Introduction to Universal Algebra

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Definition and Examples of Algebras

Operations

Definition

For A a nonempty set and n a nonnegative integer, we define $A^0 = \{\varnothing\}$ and, for $n > 0$, A^n is the set of n-tuples of elements from A.

An n-**ary operation** (or **function**) on A is any function f from A^n to A; n is the **arity** (or **rank**) of f. A **finitary operation** is an n-ary operation, for some n.

The image of $\langle a_1, \ldots, a_n \rangle$ under an n-ary operation f is denoted by $f(a_1, \ldots, a_n)$.

An operation f on A is called a **nullary operation** (or **constant**) if its arity is zero; it is completely determined by the image $f(\varnothing)$ in A of the only element $\varnothing$ in A^0. As such it is convenient to identify it with the element $f(\varnothing)$. Thus a nullary operation is thought of as an element of A.

An operation f on A is **unary**, **binary** or **ternary** if its arity is 1,2, or 3, respectively.

Languages and Algebras

Definition

A **language** (or **type**) of algebras is a set $\mathscr{F}$ of **function symbols** such that a nonnegative integer n is assigned to each member f of $\mathscr{F}$. This integer is called the **arity** (or **rank**) of f, and f is said to be an n-**ary function symbol**. The subset of n-ary function symbols in $\mathscr{F}$ is denoted by $\mathscr{F}_n$.

Definition

If $\mathscr{F}$ is a language of algebras, then an **algebra A of type** $\mathscr{F}$ is an ordered pair $\langle A, F\rangle$, where:

- A is a nonempty set;
- F is a family of finitary operations on A indexed by the language $\mathscr{F}$, such that corresponding to each n-ary function symbol f in $\mathscr{F}$, there is an n-ary operation $f^{\mathbf{A}}$ on A.

The set A is called the **universe** (or **underlying set**) of $\mathbf{A} = \langle A, F\rangle$.
The $f^{\mathbf{A}}$'s are called the **fundamental operations** of **A**.

More Algebraic Notation and Terminology

- If $\mathscr{F}$ is finite, say $\mathscr{F} = \{f_1, \ldots, f_k\}$, we often write $\langle A, f_1, \ldots, f_k \rangle$ for $\langle A, F \rangle$, usually adopting the convention:

$$\text{arity} f_1 \geq \text{arity} f_2 \geq \cdots \geq \text{arity} f_k.$$

- An algebra **A** is **unary** if all of its operations are unary.
  It is **mono-unary** if it has just one unary operation.
- **A** is a **groupoid** if it has just one binary operation. The operation is usually denoted by + or ·, and we write $a + b$ or $a \cdot b$ (or just ab) for the image of $\langle a, b \rangle$ under this operation and call it the **sum** or **product** of a and b, respectively.
- An algebra **A** is **finite** if $|A|$ is finite.
- An algebra **A** is **trivial** if $|A| = 1$.

Groups and Abelian Groups

- A **group G** is an algebra $\langle G, \cdot, {}^{-1}, 1 \rangle$ with a binary, a unary, and a nullary operation in which the following identities are true:
  - G1 $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$;
  - G2 $x \cdot 1 \approx 1 \cdot x \approx x$;
  - G3 $x \cdot x^{-1} \approx x^{-1} \cdot x \approx 1$.
- A group **G** is **Abelian** (or **commutative**) if the following identity is true:
  - G4 $x \cdot y \approx y \cdot x$.

Monoids and Quasigroups

- Groups are generalized to semigroups and monoids in one direction, and to quasigroups and loops in another direction.
- A **semigroup** is a groupoid $\langle G, \cdot \rangle$ in which (G1) is true.

  It is **commutative** (or **Abelian**) if (G4) holds.
- A **monoid** is an algebra $\langle M, \cdot, 1 \rangle$ with a binary and a nullary operation satisfying (G1) and (G2).
- A **quasigroup** is an algebra $\langle Q, /, \cdot, \backslash \rangle$ with three binary operations satisfying the following identities:

  Q1 $x \backslash (x \cdot y) \approx y; \quad (x \cdot y)/y \approx x;$

  Q2 $x \cdot (x \backslash y) \approx y; \quad (x/y) \cdot y \approx x.$
- A **loop** is a quasigroup with identity, i.e., an algebra $\langle Q, /, \cdot, \backslash, 1 \rangle$ which satisfies (Q1), (Q2) and (G2).

Rings

- A **ring** is an algebra $\langle R, +, \cdot, -, 0\rangle$, where $+$ and $\cdot$ are binary, $-$ is unary and 0 is nullary, satisfying the following conditions:
  - R1 $\langle R, +, -, 0\rangle$ is an Abelian group;
  - R2 $\langle R, \cdot\rangle$ is a semigroup;
  - R3 $x \cdot (y + z) \approx (x \cdot y) + (x \cdot z)$
    $(x + y) \cdot z \approx (x \cdot z) + (y \cdot z)$.
- A **ring with identity** is an algebra $\langle R, +, \cdot, -, 0, 1\rangle$, such that (R1)-(R3) and (G2) hold.

Modules and Algebras Over a (Fixed) Ring

- Let **R** be a given ring. A (**left**) **R-module** is an algebra $\langle M, +, -, 0, (f_r)_{r \in R} \rangle$, where $+$ is binary, $-$ is unary, 0 is nullary, and each f_r is unary, such that the following hold:
  - M1 $\langle M, +, -, 0 \rangle$ is an Abelian group;
  - M2 $f_r(x+y) \approx f_r(x) + f_r(y)$, for $r \in R$;
  - M3 $f_{r+s}(x) \approx f_r(x) + f_s(x)$ for $r, s \in R$;
  - M4 $f_r(f_s(x)) \approx f_{rs}(x)$, for $r, s \in R$.
- Let **R** be a ring with identity. A **unitary R-module** is an algebra as above satisfying (M1)-(M4) and:
  - M5 $f_1(x) \approx x$.
- Let **R** be a ring with identity. An **algebra over R** is an algebra $\langle A, +, \cdot, -, 0, (f_r)_{r \in R} \rangle$, such that the following hold:
  - A1 $\langle A, +, -, 0, (f_r)_{r \in R} \rangle$ is a unitary **R**-module;
  - A2 $\langle A, +, \cdot, -, 0 \rangle$ is a ring;
  - A3 $f_r(x \cdot y) \approx (f_r(x)) \cdot y \approx x \cdot f_r(y)$, for $r \in R$.

Semilattices and Lattices

- A **semilattice** is a semigroup $\langle S, \cdot \rangle$ which satisfies the commutative law (G4) and the idempotent law

  S1 $x \cdot x \approx x$.

- A **lattice** is an algebra $\langle L, \vee, \wedge \rangle$, with two binary operations which satisfies

  L1 (**commutative laws**)
  - (a) $x \vee y \approx y \vee x$;
  - (b) $x \wedge y \approx y \wedge x$;

  L2 (**associative laws**)
  - (a) $x \vee (y \vee z) \approx (x \vee y) \vee z$;
  - (b) $x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$;

  L3 (**idempotent laws**)
  - (a) $x \vee x \approx x$;
  - (b) $x \wedge x \approx x$;

  L4 (**absorption laws**)
  - (a) $x \approx x \vee (x \wedge y)$;
  - (b) $x \approx x \wedge (x \vee y)$.

- An algebra $\langle L, \vee, \wedge, 0, 1 \rangle$, with two binary and two nullary operations is a **bounded lattice** if it satisfies:

  BL1 $\langle L, \vee, \wedge \rangle$ is a lattice;

  BL2 $x \wedge 0 \approx 0$; $\quad x \vee 1 \approx 1$.

Subsection 2

Isomorphic Algebras and Subalgebras

Isomorphism

Definition

Let **A** and **B** be two algebras of the same type $\mathscr{F}$. Then a function $\alpha : A \to B$ is an **isomorphism** from **A** to **B** if:

- α is one-to-one and onto;
- for every n-ary $f \in \mathscr{F}$ and for all $a_1, \ldots, a_n \in A$, we have

$$\alpha(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{B}}(\alpha(a_1), \ldots, \alpha(a_n)).$$

We say **A** is **isomorphic** to **B**, written $\mathbf{A} \cong \mathbf{B}$, if there is an isomorphism from **A** to **B**.

- The properties of algebras that are invariant under isomorphism are called **algebraic properties**.
- Isomorphic algebras can be regarded as equal or the same, having the same algebraic structure, and differing only in the nature of the elements: The phrase "equal up to isomorphism" is often used.

Subalgebras and Subuniverses

Definition

Let **A** and **B** be two algebras of the same type. Then **B** is a **subalgebra** of **A** if $B \subseteq A$ and every fundamental operation of **B** is the restriction of the corresponding operation of **A**; i.e., for each function symbol f, $f^{\mathbf{B}}$ is $f^{\mathbf{A}}$ restricted to B. We write simply $\mathbf{B} \leq \mathbf{A}$.

A **subuniverse** of **A** is a subset B of A which is closed under the fundamental operations of **A**; i.e., if f is a fundamental n-ary operation of **A** and $a_1, \ldots, a_n \in B$ we would require $f(a_1, \ldots, a_n) \in B$.

- Thus, if **B** is a subalgebra of **A**, then B is a subuniverse of **A**.
- The empty set may be a subuniverse, but it is not the underlying set of any subalgebra.
- If **A** has nullary operations then every subuniverse contains them as well.

Embeddings (or Monomorphisms)

Definition

Let **A** and **B** be of the same type. A function $\alpha : A \to B$ is an **embedding** of **A** into **B** if α is one-to-one and satisfies

$$\alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) = f^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)).$$

Such an α is also called a **monomorphism**. For brevity we simply say "$\alpha : \mathbf{A} \to \mathbf{B}$ is an embedding". We say **A** can be **embedded** in **B** if there is an embedding of **A** into **B**.

Theorem

If $\alpha : \mathbf{A} \to \mathbf{B}$ is an embedding, then $\alpha(A)$ is a subuniverse of **B**.

- Let $\alpha : \mathbf{A} \to \mathbf{B}$ be an embedding. Then, for an n-ary function symbol f and $a_1,\ldots,a_n \in A$, $f^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)) = \alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) \in \alpha(A)$.

