THE LATTICE OF SUBGROUPS OF FINITE GROUPS

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF ARTS

IN THE GRADUATE SCHOOL OF THE

TEXAS WOMAN'S UNIVERSITY

COLLEGE OF NATURAL AND SOCIAL SCIENCES

BY

AWAD RASRAS

DENTON, TEXAS

DECEMBER 1982

TABLE OF CONTENTS

PREFACE

Lattice theory is a new branch of mathematics. Its concepts and methods have fundamental applications in various areas of mathematics (e.g. diverse disciplines of abstract algebra, mathematical logic, affine geometry, set and measure theory, and topology).

Most of the pioneer work was done by G. Birkhoff [5], who most deserves the title of "Father of Lattice Theory" and who has played a central role in most of its developments since the early thirties. His first papers in 1933-35 began a development which took lattice theory from a relatively obscure beginning and started it on a historical path which has led it to become a major branch of mathematics today.

The main purpose of this thesis is to examine the lattice of the set of subgroups of groups and to determine whether certain lattices are distributive, modular, complemented, or Boolean.

CHAPTER I

SOME PRELIMINARY CONCEPTS

The reader is assumed to be familiar with basic concepts of set theory and groups. However, we now give a brief summary of various concepts.

Sets. Given a set A and an object p, either p is an element of A (notation: $p \in A$) or p is not an element of A (notation: $p \notin A$). If every p that is an element of a set B is also an element of a set A, then B is called a subset of A (notation: $B \subset A$). If $B \subset A$ and $A \subset B$, then $A = B$.

Let A and B be given sets. The set of elements which belong to both A and B is called the intersection of A and B. It will be denoted by $A \cap B$. Also, the set of all elements which belong to A alone or to B alone or to both A and B is called the union of A and B. It will be denoted by $A \cup B$. The operations "$\cap$" and "$\cup$" satisfy the following properties:

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

These are the commutative, associative, and distributive laws, respectively.

The set containing no elements is called the null set, and is denoted by $\emptyset$. It follows that $\emptyset \subset A$ for every set A.

The following laws of de Morgan are often useful:

$$(A \cup B)' = A' \cap B', \quad (A \cap B)' = A' \cup B'.$$

By A' we mean the complement of A, i.e. the set of all elements in I (Universal set) which are not elements of A.

The Cartesian Product. Suppose A and B are two sets. The Cartesian Product of A and B, denoted by A X B, is $\{(a,b): a \in A \text{ and } b \in B\}$. If two sets are the same, then the Cartesian Product is A X A.

Relations. A subset R of A X A is called a relation on the set A. A relation is called reflexive if $(a,a) \in R$ for all $a \in A$; symmetric if $(a,b) \in R$ implies $(b,a) \in R$; transitive if $(a,b) \in R$ and $(b,c) \in R$ imply $(a,c) \in R$; and antisymmetric if $(a,b) \in R$ and $(b,a) \in R$ imply $a = b$.

Functions. A function f is a subset of A X B that satisfies the condition $(a,b) \in f$, $(a,c) \in f$ implies $b = c$. It means that if a is a first element of an ordered pair in f, then the corresponding second element is uniquely determined and is denoted by f(a). It is convenient to employ

the notation "f: A → B". If the set of second elements occurring in the ordered pairs of f is exactly B, we say f is an onto function. A function f is called one to one (1:1) if it satisfies: $(a,b) \in f$ and $(c,b) \in f$ implies $a = c$.

A function f: $A \times A \to A$ is called a binary operation on A. We write $((a,b),c) \in f$, for a, b, c in A. In general, it is more convenient to denote a binary operation by one of the symbols $*, \oplus, \cdot, \ldots$ So that $a * b = c$.

Groups. A group is a pair $(G,*)$ consisting of a nonempty set G and a binary operation $*$ defined on G, such that the following properties are satisfied.

1. Associativity. If a, b, and c are in G, then $(a * b) * c = a * (b * c)$.

2. Identity. There exists a unique element, e, in G (called the identity element) such that for all $a \in G$, $a * e = e * a = a$.

3. Inverse. For every a in G there exists a unique element a^{-1} in G, called the inverse of a, such that $a^{-1} * a = a * a^{-1} = e$. A group $(G,*)$ is called abelian if for every a and b in G, $a * b = b * a$.

Subgroups. A collection of elements H in G is said to be a subgroup of G if H forms a group relative to the

binary operation defined in G. For example, the set of even integers forms a subgroup of the set of integers with respect to addition.

Cyclic Group. A group G is called cyclic if, for some $a \in G$, every $x \in G$ is of the form a^m, where $m \in Z$ (Z = the set of all integers). The element a is then called a generator of G. For example, the additive group Z is cyclic with generator a = 1 since, for every $m \in Z$, $a^m = ma = m$.

Homomorphisms. Let $(G,*)$ and $(G',\circ)$ be two groups, not necessarily distinct. A mapping, M, is a set of ordered pairs (x,y), such that when $(x,y), (x,z) \in M$, $y = z$. A homomorphism from $(G,*)$ into $(G',\circ)$ is a mapping $f: G \to G'$ such that $f(a * b) = f(a) \circ f(b)$, for arbitrary $a, b \in G$.

If, in addition, f is one-to-one and onto, then f is said to be an isomorphism.

Cosets. Let G be a finite group with the group operation $\circ$, H be a subgroup of G, and a be an arbitrary element of G. We define as the right coset Ha of H in G, the subset of G

$$Ha = \{h \circ a: \quad h \in H\}$$

and as the left coset aH of H in G, the subset of G

$$aH = \{a \circ h: \quad h \in H\}$$

Normal Subgroup. A subgroup H of a group G is called a normal subgroup if for all a in G, $a^{-1}Ha = H$.

