ELSEVIER

Theoretical Computer Science 217 (1999) 279–289

Theoretical Computer Science

Congruence lattices 101[1]

G. Grätzer *

Department of Mathematics, University of Manitoba, Winnipeg, MN R3T 2N2, Canada

Abstract

This lecture – based on the author's book, *General Lattice Theory*, Birkhäuser Verlag, 1978 – briefly introduces the basic concepts of lattice theory, as needed for the lecture "Some combinatorial aspects of congruence lattice representations". © 1999—Elsevier Science B.V. All rights reserved

AMS classification: Primary 0601; Secondary 0602

Keywords: Lattice; Congruence lattice; Breadth; Order dimension; Planar; Finite; Distributive; Join-homomorphism; Automorphism group; Chopped lattice.

1. Lattices

1.1. Posets

A *partially ordered set* $\langle A; \leqslant \rangle$ consists of a nonvoid set A and a binary relation $\leqslant$ on A such that the relation $\leqslant$ satisfies properties (P1)–(P3) for all a, b, $c \in A$:

(P1) Reflexivity: $a \leqslant a$.
(P2) Antisymmetry: $a \leqslant b$ and $b \leqslant a$ imply that $a = b$.
(P3) Transitivity: $a \leqslant b$ and $b \leqslant c$ imply that $a \leqslant c$.

A poset $\langle < A; \leqslant \rangle$ that also satisfies:

(P4) Linearity: $a \leqslant b$ or $b \leqslant a$

is called a *chain* (also called *fully ordered set*, *linearly ordered set*, and so on). The *length*, $l(C)$, of a finite chain C is $\boldsymbol{C} - \mathbf{1}$. Let $\mathfrak{C}_n$ denote the set $0, \ldots, n-1$ ordered by $0 < 1 < 2 < \cdots < n-1$; then $\mathfrak{C}_n$ is an n-element chain and $l(\mathfrak{C}_n) = n - 1$.

* Corresponding author. E-mail: gratzer@cc.umanitoba.ca.
[1] The writing of this article was supported by the NSERC of Canada.

0304-3975/99/$ - see front matter
PII: S0304-3975(98)00275-8

Let $H \subseteq P$ and $a \in P$. The element a is an *upper bound* of H iff $h \leqslant a$ for all $h \in H$. An upper bound a of H is the *least upper bound* (*supremum*) of H iff, for any upper bound b of H, we have $a \leqslant b$. We shall write $a = \sup H$ or $a = \bigwedge H$. The concepts of *lower bound* and *greatest lower bound* (*infimum*) are similarly defined; the latter is denoted by $\inf H$ or $\bigwedge H$.

1.2. Lattices

A poset $\langle L; \leqslant \rangle$ is a *lattice* iff $\inf a,b$ and $\sup a,b$ exist for all a, $b \in L$.
We will use the notation

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

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

and call $\wedge$ the *meet* and $\vee$ the *join*. In lattices, they are both *binary operations*, which means that they can be applied to a pair of elements a, b of L to yield again an element of L. $\wedge$ and $\vee$ satisfy the following:

(L1)	Idempotency :	$a \wedge a = a,$	$a \vee a = a.$
(L2)	Commutativity :	$a \wedge b = b \wedge a,$	$a \vee b = b \vee a.$
(L3)	Associativity :	$(a \wedge b) \wedge c = a \wedge (b \wedge c),$	$(a \vee b) \vee c = a \vee (b \vee c).$

There is another pair of rules that connect $\wedge$ and $\vee$:

(L4) Absorption identities : $a \wedge (a \vee b) = a, \quad a \vee (a \wedge b) = a.$

An algebra $\langle L; \wedge, \vee \rangle$is called a *lattice* iff L is a nonvoid set, $\wedge$ and $\vee$ are binary operations on L, both $\wedge$ and $\vee$ are idempotent, commutative, and associative, and they jointly satisfy the two absorption identities. The following theorem states that a lattice as an algebra and a lattice as a poset are "equivalent" concepts.

