Introduction to Lattices and Order

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Introducing Congruences

Equivalence Relations and Partitions

- An **equivalence relation** on a set A is a binary relation on A which is reflexive, symmetric and transitive.
- We write $a \equiv b \pmod{\theta}$ or $a \ \theta \ b$ to indicate that a and b are related under the relation θ;

  We use instead the notation $(a, b) \in \theta$ where it is appropriate to be formally correct and to regard θ as a subset of $A \times A$.
- An equivalence relation θ on A gives rise to a partition of A into non-empty disjoint subsets. These subsets are the **equivalence classes** or **blocks** of θ. A typical block is of the form

$$[a]_\theta := \{x \in A : x \equiv a \pmod{\theta}\}.$$

- In the opposite direction, a partition of A into a union of non-empty disjoint subsets gives rise to an equivalence relation whose blocks are the subsets in the partition.

The Group Case

- Let G and H be groups and $f : G \to H$ be a group homomorphism.
- We may define an equivalence relation θ on G by

$$(\forall a, b \in G)\ a \equiv b \pmod{\theta} \iff f(a) = f(b).$$

- This relation and the partition of G it induces satisfy:
  (1) The relation θ is compatible with the group operation in the sense that, for all $a, b, c, d \in G$,

  $$a \equiv b \pmod{\theta}\ \&\ c \equiv d \pmod{\theta}\ \Rightarrow\ ac \equiv bd \pmod{\theta}.$$

  (2) The block $N = [1]_\theta := \{g \in G : g \equiv 1 \pmod{\theta}\}$ is a normal subgroup of G.
  (3) For each $a \in G$, the block $[a]_\theta := \{g \in G : g \equiv a \pmod{\theta}\}$ equals the (left) coset $aN := \{an : n \in N\}$.
  (4) The definition $$[a]_\theta[b]_\theta := [ab]_\theta, \text{ for all } a, b \in G,$$
  yields a well-defined group operation on $\{[a]_\theta : a \in G\}$;
  By (2), (3), the resulting group is the quotient group G/N and, by the Homomorphism Theorem, is isomorphic to the subgroup $f(G)$ of H.

Compatibility with Join and Meet

- We say that an equivalence relation θ on a lattice L is **compatible with join and meet** if, for all $a, b, c, d \in L$,

$$a \equiv b \pmod{\theta} \quad \text{and} \quad c \equiv d \pmod{\theta}$$

  imply

$$a \vee c \equiv b \vee d \pmod{\theta} \quad \text{and} \quad a \wedge c \equiv b \wedge d \pmod{\theta}.$$

Lemma

Let L and K be lattices and let $f : L \to K$ be a lattice homomorphism. Then the equivalence relation θ defined on L by

$$(\forall a, b \in L)\ a \equiv b \pmod{\theta} \Longleftrightarrow f(a) = f(b)$$

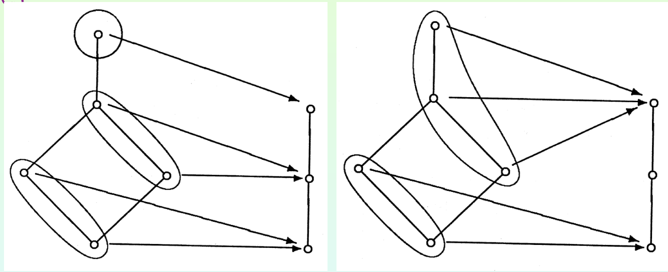
is compatible with join and meet.

- θ is an equivalence relation. Now assume $a \equiv b \pmod{\theta}$ and $c \equiv d \pmod{\theta}$. So $f(a) = f(b)$ and $f(c) = f(d)$. Hence, since f preserves join, $f(a \vee c) = f(a) \vee f(c) = f(b) \vee f(d) = f(b \vee d)$. Therefore $a \vee c \equiv b \vee d \pmod{\theta}$. Dually, θ is compatible with meet.

Congruences and Kernels of Homomorphisms

- An equivalence relation on a lattice L which is compatible with both join and meet is called a **congruence** on L.
- If L and K are lattices and $f : L \to K$ is a lattice homomorphism, then the associated congruence $\theta = \{\langle a, b\rangle : f(a) = f(b)\}$ on L, is known as the **kernel** of f and is denoted by $\ker f$.
- The set of all congruences on L is denoted by $\mathrm{Con} L$.