Definition

If $\alpha : \mathbf{A} \to \mathbf{B}$ is an embedding, $\alpha(\mathbf{A})$ denotes the subalgebra of **B** with universe $\alpha(A)$.

Structure Theorems in Algebra

- Let K be a class of algebras and let K_1 be a proper subclass of K.
- In practice, K may have been obtained from the process of abstraction of certain properties of K_1; or K_1 may be obtained from K by certain additional, more desirable, properties.
- Two basic questions arise in the quest for structure theorems:
  (1) Is every member of K isomorphic to some member of K_1?
  (2) Is every member of K embeddable in some member of K_1?

  Examples:
  - Every Boolean algebra is isomorphic to a field of sets.
  - Every group is isomorphic to a group of permutations.
  - A finite Abelian group is isomorphic to a direct product of cyclic groups.
  - A finite distributive lattice can be embedded in a power of the two-element distributive lattice.

Subsection 3

Algebraic Lattices and Subuniverses

Generated Subuniverses

Definition

Given an algebra $\mathbf{A}$, define, for every $X \subseteq A$,

$$\text{Sg}(X) = \bigcap\{B : X \subseteq B \text{ and } B \text{ is a subuniverse of } \mathbf{A}\}.$$

We read $\text{Sg}(X)$ as "the subuniverse generated by X".

Theorem

If we are given an algebra $\mathbf{A}$, then Sg is an algebraic closure operator on A.

- Observe that an arbitrary intersection of subuniverses of $\mathbf{A}$ is again a subuniverse. Hence Sg is a closure operator on A whose closed sets are precisely the subuniverses of A. Now, for any $X \subseteq A$, define

$$E(X) = X \cup \{f(a_1,\ldots,a_n) : f \text{ is a fundamental } n\text{-ary operation on } A, n \in \omega, \text{ and } a_1,\ldots,a_n \in X\}.$$

Generated Subuniverses (Algebraicity)

- We defined, for $X \subseteq A$,

$$E(X) = X \cup \{f(a_1,\ldots,a_n) : f \text{ is a fundamental } n\text{-ary operation on } A, n \in \omega, \text{ and } a_1,\ldots,a_n \in X\}.$$

Then define $E^n(X)$, for $n \geq 0$, by induction, as follows:

$$E^0(X) = X, \quad E^{n+1}(X) = E(E^n(X)).$$

As all the fundamental operations on A are finitary and $X \subseteq E(X) \subseteq E^2(X) \subseteq \cdots$, we can show that

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

Therefore, if $a \in \mathrm{Sg}(X)$, then $a \in E^n(X)$, for some $n \in \omega$. Hence, for some finite $Y \subseteq X$, $a \in E^n(Y)$. Thus, $a \in \mathrm{Sg}(Y)$. But this says Sg is an algebraic closure operator.

The Lattice of Subuniverses

Corollary

If $\mathbf{A}$ is an algebra then $\mathbf{L}_{\mathrm{Sg}}$, the lattice of subuniverses of $\mathbf{A}$ is an algebraic lattice.

- The corollary says that the subuniverses of $\mathbf{A}$, with $\subseteq$ as the partial order, form an algebraic lattice.

Definition

Given an algebra $\mathbf{A}$, $\mathrm{Sub}(\mathbf{A})$ denotes the set of subuniverses of $\mathbf{A}$, and $\mathbf{Sub}(\mathbf{A})$ is the corresponding algebraic lattice, the **lattice of subuniverses of A**.

For $X \subseteq A$, we say X **generates A** (or $\mathbf{A}$ is **generated by** X; or X is a **set of generators of A**) if $\mathrm{Sg}(X) = A$.

The algebra $\mathbf{A}$ is **finitely generated** if it has a finite set of generators.

Algebraic Lattices and Lattices of Subuniverses

- Every algebraic lattice is isomorphic to the lattice of subuniverses of some algebra:

Theorem (Birkhoff and Frink)

If $\mathbf{L}$ is an algebraic lattice, then $\mathbf{L} \cong \mathbf{Sub}(\mathbf{A})$, for some algebra $\mathbf{A}$.

- Let C be an algebraic closure operator on a set A, such that $\mathbf{L} \cong \mathbf{L}_C$. For each finite subset B of A and each $b \in C(B)$, define an n-ary function $f_{B,b}$ on A, where $n = |B|$, by $f_{B,b}(a_1,\ldots,a_n) = \begin{cases} b, & \text{if } B = \{a_1,\ldots,a_n\} \\ a_1, & \text{otherwise} \end{cases}$. Call the resulting algebra $\mathbf{A}$. Then clearly $f_{B,b}(a_1,\ldots,a_n) \in C(\{a_1,\ldots,a_n\})$. Hence, for $X \subseteq A$, $\mathrm{Sg}(X) \subseteq C(X)$. On the other hand, $C(X) = \bigcup\{C(B) : B \subseteq X \text{ and B is finite}\}$ and, for B finite, $C(B) = \{f_{B,b}(a_1,\ldots,a_n) : B = \{a_1,\ldots,a_n\}, b \in C(B)\} \subseteq \mathrm{Sg}(B) \subseteq \mathrm{Sg}(X)$ imply $C(X) \subseteq \mathrm{Sg}(X)$. Hence, $C(X) \subseteq \mathrm{Sg}(X)$. Thus, $\mathbf{L}_C = \mathbf{Sub}(\mathbf{A})$. So $\mathbf{Sub}(\mathbf{A}) \cong \mathbf{L}$.

Algebras Generated by Sets of Specific Cardinality

- For a given type there cannot be "too many" algebras (up to isomorphism) generated by sets no larger than a given cardinality.
- Recall that ω is the smallest infinite cardinal.

Corollary

If $\mathbf{A}$ is an algebra and $X \subseteq A$, then

$$|\mathrm{Sg}(X)| \leq |X| + |\mathscr{F}| + \omega.$$

- Using induction on n, one has

$$|E^n(X)| \leq |X| + |\mathscr{F}| + \omega.$$

  - $|E^0(X)| = |X| \leq |X| + |\mathscr{F}| + \omega$;
  - $|E^{n+1}(X)| = |E(E^n(X))| \leq |E^n(X)| + |\mathscr{F}| + \omega \leq |X| + |\mathscr{F}| + \omega$.

  So the result follows from $\mathrm{Sg}(X) = X \cup E(X) \cup E^2(X) \cup \cdots$.

n-ary Closure Operators

Definition

Let C be a closure operator on A. For $n < \omega$, let C_n be the function defined on Su(A) by

$$C_n(X) = \bigcup \{C(Y) : Y \subseteq X, |Y| \leq n\}.$$

We say that C is n-**ary**, if

$$C(X) = C_n(X) \cup C_n^2(X) \cup \cdots,$$

where:

- $C_n^1(X) = C_n(X)$;
- $C_n^{k+1}(X) = C_n(C_n^k(X))$.

Generation and n-ary Closure Operators

Lemma

Let $\mathbf{A}$ be an algebra all of whose fundamental operations have arity at most n. Then Sg is an n-ary closure operator on A.

- Recall the definition

$$\begin{aligned} E(X) &= X \cup \{f(a_1, \ldots, a_n) : f \text{ is a fundamental } n\text{-ary operation} \\ &\qquad \text{on } A, n \in \omega, \text{ and } a_1, \ldots, a_n \in X\}. \end{aligned}$$

Note that $E(X) \subseteq \mathrm{Sg}_n(X) \subseteq \mathrm{Sg}(X)$. Hence,

$$\begin{aligned} \mathrm{Sg}(X) &= X \cup E(X) \cup E^2(X) \cup \cdots \\ &\subseteq \mathrm{Sg}_n(X) \cup \mathrm{Sg}_n^2(X) \cup \cdots \\ &\subseteq \mathrm{Sg}(X). \end{aligned}$$

So $\mathrm{Sg}(X) = \mathrm{Sg}_n(X) \cup \mathrm{Sg}_n^2(X) \cup \cdots$.

Subsection 4

Congruences and Quotient Algebras

The Compatibility Condition

Definition

Let **A** be an algebra of type $\mathscr{F}$ and let $\theta \in \text{Eq}(A)$. Then θ is a **congruence** on **A** if θ satisfies the following **compatibility property**:

CP For each n-ary function symbol $f \in \mathscr{F}$, and elements $a_i, b_i \in A$, if $a_i \ \theta \ b_i$ holds, for $1 \le i \le n$, then $f^{\mathbf{A}}(a_1, \dots, a_n) \ \theta \ f^{\mathbf{A}}(b_1, \dots, b_n)$ holds.

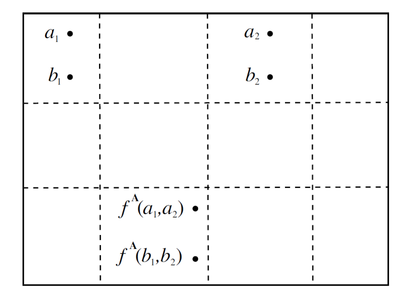
- The compatibility property allows introducing an algebraic structure on the set of equivalence classes A/θ:

  If $a_1, \dots, a_n$ are elements of A and f is an n-ary symbol in $\mathscr{F}$, then the easiest choice of an equivalence class to be the value of f applied to $\langle a_1/\theta, \dots, a_n/\theta \rangle$ is $f^{\mathbf{A}}(a_1, \dots, a_n)/\theta$.

  This will indeed define a function on A/θ iff (CP) holds.

Illustration of the Algebraic Structure on A/θ

- The Compatibility Condition for a binary operation is illustrated below:



A is subdivided into the equivalence classes of θ.

Then selecting a_1, b_1 in the same equivalence class and a_2, b_2 in the same equivalence class, we want $f^{\mathbf{A}}(a_1, a_2)$ and $f^{\mathbf{A}}(b_1, b_2)$ to be in the same equivalence class.

Quotient Algebras

Definition

The set of all congruences on an algebra **A** is denoted by Con**A**. Let θ be a congruence on an algebra **A**. Then the **quotient algebra of A by** θ, written $\mathbf{A}/\theta$, is the algebra whose universe is A/θ and whose fundamental operations satisfy

$$f^{\mathbf{A}/\theta}(a_1/\theta,\ldots,a_n/\theta) = f^{\mathbf{A}}(a_1,\ldots,a_n)/\theta,$$

where $a_1,\ldots,a_n \in A$ and f is an n-ary function symbol in $\mathscr{F}$.

