LATTICE AUTOMORPHISMS

Thesis by

Sherwin P. Avann

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

California Institute of Technology

Pasadena, California

1940

TABLE OF CONTENTS

I

Introduction

II

The Group of Automorphisms of a Lattice

III

Supplementary Results

I

Introduction

1. Summary. The subject of lattice automorphisms has been introduced by G. Birkhoff in his paper "On the Structure of Abstract Algebras" (Birkhoff [3]). In this paper the subject has been pursued further. Among the results are a necessary and sufficient condition that a point lattice with n points have the symmetric group on n letters as its group of automorphisms, and the construction of a lattice with a given arbitrary abelian automorphism group. A few results are added which are not directly connected with the study of automorphisms. Of these is a test for modularity of a lattice in terms of bonds (coverings) which is useful.

For his many helpful suggestions during the course of this investigation I am indebted to Professor Morgan Ward.

2. Notation and terminology. We shall generally denote a lattice by a script $\mathcal{L}$ and its elements by capitals A, B, C, X, Y. $A \in \mathcal{L}$ means A is an element of $\mathcal{L}$. We write $A \supset B$ $(A \subset C)$ for A contains B (A contained in C). When $A \supset B$ and $A \subset B$, we write $A = B$. A covers B (A is covered by C) is written $A > B$ $(A < C)$. $A \wedge B$ and (A, B) indicate the join and meet respectively, of A and B . Let $\mathcal{M}$ represent a set of elements of $\mathcal{L}$: $A_1, A_2, \cdots, A_n$; we write $\Lambda \mathcal{M} = \overset{n}{\underset{1}{\Lambda}} A_i = A_1 \wedge A_2 \wedge \cdots \wedge A_n$ and $\Delta \mathcal{M} = \overset{n}{\underset{1}{\Delta}} A_i = (A_1, A_2, \cdots, A_n)$. $J = \Lambda \mathcal{L}$ and $M = \Delta \mathcal{L}$ will represent the join and meet respectively of all elements of the lattice. We call $N \in \mathcal{L}$ a node if $A \subset N$ or $N \subset A$ for every $A \in \mathcal{L}$. The elements covering M are called points and those covered by J dual points. Dedekind or modular lattices will be represented by $\mathcal{B}$ and distributive lattices by $\mathcal{C}$. Sublattices will be indicated by $\mathcal{U}_i$. The automorphism group will be denoted by $\mathcal{G}$ and a subgroup by $\mathcal{H}_i$. The symmetric group on n letters is denoted by $\mathcal{S}_n$. New notations will be introduced when needed.

II

The Group of Automorphisms of a Lattice

3. Definition. An automorphism of a lattice $\mathcal{L}$ is a one-to-one correspondence between the elements of $\mathcal{L}$ and themselves which is preserved under the two fundamental operations of join and meet in $\mathcal{L}$.

We denote the automorphisms of $\mathcal{L}$ by small Greek letters. If α is an automorphism of $\mathcal{L}$, we denote the element corresponding to A by A^{α} and write:

$$\alpha: A \longleftrightarrow A^{\alpha}$$

We call A^{α} an "image" of A.

By definition:

$$(A \cap B)^{\alpha} = A^{\alpha} \cap B^{\alpha}$$

$$(A , B)^{\alpha} = (A^{\alpha} , B^{\alpha})$$

for all A , B of $\mathcal{L}$. By an easy induction we get:

$$(\bigwedge_1^n A_i)^{\alpha} = \bigwedge_1^n A_i^{\alpha}$$

$$(\Delta_1^n A_i)^{\alpha} = \Delta_1^n A_i^{\alpha}$$

We can further generalize the application of the definition to get the image under α of a function of a set of elements of $\mathcal{L}$, consisting of successive joins and meets of these elements, equal to the same function of the respective images of the elements.

The identity automorphism ι is given by:

$$\iota : A \longleftrightarrow A$$

for every $A \in \mathcal{L}$. Thus $A^{\iota} = A$.

If α and β are two automorphisms of $\mathcal{L}$, we write $(A^{\alpha})^{\beta} = A^{\alpha\beta}$. By the product $\alpha\beta$ we mean the result of applying

α, followed by β acting on the elements of $\mathcal{L}$, and we write:

$$\alpha\beta : A \longleftrightarrow A^{\alpha\beta}$$

By the inverse α^{-1} of α we mean:

$$\alpha^{-1} : A^{\alpha} \longleftrightarrow A$$

for all $A \in \mathcal{L}$. Evidently $\alpha^{-1}\alpha = \alpha\alpha^{-1} = \iota$.

We close this section with the fundamental

THEOREM 3.1. The set $\mathcal{G}$ of all the automorphisms α of a lattice $\mathcal{L}$ form a group, the automorphism group of the lattice.

The theorem is easily verified and the proof is omitted.

4. Fundamental properties of automorphisms. In this section we shall state a number of lemmas most of which are obvious from the definition of an automorphism of a lattice. We omit the proofs.

LEMMA 4.1. An automorphism α preserves the relations $\supset$ and $\subset$.

LEMMA 4.2. Chains are preserved by α .

LEMMA 4.3. The elements M and J and the nodes N_i of $\mathcal{L}$, when they exist, are invariant under every α of $\mathcal{L}$.

LEMMA 4.4. The Dedekind property is preserved by every α .

LEMMA 4.5. The distributive property is preserved by every α .

LEMMA 4.6. Complemented elements are carried into complemented elements by every α .

LEMMA 4.7. An automorphism α preserves the covering relations $>$ and $<$.

LEMMA 4.8. Descending and ascending chain conditions are preserved by α .

LEMMA 4.9. If an element is expressible as the join of points, so too is its image under α .

We note that if A contains only the n points $X_1, X_2, \cdots, X_n$ then A^α contains only the n points $X_1^\alpha, X_2^\alpha, \cdots, X_n^\alpha$. This important fact is clear from the 1-1 ordering imposed by α .

LEMMA 4.10. In a finite lattice with rank function defined, rank is preserved by α .

Notation. For the following lemma we adopt a new notation. Let u_X be the number of elements covering the element X and d_X be the number of elements covered by X . Then, u_X and d_X denote the number of bonds emanating upward and downward, respectively from X in the lattice diagram. If $u_X = 5$ and $d_X = 7$, we shall call X a $(5 - 7)$ element. M is then an $(n - 0)$ element, where n is the number of points; J is a $(0, m)$ element. We shall use this notation again later on.

LEMMA 4.11. An $(r - s)$ element is carried into an $(r - s)$ element by an automorphism of $\mathcal{L}$.

We conclude this section with the proof of the simple but important

THEOREM 4.1. An automorphism α carries sublattices into sublattices of like kind; i.e., distributive sublattices go into distributive sublattices, point sublattices are carried into point sublattices, and so on.

Let $\mathcal{U}_0$ be a sublattice of $\mathcal{L}$, and $\mathcal{U}_0^\alpha$ be the set of elements of $\mathcal{L}$ corresponding under α to the elements of $\mathcal{U}_0$.

If A and B are any elements of $\mathcal{U}_0$, $A^\alpha \cap B^\alpha = (A \cap B)^\alpha \leftrightarrow A \cap B \in \mathcal{U}_0$. Hence $A^\alpha \cap B^\alpha \in \mathcal{U}_0^\alpha$. Similarly $(A^\alpha , B^\alpha) \in \mathcal{U}_0^\alpha$. $\mathcal{U}_0^\alpha$ is a sublattice of $\mathcal{L}$, since it is closed with respect to join and meet. That $\mathcal{U}_0$ and $\mathcal{U}_0^\alpha$ are sublattices of like kind follows immediately from the preceding lemmas.

5. Permutation properties. The automorphism group $\mathcal{G}$ of a lattice $\mathcal{L}$ is a permutation group on its elements. If $B = A^\alpha$ is the image of A under some α of $\mathcal{G}$, we call A and B conjugate elements and write $A \sim B$. The relation of conjugacy is clearly an equivalence relation. It enables us to divide $\mathcal{L}$ into classes $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, \cdots$, of conjugate elements where the set $\mathcal{M}_i$ consists of all images of some $A_i \in \mathcal{L}$. These classes are then the transitive systems of $\mathcal{G}$ when it is represented as a permutation group on the elements of $\mathcal{L}$.