Examples:



Properties of Congruences

Lemma

(i) An equivalence relation θ on a lattice L is a congruence if and only if, for all $a, b, c \in L$,

$$a \equiv b \pmod{\theta} \Rightarrow a \vee c \equiv b \vee c \pmod{\theta} \text{ and } a \wedge c \equiv b \wedge c \pmod{\theta}.$$

(ii) Let θ be a congruence on L and let $a, b, c \in L$.
  (a) If $a \equiv b \pmod{\theta}$ and $a \leq c \leq b$, then $a \equiv c \pmod{\theta}$.
  (b) $a \equiv b \pmod{\theta}$ if and only if $a \wedge b \equiv a \vee b \pmod{\theta}$.

(i) Assume that θ is a congruence on L. Suppose $a \equiv b \pmod{\theta}$. But $c \equiv c \pmod{\theta}$. Hence, $a \vee c \equiv b \vee c \pmod{\theta}$ and $a \wedge c \equiv b \wedge c \pmod{\theta}$. Suppose, conversely, that the given conditions hold. Let $a, b, c, d \in L$, such that $a \equiv c \pmod{\theta}$ and $b \equiv d \pmod{\theta}$. Then $a \vee b \equiv c \vee b \equiv c \vee d$. Similarly, $a \wedge b \equiv c \wedge d \pmod{\theta}$. Thus, θ is a congruence on L.

Properties of Congruences (Cont'd)

(ii) Let θ be a congruence on L.

(a) Note $a \leq c \leq b$ implies $a = a \wedge c$ and $c = b \wedge c$. Assume $a \equiv b \pmod{\theta}$. Then $a \wedge c \equiv b \wedge c \pmod{\theta}$. So $a \equiv c \pmod{\theta}$.

(b) Suppose $a \equiv b \pmod{\theta}$. Then $a \vee a \equiv b \vee a \pmod{\theta}$ and $a \wedge a \equiv b \wedge a \pmod{\theta}$. By the lattice identities, $a \equiv a \vee b \pmod{\theta}$ and $a \equiv a \wedge b \pmod{\theta}$. Since θ is transitive and symmetric, we deduce $a \wedge b \equiv a \vee b \pmod{\theta}$.

Conversely, assume $a \wedge b \equiv a \vee b \pmod{\theta}$. We have $a \wedge b \leq a \leq a \vee b$. So, by Part (a), $a \wedge b \equiv a \pmod{\theta}$, and similarly $a \wedge b \equiv b \pmod{\theta}$. Because θ is symmetric and transitive, it follows that $a \equiv b \pmod{\theta}$.

Quotient Lattices

- Given an equivalence relation θ on a lattice L, we try to define operations $\vee$ and $\wedge$ on the set of blocks $L/\theta := \{[a]_\theta : a \in L\}$. For all $a, b \in L$, we "define"
$$[a]_\theta \vee [b]_\theta := [a \vee b]_\theta \quad \text{and} \quad [a]_\theta \wedge [b]_\theta := [a \wedge b]_\theta.$$
These operations are well-defined when they are independent of the elements chosen to represent the equivalence classes:
$$[a_1]_\theta = [a_2]_\theta \quad \text{and} \quad [b_1]_\theta = [b_2]_\theta$$
imply
$$[a_1 \vee b_1]_\theta = [a_2 \vee b_2]_\theta \text{ and } [a_1 \wedge b_1]_\theta = [a_2 \wedge b_2]_\theta,$$
for all $a_1, a_2, b_1, b_2 \in L$. But, for all $a_1, a_2 \in L$,
$$[a_1]_\theta = [a_2]_\theta \iff a_1 \in [a_2]_\theta \iff a_1 \equiv a_2 \pmod{\theta}.$$
Hence, $\vee$ and $\wedge$ are well defined on L/θ if and only if θ is a congruence.
- When θ is a congruence on L, we call $\langle L/\theta; \vee, \wedge\rangle$ the **quotient lattice of L modulo θ**.

