Congruence relations

1. The concept

Let's start with a familiar case: congruence mod n on the ring $\mathbf{Z}$ of integers. Just to be specific, let's use $n = 6$. This congruence is an equivalence relation that is compatible with the ring operations, in the following sense:

$$\Rightarrow \frac{\begin{array}{rcl} a & \equiv & b \\ a' & \equiv & b' \end{array}}{a + a' \equiv b + b'} \qquad \Rightarrow \frac{\begin{array}{rcl} a & \equiv & b \\ a' & \equiv & b' \end{array}}{aa' \equiv bb'} \qquad \Rightarrow \frac{a \equiv b}{-a \equiv -b}$$

and of course $0 \equiv 0$.

The same definition works for algebraic systems in general:

1.1 *Definition.* A *congruence relation* on an algebra $\mathcal{A} = \langle A; f_1, \ldots, f_m \rangle$ is an equivalence relation $\equiv$ that is compatible with the operations, in the sense that for each basis operation f_i, if f_i is n_i-ary we have

$a_1 \equiv b_1, \ \ldots \ , a_{n_i} \equiv b_{n_i} \Rightarrow f_i(a_1, \ldots, a_{n_i}) \equiv f_i(b_1, \ldots, b_{n_i})$.

Terminology. Often we name a congruence relation θ, say, and write either $a \theta b$ or $a \equiv b \ (\theta)$. Also, we may say "congruence" instead of "congruence relation". Just as for equivalence relations in general, we can speak of the *blocks* of a congruence relation (or "classes", but that usage is somewhat old). For $a \in A$, the block of a is often called $\bar{a}$.

2. Examples

(1) In $\mathbf{Z}$, a congruence relation is the same as congruence mod n for some n. The case $n = 0$ is allowed, giving the equality relation.

(2) In a group, a congruence relation is the same thing as the coset decomposition for a normal subgroup.

(3) In a commutative ring, a congruence relation is the same thing as the coset decomposition for an ideal.

(4) In a finite chain C, a congruence relation is any decomposition into intervals, as in Figure 1(a).

(5) Lattices in general can have congruence relations, as in Figure 1(b).

(6) For a homomorphism $\varphi : \mathcal{A} \to \mathcal{B}$, the kernel of φ is a congruence relation.

Here the *kernel* of a homomorphism means the equivalence relation that φ induces on its domain: $a \equiv a' \Leftrightarrow \varphi(a) = \varphi(a')$. This is a contrast with the specific cases of groups and rings, where the kernel is a normal subgroup. However, Example (2) shows that the two definitions are equivalent.

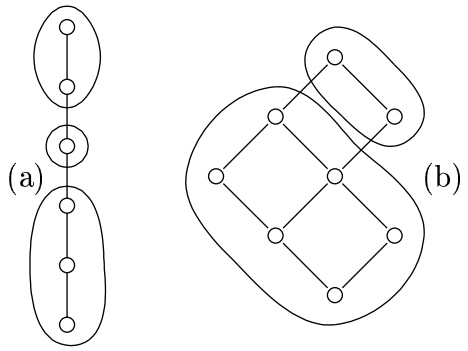

Figure 1: Congruence relations on lattices

3. The congruence lattice of an algebra

It is easy to see that an intersection of congruence relations on $\mathcal{A}$ is again a congruence relation. Therefore the congruence relations on $\mathcal{A}$ form a complete lattice, $\mathrm{Con}(\mathcal{A})$. In fact, $\mathrm{Con}(\mathcal{A})$ is simply a sublattice of $\mathrm{Equiv}(A)$. Some examples:

(a) For a group G, the lattice $\mathrm{Con}(G)$ is essentially the same thing as the lattice of normal subgroups, $\mathrm{Normal}(G)$.

(b) For a commutative ring R, the lattice $\mathrm{Con}(R)$ is essentially the same thing as the lattice of ideals of R.

(c) The congruence lattice of a four-element chain is the Boolean lattice $\mathbf{2}^3$.

