5. Congruence Relations

"You're young, Myrtle Mae. You've got a lot to learn, and I hope you never learn it."
– Vita in "Harvey"

You are doubtless familiar with the connection between homomorphisms and normal subgroups of groups. In this chapter we will establish the corresponding ideas for lattices (and other general algebras). Borrowing notation from group theory, if X is a set and θ an equivalence relation on X, for $x \in X$ let $x\theta$ denote the equivalence class $\{y \in X : x \; \theta \; y\}$, and let

$$X/\theta = \{x\theta : x \in X\}.$$

Thus the elements of X/θ are the equivalence classes of θ.

Recall that if $\mathcal{L}$ and $\mathcal{K}$ are lattices and $h : \mathcal{L} \to \mathcal{K}$ is a homomorphism, then the *kernel* of h is the induced equivalence relation,

$$\ker h = \{(x, y) \in L^2 : h(x) = h(y)\}.$$

We can define lattice operations naturally on the equivalence classes of $\ker h$, *viz.,* if $\theta = \ker h$, then

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

The homomorphism property shows that these operations are well defined, for if $(x, y) \in \ker h$ and $(r, s) \in \ker h$, then $h(x \vee r) = h(x) \vee h(r) = h(y) \vee h(s) = h(y \vee s)$, whence $(x \vee r, y \vee s) \in \ker h$. Moreover, $L/\ker h$ with these operations forms an algebra $\mathcal{L}/\ker h$ isomorphic to the image $h(\mathcal{L})$, which is a sublattice of $\mathcal{K}$. Thus $\mathcal{L}/\ker h$ is also a lattice.

Theorem 5.1. First Isomorphism Theorem. *Let $\mathcal{L}$ and $\mathcal{K}$ be lattices, and let $h : \mathcal{L} \to \mathcal{K}$ be a lattice homomorphism. Then $L/\ker h$ with the operations defined by (§) is a lattice $\mathcal{L}/\ker h$, which is isomorphic to the image $h(\mathcal{L})$ of $\mathcal{L}$ in $\mathcal{K}$.*

Let us define a *congruence relation* on a lattice $\mathcal{L}$ to be an equivalence relation θ such that $\theta = \ker h$ for some homomorphism h.[1] We have seen that, in addition to

[1] This is not the standard definition, but we are about to show it is equivalent to it.

being equivalence relations, congruence relations must preserve the operations of $\mathcal{L}$: if θ is a congruence relation, then

$$(\dagger) \qquad x \;\theta\; y \text{ and } r \;\theta\; s \text{ implies } x \vee r \;\theta\; y \vee s,$$

and analogously for meets. Note that (†) is equivalent for an equivalence relation θ to the apparently weaker, and easier to check, condition

$$(\dagger') \qquad x \;\theta\; y \text{ implies } x \vee z \;\theta\; y \vee z.$$

For (†) implies (†′) because every equivalence relation is reflexive, while if θ has the property (†′) and the hypotheses of (†) hold, then applying (†) twice yields $x \vee r \;\theta\; y \vee r \;\theta\; y \vee s$.

We want to show that, conversely, any equivalence relation satisfying (†′) and the corresponding implication for meets is a congruence relation.

Theorem 5.2. *Let $\mathcal{L}$ be a lattice, and let θ be an equivalence relation on L satisfying*

$$(\ddagger) \qquad \begin{aligned} &x \;\theta\; y \textit{ implies } x \vee z \;\theta\; y \vee z, \\ &x \;\theta\; y \textit{ implies } x \wedge z \;\theta\; y \wedge z. \end{aligned}$$

Define join and meet on L/θ by the formulas (§). Then $\mathcal{L}/\theta = (L/\theta, \wedge, \vee)$ is a lattice, and the map $h : \mathcal{L} \to \mathcal{L}/\theta$ defined by $h(x) = x\theta$ is a surjective homomorphism with $\ker h = \theta$.

Proof. The conditions (‡) ensure that the join and meet operations are well defined on L/θ. By definition, we have

$$h(x \vee y) = (x \vee y)\theta = x\theta \vee y\theta = h(x) \vee h(y)$$

and similarly for meets, so h is a homomorphism. The range of h is clearly L/θ.

It remains to show that $\mathcal{L}/\theta$ satisfies the equations defining lattices. This follows from the general principle that homomorphisms preserve the satisfaction of equations, i.e., if $h : \mathcal{L} \twoheadrightarrow \mathcal{K}$ is a surjective homomorphism and an equation $p = q$ holds in $\mathcal{L}$, then it holds in $\mathcal{K}$. (See Exercise 4.) For example, to check commutativity of meets, let $a, b \in K$. Then there exist $x, y \in L$ such that $h(x) = a$ and $h(y) = b$. Hence

$$\begin{aligned} a \wedge b = h(x) \wedge h(y) &= h(x \wedge y) \\ &= h(y \wedge x) = h(y) \wedge h(x) = b \wedge a. \end{aligned}$$

Similar arguments allow us to verify the commutativity of joins, the idempotence and associativity of both operations, and the absorption laws. Thus a homomorphic image of a lattice is a lattice.[2] As $h : \mathcal{L} \to \mathcal{L}/\theta$ is a surjective homomorphism, we conclude that $\mathcal{L}/\theta$ is a lattice, which completes the proof. $\square$

Thus congruence relations are precisely equivalence relations that satisfy (‡). But the conditions of (‡) and the axioms for an equivalence relation are all finitary closure rules on L^2. Hence, by Theorem 3.1, the set of congruence relations on a lattice $\mathcal{L}$ forms an algebraic lattice $\mathbf{Con}\,\mathcal{L}$. The closure operator on L^2 that gives the congruence generated by a set of pairs is denoted by "con" or sometimes "Cg." So, with the former notation, for a set Q of ordered pairs, con Q is the congruence relation generated by Q; for a single pair, $Q = \{(a, b)\}$, we write just $\mathrm{con}(a, b)$.