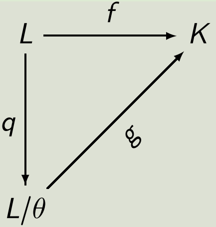
Natural Quotient Map and Homomorphism Theorem

Lemma

Let θ be a congruence on the lattice L. Then $\langle L/\theta; \vee, \wedge\rangle$ is a lattice and the natural quotient map $q : L \to L/\theta$, defined by $q(a) := [a]_\theta$, is a homomorphism.

Theorem

Let L and K be lattices, let f be a homomorphism of L onto K and define $\theta = \ker f$. Then the map $g : L/\theta \to K$, given by $g([a]_\theta) = f(a)$, for all $[a]_\theta \in L/\theta$, is well defined, i.e., $(\forall a, b \in L)[a]_\theta = [b]_\theta$ implies $g([a]_\theta) = g([b]_\theta)$. Moreover g is an isomorphism between L/θ and K. Furthermore, if q denotes the quotient map, then $\ker q = \theta$ and the diagram commutes.



Boolean Congruences and Boolean Homomorphisms

- For the Boolean algebra version of the Homomorphism Theorem, define an equivalence relation θ on a Boolean algebra B to be a **Boolean congruence** if it is a lattice congruence such that $a \equiv b \pmod{\theta}$ implies $a' \equiv b' \pmod{\theta}$, for all $a, b \in B$.

Theorem

Let B and C be Boolean algebras, let f be a Boolean homomorphism of B onto C. Define $\theta = \ker f$. Then θ is a Boolean congruence and the map $g : B/\theta \to C$, given by

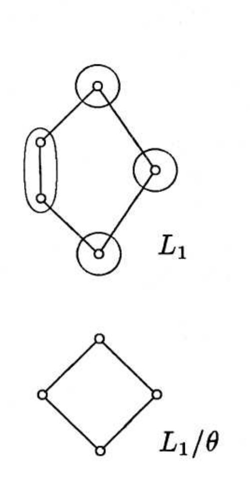
$$g([a]_\theta) = f(a), \text{ for all } [a]_\theta \in B/\theta,$$

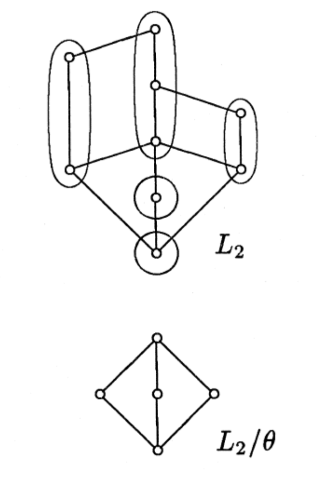
is a well-defined isomorphism between B/θ and C.

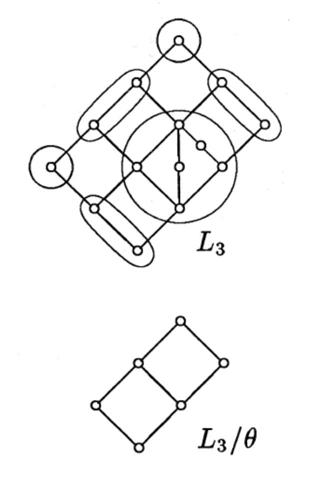
Subsection 2

Congruences and Diagrams

Examples of Congruences and Quotient Lattices







Blocks of Congruences

- When considering the blocks of a congruence θ on L, it is best to think of each block X as an entity in its own right rather than as the block $[a]_\theta$ associated with some $a \in L$, as the latter gives undue emphasis to the element a.

  Intuitively, the quotient lattice L/θ is obtained by collapsing each block to a point.
- Assume we are given a diagram of a finite lattice L and loops are drawn on the diagram representing a partition of L.

  We try to look at the two natural geometric questions:
  (a) How can we tell if the equivalence relation corresponding to the partition is a congruence?
  (b) If we know that the loops define the blocks of a congruence θ, how do we go about drawing L/θ?

Drawing L/θ

- By providing a description of the order and the covering relation on L/θ, the following lemma provides an answer on the drawing question:

Lemma

Let θ be a congruence on a lattice L and let X and Y be blocks of θ.

