Introduction to Universal Algebra

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Class Operators and Varieties

Operators on Classes of Algebras

Definition

We introduce the following operators mapping classes of algebras to classes of algebras (all of the same type):

$\mathbf{A} \in I(K)$	iff	$\mathbf{A}$ is isomorphic to some member of K
$\mathbf{A} \in S(K)$	iff	$\mathbf{A}$ is a subalgebra of some member of K
$\mathbf{A} \in H(K)$	iff	$\mathbf{A}$ is a homomorphic image of some member of K
$\mathbf{A} \in P(K)$	iff	$\mathbf{A}$ is a direct product of a nonempty family of algebras in K
$\mathbf{A} \in P_S(K)$	iff	$\mathbf{A}$ is a subdirect product of a nonempty family of algebras in K.

If O_1 and O_2 are two operators on classes of algebras we write $O_1 O_2$ for the composition of the two operators. $\leq$ denotes the usual partial ordering: $O_1 \leq O_2$ if $O_1(K) \subseteq O_2(K)$, for all classes of algebras K. An operator O is **idempotent** if $O^2 = O$. A class K of algebras is **closed** under an operator O if $O(K) \subseteq K$.

- For any operator O above, $O(\varnothing) = \varnothing$.
- If $\prod \varnothing$ is included (so that $P(K)$ and $P_S(K)$ always contain a trivial algebra) some problems occur in formulating preservation theorems.

Operator Inequalities

Lemma

The following inequalities hold:

$$SH \leq HS, \quad PS \leq SP, \quad PH \leq HP.$$

Also the operators, H, S and IP are idempotent.

- Suppose $\mathbf{A} \in SH(K)$. Then, for some $\mathbf{B} \in K$ and onto homomorphism $\alpha : \mathbf{B} \to \mathbf{C}$, we have $\mathbf{A} \leq \mathbf{C}$. Thus, $\alpha^{-1}(\mathbf{A}) \leq \mathbf{B}$. But $\alpha(\alpha^{-1}(\mathbf{A})) = \mathbf{A}$. Hence, $\mathbf{A} \in HS(K)$.

  If $\mathbf{A} \in PS(K)$, then $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$, for suitable $\mathbf{A}_i \leq \mathbf{B}_i \in K$, $i \in I$. But $\prod_{i \in I} \mathbf{A}_i \leq \prod_{i \in I} \mathbf{B}_i$. Hence, $\mathbf{A} \in SP(K)$.

  If $\mathbf{A} \in PH(K)$, then there are algebras $\mathbf{B}_i \in K$ and epimorphisms $\alpha_i : \mathbf{B}_i \to \mathbf{A}_i$, such that $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$. We can show that the mapping $\alpha : \prod_{i \in I} \mathbf{B}_i \to \prod_{i \in I} \mathbf{A}_i$, defined by $\alpha(b)(i) = \alpha_i(b(i))$ is an epimorphism. Hence, $\mathbf{A} \in HP(K)$.

Operator Inequalities (Cont'd)

- Suppose $\mathbf{A} \in H^2(K)$. Then, there exists an epimorphism $\beta : \mathbf{C} \to \mathbf{A}$ and an epimorphism $\alpha : \mathbf{B} \to \mathbf{C}$, where $\mathbf{B} \in K$. Thus, $\beta \circ \alpha : \mathbf{B} \to \mathbf{A}$ is an epimorphism, with $\mathbf{B} \in K$. Hence, $\mathbf{A} \in H(K)$. Therefore, $H^2(K) \subseteq H(K)$. The reverse inclusion is trivial.
- Suppose $\mathbf{A} \in S^2(K)$. Then $\mathbf{A} \leq \mathbf{C}$, where $\mathbf{C} \leq \mathbf{B}$, for some $\mathbf{B} \in K$. Thus, $\mathbf{A} \leq \mathbf{B}$, with $\mathbf{B} \in K$ and, hence, $\mathbf{A} \in S(K)$. Therefore, $S^2(K) \subseteq S(K)$. The reverse inclusion is trivial.
- Suppose $\mathbf{A} \in (IP)^2(K)$. Then $\mathbf{A} \cong \prod_{i \in I} \mathbf{A}_i$, where, for all $i \in I$, $\mathbf{A}_i \cong \prod_{j \in J_i} \mathbf{A}_{ij}$, with $\mathbf{A}_{ij} \in K$, for all $i \in I$, $j \in J_i$. But then

$$\mathbf{A} \cong \prod_{i \in I} \mathbf{A}_i \cong \prod_{i \in I} \prod_{j \in J_i} \mathbf{A}_{ij} \cong \prod_{\substack{i \in I \\ j \in J_i}} \mathbf{A}_{ij}.$$

Since $\{\mathbf{A}_{ij} : i \in I, j \in J_i\} \subseteq K$, we get that $\mathbf{A} \in IP(K)$. Thus, $(IP)^2(K) \subseteq IP(K)$. The reverse inclusion is trivial.

Varieties

Definition

A nonempty class K of algebras of type $\mathscr{F}$ is called a **variety** if it is closed under subalgebras, homomorphic images and direct products.

- Note that:
  - all algebras of type $\mathscr{F}$ form a variety;
  - the intersection of a class of varieties of type $\mathscr{F}$ is again a variety.

  Thus, for every class K of algebras of the same type there is a smallest variety containing K.

Definition

If K is a class of algebras of the same type, let $V(K)$ denote the smallest variety containing K. We say that $V(K)$ is the **variety generated by** K. If K has a single member $\mathbf{A}$, we write simply $V(\mathbf{A})$. A variety V is **finitely generated** if $V = V(K)$, for some finite set K of finite algebras.

Tarski's Characterization of Varieties

Theorem (Tarski)

$V = HSP$.

- Since $HV = SV = IPV = V$ and $I \leq V$, we have $HSP \leq HSPV = V$.

  We also have:
  - $H(HSP) = HSP$;
  - $S(HSP) \leq HSSP = HSP$;
  - $P(HSP) \leq HPSP \leq HSPP \leq HSIPIP = HSIP \leq HSHP \leq HHSP = HSP$.