Theorem. (i) *Let the poset* $\mathfrak{L} = \langle L; \leqslant \rangle$ *be a lattice. Set*

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

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

Then the algebra $\mathfrak{L}^a = \langle L; \wedge, \vee \rangle$ *is a lattice.*
(ii) *Let the algebra* $\mathfrak{L} = \langle L; \wedge, \vee \rangle$ *be a lattice. Set*

$$a \leqslant b \quad \textit{iff} \quad a \wedge b = a.$$

Then $\mathfrak{L}^p = \langle L; \leqslant \rangle$ *is a poset, and the poset* $\mathfrak{L}^p$ *is a lattice.*
(iii) *Let the poset* $\mathfrak{L} = \langle L; \leqslant \rangle$ *be a lattice. Then* $(\mathfrak{L}^a)^p = \mathfrak{L}$.
(iv) *Let the algebra* $\mathfrak{L} = \langle L; \wedge, \vee \rangle$ *be a lattice. Then* $(\mathfrak{L}^p)^a = \mathfrak{L}$.

2. Diagrams

In the poset $\langle P; \leqslant \rangle$, *a covers b*, in notation, $a \succ b$ (or *b is covered by a*, in notation, $b \prec a$) iff $b < a$ and $b < x < a$ holds for no x. The covering relation determines the partial ordering in a finite poset.

The *diagram* of a poset $\langle P; \leqslant \rangle$ represents the elements with small circles; the circles representing two elements x, y are connected by a straight line iff one covers the other; if $x \succ y$, then the circle representing x is higher than the circle representing y. Three small examples are shown in Figs. 1 and 2.

Note that in a diagram the intersection of two lines does not indicate an element. A diagram is *planar* if no two lines intersect. Figs. 1 and 2 show planar diagrams; Fig. 3 is not a planar diagram.

The *order dimension* of a finite poset $\langle P, \leqslant \rangle$ is the smallest integer $n \geqslant 1$ such that $\leqslant$ can be represented as the intersection of the partial ordering relations of n chains defined on the set P. The order dimension of a finite lattice L is 1 iff L is a chain. The order dimension of L is 2 iff L has a planar diagram. The order dimension of the lattice of Fig. 3 is 3.

A finite lattice L is of *breadth* n, if n is the smallest natural number with the following property: for every $X \subseteq L$, there is a subset $X' \subseteq X$ such that $\bigwedge X = \bigwedge X'$

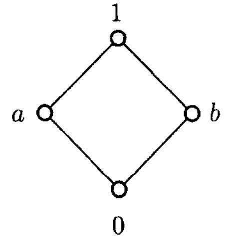

Fig. 1.

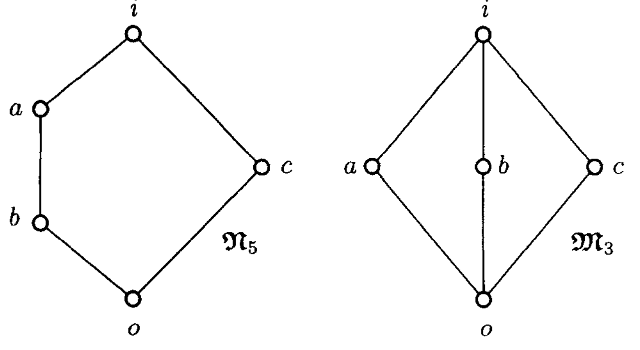

Fig. 2.

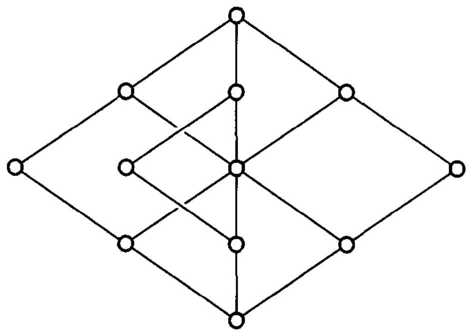

Fig. 3.

and $|X'| \leqslant n$. Interestingly, this concept is self-dual (that is, defining it for joins yields the same number).