(i) $X \leq Y$ in L/θ if and only if there exist $a \in X$ and $b \in Y$, such that $a \leq b$.

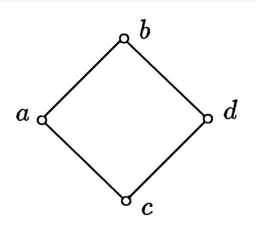
(ii) $X \lessdot Y$ in L/θ if and only if $X < Y$ in L/θ and $a \leq c \leq b$ implies $c \in X$ or $c \in Y$, for all $a \in X$, all $b \in Y$ and all $c \in L$.

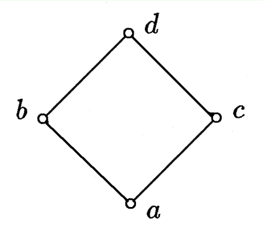
(iii) If $a \in X$ and $b \in Y$, then $a \vee b \in X \vee Y$ and $a \wedge b \in X \wedge Y$.

Quadrilaterals in Lattice Diagrams

- Let L be a lattice and suppose that $\{a, b, c, d\}$ is a 4-element subset of L.
- Then a, b and c, d are said to be opposite sides of the **quadrilateral** $\langle a, b; c, d \rangle$ if:
  - $a < b$ and $c < d$ and
  - either

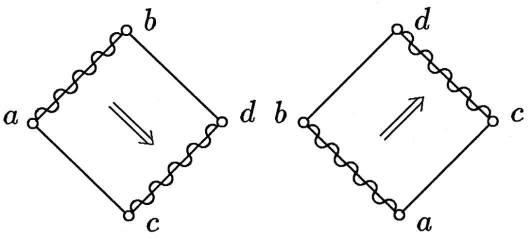
$$(a \vee d = b \text{ and } a \wedge d = c) \quad \text{or} \quad (b \vee c = d \text{ and } b \wedge c = a).$$





Quadrilateral-Closed Block of a Partition

- Let L be a lattice.
- We say that the blocks of a partition of L are **quadrilateral-closed** if whenever a, b and c, d are opposite sides of a quadrilateral and $a, b \in A$ for some block A then $c, d \in B$ for some block B.



(for a covering pair $a \prec b$, we indicate $a \equiv b \pmod{\theta}$ on a diagram by drawing a wavy line from a to b).

Properties of the Blocks

- The blocks of a congruence:
  - are sublattices;
  - are convex (a subset Q of an ordered set P is convex if $x \leq z \leq y$ implies $z \in Q$ whenever $x, y \in Q$ and $z \in P$);
  - are quadrilateral closed.
- Moreover, as we shall see in the next slide, these properties characterize blocks of lattice congruences.

Characterization of Lattice Congruences

Theorem

Let L be a lattice and let θ be an equivalence relation on L. Then θ is a congruence if and only if:

(i) each block of θ is a sublattice of L,

(ii) each block of θ is convex,

(iii) the blocks of θ are quadrilateral-closed.

- Assume that θ is a congruence on L and let X and Y be blocks of θ.
  (i) If $a, b \in X$, then $a \vee b \in X \vee X = X$ and $a \wedge b \in X \wedge X = X$. Hence X is a sublattice of L.
  (ii) Let $a, b \in X$, let $c \in L$, with $a \leq c \leq b$ and assume that c belongs to the block Z of θ. Then, we have $X \leq Z \leq X$ in L/θ and hence $X = Z$. Thus $c \in Z = X$ and hence X is convex.
  (iii) Let a, b and c, d be opposite sides of a quadrilateral, with $a \vee d = b$ and $a \wedge d = c$. We assume that $a, b \in X$ and $d \in Y$. We must prove that $c \in Y$. Since $d \leq b$ we have $Y \leq X$. Thus, $c = a \wedge d \in X \wedge Y = Y$.

Characterization of Lattice Congruences (Converse)

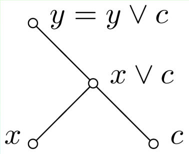
- Assume that (i), (ii) and (iii) hold. We know θ is a congruence provided that, for all $a, b, c \in L$, $a \equiv b \pmod{\theta}$ implies $a \vee c \equiv b \vee c \pmod{\theta}$ and $a \wedge c \equiv b \wedge c \pmod{\theta}$.