- Note that quotient algebras of **A** are of the same type as **A**.

Group Congruences and Normal Subgroups

- Let **G** be a group.

  Then one can establish the following connection between congruences on **G** and normal subgroups of **G**:

  (a) If $\theta \in \text{Con}\mathbf{G}$, then $1/\theta$ is the universe of a normal subgroup of **G**;
  For $a, b \in G$, we have $\langle a, b\rangle \in \theta$ iff $\langle a \cdot b^{-1}, 1\rangle \in \theta$ iff $a \cdot b^{-1} \in 1/\theta$.

  (b) If **N** is a normal subgroup of **G**, then the binary relation defined on G by

  $$\langle a, b\rangle \in \theta \quad \text{iff} \quad a \cdot b^{-1} \in N$$

  is a congruence on **G**, with $1/\theta = N$.

  Thus, the mapping $\theta \mapsto 1/\theta$ is an order-preserving bijection between congruences on **G** and normal subgroups of **G**.

Ring Congruences and Ideals

- Let **R** be a ring.

  The following establishes a similar connection between the congruences on **R** and ideals of **R**:

  (a) If $\theta \in \mathrm{Con}\mathbf{R}$, then $0/\theta$ is an ideal of **R**;
  For $a, b \in R$, we have $\langle a, b\rangle \in \theta$ iff $\langle a-b, 0\rangle \in \theta$ iff $a - b \in 0/\theta$.

  (b) If I is an ideal of **R**, then the binary relation θ defined on R by

  $$\langle a, b\rangle \in \theta \quad \text{iff} \quad a - b \in I$$

  is a congruence on **R**, with $0/\theta = I$.

  Thus the mapping $\theta \mapsto 0/\theta$ is an order-preserving bijection between congruences on **R** and ideals of **R**.

Lattice Congruences

- In the preceding two examples any congruence on the algebra (group or ring) was determined by a single equivalence class of the congruence ($1/\theta$ and $0/\theta$, respectively).
- The next example shows this need not be the case:

  Let **L** be a lattice which is a chain, and let θ be an equivalence relation on L, such that the equivalence classes of θ are convex subsets of L (i.e., if $a\ \theta\ b$ and $a \leq c \leq b$, then $a\ \theta\ c$.) Then θ is a congruence on **L**.

Lattice Structure of Con**A**

Theorem

$\langle \text{Con}\mathbf{A}, \subseteq\rangle$ is a complete sublattice of $\langle \text{Eq}(A), \subseteq\rangle$, the lattice of equivalence relations on A.

- Con**A** is closed under arbitrary intersections. For arbitrary joins in Con**A** suppose $\theta_i \in \text{Con}\mathbf{A}$ for $i \in I$. Then, if f is a fundamental n-ary operation of **A** and

$$\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle \in \bigvee_{i \in I} \theta_i,$$

where $\bigvee$ is the join of $\text{Eq}(A)$, then, there exist $i_0, \ldots, i_k \in I$, for some $k \in \omega$, such that

$$\langle a_j, b_j\rangle \in \theta_{i_0} \circ \theta_{i_1} \circ \cdots \circ \theta_{i_k}, \quad 1 \le j \le n.$$

That is, for all $j = 1, \ldots, n$, there exist $c_{j0}, \ldots, c_{j(k-1)} \in A$, such that

$$a_j \ \theta_{i_0} \ c_{j0} \ \theta_{i_1} \ \cdots \ \theta_{i_{k-1}} \ c_{j(k-1)} \ \theta_{i_k} \ b_j.$$

Lattice Structure of Con**A** (Cont'd)

- For all $j = 1, \ldots, n$, there exist $c_{j0}, \ldots, c_{j(k-1)} \in A$, such that

$$a_j \ \theta_{i_0} \ c_{j0} \ \theta_{i_1} \ \cdots \ \theta_{i_{k-1}} \ c_{j(k-1)} \ \theta_{i_k} \ b_j.$$

Since $\theta_i \in \mathrm{Con}\mathbf{A}$, for all $i \in I$, we get

$$f(a_1, \ldots, a_n) \ \theta_{i_0} \ f(c_{10}, \ldots, c_{n0}) \ \theta_{i_1} \ \cdots \ \theta_{i_{k-1}} \ f(c_{1(k-1)}, \ldots, c_{n(k-1)}) \ \theta_{i_k} \ f(b_1, \ldots, b_n).$$

Hence

$$\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n) \rangle \in \theta_{i_0} \circ \theta_{i_1} \circ \cdots \circ \theta_{i_k} \subseteq \bigvee_{i \in I} \theta_i.$$

Therefore, $\bigvee_{i \in I} \theta_i$ is a congruence relation on **A**.

Definition

The **congruence lattice of A** denoted by **ConA**, is the lattice whose universe is Con**A**, and meets and joins are calculated the same as when working with equivalence relations.

Congruence Lattices of Algebras

Theorem

For **A** an algebra, there is an algebraic closure operator Θ on $A \times A$, such that the closed subsets of $A \times A$ are precisely the congruences on **A**. Hence **ConA** is an algebraic lattice.

- We define an algebraic structure on $A \times A$. For each n-ary function symbol f in the type of **A**, define a corresponding n-ary function f on $A \times A$ by $f(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) = \langle f^{\mathbf{A}}(a_1, \ldots, a_n), f^{\mathbf{A}}(b_1, \ldots, b_n)\rangle$. Then we add:
  - the nullary operations $\langle a, a\rangle$, for each $a \in A$;
  - a unary operation s, defined by $s(\langle a, b\rangle) = \langle b, a\rangle$;
  - a binary operation t defined by $t(\langle a, b\rangle, \langle c, d\rangle) = \begin{cases} \langle a, d\rangle, & \text{if } b = c \\ \langle a, b\rangle, & \text{otherwise} \end{cases}$.

  Now we can verify that B is a subuniverse of this new algebra iff B is a congruence on **A**. Let Θ be the Sg closure operator on $A \times A$ for the algebra we have just described. Thus, **ConA** is an algebraic lattice.

Compact Elements of **ConA** and Congruence Generation

- The compact members of **ConA** are the finitely generated members $\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle)$ of **ConA**.

Definition

For **A** an algebra and $a_1, \ldots, a_n \in A$, let $\Theta(a_1, \ldots, a_n)$ denote the congruence generated by $\{\langle a_i, a_j\rangle : 1 \le i, j \le n\}$, i.e., the smallest congruence such that $a_1, \ldots, a_n$ are in the same equivalence class. The congruence $\Theta(a_1, a_2)$ is called a **principal congruence**. For arbitrary $X \subseteq A$, let $\Theta(X)$ be defined to mean the congruence generated by $X \times X$.

The Case of Groups and Rings

(1) If **G** is a group and $a,b,c,d \in G$, then $\langle a,b\rangle \in \Theta(c,d)$ iff ab^{-1} is a product of conjugates of cd^{-1} and conjugates of dc^{-1}.

This follows from the fact that the smallest normal subgroup of **G** containing a given element u has as its universe the set of all products of conjugates of u and conjugates of u^{-1}.

(2) If **R** is a ring with unity and $a,b,c,d \in R$, then $\langle a,b\rangle \in \Theta(c,d)$ iff $a-b$ is of the form $\sum_{1\le i\le n} r_i(c-d)s_i$, where $r_i,s_i \in R$.

This follows from the fact that the smallest ideal of **R** containing a given element e of R is precisely the set $\{\sum_{1\le i\le n} r_i e s_i : r_i,s_i \in R, n \ge 1\}$.

Properties of Congruences

Theorem

Let $\mathbf{A}$ be an algebra, and suppose $a_1, b_1, \ldots, a_n, b_n \in A$ and $\theta \in \mathrm{Con}\mathbf{A}$. Then:

(a) $\Theta(a_1, b_1) = \Theta(b_1, a_1)$;

(b) $\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) = \Theta(a_1, b_1) \vee \cdots \vee \Theta(a_n, b_n)$;

(c) $\Theta(a_1, \ldots, a_n) = \Theta(a_1, a_2) \vee \Theta(a_2, a_3) \vee \cdots \vee \Theta(a_{n-1}, a_n)$;

(d) $\theta = \bigcup\{\Theta(a, b) : \langle a, b\rangle \in \theta\} = \bigvee\{\Theta(a, b) : \langle a, b\rangle \in \theta\}$;

(e) $\theta = \bigcup\{\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) : \langle a_i, b_i\rangle \in \theta, n \geq 1\}$.

(a) $\langle b_1, a_1\rangle \in \Theta(a_1, b_1)$. Hence, $\Theta(b_1, a_1) \subseteq \Theta(a_1, b_1)$. By symmetry, $\Theta(a_1, b_1) = \Theta(b_1, a_1)$.

(b) For $1 \leq i \leq n$, $\langle a_i, b_i\rangle \in \Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle)$. Hence $\Theta(a_i, b_i) \subseteq \Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle)$, whence $\Theta(a_1, b_1) \vee \cdots \vee \Theta(a_n, b_n) \subseteq \Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle)$.

Properties of Congruences (Cont'd)

On the other hand, for $1 \leq i \leq n$,
$\langle a_i, b_i \rangle \in \Theta(a_i, b_i) \subseteq \Theta(a_1, b_1) \vee \cdots \vee \Theta(a_n, b_n)$. So
$\{\langle a_1, b_1 \rangle, \ldots, \langle a_n, b_n \rangle\} \subseteq \Theta(a_1, b_1) \vee \cdots \vee \Theta(a_n, b_n)$. Hence,
$\Theta(\langle a_1, b_1 \rangle, \ldots, \langle a_n, b_n \rangle) \subseteq \Theta(a_1, b_1) \vee \cdots \vee \Theta(a_n, b_n)$. So
$\Theta(\langle a_1, b_1 \rangle, \ldots, \langle a_n, b_n \rangle) = \Theta(a_1, b_1) \vee \cdots \vee \Theta(a_n, b_n)$.