Moreover, the equivalence relation join (the transitive closure of the union) of a set of congruence relations again satisfies (‡). For if θ_i $(i \in I)$ are congruence relations and $x\,\theta_{i_1}\,r_1\,\theta_{i_2}\,r_2\,\ldots\,\theta_{i_n}\,y$, then $x \vee z\,\theta_{i_1}\,r_1 \vee z\,\theta_{i_2}\,r_2 \vee z\,\ldots\,\theta_{i_n}\,y \vee z$, and likewise for meets. Thus the transitive closure of $\bigcup_{i\in I}\theta_i$ is a congruence relation, and so it is the join $\bigvee_{i\in I}\theta_i$ in $\mathbf{Con}\,\mathcal{L}$. Since the meet is also the same (set intersection) in both lattices, $\mathbf{Con}\,\mathcal{L}$ is a complete sublattice of $\mathbf{Eq}\,L$.

Theorem 5.3. $\mathbf{Con}\,\mathcal{L}$ *is an algebraic lattice. A congruence relation* θ *is compact in* $\mathbf{Con}\,\mathcal{L}$ *if and only if it is finitely generated, i.e., there exist finitely many pairs* $(a_1, b_1), \ldots, (a_k, b_k)$ *of elements of* L *such that* $\theta = \bigvee_{1\le i\le k}\mathrm{con}(a_i, b_i)$.

Note that the universal relation and the equality relation on L^2 are both congruence relations; they are the greatest and least elements of $\mathbf{Con}\,\mathcal{L}$, respectively. Also, since $x\ \theta\ y$ if and only if $x \wedge y\ \theta\ x \vee y$, a congruence relation is determined by the ordered pairs (a, b) with $a < b$ which it contains.

A subset $S \subseteq \mathcal{L}$ is *convex* if $x \le y \le z$ and $x,\ z \in S$ implies $y \in S$. The reader should verify that *if* θ *is a congruence relation on a lattice* $\mathcal{L}$*, then every congruence class is a convex sublattice of* $\mathcal{L}$*.* This observation helps immensely in computing lattice congruences.

A congruence relation θ is *principal* if $\theta = \mathrm{con}(a, b)$ for some pair $a,\ b \in L$. The principal congruence relations are join dense in $\mathbf{Con}\,\mathcal{L}$: for any congruence relation θ, we have

$$\theta = \bigvee\{\mathrm{con}(a, b) : a\ \theta\ b\}.$$

It follows from the general theory of algebraic closure operators that principal congruence relations are compact, but this can be shown directly as follows: if $\mathrm{con}(a, b) \le \bigvee_{i\in I}\theta_i$, then there exist elements $c_1, \ldots, c_m$ and indices $i_0, \ldots, i_m$ such that

$$a\ \theta_{i_0}\ c_1\ \theta_{i_1}\ c_2 \ldots \theta_{i_m}\ b\ ,$$

whence $(a, b) \in \theta_{i_0} \vee \ldots \vee \theta_{i_m}$ and thus $\mathrm{con}(a, b) \le \bigvee_{0\le j\le m}\theta_{i_j}$.

One of the most basic facts about congruences says that congruences of $\mathcal{L}/\theta$ correspond to congruences on $\mathcal{L}$ containing θ.

[2]The corresponding statement is true for any equationally defined class of algebras, including modular, Arguesian and distributive lattices.

Theorem 5.4. Second Isomorphism Theorem. *If $\theta \in \mathbf{Con}\,\mathcal{L}$, then $\mathbf{Con}\,(\mathcal{L}/\theta)$ is isomorphic to the filter $\uparrow\theta$ in $\mathbf{Con}\,\mathcal{L}$, i.e., $\mathbf{Con}\,(\mathcal{L}/\theta) \cong \{\varphi \in \mathbf{Con}\,\mathcal{L} : \varphi \geq \theta\}$.*

Proof. A congruence relation on $\mathcal{L}/\theta$ is an equivalence relation R on the θ-classes of L such that

$$x\theta\; R\; y\theta \quad \text{implies} \quad x\theta \vee z\theta\; R\; y\theta \vee z\theta$$

and analogously for meets. Given $R \in \mathbf{Con}\,\mathcal{L}/\theta$, define the corresponding relation ρ on L by $x\,\rho\,y$ iff $x\theta\; R\; y\theta$. Clearly $\rho \in \mathbf{Eq}\; L$ and $\theta \leq \rho$. Moreover, if $x\,\rho\,y$ and $z \in L$, then

$$(x \vee z)\theta \;=\; x\theta \vee z\theta\; R\; y\theta \vee z\theta \;=\; (y \vee z)\theta,$$

whence $x \vee z\;\; \rho\;\; y \vee z$, and similarly for meets. Hence $\rho \in \mathbf{Con}\,\mathcal{L}$, and we have established an order preserving map $f : \mathbf{Con}\,\mathcal{L}/\theta \to \uparrow\theta$.