  Let $a, b, c \in L$ with $a \equiv b \pmod{\theta}$. By duality it is enough to show that $a \vee c \equiv b \vee c \pmod{\theta}$. Define $X := [a]_\theta = [b]_\theta$. Since X is a sublattice of L, we have $x := a \wedge b \in X$ and $y := a \vee b \in X$.

  Claim: $x \vee c \equiv y \vee c \pmod{\theta}$.

  We distinguish two cases:

  - $c \leq y$: We have $x \leq x \vee c \leq y \vee c = y$ (the second inequality holds because $x \leq y$). Since the block X contains both x and y and is convex, we get $x \vee c \equiv y \vee c \pmod{\theta}$.



Characterization of Lattice Congruences (Cont'd)

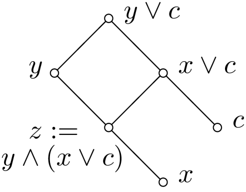
- Goal: Show that, for $a, b, c \in L$ with $a \equiv b \pmod{\theta}$, $a \vee c \equiv b \vee c \pmod{\theta}$.

  We set $X := [a]_\theta = [b]_\theta$, $x := a \wedge b \in X$ and $y := a \vee b \in X$.

  Claim: $x \vee c \equiv y \vee c \pmod{\theta}$.

  We are left with the second case:

  - $c \nleq y$: Since $x \leq y$, we have $x \vee c \leq y \vee c$. If $x \vee c = y \vee c$, then $x \vee c \equiv y \vee c \pmod{\theta}$ as θ is reflexive. Thus, we may assume that $x \vee c < y \vee c$. Since x is a lower bound of $\{y, x \vee c\}$ we have $x \leq z := y \wedge (x \vee c) \leq y$.



    Now $x \leq z \leq x \vee c$ implies $z \vee c = x \vee c$ and hence $z \neq y$ as $y \vee c > x \vee c$. Consequently, z, y and $x \vee c, y \vee c$ are opposite sides of a quadrilateral. Since the block X is convex and $x, y \in X$, it follows that $z \in X$. Since $z, y \in X$ and θ is quadrilateral-closed it follows that $x \vee c$ and $y \vee c$ belong to the same block, say Y. Thus $x \vee c \equiv y \vee c \pmod{\theta}$, as claimed.

Characterization of Lattice Congruences (Conclusion)

- We show $a \vee c \equiv b \vee c \pmod{\theta}$ by showing that $a \vee c$ and $b \vee c$ both belong to the block Y.

  Since $a \wedge b \leq a \leq a \vee b$ and $a \wedge b \leq b \leq a \vee b$ we have

  $$x \vee c = (a \wedge b) \vee c \leq a \vee c \leq a \vee b \vee c = y \vee c$$

  and

  $$x \vee c = (a \wedge b) \vee c \leq b \vee c \leq a \vee b \vee c = y \vee c.$$

  But $x \vee c, y \vee c \in Y$ and Y is convex.

  Therefore, $a \vee c, b \vee c \in Y$.

Subsection 3

The Lattice of Congruences of a Lattice

The Complete Lattice of Congruences of a Lattice

- An equivalence relation θ on a lattice L is a subset of L^2.
- We can rewrite the compatibility conditions in the form

$$(a,b) \in \theta \text{ and } (c,d) \in \theta \quad \text{imply } (a \vee c, b \vee d) \in \theta \text{ and } (a \wedge c, b \wedge d) \in \theta.$$

  This says precisely that θ is a sublattice of L^2.
- Thus, we could define congruences to be those subsets of L^2 which are both equivalence relations and sublattices of L^2.
- With this viewpoint, the set $\mathrm{Con} L$ of congruences on a lattice L is a family of sets, and is ordered by inclusion.

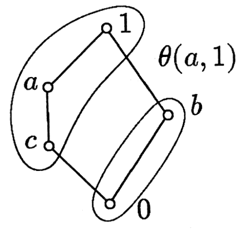
  It is easily seen to be a topped $\bigcap$-structure on L^2.
- Hence, $\mathrm{Con} L$, when ordered by inclusion, is a complete lattice, with least element, $\mathbf{0}$, and greatest element, $\mathbf{1}$, given by $\mathbf{0} = \{(a,a) : a \in L\}$ and $\mathbf{1} = L^2$.