The breadth of a planar lattice is 2. The lattice of Fig. 3 is also of breadth 2. The breadth is always less than or equal to the order dimension. David Kelly proved that for every $n \geqslant 3$, there is a (modular) lattice of breadth 3 and order dimension n.

3. Some algebraic concepts

Let L be a lattice. $K \subseteq L$ is a *sublattice* of L (or L is an *extension* of K) if K is closed under the operations of L and the operations of K are the restrictions of the operations of L to K. If a, $b \in L$, then

$$[a,b] = \{x \mid a \leqslant x \leqslant b\}$$

is a sublattice of L, called an *interval*. If a covered by b, then $[a,b]$ is a *prime interval*; it has only two elements.

A related concept is an ideal. A sublattice I of a lattice L is an *ideal*, if $a \wedge i \in I$ for all $i \in I$ and $a \in L$. The ideals of a lattice form a lattice under set inclusion; $\mathrm{Id}\,L$ is the notation for this lattice.

A *homomorphism* φ of the lattice L into the lattice K is a map of L into K satisfying both

$$(a \wedge b)\varphi = a\varphi \wedge b\varphi,$$

$$(a \vee b)\varphi = a\varphi \vee b\varphi.$$

If only the first (resp., second) holds, then φ is a *meet-homomorphism* (resp., *join-homomorphism*).

Figs. 4–6 show three maps of the four-element lattice L of Fig. 1 into the three-element chain $\mathfrak{C}_3$. The map of Fig. 4 is *isotone* (that is, if $x \leqslant y$ in L, then $x\varphi \leqslant y\varphi$ in K) but is neither a meet-nor a join-homomorphism. The map of Fig. 5 is a

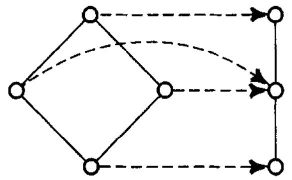

Fig. 4.

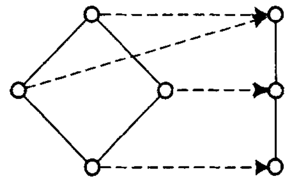

Fig. 5.

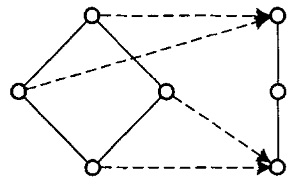

Fig. 6.

join-homomorphism but is not a meet-homomorphism, thus not a homomorphism. The map of Fig. 6 is a homomorphism.

A one-to-one and onto homomorphism is an *isomorphism*. An isomorphism of a lattice with itself is called an *automorphism*. The automorphisms of a lattice L form a group under composition, called the *automorphism group* of L; it is denoted by $\operatorname{Aut} L$.

An *equivalence relation* Θ (that is, a reflexive, symmetric, and transitive binary relation) on a lattice L is called a *congruence relation* of L iff

$$a_0 \equiv b_0 \pmod{\Theta},$$

$$a_1 \equiv b_1 \pmod{\Theta}$$

imply that

$$a_0 \wedge a_1 \equiv b_0 \wedge b_1 \pmod{\Theta},$$

$$a_0 \vee a_1 \equiv b_0 \vee b_1 \pmod{\Theta}$$

Substitution Property: Trivial examples are ω, ι, defined by $x \cong y$ (ω) iff $x = y$; $x \cong y$ (ι) for all x and y. (ω is the Greek o and stands for 0; ι is the Greek i

and stands for identity and 1.) For $a \in L$, we write $[a]\Theta$ for the *congruence class* containing a, that is

$$[a]\Theta = \{x \mid x \equiv a \ (\Theta)\}.$$

Homomorphisms and congruence relations express two sides of the same phenomenon. Let L be a lattice and let Θ be a congruence relation on L. Let L/Θ denote the set of blocks of the partition of L induced by Θ, that is,

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

Set

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

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

This defines $\wedge$ and $\vee$ on L/Θ. The lattice axioms are easily verified. The lattice L/Θ is the *quotient lattice* of L modulo Θ, and the map

$$\varphi_\Theta : x \to [x]\Theta \quad (x \in L)$$

is a homomorphism of L onto L/Θ.