The following theorems will be helpful in our work; they can be found in Barnes [3] and will be stated without proofs.

1. A nonempty set H in G is a subgroup of G if when a, b are in H, then ab^{-1} is also in H.

2. If G is a finite group of order n and H is a subgroup of order r, then r divides n.

3. Every subgroup of a cyclic group is cyclic.

4. If H and K are normal subgroups of the finite group G, then HK = KH is a normal subgroup.

5. The intersection of any two normal subgroups of a group G is also a normal subgroup of G.

CHAPTER II

LATTICES

Partial Ordering. A binary relation on a set S is called a partial ordering of S when it is reflexive, antisymmetric, and transitive; such relations are commonly indicated by using the special relation symbol $\leq$. The hypotheses for a partial ordering may be written as follows:

P_1. $x \leq x$ for all $x \in S$

P_2. $x \leq y$ and $y \leq x$ imply $x = y$

P_3. $x \leq y$ and $y \leq z$ imply $x \leq z$.

Example 1. The relation "is a divisor of", written m/n, is a partial ordering of the set of positive integers.

Example 2. For any set U, the relation "is a subset of", written $S \subset T$, is another partial ordering of the power set $\mathcal{P}(U)$ of all subsets of U.

Definition 1. A partially ordered set, or poset, is a pair $[S,\leq]$, where $\leq$ is a partial ordering of S.

The converse of any partial ordering $\leq$ is again a partial ordering, called the dual of $\leq$ and denoted $\geq$. Thus, $x \geq y$ if $y \leq x$. Also, posets having only a few elements can be visualized in terms of their diagrams. These

diagrams can be drawn by using small circles to signify elements and drawing a rising line from each element to each next larger element. Thus, Figure 1 shows the power set of all subsets of A = {1, 2, 3} partially ordered by the inclusion relation; Figure 2 diagrams the poset [{2, 3, 5, 7, 14, 15, 21}, |].

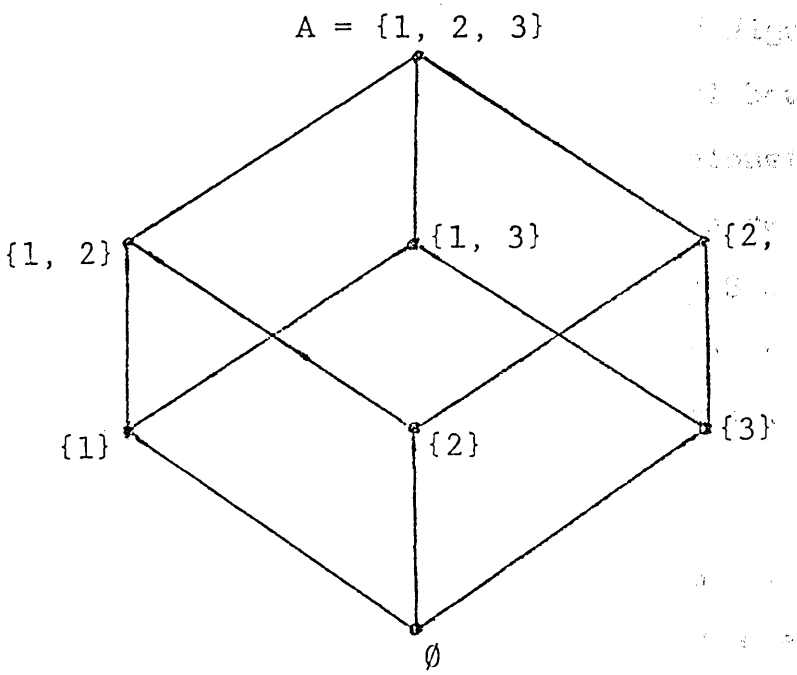

Figure 1

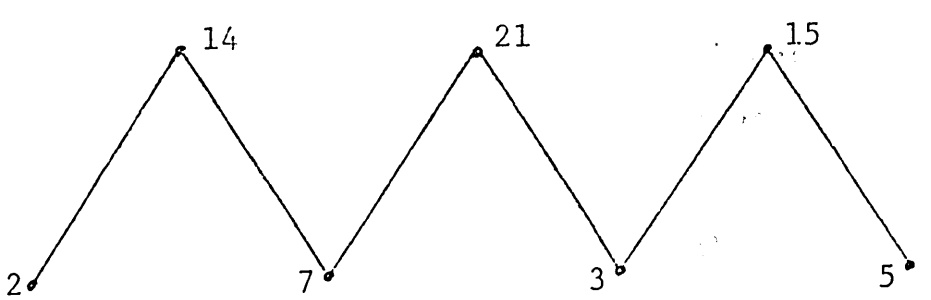

Figure 2

Duality Principle. From the fact that the converse of any partial ordering of a set S is itself a partial ordering, it follows that we can replace the relation $\leq$ in any theorem about posets by the relation $\geq$ without affecting its truth. This is called the duality principle of the theory of posets.

In the poset $[\mathcal{P}(\{1, 2, 3\}), \subset]$ of Figure 1, the elements $\emptyset$ and $A = \{1, 2, 3\}$ are universal bounds, in the sense that $\emptyset \leq x \leq A$ for any element x belonging to $\mathcal{P}(A)$ (the power set of A). This concept can be defined in any poset $P = [S, \leq]$; the elements 0 and I of S are universal bounds of P (in detail, 0 is called the least element and I the greatest element of P) when $0 \leq x$ and $x \leq I$ for any element $x \in S$.

Lemma 1. A given poset $[S, \leq]$ can have at most one least element and at most one greatest element.

Proof. Let 0 and 0* both be universal lower bounds of $[S, \leq]$, then $0 \leq 0^*$ (since 0 is a universal lower bound), and $0^* \leq 0$ (since 0* is also a universal lower bound). Hence, by P_2, antisymmetric property, $0 = 0^*$. The proof for I is similar.