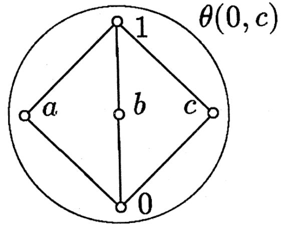
Principal Congruences

- The smallest congruence collapsing a given pair of elements a and b is denoted by $\theta(a,b)$ and called the **principal congruence generated by** (a,b).
- Since $\mathrm{Con}L$ is a topped $\bigcap$-structure, $\theta(a,b)$ exists for all $(a,b) \in L^2$:

$$\theta(a,b) = \bigwedge\{\theta \in \mathrm{Con}L : (a,b) \in \theta\}.$$

Example: The diagrams of $\mathbf{N}_5$ with the partition corresponding to the principal congruence $\theta(a,1)$ and $\mathbf{M}_3$

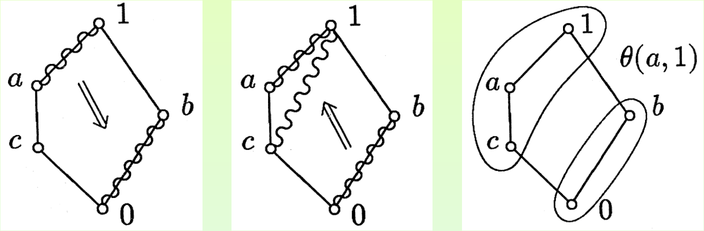




with that corresponding to $\theta(0,c)$.

The Case of $\mathbf{N}_5$

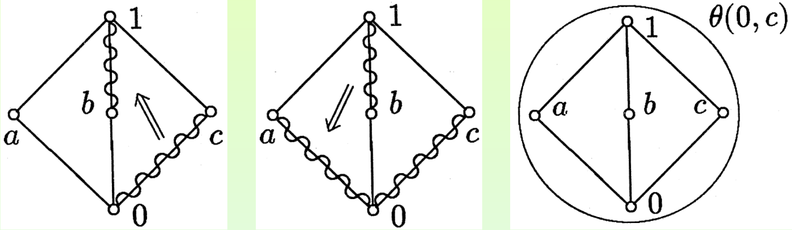
- To find the blocks of the principal congruence $\theta(a,1)$ on $\mathbf{N}_5$:



- We first use the quadrilateral $\langle a,1;0,b\rangle$ to show that $a \equiv 1$ implies $0 \equiv b$ (here $\equiv$ denotes equivalence with respect to $\theta(a,1)$).
- The quadrilateral $\langle 0,b;c,1\rangle$ yields $c \equiv 1 \pmod{\theta}$.
- Since blocks of $\theta(a,1)$ are convex, we deduce that $a,c,1$ lie in the same block.
- It is clear that $\{0,b\}$ and $\{a,c,1\}$ are convex sublattices and together are quadrilateral-closed. Thus they form the blocks of $\theta(a,1)$ on $\mathbf{N}_5$.

The Case of $\mathbf{M}_3$

- To find the blocks of the principal congruence $\theta(0, c)$ on $\mathbf{M}_3$:



- Start with the pair $(0, c)$.
- After two applications of quadrilateral closure, we deduce that $a, c, 0$ lie in the same block, say A.
- Since the blocks of a congruence are sublattices, we have $1 = a \vee c \in A$ and $0 = a \wedge c \in A$.
- Thus, since blocks are convex, A is the only block. Hence $\theta(0, c) = \mathbf{1}$.

Join Density of Set of Principal Congruences

Lemma

Let L be a lattice and let $\theta \in \mathrm{Con}L$. Then $\theta = \bigvee\{\theta(a,b) : (a,b) \in \theta\}$.
Consequently the set of principal congruences is join-dense in $\mathrm{Con}L$.