Conversely, let $\sigma \in \uparrow\theta$ in $\mathbf{Con}\,\mathcal{L}$, and define a relation S on L/θ by $x\theta\; S\; y\theta$ iff $x\,\sigma\,y$. Since $\theta \leq \sigma$ the relation S is well defined. If $x\theta\; S\; y\theta$ and $z \in L$, then $x\,\sigma\,y$ implies $x \vee z\,\sigma\,y \vee z$, whence

$$x\theta \vee z\theta \;=\; (x \vee z)\theta\; S\; (y \vee z)\theta \;=\; y\theta \vee z\theta,$$

and likewise for meets. Thus S is a congruence relation on $\mathcal{L}/\theta$. This gives us an order preserving map $g : \uparrow\theta \to \mathbf{Con}\,\mathcal{L}/\theta$.

The definitions make f and g inverse maps, so they are in fact isomorphisms. □

It is interesting to interpret Theorem 5.4 in terms of homomorphisms. Essentially it corresponds to the fact that *if $h : \mathcal{L} \twoheadrightarrow \mathcal{K}$ and $f : \mathcal{L} \to \mathcal{M}$ are homomorphisms with h surjective, then there is a homomorphism $g : \mathcal{K} \to \mathcal{M}$ with $f = gh$ if and only if* $\ker h \;\leq\; \ker f$. This version of the Second Isomorphism Theorem will be used repeatedly in Chapters 6 and 7.

A lattice $\mathcal{L}$ is called *simple* if $\mathbf{Con}\;\mathcal{L}$ is a two element chain, i.e., $|L| > 1$ and $\mathcal{L}$ has no congruences except equality and the universal relation. For example, the two-dimensional modular lattice $\mathcal{M}_n$ is simple whenever $n \geq 3$. A lattice is *subdirectly irreducible* if it has a unique minimum nonzero congruence relation, i.e., if 0 is completely meet irreducible in $\mathbf{Con}\,\mathcal{L}$. So every simple lattice is subdirectly irreducible, and $\mathcal{N}_5$ is an example of a subdirectly irreducible lattice that is not simple .

The following are immediate consequences of the Second Isomorphism Theorem.

Corollary. *$\mathcal{L}/\theta$ is simple if and only if $1 \succ \theta$ in $\mathbf{Con}\,\mathcal{L}$.*

Corollary. *$\mathcal{L}/\theta$ is subdirectly irreducible if and only if θ is completely meet irreducible in $\mathbf{Con}\,\mathcal{L}$.*

Now we turn our attention to a decomposition of lattices which goes back to R. Remak in 1930 (for groups) [10]. In what follows, it is important to remember that the zero element of a congruence lattice is the equality relation.

Theorem 5.5. *If $0 = \bigwedge_{i \in I} \theta_i$ in* **Con** *$\mathcal{L}$, then $\mathcal{L}$ is isomorphic to a sublattice of the direct product $\prod_{i \in I} \mathcal{L}/\theta_i$, and each of the natural homomorphisms $\pi_i : \mathcal{L} \to \mathcal{L}/\theta_i$ is surjective.*

Conversely, if $\mathcal{L}$ is isomorphic to a sublattice of a direct product $\prod_{i \in I} \mathcal{K}_i$ and each of the projection homomorphisms $\pi_i : \mathcal{L} \to \mathcal{K}_i$ is surjective, then $\mathcal{K}_i \cong \mathcal{L}/\ker \pi_i$ and $\bigwedge_{i \in I} \ker \pi_i = 0$ in **Con** *$\mathcal{L}$.*

Proof. For any collection θ_i $(i \in I)$ in **Con** $\mathcal{L}$, there is a natural homomorphism $\pi : \mathcal{L} \to \prod \mathcal{L}/\theta_i$ with $(\pi(x))_i = x\theta_i$. Since two elements of a direct product are equal if and only if they agree in every component, $\ker \pi = \bigwedge \theta_i$. So if $\bigwedge \theta_i = 0$, then π is an embedding.

Conversely, if $\pi : \mathcal{L} \to \prod \mathcal{K}_i$ is an embedding, then $\ker \pi = 0$, while as above $\ker \pi = \bigwedge \ker \pi_i$. Clearly, if $\pi_i(\mathcal{L}) = \mathcal{K}_i$ then $\mathcal{K}_i \cong \mathcal{L}/\ker \pi_i$. □

A representation of $\mathcal{L}$ satisfying either of the equivalent conditions of Theorem 5.5 is called a *subdirect decomposition*, and the corresponding external construction is called a *subdirect product*. For example, Figure 5.1 shows how a six element lattice $\mathcal{L}$ can be written as a subdirect product of two copies of $\mathcal{N}_5$.