  Hence, for any K, $HSP(K)$ is closed under H, S and P. But $V(K)$ is the smallest class containing K and closed under H, S and P. Therefore, $V \leq HSP$.

  We conclude that $V = HSP$.

Birkhoff's Theorem for Varieties

Theorem (Birkhoff's Theorem for Varieties)

If K is a variety, then every member of K is isomorphic to a subdirect product of subdirectly irreducible members of K.

Corollary

A variety is generated by its subdirectly irreducible members.

- Let K be a variety and $\mathbf{A} \in K$. By Birkhoff's Theorem, $\mathbf{A} \in IP_S(K_{SI})$, where K_{SI} denotes the class of all subdirectly irreducible members of K. Now we have

$$\mathbf{A} \in IP_S(K_{SI}) \subseteq ISP(K_{SI}) \subseteq V(K_{SI}).$$

  Therefore, K is generated by its subdirectly irreducible members.

Subsection 2

Terms, Term Algebras and Free Algebras

Terms

Definition

Let X be a set of (distinct) objects called **variables**. Let $\mathscr{F}$ be a type of algebras. The set $T(X)$ of **terms of type $\mathscr{F}$ over X** is the smallest set such that:

(i) $X \cup \mathscr{F}_0 \subseteq T(X)$.

(ii) If $p_1, \ldots, p_n \in T(X)$ and $f \in \mathscr{F}_n$, then the "string" $f(p_1, \ldots, p_n) \in T(X)$.

- $T(X) \neq \emptyset$ iff $X \cup \mathscr{F}_0 \neq \emptyset$.
- For a binary function symbol $\bullet$, we often write $p_1 \bullet p_2$ instead of $\bullet(p_1, p_2)$.
- For $p \in T(X)$, we often write p as $p(x_1, \ldots, x_n)$ to indicate that the variables occurring in p are among $x_1, \ldots, x_n$.
- A term p is n-**ary** if the number of variables appearing explicitly in p is $\leq n$.

Examples

(1) Let $\mathscr{F}$ consist of a single binary function symbol $\bullet$. Let $X = \{x, y, z\}$. The following

$$x, \quad y, \quad z, \quad x \bullet y, \quad y \bullet z, \quad x \bullet (y \bullet z), \quad (x \bullet y) \bullet z$$

are some of the terms over X.

(2) Let $\mathscr{F}$ consist of two binary operation symbols $+$ and $\cdot$. Let X be as before. The following

$$x, \quad y, \quad z, \quad x \cdot (y + z), \quad (x \cdot y) + (x \cdot z)$$

are some of the terms over X.

(3) The classical polynomials over the field of real numbers $\mathbb{R}$ are really the terms of type $\mathscr{F}$, consisting of $+, \cdot$ and $-$, together with a nullary function symbol r, for each $r \in R$.

Term Functions

Definition

Given a term $p(x_1,\ldots,x_n)$ of type $\mathscr{F}$ over some set X and given an algebra $\mathbf{A}$ of type $\mathscr{F}$, we define a mapping $p^{\mathbf{A}}: A^n \to A$ as follows:

(1) if p is a variable x_i, then

$$p^{\mathbf{A}}(a_1,\ldots,a_n) = a_i,$$

for $a_1,\ldots,a_n \in A$, i.e., $p^{\mathbf{A}}$ is the i-th projection map;

(2) if p is of the form $f(p_1(x_1\ldots,x_n),\ldots,p_k(x_1,\ldots,x_n))$, where $f \in \mathscr{F}_k$, then

$$p^{\mathbf{A}}(a_1,\ldots,a_n) = f^{\mathbf{A}}(p_1^{\mathbf{A}}(a_1,\ldots,a_n),\ldots,p_k^{\mathbf{A}}(a_1,\ldots,a_n)).$$

In particular if $p = f \in \mathscr{F}_0$, then $p^{\mathbf{A}} = f^{\mathbf{A}}$.

We say $p^{\mathbf{A}}$ is the **term function** on $\mathbf{A}$ corresponding to the term p. Often the superscript $^{\mathbf{A}}$ is omitted.

Properties of Term Functions

Theorem

For any type $\mathscr{F}$ and algebras $\mathbf{A},\mathbf{B}$ of type $\mathscr{F}$, we have the following:

(a) Let p be an n-ary term of type $\mathscr{F}$. Let $\theta \in \mathrm{Con}\mathbf{A}$. Suppose $\langle a_i, b_i\rangle \in \theta$, for $1 \le i \le n$. Then $p^{\mathbf{A}}(a_1,\ldots,a_n)\ \theta\ p^{\mathbf{A}}(b_1,\ldots,b_n)$.

(b) If p is an n-ary term of type $\mathscr{F}$ and $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism, then

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

for $a_1,\ldots,a_n \in A$.

(c) Let S be a subset of A. Then

$$\begin{aligned}\mathrm{Sg}(S) \quad = \quad \{p^{\mathbf{A}}(a_1,\ldots,a_n) : {} & p \text{ is an } n\text{-ary term of type } \mathscr{F}, \\ & n < \omega,\ a_1,\ldots,a_n \in S\}.\end{aligned}$$

Proof of Part (a)

- Given a term p define the **length** $\ell(p)$ of p to be the number of occurrences of n-ary operation symbols in p, for $n \geq 1$. Note that $\ell(p) = 0$ iff $p \in X \cup \mathscr{F}_0$.

