Universal Algebra Week 4

James Newman Winter 2019

Theorem. $\mathrm{Sg}(X) = X \cup E(X) \cup E^2(X) \cup \dots$

Proof. First by induction, $E^k(X) \subseteq \mathrm{Sg}(X)$ for all $k \in \mathbb{N}$.

(i) The base case when $k = 0$ holds: $E^0(X) = X \subseteq \mathrm{Sg}(X)$ because $\mathrm{Sg}(X)$ is the intersection of supersets of X.

(ii) Assume that $E^k(X) \subseteq \mathrm{Sg}(X)$. Then take any $a \in E^{k+1}(X) = E(E^k(X)) = E^k(X) \cup \{f(a_1, \dots, a_n) \mid f$ is a fundamental n-ary operation on A and $a_1, \dots, a_n \in E^k(X)\}$. In the first case $a \in E^k(X)$, which case clearly $a \in \mathrm{Sg}(X)$ as $E^k(X) \subseteq \mathrm{Sg}(X)$. Otherwise $a \in \{f(a_1, \dots, a_n)\}$ So $a = f(a_1, \dots, a_n)$ for $a_1, \dots, a_n \in E^k(X)$. Then $a_1, \dots, a_n \in \mathrm{Sg}(X)$ because $E^k(X) \subseteq \mathrm{Sg}(X)$. Take any subuniverse B such that $X \subseteq B$. Then $a_1, \dots, a_n \in B$ because $a_1, \dots, a_n \in \mathrm{Sg}(X)$. Thus $f(a_1, \dots, a_n) \in B$ because B is a subuniverse and is closed. Therefore $a = f(a_1, \dots, a_n) \in \mathrm{Sg}(X)$ because it is in every subuniverse that contains X. In either case, $a \in \mathrm{Sg}(X)$, thus $E^{k+1}(X) \subseteq \mathrm{Sg}(X)$ since if $a \in E^{k+1}(X)$ then $a \in \mathrm{Sg}(X)$.

Thus by induction $E^k(X) \subseteq \mathrm{Sg}(X)$ for all $k \in \mathbb{N}$. Then it is clear that $X \cup E(X) \cup E^2(X) \cup \dots \subseteq \mathrm{Sg}(X)$.

Next, $X \cup E(X) \cup E^2(X) \cup \dots$ is a subuniverse. Take any n-ary operation f on A and $a_1, \dots, a_n \in X \cup E(X) \cup E^2(X) \cup \dots$. Since $\{a_1, \dots, a_n\}$ is finite, each a_n is in some $E^k(X)$ and $X \subseteq E(X) \subseteq E^2(X) \subseteq \dots$, there is some $E^k(X)$ such that $a_1, \dots, a_n \in E^k(X)$. Then by definition $f(a_1, \dots, a_n) \in E^{k+1}(X)$, and so $f(a_1, \dots, a_n) \in X \cup E(X) \cup E^2(X) \cup \dots$ because $E^{k+1} \subseteq X \cup \dots \cup E^K(X) \cup E^{k+1}(X) \cup \dots$. Therefore it is closed and contains X so is a subuniverse.

Assume $x \notin X \cup E(X) \cup E^2(X) \cup \dots$. Then since it is a subuniverse containing X and $\mathrm{Sg}(X)$ is the intersection of all such subuniverses, $x \notin \mathrm{Sg}(X)$. Then by contrapositive, if $x \in \mathrm{Sg}(X)$ then $x \in X \cup E(X) \cup E^2(X) \cup \dots$. That is $\mathrm{Sg}(X) \subseteq X \cup E(X) \cup E^2(X) \cup \dots$.

With both directions of the inclusion demonstrated, they are equal. □

Theorem. If $\sim \in \mathrm{Con}\,\mathbf{G}$ then $1/\sim$ is the universe of a normal subgroup of $\mathbf{G}$, and for $a, b \in G$ we have $a \sim b$ if and only if $a \cdot b^{-1} \in 1/\sim$.

Proof. Assume $\sim \in \mathrm{Con}\,\mathbf{G}$. Let $N = 1/\sim$

For any $g \in G$, assume $g \cdot a \cdot g^{-1} \in gNg^{-1}$. Then $a \in N$ and thus $1 \sim a$. Then by compatibility,

$$\begin{aligned} g \cdot 1 &\sim g \cdot a \\ g &\sim g \cdot a \\ g \cdot g^{-1} &\sim g \cdot a \cdot g^{-1} \\ 1 &\sim g \cdot a \cdot g^{-1} \end{aligned}$$

Then $g \cdot a \cdot g^{-1} \in N$. So $gNg^{-1} \subseteq N$ for all $g \in G$ and thus $N = 1/\sim$ is the universe of normal subgroup of $\mathbf{G}$.

