 \leq ..... \leq x_{n-1} \leq \hat{1}$. Thus, for $n \geq 2$, $Z(P, n) = \zeta^n(\hat{0}, \hat{1})$. It can be shown that $\zeta^n(\hat{0}, \hat{1})$ is a polynomial function in n and hence the equality $Z(P, n) = \zeta^n(\hat{0}, \hat{1})$ holds for all $n \in \mathbb{Z}$. Since $\zeta^{-1} = \mu$, we see that

$$Z(P, -1) = \zeta^{-1}(\hat{0}, \hat{1}) = \mu(\hat{0}, \hat{1}).$$

□

Remark 7.3.4. Since $Z(P, -1) = \mu(\hat{0}, \hat{1})$ for a poset P with $\hat{0}$ and $\hat{1}$, the zeta polynomial $Z(P, n)$ of a poset can be used to calculate the Möbius function. For $P = B_d$, we see that $Z(B_d, n) = n^d$. Hence, $\mu_{B_d}(\hat{0}, \hat{1}) = Z(B_d, -1) = (-1)^d$, as deduced earlier.

Bibliography

[Aig79] Martin Aigner, *Combinatorial Theory* , 1979.

[Bir67] Garrett Birkhoff, *Lattice Theory*, 3rd ed., American Math. Soc., Providence, R.I., 1967.

[Bly05] T.S. Blyth, *Lattices and Ordered Algebraic Structures*, Springer, 2005.

[Far79] F. D. Farmer, *Cellular homology for posets*, Math. Japonica 23 (1979), 607-613.

[Grä71] George Grätzer , *Lattice Theory: First Concepts and Distributive Lattices*, 1971.

[Grä78] George Grätzer , *General Lattice Theory*, Academic Press, New York, 1978.

[Hal36] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. 7 (1936), 134-151.

[Koz07] Dmitry Kozlov, *Combinatorial Algebraic Topology*, Algorithms and Computations in Mathematics, Volume 21, (2007) Springer.

[KRY09] Joseph P. S. Kung, Gian-Carlo Rota, and Catherine H. Yan 2009, *Combinatorics: The Rota Way.*

[Rom08] Steven Roman, *Lattices and Ordered Sets*, Springer, 2008.

[Rot64] Gian-Carlo Rota, *On the Foundations of Combinatorial Theory I. Theory of Möbius Functions*, Z. Wahrseheinlichkeitstheorie 2 (1964), 340-368.

[RW99] Kenneth A. Ross, Charles R. B. Wright, *Discrete Mathematics*, Fourth Edition, 1999.

[Sta74] R. Stanley, *Combinatorial Reciprocity Theorems*, Advances in Math. 14 (1974), 194-253.

[Sta97] Richard P. Stanley, *Enumerative Combinatorics*, Volume I, Cambridge University Press 1997.