Consider a class $\mathcal{M}$ of equivalent (conjugate) elements $A_1, A_2, \cdots, A_n$. From well known theorems* of group theory we get the next four theorems.

THEOREM 5.1. If the transpositions $(A_1A_2), (A_1A_3), \cdots, (A_1A_n)$ are all elements of $\mathcal{G}$, then the symmetric group $\mathcal{S}_n$ is a subgroup of $\mathcal{G}$.

THEOREM 5.2. If the cycles $(A_1A_2A_3), (A_1A_2A_4), \cdots, (A_1A_2A_n)$ are all elements of $\mathcal{G}$, then the alternating group $\mathcal{A}_n$ is a subgroup of $\mathcal{G}$.

THEOREM 5.3. The set of all automorphisms leaving an element A_1

* Carmichael "Introduction to the Theory of Groups of Finite Order," Corollary to Theorem II, p. 8; Corollary to Theorem IV, p. 11;

unaltered forms a subgroup of $\mathcal{G}$. The index of this subgroup is the number n of images of A_1.

If $\mathcal{G}$ has prime order p, this subgroup must be the identity element ι of index p or $\mathcal{G}$ itself of index one. Hence we have

COROLLARY 5.3. If the automorphism group $\mathcal{G}$ of $\mathcal{L}$ has prime order p, every element is either invariant or has exactly p images, including itself.

Hence, when the order of $\mathcal{G}$ is a prime p, the classes $\mathcal{M}_i$ of conjugate elements of $\mathcal{L}$ consist of p elements or one element each. The elements of each class of order p may be so ordered that an automorphism α will be the same permutation on each class. Either α will permute all elements of each class or $\alpha = \iota$. Furthermore if $\alpha \neq \iota$, it is a cyclic permutation on all the A_i of a class. Otherwise we could write α as a product of cyclic permutations on the A_i no two of which have a letter in common.* Then the order of α would be the least common multiple of the degrees of the cyclic permutations which compose it.** This is a contradiction, since the order of α is p, a prime.

The remaining elements of $\mathcal{G}$ can be written as powers of α, since a group of prime order is cyclic and is generated by any element other than the identity. Hence we can write $\mathcal{G} = [(A_1A_2\cdot\cdot\cdot A_p)^k]$ where k has one of the values $1, 2, \cdot\cdot\cdot (p-1)$.

Now consider the automorphism group $\mathcal{G}$ of a point lattice $\mathcal{L}$. Since covering is preserved, the points are permuted among themselves

* Ibid. Theorem I, p. 7.

** Ibid. Theorem V, p. 11.

and may be divided into classes of conjugate elements. That *every* $\alpha \neq \iota$ will permute points is clear from the definition of a point lattice and the fact that chains are preserved. Hence we have

THEOREM 5.4. The automorphism group of a point lattice is a permutation group on its points.

COROLLARY 5.4. The automorphism group of a point lattice of n points is a subgroup of the symmetric group $\mathcal{S}_n$.

6. *Invariant sublattices and subgroups*. We state here a theorem of Birkhoff.* Its proof is left to the reader.

THEOREM 6.1. The set of elements of $\mathcal{L}$ invariant under α form a sublattice. This sublattice is called the centralization of α. More generally, to a subgroup $\mathcal{H}$ of the automorphism group $\mathcal{G}$ corresponds a sublattice $\mathcal{U}$ consisting of all elements invariant under every α of $\mathcal{H}$--the centralization of $\mathcal{H}$. If $\mathcal{G} = \mathcal{H}_0 \supset \mathcal{H}_1 \supset \cdots \supset \mathcal{H}_n = \iota$, and if $\mathcal{U}_0, \mathcal{U}_1, \cdots, \mathcal{U}_n$ are the centralizations corresponding to $\mathcal{H}_0, \mathcal{H}_1, \cdots, \mathcal{H}_n$ respectively, then $\mathcal{U}_0 \subset \mathcal{U}_1 \subset \cdots \subset \mathcal{U}_n = \mathcal{L}$ with $\mathcal{U}_i$ a sublattice of $\mathcal{U}_{i+1}$ $(i = 0, 1, 2, \cdots, (n - 1))$.

The analogue of this theorem is the following theorem for which we shall have use later.

THEOREM 6.2. The set of all automorphisms of $\mathcal{G}$ leaving a given element A unaltered forms a subgroup of $\mathcal{G}$. More generally, to a sublattice $\mathcal{U}$ of $\mathcal{L}$ correspond a subgroup $\mathcal{H}$ of $\mathcal{G}$ which leaves it *absolutely* unaltered.

* Birkhoff (3) --"On the Structure of Abstract Algebras," p. 435.

The first part of the theorem is merely a restatement of Theorem 5.3.

We note that the subgroup $\mathcal{H}$ that leaves a sublattice $\mathcal{U}$ absolutely unaltered is a subgroup of a larger subgroup $\mathcal{H}_0$ which leaves $\mathcal{U}$ unaltered merely as a sublattice.

THEOREM 6.3. Let A and B be two invariant elements of $\mathcal{L}$, with $A \supset B$. Then the quotient lattice $\frac{A}{B}$ is invariant as a sublattice of $\mathcal{L}$.

This theorem is an immediate consequence of Lemma 4.2.

COROLLARY 6.3. Let $\mathcal{M}$ be a class of conjugate elements $A_1, A_2, \cdots, A_n$ of $\mathcal{L}$. Then $\frac{\Lambda \mathcal{M}}{\Delta \mathcal{M}} = \frac{\overset{n}{\Lambda} A_i}{\overset{n}{\underset{1}{\Delta}} A_i}$ is invariant as a sublattice of $\mathcal{L}$.

For $\overset{n}{\underset{1}{\Lambda}} A_i$ and $\overset{n}{\underset{1}{\Delta}} A_i$ are invariant under every automorphism.

We need not restrict Theorem 6.3 and its corollary to the whole automorphism group $\mathcal{G}$. We can consider quotient lattices invariant under a subgroup $\mathcal{H}$ of $\mathcal{G}$. A more general result than Theorem 6.3 is the following: If $A \longleftrightarrow A^{\alpha}$ and $B \longleftrightarrow B^{\alpha}$ under α, with $A \supset B$ and $A^{\alpha} \supset B^{\alpha}$, then $\frac{A}{B} \cong \frac{A^{\alpha}}{B^{\alpha}}$.

Definition. Let $N_1, N_2, \cdots, N_r$ be the nodes of a lattice $\mathcal{L}$, with $J \supset N_r \supset N_{r-1} \supset \cdots \supset N_1 \supset M$. The quotient lattices $\frac{J}{N_r}, \frac{N_r}{N_{r-1}}, \cdots, \frac{N_2}{N_1}, \frac{N_1}{M}$ are called the principal sublattices (Hauptunterverbände) of $\mathcal{L}$.

From Lemma 4.3 and Theorem 6.3 we get immediately

THEOREM 6.4. The principal sublattices of $\mathcal{L}$ are invariant as sublattices under the automorphisms of $\mathcal{L}$.

The automorphisms of any one principal sublattice are certainly independent of those of the other principal sublattices. We therefore conclude

THEOREM 6.5. The automorphism group $\mathcal{G}$ of a lattice $\mathcal{L}$ with one or more nodes is the direct product of the groups of its principal sublattices.

From this it is seen that in the study of lattice automorphism groups we can confine ourselves to lattices without nodes.

We shall make use of this important theorem later on.

7. Point lattice with the symmetric group. In this section is given a necessary and sufficient condition that a point lattice with n points have the symmetric automorphism group $\mathcal{S}_n$.

Definition. Let $\mathcal{L}$ be an Archimaedian lattice in which all chains between an arbitrary pair of dependent elements are of equal length. We shall call $\mathcal{L}$ an equal-chain lattice (ausgeglichener Verband).