(c) For $1 \leq i \leq n-1$, $\langle a_i, a_{i+1} \rangle \in \Theta(a_1, \ldots, a_n)$. So $\Theta(a_i, a_{i+1}) \subseteq \Theta(a_1, \ldots, a_n)$. Hence, $\Theta(a_1, a_2) \vee \cdots \vee \Theta(a_{n-1}, a_n) \subseteq \Theta(a_1, \ldots, a_n)$.

Conversely, for $1 \leq i < j \leq n$, $\langle a_i, a_j \rangle \in \Theta(a_i, a_{i+1}) \circ \cdots \circ \Theta(a_{j-1}, a_j)$. So,
$\langle a_i, a_j \rangle \in \Theta(a_i, a_{i+1}) \vee \cdots \vee \Theta(a_{j-1}, a_j)$. Hence,
$\langle a_i, a_j \rangle \in \Theta(a_1, a_2) \vee \cdots \vee \Theta(a_{n-1}, a_n)$. By Part (a),
$\Theta(a_1, \ldots, a_n) \subseteq \Theta(a_1, a_2) \vee \cdots \vee \Theta(a_{n-1}, a_n)$. Therefore,
$\Theta(a_1, \ldots, a_n) = \Theta(a_1, a_2) \vee \cdots \vee \Theta(a_{n-1}, a_n)$.

Properties of Congruences (Conclusion)

(d) For $\langle a, b\rangle \in \theta$, $\langle a, b\rangle \in \Theta(a, b) \subseteq \theta$. So $\theta \subseteq \bigcup\{\Theta(a, b) : \langle a, b\rangle \in \theta\} \subseteq \bigvee\{\Theta(a, b) : \langle a, b\rangle \in \theta\} \subseteq \theta$. Hence $\theta = \bigcup\{\Theta(a, b) : \langle a, b\rangle \in \theta\} = \bigvee\{\Theta(a, b) : \langle a, b\rangle \in \theta\}$.

(e) For $\langle a, b\rangle \in \theta$, $\langle a, b\rangle \in \Theta(a, b) \subseteq \bigcup\{\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) : \langle a_i, b_i\rangle \in \theta, n \geq 1\}$. So $\theta \subseteq \bigcup\{\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) : \langle a_i, b_i\rangle \in \theta, n \geq 1\}$.

Conversely, if $n \geq 1$ and $\langle a_i, b_i\rangle \in \theta$, for all $1 \leq i \leq n$, then $\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) \subseteq \theta$. Hence, $\bigcup\{\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) : \langle a_i, b_i\rangle \in \theta, n \geq 1\} \subseteq \theta$.

Therefore, $\theta = \bigcup\{\Theta(\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle) : \langle a_i, b_i\rangle \in \theta, n \geq 1\}$.

On Properties of Congruence Lattices

- In 1963 Grätzer and Schmidt proved:

  For every algebraic lattice $\mathbf{L}$, there is an algebra $\mathbf{A}$, such that $\mathbf{L} \cong \mathbf{ConA}$.
- For particular classes of algebras one might find that some additional properties hold for the corresponding classes of congruence lattices:
  - The congruence lattices of lattices satisfy the distributive law;
  - The congruence lattices of groups (or rings) satisfy the modular law.

Congruence-Distributivity and Congruence-Permutability

Definition

An algebra **A** is **congruence-distributive** (**congruence-modular**) if **ConA** is a distributive (modular) lattice.
If $\theta_1, \theta_2 \in \text{Con}\mathbf{A}$ and

$$\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1,$$

then we say θ_1 and θ_2 are **permutable**, or θ_1 and θ_2 **permute**.
A is **congruence-permutable** if every pair of congruences on **A** permutes.
A class K of algebras is **congruence-distributive**, **congruence-modular**, respectively **congruence-permutable** iff every algebra in K has the desired property.

Characterization of Congruence Permutability

Theorem

Let **A** be an algebra and suppose $\theta_1, \theta_2 \in \text{Con}\mathbf{A}$. Then the following are equivalent:

(a) $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$;

(b) $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$;

(c) $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$.

(a)⇒(b): Recall that

$$\theta_1 \vee \theta_2 = \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \cdots.$$

By hypothesis, since, for any equivalence relation θ, we have $\theta \circ \theta = \theta$, we get $\theta_1 \vee \theta_2 = \theta_1 \cup (\theta_1 \circ \theta_2) = \theta_1 \circ \theta_2$.

Characterization of Congruence Permutability (Cont'd)

(c)⇒(a): Suppose $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$. Apply the relational inverse operation $^\vee$ to get $(\theta_1 \circ \theta_2)^\vee \subseteq (\theta_2 \circ \theta_1)^\vee$. Hence, we get $\theta_2^\vee \circ \theta_1^\vee \subseteq \theta_1^\vee \circ \theta_2^\vee$. But the inverse of an equivalence relation is just that equivalence relation, whence $\theta_2 \circ \theta_1 \subseteq \theta_1 \circ \theta_2$. We conclude that $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$.

(b)⇒(c): We have $\theta_2 \circ \theta_1 \subseteq \theta_1 \vee \theta_2$. Thus, from (b) we deduce $\theta_2 \circ \theta_1 \subseteq \theta_1 \circ \theta_2$. Then, from (c)⇒(a) it follows that $\theta_2 \circ \theta_1 = \theta_1 \circ \theta_2$. Hence (c) holds.

Congruence-Permutability Implies Congruence-Modularity

Theorem (Birkhoff)

If $\mathbf{A}$ is congruence-permutable, then $\mathbf{A}$ is congruence-modular.

- Let $\theta_1, \theta_2, \theta_3 \in \mathrm{Con}\mathbf{A}$, with $\theta_1 \subseteq \theta_2$. We want to show that

$$\theta_2 \cap (\theta_1 \vee \theta_3) \subseteq \theta_1 \vee (\theta_2 \cap \theta_3).$$

Suppose $\langle a, b\rangle \in \theta_2 \cap (\theta_1 \vee \theta_3)$. Then, since $\theta_1 \vee \theta_3 = \theta_1 \circ \theta_3$, there is a c, such that $a \; \theta_1 \; c \; \theta_3 \; b$. By symmetry, $\langle c, a\rangle \in \theta_1$. Hence $\langle c, a\rangle \in \theta_2$. Then, by transitivity, $\langle c, b\rangle \in \theta_2$. Thus, $\langle c, b\rangle \in \theta_2 \cap \theta_3$. So we get $a \; \theta_1 \; c \; (\theta_2 \cap \theta_3) \; b$. Therefore,

$$\langle a, b\rangle \in \theta_1 \circ (\theta_2 \cap \theta_3) \subseteq \theta_1 \vee (\theta_2 \cap \theta_3).$$

Subsection 5

Homomorphisms and the Homomorphism Theorems

Homomorphisms

Definition

Suppose **A** and **B** are two algebras of the same type $\mathscr{F}$. A mapping $\alpha : A \to B$ is called a **homomorphism** from **A** to **B** if

$$\alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) = f^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)),$$

for each n-ary f in $\mathscr{F}$ and each sequence $a_1,\ldots,a_n$ from A.

If, in addition, the mapping α is onto, then α is called an **epimorphism** and **B** is said to be a **homomorphic image** of **A**. In this terminology an **isomorphism** is a homomorphism which is one-to-one and onto.

In case $\mathbf{A} = \mathbf{B}$, a homomorphism is also called an **endomorphism** and an isomorphism is referred to as an **automorphism**.

The phrase "$\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism" is often used to express the fact that α is a homomorphism from **A** to **B**.

Example: Lattice, group, ring, module, and monoid homomorphisms are all special cases of homomorphisms as defined above.

Equality of Homomorphisms

Theorem

Let $\mathbf{A}$ be an algebra generated by a set X. If $\alpha : \mathbf{A} \to \mathbf{B}$ and $\beta : \mathbf{A} \to \mathbf{B}$ are two homomorphisms which agree on X (i.e., $\alpha(a) = \beta(a)$, for $a \in X$), then $\alpha = \beta$.

- Recall the definition of E:

$$\begin{array}{rcl} E(X) & = & X \cup \{f(a_1, \ldots, a_n) : f \text{ is a fundamental } n\text{-ary operation} \\ & & \text{on } A, n \in \omega, \text{ and } a_1, \ldots, a_n \in X\}. \end{array}$$

  Note that if α and β agree on X, then α and β agree on $E(X)$: If f is an n-ary function symbol and $a_1, \ldots, a_n \in X$, then

$$\begin{array}{rcl} \alpha(f^{\mathbf{A}}(a_1, \ldots, a_n)) & = & f^{\mathbf{B}}(\alpha(a_1), \ldots, \alpha(a_n)) \\ & = & f^{\mathbf{B}}(\beta(a_1), \ldots, \beta(a_n)) \\ & = & \beta(f^{\mathbf{A}}(a_1, \ldots, a_n)). \end{array}$$

  Thus, by induction, if α and β agree on X, then they agree on $E^n(X)$, for $n < \omega$. Hence, they agree on $\mathrm{Sg}(X)$.

Images and Inverse Images of Subuniverses

Theorem

Let $\alpha : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Then the image of a subuniverse of $\mathbf{A}$ under α is a subuniverse of $\mathbf{B}$, and the inverse image of a subuniverse of $\mathbf{B}$ is a subuniverse of $\mathbf{A}$.

- Let S be a subuniverse of $\mathbf{A}$. Let f be an n-ary member of $\mathscr{F}$ and let $a_1, \ldots, a_n \in S$. Then $f^{\mathbf{B}}(\alpha(a_1), \ldots, \alpha(a_n)) = \alpha(f^{\mathbf{A}}(a_1, \ldots, a_n)) \in \alpha(S)$. So $\alpha(S)$ is a subuniverse of $\mathbf{B}$.

  If S is a subuniverse of $\mathbf{B}$ and $\alpha(a_1), \ldots, \alpha(a_n) \in S$, then, by the preceding equation, $\alpha(f^{\mathbf{A}}(a_1, \ldots, a_n)) \in S$. So $f^{\mathbf{A}}(a_1, \ldots, a_n)$ is in $\alpha^{-1}(S)$. Thus, $\alpha^{-1}(S)$ is a subuniverse of $\mathbf{A}$.