(a) We proceed by induction on $\ell(p)$.
  - If $\ell(p) = 0$, then either $p = x_i$, for some i, or $p = a \in \mathscr{F}_0$.
    - If $p = x_i$, for some i, $\langle p^{\mathbf{A}}(a_1,\ldots,a_n), p^{\mathbf{A}}(b_1,\ldots,b_n)\rangle = \langle a_i, b_i\rangle \in \theta$;
    - If $p = a$, for some $a \in \mathscr{F}_0$, then $\langle p^{\mathbf{A}}(a_1,\ldots,a_n), p^{\mathbf{A}}(b_1,\ldots,b_n)\rangle = \langle a^{\mathbf{A}}, a^{\mathbf{A}}\rangle \in \theta$.
  - Now suppose $\ell(p) > 0$ and the assertion holds for every term q with $\ell(q) < \ell(p)$. Then we know p is of the form $f(p_1(x_1,\ldots,x_n),\ldots, p_k(x_1,\ldots,x_n))$. Since $\ell(p_i) < \ell(p)$, we must have, for $1 \leq i \leq k$, $\langle p_i^{\mathbf{A}}(a_1,\ldots,a_n), p_i^{\mathbf{A}}(b_1,\ldots,b_n)\rangle \in \theta$. Hence,

$$\langle f^{\mathbf{A}}(p_1^{\mathbf{A}}(a_1,\ldots,a_n),\ldots,p_k^{\mathbf{A}}(a_1,\ldots,a_n)), f^{\mathbf{A}}(p_1^{\mathbf{A}}(b_1,\ldots,b_n),\ldots,p_k^{\mathbf{A}}(b_1,\ldots,b_n))\rangle \in \theta.$$

  Consequently $\langle p^{\mathbf{A}}(a_1,\ldots,a_n), p^{\mathbf{A}}(b_1,\ldots,b_n)\rangle \in \theta$.

Proof of Part (b)

(b) The proof of this is an induction argument on $\ell(p)$.

- If $\ell(p) = 0$, then $p = x_i$, for some i, or $p = a \in \mathscr{F}_0$.
  - If $p = x_i$, for some i, then
  $$\alpha(p^{\mathbf{A}}(a_1,\ldots,a_n)) = \alpha(a_i) = p^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)).$$
  - If $p = a \in \mathscr{F}_0$, then, by definition, $\alpha(a^{\mathbf{A}}) = a^{\mathbf{B}}$.
- Suppose $\ell(p) > 0$. Then $p = f(p_1(x_1,\ldots,x_n),\ldots,p_k(x_1,\ldots,x_n))$, for some $f \in \mathscr{F}_k$, where $\ell(p_1),\ldots,\ell(p_k) < \ell(p)$. Thus, we get

$$\begin{array}{rcl}
\alpha(p^{\mathbf{A}}(a_1,\ldots,a_n)) & = & \alpha(f^{\mathbf{A}}(p_1^{\mathbf{A}}(a_1,\ldots,a_n),\ldots,p_k^{\mathbf{A}}(a_1,\ldots,a_n))) \\
& = & f^{\mathbf{B}}(\alpha(p_1^{\mathbf{A}}(a_1,\ldots,a_n)),\ldots,\alpha(p_k^{\mathbf{A}}(a_1,\ldots,a_n))) \\
& = & f^{\mathbf{B}}(p_1^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)),\ldots, \\
& & \qquad p_k^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n))) \\
& = & p^{\mathbf{B}}(\alpha(a_1),\ldots,\alpha(a_n)).
\end{array}$$

Proof of Part (c)

(c) By induction, we show that, for $k \geq 1$,

$$E^k(S) \subseteq \{p^{\mathbf{A}}(a_1,\ldots,a_n) : p \text{ is an } n\text{-ary term}; \\ \ell(p) \leq k,\ n < \omega,\ a_1,\ldots,a_n \in S\}.$$

The right side is always $\subseteq \mathrm{Sg}(S)$ since (by induction) every subuniverse B of $\mathbf{A}$ is closed under the term functions of $\mathbf{A}$.

Thus,

$$\begin{array}{rcl} \mathrm{Sg}(S) & = & \bigcup_{k<\infty} E^k(S) \\ & \subseteq & \{p^{\mathbf{A}}(a_1,\ldots,a_n) : p \text{ is an } n\text{-ary term of type } \mathscr{F}, \\ & & \qquad n < \omega,\ a_1,\ldots,a_n \in S\} \\ & \subseteq & \mathrm{Sg}(S). \end{array}$$

The Term Algebra and the Universal Mapping Property

Definition

Given $\mathscr{F}$ and X, if $T(X) \neq \emptyset$, then the **term algebra of type** $\mathscr{F}$ over X, written $\mathbf{T}(X)$, has as its universe the set $T(X)$ and the fundamental operations satisfy

$$f^{\mathbf{T}(X)} : \langle p_1, \ldots, p_n \rangle \mapsto f(p_1, \ldots, p_n),$$

for $f \in \mathscr{F}_n$ and $p_i \in T(X)$, $1 \leq i \leq n$. $\mathbf{T}(\emptyset)$ exists iff $\mathscr{F}_0 \neq \emptyset$.

- $\mathbf{T}(X)$ is generated by X.

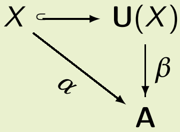
Definition

Let K be a class of algebras of type $\mathscr{F}$ and let $\mathbf{U}(X)$ be an algebra of type $\mathscr{F}$ which is generated by X. If, for every $\mathbf{A} \in K$ and for every map $\alpha : X \to A$, there is a homomorphism $\beta : \mathbf{U}(X) \to \mathbf{A}$, which extends α (i.e., $\beta(x) = \alpha(x)$, for $x \in X$), then we say $\mathbf{U}(X)$ has the **universal mapping property** for K over X. X is called a set of **free generators** of $\mathbf{U}(X)$, and $\mathbf{U}(X)$ is said to be **freely generated by** X.

Uniqueness of the Universal Mapping

Lemma

Suppose $\mathbf{U}(X)$ has the universal mapping property for K over X. Then, if we are given $\mathbf{A} \in K$ and $\alpha : X \to A$, there is a unique extension β of α, such that β is a homomorphism from $\mathbf{U}(X)$ to $\mathbf{A}$.