Notation. We shall denote the points of a point lattice by numbers $1, 2, \cdots, n$. Since each element is the join of all the points it contains, we shall incorporate this idea in our notation. If an element contains 1, 2, 4 and 7 and no other points, we shall write 1247 instead of $1 \wedge 2 \wedge 4 \wedge 7$. Then by the properties of a point lattice the join of 12479 and 2589 is 1245789. We use this notation in

THEOREM 7.1. Let $\mathcal{L}$ be an equal chain point lattice of rank ρ with n points. Let each rank consist of all the combinations of the n points taken k at a time, k obviously increasing with the rank r.

Then, as r takes in the successive values $1, 2, \cdots, (\rho - 2), (\rho - 1), \rho$, k takes on the successive values, $1, 2, \cdots, (\rho - 2), (\rho - 1), n$ respectively. In other words M is of rank zero, the C_1^n points $1, 2, \cdots, n$ are of rank 1; those of rank 2 are the C_2^n elements $12, 13, \cdots, 1n, 23, \cdots, (n-1)n$; and so on till we have the elements of rank $\rho - 1$ consisting of the n points taken $\rho - 1$ at a time; then k jumps to the value n for $r = \rho$ and we get J alone of rank ρ.

If k skipped an integral value except between the rank $\rho - 1$ and rank ρ we would not have unique join of elements. This is best illustrated by the example of Figure 1.

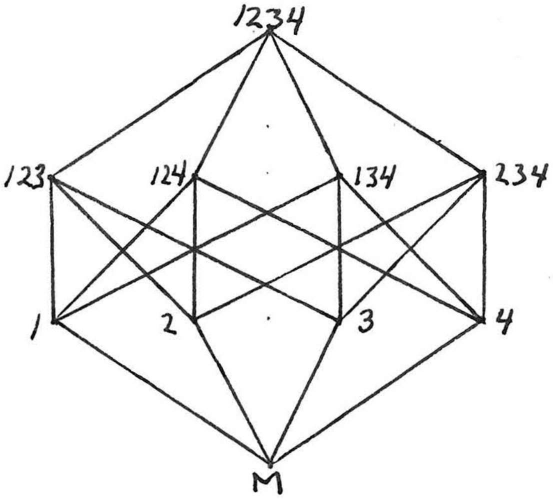

Figure 1 .

This is not the diagram of a lattice because the join, say, of 1 and 2 is not unique.

THEOREM 7.2. A point lattice $\mathcal{L}$ with n points has the symmetric group $\mathcal{S}_n$ as its automorphism group if and only if it is an equal-chain point lattice with each rank consisting of all the C_k^n combinations of the n points taken k at a time, k constant for each rank, hence if and only if $\mathcal{L}$ is of the form given in Theorem 7.1.

Suppose $\mathcal{S}_n$ is the group of automorphisms of $\mathcal{L}$. Let the points contained in an arbitrary element A be 1, 2, $\cdots$, r. Then in our notation $A = 123 \cdots r$. $A^\alpha = (123 \cdots r)^\alpha = 1^\alpha 2^\alpha 3^\alpha \cdots r^\alpha$. Since α ranges over all permutations of the n points, we see that A^α ranges over all the C_r^n elements represented by taking the n points r at a time. Thus $\mathcal{L}$ consists of a number of such sets with different r. It is clear that each set is of constant rank so that $\mathcal{L}$ is an equal-chain point lattice. The remainder of the proof of the necessity follows immediately from Theorem 7.1.

The sufficiency is evident from the symmetrical way in which the elements are represented in terms of the n points.

When $\rho = n$ in this type of lattice we have the Boolean algebra consisting of all subsets of n points. (See Theorem 24.2, Birkhoff (1)). This lattice is the distributive lattice generated by n points. The diagram of the Boolean algebra with n = 5 is given in the figure on the next page.

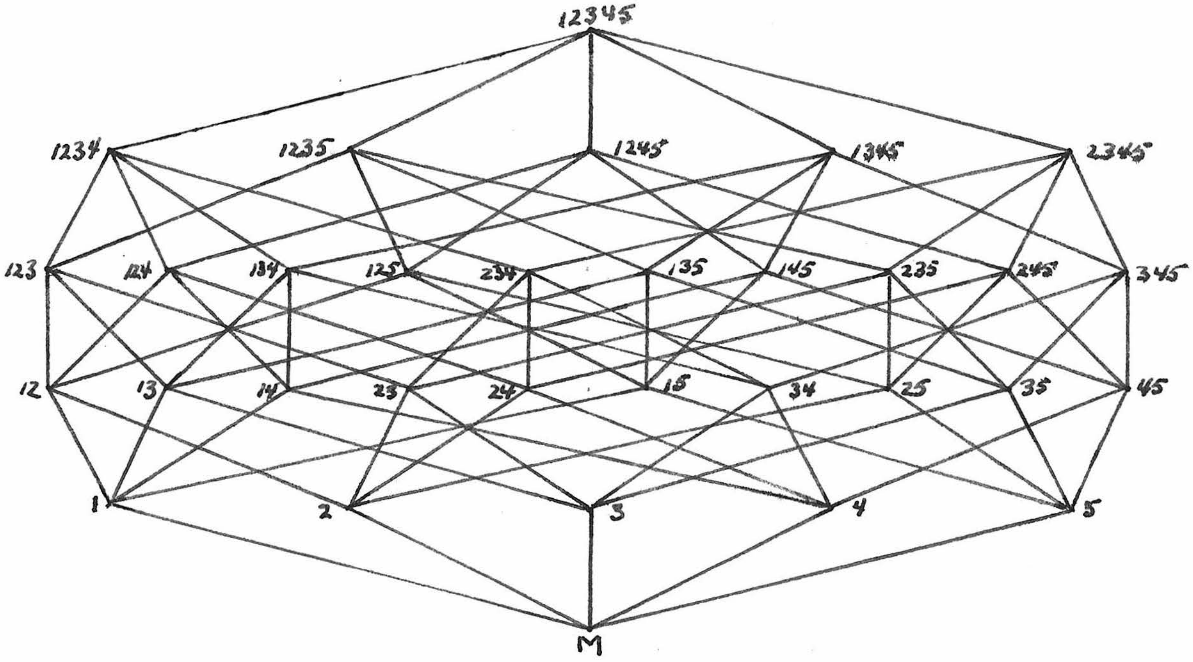

Figure 2

When $\rho = n - k$, the lattice of Theorems 7.1 and 7.2 is obtained from the Boolean algebra of n points by omitting the elements of rank $n - k, n - k + 1, \cdots, n - 1$. A simple case for which $\rho = 3$ and $n = 5$ is illustrated below.

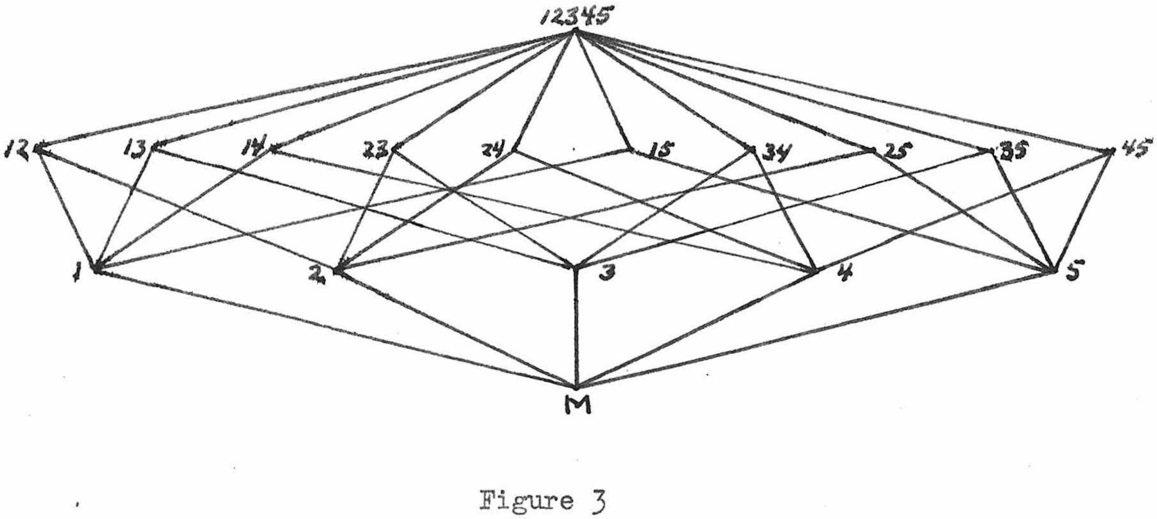

Figure 3

This type lattice is seen to be a Birkhoff lattice in which the ξ condition holds.* The ξ' condition fails for the elements covered by J except for the case $\rho = 2$.