Posets need not have any universal bounds. Thus, under the usual relation of inequality, the real numbers form a poset $[R, \leq]$ which has no universal bounds.

Greatest Lower and Least Upper Bounds. Given a subset S of a poset P, define $a \in P$ to be a lower bound of S when $a \leq x$ for all $x \in S$, and define a to be an upper bound of S when $a \geq x$ for all $x \in S$. Define $b \in P$ to be the greatest lower bound of S when (i) b is a lower bound of S and (ii) $b \geq b^*$ for any other lower bound b^* of S. In this event, we write $b = \text{glb } S$. Dually, define $c \in P$ to be the least upper bound of S when (i) $c \geq x$ for all $x \in S$ and (ii) $c \leq c^*$ for any other upper bound c^* of S. We write $c = \text{lub } S$.

Lemma 2. A subset S of a poset P can have at most one glb and at most one lub.

Proof. If b_1 and b_2 are both glbs of S, then $b_1 \leq b_2$, because b_1 is a lower bound and b_2 is a greatest lower bound, and $b_2 \leq b_1$ because b_2 is a lower bound and $b_1 = \text{glb } S$, that is, $b_1 \leq b_2$ and $b_2 \leq b_1$. Hence, by P_2 (antisymmetric property) we conclude that $b_1 = b_2$. The proof that lub S is unique is similar to the above.

Definition 2. A lattice is a poset in which any two elements a and b have a glb called the meet, $a \wedge b$, and a lub called the join, $a \vee b$.

Example 3. The set {a, b, c, d, e, f} is not a lattice with respect to the partial order pictured in Figure 3, because {a, b} has no join (lub).

Example 4. The set {x, y, z, k, g} is a lattice with respect to the partial order pictured in Figure 4, because any two elements belonging to the set have a join and a meet, i.e.:

$$x \wedge k = x, \quad x \vee k = k$$

$$z \wedge y = x, \quad z \vee y = g$$

$$y \wedge k = x, \quad y \vee k = g.$$

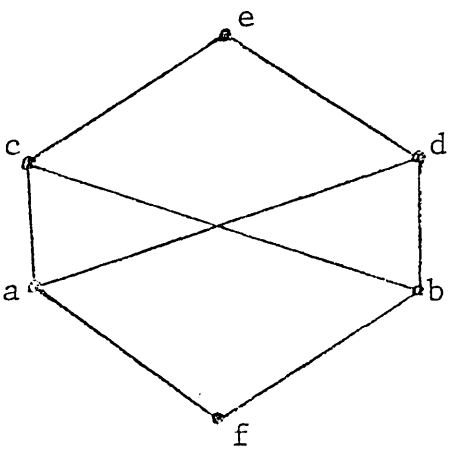

Figure 3

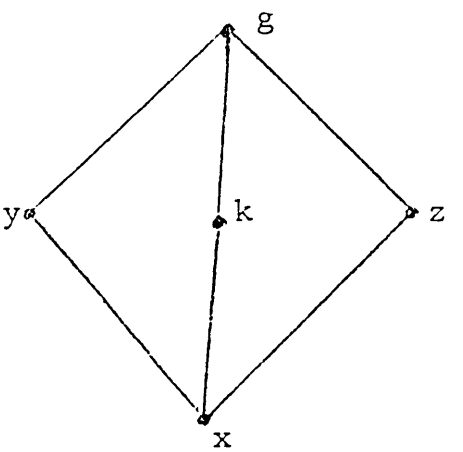

Figure 4

Theorem 1. For any elements a, b, c of a lattice $(L,\leq)$:

1. $a \wedge a = a$ and $a \vee a = a$ (idempotence)
2. $a \wedge b = b \wedge a$ and $a \vee b = b \vee a$ (commutativity)
3. $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and $a \vee (b \vee c) = (a \vee b) \vee c$ (associativity)
4. $a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$ (absorption)

Proof. By the duality principle, which interchanges $\wedge$ and $\vee$, it suffices to prove one of the two identities in each of 1 - 4; we shall prove the first.

1. By P_1, (reflexivity), $a \leq a$, while trivially, $d \in L$, $d \leq a$ and $d \leq a$ imply $d \leq a$, hence $a = a \wedge a$.

2. $a \wedge b = \text{glb}\{a, b\} = \text{glb}\{b, a\} = b \wedge a$.

3. Set $d_1 = a \wedge (b \wedge c)$ and $d_2 = \text{glb}(a, b, c)$. Then $d_1 \leq a$, $d_1 \leq b$, $d_1 \leq c$. Hence $d_1 \leq d_2$. On the other hand, $d_2 \leq (b \wedge c)$, $d_2 \leq a$. Hence $d_2 \leq d_1$. It follows from the antisymmetric property of $\leq$ that $d_1 = d_2$. By similar argument, we could complete the proof of the associativity of $\wedge$ [9, p. 7].

4. Clearly $a \leq a$ and $a \leq a \vee b$. Hence by definition of glb, $a \leq a \wedge (a \vee b)$. But $a \wedge (a \vee b) \leq a$ therefore $a \wedge (a \vee b) = a$. Similarly, $a \vee (a \wedge b) = a$.

Theorem 2. A lattice is a set L of elements which satisfies the four properties in Theorem 1.

Proof. We already know, by Theorem 2, that any lattice satisfies the above properties. Conversely, assume that $(L, \wedge, \vee)$ is a structure satisfying 1 - 4 of Theorem 1. Define $a \leq b$ by $a \wedge b = a$. Notice that if $a \leq b$, then $b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$. Now we shall show that $(L, \leq)$ is a poset.