Definition

If $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism and $\mathbf{C} \leq \mathbf{A}$, $\mathbf{D} \leq \mathbf{B}$, let $\alpha(\mathbf{C})$ be the subalgebra of $\mathbf{B}$, with universe $\alpha(C)$, and let $\alpha^{-1}(\mathbf{D})$ be the subalgebra of $\mathbf{A}$, with universe $\alpha^{-1}(D)$, provided $\alpha^{-1}(D) \neq \emptyset$.

Composition of Homomorphisms

Theorem

Suppose $\alpha : \mathbf{A} \to \mathbf{B}$ and $\beta : \mathbf{B} \to \mathbf{C}$ are homomorphisms. Then the composition $\beta \circ \alpha$ is a homomorphism from $\mathbf{A}$ to $\mathbf{C}$.

- For f an n-ary function symbol and $a_1, \ldots, a_n \in A$, we have

$$\begin{array}{rcl}(\beta \circ \alpha)(f^{\mathbf{A}}(a_1, \ldots, a_n)) & = & \beta(\alpha(f^{\mathbf{A}}(a_1, \ldots, a_n))) \\ & = & \beta(f^{\mathbf{B}}(\alpha(a_1), \ldots, \alpha(a_n))) \\ & = & f^{\mathbf{C}}(\beta(\alpha(a_1)), \ldots, \beta(\alpha(a_n))) \\ & = & f^{\mathbf{C}}((\beta \circ \alpha)(a_1), \ldots, (\beta \circ \alpha)(a_n)).\end{array}$$

Homomorphisms and Generation

Theorem

If $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism and X is a subset of $\mathbf{A}$, then

$$\alpha(\mathrm{Sg}(X)) = \mathrm{Sg}(\alpha(X)).$$

- We have, for all $Y \subseteq A$,

$$\begin{array}{rcl}
\alpha(E(Y)) & = & \alpha(Y \cup \{f^{\mathbf{A}}(a_1,\ldots,a_n) : f \in \mathscr{F}_n, n \in \omega, a_1,\ldots,a_n \in Y\}) \\
 & = & \alpha(Y) \cup \{\alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) : f \in \mathscr{F}_n, n \in \omega, a_1,\ldots,a_n \in Y\} \\
 & = & \alpha(Y) \cup \{f^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)) : f \in \mathscr{F}_n, n \in \omega, a_1,\ldots,a_n \in Y\} \\
 & = & \alpha(Y) \cup \{f^{\mathbf{B}}(b_1,\ldots,b_n) : f \in \mathscr{F}_n, n \in \omega, b_1,\ldots,b_n \in \alpha(Y)\} \\
 & = & E(\alpha(Y)).
\end{array}$$

Thus, by induction on n, $\alpha(E^n(X)) = E^n(\alpha(X))$, for $n \geq 1$. Hence

$$\begin{array}{rcl}
\alpha(\mathrm{Sg}(X)) & = & \alpha(X \cup E(X) \cup E^2(X) \cup \cdots) \\
 & = & \alpha(X) \cup \alpha(E(X)) \cup \alpha(E^2(X)) \cup \cdots \\
 & = & \alpha(X) \cup E(\alpha(X)) \cup E^2(\alpha(X)) \cup \cdots = \mathrm{Sg}(\alpha(X)).
\end{array}$$

The Kernel of a Homomorphism

Definition

Let $\alpha : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Then the **kernel** of α, written $\ker(\alpha)$, and sometimes just $\ker\alpha$, is defined by

$$\ker(\alpha) = \{\langle a, b\rangle \in A^2 : \alpha(a) = \alpha(b)\}.$$

Theorem

Let $\alpha : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Then $\ker(\alpha)$ is a congruence on $\mathbf{A}$.

- If $\langle a_i, b_i\rangle \in \ker(\alpha)$, for $1 \le i \le n$ and f is n-ary in $\mathscr{F}$, then

$$\begin{aligned} \alpha(f^{\mathbf{A}}(a_1,\dots,a_n)) &= f^{\mathbf{B}}(\alpha(a_1),\dots,\alpha(a_n)) \\ &= f^{\mathbf{B}}(\alpha(b_1),\dots,\alpha(b_n)) \\ &= \alpha(f^{\mathbf{A}}(b_1,\dots,b_n)). \end{aligned}$$

  Hence $\langle f^{\mathbf{A}}(a_1,\dots,a_n), f^{\mathbf{A}}(b_1,\dots,b_n)\rangle \in \ker(\alpha)$. Clearly $\ker(\alpha)$ is an equivalence relation. Thus, $\ker(\alpha)$ is actually a congruence on $\mathbf{A}$.

The Natural Map

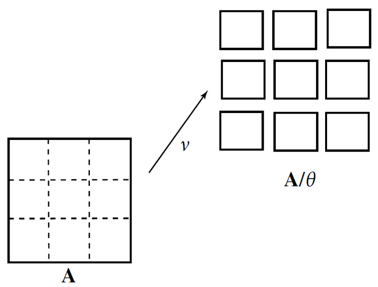
Definition

Let $\mathbf{A}$ be an algebra and let $\theta \in \mathrm{Con}\mathbf{A}$. The **natural map** $\nu_\theta : A \to A/\theta$ is defined by

$$\nu_\theta(a) = a/\theta.$$

When there is no ambiguity we write simply ν instead of ν_θ.

- The figure shows how one might visualize the natural map:



The Natural Homomorphism

Theorem

The natural map from an algebra to a quotient of the algebra is an onto homomorphism.

- Let $\theta \in \mathrm{Con}\mathbf{A}$ and let $\nu : A \to A/\theta$ be the natural map. Then, for f an n-ary function symbol and $a_1, \ldots, a_n \in A$, we have

$$\begin{array}{rcl} \nu(f^{\mathbf{A}}(a_1, \ldots, a_n)) & = & f^{\mathbf{A}}(a_1, \ldots, a_n)/\theta \\ & = & f^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta) \\ & = & f^{\mathbf{A}/\theta}(\nu(a_1), \ldots, \nu(a_n)). \end{array}$$

  So ν is a homomorphism. Clearly ν is onto.

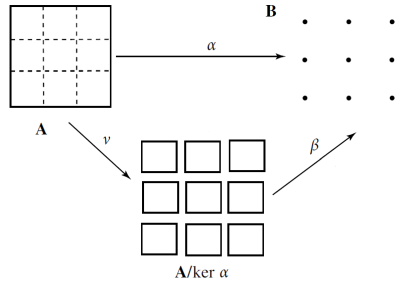
Definition

The **natural homomorphism** from an algebra to a quotient of the algebra is given by the natural map.

The Homomorphism Theorem

Theorem (Homomorphism Theorem)

Suppose $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism onto $\mathbf{B}$. Then there is an isomorphism β from $\mathbf{A}/\ker(\alpha)$ to $\mathbf{B}$ defined by $\alpha = \beta \circ \nu$, where ν is the natural homomorphism from $\mathbf{A}$ to $\mathbf{A}/\ker(\alpha)$.



- First note that if $\alpha = \beta \circ \nu$, then we must have $\beta(a/\theta) = \alpha(a)$. The second of these equalities does indeed define a function β and β satisfies $\alpha = \beta \circ \nu$. We verify that β is a bijection:
  - If $b \in B$, exists $a \in A$, such that $b = \alpha(a)$. Then $\beta(a/\ker\alpha) = \alpha(a) = b$;
  - Suppose $a, a' \in A$. Then $\beta(a/\ker\alpha) = \beta(a'/\ker\alpha)$ iff $\alpha(a) = \alpha(a')$ iff $\langle a, a' \rangle \in \ker\alpha$ iff $a/\ker\alpha = a'/\ker\alpha$.

The Homomorphism Theorem (Cont'd)

- To show that β is actually an isomorphism, suppose f is an n-ary function symbol and $a_1,\ldots,a_n \in A$. Then

$$\begin{array}{rcl}\beta(f^{\mathbf{A}/\theta}(a_1/\theta,\ldots,a_n/\theta)) & = & \beta(f^{\mathbf{A}}(a_1,\ldots,a_n)/\theta) \\ & = & \alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) \\ & = & f^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)) \\ & = & f^{\mathbf{B}}(\beta(a_1/\theta),\ldots,\beta(a_n/\theta)).\end{array}$$

- An algebra is a homomorphic image of an algebra **A** iff it is isomorphic to a quotient of the algebra **A**.

  Thus, the "external" problem of finding all homomorphic images of **A** reduces to the "internal" problem of finding all congruences on **A**.
- The Homomorphism Theorem is also called "The First Isomorphism Theorem".

Quotient of a Congruence by a Smaller Congruence

Definition

Suppose **A** is an algebra and $\phi, \theta \in \mathrm{Con}\mathbf{A}$, with $\theta \subseteq \phi$. Then, let

$$\phi/\theta = \{\langle a/\theta, b/\theta\rangle \in (A/\theta)^2 : \langle a, b\rangle \in \phi\}.$$

Lemma

If $\phi, \theta \in \mathrm{Con}\mathbf{A}$ and $\theta \subseteq \phi$, then ϕ/θ is a congruence on $\mathbf{A}/\theta$.

- Let f be an n-ary function symbol and suppose $\langle a_i/\theta, b_i/\theta\rangle \in \phi/\theta$, for $1 \le i \le n$. Then $\langle a_i, b_i\rangle \in \phi$. So $\langle f^{\mathbf{A}}(a_1, \ldots, a_n), f^{\mathbf{A}}(b_1, \ldots, b_n)\rangle \in \phi$, and, thus, $\langle f^{\mathbf{A}}(a_1, \ldots, a_n)/\theta, f^{\mathbf{A}}(b_1, \ldots, b_n)/\theta\rangle \in \phi/\theta$. Therefore, $\langle f^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta), f^{\mathbf{A}/\theta}(b_1/\theta, \ldots, b_n/\theta)\rangle \in \phi/\theta$.

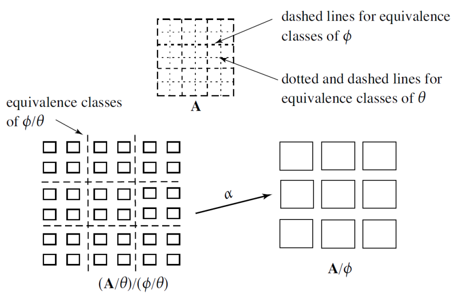
Second Isomorphism Theorem

Theorem (Second Isomorphism Theorem)

If $\phi, \theta \in \text{Con}\mathbf{A}$ and $\theta \subseteq \phi$, then the map $\alpha : (A/\theta)/(\phi/\theta) \to A/\phi$, defined by

$$\alpha((a/\theta)/(\phi/\theta)) = a/\phi$$

is an isomorphism from $(\mathbf{A}/\theta)/(\phi/\theta)$ to $\mathbf{A}/\phi$.