Next, we introduce direct products. Let L and K be lattices and form the set $L \times K$ of all ordered pairs $\langle a, b\rangle$ with $a \in L$, $b \in K$. Define $\wedge$ and $\vee$ in $L \times K$ "componentwise":

$$\langle a_0, b_0\rangle \wedge \langle a_1, b_1\rangle = \langle a_0 \wedge a_1, b_0 \wedge b_1\rangle,$$

$$\langle a_0, b_0\rangle \vee \langle a_1, b_1\rangle = \langle a_0 \vee a_1, b_0 \vee b_1\rangle.$$

This makes $L \times K$ into a lattice, called the *direct product* of L and K (for an example, see Fig. 7).

Finally, we define identities and inequalities.

From variables x_0, x_1, ..., x_n, ..., we can form *polynomials* (terms) in the usual manner using $\wedge$, $\vee$, and, of course, parentheses. Examples of polynomials are

$$x_0,\ x_3,\ x_0 \vee x_0,\ (x_0 \wedge x_2) \vee (x_3 \wedge x_0),\ (x_0 \wedge x_1) \vee (x_0 \wedge x_2) \vee (x_1 \wedge x_2).$$

A polynomial is just a sequence of symbols. It is defined because in terms of such a sequence of symbols we can define a function on any lattice. For instance, if $p = (x_0 \wedge x_1) \vee (x_2 \vee x_1)$, then $p(a,b,c) = (a \wedge b) \vee (c \vee b) = b \vee c = i$ in $\mathfrak{N}_5$.

A *lattice identity* is an expression of the form $p = q$, where p and q are polynomials. An *identity* $p = q$ *holds in the lattice* L iff $p(a_0, \ldots, a_{n-1}) = q(a_0, \ldots, a_{n-1})$ holds for any $a_0, \ldots, a_{n-1} \in L$. Similarly, we define a *lattice inequality* $p \leqslant q$.

The two identities

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

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

are equivalent; a lattice satisfying one (or both) is called *distributive*.

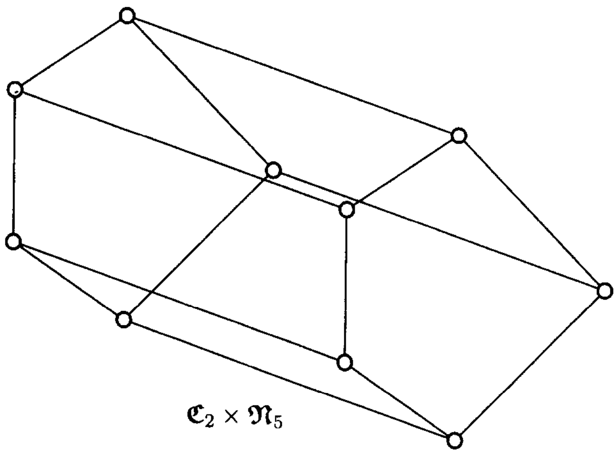

Fig. 7.

A distributive lattice B is called *Boolean* if it has a smallest element 0 and a largest element 1, and every element x has a complement x', that is

$$x \wedge x' = 0,$$

$$x \vee x' = 1.$$

Every finite Boolean lattice is isomorphic to some $\mathfrak{B}_n = (\mathfrak{C}_2)^n$ $(= \underbrace{\mathfrak{C}_2 \times \cdots \times \mathfrak{C}_2}_{n\text{-times}})$.

The identity

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

is equivalent to the condition

$$x \geqslant z \text{ implies that } (x \wedge y) \vee z = x \wedge (y \vee z).$$

A lattice satisfying either condition is called *modular*.