Next, for $a, b \in G$,

$$\begin{aligned} a \sim b && \text{iff} \\ a \cdot b^{-1} \sim b \cdot b^{-1} && \text{iff} \\ a \cdot b^{-1} \sim 1 && \text{iff} \\ a \cdot b^{-1} \in N && \end{aligned}$$

by compatibility and properties of groups. $\square$

Theorem. If $\mathbf{N}$ is a normal subgroup of a group $\mathbf{G}$, then the relationship $\sim$ defined as

$$a \sim b \text{ iff } a \cdot b^{-1} \in N$$

is a congruence on $\mathbf{G}$ with $1/\sim = N$.

Proof. Assume $\mathbf{N}$ is a normal subgroup of a group $\mathbf{G}$ and define $\sim$ as above. First we confirm $\sim$ is an equivalence relation:

1. For any $a \in G$ we have that $a \sim a$ because $a \cdot a^{-1} = 1 \in N$.

2. For any $a, b \in G$ assume $a \sim b$. Then $a \cdot b^{-1} \in N$ so its inverse $b \cdot a^{-1} \in N$, and thus $b \sim a$.

3. For any $a, b, c \in G$ assume $a \sim b$ and $b \sim c$. That is, $a \cdot b^{-1} \in N$ and $b \cdot c^{-1} \in N$. Then since $\mathbf{N}$ is closed, $a \cdot b^{-1} \cdot b \cdot c^{-1} = a \cdot c^{-1} \in N$. Thus $a \sim c$.

Therefore $\sim$ is an equivalence relation.

Next we check the compatibility property.

1. Take any $a, b \in G$ such that $a \sim b$. Then $b \sim a$, i.e. $b \cdot a^{-1} \in N$. Then because N is normal, $a^{-1}ba^{-1}a = a^{-1}b = a^{-1}(b^{-1})^{-1} \in N$. Therefore $a^{-1} \sim b^{-1}$.

2. Next take any $a_1, a_2, b_1, b_2 \in G$ such that $a_1 \sim b_1$ and $a_2 \sim b_2$. Then $a_1 b_1^{-1} \in N$ and $a_2 b_2^{-1} \in N$. Because N is normal and $a_1 b_1^{-1} \in N$ we have that $b_1^{-1} a_1 b_1^{-1} b_1 = b_1^{-1} a_1 \in N$. Next since $b_1^{-1} a_1 \in N$ and $a_2 b_2^{-1} \in N$ their product $b_1^{-1} a_1 a_2 b_2^{-1} \in N$. Again since N is normal, $b_1 \cdot b_1^{-1} \cdot a_1 \cdot a_2 \cdot b_2^{-1} \cdot b_1^{-1} = a_1 \cdot a_2 \cdot b_2^{-1} \cdot b_1^{-1} = (a_1 \cdot a_2) \cdot (b_1 \cdot b_2)^{-1} \in N$. Therefore $a_1 \cdot a_2 \sim b_1 \cdot b_2$.

Finally, since $\sim$ is an equivalence relationship that satisfies the compatibility property it is a congruence on $\mathbf{G}$. $\square$

Theorem. The normal subgroups of a group form an algebraic lattice which is modular.

Proof. Take any group $\mathbf{G}$. By Exercise 1 the lattice of normal subgroups of $\mathbf{G}$ is isomorphic to the lattice of congruences on $\mathbf{G}$. By theorem 5.5, the lattice of congruences on $\mathbf{G}$ is algebraic. By theorem 5.10, if $\mathbf{G}$ is congruence permutable, then $\mathbf{G}$ is congruence modular. Then it is sufficient to show that $\mathbf{G}$ is congruence permutable to show that the lattice of normal subgroups of $\mathbf{G}$ is algebraic and modular.

Take any $\sim_1, \sim_2 \in \text{Con } \mathbf{G}$. Take any $a, b \in G$ such that $a \sim_1 \circ \sim_2 b$. Then there is a $c \in G$ such that $a \sim_1 c$ and $c \sim_2 b$. Then by compatbility

$$\begin{array}{lllcll} c & \sim_2 & b & \qquad & a & \sim_1 c \\ 1 & \sim_2 & c^{-1}b & & ac^{-1} & \sim_1 1 \\ a & \sim_2 & ac^{-1}b & & ac^{-1}b & \sim_1 b \end{array}$$

Then $a \sim_2 \circ \sim_1 b$. Thus $\sim_1 \circ \sim_2 \subseteq \sim_2 \circ \sim_1$, and by theorem 5.9, $\sim_1 \circ \sim_2 = \sim_2 \circ \sim_1$. That is, $\mathbf{G}$ is congruence permutable and thus also congruence modular.