- Suppose β, β' both extend α and let $a \in \mathbf{U}(X)$. Then, there exists n-ary p and $x_1, \ldots, x_n \in X$, such that $a = p^{\mathbf{U}(X)}(x_1, \ldots, x_n)$. Therefore,

$$\begin{aligned} \beta(a) &= \beta(p^{\mathbf{U}(X)}(x_1, \ldots, x_n)) = p^{\mathbf{A}}(\beta(x_1), \ldots, \beta(x_n)) \\ &= p^{\mathbf{A}}(\beta'(x_1), \ldots, \beta'(x_n)) = \beta'(p^{\mathbf{U}(X)}(x_1, \ldots, x_n)) \\ &= \beta'(a). \end{aligned}$$

Uniqueness of the "Free Algebra"

- For a given cardinal m, there is, up to isomorphism, at most one algebra in a class K which has the universal mapping property for K over a set of free generators of size m.

Theorem

Suppose $\mathbf{U}_1(X_1)$ and $\mathbf{U}_2(X_2)$ are two algebras with the universal mapping property for K over the indicated sets. If $\mathbf{U}_1(X_1), \mathbf{U}_2(X_2) \in K$ and $|X_1| = |X_2|$, then $\mathbf{U}_1(X_1) \cong \mathbf{U}_2(X_2)$.

- The identity map $\iota_j : X_j \to X_j$, $j = 1,2$, has as its unique extension to a homomorphism from $\mathbf{U}_j(X_j)$ to $\mathbf{U}_j(X_j)$ the identity map. Now let $\alpha : X_1 \to X_2$ be a bijection. Then we have homomorphisms $\beta : \mathbf{U}_1(X_1) \to \mathbf{U}_2(X_2)$ extending α, and $\gamma : \mathbf{U}_2(X_2) \to \mathbf{U}_1(X_1)$ extending α^{-1}. But $\beta \circ \gamma$ is an endomorphism of $\mathbf{U}_2(X_2)$ extending ι_2. It follows that $\beta \circ \gamma$ is the identity map on $\mathbf{U}_2(X_2)$. Likewise $\gamma \circ \beta$ is the identity map on $\mathbf{U}_1(X_1)$. Thus, β is a bijection. So $\mathbf{U}_1(X_1) \cong \mathbf{U}_2(X_2)$.

Universal Mapping Property of the Term Algebra

Theorem

For any type $\mathscr{F}$ and set X of variables, where $X \neq \emptyset$ if $\mathscr{F}_0 = \emptyset$, the term algebra $\mathbf{T}(X)$ has the universal mapping property for the class of all algebras of type $\mathscr{F}$ over X.

- Let $\alpha : X \to A$, where $\mathbf{A}$ is of type $\mathscr{F}$. Define $\beta : T(X) \to A$ recursively by:
  - $\beta x = \alpha x$, for $x \in X$;
  - For all $f \in \mathscr{F}_n$ and all $p_1, \ldots, p_n \in T(X)$,

$$\beta(f(p_1, \ldots, p_n)) = f^{\mathbf{A}}(\beta(p_1) \ldots, \beta(p_n)).$$

Then, for every n-ary term $p(x_1, \ldots, x_n)$,

$$\beta(p(x_1, \ldots, x_n)) = p^{\mathbf{A}}(\alpha(x_1), \ldots, \alpha(x_n)),$$

and β is the desired homomorphism extending α.

K-Free Algebras

Definition

Let K be a family of algebras of type $\mathscr{F}$. Given a set X of variables, let

$$\Phi_K(X) = \{\phi \in \mathrm{Con}\,\mathbf{T}(X) : \mathbf{T}(X)/\phi \in IS(K)\}.$$

Define the congruence $\theta_K(X)$ on $\mathbf{T}(X)$ by

$$\theta_K(X) = \bigcap \Phi_K(X).$$

Then letting $\overline{X} = X/\theta_K(X)$, define $\mathbf{F}_K(\overline{X})$, the K-**free algebra over** $\overline{X}$, by $\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\theta_K(X)$.
For $x \in X$, we write $\overline{x}$ for $x/\theta_K(X)$, and for $p = p(x_1,\ldots,x_n) \in T(X)$, we write $\overline{p}$ for $p^{\mathbf{F}_K(\overline{X})}(\overline{x}_1,\ldots,\overline{x}_n)$.
If X is finite, say $X = \{x_1,\ldots,x_n\}$, we often write $\mathbf{F}_K(\overline{x}_1,\ldots,\overline{x}_n)$, for $\mathbf{F}_K(\overline{X})$.
$F_K(\overline{X})$ is the universe of $\mathbf{F}_K(\overline{X})$.

Remarks on K-Free Algebras

(1) $\mathbf{F}_K(\overline{X})$ exists iff $\mathbf{T}(X)$ exists iff $X \neq \emptyset$ or $\mathscr{F}_0 \neq \emptyset$, i.e., $X \cup \mathscr{F}_0 \neq \emptyset$.

(2) If $\mathbf{F}_K(\overline{X})$ exists, then $\overline{X}$ is a set of generators of $\mathbf{F}_K(\overline{X})$ as X generates $\mathbf{T}(X)$.

(3) If $\mathscr{F}_0 \neq \emptyset$, then the algebra $\mathbf{F}_K(\overline{\emptyset})$ is often referred to as an **initial object**.

(4) If $K = \emptyset$ or K consists solely of trivial algebras, then $\mathbf{F}_K(\overline{X})$ is a trivial algebra as $\theta_K(X) = \nabla$.

(5) If K has a nontrivial algebra $\mathbf{A}$ and $\mathbf{T}(X)$ exists, then $X \cap (x/\theta_K(X)) = \{x\}$ as distinct members x, y of X can be separated by some homomorphism $\alpha : \mathbf{T}(X) \to \mathbf{A}$. In this case $|\overline{X}| = |X|$.

(6) If $|X| = |Y|$ and $\mathbf{T}(X)$ exists, then clearly $\mathbf{F}_K(\overline{X}) \cong \mathbf{F}_K(\overline{Y})$ under an isomorphism which maps X to Y as $\mathbf{T}(X) \cong \mathbf{T}(Y)$ under an isomorphism mapping X to Y. Thus $\mathbf{F}_K(\overline{X})$ is determined, up to isomorphism, by K and $|X|$.