A more complicated identity is the *arguesian* identity:

$$p \leqslant ((c \vee x_2) \wedge x_0) \vee ((c \vee x_5) \wedge x_3),$$

where

$$p = (x_0 \vee x_3) \wedge (x_1 \vee x_4) \wedge (x_2 \vee x_5),$$

$$c_{ij} = (x_i \vee x_j) \wedge (x_{3+i} \vee x_{3+j}), \qquad 0 \leqslant i < j \leqslant 2,$$

$$c = c_{01} \wedge (c_{02} \vee c_{12}).$$

An arguesian lattice is modular. The subspace lattice of a projective space is arguesian iff Desargues' Theorem holds for the projective space. The lattice of all subspaces of a vector space is arguesian.

4. Distributive lattices

The two typical examples of nondistributive lattices are $\mathfrak{M}_3$ and $\mathfrak{N}_5$, whose diagrams are given in Fig. 2.

Theorem. *A lattice L is distributive iff L does not contain $\mathfrak{M}_3$ or $\mathfrak{N}_5$ as a sublattice.*

For a distributive lattice D, let $\mathrm{J}(D)$ denote the set of all nonzero join-irreducible elements, that is, all elements $a \in D$ for which $a = x \vee y$ implies that $a = x$ or $a = y$. We regard $\mathrm{J}(D)$ as a poset under the partial ordering of D. For $a \in D$, set

$$r(a) = \{x \mid x \leqslant a,\ x \in \mathrm{J}(D)\} = (a] \cap \mathrm{J}(D).$$

For a poset P, call $A \subseteq P$ *hereditary* iff $x \in A$ and $y \leqslant x$ imply that $y \in A$. Let $\mathrm{H}(P)$ denote the set of all hereditary subsets partially ordered by set inclusion. Note that $\mathrm{H}(P)$ is a lattice in which meet and join are intersection and union, respectively, and thus $\mathrm{H}(P)$ is distributive.

The structure of finite distributive lattices is revealed by the following result:

Theorem. *Let D be a finite distributive lattice. Then the map*

$$\varphi : a \to r(a)$$

is an isomorphism between D and $\mathrm{H}(\mathrm{J}(D))$.

Corollary. *The correspondence $D \to \mathrm{J}(D)$ makes the class of all finite distributive lattices with more than one element corresponding to the class of all finite posets. Isomorphic lattices correspond to isomorphic posets, and vice versa.*

5. Congruence lattices

Let $\mathrm{Con}\, L$ denote the set of all congruence relations on L partially ordered by set inclusion.

Theorem (R.P. Dilworth). $\mathrm{Con}\, L$ *is a lattice. For $\Theta, \Phi \in \mathrm{Con}\, L$, $\Theta \wedge \Phi = \Theta \cap \Phi$. The join, $\Theta \vee \Phi$, can be described as follows*:

> *$x \equiv y\ (\Theta \vee \Phi)$ iff there is a sequence $z_0 = x \wedge y, z_1, \ldots, z_{n-1} = x \vee y$ of elements of L such that $z_0 \leqslant z_1 \leqslant \ldots \leqslant z_{n-1}$ and for each i, $0 \leqslant i < n-1$, $z_i \equiv z_{i+1}\ (\Theta)$ or $z_i \equiv z_{i+1}\ (\Phi)$.*

Theorem (N. Funayama, T. Nakayama). *Let L be an arbitrary lattice. Then* $\mathrm{Con}\, L$, *the lattice of all congruence relations of L, is distributive.*

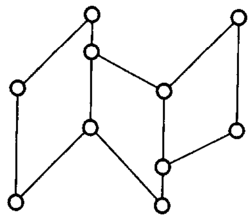

Fig. 8.

Let L be a lattice and let $H \subseteq L^2$. We denote by $\Theta(H)$ the smallest congruence relation such that $a \equiv b$ for all $\langle a,b\rangle \in H$, and call it the *congruence relation generated by* H. For any $H \subseteq L^2$, $\Theta(H)$ exists.