In the latter case the lattice is modular, but is distributive only when n = 2 . A diagram of this case is given in Figure 4.

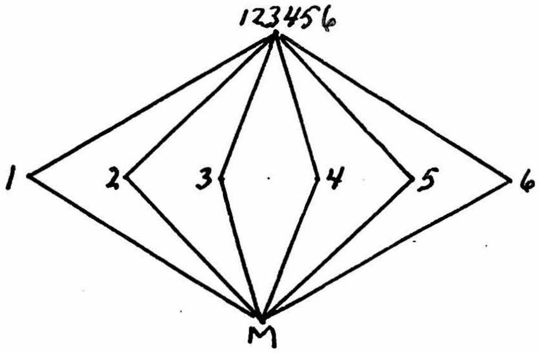

Figure 4

The Boolean algebra is the most interesting case of this type of lattice. Every distributive lattice of rank n is a sublattice of the Boolean algebra of n points. From this follows

THEOREM 7.3. The automorphism group of a distributive lattice of rank n is a subgroup of the symmetric group $\mathcal{S}_n$.

In the next three sections we shall be concerned with the automorphism groups of distribution lattices.

* Birkhoff (1)--"On the Combinations of Subalgebras," p. 445.

8. Notation for distributive lattices. The notation we now develop for the elements of a distributive lattice $\mathcal{C}$ will be useful in studying its automorphism group. We use Theorems 17.2 and 17.3 of Birkhoff's paper.*

The generators are labeled in order of rank. The n point generators are represented by the integers 1, 2, 3, $\cdots$, n. These, of course, generate the Boolean algebra $\mathcal{C}_n$ of rank n of Section 7. Then, by Theorem 17.2 mentioned above each element of $\mathcal{C}_n$ is identified with a subset of the n points in such a way that the join of two elements X and Y is identified with the logical sum of the subsets of X and Y and the meet with their common part. Now consider the generators of rank 2 and suppose there are p of them. If they cover, say, 1, 4, 7, $\cdots$, (n - 3), (n - 1) respectively we denote them by 1(n + 1), 4(n + 2), 7(n + 3), $\cdots$, (n - 3)(n + p - 1), and (n - 1)(n + p) respectively. The elements generated by these new elements and those of $\mathcal{C}_n$ are gotten by taking the logical sum as the join and the common part as the meet. We obtain the representation of the generators of third and higher orders in the same manner, and get the resulting generated elements as before by taking logical sum and common part for join and meet respectively. Thus if the rth generator covers 135789 we designate it by 135789r. Also 135789 $\wedge$ 1468 = 13456789 and (135789,1468) = 18. It must be remembered that the number of the generators is equal to the rank of the distributive lattice.

* Birkhoff (1)--"On the Combination of Subalgebras," pp. 454-456.

To illustrate this notation the diagram of a lattice of rank 10 is given below. Its generators, enclosed by squares, are 1, 2, 3 of rank 1 ; 124, 125 covering 12 and 236, 237 covering 23 all of rank 3 ; 12345678 of rank 8; and 123456789, 12345678t of rank 9 .

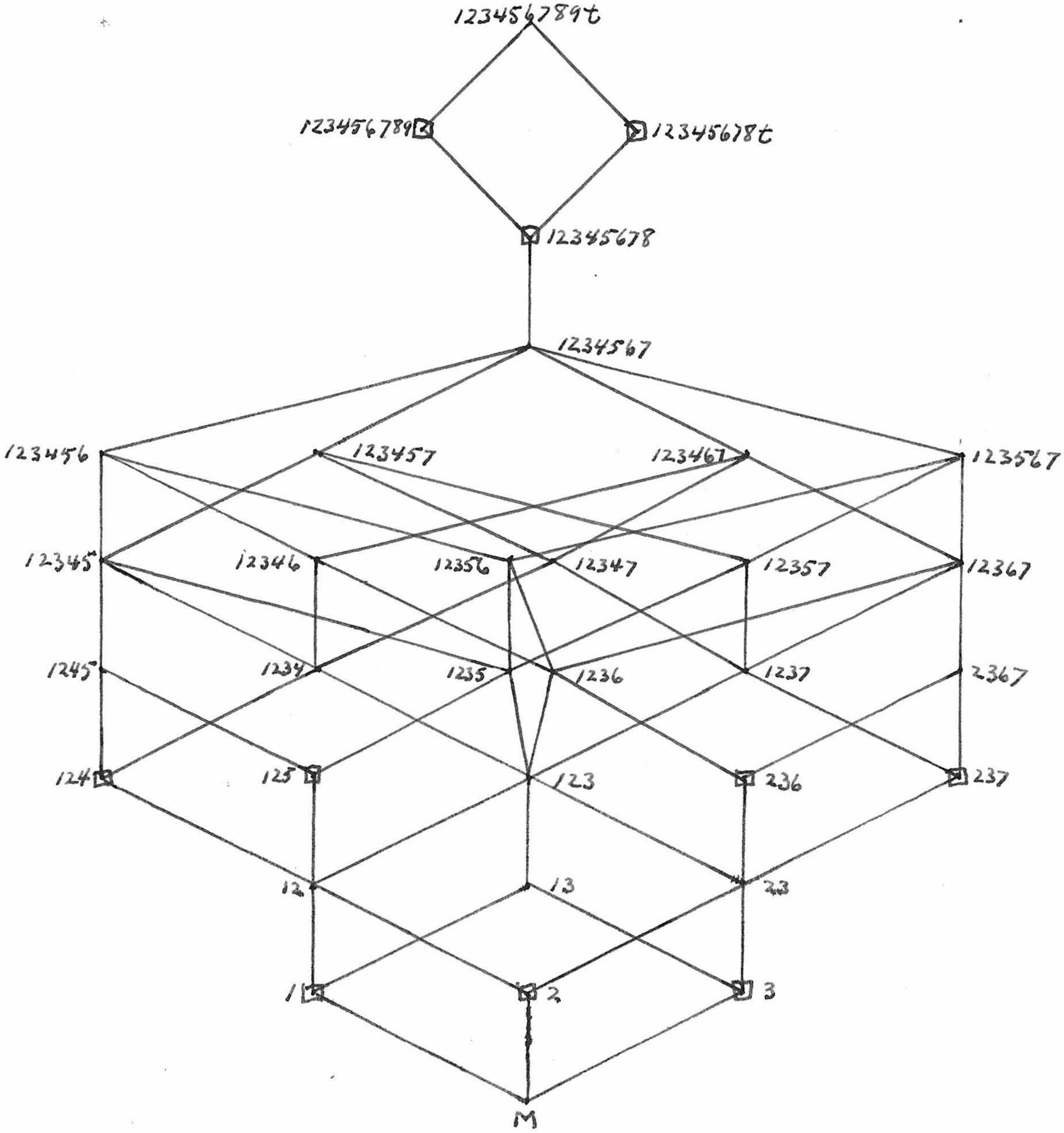

Figure 5

The group of this lattice is the direct product of the four groups $\{\iota, (9t)\}$, $\{\iota, (12)(47)(56)\}$, $\{\iota, (45)\}$, and $\{\iota, (67)\}$. It is therefore of order 16 . It is noted that the four generators 124, 125, 236, 237 form a simply transitive system with the two sets 124, 125 and 236, 237 as systems of imprimitivity.