1. Let $a \in L$. $a \wedge a = a \leftrightarrow a \leq a$, by using property 1 in Theorem 2 so $\leq$ is reflexive.

2. Let $a, b \in L$. $a \leq b \leftrightarrow a \wedge b = a$, $b \leq a \leftrightarrow b \wedge a = b$. By using property 2 in Theorem 1, we conclude $a = a \wedge b = b \wedge a = b$, so $\leq$ is antisymmetric.

3. Let $a, b, c \in L$. $a \leq b \leftrightarrow a \wedge b = a$, $b \leq c \leftrightarrow b \wedge c = b$, $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$. So, $\leq$ is transitive, and $(L, \leq)$ is a poset.

Now we need to show if $x, y \in L$, then $x \wedge y$ is the glb and $x \vee y$ is the lub of $\{x, y\}$. In other words we need to show $x \wedge y \leq x$ and $x \wedge y \leq y$, and if $z \leq x$ and $z \leq y$ then $z \leq x \wedge y$. $(x \wedge y) \wedge x = x \wedge (y \wedge x) = x \wedge (x \wedge y) = (x \wedge x) \wedge y = x \wedge y$, so $x \wedge y \leq x$. $(x \wedge y) \wedge y = x \wedge (y \wedge y) = x \wedge y$, so $x \wedge y \leq y$. Hence, $x \wedge y$ is a lower bound of $\{x, y\}$.

To show that $x \wedge y$ is the glb $\{x, y\}$, assume $z \leq x$ and $z \leq y$ for some $z \in L$. Now, $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$, so $z \leq x \wedge y$, and $x \wedge y$ is glb $\{x, y\}$. In a similar way we could show that $x \vee y$ is the lub $\{x, y\}$.

Sublattices. A nonempty subset S of a lattice L, $S \subset L$, is called a sublattice if $a, b \in S$ implies $a \wedge b \in S$ and $a \vee b \in S$. In the lattice which is pictured in Figure 4 (Example 4), the subset $S = \{k\}$ is a sublattice, i.e., $k \wedge k = k$ and $k \vee k = k$. Also $S' = \{x, y\}$ is a sublattice, i.e., $x \wedge y = x$ and $x \vee y = y$.

Example 5. The set $L = \{A, B, C, D, E\}$ is a lattice with respect to the partial order pictured in Figure 5. But the set $\{A, B, C, E\}$ is not a sublattice because $B \wedge C = D$, which is an element in L, but not in $\{A, B, C, E\}$. However, $\{A, B, C, E\}$ is a partially ordered set and a lattice.

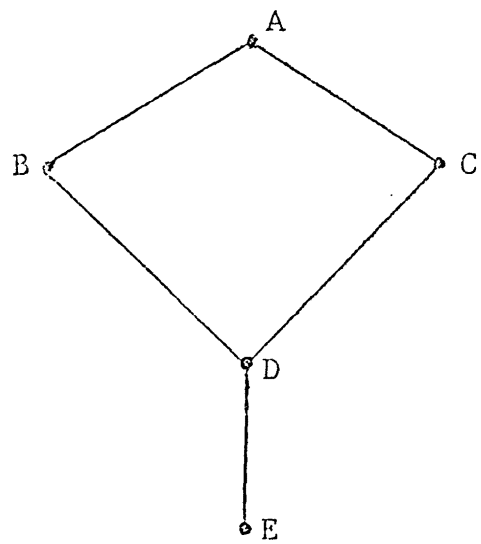

Figure 5

Definition 3. A lattice L is called distributive if the operations $\wedge$ and $\vee$ satisfy the distributive law $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Theorem 3. In a distributive lattice the law $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ is also valid.

Proof. $(a \wedge b) \vee (a \wedge c)$

$= [(a \wedge b) \vee a] \wedge [(a \wedge b) \vee c]$

$= a \wedge [(a \wedge b) \vee c]$

$= a \wedge [(a \vee c) \wedge (b \vee c)]$

$= [a \wedge (a \vee c)] \wedge (b \vee c)$

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

Definition 4. A complement of an element a in a lattice L with universal bounds 0, I is an element $x \in L$ such that $a \wedge x = 0$ and $a \vee x = I$.

Lemma 3. In any distributive lattice the set of all complemented elements is a sublattice.

Proof. Let a, a' and b, b' be complementary pairs, then $(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = 0 \vee 0 = 0$. $(a \wedge b) \vee (a' \vee b') = (a \vee a' \vee b') \wedge (b \vee a' \vee b') = I \wedge I = I$. Hence, $a \wedge b$ and $a' \vee b'$ are complementary. A similar arguement shows that $a \vee b$, $a' \wedge b'$ are complementary.

Definition 5. A complemented lattice is a lattice with universal bounds 0 and I in which every element a has at least one complement x with $a \wedge x = 0$, and $a \vee x = I$.

Definition 6. A Boolean lattice is a lattice which is both complemented and distributive.

Definition 7. A lattice L is called modular if it satisfies the following: if $a \leq c$, then $a \vee (b \wedge c) = (a \vee b) \wedge c$.

Theorem 4. Every distributive lattice is a modular lattice.

Proof. Suppose x, y and z are in the distributive lattice L, such that $x \leq z$. Then, by the definition of distributive lattice, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, but $x \leq z \rightarrow x \wedge z = x$ and $x \vee z = z$. Thus, $x \vee (y \wedge z) = (x \vee y) \wedge z$. So L is modular.