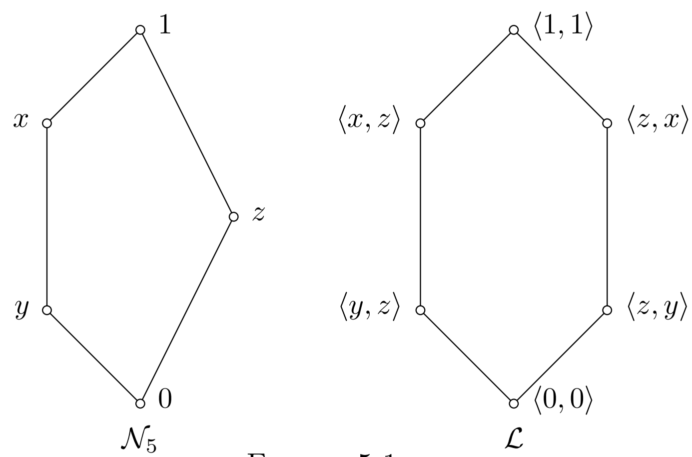

Figure 5.1

Next we should show that subdirectly irreducible lattices are indeed those that have no proper subdirect decomposition.

Theorem 5.6. *The following are equivalent for a lattice $\mathcal{L}$.*

(1) *$\mathcal{L}$ is subdirectly irreducible, i.e., 0 is completely meet irreducible in* **Con** *$\mathcal{L}$.*
(2) *There is a unique minimal nonzero congruence μ on $\mathcal{L}$ with the property that $\theta \geq \mu$ for every nonzero $\theta \in$* **Con** *$\mathcal{L}$.*
(3) *If $\mathcal{L}$ is isomorphic to a sublattice of $\prod \mathcal{K}_i$, then some projection homomorphism π_i is one-to-one.*
(4) *There exists a pair of elements $a < b$ in $\mathcal{L}$ such that $a \; \theta \; b$ for every nonzero congruence θ.*

The congruence μ of condition (2) is called the *monolith* of the subdirectly irreducible lattice $\mathcal{L}$, and the pair (a, b) of condition (4), which need not be unique, is called a *critical pair*.

Proof. The equivalence of (1), (2) and (3) is a simple combination of Theorems 3.8 and 5.5. We get (2) implies (4) by taking $a = x \wedge y$ and $b = x \vee y$ for any pair of distinct elements with $x \, \mu \, y$. On the other hand, if (4) holds we obtain (2) with $\mu = \text{con}(a, b)$. $\square$

Now we see the beauty of Birkhoff's Theorem 3.9, that every element in an algebraic lattice is a meet of completely meet irreducible elements. By applying this to the zero element of $\mathbf{Con}\,\mathcal{L}$, we obtain the following fundamental result.

Theorem 5.7. *Every lattice is a subdirect product of subdirectly irreducible lattices.*

It should be clear that, with the appropriate modifications, Theorems 5.5 to 5.7 yield subdirect decompositions of groups, rings, semilattices, etc. into subdirectly irreducible algebras of the same type. Keith Kearnes [8] has shown that there are interesting varieties of algebras whose congruence lattices are strongly atomic. By Theorem 3.10, these algebras have irredundant subdirect decompositions.

Subdirectly irreducible lattices play a particularly important role in the study of varieties; see Chapter 7.

So far we have just done universal algebra with lattices: with the appropriate modifications, we can characterize congruence relations and show that $\mathbf{Con}\,\mathcal{A}$ is an algebraic lattice for any algebra $\mathcal{A}$. (See Exercises 10 and 11.) However, the next property is special to lattices and related structures. It was first discovered by N. Funayama and T. Nakayama [5] in the early 1940's.

Theorem 5.8. *If $\mathcal{L}$ is a lattice, then* $\mathbf{Con}\,\mathcal{L}$ *is a distributive algebraic lattice.*

Proof. In any lattice $\mathcal{L}$, let

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

Then it is easy to see that $m(x, y, z)$ is a *majority polynomial*, in that if any two variables are equal then $m(x, y, z)$ takes on that value:

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

Now let $\alpha, \beta, \gamma \in \mathbf{Con}\,\mathcal{L}$. Clearly $(\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \leq \alpha \wedge (\beta \vee \gamma)$. To show the reverse inclusion, let $(x, z) \in \alpha \wedge (\beta \vee \gamma)$. Then $x \, \alpha \, z$ and there exist $y_1, \ldots, y_k$ such that

$$x = y_0 \; \beta \; y_1 \; \gamma \; y_2 \; \beta \ldots y_k = z\,.$$

Let $t_i = m(x, y_i, z)$ for $0 \leq i \leq k$. Then

$$t_0 = m(x, x, z) = x$$
$$t_k = m(x, z, z) = z$$

and for all i,

$$t_i = m(x, y_i, z) \; \alpha \; m(x, y_i, x) = x \; ,$$

so $t_i \, \alpha \, t_{i+1}$ by Exercise 4(b). If i is even, then

$$t_i = m(x, y_i, z) \; \beta \; m(x, y_{i+1}, z) = t_{i+1} \; ,$$

whence $t_i \; \alpha \wedge \beta \; t_{i+1}$. Similarly, if i is odd then $t_i \; \alpha \wedge \gamma \; t_{i+1}$. Thus

$$x = t_0 \; \alpha \wedge \beta \; t_1 \; \alpha \wedge \gamma \; t_2 \; \alpha \wedge \beta \ldots t_k = z$$

and we have shown that $\alpha \wedge (\beta \vee \gamma) \leq (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$. As inclusion holds both ways, we have equality. Therefore **Con** $\mathcal{L}$ is distributive. □