- Let $a, b \in A$. From $(a/\theta)/(\phi/\theta) = (b/\theta)/(\phi/\theta)$ iff $a/\phi = b/\phi$, it follows that α is a well-defined bijection.

Second Isomorphism Theorem (Cont'd)

- For f an n-ary function symbol and $a_1,\ldots,a_n \in A$, we have

$$\begin{aligned}\alpha(f^{(\mathbf{A}/\theta)/(\phi/\theta)}&((a_1/\theta)/(\phi/\theta),\ldots,(a_n/\theta)/(\phi/\theta)))\\ &= \alpha(f^{\mathbf{A}/\theta}(a_1/\theta,\ldots,a_n/\theta)/(\phi/\theta))\\ &= \alpha((f^{\mathbf{A}}(a_1,\ldots,a_n)/\theta)/(\phi/\theta))\\ &= f^{\mathbf{A}}(a_1,\ldots,a_n)/\phi\\ &= f^{\mathbf{A}/\phi}(a_1/\phi,\ldots,a_n/\phi)\\ &= f^{\mathbf{A}/\phi}(\alpha((a_1/\theta)/(\phi/\theta)),\ldots,\alpha((a_n/\theta)/(\phi/\theta))).\end{aligned}$$

So α is an isomorphism.

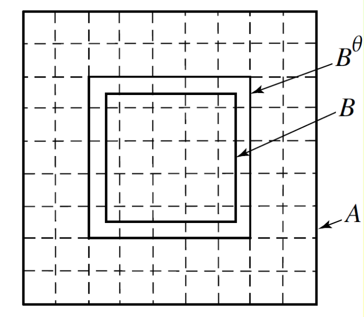
Restriction of a Congruence to a Subset

Definition

Let **A** be an algebra. Suppose B is a subset of A and θ is a congruence on **A**. Let

$$B^\theta = \{a \in A : B \cap a/\theta \neq \emptyset\}.$$

Let $\mathbf{B}^\theta$ be the subalgebra of **A** generated by B^θ. Also define $\theta\restriction_B$ to be $\theta \cap B^2$, the **restriction of** θ **to** B.



The dashed-line subdivisions of A are the equivalence classes of θ.

Lemma on the Restriction of a Congruence to a Subset

Lemma

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ and $\theta \in \mathrm{Con}\mathbf{A}$, then

(a) The universe of $\mathbf{B}^\theta$ is B^θ.

(b) $\theta\restriction_B$ is a congruence on $\mathbf{B}$.

(a) Suppose f is an n-ary function symbol. Let $a_1,\ldots,a_n \in B^\theta$. Then one can find $b_1,\ldots,b_n \in B$, such that $\langle a_i, b_i\rangle \in \theta$, $1 \le i \le n$. Hence, $\langle f^{\mathbf{A}}(a_1,\ldots,a_n), f^{\mathbf{A}}(b_1,\ldots,b_n)\rangle \in \theta$, so $f^{\mathbf{A}}(a_1,\ldots,a_n) \in B^\theta$. Thus, B^θ is a subuniverse of $\mathbf{A}$.

(b) To verify that $\theta\restriction_B$ is a congruence on $\mathbf{B}$, let f be an n-ary function symbol in $\mathscr{F}$, $a_1,\ldots,a_n,b_1,\ldots,b_n \in B$, such that $\langle a_i, b_i\rangle \in \theta$, $1 \le i \le n$. Then

$$f^{\mathbf{B}}(a_1,\ldots,a_n) = f^{\mathbf{A}}(a_1,\ldots,a_n)\ \theta\ f^{\mathbf{A}}(b_1,\ldots,b_n) = f^{\mathbf{B}}(b_1,\ldots,b_n).$$

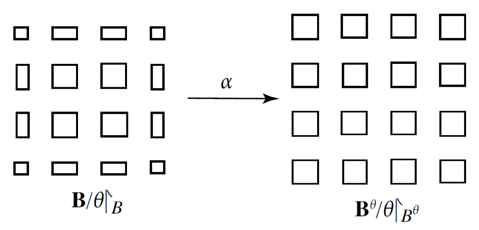
Hence, $\langle f^{\mathbf{B}}(a_1,\ldots,a_n), f^{\mathbf{B}}(b_1,\ldots,b_n)\rangle \in \theta\restriction_B$.

The Third Isomorphism Theorem

Theorem (Third Isomorphism Theorem)

If **B** is a subalgebra of **A** and $\theta \in \mathrm{Con}\mathbf{A}$, then

$$\mathbf{B}/\theta\restriction_B \cong \mathbf{B}^\theta/\theta\restriction_{B^\theta}.$$



- We can verify that the map α which is defined by

$$\alpha(b/\theta\restriction_B) = b/\theta\restriction_{B^\theta}$$

gives the desired isomorphism.

The Correspondence Theorem

- If $\mathbf{L}$ is a lattice and $a, b \in L$, with $a \leq b$, then the interval $[a, b]$ is a subuniverse of $\mathbf{L}$.

Definition

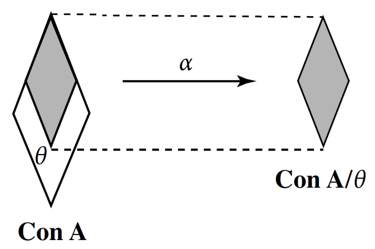
For $[a, b]$ a closed interval of a lattice $\mathbf{L}$, where $a \leq b$, let $\mathbf{[}a, b\mathbf{]}$ denote the corresponding sublattice of $\mathbf{L}$.

Theorem (Correspondence Theorem)

Let $\mathbf{A}$ be an algebra and let $\theta \in \text{Con}\mathbf{A}$. Then the mapping α defined on $[\theta, \nabla_A]$ by

$$\alpha(\phi) = \phi/\theta$$

is a lattice isomorphism from $\mathbf{[}\theta, \nabla_A\mathbf{]}$ to $\mathbf{Con}\mathbf{A}/\theta$, where $\mathbf{[}\theta, \nabla_A\mathbf{]}$ is a sublattice of $\mathbf{Con}\mathbf{A}$.



Proof of the Correspondence Theorem

- To see that α is one-to-one, let $\phi,\psi \in [\theta,\nabla_A]$, with $\phi \neq \psi$. Then, without loss of generality, we can assume that there are elements $a,b \in A$, with $\langle a,b\rangle \in \phi - \psi$. Thus, $\langle a/\theta, b/\theta\rangle \in (\phi/\theta)-(\psi/\theta)$. So $\alpha(\phi) \neq \alpha(\psi)$.

  To show that α is onto, let $\psi \in \text{Con}\mathbf{A}/\theta$. Define ϕ to be $\ker(\nu_\psi \nu_\theta)$. Then for $a,b \in A$,

  $$\langle a/\theta, b/\theta\rangle \in \phi/\theta \text{ iff } \langle a,b\rangle \in \phi \text{ iff } \langle a/\theta, b/\theta\rangle \in \psi.$$

  So $\phi/\theta = \psi$.

  Finally, we will show that α is an isomorphism. If $\phi,\psi \in [\theta,\nabla_A]$, then it is clear that

  $$\phi \subseteq \psi \text{ iff } \phi/\theta \subseteq \psi/\theta \text{ iff } \alpha(\phi) \subseteq \alpha(\psi).$$

Subsection 6

Direct Products and Factor Congruences

Direct Products

- Subalgebras and quotient algebras, do not give a means of creating algebras of larger cardinality than what we start with, or of combining several algebras into one.

Definition

Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be two algebras of the same type $\mathscr{F}$. Define the **(direct) product** $\mathbf{A}_1 \times \mathbf{A}_2$ to be the algebra whose universe is the set $A_1 \times A_2$ and such that for $f \in \mathscr{F}_n$ and $a_i \in A_1, a_i' \in A_2, 1 \le i \le n$,

$$f^{\mathbf{A}_1 \times \mathbf{A}_2}(\langle a_1, a_1' \rangle, \dots, \langle a_n, a_n' \rangle) = \langle f^{\mathbf{A}_1}(a_1, \dots, a_n), f^{\mathbf{A}_2}(a_1', \dots, a_n') \rangle.$$

- In general neither $\mathbf{A}_1$ nor $\mathbf{A}_2$ is embeddable in $\mathbf{A}_1 \times \mathbf{A}_2$; In special cases, e.g., groups, this is possible because there is always a trivial subalgebra.

Definition

The mapping $\pi_i : A_1 \times A_2 \to A_i$, $i \in \{1, 2\}$, defined by $\pi_i(\langle a_1, a_2 \rangle) = a_i$, is called the **projection map on the** i-th **coordinate** of $A_1 \times A_2$.

Properties of Projection Maps

Theorem

For $i = 1$ or 2, the mapping $\pi_i : A_1 \times A_2 \to A_i$ is a surjective homomorphism from $\mathbf{A} = \mathbf{A}_1 \times \mathbf{A}_2$ to $\mathbf{A}_i$. Furthermore, in $\mathbf{Con}\mathbf{A}_1 \times \mathbf{A}_2$ we have:

(a) $\ker\pi_1 \times \ker\pi_2 = \Delta$;

(b) $\ker\pi_1$ and $\ker\pi_2$ permute;

(c) $\ker\pi_1 \vee \ker\pi_2 = \nabla$.

- Clearly π_i is surjective. If $f \in \mathscr{F}_n$ and $a_i \in A_1$, $a_i' \in A_2$, $1 \le i \le n$, then

$$\begin{array}{rcl}\pi_1(f^{\mathbf{A}}(\langle a_1, a_1'\rangle, \ldots, \langle a_n, a_n'\rangle) & = & \pi_1(\langle f^{\mathbf{A}_1}(a_1, \ldots, a_n), f^{\mathbf{A}_2}(a_1', \ldots, a_n')\rangle) \\ & = & f^{\mathbf{A}_1}(a_1, \ldots, a_n) \\ & = & f^{\mathbf{A}_1}(\pi_1(\langle a_1, a_1'\rangle), \ldots, \pi_1(\langle a_n, a_n'\rangle)).\end{array}$$

So π_1 is a homomorphism. Similarly, π_2 is a homomorphism.