4. Factor algebras

For a group G with normal subgroup H, we can form G/H. For a commutative ring R with ideal I, we can form R/I. In general:

4.1 *Definition.* For an algebra $\mathcal{A} = \langle A; f_1, \ldots, f_m \rangle$ and $\theta \in \mathrm{Con}(\mathcal{A})$, let $\mathcal{A}/\theta$ be the algebra whose elements are the blocks of θ and whose operations are defined as follows: For each basic operation f_i on A, define a corresponding operation f_i on $\mathcal{A}/\theta$ by

$f_i(\bar{a}_1, \ldots, \bar{a}_{n_i}) = \overline{f}_i(a_1, \ldots, a_{n_i})$.

This operation is well defined, since by the definition of a congruence relation the result does not depend on which representatives are chosen for the blocks. Just as for groups or rings, $\mathcal{A}/\theta$ is called a "factor algebra" or "quotient algebra" obtained by "factoring out θ". Don't confuse this with the concept of a "field of quotients".

4.2 *Definition.* The *natural map* of $\mathcal{A}$ onto $\mathcal{A}/\theta$ is $\pi : \mathcal{A} \to \mathcal{A}/\theta$ given by $\pi(a) = \bar{a}$.

4.3 *Proposition.* The natural map of $\mathcal{A}$ onto $\mathcal{A}/\theta$ is a surjective homomorphism with kernel θ.

This natural map can also be called the *natural homomorphism* or *natural surjection.* See Figure 2.

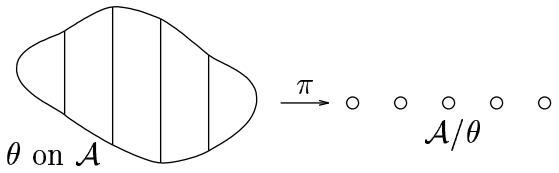

Figure 2: The natural homomorphism

4.4 *Corollary.* Every congruence relation is the kernel of some homomorphism.

4.5 *Note.* If $\theta_1 \subseteq \theta_2$, then there is a natural surjection $\mathcal{A}/\theta_1 \to \mathcal{A}/\theta_2$. To remember the direction of this map, think of $\mathcal{A}/\theta_1$ as bigger than $\mathcal{A}/\theta_2$, since in $\mathcal{A}/\theta_1$, less has been factored out.

5. The first isomorphism theorem

For groups, recall the "first isomorphism theorem": If $\varphi : G \to H$, then $\text{im}\ \varphi \cong G/\ker\varphi$. Or equivalently, if $\varphi : G \to H$ is a surjection with kernel K, then $H \cong G/K$.

This theorem is useful in examples. It also shows that the homomorphic images of a group G are determined up to isomorphism by information internal to G. In particular, if G is finite then up to isomorphism G has only finitely many homomorphic images.

For algebras in general, the situation is the same:

5.1 *Theorem* (**first isomorphism theorem**). Let $\varphi : \mathcal{A} \to \mathcal{B}$ be a homomorphism. Then $\text{im}\ \varphi \cong A/\ker\ \varphi$. Equivalently, if $\varphi : \mathcal{A} \to \mathcal{B}$ is a surjective homomorphism with kernel θ, then $\mathcal{B} \cong \mathcal{A}/\theta$.

5.2 *Corollary.* The possible homomorphic images of $\mathcal{A}$ are determined up to isomorphism by the internal structure of $\mathcal{A}$.

6. The correspondence theorem

One version for groups: If $\varphi : G \to H$ is a surjective homomorphism, then there is a one-to-one correspondence between the normal subgroups of H and the normal subgroups of G that contain $\ker \varphi$. In fact, the subgroup of G corresponding to a normal subgroup K of H is simply $\varphi^{-1}(K)$.

The generalization to algebras is this:

6.1 *Theorem* (**correspondence theorem**). If $\varphi : \mathcal{A} \to \mathcal{B}$ is a surjective homomorphism, then there is a one-to-one correspondence between congruence relations on $\mathcal{B}$ and the congruence relations on $\mathcal{A}$ that contain $\ker \varphi$.

6.2 *Note.* Using the first isomorphism theorem, equivalent versions can be given for the natural maps $G \to G/N$ (where $N \lhd G$) or $\mathcal{A} \to \mathcal{A}/\theta$ (where $\theta \in \mathrm{Con}(\mathcal{A})$).