In the 1940's, R.P. Dilworth proved that every finite distributive lattice is isomorphic to the congruence lattice of a lattice. (This result appeared as a (starred) exercise in the 1948 edition of Birkhoff's *Lattice Theory* book.) For a long time thereafter, it was conjectured that every distributive algebraic lattice was the congruence lattice of a lattice, and evidence in favor of the conjecture was amassed. A distributive algebraic lattice $\mathcal{D}$ is isomorphic to the congruence lattice of a lattice if

(i) $\mathcal{D} \cong \mathcal{O}(\mathcal{P})$ for some ordered set $\mathcal{P}$ (R. P. Dilworth, see [6]), or
(ii) the compact elements are a sublattice of $\mathcal{D}$ (E. T. Schmidt [12]), or
(iii) $\mathcal{D}$ has at most $\aleph_1$ compact elements (A. Huhn [7]).

In Chapter 10 we will prove (i), which includes the fact that every finite distributive lattice is isomorphic to the congruence lattice of a (finite) lattice.

But in 2005, Fred Wehrung constructed distributive algebraic lattices that are not isomorphic to congruence lattices of lattices [15]. Wehrung's original counterexamples have $\aleph_{\omega+1}$ or more compact elements, but Pavel Růžička refined Wehrung's arguments to produce a counterexample with $\aleph_2$ compact elements [11].

This completely settles the problem for lattices, but it remains an open question whether every distributive algebraic lattice is isomorphic to the congruence lattice of an algebra with finitely many operations. Surveys on this problem, but pre-dating Wehrung's results, can be found in M. Tischendorf [13] and M. Ploščica, J. Tůma and F. Wehrung [9], [15].

We need to understand the congruence operator $\operatorname{con} Q$, where Q is a set of pairs, a little better. A *weaving polynomial* on a lattice $\mathcal{L}$ is a member of the set W of unary functions defined recursively by

(1) $w(x) = x \in W$,
(2) if $w(x) \in W$ and $a \in L$, then $u(x) = w(x) \wedge a$ and $v(x) = w(x) \vee a$ are in W,
(3) only these functions are in W.

Thus every weaving polynomial looks something like

$$w(x) = (\dots(((x \wedge s_1) \vee s_2) \wedge s_3)\dots) \vee s_k$$

where $s_i \in L$ for $1 \le i \le k$. The following characterization is a modified version of one found in Dilworth [2].

Theorem 5.9. *Suppose $a_i < b_i$ for $i \in I$. Then $(x, y) \in \bigvee_{i \in I} \operatorname{con}(a_i, b_i)$ if and only if there exist finitely many $r_j \in L$, $w_j \in W$, and $i_j \in I$ such that*

$$x \vee y = r_0 \ge r_1 \ge \cdots \ge r_k = x \wedge y$$

with $w_j(b_{i_j}) = r_j$ and $w_j(a_{i_j}) = r_{j+1}$ for $0 \le j < k$.

Proof. Let R be the set of all pairs (x, y) satisfying the condition of the theorem. It is clear that

(1) $(a_i, b_i) \in R$ for all i,
(2) $R \subseteq \bigvee_{i \in I} \operatorname{con}(a_i, b_i)$.

Hence, if we can show that R is a congruence relation, it will follow that $R = \bigvee_{i \in I} \operatorname{con}(a_i, b_i)$.

Note that $(x, y) \in R$ if and only if $(x \wedge y, x \vee y) \in R$. It also helps to observe that if $x \, R \, y$ and $x \le u \le v \le y$, then $u \, R \, v$. To see this, replace the weaving polynomials $w(t)$ witnessing $x \, R \, y$ by new polynomials $w'(t) = (w(t) \vee u) \wedge v$.

First we must show $R \in \mathbf{Eq}\ L$. Reflexivity and symmetry are obvious, so let $x \, R \, y \, R \, z$ with

$$x \vee y = r_0 \ge r_1 \ge \cdots \ge r_k = x \wedge y$$

using polynomials $w_j \in W$, and

$$y \vee z = s_0 \ge s_1 \ge \cdots \ge s_m = y \wedge z$$

via polynomials $v_j \in W$, as in the statement of the theorem. Replacing $w_j(t)$ by $w_j'(t) = w_j(t) \vee y \vee z$, we obtain

$$x \vee y \vee z = r_0 \vee y \vee z \ge r_1 \vee y \vee z \ge \cdots \ge (x \wedge y) \vee y \vee z = y \vee z.$$

Likewise, replacing $w_j(t)$ by $w_j''(t) = w_j(t) \wedge y \wedge z$, we have

$$y \wedge z = (x \vee y) \wedge y \wedge z \ge r_1 \wedge y \wedge z \ge \cdots \ge r_k \wedge y \wedge z = x \wedge y \wedge z.$$

Combining the two new sequences with the original one for $y \, R \, z$, we get a sequence from $x \vee y \vee z$ down to $x \wedge y \wedge z$. Hence $x \wedge y \wedge z \; R \; x \vee y \vee z$. By the observations above, $x \wedge z \; R \; x \vee z$ and $x \, R \, z$, so R is transitive.