Therefore the lattice of normal subgroups of a group form an algebraic and modular lattice. □

Theorem. If $\mathbf{A}$ is a unary algebra and B is a subuniverse then the relation $\sim$ defined by $a \sim b$ if and only if $a = b$ or $a, b \in B$ is a congruence on $\mathbf{A}$.

Proof. Assume $\mathbf{A}$ is a unary algebra and B is a subuniverse. Defined the realtion $\sim$ by $a \sim b$ if and only if $a = b$ or $a, b \in B$. Then

1. For all $a \in A$, $a \sim a$ because $a = a$.
2. For all $a, b \in A$, if $a \sim b$ then $b \sim a$ because if $a = b$ or $a, b \in B$ then $b = a$ or $b, a \in B$.
3. Take any $a, b, c \in A$ such that $a \sim b$ and $b \sim c$. Then by cases
   (a) $a, b \in B$ and $b, c \in B$ in which case $a, c \in B$ and $a \sim c$.
   (b) $a, b \in B$ and $b = c$ in which case $a, c \in B$ and $a \sim c$.
   (c) $a = b$ and $b = c$ in which case $a = c$ and $a \sim c$.

Thus $\sim$ is an equivalence relation. To show it is compatible, take any operation f of $\mathbf{A}$ and any $a, b \in A$ such that $a \sim b$. Since $\mathbf{A}$ is a unary algebra, f is unary. Then either

1. $a = b$ so $f(a) = f(b)$ and thus $f(a) \sim f(b)$.
2. $a, b \in B$ then because B is a subuniverse and is closed under f, $f(a), f(b) \in B$, so $f(a) \sim f(b)$.

Therefore $\sim$ is a compatible equivalence relation on A and thus a congruence of $\mathbf{A}$. □

Theorem. If $\mathbf{L}$ is a distributive lattice and $a, b, c, d \in L$, then $\langle a, b\rangle \in \Theta(c, d)$ iff $c \wedge d \wedge a = c \wedge d \wedge b$ and $c \vee d \vee a = c \vee d \vee b$.

Proof. Assume $\mathbf{L}$ is a distributive lattice. Let $X = \{\langle c, d\rangle\} \subseteq L \times L$. Then by the construction in theorem 5.5, $\Theta(c, d) = \mathrm{Sg}(X) = X \cup E(X) \cup E^2(X) \cup \ldots$ where for all $X \subseteq L \times L$.

$$\begin{aligned}E(X) = X& \\ &\cup \{1_a = \langle a, a\rangle \text{ for all } a \in L\} \\ &\cup \{s(\langle b, a\rangle) = \langle a, b\rangle \text{ for all } \langle b, a\rangle \in X\} \\ &\cup \{\text{if } b = c \text{ then } \langle a, d\rangle \text{ else } \langle a, b\rangle \text{ for } \langle a, b\rangle, \langle c, d\rangle \in X\} \\ &\cup \{\langle a_1 \wedge a_2, b_1 \wedge b_2\rangle \text{ for all } \langle a_1, a_2\rangle, \langle b_1, b_2\rangle \in X\} \\ &\cup \{\langle a_1 \vee a_2, b_1 \vee b_2\rangle \text{ for all } \langle a_1, a_2\rangle, \langle b_1, b_2\rangle \in X\}\end{aligned}$$

We will show by induction that for all $k \in \mathbb{N}$ and $a, b \in L$ if $\langle a, b\rangle \in E^k(c, d)$ then $c \wedge d \wedge a = c \wedge d \wedge b$ and $c \vee d \vee a = c \vee d \vee b$.

1. In the base case $k = 0$. Assume $\langle a, b\rangle \in E^0(X) = \{\langle c, d\rangle\}$. Then $a = c$, $b = d$ and

$$\begin{aligned}c \wedge d \wedge a &= c \wedge d \wedge c \\ &= c \wedge c \wedge d \\ &= c \wedge d \\ &= c \wedge d \wedge d \\ &= c \wedge d \wedge b.\end{aligned}$$

   Dually, $c \vee d \vee a = c \vee d \vee b$.