This notation has several important useful properties. The rank of an element is merely the number of digits or letters in its representation. Furthermore, we can tell at a glance which generators are contained in a particular element.

Now the structure of a distributive lattice is determined uniquely by the manner in which transitivity is ascribed to the generators. An automorphism will then permute certain generators of the same rank, since the generators determine absolutely the complete structure of the lattice. Using the notation here developed, an automorphism α will then be a permutation on the end digits of the representations of the generators. Applying this permutation to the representation of an element A we get automatically the image A^{α} of A .

9. Direct product of linear lattices. The direct product of two linear lattices of rank m and n respectively, is represented by a rectangular checkerboard diagram. We show the diagram of the direct product of the linear lattices of rank 3 and 5 in Figure 6.

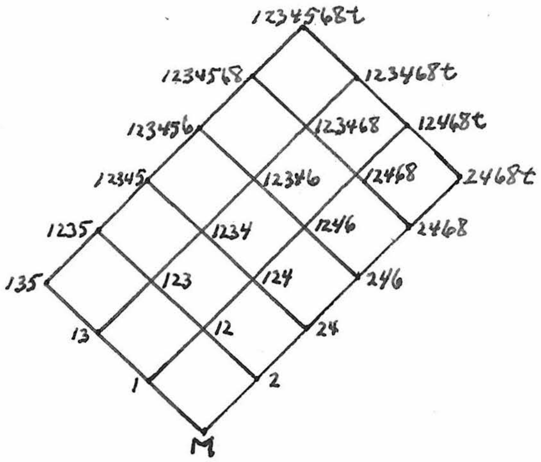

Figure 6

The direct product of n linear lattices of rank ρ_1, ρ_2, $\cdots$, ρ_n respectively, is represented by the projection upon two dimensions of a generalized rectangular network structure of n dimensions. A lattice of this type is a g.c.d.-l.c.m. lattice. The elements are factors of the positive integer n where $n = p_1^{\rho_1} p_2^{\rho_2} \cdots p_n^{\rho_n}$. The join of two elements is taken to be the l.c.m. of the elements, while their meet is their g.c.d. The generators are $p_1, p_1^2, \cdots, p^{\rho_1}$; $p_2, p_2^2, \cdots, p_2^{\rho_2}$; $\cdots$; $p_n, p_n^2, \cdots, p_n^{\rho_n}$. The automorphism group of this lattice is easily seen to be the direct product of symmetric groups:

$$\mathcal{G} = \mathcal{S}_{r_1} \times \mathcal{S}_{r_2} \times \cdots \times \mathcal{S}_{r_k}$$

where

(i) r_i is the number of ρ_j equal to i

(ii) the $\mathcal{S}_{r_i}$ are deleted when $r_i = 1$

(iii) $r_1 = 2r_2 + 3r_3 + \cdots + kr_k = \rho = \rho_1 + \rho_2 + \cdots + \rho_n$.

A special case of this type of lattice is the Boolean Algebra $\mathcal{C}_n$ of rank n of Section 7. This lattice is the direct product of n linear lattices of rank 1. Hence $r_1 = n$ and $0 = r_2 = r_3 = \cdots$ so that $\mathcal{G} = \mathcal{S}_n$, as we have already seen.

Suppose we have given the direct product $\mathcal{C}$ of k such Boolean algebras $\mathcal{C}_i$ of rank $n_1, n_2, \cdots, n_k$ respectively. Since each $\mathcal{C}_i$ is the direct product of n_i linear lattices of rank 1, $\mathcal{C}$ is the direct product of $n_1 + n_2 + \cdots + n_k$ linear lattices of rank 1 and therefore is the Boolean algebra of rank $\sum_1^k n_i$ with group $\mathcal{S}_{\sum_1^k n_i}$.

This example illustrates the fact that the direct product of the groups of several lattices is merely a <u>subgroup</u> of the group of the direct product of these lattices. The simplest case is given below.

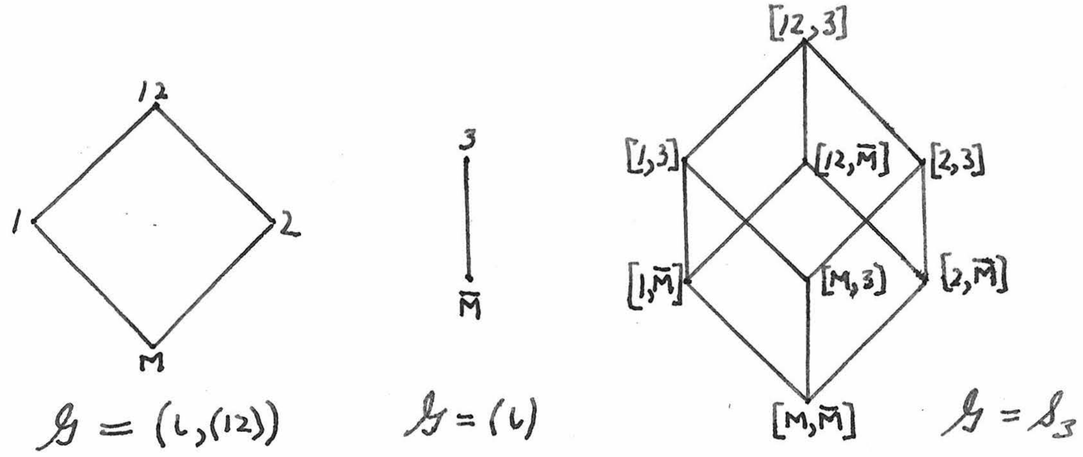

Figure 7

10. <u>Lattice with given group</u>. In the preceding sections we have dealt with a few of the aspects of the problem of finding the group of a given lattice. Finding the group of a lattice is a separate problem for each lattice in the most general case. We can establish significant

theorems on the group of a lattice only for well-behaved types such as equal-chain lattices and distributive lattices.

In this section we shall be concerned with the converse problem, the construction of a lattice having a given group for its automorphism group. The problem has been solved for the case of finite abelian groups. We state this result now in

THEOREM 10.1. Given an arbitrary finite abelian group $\mathcal{G}$. There exists a distributive lattice $\mathcal{L}$ with $\mathcal{G}$ as its automorphism group.

Any finite abelian group is the direct product of cyclic groups.* Theorem 6.5 states that the group of a lattice with nodes is the direct product of the groups of the principal sublattices. Our problem is therefore reduced to constructing the principal sublattices having the cyclic groups for automorphism groups.

We do this using the notation developed for distributive lattices in Section 8. Let n be the order of the cyclic group.

Case $n = 2$. We take the Boolean Algebra of rank 2 . (See Figure 7).

We omit the cases $n = 3$ and $n = 4$ for the time being.

Case $n = 5$. We take as generators the set of five points, 1, 2, 3, 4, 5, the set of rank three $12a_3$, $23a_4$, $34a_5$, $45a_1$, $51a_2$, and the set of rank seven $1234a_3a_4b_5$, $2345a_4a_5b_1$, $3451a_5a_1b_2$, $4512a_1a_2b_3$, $5123a_2a_3b_4$. Let α be the permutation $(12345)(a_1a_2a_3a_4a_5)(b_1b_2b_3b_4b_5)$. On account of the cyclic manner in which we have defined the generators, α and its powers α^k ($k = 2, 3, 4, 5$ with $\alpha^5 = \iota$) are automorphisms of the distributive lattice which we shall denote by $\mathcal{C}_5$. Each set of generators is permuted cyclically by α .

[*] Carmichael--"Introduction to the Theory of Groups of Finite Order," p. 66, Theorems XIV and XV.