Now we must check (‡). Let $x \, R \, y$ as before, and let $z \in L$. Replacing $w_j(t)$ by $u_j(t) = w_j(t) \vee z$, we obtain a sequence from $x \vee y \vee z$ down to $(x \wedge y) \vee z$. Thus $(x \wedge y) \vee z \; R \; x \vee y \vee z$, and since $(x \wedge y) \vee z \le (x \vee z) \wedge (y \vee z) \le x \vee y \vee z$, this implies $x \vee z \; R \; y \vee z$. The argument for meets is done similarly, and we conclude that R is a congruence relation, as desired. □

The condition of Theorem 5.9 is a bit unwieldy, but not as bad to use as you might think. Let us look at some consequences of the theorem.

Corollary. *If* $\theta_i \in \mathbf{Con}\,\mathcal{L}$ *for* $i \in I$*, then* $(x, y) \in \bigvee_{i \in I} \theta_i$ *if and only if there exist finitely many* $r_j \in L$ *and* $i_j \in I$ *such that*

$$x \vee y = r_0 \geq r_1 \geq \cdots \geq r_k = x \wedge y$$

and $r_j \; \theta_{i_j} \; r_{j+1}$ *for* $0 \leq j < k$*.*

At this point we need some basic facts about distributive algebraic lattices (like **Con** $\mathcal{L}$). Recall that an element p of a complete lattice is *completely join irreducible* if $p = \bigvee Q$ implies $p = q$ for some $q \in Q$. An element p is *completely join prime* if $p \leq \bigvee Q$ implies $p \leq q$ for some $q \in Q$. Clearly every completely join prime element is completely join irreducible, but in general completely join irreducible elements need not be join prime.

Now every algebraic lattice has lots of completely meet irreducible elements (by Theorem 3.9), but they may have no completely join irreducible elements. This happens, for example, in the lattice consisting of the empty set and all cofinite subsets of an infinite set (which is distributive and algebraic). However, such completely join irreducible elements as there are in a distributive algebraic lattice are completely join prime!

Theorem 5.10. *The following are equivalent for an element* p *in an algebraic distributive lattice.*

(1) *p is completely join prime.*
(2) *p is completely join irreducible.*
(3) *p is compact and (finitely) join irreducible.*

Proof. Clearly (1) implies (2), and since every element in an algebraic lattice is a join of compact elements, (2) implies (3).

Let p be compact and finitely join irreducible, and assume $p \leq \bigvee Q$. As p is compact, $p \leq \bigvee F$ for some finite subset $F \subseteq Q$. By distributivity, this implies $p = p \wedge (\bigvee F) = \bigvee_{q \in F} p \wedge q$. Since p is join irreducible, $p = p \wedge q \leq q$ for some $q \in F$. Thus p is completely join prime. (Cf. Exercise 3.1) □

We will return to the theory of distributive lattices in Chapter 8, but let us now apply what we know to **Con** $\mathcal{L}$. As an immediate consequence of the Corollary to Theorem 5.9 we have the following.

Theorem 5.11. *If* $a \prec b$*, then* $\operatorname{con}(a, b)$ *is completely join prime in* **Con** $\mathcal{L}$*.*

The converse is false, as there are infinite simple lattices with no covering relations (E. T. Schmidt). However, for finite lattices, or more generally principally chain finite lattices, the converse does hold. A lattice is *principally chain finite* if every principal ideal $\downarrow c$ satisfies the ACC and DCC. This is a fairly natural finiteness condition that includes many interesting infinite lattices, and many results for finite lattices can be extended to principally chain finite lattices with a minimum of effort. Recall that if x is a join irreducible element in such a lattice, then x_* denotes the unique element such that $x \succ x_*$.

Theorem 5.12. *Let $\mathcal{L}$ be a principally chain finite lattice. Then every congruence relation on $\mathcal{L}$ is the join of completely join irreducible congruences. Moreover, every completely join irreducible congruence is of the form $\mathrm{con}(x, x_*)$ for some join irreducible element x of $\mathcal{L}$.*

Proof. Every congruence relation is a join of compact congruences, and every compact congruence is a join of finitely many congruences $\mathrm{con}(a, b)$ with $a > b$. In a principally chain finite lattice, every chain in a/b is finite by Exercise 1.5, so there exists a covering chain $a = r_0 \succ r_1 \succ \cdots \succ r_k = b$. Clearly $\mathrm{con}(a, b) = \bigvee_{0 \leq j < k} \mathrm{con}(r_j, r_{j+1})$, and these latter are completely join prime by Theorem 5.11. Thus every congruence relation on $\mathcal{L}$ is the join of completely join irreducible congruences $\mathrm{con}(r, s)$ with $r \succ s$.

Now let $a \succ b$ be any covering pair in $\mathcal{L}$. By the DCC for $\downarrow a$, there is an element x that is minimal with respect to the properties $x \leq a$ and $x \not\leq b$. Since any element strictly below x is below b, the element x is join irreducible and $x_* = x \wedge b$. It is also true that $a = x \vee b$, since $b < x \vee b \leq a$, and it follows easily from these two facts that $\mathrm{con}(a, b) = \mathrm{con}(x, x_*)$. □

There is much more to be said about congruence lattices of finite lattices, or more generally, principally chain finite lattices. We will return to these matters in Chapter 10. See also the references there.