We shall use the notation $\Theta(a,b)$ for $\Theta(H)$ if $H = \{\langle a,b\rangle\}$. Note that $\Theta(a,b)$ is the smallest congruence relation under which $a \equiv b$. The congruence relation $\Theta(a,b)$ is called *principal.*

If L is finite, knowing J(Con L), one knows Con L. In a finite lattice L, Θ is a join-irreducible congruence relation iff it is of the form $\Theta(a,b)$, where a is covered by b. Such $\Theta(a,b)$ are usually easy to compute: for c covered by d, the congruence $c \equiv d$ $(\Theta(a,b))$ holds iff we can get from a, b to c, d with a finite number of up- and down-steps, as illustrated by Fig. 8. (In general, $c \equiv d$ $(\Theta(a,b))$ iff $x \equiv y$ $(\Theta(a,b))$ for any $c \leqslant x \prec y \leqslant d$.) An up-step joins the pair of elements with an element; a down-step meets the pair of elements with an element. Note that we start with — and end up with — a covering pair of elements, but the intermediate steps are not necessarily covering pairs. However, if L is also modular, then all the immediate steps are covering pairs, which implies the following result: Con L is Boolean for a finite modular lattice L.

Another property of congruence lattices is given in the following definition.

Definition. (i) Let L be a complete lattice and let a be an element of L. Then a is called *compact* iff $a \leqslant \bigvee X$ for some $X \subseteq L$ implies that $a \leqslant \bigvee X_1$, for some finite $X_1 \subseteq X$.

(ii) A complete lattice is called *algebraic* iff every element is the join of compact elements.

It is easy to see that every principal congruence relation is compact, which implies that for an arbitrary lattice L, Con L is an algebraic lattice.

Lemma. *Let L be an arbitrary lattice. Then* Con L *is a distributive algebraic lattice.*

The converse is a long-standing conjecture of lattice theory. We shall outline the proof for the finite case (R.P. Dilworth, G. Grätzer, E.T. Schmidt).

Theorem. *Let D be a finite distributive lattice. Then there exists a finite lattice L such that D is isomorphic to* Con L.

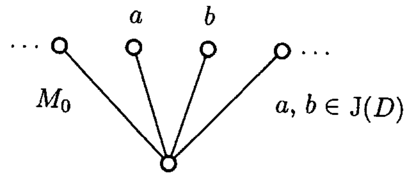

Fig. 9.

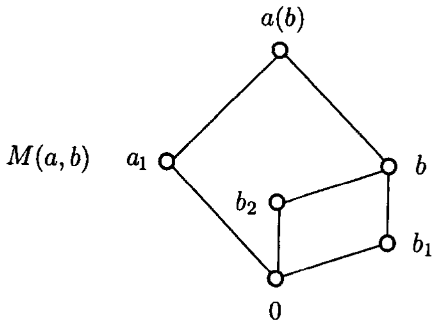

Fig. 10.

Let M be a finite poset such that $\inf\{a,b\}$ exists in M for any $a,b \in M$. We define in M: $a \wedge b = \inf\{a,b\}$ for all $a,b \in M$; and $a \wedge b = \sup\{a,b\}$ whenever $\sup\{a,b\}$ exists. This makes M into a *chopped lattice*. (From a finite lattice L with unit element 1, we can obtain a chopped lattice. $M - L - \{1\}$, and conversely). An equivalence relation Θ on M is a *congruence relation* iff $a_0 \equiv b_0$ (Θ) and $a_1 \equiv b_1$ (Θ) imply that $a_0 \wedge a_1 \equiv b_0 \wedge b_1$ (Θ) and that $a_0 \vee a_1 \equiv b_0 \vee b_1$ (Θ) whenever $a_0 \vee a_1$ and $b_0 \vee b_1$ both exist. Then the set $\mathrm{Con}\, M$ of all congruence relations is again a lattice.