We must now show that there are no other automorphisms of $\mathcal{C}_5$. The five powers of α beginning with the first carry the points 1 and 2 into the ordered pairs 2,3; 3,4; 4,5; 5,1; 1,2 respectively. We now show from consideration of the second and third sets of generators that only these powers of α can do this. Since the three sets of generators must be permuted among themselves, it is evident from the second set that consecutive integers must be carried into consecutive integers. If β exists carrying 1 and 2 into 3 and 2, 4 and 3, or 5 and 4 respectively, then $\alpha\beta^{-1}$, $\alpha^2\beta^{-1}$, or $\alpha^3\beta^{-1}$ will transpose 1 and 2. In any event we need consider only the existence of an automorphism transposing 1 and 2 . If one exists $12a_3$ is invariant, $23a_4 \longrightarrow 15a_2$ so that $3 \longrightarrow 5$ and $a_4 \longrightarrow a_2$, $34a_5 \longrightarrow 45a_1$ and $45a_1 \longrightarrow 34a_5$. Out of this we get the permutation $\begin{pmatrix} 12345a_1a_2a_3a_4a_5b_1b_2b_3b_4b_5 \\ 21543a_5a_4a_3a_2a_1 \quad ? \end{pmatrix}$. To determine the images of the b_i we consider the third set of generators. We find that $1234a_3a_4b_5 \longrightarrow 4512a_2a_3b_u$. But there is no such generator for any value of u . Hence there are no other automorphisms than those of the cyclic group α , and we have completed the case $n = 5$.

For the case $n > 5$ we apply the same argument to the analogous sets of generators 1, 2, $\cdot \cdot \cdot$, n; $12a_3$, $23a_4$, $\cdot \cdot \cdot$, $(n - 2)(n - 1)a_n$, $(n - 1)na_1$, $n1a_2$; and $1234a_3a_4b_5$, $2345a_4a_5b_6$, $\cdot \cdot \cdot$, $(n - 1)n12a_1a_2b_3$, $n123a_2a_3b_4$.

This method of choosing generators breaks down for the case $n = 4$. To get a distributive lattice $\mathcal{C}_4$ with the cyclic group of order 4 as automorphism group we take for generators the following four sets: 1, 2, 3, 4; $12a_3$, $23a_4$, $34a_1$, $41a_2$; $12b_3$, $23b_4$, $34b_1$, $41b_2$; and $123a_3b_4c_1$, $234a_4b_1c_2$, $341a_1b_2c_3$, $412a_2b_3c_4$. The four powers of

$\alpha = (1234)(a_1a_2a_3a_4)(b_1b_2b_3b_4)(c_1c_2c_3c_4)$ are obviously automorphisms. Furthermore, from the second set of generators we see that a pair of cyclically consecutive members of 1, 2, 3, 4 (as elements or subscripts of elements) must go into a pair of consecutive numbers in the same or inverse order. If a pair goes into a pair in the same order, it is easily seen that the resulting automorphism must be a power of α . If the pair goes into a pair in reverse order, we need consider, as we did in case $n = 5$, only the possibility of a transposition of 1 and 2. If one exists we get the permutation $\begin{pmatrix} 1234a_1a_2a_3a_4b_1b_2b_3b_4c_1c_2c_3c_4 \\ 2143a_1a_4a_3a_2b_1b_4b_3b_2 \quad ? \end{pmatrix}$ upon consideration of the second and third sets of generators. But this means that $123a_3b_4c_1 \longrightarrow 412a_3b_2c_u$ which does not exist for any value of u . Hence the powers of α are the only automorphisms of this lattice.

We must take even more complicated (comparatively) sets of generators for a distributive lattice with automorphism group cyclic of order three. The sets are 1, 2, 3; 4, 5, 6; 7; $124a_3$, $235a_1$, $316a_2$; and $1257b_3$, $2367b_1$, $3147b_2$. Here $\alpha = (123)(456)(a_1a_2a_3)(b_1b_2b_3)$. Now $\alpha, \alpha^2, \alpha^3 = \iota$ are automorphisms because of the cyclic order in which the letters appear in the generators. If β exists carrying 1 into 5 then $\beta\alpha^2$ carries 1 into 4, or if β exists carrying 1 into 6, $\beta\alpha$ carries 1 into 4. If an automorphism exists carrying 1 into 4, then $124a_3 \longrightarrow 124a_3$ and a_3 is invariant. We have two subcases: $4 \longrightarrow 1$ and $4 \longrightarrow 2$. If $4 \longrightarrow 1$ then $2 \longrightarrow 2$, $235a_1 \longrightarrow 235a_1$, and $316a_2 \longrightarrow 235a_1$. The latter is impossible, since $1 \longrightarrow 4$. If $4 \longrightarrow 2$ then $2 \longrightarrow 1$, $235a_1 \longrightarrow 316a_2$, and $316a_2 \longrightarrow 235a_1$. Again the latter is impossible since $1 \longrightarrow 4$. We have excluded the possibility of an automorphism carrying 1 into 4, 5 or 6 .

Similarly 2 and 3 cannot go into 4, 5 or 6. Hence 1, 2, 3 are permuted among themselves and 4, 5, 6 among themselves. If 1 is invariant and 2 and 3 are transposed, then $235a_1$ and 5 are invariant and 4 and 6 are transposed from a consideration of the fourth set of generators. But in the fifth set $1257b_3 \longrightarrow 1357b_u$ which does not exist for any value of u. Hence no automorphism leaves 1 invariant while transposing 2 and 3. Similarly no automorphism transposes 3 and 1 or 1 and 2. On the other hand, the automorphisms that permute 1, 2, 3 cyclically are easily seen to be the three powers of α. Therefore, $\alpha, \alpha^2, \alpha^3 = \iota$ constitute the cyclic automorphism group of order three of this lattice.

We have now completed the demonstration of the existence of distributive lattices with cyclic automorphism groups of all orders. Given an arbitrary finite abelian group, we express it as the direct product of cyclic groups. We then construct a distributive lattice with nodes having for its chief sublattices lattices with these cyclic groups as automorphism groups. This distributive lattice is the one required by the theorem and the proof is complete.

It should be emphasized that this method of construction is by no means unique. We could have constructed lattices with cyclic groups of order 4 or greater in the same manner as we constructed the one with cyclic group of order 3. We chose a simpler set of generators for order 4 and a still simpler set for order 5 or greater. The theorem is merely an existence theorem.

The construction of lattices having various types of non-abelian automorphism groups will be the subject of further investigation by the author.

11. Two examples. The diagram of Figure 8 is that of the so-called "symmetrical equivalence lattice of degree four" *. This is a modular point (and dual point) lattice. Its group has order 24. In fact its group must be isomorphic with the symmetric group $\mathcal{S}_4$.** The elements are listed in Table I.

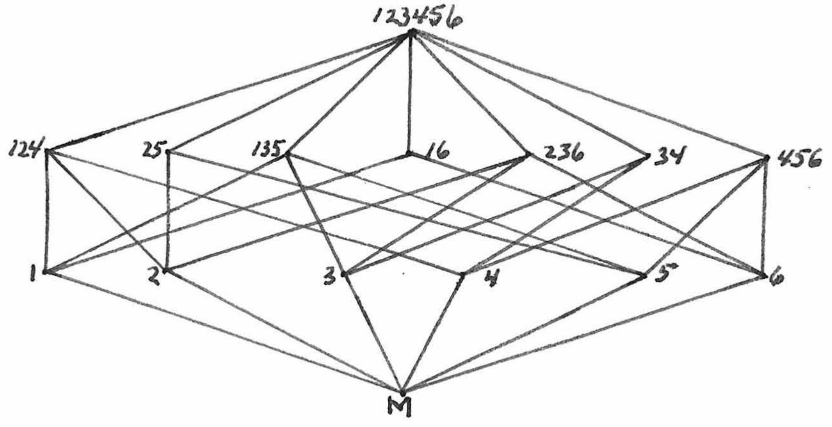

Figure 8

	α: $(14)(36)$	a: $(25)(1364)$	1: $(124)(356)^2$
ι: $()$	β: $(13)(46)$	$\bar{a}$: $(25)(1463)$	$\bar{1}$: $(124)^2(356)$
	γ: $(24)(35)$	b: $(16)(2354)$	2: $(135)(246)^2$
A: $(16)(34)$	$\bar{\alpha}$: $(23)(45)$	$\bar{b}$: $(16)(2453)$	$\bar{2}$: $(135)^2(246)$
B: $(25)(34)$	$\bar{\beta}$: $(15)(26)$	c: $(34)(1265)$	3: $(145)^2(236)$
C: $(16)(25)$	$\bar{\gamma}$: $(12)(56)$	$\bar{c}$: $(34)(1562)$	$\bar{3}$: $(145)(236)^2$
			4: $(123)^2(456)$
			$\bar{4}$: $(123)(456)^2$

Table I

[*] Birkhoff (3)--"On the Structure of Abstract Algebras," pp. 436-7 and ¶18, pp. 447-8.