We have ignored congruence lattices of semilattices, interesting on their own and applicable in universal algebra. Unlike congruence lattices of lattices, which are distributive, congruence lattices of semilattices satisfy no lattice identities. For the basic results, see Freese and Nation [4], Fajtlowicz and Schmidt [3], and Adaricheva [1].

Exercises for Chapter 5

1. Find **Con** $\mathcal{L}$ for the lattices (a) $\mathcal{M}_n$ where $n \geq 3$, (b) $\mathcal{N}_5$, (c) the lattice $\mathcal{L}$ of Figure 5.1, and the lattices in Figure 5.2.

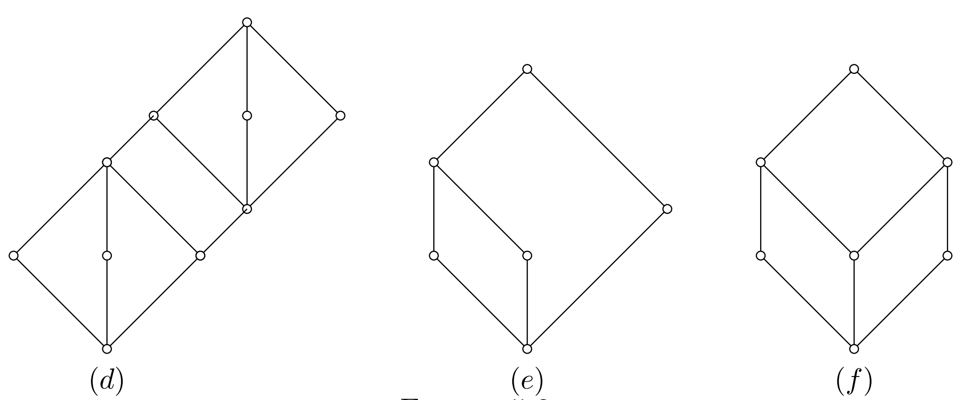

Figure 5.2

2. An element p of a lattice $\mathcal{L}$ is *join prime* if for any finite subset F of L, $p \leq \bigvee F$ implies $p \leq f$ for some $f \in F$. Let $\mathrm{P}(\mathcal{L})$ denote the set of join prime elements of $\mathcal{L}$, and define

$$x \,\Delta\, y \qquad \text{iff} \qquad \downarrow x \cap \mathrm{P}(\mathcal{L}) = \downarrow y \cap \mathrm{P}(\mathcal{L}).$$

Prove that Δ is a congruence relation on $\mathcal{L}$.

3. Let X be any set. Define a binary relation on $\mathfrak{P}(X)$ by $A \approx B$ iff the symmetric difference $(A - B) \cup (B - A)$ is finite. Prove that $\approx$ is a congruence relation on $\mathfrak{P}(X)$.

4. Lattice *terms* are defined in the proof of Theorem 6.1.

(a) Show that if $p(x_1, \ldots, x_n)$ is a lattice term and $h : \mathcal{L} \to \mathcal{K}$ is a homomorphism, then $h(p(a_1, \ldots, a_n)) = p(h(a_1), \ldots, h(a_n))$ for all $a_1, \ldots, a_n \in L$.

(b) Show that if $p(x_1, \ldots, x_n)$ is a lattice term and $\theta \in \mathbf{Con}\,\mathcal{L}$ and $a_i \;\theta\; b_i$ for $1 \leq i \leq n$, then $p(a_1, \ldots, a_n) \;\theta\; p(b_1, \ldots, b_n)$.

(c) Let $p(x_1, \ldots, x_n)$ and $q(x_1, \ldots, x_n)$ be lattice terms, and let $h : \mathcal{L} \twoheadrightarrow \mathcal{K}$ be a surjective homomorphism. Prove that if $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$ for all $a_1, \ldots, a_n \in L$, then $p(c_1, \ldots, c_n) = q(c_1, \ldots, c_n)$ holds for all $c_1, \ldots, c_n \in K$.

5. Show that each element of a finite distributive lattice has a unique irredundant decomposition. What does this say about subdirect decompositions of finite lattices?

6. Let $\theta \in \mathbf{Con}\,\mathcal{L}$.

(a) Show that $x \succ y$ implies $x\theta \succ y\theta$ or $x\theta = y\theta$.

(b) Prove that if $\mathcal{L}$ is a finite semimodular lattice, then so is $\mathcal{L}/\theta$.

(c) Prove that a subdirect product of semimodular lattices is semimodular.

7. Let $\mathcal{L}$ be a finitely generated lattice, and let θ be a congruence on $\mathcal{L}$ such that $\mathcal{L}/\theta$ is finite. Prove that θ is compact.

8. Prove that $\mathbf{Con}\,\mathcal{L}_1 \times \mathcal{L}_2 \;\cong\; \mathbf{Con}\,\mathcal{L}_1 \times \mathbf{Con}\,\mathcal{L}_2$. (Note that this is not true for groups; see Exercise 9.)