CHAPTER III

THE LATTICE OF SUBGROUPS OF FINITE GROUPS

Suppose G is a group with respect to the binary operation $*$. Let L(G) denote the set of all subgroups S, T, ... of G; define $S \leq T$ to mean $S \subseteq T$. Clearly L(G) is a poset. Moreover, the intersection $S \cap T$ of any two subgroups S and T of G is itself a subgroup of G which contains every subgroup contained in both S and T. Therefore, $S \cap T = \text{glb}\{S, T\} = S \wedge T$ in the poset L(G). The set $\{s_1t_1s_2t_2 \ldots s_kt_k$: $s_1, \ldots, s_k \in S$ and $t_1, \ldots, t_k \in T$, $k \in$ Set of all positive integers$\}$ is a subgroup of G which is contained in every subgroup of G containing both S and T. Hence this set is the lub of S and T in the poset L(G) and may be written as $S \vee T = \text{lub}\{S, T\}$. This proves that the poset L(G) is a lattice [4. p. 258].

Example 6. As a first example we will consider the group of symmetries of the square. The elements of this group G are taken to be certain rigid motions of the square, that is, displacements throughout which the shape of the square is unaltered. Permitted motions are the following: the identity motion e in which the square remains fixed; clockwise rotations r_1, r_2, and r_3 about

the center, through angles of 90, 180, and 270 degrees, respectively; reflections h and v about horizontal and vertical lines through the center; reflections d_1 and d_2 about the diagonal lines.

Two such motions can be "multiplied" by performing them in succession. If x and y are motions, then x * y is to be interpreted as the motion that achieves the same result as y followed by x. For example, h * r_1 is that element of G which has the same net effect as r_1 followed by h, we see that h * r_1 produces the same result as the single motion d_2; hence h * r_1 = d_2. The complete multiplication table for (G,*) appears below.

*	e	r_1	r_2	r_3	h	v	d_1	d_2
e	e	r_1	r_2	r_3	h	v	d_1	d_2
r_1	r_1	r_2	r_3	e	d_1	d_2	v	h
r_2	r_2	r_3	e	r_1	v	h	d_2	d_1
r_3	r_3	e	r_1	r_2	d_2	d_1	h	v
h	h	d_2	v	d_1	e	r_2	r_3	r_1
v	v	d_1	h	d_2	r_2	e	r_1	r_3
d_1	d_1	h	d_2	v	r_1	r_3	e	r_2
d_2	d_2	v	d_1	h	r_3	r_1	r_2	e

Table 1

Let L(G) denote the set of all subgroups of G.

L(G) = {{e}, {e, r_2}, {e, h}, {e, v}, {e, d_1}, {e, d_2}, {e, r_1, r_2, r_3}, {e, r_2, h, v}, {e, r_2, d_1, d_2}, G}.

Clearly L(G) is a lattice. A diagram for this lattice is pictured in Figure 6.

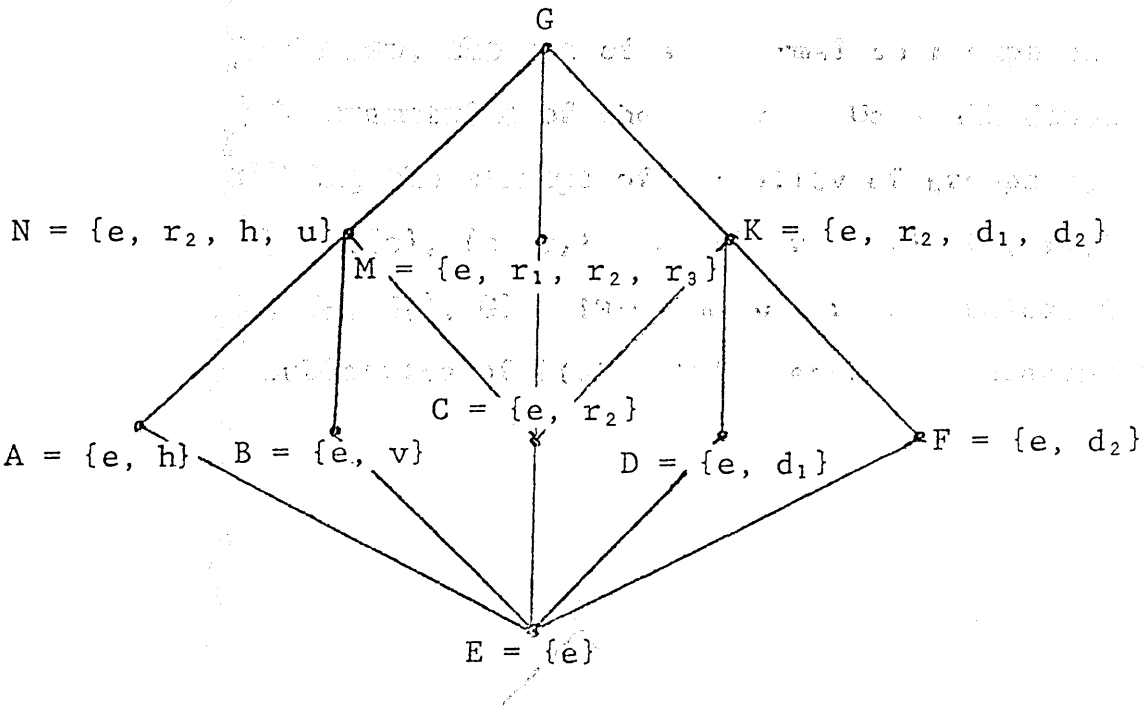

Figure 6

Consider the elements $B = \{e, v\}$, $C = \{e, r_2\}$, and $F = \{e, d_2\}$ of L(G). $C \wedge (F \vee B) = C \wedge G = C$, but $(C \wedge F) \vee (C \wedge B) = E \vee E = E$, so L(G) is not a distributive lattice. Consider again the elements B, D, and N of L(G). We notice that L(G) is not a modular lattice, since while $B \leq N$, $B \vee (D \wedge N) = B \vee E = B$, but $(B \vee D) \wedge N = G \wedge N = N$, which means that $B \vee (D \wedge N) \neq (B \vee D) \wedge N$. Also, we notice that $C \in L(G)$ doesn't have a complement, so L(G) is not a complemented lattice. Notice that B has

a complement D, since $B \wedge D = E = \{e\}$, and $B \vee D = G$; M has a complement A, since $M \wedge A = E = \{e\}$, and $M \vee A = G$. Moreover, L(G) is not a Boolean lattice since it is neither complemented nor distributive.