6.3 *Note.* For groups, one can also say that there is a one-to-one correspondence between *all* subgroups of H, normal or not, and those subgroups of G that contain $\ker \varphi$. For algebras in general, this becomes a statement about subalgebras rather than about congruence relations.

7. Intersections of congruence relations

Suppose $\theta_1, \theta_2 \in \mathrm{Con}(\mathcal{A})$. Let $\pi_1 : \mathcal{A} \to \mathcal{A}/\theta_1$ and $\pi_2 : \mathcal{A} \to \mathcal{A}/\theta_2$ be the natural homomorphisms. Combining these, we get a a homomorphism $\pi_1 \times \pi_2 : \mathcal{A} \to \mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$ (not necessarily onto). What is its kernel? By considering when $a, a' \in A$ have equal images, we see that the kernel is $\theta_1 \cap \theta_2$. From this and the first isomorphism theorem we get this fact:

7.1 *Theorem* (**subdirect embedding theorem**). For an algebra $\mathcal{A}$ and $\theta_1, \theta_2 \in \mathrm{Con}(\mathcal{A})$, there is a natural embedding of $\mathcal{A}/(\theta_1 \cap \theta_2) \hookrightarrow \mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$.

("Subdirect" means that the image of the embedding inside the product is large enough to map onto each factor. This will be important later.)

7.2 *Corollary.* If $\mathcal{A}$ has congruence relations θ_1, θ_2 with $\theta_1 \cap \theta_2 = 0$ (the equality relation), then $\mathcal{A} \hookrightarrow \mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$ (an embedding).

8. Congruence relations on lattices

8.1 **Principles** For $\theta \in \mathrm{Con}(A)$:

(1) If $a \equiv b (\text{mod } \theta)$, then $a \wedge b \equiv a \vee b (\text{mod } \theta)$.

(2) If $a \leq t \leq b$ and $a \equiv b (\text{mod } \theta)$, then $t \equiv a \equiv b \ (\text{mod } \theta)$.

(3) If $a \wedge b \equiv a (\text{mod } \theta)$, then $b \equiv a \vee b (\text{mod } \theta)$, and dually.

(4) If $a \equiv b (\text{mod } \theta)$ and $b \equiv c (\text{mod } \theta)$, then $a \equiv c (\text{mod } \theta)$.

8.2 **Theorems**

(A) A nonempty relation θ on a lattice is a congruence relation if and only if θ satisfies (1) through (4).

(B) For elements a_0, b_0 of a lattice L, $\text{con}(a_0, b_0)$, the smallest congruence relation on L that identifies a_0 and b_0, can be constructed by applying (1) (unless $a_0 \leq b_0$ already), then (2) and (3) repeatedly, and then (4) repeatedly. This is the *principal* congruence relation $\text{con}(a, b)$ (lower-case c).

For examples to try, see Figure 3. Congruence relations can be indicated by darkening each covering between two elements in the same block.