Lemma 1. *Let D be a finite distributive lattice. Then there exists a chopped lattice M such that* $\mathrm{Con}\, M$ *is isomorphic to D.*

We outline the construction of M. Take the set $M_0 = \mathrm{J}(D) \cup \{0\}$, and make it a chopped lattice by defining $\inf\{a,b\} = 0$ if $a \neq b$, as illustrated in Fig. 9. Note that $a \equiv b$ (Θ) and $a \neq b$ imply in M_0 that $a \equiv 0$ (Θ) and $b \equiv 0$ (Θ); therefore, the congruence relations of M_0 are in one-to-one correspondence with subsets of $\mathrm{J}(D)$. Thus $\mathrm{Con}\, M_0$ is a Boolean lattice whose atoms are associated with elements of $\mathrm{J}(D)$; the congruence Φ_a associated with $a \in \mathrm{J}(D)$ can be described as follows: $a \equiv 0$ (Φ_a) and if $\{x,y\} \neq \{a,0\}$, then $x \equiv y$ (Φ_a) implies that $x = y$.

If $\mathrm{J}(D)$ is unordered, then we are ready. However, if, say, $a,b \in \mathrm{J}(D)$ and $a > b$ in D, then we must have $\Phi_a > \Phi_b$. we make this happen by using the lattice $M(a,b)$ of Fig. 10. Note that $M(a,b)$ has three congruence relations, namely, ω, ι, and Θ, where Θ is the congruence relation with congruence classes $\{0,b_1,b_2,b\}$ and $\{a_1,a(b)\}$. Thus

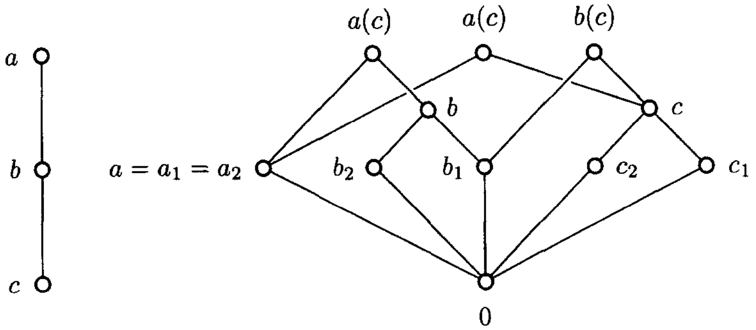

Fig. 11.

$\Theta(a_1, 0) = \iota$. In other words, $a_1 \equiv 0$ "implies" that $b_1 \equiv 0$, but $b_1 \equiv 0$ "does not imply" that $a_1 \equiv 0$.

We construct M by "inserting" $M(a,b)$ in M_0 whenever $a > b$ in $\mathrm{J}(D)$. Fig. 11 gives M if $\mathrm{J}(D)$ is the three-element chain.

For x, $y \in M$, let us define $x \leqslant y$ to mean that for some a, $b \in \mathrm{J}(D)$ with $a > b$, we have x, $y \in M(a,b)$ and $x \leqslant y$ in the lattice $M(a,b)$ as illustrated in Fig. 11. It is easily seen that $x \leqslant y$ does not depend on the choice of a and b, and that $\leqslant$ is a partial ordering relation under which M is a chopped lattice.

It is routine to check that $\mathrm{Con}\, M \cong D$.

The next lemma "completes" M to a lattice, while preserving the congruence lattice.

An *ideal* I of a chopped lattice M is a subset $I \subseteq M$ with the property that for $i \in I$ and $a \in M$, $i \wedge a \in I$ and for x, $y \in I$, $x \vee y \in I$ provided that $x \vee y$ exists in M. The ideals of M form a lattice $\mathrm{Id}\, M$.

Lemma 2 (G. Grätzer, H. Lakser). *Let M be a chopped lattice. Then for every congruence relation Θ of M, there exists exactly one congruence relation $\bar{\Theta}$ of* $\mathrm{Id}\, M$ *such that for a, $b \in M$,*

$$(a] \equiv (b] \; (\bar{\Theta}) \quad \textit{iff} \quad a \equiv b \; (\Theta).$$

The proof of the theorem is immediate from these two lemmas. For the finite distributive lattice D, take the chopped lattice M of Lemma 1; then M satisfies $\mathrm{Con}\, M \cong D$. Define the lattice L as $\mathrm{Id}\, M$. By Lemma 2, $\mathrm{Con}\, L \cong \mathrm{Con}\, M$. Hence $\mathrm{Con}\, L \cong D$. Since M is finite, so is L.