Universal Mapping Property of $\mathbf{F}_K(\overline{X})$

Theorem (Birkhoff)

Suppose $\mathbf{T}(X)$ exists, i.e., $X \cup \mathscr{F}_0 \neq \emptyset$. Then $\mathbf{F}_K(\overline{X})$ has the universal mapping property for K over $\overline{X}$.

- Given $\mathbf{A} \in K$ let α be a map from $\overline{X}$ to A. Let $\nu : \mathbf{T}(X) \to \mathbf{F}_K(\overline{X})$ be the natural homomorphism. Then $\alpha \circ \nu$ maps X into A. By the universal mapping property of $\mathbf{T}(X)$, there is a homomorphism $\mu : \mathbf{T}(X) \to \mathbf{A}$ extending $(\alpha \circ \nu) \restriction_X$. Since $\mathbf{T}(X)/\ker\mu \cong \mu(\mathbf{T}(X)) \leq \mathbf{A}$, $\ker\mu \in \Phi_K(X)$. Thus, $\theta_K(X) \subseteq \ker\mu$. Hence, there is a homomorphism $\beta : \mathbf{F}_K(\overline{X}) \to \mathbf{A}$, such that $\mu = \beta \circ \nu$, as $\ker\nu = \theta_K(X)$. But then, for $x \in X$, $\beta(\overline{x}) = \beta \circ \nu(x) = \mu(x) = \alpha \circ \nu(x) = \alpha(\overline{x})$. So β extends α. Thus, $\mathbf{F}_K(\overline{X})$ has the universal mapping property for K over $\overline{X}$.
- If $\mathbf{F}_K(\overline{X}) \in K$, then it is, up to isomorphism, the unique algebra in K, with the universal mapping property freely generated by a set of generators of size $|\overline{X}|$.

Examples

(1) $\mathbf{T}(X)$ is isomorphic to the free algebra for the class K of all algebras of type $\mathscr{F}$ over X, since $\theta_K(X) = \Delta$. The corresponding free algebra is sometimes called the **absolutely free algebra** $\mathbf{F}(\overline{X})$ of type $\mathscr{F}$.

(2) Given X, let X^* be the set of finite strings of elements of X, including the empty string. We can construct a monoid $\langle X^*, \cdot, 1\rangle$ by defining $\cdot$ to be concatenation, and 1 is the empty string. By checking the universal mapping property one sees that $\langle X^*, \cdot, 1\rangle$ is, up to isomorphism, the free monoid freely generated by $\overline{X}$.

Free Algebras and Algebras

Corollary

If K is a class of algebras of type $\mathscr{F}$ and $\mathbf{A} \in K$, then for sufficiently large X, $\mathbf{A} \in H(\mathbf{F}_K(\overline{X}))$.

- Choose $|X| \geq |A|$ and let $\alpha : \overline{X} \to A$ be a surjection. Then let $\beta : \mathbf{F}_K(\overline{X}) \to \mathbf{A}$ be a homomorphism extending α.
- In general $\mathbf{F}_K(\overline{X})$ is not isomorphic to a member of K.

  Example: Let $K = \{\mathbf{L}\}$, where $\mathbf{L}$ be a two-element lattice. Then $\mathbf{F}_K(\overline{x}, \overline{y}) \notin I(K)$.
- On the other hand, $\mathbf{F}_K(\overline{X})$ can be embedded in a product of members of K.

Free Algebras in Varieties

Theorem (Birkhoff)

Suppose $\mathbf{T}(X)$ exists, i.e., $X \cup \mathscr{F}_0 \neq \emptyset$. Then, for $K \neq \emptyset$, $\mathbf{F}_K(\overline{X}) \in ISP(K)$. Thus, if K is closed under I, S and P, in particular if K is a variety, then $\mathbf{F}_K(\overline{X}) \in K$.

- We have $\theta_K(X) = \bigcap \Phi_K(X)$. Hence,

$$\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\theta_K(X) \in IP_S(\{\mathbf{T}(X)/\theta : \theta \in \Phi_K(X)\}).$$

Thus, $\mathbf{F}_K(\overline{X}) \in IP_S IS(K)$. But $P_S \leq SP$ and $PS \leq SP$. Therefore,

$$\mathbf{F}_K(\overline{X}) \in IP_S S(K) \subseteq ISPS(K) \subseteq ISSP(K) = ISP(K).$$

Nontrivial Simple Algebras in Varieties

- We know that if a variety has a nontrivial algebra in it, then it must have a nontrivial subdirectly irreducible algebra in it.

Theorem (Magari)

If we are given a variety V with a nontrivial member, then V contains a nontrivial simple algebra.

- Let $X = \{x, y\}$, and let $S = \{p(\overline{x}) : p \in T(\{x\})\}$, a subset of $F_V(\overline{X})$. First, suppose that $\Theta(S) \neq \nabla$ in $\mathrm{Con}\mathbf{F}_V(\overline{X})$.

  Claim: For $\theta \in [\Theta(S), \nabla]$, $\theta = \nabla$ iff $\langle \overline{x}, \overline{y} \rangle \in \theta$.

  Suppose $\Theta(S) \subseteq \theta$ and $\langle \overline{x}, \overline{y} \rangle \in \theta$. Then for any term $p(x, y)$, we have $p^{\mathbf{F}_V(\overline{X})}(\overline{x}, \overline{y}) \ \theta \ p^{\mathbf{F}_V(\overline{X})}(\overline{x}, \overline{x}) \ \Theta(S) \ \overline{x}$. Hence $\theta = \nabla$.

  By the claim, every chain in $[\Theta(S), \nabla] - \{\nabla\}$ has a maximal element. By Zorn's Lemma, $[\Theta(S), \nabla] - \{\nabla\}$ has a maximal element θ_0. Then $\mathbf{F}_V(\overline{X})/\theta_0$ is a simple algebra and it is in V.