[**] Ibid. Theorem 23, p. 449.

The second example, given in Figure 9, is that of the smallest non-trivial projective geometry. It is of rank 3, with seven points and seven dual points. It is surprising that its automorphism group turns out to be the smallest non-cyclic, non-alternating simple group. Projective geometries and simple non-cyclic, non-alternating groups are few in number. Whether or not there is a relation between them as hinted by the example will be a subject of later investigation.

The automorphism group, as a permutation group on the points, is doubly transitive. It is generated by (1423576) and (23)(56). We list the elements in Table II.

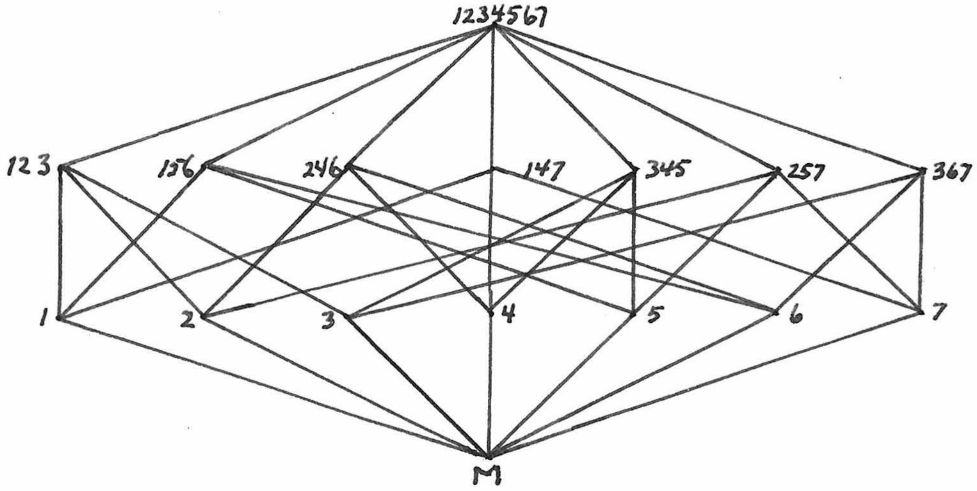

Figure 9

1 → 1	23 → 23	= ε, (56)(47), (57)(46), (45)(67)
	23 → 32	(23)(47), (23)(56), (23)(4675), (23)(4576)
	23 → 47	(24)(37), (2437)(56), (245)(376), (246)(375)
	23 → 74	(27)(34), (2734)(56), (275)(346), (276)(345)
	23 → 56	(25)(36), (2536)(47), (254)(367), (257)(364)
	23 → 65	(2635)(47), (26)(35), (267)(354), (264)(357)
1 → 2	23 → 13	(12)(45), (12)(4756), (12)(67), (12)(4657)
	23 → 31	(123)(467), (123)(576), (123)(475), (123)(456)
	23 → 46	(1243657), (124)(367), (1245)(36), (1247536)
	23 → 64	(1263475), (126)(345), (1267)(34), (1265734)
	23 → 57	(1253746), (125)(376), (1254)(37), (1256437)
	23 → 75	(127)(354), (1273564), (1276)(35), (1274635)
1 → 3	23 → 12	(132)(465), (132)(476), (132)(567), (132)(457)
	23 → 21	(13)(4567), (13)(57), (13)(4765), (13)(46)
	23 → 45	(135)(246), (1352476), (1356724), (1357)(24)
	23 → 54	(1342567), (134)(257), (1347625), (1346)(25)
	23 → 67	(1375)(26), (1374526), (1372654), (137)(264)
	23 → 76	(1365427), (1364)(27), (1362745), (136)(275)
1 → 4	23 → 26	(147)(365), (14)(36), (145)(367), (1436)(57)
	23 → 62	(1432675), (1457326), (14)(2653), (147)(263)
	23 → 35	(1467235), (1423576), (147)(235), (14)(2356)
	23 → 53	(14)(25), (147)(256), (1425)(67), (146)(257)
	23 → 17	(1452)(37), (1437562), (1465372), (142)(376)
	23 → 71	(1427653), (1463)(27), (143)(275), (1456273)
1 → 5	23 → 16	(152)(367), (1574362), (1536472), (1542)(36)
	23 → 61	(153)(264), (1547263), (1526743), (1573)(26)
	23 → 27	(1537)(46), (154)(376), (15)(37), (156)(374)
	23 → 72	(15)(2743), (156)(273), (1532764), (1546327)
	23 → 34	(15)(2347), (156)(234), (1523467), (1576234)
	23 → 43	(1524)(67), (157)(246), (15)(24), (156)(247)
1 → 6	23 → 15	(1647352), (162)(354), (1672)(35), (1635742)
	23 → 51	(1674253), (163)(257), (1643)(25), (1625473)
	23 → 24	(167)(345), (1634)(57), (165)(347), (16)(34)
	23 → 42	(165)(243), (16)(2473), (1675324), (1632457)
	23 → 37	(1645237), (1623754), (165)(237), (16)(2374)
	23 → 73	(165)(274), (16)(27), (164)(275), (1627)(45)
1 → 7	23 → 14	(1734652), (1762)(34), (172)(345), (1756342)
	23 → 41	(1753)(24), (1724563), (1765243), (173)(246)
	23 → 25	(174)(356), (17)(35), (1735)(46), (176)(354)
	23 → 52	(1764325), (1732546), (17)(2563), (174)(253)
	23 → 36	(1754236), (1723645), (17)(2365), (174)(236)
	23 → 63	(174)(265), (17)(26), (1726)(45), (175)(264)

Table II

III

Supplementary Theorems

12. Modular lattices. In this section will be given some supplementary results not directly connected with automorphisms of lattices. We give first a proof of a theorem of Birkhoff.* His proof appears incomplete The proof given here is along a different line.

THEOREM 12.1. If $X_1, X_2, \cdots, X_w$ are the points of a finite modular lattice $\mathcal{B}$, and if $Y \subset \bigwedge_1^w X_i$, then Y is the join of the X_i which it contains.

To prove this theorem we make an induction on the rank. The theorem is true for elements of rank $r = 1$. Assume the theorem is true for rank $r = n$. Let Y be an arbitrary element of rank $r = n + 1$ contained in $\bigwedge_1^w X_i$, and let $Y_1, Y_2, \cdots, Y_m$ be the elements (of rank $r = n$) covered by Y. Then, since $Y_\sigma \subset Y \subset \bigwedge_1^w X_i$, $Y_\sigma = \bigwedge_{\tau=1}^{\mu_\sigma} X_{\sigma\tau}$ where $X_{\sigma\tau}$ ($\tau = 1, 2, \cdots, \mu_\sigma$) are the points contained in Y_σ, ($\sigma = 1, 2, \cdots, m$). $Y = \bigwedge_1^m Y_i$ = the join of the $X_{\sigma\tau}$ contained in the Y_i. If X_o is any other point not included among the $X_{\sigma\tau}$, $X_o \cap \bigwedge_{\sigma=1}^{m} \bigwedge_{\tau=1}^{\mu_\sigma} X_{\sigma\tau} = X_o \cap Y$ has rank $n + 2$ by the law of rank in a modular lattice. Hence $X_o \not\subset Y$, Y contains only the points $X_{\sigma\tau}$ and is the join of these points. Since Y was an arbitrary element of rank $r = n + 1$, the theorem holds for all elements of that rank contained in $\bigwedge_1^w X_i$. The induction on r ($r = 1, 2, \cdots, w$) is now complete.