Consider now, the set of all normal subgroups of G, the group of symmetries of the square. We shall denote it by M(G). Using the concept of normality of groups we find that $M(G) = \{\{e\}, \{e, r_2\}, \{e, r_1, r_2, r_3\}, \{e, r_2, v, h\}, \{e, r_2, d_1, d_2\}, G\}$. $[M(G), \wedge, \vee]$ is a lattice, in fact it is a sublattice of L(G). This lattice is diagramed in Figure 7.

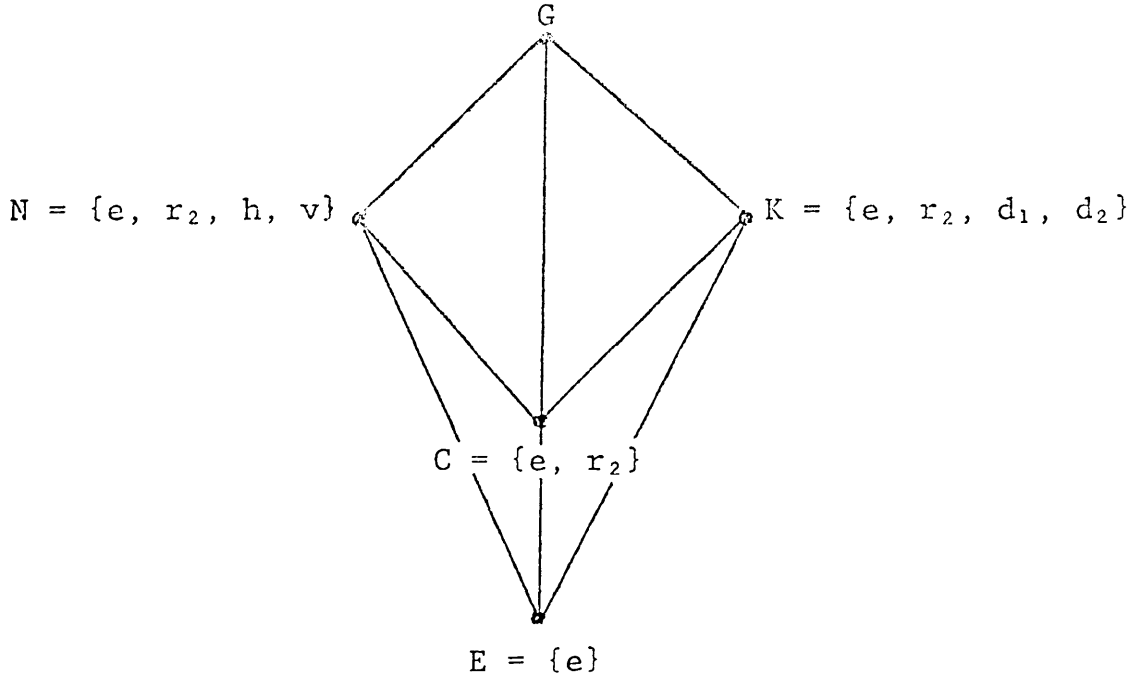

Figure 7

The lattice M(G) is not distributive, since if we consider the elements M, N, and K of M(G), we could find out that the distributive law is not satisfied, i.e., $M \vee (K \wedge N) = M \vee C = M$, but $(M \vee K) \wedge (M \vee N) = G \wedge G = G$. Easy verification shows that $[M(G), \wedge, \vee]$ is a modular lattice. In fact, we will prove later in this chapter that the set of all normal subgroups of any group forms a modular lattice. Also, the set of all normal subgroups does not form a complemented lattice, since $C \in M(G)$, has no complement; it is not a Boolean lattice since it is neither distributive nor complemented.

Example 7. Consider Z_{12}, the group of integers module 12 with respect to the binary operation addition. This group is generated by 1, 5, 7, or 11. So Z_{12} is a cyclic group. By Theorem 2 at the end of Chapter I, we notice that all subgroups are cyclic, so they are abelian, hence, normal subgroups. $L(G) = \{\{\overline{0}\}, \{\overline{0}, \overline{6}\}, \{\overline{0}, \overline{4}, \overline{8}\}, \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}, \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}, G = Z_{12}\}$. The diagram for this lattice is shown in Figure 8.

If we consider any three elements of L(G), we could easily show that they satisfy the distributive laws. For example C, D, and F belong to L(G). $C \wedge (D \vee F) = C \wedge G = C$ and $(C \wedge D) \vee (C \wedge F) = E \vee C = C$. L(G) is a distributive lattice. In fact, we will prove that the set of all subgroups of a cyclic group forms a distributive lattice.