Nontrivial Simple Algebras in Varieties (Cont'd)

- Now suppose that $\Theta(S) = \nabla$. Then, since Θ is an algebraic closure operator, it follows that, for some finite subset S_0 of S, we must have $\langle \overline{x}, \overline{y} \rangle \in \Theta(S_0)$. Let $\mathbf{S}$ be the subalgebra of $\mathbf{F}_V(\overline{X})$, with universe S ($S = \mathrm{Sg}(\{\overline{x}\})$). Since V is nontrivial, $\overline{x} \neq \overline{y}$ in $\mathbf{F}_V(\overline{X})$. Since $\langle \overline{x}, \overline{y} \rangle \in \Theta(S)$, S is nontrivial.

  Claim: $\nabla_S = \Theta(S_0)$, where Θ in this case is understood to be the appropriate closure operator on S.

  Let $p(\overline{x}) \in S$ and let $\alpha : \mathbf{F}_V(\overline{X}) \to \mathbf{S}$ be the homomorphism defined by

  $$\alpha(\overline{x}) = \overline{x}, \quad \alpha(\overline{y}) = p(\overline{x}).$$

  Since $\langle \overline{x}, \overline{y} \rangle \in \Theta(S_0)$ in $\mathbf{F}_V(\overline{X})$, we get $\langle \overline{x}, p(\overline{x}) \rangle \in \Theta(S_0)$ in $\mathbf{S}$ as $\alpha(S_0) = S_0$.

  Using Zorn's Lemma, we can find a maximal congruence θ on $\mathbf{S}$ as ∇_S is finitely generated. Hence, $\mathbf{S}/\theta$ is a simple algebra in V.

Local Finiteness

Definition

An algebra $\mathbf{A}$ is **locally finite** if every finitely generated subalgebra is finite. A class K of algebras is **locally finite** if every member of K is locally finite.

Theorem

A variety V is locally finite iff

$$|X| < \omega \;\Rightarrow\; |F_V(\overline{X})| < \omega.$$

($\Rightarrow$): Clear, since $\overline{X}$ generates $\mathbf{F}_V(\overline{X})$.

($\Leftarrow$): Let $\mathbf{A}$ be a finitely generated member of V, and let $B \subseteq A$ be a finite set of generators. Choose X, such that we have a bijection $\alpha : \overline{X} \to B$. Extend this to a homomorphism $\beta : \mathbf{F}_V(\overline{X}) \to \mathbf{A}$. As $\beta(\mathbf{F}_V(\overline{X}))$ is a subalgebra of $\mathbf{A}$ containing B, it must equal $\mathbf{A}$. Thus β is surjective, and as $\mathbf{F}_V(\overline{X})$ is finite so is $\mathbf{A}$.

Variety Generated by Finitely Many Finite Algebras

Theorem

Let K be a finite set of finite algebras. Then $V(K)$ is a locally finite variety.

Claim: $P(K)$ is locally finite.

Let $\mathbf{A} \in P(K)$ and $S = \{a_1, \ldots, a_n\}$ a finite subset of $\mathbf{A}$. We must show $\mathrm{Sg}^{\mathbf{A}}(S)$ is finite. But

$$\mathrm{Sg}^{\mathbf{A}}(S) = \{p^{\mathbf{A}}(a_1, \ldots, a_n) : p \text{ is an } n\text{-ary term of type } \mathscr{F}\}.$$

Thus, it suffices to show that the set $T(\{x_1, \ldots, x_n\})/\sim^K$ is finite, where $\sim^K$ is the equivalence relation on $T(\{x_1, \ldots, x_n\})$, defined, for all $p, q \in T(\{x_1, \ldots, x_n\})$, by

$$p \sim^K q \quad \text{iff} \quad p^{\mathbf{K}} = q^{\mathbf{K}}, \text{ for all } \mathbf{K} \in K.$$

Variety Generated by Finitely Many Finite Algebras (Cont'd)

- We must show that the set $T(\{x_1,\ldots,x_n\})/\sim^K$ is finite.

  This is clear, since, if $K = \{\mathbf{A}_1,\ldots\mathbf{A}_m\}$ and $|A_i| = k_i$, $1 \leq i \leq m$, then there are at most $k_1^n \cdot k_2^n \cdot \cdots \cdot k_m^n$ different functions on n-variables agreeing on every member of K.

  Now note that $SP(K)$ is locally finite.

  And, since every finitely generated member of $HSP(K)$ is a homomorphic image of a finitely generated member of $SP(K)$, $HSP(K)$ is locally finite. Hence, V is locally finite.

Subsection 3

Identities, Free Algebras and Birkhoff's Theorem

Identities and Satisfiability

Definition

An **identity** of type $\mathscr{F}$ over X is an expression of the form $p \approx q$, where $p, q \in T(X)$. Let $\mathrm{Id}(X)$ be the set of identities of type $\mathscr{F}$ over X.

An algebra $\mathbf{A}$ of type $\mathscr{F}$ **satisfies** an identity $p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$ if, for every choice of $a_1, \ldots, a_n \in A$, we have $p^{\mathbf{A}}(a_1, \ldots, a_n) = q^{\mathbf{A}}(a_1, \ldots, a_n)$. If so, then we say that the identity is **true in A**, or **holds in A**, and write $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$, or more briefly $\mathbf{A} \models p \approx q$.

- If Σ is a set of identities, we say **A satisfies** Σ, written $\mathbf{A} \models \Sigma$, if $\mathbf{A} \models p \approx q$, for each $p \approx q \in \Sigma$.
- A class K of algebras **satisfies** $p \approx q$, written $K \models p \approx q$, if each member of K satisfies $p \approx q$. Set $\mathrm{Id}_K(X) = \{p \approx q \in \mathrm{Id}(X) : K \models p \approx q\}$.
- If Σ is a set of identities, we say K **satisfies** Σ, written $K \models \Sigma$, if $K \models p \approx q$, for each $p \approx q \in \Sigma$.

We use the symbol $\not\models$ for "does not satisfy".