Properties of Projection Maps (Cont'd)

- We have

$$\begin{array}{rll}\langle\langle a_1,a_2\rangle,\langle b_1,b_2\rangle\rangle\in\ker\pi_i & \text{iff} & \pi_i(\langle a_1,a_2\rangle)=\pi_i(\langle b_1,b_2\rangle)\\ & \text{iff} & a_i=b_i.\end{array}$$

Thus, $\ker\pi_1\cap\ker\pi_2=\Delta$.

Also, if $\langle a_1,a_2\rangle,\langle b_1,b_2\rangle$ are any two elements of $A_1\times A_2$, then

$$\langle a_1,a_2\rangle\ \ker\pi_1\ \langle a_1,b_2\rangle\ \ker\pi_2\ \langle b_1,b_2\rangle.$$

So $\nabla=\ker\pi_1\circ\ker\pi_2$. But then $\ker\pi_1$ and $\ker\pi_2$ permute, and their join is ∇.

Factor Congruences

Definition

A congruence θ on $\mathbf{A}$ is a **factor congruence** if there is a congruence θ^* on $\mathbf{A}$, such that

$$\theta \cap \theta^* = \Delta, \quad \theta \vee \theta^* = \nabla, \quad \theta \text{ permutes with } \theta^*.$$

The pair θ, θ^* is called a **pair of factor congruences** on $\mathbf{A}$.

Theorem

If θ, θ^* is a pair of factor congruences on $\mathbf{A}$, then $\mathbf{A} \cong \mathbf{A}/\theta \times \mathbf{A}/\theta^*$ under the map $\alpha(a) = \langle a/\theta, a/\theta^* \rangle$.

- If $a, b \in A$, and $\alpha(a) = \alpha(b)$, then $a/\theta = b/\theta$ and $a/\theta^* = b/\theta^*$, so $\langle a, b \rangle \in \theta$ and $\langle a, b \rangle \in \theta^*$, whence $a = b$. Therefore, α is injective.

  Next, given $a, b \in A$, there is a $c \in A$, with $a \ \theta \ c \ \theta^* \ b$. Hence, $\alpha(c) = \langle c/\theta, c/\theta^* \rangle = \langle a/\theta, b/\theta^* \rangle$, whence α is onto.

Factor Congruences (Cont'd)

- Finally, for $f \in \mathscr{F}_n$ and $a_1, \ldots, a_n \in A$,

$$\begin{array}{rcl}\alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) & = & \langle f^{\mathbf{A}}(a_1,\ldots,a_n)/\theta, f^{\mathbf{A}}(a_1,\ldots,a_n)/\theta^*\rangle \\ & = & \langle f^{\mathbf{A}/\theta}(a_1/\theta,\ldots,a_n/\theta), f^{\mathbf{A}/\theta^*}(a_1/\theta^*,\ldots,a_n/\theta^*)\rangle \\ & = & f^{\mathbf{A}/\theta\times\mathbf{A}/\theta^*}(\langle a_1/\theta, a_1/\theta^*\rangle,\ldots,\langle a_n/\theta, a_n/\theta^*\rangle) \\ & = & f^{\mathbf{A}/\theta\times\mathbf{A}/\theta^*}(\alpha(a_1),\ldots,\alpha(a_n)).\end{array}$$

  Hence α is indeed an isomorphism.

Direct Indecomposability

Definition

An algebra **A** is (**directly**) **indecomposable** if **A** is not isomorphic to a direct product of two nontrivial algebras.

Example: Any finite algebra **A**, with $|A|$ a prime number must be directly indecomposable.

Corollary

A is directly indecomposable iff the only factor congruences on **A** are Δ and ∇.

Direct Products in General

Definition

Let $(\mathbf{A}_i)_{i\in I}$ be an indexed family of algebras of type $\mathscr{F}$. The (**direct**) **product** $\mathbf{A} = \prod_{i\in I}\mathbf{A}_i$ is an algebra with universe $\prod_{i\in I} A_i$ and such that for $f \in \mathscr{F}_n$ and $a_1,\ldots,a_n \in \prod_{i\in I} A_i$,

$$f^{\mathbf{A}}(a_1,\ldots,a_n)(i) = f^{\mathbf{A}_i}(a_1(i),\ldots,a_n(i)), \quad i \in I,$$

i.e., $f^{\mathbf{A}}$ is defined coordinate-wise.

The empty product $\prod\varnothing$ is the trivial algebra with universe $\{\varnothing\}$.

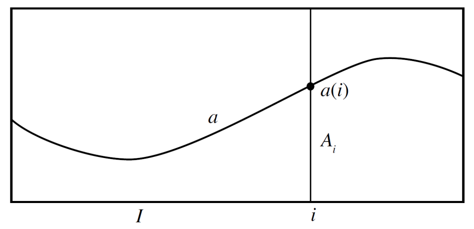
As before, we have **projection maps** $\pi_j : \prod_{i\in I} A_i \to A_j$, for $j \in I$, defined by $\pi_j(a) = a(j)$, which give surjective homomorphisms $\pi_j : \prod_{i\in I}\mathbf{A}_i \to \mathbf{A}_j$.

If $I = \{1,2,\ldots,n\}$, we also write $\mathbf{A}_1 \times\cdots\times \mathbf{A}_n$.

If I is arbitrary but $\mathbf{A}_i = \mathbf{A}$, for all $i \in I$, then we usually write $\mathbf{A}^I$ for the direct product, and call it a (**direct**) **power** of $\mathbf{A}$. $\mathbf{A}^\varnothing$ is a trivial algebra.

Visualization and Basic Properties of Direct Products

- A direct product $\prod_{i\in I} A_i$ of sets is often visualized as a rectangle with base I and vertical cross sections A_i.



An element a of $\prod_{i\in I} A_i$ is then a curve.

Theorem

If $\mathbf{A}_1, \mathbf{A}_2$ and $\mathbf{A}_3$ are of type $\mathscr{F}$, then:

(a) $\mathbf{A}_1 \times \mathbf{A}_2 \cong \mathbf{A}_2 \times \mathbf{A}_1$ under $\alpha(\langle a_1, a_2\rangle) = \langle a_2, a_1\rangle$.

(b) $\mathbf{A}_1 \times (\mathbf{A}_2 \times \mathbf{A}_3) \cong \mathbf{A}_1 \times \mathbf{A}_2 \times \mathbf{A}_3$ under $\alpha(\langle a_1, \langle a_2, a_3\rangle\rangle) = \langle a_1, a_2, a_3\rangle$.

Direct Product Decomposition of Finite Algebras

Theorem

Every finite algebra is isomorphic to a direct product of directly indecomposable algebras.

- Let $\mathbf{A}$ be a finite algebra. We proceed by induction on $|A|$.
  - If $\mathbf{A}$ is trivial, then $\mathbf{A}$ is indecomposable.
  - Suppose $\mathbf{A}$ is a nontrivial finite algebra such that for every $\mathbf{B}$, with $|B| < |A|$, we know that $\mathbf{B}$ is isomorphic to a product of indecomposable algebras.
    - If $\mathbf{A}$ is indecomposable we are finished.
    - If not, then $\mathbf{A} \cong \mathbf{A}_1 \times \mathbf{A}_2$, with $1 < |A_1|, |A_2|$. Then, $|A_1|, |A_2| < |A|$. So, by the induction hypothesis, $\mathbf{A}_1 \cong \mathbf{B}_1 \times \cdots \times \mathbf{B}_m$; $\mathbf{A}_2 \cong \mathbf{C}_1 \times \cdots \times \mathbf{C}_n$, where the $\mathbf{B}_i$ and $\mathbf{C}_j$ are indecomposable. Consequently, $\mathbf{A} \cong \mathbf{B}_1 \times \cdots \times \mathbf{B}_m \times \mathbf{C}_1 \times \cdots \times \mathbf{C}_n$.

Combining Homomorphisms Using Products

- Using direct products there are two obvious ways of combining families of homomorphisms into single homomorphisms.

Definition

(i) If we are given maps $\alpha_i : A \to A_i$, $i \in I$, then the **natural map** $\alpha : A \to \prod_{i\in I} A_i$ is defined by $(\alpha(a))(i) = \alpha_i(a)$.

(ii) If we are given maps $\alpha_i : A_i \to B_i$, $i \in I$, then the **natural map** $\alpha : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$ is defined by $(\alpha(a))(i) = \alpha_i(a(i))$.

Theorem

(a) If $\alpha_i : \mathbf{A} \to \mathbf{A}_i$, $i \in I$, is an indexed family of homomorphisms, then the natural map α is a homomorphism from $\mathbf{A}$ to $\mathbf{A}^* = \prod_{i\in I} \mathbf{A}_i$.

(b) If $\alpha_i : \mathbf{A}_i \to \mathbf{B}_i$, $i \in I$, is an indexed family of homomorphisms, then the natural map α is a homomorphism from $\mathbf{A}^* = \prod_{i\in I} \mathbf{A}_i$ to $\mathbf{B}^* = \prod_{i\in I} \mathbf{B}_i$.

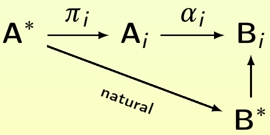
Proof of the Natural Map Theorem

- Suppose $\alpha_i : \mathbf{A} \to \mathbf{A}_i$ is a homomorphism for $i \in I$. Then for $a_1, \ldots, a_n \in A$ and $f \in \mathscr{F}_n$, we have, for $i \in I$,

$$\begin{array}{rcl}(\alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)))(i) & = & \alpha_i(f^{\mathbf{A}}(a_1,\ldots,a_n)) \\ & = & f^{\mathbf{A}_i}(\alpha_i(a_1),\ldots,\alpha_i(a_n)) \\ & = & f^{\mathbf{A}_i}((\alpha(a_1))(i),\ldots,(\alpha(a_n))(i)) \\ & = & f^{\mathbf{A}^*}(\alpha(a_1),\ldots,\alpha(a_n))(i).\end{array}$$

Hence, $\alpha(f^{\mathbf{A}}(a_1,\ldots,a_n)) = f^{\mathbf{A}^*}(\alpha(a_1),\ldots,\alpha(a_n))$, so α is indeed a homomorphism.