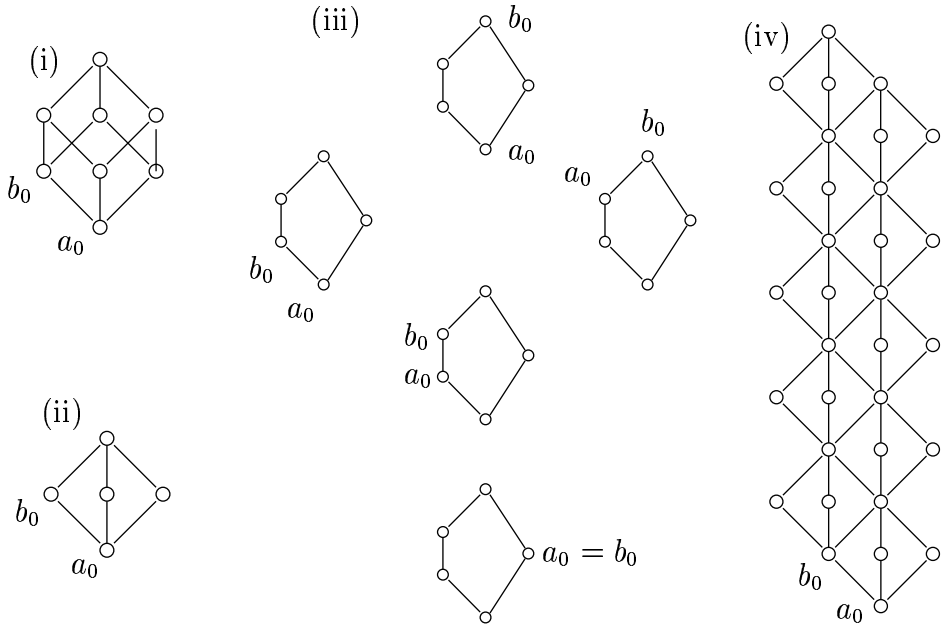

Figure 3: Some lattices for which to find congruence lattices

9. Problems

Problem D-1. Verify that any congruence relation on a group is simply the coset decomposition determined by some normal subgroup.

Problem D-2. For general algebras, prove (a) the first isomorphism theorem (Theorem 5.1); (b) the correspondence theorem (Theorem 6.1).

Problem D-3. (a) Any function $f : X \to Y$ on sets induces an equivalence relation on its domain X, where $x \sim x'$ means $f(x) = f(x')$. Show that for groups G and H, if $\varphi : G \to H$ is a homomorphism then any single block of the equivalence relation it induces determines all the blocks. (This is why the "kernel" of φ is defined to be a single block, the one containing e.)

(b) Give an example of two algebras and two homomorphisms φ, φ' between them such that φ and φ' give different equivalence relations that do have at least one block in common. (This is why the "kernel" of φ is defined to be the whole equivalence relation rather than a single block, for algebras in general.)

Problem D-4. Explain how the congruence lattice of $\mathcal{A}$ is a sublattice of the partition lattice of A as a set.

Problem D-5. State and prove a version of Theorem 7.1 that refers to two surjective homomorphisms $\varphi_i : \mathcal{A} \to \mathcal{B}_i$ $(i = 1, 2)$, rather than to two congruence relations on $\mathcal{A}$.

Problem D-6. If $\varphi : \mathcal{A} \to \mathcal{B}$ is a surjective homomorphism, show that there is a lattice embedding of $\mathrm{Con}(\mathcal{B})$ into $\mathrm{Con}(\mathcal{A})$, with the image being an interval.

Problem D-7. Invent a correspondence theorem (like Theorem 6.1) for a surjective homomorphism $\varphi : \mathcal{A} \to \mathcal{B}$ that relates subalgebras of $\mathcal{B}$ to certain subalgebras of $\mathcal{A}$. Somehow describe which ones. (No proof is required.)

Problem D-8. Show that the subdirect embedding theorem (7.1) holds for the intersection of a possibly infinite family of congruence relations.

Problem D-9. For the case $\mathcal{A} = \mathbf{Z}$, the ring of integers, give (a) an example of the subdirect embedding theorem in which the two congruence relations come from prime ideals, and (b) an example where neither comes from a prime ideal. In each case, say what the embedding does to each element.

Problem D-10. Prove that the congruence lattice of a chain of length n (as an algebra with lattice operations) is the Boolean lattice $\mathbf{2}^n$. (The *length* of a chain is the number of jumps, so a chain of length n has $n + 1$ elements.)

Problem D-11. Let $\mathcal{D}$ be a distributive lattice and consider any $d \in D$. Define maps $f_{\vee d} : D \to D$ and $f_{\wedge d} : D \to D$ by $f_{\vee d}(x) = d \vee x$ and $f_{\wedge d}(x) = d \wedge x$. (a) Show that $f_{\vee d}$ and $f_{\wedge d}$ are homomorphisms. (b) Show that the intersection of their kernels is 0 (i.e., equality). (c) Use Theorems 7.1 and 5.1 to show that $\mathcal{D} \hookrightarrow (d] \times [d)$.

Problem D-12. Compute all the principal congruence relations in Figure 3. Indicate blocks by darkening coverings between two elements in the same block. You may omit examples already done in lecture.