Free Algebras and Satisfiability of Identitites

Lemma

If K is a class of algebras of type $\mathscr{F}$ and $p \approx q$ is an identity of type $\mathscr{F}$ over X, then $K \models p \approx q$ iff, for every $\mathbf{A} \in K$ and for every homomorphism $\alpha : \mathbf{T}(X) \to \mathbf{A}$, we have $\alpha(p) = \alpha(q)$.

($\Rightarrow$) Let $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n)$. Suppose $K \models p \approx q$, $\mathbf{A} \in K$, and $\alpha : \mathbf{T}(X) \to \mathbf{A}$ is a homomorphism. Then

$$\begin{array}{rl} & p^{\mathbf{A}}(\alpha(x_1), \ldots, \alpha(x_n)) = q^{\mathbf{A}}(\alpha(x_1), \ldots, \alpha(x_n)) \\ \Rightarrow & \alpha(p^{\mathbf{T}(X)}(x_1, \ldots, x_n)) = \alpha(q^{\mathbf{T}(X)}(x_1, \ldots, x_n)) \\ \Rightarrow & \alpha(p) = \alpha(q). \end{array}$$

($\Leftarrow$) For the converse choose $\mathbf{A} \in K$ and $a_1, \ldots, a_n \in A$. By the universal mapping property of $\mathbf{T}(X)$, there is a homomorphism $\alpha : \mathbf{T}(X) \to \mathbf{A}$, such that $\alpha(x_i) = a_i$, $1 \leq i \leq n$. But then $p^{\mathbf{A}}(a_1, \ldots, a_n) = p^{\mathbf{A}}(\alpha(x_1), \ldots, \alpha(x_n)) = \alpha(p) = \alpha(q) = q^{\mathbf{A}}(\alpha(x_1), \ldots, \alpha(x_n)) = q^{\mathbf{A}}(a_1, \ldots, a_n)$. So $K \models p \approx q$.

Basic Class Operators Preserve Identities

Lemma

For any class K of type $\mathscr{F}$, all of the classes $K, I(K), S(K), H(K), P(K)$ and $V(K)$ satisfy the same identities over any set of variables X.

- Clearly K and $I(K)$ satisfy the same identities. As $I \leq IS, I \leq H$ and $I \leq IP$, we must have $\mathrm{Id}_K(X) \supseteq \mathrm{Id}_{S(K)}(X), \mathrm{Id}_{H(K)}(X), \mathrm{Id}_{P(K)}(X)$. For the remainder of the proof suppose $K \models p(x_1,\ldots,x_n) \approx q(x_1,\ldots,x_n)$.
  Let $\mathbf{B} \leq \mathbf{A} \in K$ and $b_1,\ldots,b_n \in B$. As $b_1,\ldots,b_n \in A$, we have $p^{\mathbf{A}}(b_1,\ldots,b_n) = q^{\mathbf{A}}(b_1,\ldots,b_n)$. Hence, $p^{\mathbf{B}}(b_1,\ldots,b_n) = q^{\mathbf{B}}(b_1,\ldots,b_n)$. so $\mathbf{B} \models p \approx q$. Thus, $\mathrm{Id}_K(X) = \mathrm{Id}_{S(K)}(X)$.

  Let $\alpha : \mathbf{A} \to \mathbf{B}$ be a surjective homomorphism with $\mathbf{A} \in K$. If $b_1,\ldots,b_n \in B$, choose $a_1,\ldots,a_n \in A$, such that $\alpha(a_1) = b_1,\ldots,\alpha(a_n) = b_n$. Then, $p^{\mathbf{A}}(a_1,\ldots,a_n) = q^{\mathbf{A}}(a_1,\ldots,a_n)$, implies $\alpha(p^{\mathbf{A}}(a_1,\ldots,a_n)) = \alpha(q^{\mathbf{A}}(a_1,\ldots,a_n))$. Hence $p^{\mathbf{B}}(b_1,\ldots,b_n) = q^{\mathbf{B}}(b_1,\ldots,b_n)$. Thus, $\mathbf{B} \models p \approx q$. So $\mathrm{Id}_K(X) = \mathrm{Id}_{H(K)}(X)$.

Basic Class Operators Preserve Identities (Cont'd)

- Lastly, suppose $\mathbf{A}_i \in K$, for $i \in I$. Then, for $a_1, \ldots, a_n \in A = \prod_{i \in I} A_i$, we have

$$p^{\mathbf{A}_i}(a_1(i), \ldots, a_n(i)) = q^{\mathbf{A}_i}(a_1(i), \ldots, a_n(i)),$$

hence

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

so

$$p^{\mathbf{A}}(a_1, \ldots, a_n) = q^{\mathbf{A}}(a_1, \ldots, a_n).$$

Thus, $\mathrm{Id}_K(X) = \mathrm{Id}_{P(K)}(X)$.

As $V = HSP$, the proof is complete.

Characterization of Satisfiability

Theorem

Given a class K of algebras of type $\mathscr{F}$ and terms $p,q \in T(X)$ of type $\mathscr{F}$, we have:

$$K \models p \approx q \;\Leftrightarrow\; \mathbf{F}_K(\overline{X}) \models p \approx q \;\Leftrightarrow\; \overline{p} = \overline{q} \text{ in } \mathbf{F}_K(\overline{X}) \;\Leftrightarrow\; \langle p,q\rangle \in \theta_K(X).$$