- We verify that θ is the least upper bound in $\langle \mathrm{Con}L; \subseteq\rangle$ of the set $S = \{\theta(a,b) : (a,b) \in \theta\}$.
  - First, note that the definition of $\theta(a,b)$ implies that $\theta(a,b) \subseteq \theta$, whenever $(a,b) \in \theta$. Therefore θ is an upper bound for S.
  - Now assume that ψ is any upper bound for S. This means that $\theta(a,b) \subseteq \psi$, for any pair $(a,b) \in \theta$. But $(a,b) \in \theta(a,b)$ always. So $(a,b) \in \theta$ implies $(a,b) \in \psi$, as required.

The Join of Two Congruences

- The join in Con$L$ is not generally given by set union, since the union of two equivalence relations is often not an equivalence relation due to failure of transitivity.
- Let L be a lattice and let $\alpha, \beta \in \text{Con}L$. We say that a sequence $z_0, z_1, \ldots, z_n$ **witnesses** $a\ (\alpha \vee \beta)\ b$ if $a = z_0$, $z_n = b$ and $z_{k-1}\ \alpha\ z_k$ or $z_{k-1}\ \beta\ z_k$, for $1 \leq k \leq n$.

  Claim: $a\ (\alpha \vee \beta)\ b$ if and only if for some $n \in \mathbb{N}$, there exists a sequence $z_0, z_1, \ldots, z_n$, which witnesses $a\ (\alpha \vee \beta)\ b$.

  To prove the claim, define a relation θ on L by $a\ \theta\ b$ if and only if for some $n \in \mathbb{N}$, there exists a sequence $z_0, z_1, \ldots, z_n$ which witnesses $a\ (\alpha \vee \beta)\ b$. We shall check:

  (i) $\theta \in \text{Con}L$;
  (ii) $\alpha \subseteq \theta$ and $\beta \subseteq \theta$;
  (iii) if $\alpha \subseteq \gamma$ and $\beta \subseteq \gamma$, for some $\gamma \in \text{Con}L$, then $\theta \subseteq \gamma$.

  Consequently θ is indeed the least upper bound of α and β in Con$L$.

The Join of Two Congruences: $\theta \in \mathrm{Con} L$

- We show θ is a congruence relation on L.
  - If $a \in L$, then, by reflexivity of α, $a \; \alpha \; a$. Hence $a \; \theta \; a$ and θ is reflexive;
  - If $a \; \theta \; b$, then, there exist $a = z_0, z_1, \ldots, z_{n-1}, z_n = b$, such that $a = z_0 \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \overset{\alpha}{\underset{\beta}{\text{or}}} z_n = b$. Since α and β are symmetric, $b = z_n \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \overset{\alpha}{\underset{\beta}{\text{or}}} z_0 = a$. Thus, $b \; \theta \; a$ and θ is symmetric.
  - Suppose $a \; \theta \; b$ and $b \; \theta \; c$. Then, there exist $a = z_0, z_1, \ldots, z_{n-1}, z_n = b$, such that $a = z_0 \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \overset{\alpha}{\underset{\beta}{\text{or}}} z_n = b$ and there exist $b = w_0, w_1, \ldots, w_{m-1}, w_m = c$, such that $b = w_0 \overset{\alpha}{\underset{\beta}{\text{or}}} w_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} w_{m-1} \overset{\alpha}{\underset{\beta}{\text{or}}} w_m = c$.
    Thus, we have
    $a = z_0 \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \overset{\alpha}{\underset{\beta}{\text{or}}} z_n = w_0 \overset{\alpha}{\underset{\beta}{\text{or}}} w_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} w_{m-1} \overset{\alpha}{\underset{\beta}{\text{or}}} w_m = c$.
    Hence, $a \; \theta \; c$ and θ is also transitive.

The Join of Two Congruences: $\theta \in \mathrm{Con}L$ & $\theta = \alpha \vee \beta$

- Suppose $a \ \theta \ b$ and $c \in L$. Then there exist $a = z_0, z_1, \ldots, z_{n-1}, z_n = b$, such that $a = z_0 \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \overset{\alpha}{\underset{\beta}{\text{or}}} z_n = b$. Since both α and β are congruences,

$$a \vee c = z_0 \vee c \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \vee c \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \vee c \overset{\alpha}{\underset{\beta}{\text{or}}} z_n \vee c = b \vee c.$$