2. In the inductive case, assume the inductive hypothesis that if $\langle a, b\rangle \in E^k(X)$ then $c \wedge d \wedge a = c \wedge d \wedge b$ and $c \vee d \vee a = c \vee d \vee b$. Next, assume $\langle a, b\rangle \in E^{k+1}(X) = E(E^k(X))$. By cases, either

   (a) $\langle a, b\rangle \in E^k(X)$, in which case the goal holds immediately from the inductive hypothesis.

   (b) $\langle a, b\rangle = 1_c = \langle c, c\rangle$ for some $c \in L$, in which case the goal is trivially true.

   (c) $\langle a, b\rangle = s(\langle b, a\rangle)$ with $\langle b, a\rangle \in E^k(X)$, in which case again the goal holds from the inductive hypothesis.

   (d) $\langle a, b\rangle = t(\langle e, f\rangle, \langle g, h\rangle)$ for some $\langle e, f\rangle, \langle g, h\rangle \in E^k(X)$. There are two cases:

      i. When $f = g$, $\langle a, b\rangle = \langle e, f\rangle$. By the inductive hypothesis, $c \wedge d \wedge e = c \wedge d \wedge f$ and $c \wedge d \wedge g = c \wedge d \wedge h$. But then by substitution since $f = g$, $a = e$, and $b = f$,

$$c \wedge d \wedge a = c \wedge d \wedge f = c \wedge d \wedge b.$$

      Dually, $c \vee d \vee a = c \vee d \vee b$.

ii. Otherwise $\langle a, b\rangle = \langle e, f\rangle$, and thus $\langle a, b\rangle \in E^k(X)$ and by the inductive hypothesis the goal holds.

(e) In another case, $\langle a, b\rangle = \langle a_1 \wedge a_2, b_1 \wedge b_2\rangle = \langle a_1, b_1\rangle \wedge \langle a_2, b_2\rangle$ for some $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in E^K(X)$. Then by the inductive hypothesis

$$c \vee d \vee a_1 = c \vee d \vee b_1 \quad \text{and} \quad c \vee d \vee a_2 = c \vee d \vee b_2.$$

Thus

$$(c \vee d \vee a_1) \wedge (c \vee d \vee a_2) = (c \vee d \vee b_1) \wedge (c \vee d \vee b_2)$$

Then because **L** is distributive,

$$c \vee d \vee (a_1 \wedge a_2) = c \vee d \vee (b_1 \wedge b_2)$$

Therefore by substitution

$$c \vee d \vee a = c \vee d \vee b.$$

Additionally, by the inductive hypothesis

$$c \wedge d \wedge a_1 = c \wedge d \wedge b_1 \quad \text{and} \quad c \wedge d \wedge a_2 = c \wedge d \wedge b_2.$$

Thus

$$c \wedge d \wedge a_1 \wedge c \wedge d \wedge a_2 = c \wedge d \wedge b_1 \wedge c \wedge d \wedge b_2.$$

Then by associativity and commutativity of the lattice **L**,

$$(c \wedge c) \wedge (d \wedge d) \wedge (a_1 \wedge a_2) = (c \wedge c) \wedge (d \wedge d) \wedge (b_1 \wedge b_2).$$

Therefore, by substitution and lattice idempotency,

$$c \wedge d \wedge a = c \wedge d \wedge b.$$

(f) In the final case, $\langle a, b\rangle = \langle a_1 \vee a_2, b_1 \vee b_2\rangle = \langle a_1, b_1\rangle \vee \langle a_2, b_2\rangle$ for some $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in E^K(X)$. The proof in this case is dual to the proof in (e).

Therefore if $c \vee d \vee a = c \vee d \vee b$ and $c \wedge d \wedge a = c \wedge d \wedge b$ for all $\langle a, b\rangle \in E^k(X)$ then $c \vee d \vee a = c \vee d \vee b$ and $c \wedge d \wedge a = c \wedge d \wedge b$ for all $\langle a, b\rangle \in E^{k+1}(X)$.

Having proven the base case and inductive case, for all $k \in \mathbb{N}$ and $a, b \in L$, $c \wedge d \wedge a = c \wedge d \wedge b$ and $c \vee d \vee a = c \vee d \vee b$ when $\langle a, b\rangle \in E^k(X)$. Furthermore when $\langle a, b\rangle \in \Theta(c, d)$, $\langle a, b\rangle \in E^k(\{\langle c, d\rangle\})$ for some $k \in \mathbb{N}$. Therefore $c \wedge d \wedge a = c \wedge d \wedge b$ and $c \vee d \vee a = c \vee d \vee b$ when $\langle a, b\rangle \in \Theta(c, d)$. $\square$