COROLLARY 12.1 A. The quotient sublattice $\dfrac{\bigwedge_1^w X_i}{M}$ is a point lattice. If $\bigwedge_1^w X_i = J$ then $\mathcal{B}$ is a point lattice (and also a dual point lattice).

[*] Birkhoff (1)--"On the Combination of Subalgebras," Theorem 11.4, p. 449.

The statement of the parentheses is gotten merely by dualizing the proof of the theorem.

COROLLARY 12.1 B. If $F_1, F_2, \cdot \cdot \cdot, F_w$ are the elements covering an element F in a finite modular lattice $\mathcal{B}$, and if Y is an element satisfying the relation $\bigwedge_1^w F_i \supset Y \supset F$, then Y is the join of the F_i which it contains. The quotient lattice $\frac{\bigwedge_1^w F_i}{F}$ is a point lattice and is the dual of a point lattice.

In the following theorem we employ the notation introduced for Lemma 4.11.

THEOREM 12.2. In a modular point (dual point) lattice $\mathcal{B}$ the only (1 - k) elements are the dual points (elements covered by J) of $\mathcal{B}$; the only (k - 1) elements are the points of $\mathcal{B}$.

Let Y be a (1 - k) element. Y is the join of the points which it contains by Theorem 12.1. By the law of rank the elements $Y_i = Y \cap X_i$, where X_i ranges over all points not contained in Y, all cover Y. They must then all be equal to an element, say Z. Since Z contains all the points it is J so that Y is a dual point. We note in passing that there can then be only one X_i not contained in Y. The second part of the theorem is merely the dual of the first part, since a modular point lattice is its own dual.

COROLLARY 12.2. A modular point (dual point) lattice has (1 - 1) elements if and only if it is of rank two.

The following theorem is a useful test for the modularity of a lattice when the lattice diagram is given. We employ the notation of Lemma 4.11.

THEOREM 12.3. Let Y be a (u - d) element in a finite modular lattice $\mathcal{B}$. Let $X_1, X_2, \cdot \cdot \cdot, X_d$ be the elements covered by Y

and $Y_1, Y_2, \cdots, Y_u$ be the elements covering Y. Then

$$D_Y \equiv \sum_{\sigma=1}^{d} (u_{X_\sigma} - 1) = \sum_{\tau=1}^{u} (d_{Y_\tau} - 1) \equiv U_Y .$$

This theorem states that in the lattice diagram the sum of all the bonds emanating downward from the elements covering Y diminished by the number of these elements is equal to the number of bonds emanating upward from the elements covered by Y diminished by the number of these elements.

Let $X^1_\sigma = Y, X^2_\sigma, \cdots, X_\sigma^{u_{X_\sigma}}$ be the u_{X_σ} elements covering X_σ.

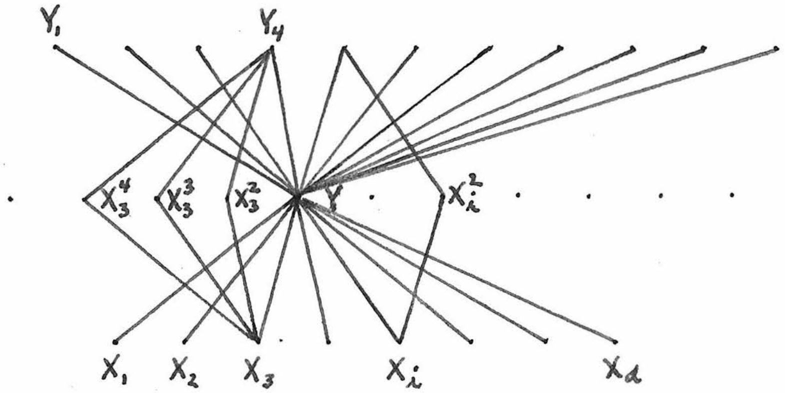

Figure 10

These $X^{i_\sigma}_\sigma$ are all distinct for every σ and $i \neq 1$. Otherwise there would be no unique join of two X_σ covered by a common X^i_σ $(\neq Y)$ as indicated in Figure 11. Now in a modular lattice when A and B each cover (A, B), then $A \cap B$ covers both

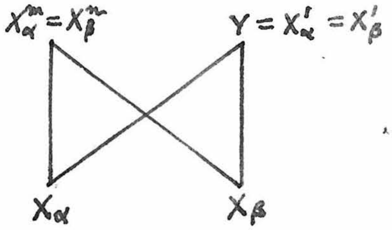

Figure 11

A and B . Hence the elements $X_\sigma^{i_\sigma} \cap Y$ $(i_\sigma \neq 1)$ cover Y and are among the Y_τ . These $(u_{X_\sigma} - 1)$ elements $X_\sigma^{i_\sigma}$ $(i_\sigma = 2, 3, \cdots, u_{X_\sigma})$ then account for all the $(u_{X_\sigma} - 1)$ bonds emanating upward from the X_σ and $(u_{X_\sigma} - 1)$ bonds emanating downward from the Y_τ excluding in each case bonds emanating from Y . Summing on σ we have the inequality

$$D_Y \equiv \sum_{\sigma=1}^{d} (u_{X_\sigma} - 1) \leqq \mathcal{U}_Y \equiv \sum_{\tau=1}^{u} (d_{Y_\tau} - 1) .$$

Dualizing the argument we get $\mathcal{U}_Y \leqq D_Y$. Hence

$$D_Y \equiv \sum_{\sigma=1}^{d} (u_{X_\sigma} - 1) = \sum_{\tau=1}^{u} (d_{Y_\tau} - 1) \equiv \mathcal{U}_Y$$

and the theorem is proved.

We note that $D_Y = \mathcal{U}_Y$ represents the number of elements other than Y which are covered by elements covering Y and that these elements are elements other than Y covering the elements covered by Y .

13. Conclusion. Several of the results of this paper will be further developed in a later investigation. The problem of determining the group of a distributive lattice will be carried further. Also the problem of constructing a lattice, given its automorphism group, will be extended to certain non-abelian groups. Another problem will be the investigation of the relation of normal divisors of the automorphism group to the structure of the lattice and related ideas. The further study of the automorphisms of lattices will be confined to distributive and other special types of lattices where results are more likely to be significant.

REFERENCES

A. A. Albert

1. Modern Higher Algebra, The University of Chicago Press, Chicago, 1937.

G. Birkhoff

1. On the combination of subalgebras, Cambridge Phil. Proc., vol. 29 (1933), pp. 441-464.
2. Applications of lattice algebra, Cambridge Phil. Proc., vol. 30 (1934), pp. 115-122.
3. On the structure of abstract algebras, Cambridge Phil. Proc., vol. 31, (1935), pp. 433-454.

R. D. Carmichael

1. Introduction to the Theory of Groups of Finite Order, Boston 1937.

R. Dedekind

1. Über die von drei Modula erzeugte Dualgruppe, Ges. Werke II (1931), Abh. XXX pp. 236-271.

F. Klein-Barmen)

1. Beitrage zur Theorie der Verbände, Math. Zeitschr. 39 (1934), pp. 227-239.
2. Grundzüge der Theorie der Verbände, Math. Annalen 111 (1935), pp. 596-621.
3. Über ausgeglichene Verbände, Math. Annalen 112 (1936), pp. 411-18.
4. Dedekindsche und distributive Verbände , Math, Zeitschr. 41 (1936), pp. 261-280.
5. Birkhoffsche und harmonische Verbände, Math. Zeitschr. 42 (1936), pp. 58-81.

A. Kurosch

1. Durchschnitts Darstellungen mit irreduzibleKomponenten in Ringen und in sogennanten Dualgruppen, Trans. Moscow Math. Soc., vol. 42 (1935), pp. 613-616.

E. Netto

1. Theory of Substitutions, (translated by F. N. Cole), The Inland Press, Ann Arbor, Michigan.

O. Ore

1. On the Foundation of abstract algebra I, Annals of Math., vol. 36 (1935), pp. 406-437.

B. L. van der Waerden

1. Moderne Algebra I, Berlin 1930.

H. Weber

1. Lehrbuch der Algebra, vol. II, Braunschweig 1899.