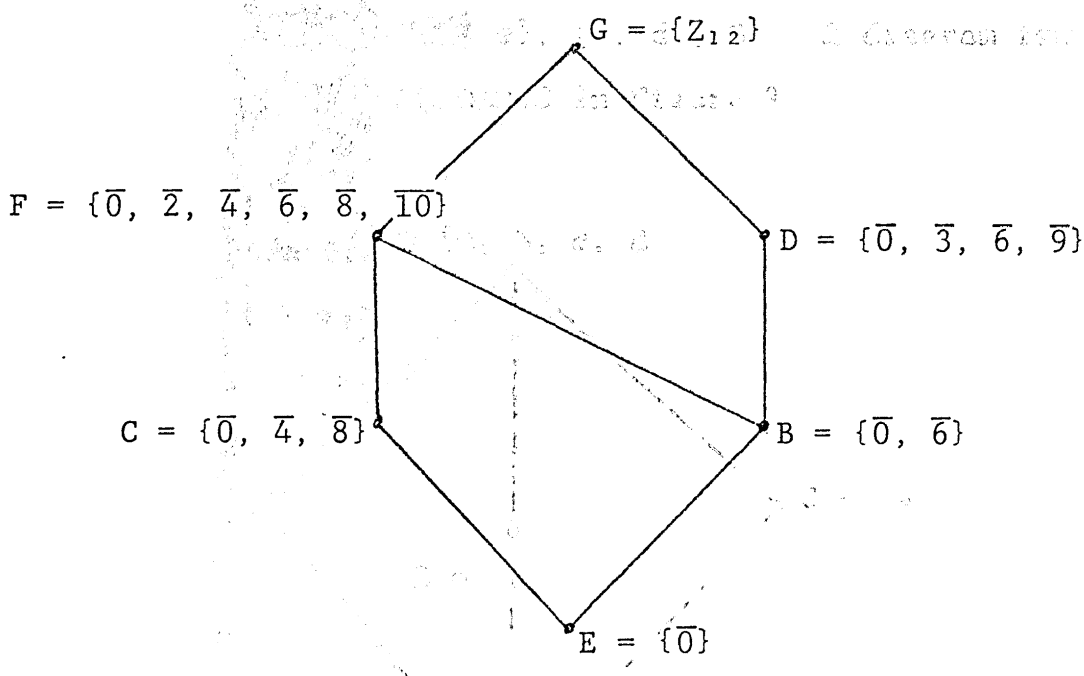

Figure 8

By Theorem 4 we conclude that L(C) is a modular lattice. Also, L(G) is not a complemented lattice since the element B = {0̄, 6̄} has no complement in L(C); it is not a Boolean lattice because it is not complemented.

Example 8. Consider the group G = {a, b, c, d} with the following operation table:

∘	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Table 2

This group is abelian. The set of all subgroups is $L(G) = \{\{a\}, \{a, b\}, \{a, c\}, \{a, d\}, G\}$. A diagram for the lattice L(G) is pictured in Figure 9.

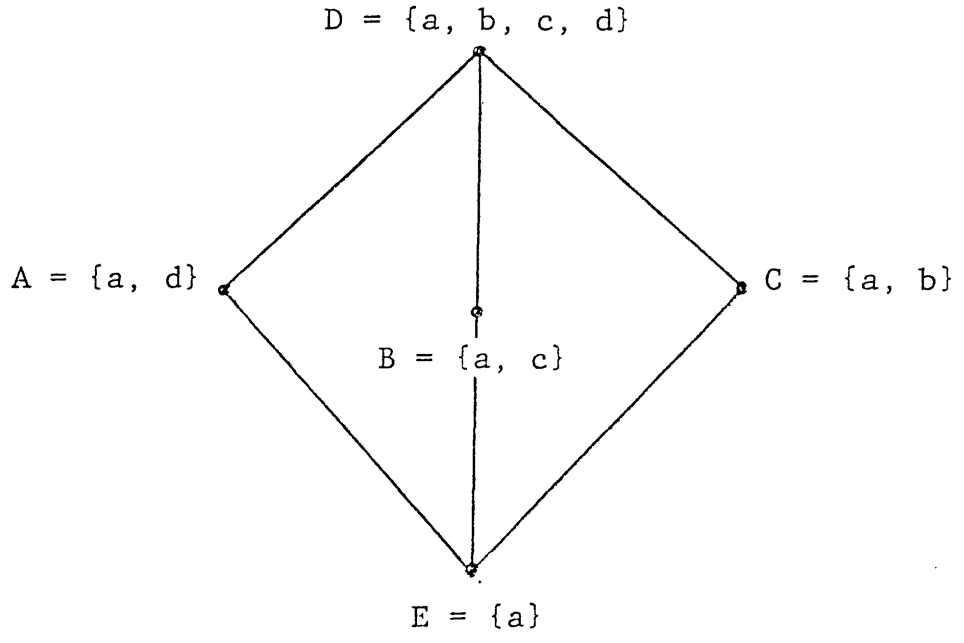

Figure 9

Now, consider the elements A, B, and C of L(G). We notice that the distributive law does not hold since, $A \wedge (B \vee C) = A \wedge D = A$ but, $(A \wedge B) \vee (A \wedge C) = E \vee E = E$. L(G) is a modular lattice since for any three elements A, B, and D such that $A \leq D \rightarrow A \vee (B \wedge D) = (A \vee B) \wedge D$. L(G) is a complemented lattice. Also, it is not a Boolean lattice since it is not distributive.

Theorem 5. If H and K are normal subgroups of the group G, Then $H \vee K = HK$.

Proof. Recall that $H \vee K = \{h_1k_1h_2k_2 \ldots h_tk_t : h_t \in H \text{ and } k_t \in K\}$. Clearly $HK \subseteq H \vee K$. Let $x \in H \vee K$. By using mathematical induction we will show that $x \in HK$. Suppose $x = h_1k_1h_2k_2 \ldots h_nk_n$ for some positive integer n. For $n = 1$, $x = h_1k_1$ which is an element of HK. Assume that all the products of length n are in HK, we need to show that all the products of length $n + 1$ are in HK too. Suppose $x = h_1k_1h_2k_2 \ldots h_nk_nh_{n+1}k_{n+1}$, for some positive integer n. Since all the products of length n are in HK, we could write $x = hkh_{n+1}k_{n+1}$. Then $x = hk(k^{-1}h'k)k_{n+1}$, since H is a normal subgroup, and $x = hh'kk_{n+1} = h''k'$ which is an element of HK. So $x \in HK$ and the proof is complete.

Theorem 6. The set of all normal subgroups of a group G forms a modular lattice.