  Hence, $a \vee c \ \theta \ b \vee c$ and, dually, $a \wedge c \ \theta \ b \wedge c$. Hence, θ is a congruence relation.
- Clearly, by definition, if $a \ \alpha \ b$, then $a \ \theta \ b$. Similarly, if $a \ \beta \ b$, then $a \ \theta \ b$. Hence, $\alpha \subseteq \theta$ and $\beta \subseteq \theta$, i.e., θ is an upper bound of $\{\alpha, \beta\}$.
- To show that it is a least upper bound, suppose $\alpha \subseteq \gamma$ and $\beta \subseteq \gamma$, for some $\gamma \in \mathrm{Con}L$. To show $\theta \subseteq \gamma$, let $a \ \theta \ b$. Then, there exist $a = z_0, z_1, \ldots, z_{n-1}, z_n = b$, such that $a = z_0 \overset{\alpha}{\underset{\beta}{\text{or}}} z_1 \overset{\alpha}{\underset{\beta}{\text{or}}} \cdots \overset{\alpha}{\underset{\beta}{\text{or}}} z_{n-1} \overset{\alpha}{\underset{\beta}{\text{or}}} z_n = b$. Thus, by hypothesis, $a = z_0 \ \gamma \ z_1 \ \gamma \cdots \gamma \ z_{n-1} \ \gamma \ z_n = b$. By transitivity of γ, $a \ \gamma \ b$. Thus, $\theta \subseteq \gamma$ and, therefore, $\theta = \alpha \vee \beta$.

Congruence Lattices of Lattices are Distributive

- Consider the **median term**, $m(x,y,z) := (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$. It satisfies the identities $m(x,x,y) = m(x,y,x) = m(y,x,x) = x$.

Theorem

The lattice $\mathrm{Con}L$ is distributive for any lattice L.

- Let $\alpha, \beta, \gamma \in \mathrm{Con}L$. It suffices to show $\alpha \wedge (\beta \vee \gamma) \leq (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$. Assume that $a\ (\alpha \wedge (\beta \vee \gamma))\ b$. Then $a\ \alpha\ b$. And there is a sequence $a = z_0, z_1, \ldots, z_n = b$ which witnesses $a\ (\alpha \vee \gamma)\ b$. By the median identities $a = m(a,b,z_0)$ and $b = m(a,b,z_n)$. Furthermore, since $a\ \alpha\ b$, for $i = 0, \ldots, n-1$, we have $m(a,b,z_i)\ \alpha\ m(a,a,z_i) = a$ $= m(a,a,z_{i+1})\ \alpha\ m(a,b,z_{i+1})$. So $m(a,b,z_i)\ \alpha\ m(a,b,z_{i+1})$. Observe also that, if $c\ \theta\ d$, then $m(a,b,c)\ \theta\ m(a,b,d)$, for all $c, d \in L$ and all $\theta \in \mathrm{Con}L$. For $i = 0, \ldots, n-1$, we can apply this with $c = z_i, d = z_{i+1}$ and θ as either β or γ. Thus, $a = m(a,b,z_0)$, $m(a,b,z_1), \ldots, m(a,b,z_n) = b$ witnesses $a\ ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma))\ b$.

Groups Revisited

- Let G be a group.
- We showed that there is a correspondence between normal subgroups of G and equivalence relations compatible with the group structure, that is, group congruences.
- Denote the set of all such congruences by $\mathrm{Con}\, G$.
- Each congruence is regarded as a subset of $G \times G$ and $\mathrm{Con}\, G$ is given the inclusion order inherited from $\mathcal{P}(G \times G)$.

  This makes $\mathrm{Con}\, G$ into a topped $\bigcap$-structure, and so a complete lattice, in just the same way that $\mathrm{Con} L$ is, for L a lattice.
- It is then easy to see that $\mathrm{Con}\, G \cong \mathcal{N}\text{-}\mathrm{Sub}\, G$.
- We have already seen that $\mathcal{N}\text{-}\mathrm{Sub}\, G$ is modular.
- Consequently, $\mathrm{Con}\, G$ is modular.
- However, even for very small groups it may not be distributive.

  Example: For $G = \mathbf{V}_4$, the Klein 4-group, we have $\mathcal{N}\text{-}\mathrm{Sub}\, G \cong \mathbf{M}_3$.