9. Find the congruence lattice of the abelian group $Z_p \times Z_p$, where p is prime. Find all finite abelian groups whose congruence lattice is distributive. (Recall that the congruence lattice of an abelian group is isomorphic to its subgroup lattice.)

For Exercises 10 and 11 we refer to §3 (Universal Algebra) of Appendix 1.

10. Let $\mathcal{A} = \langle A; \mathcal{F}, \mathcal{C} \rangle$ be an algebra.

(a) Prove that if $h : \mathcal{A} \to \mathcal{B}$ is a homomorphism and $\theta = \ker h$, then for each $f \in \mathcal{F}$,

$$(\yen) \qquad x_i \,\theta\, y_i \text{ for } 1 \leq i \leq n \quad \text{implies} \quad f(x_1, \ldots, x_n) \;\theta\; f(y_1, \ldots, y_n).$$

(b) Prove that (¥) is equivalent to the apparently weaker condition that for all $f \in \mathcal{F}$ and every i,

$$(\$) \qquad x_i \,\theta\, y \quad \text{implies} \quad f(x_1, \ldots, x_i, \ldots x_n) \;\theta\; f(x_1, \ldots, y, \ldots x_n).$$

(c) Show that if $\theta \in \mathbf{Eq}\,A$ satisfies (¥), then the natural map $h : \mathcal{A} \to \mathcal{A}/\theta$ is a homomorphism with $\theta = \ker h$.

Thus congruence relations, defined as homomorphism kernels, are precisely equivalence relations satisfying (¥).

11. Accordingly, let $\mathbf{Con}\,\mathcal{A} = \{\theta \in \mathbf{Eq}\,A : \theta \text{ satisfies } (¥)\}$.

(a) Prove that $\mathbf{Con}\,\mathcal{A}$ is a complete sublattice of $\mathbf{Eq}\,A$. (In particular, you must show that $\bigvee$ and $\bigwedge$ are the same in both lattices.)

(b) Show that $\mathbf{Con}\,\mathcal{A}$ is an algebraic lattice.

12. Let $\mathcal{A} = \mathcal{B} \times \mathcal{C}$ be a direct product of two algebras. Let π_1 and π_2 denote the kernels of the projections onto $\mathcal{B}$ and $\mathcal{C}$. Prove that:

(i) $\mathcal{A}/\pi_1 \cong \mathcal{B}$ and $\mathcal{A}/\pi_2 \cong \mathcal{C}$.

(ii) In $\mathbf{Con}\,\mathcal{A}$, $\pi_1 \wedge \pi_2 = 0$ and $\pi_1 \vee \pi_2 = \pi_1 \circ \pi_2 = \pi_2 \circ \pi_1 = 1$.

Conversely, let $\mathcal{A}$ be an algebra with congruences φ_1 and φ_2 satisfying the analogues of the properties in (ii). Prove that $\mathcal{A} \cong \mathcal{A}/\varphi_1 \times \mathcal{A}/\varphi_2$.

References

1. K. V. Adaricheva, *A characterization of congruence lattices of finite semilattices*, Algebra i Logika **35** (1996), 3–30.
2. R. P. Dilworth, *The structure of relatively complemented lattices*, Ann. of Math. **51** (1950), 348–359.
3. S. Fajtlowicz and J. Schmidt, *Bézout families, join-congruences and meet-irreducible ideals*, Lattice Theory (Proc. Colloq., Szeged, 1974),Colloq. Math. Soc. Janos Bolyai, Vol. 14, North Holland, Amsterdam, 1976, pp. 51–76.
4. R. Freese and J. B. Nation, *Congruence lattices of semilattices*, Pacific J. Math. **49** (1973), 51–58.
5. N. Funayama and T. Nakayama, *On the distributivity of a lattice of lattice-congruences*, Proc. Imp. Acad. Tokyo **18** (1942), 553–554.
6. G. Grätzer and E. T. Schmidt, *On congruence lattices of lattices*, Acta Math. Acad. Sci. Hungar. **13** (1962), 179–185.
7. A. Huhn, *On the representation of distributive algebraic lattices I–III*, Acta Sci. Math. (Szeged), **45** (1983), 239–246; **53** (1989), 3–10 and 11–18.
8. K. A. Kearnes, *Atomicity and Nilpotence*, Canadian J. Math. **42** (1990), 1–18.
9. M. Ploščica, J. Tůma and F. Wehrung, *Congruence lattices of free lattices in nondistributive varieties*, Coll. Math. **76** (1998), 269–278.
10. R. Remak, *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produckte*, Jour. für Math. **163** (1930), 1–44.
11. P. Růžička, *Free trees and the optimal bound in Wehrung's theorem*, Fund. Math. **198** (2008), 217–228.
12. E. T. Schmidt, *The ideal lattice of a distributive lattice with* 0 *is the congruence lattice of a lattice*, Acta Sci. Math. (Szeged). **43** (1981), 153–168.
13. M. Tischendorf, *On the representation of distributive semilattices*, Algebra Universalis **31** (1994), 446-455.
14. J. Tůma and F. Wehrung, *A survey on recent results on congruence lattices of lattices*, Algebra Universalis **45** (2002), 439-471.
15. F. Wehrung, *A solution to Dilworth's congruence lattice problem*, Adv. Math. **216** (2007), 610–625.