Proof. Let L(G) denote the set of all subgroups of G; and let $H \leq K$ mean that $H \subset K$. Let M(G) denote the set of all normal subgroups of G. We showed at the begining of this chapter that $H \wedge K = H \cap K = \text{glb } \{H, K\}$ and $H \vee K = \{h_1k_1h_2k_2 \ldots h_tk_t : h_t \in H \text{ and } k_t \in K\} = \text{lub } \{H, K\}$. Using the theorems which are written at the end of Chapter I and Theorem 5, we would say that $H \wedge K$,

and $H \vee K = HK$ are normal subgroups, which proves that M(G) is a lattice. Also, M(G) is a sublattice of L(G).

To show that M(G) is a modular lattice, we need to prove that if H, K, and F are normal subgroups, of G then: if $H \leq F$ then $H \vee (K \wedge F) = (H \vee K) \wedge F$. We will show first that $H \vee (K \wedge F) \subseteq (H \vee K) \wedge F$. $H \subseteq H \vee K$ and $H \subseteq F$ (given) implies $H \subseteq (H \vee K) \wedge F$ and $K \wedge F \subseteq F$ and $K \wedge F \subseteq K \subseteq H \vee K$, this implies $K \wedge F \subseteq (H \vee K) \wedge F$.

So $H \vee (K \wedge F) \subseteq (H \vee K) \wedge F$.

To show that $(H \vee K) \wedge F \subseteq H \vee (K \wedge F)$, take $x \in (H \vee K) \wedge F$. So $x \in H \vee K$, and $x \in F$. This means that $x = hk$ and $x = f$ (notice that $H \vee K = HK$, since H and K are normal subgroups of G). So $hk = f$, $k = h^{-1}f$ for $h \in H$, $k \in K$, and $f \in F$. Since $h \in F$($H \subseteq F$ is given), $h^{-1} \in F$ and $h^{-1}f \in F$. So $k \in F$ and $k \in K \wedge F$. So $x = hk \in H \vee (K \wedge F)$ and this completes the proof.

Theorem 7. The lattice L(G) of all subgroups of a cyclic group G forms a distributive lattice.

Proof. Let G be a cyclic group; let A, B, and C be subgroups of G (they are cyclic since G is cyclic). L(G) is distributive if $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$. We shall show first that $(A \wedge B) \vee (A \wedge C) \subseteq A \wedge (B \vee C)$. $A \wedge B \subseteq A$ and $A \wedge B \subseteq B \vee C$, so $A \wedge B \subseteq A \wedge (B \vee C)$. $A \wedge C \subseteq A$ and $A \wedge C \subseteq B \vee C$, so $A \wedge C \subseteq A \wedge (B \vee C)$ which

implies that $(A \wedge B) \vee (A \wedge C) \subseteq A \wedge (B \vee C)$.

To show that $A \wedge (B \vee C) \subseteq (A \wedge B) \vee (A \wedge C)$, suppose $x \in A \wedge (B \vee C)$. It means that $x \in A$ and $x \in B \vee C$. So $x = a$, $x = bc$ for some $a \in A$, $b \in B$, and $c \in C$. This implies that $a = bc$. Since A, B, and C are cyclic subgroups, b and c can be represented as power of a generator $d \in G$. $b = d^m$, $c = d^n$, hence $a = d^{m+n}$. If $m' = \text{lcm}\{m, m+n\} = [m, m+n]$, and $n' = \text{lcm}\{n, m+n\} = [n, m+n]$, then clearly $d^{m'} \in A \wedge B$ and $d^{n'} \in A \wedge C$. If $h = \gcd\{m', n'\} = (m', n')$, then $d^h \in (A \wedge B) \vee (A \wedge C)$. But from number theory, $h = (m', n') = ([m, m+n], [n, m+n]) = [(m,n), m+n] = m+n$.
So $d^{m+n} \in (A \wedge B) \vee (A \wedge C) \leftrightarrow a \in (A \wedge B) \vee (A \wedge C)$.
So, $x \in (A \wedge B) \vee (A \wedge C)$, and the proof is complete [5, p. 96].

We will end this chapter by summarizing all the work that we have already done in the following table. Notice that the + means the property is always true; -- means it is not necessarily true.

Although all the examples, which are used, involve finite groups, the proofs, do not depend on the finite property. So all results are valid for lattices of subgroups of any group.

Lattice of / Lattice Property	All Subgroups of a Group G	All Normal Subgroups of a Group G	All Subgroups of a Cyclic Group G	All Subgroups of a Abelian Group G
Sublattice	+	+	+	+
Distributive	--	--	+	--
Modular	--	+	+	+
Complemented	--	--	--	--
Boolean	--	--	--	--

Table 3

BIBLIOGRAPHY

1. J. C. Abbott, Trends in Lattice Theory. New York: Van Nostrand and Reinhold Company, 1970.
2. American Mathematical Society. Lattice Theory. Providence, Rhode Island: American Mathematical Society, 1960.
3. Wilfred E. Barnes. Introduction to Abstract Algebra. Boston, Mass.: D. C. Health and Company, 1963.
4. Garrett Birkhoff, and Thomas Bartee. Modern Applied Algebra. New York: McGraw-Hill Book Company, 1970.
5. Garrett Birkhoff. Lattice Theory. Providence, Rhode Island: Mathematical Society, 1948.
6. George Gratzer. Lattice Theory. San Francisco: Witt, Freeman and Company, 1971.
7. K. A. Hirsch. The Theory of Groups. New York: Chelsea Publishing Company, 1960.
8. D. E. Rutherford. Introduction to Lattice Theory. New York: Hafner Publishing Company, 1965.
9. Wolfgang J. Thron. Topological Structures. New York: Rinehart and Winston, Inc., 1966.