Case (b) is a consequence of (a) using the homomorphisms $\alpha_i \circ \pi_i$:



Separation of Points

Definition

If $a_1, a_2 \in A$ and $\alpha : A \to B$ is a map, we say α **separates** a_1 and a_2 if

$$\alpha(a_1) \neq \alpha(a_2).$$

The maps $\alpha_i : A \to A_i$, $i \in I$, **separate points** if for each $a_1, a_2 \in A$, with $a_1 \neq a_2$, there is an α_i, such that $\alpha_i(a_1) \neq \alpha_i(a_2)$.

Lemma

For an indexed family of maps $\alpha_i : A \to A_i$, $i \in I$, the following are equivalent:

(a) The maps α_i separate points.

(b) The natural map $\alpha : A \to \prod_{i \in I} A_i$ is injective.

(c) $\bigcap_{i \in I} \ker \alpha_i = \Delta$.

Proof of the Separation of Points Lema

(a)⇒(b): Suppose $a_1, a_2 \in A$ and $a_1 \neq a_2$. Then, for some i, $\alpha_i(a_1) \neq \alpha_i(a_2)$. Hence $(\alpha(a_1))(i) \neq (\alpha(a_2))(i)$. So $\alpha(a_1) \neq \alpha(a_2)$.

(b)⇒(c): For $a_1, a_2 \in A$, with $a_1 \neq a_2$, we have $\alpha(a_1) \neq \alpha(a_2)$, hence $(\alpha(a_1))(i) \neq (\alpha(a_2))(i)$, for some i; so $\alpha_i(a_1) \neq \alpha_i(a_2)$, for some i; and this implies $\langle a_1, a_2 \rangle \notin \ker\alpha_i$, so $\bigcap_{i \in I} \ker\alpha_i = \Delta$.

(c)⇒(a): For $a_1, a_2 \in A$, with $a_1 \neq a_2$, $\langle a_1, a_2 \rangle \notin \bigcap_{i \in I} \ker\alpha_i$ so, for some i, $\langle a_1, a_2 \rangle \notin \ker\alpha_i$, hence $\alpha_i(a_1) \neq \alpha_i(a_2)$.

Theorem

If we are given an indexed family of homomorphisms $\alpha_i : \mathbf{A} \to \mathbf{A}_i$, $i \in I$, then the natural homomorphism $\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$ is an embedding iff $\bigcap_{i \in I} \ker\alpha_i = \Delta$ iff the maps α_i separate points.

- This is immediate from the lemma.

Subsection 7

Subdirect Products and Simple Algebras

Subdirect Products and Subdirect Embeddings

Definition

An algebra $\mathbf{A}$ is a **subdirect product** of an indexed family $(\mathbf{A}_i)_{i\in I}$ of algebras if:

(i) $\mathbf{A} \leq \prod_{i\in I} \mathbf{A}_i$;

(ii) $\pi_i(\mathbf{A}) = \mathbf{A}_i$, for each $i \in I$.

An embedding $\alpha : \mathbf{A} \to \prod_{i\in I} \mathbf{A}_i$ is **subdirect** if $\alpha(\mathbf{A})$ is a subdirect product of the $\mathbf{A}_i$.

- If $I = \emptyset$, then $\mathbf{A}$ is a subdirect product of $\emptyset$ iff $\mathbf{A} = \prod \emptyset$, a trivial algebra.

The Subdirect Embedding Lemma

Lemma

If $\theta_i \in \text{Con}\mathbf{A}$, for $i \in I$, and $\bigcap_{i\in I}\theta_i = \Delta$, then the natural homomorphism $\nu : \mathbf{A} \to \prod_{i\in I}\mathbf{A}/\theta_i$, defined by

$$\nu(a)(i) = a/\theta_i$$

is a subdirect embedding.

- Let ν_i be the natural homomorphism from $\mathbf{A}$ to $\mathbf{A}/\theta_i$, for $i \in I$.
    - Since $\ker\nu_i = \theta_i$ and $\bigcap_{i\in I}\theta_i = \Delta$, it follows that ν is an embedding.
    - Since each ν_i is surjective, ν is a subdirect embedding.

Subdirect Irreducibility

Definition

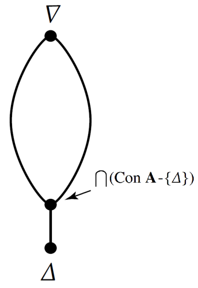
An algebra **A** is **subdirectly irreducible** if, for every subdirect embedding

$$\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i,$$

there is an $i \in I$, such that $\pi_i \circ \alpha : \mathbf{A} \to \mathbf{A}_i$ is an isomorphism.

Theorem

An algebra **A** is subdirectly irreducible iff **A** is trivial or there is a minimum congruence in $\mathrm{Con}\mathbf{A} - \{\Delta\}$. In the latter case the minimum element is $\bigcap(\mathrm{Con}\mathbf{A} - \{\Delta\})$, a principal congruence, and the congruence lattice of **A** looks as in the diagram.



Subdirect Irreducibility (Cont'd)

($\Rightarrow$): If $\mathbf{A}$ is not trivial and $\text{Con}\mathbf{A} - \{\Delta\}$ has no minimum element, then $\bigcap(\text{Con}\mathbf{A} - \{\Delta\}) = \Delta$. Let $I = \text{Con}\mathbf{A} - \{\Delta\}$. Then the natural map $\alpha : \mathbf{A} \to \prod_{\theta \in I} \mathbf{A}/\theta$ is a subdirect embedding by the lemma. The natural map $\mathbf{A} \to \mathbf{A}/\theta$ is not injective for $\theta \in I$, whence $\mathbf{A}$ is not subdirectly irreducible.

($\Leftarrow$): If $\mathbf{A}$ is trivial and $\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$ is a subdirect embedding then each $\mathbf{A}_i$ is trivial. Hence, each $\pi_i \circ \alpha$ is an isomorphism.

So suppose $\mathbf{A}$ is not trivial, and let $\theta = \bigcap(\text{Con}\mathbf{A} - \{\Delta\}) \neq \Delta$. Choose $\langle a, b\rangle \in \theta$, $a \neq b$. If $\alpha : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$ is a subdirect embedding, then for some i, $(\alpha(a))(i) \neq (\alpha(b))(i)$. Hence $(\pi_i \circ \alpha)(a) \neq (\pi_i \circ \alpha)(b)$. Thus, $\langle a, b\rangle \notin \ker(\pi_i \circ \alpha)$ so $\theta \nsubseteq \ker(\pi_i \circ \alpha)$. This implies $\ker(\pi_i \circ \alpha) = \Delta$ so $\pi_i \circ \alpha : \mathbf{A} \to \mathbf{A}_i$ is an isomorphism. Consequently, $\mathbf{A}$ is subdirectly irreducible.

If $\text{Con}\mathbf{A} - \{\Delta\}$ has a minimum element θ, then for $a \neq b$ and $\langle a, b\rangle \in \theta$, we have $\Theta(a, b) \subseteq \theta$, whence $\theta = \Theta(a, b)$.

Subdirect Irreducibility and Direct Indecomposability

Examples:

(1) A finite Abelian group **G** is subdirectly irreducible iff it is cyclic and $|G| = p^n$, for some prime p.
(2) Given a prime number p, the Prüfer p-group $\mathbb{Z}_{p^\infty}$, the group of p^n-th roots of unity, $n \in \omega$, is subdirectly irreducible.
(3) Every simple group is subdirectly irreducible.
(4) A vector space over a field F is subdirectly irreducible iff it is trivial or one-dimensional.
(5) Any two-element algebra is subdirectly irreducible.

- A directly indecomposable algebra need not be subdirectly irreducible - for example, a three-element chain as a lattice.

Theorem

A subdirectly irreducible algebra is directly indecomposable.

- Clearly the only factor congruences on a subdirectly irreducible algebra are Δ and ∇. Such an algebra is directly indecomposable.

Subdirect Decomposability

Theorem (Birkhoff)

Every algebra **A** is isomorphic to a subdirect product of subdirectly irreducible algebras (which are homomorphic images of **A**).

- As trivial algebras are subdirectly irreducible, we only need to consider the case of nontrivial **A**. For $a, b \in A$, with $a \neq b$, we can find, using Zorn's lemma, a congruence $\theta_{a,b}$ on **A** which is maximal with respect to the property $\langle a, b \rangle \notin \theta_{a,b}$. Then clearly $\Theta(a, b) \vee \theta_{a,b}$ is the smallest congruence in $[\theta_{a,b}, \nabla] - \{\theta_{a,b}\}$, so we see that $\mathbf{A}/\theta_{a,b}$ is subdirectly irreducible. As $\bigcap\{\theta_{a,b} : a \neq b\} = \Delta$, we can apply a preceding result to show that **A** is subdirectly embeddable in the product of the indexed family of subdirectly irreducible algebras $(\mathbf{A}/\theta_{a,b})_{a \neq b}$.

Corollary

Every finite algebra is isomorphic to a subdirect product of a finite number of subdirectly irreducible finite algebras.

Simple Algebras

Definition

An algebra $\mathbf{A}$ is **simple** if $\text{Con}\mathbf{A} = \{\Delta, \nabla\}$. A congruence θ on an algebra $\mathbf{A}$ is **maximal** if the interval $[\theta, \nabla]$ of $\text{Con}\mathbf{A}$ has exactly two elements.

- We do not require that a simple algebra be nontrivial.
- Just as the quotient of a group by a normal subgroup is simple and nontrivial iff the normal subgroup if maximal, we have a similar result for arbitrary algebras.

Theorem

Let $\theta \in \text{Con}\mathbf{A}$. Then $\mathbf{A}/\theta$ is a simple algebra iff θ is a maximal congruence on $\mathbf{A}$ or $\theta = \nabla$.

- We know that $\mathbf{Con}\mathbf{A}/\theta \cong [\theta, \nabla_A]$. So the theorem is an immediate consequence of the definition.