- Let $\mathbf{F} = \mathbf{F}_K(\overline{X}), p = p(x_1,\ldots,x_n), q = q(x_1,\ldots,x_n)$ and let $\nu : \mathbf{T}(X) \to \mathbf{F}$ be the natural homomorphism.
  - Certainly $K \models p \approx q$ implies $\mathbf{F} \models p \approx q$, as $\mathbf{F} \in ISP(K)$.
  - Assume $\mathbf{F} \models p \approx q$. Then $p^{\mathbf{F}}(\overline{x}_1,\ldots,\overline{x}_n) = q^{\mathbf{F}}(\overline{x}_1,\ldots,\overline{x}_n)$, hence $\overline{p} \approx \overline{q}$.
  - Now suppose $\overline{p} = \overline{q}$ in $\mathbf{F}$. Then $\nu(p) = \overline{p} = \overline{q} = \nu(q)$. so $\langle p,q\rangle \in \ker\nu = \theta_K(X)$.
  - Finally, suppose $\langle p,q\rangle \in \theta_K(X)$. Given $\mathbf{A} \in K$ and $a_1,\ldots,a_n \in A$, choose $\alpha : \mathbf{T}(X) \to \mathbf{A}$, such that $\alpha(x_i) = a_i$, $1 \le i \le n$. We have $\ker\alpha \in \Phi_K(X)$. Hence, $\ker\alpha \supseteq \ker\nu = \theta_K(X)$. It follows that there is a homomorphism $\beta : \mathbf{F} \to \mathbf{A}$, such that $\alpha = \beta \circ \nu$. Then $\alpha(p) = \beta \circ \nu(p) = \beta \circ \nu(q) = \alpha(q)$. Consequently $K \models p \approx q$.

Various Sets of Variables

Corollary

Let K be a class of algebras of type $\mathscr{F}$, and suppose $p, q \in T(X)$. Then for any set of variables Y, with $|Y| \geq |X|$, we have

$$K \models p \approx q \quad \text{iff} \quad \mathbf{F}_K(\overline{Y}) \models p \approx q.$$

($\Rightarrow$) This is obvious, as $\mathbf{F}_K(\overline{Y}) \in ISP(K)$.

($\Leftarrow$) Choose $X_0 \supseteq X$, such that $|X_0| = |Y|$. Then $\mathbf{F}_K(\overline{X}_0) \cong \mathbf{F}_K(\overline{Y})$, and, since, by the theorem,

$$K \models p \approx q \quad \text{iff} \quad \mathbf{F}_K(\overline{X}_0) \models p \approx q,$$

it follows that

$$K \models p \approx q \quad \text{iff} \quad \mathbf{F}_K(\overline{Y}) \models p \approx q.$$

Identities Over Various Sets of Variables

Corollary

Suppose K is a class of algebras of type $\mathscr{F}$ and X is a set of variables. Then, for any infinite set of variables Y,

$$\mathrm{Id}_K(X) = \mathrm{Id}_{\mathbf{F}_K(\overline{Y})}(X).$$

- For $p \approx q \in \mathrm{Id}_K(X)$, say $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n)$, we have $p, q \in T(\{x_1, \ldots, x_n\})$. As $|\{x_1, \ldots, x_n\}| < |Y|$, by the preceding corollary,

$$K \models p \approx q \quad \text{iff} \quad \mathbf{F}_K(\overline{Y}) \models p \approx q,$$

so the corollary is proved.

Equational Classes of Algebras

Definition

Let Σ be a set of identities of type $\mathscr{F}$ and define $M(\Sigma)$ to be the class of algebras $\mathbf{A}$ satisfying Σ. A class K of algebras is an **equational class** if there is a set of identities Σ, such that $K = M(\Sigma)$. In this case, we say that K is **defined**, or **axiomatized**, by Σ.

Lemma

If V is a variety and X is an infinite set of variables, then $V = M(\mathrm{Id}_V(X))$.

- Let $V' = M(\mathrm{Id}_V(X))$. V' is a variety by a preceding result. Also, $V' \supseteq V$ and $\mathrm{Id}_{V'}(X) = \mathrm{Id}_V(X)$. So, we get $\mathbf{F}_{V'}(\overline{X}) = \mathbf{F}_V(\overline{X})$. Now given any infinite set of variables Y, we have $\mathrm{Id}_{V'}(Y) = \mathrm{Id}_{\mathbf{F}_{V'}(\overline{X})}(Y) = \mathrm{Id}_{\mathbf{F}_V(\overline{X})}(Y) = \mathrm{Id}_V(Y)$. Thus, $\theta_{V'}(Y) = \theta_V(Y)$ and $\mathbf{F}_{V'}(\overline{Y}) = \mathbf{F}_V(\overline{Y})$.

  For $\mathbf{A} \in V'$, we have for suitable infinite Y, $\mathbf{A} \in H(\mathbf{F}_{V'}(\overline{Y}))$. Thus, $\mathbf{A} \in H(\mathbf{F}_V(\overline{Y}))$. So $\mathbf{A} \in V$. Therefore, $V' \subseteq V$.

Birkhoff's Variety Theorem

Theorem (Birkhoff)

K is an equational class iff K is a variety.

($\Rightarrow$) Suppose $K = M(\Sigma)$. Then $V(K) \models \Sigma$. Hence, $V(K) \subseteq M(\Sigma) = K$. so $V(K) = K$, i.e., K is a variety.

($\Leftarrow$) By the preceding lemma, $K = M(\mathrm{Id}_K(X))$, for an infinite X.

Corollary

Let K be a class of algebras of type $\mathscr{F}$. If $\mathbf{T}(X)$ exists, i.e., $X \cup \mathscr{F}_0 \neq \emptyset$, and K' is any class of algebras such that $K \subseteq K' \subseteq V(K)$, then $\mathbf{F}_{K'}(\overline{X}) = \mathbf{F}_K(\overline{X})$. In particular, if $K \neq \emptyset$, $\mathbf{F}_{K'}(\overline{X}) \in ISP(K)$.

- Since $\mathrm{Id}_K(X) = \mathrm{Id}_{V(K)}(X)$, it follows that $\mathrm{Id}_K(X) = \mathrm{Id}_{K'}(X)$. Thus $\theta_{K'}(X) = \theta_K(X)$, so $\mathbf{F}_{K'}(\overline{X}) = \mathbf{F}_K(\overline{X})$. The last statement of the corollary now follows.

Large K-Free Algebras

Theorem

Let K be a nonempty class of algebras of type $\mathscr{F}$. Then, for some cardinal m, if $|X| \geq m$, we have $\mathbf{F}_K(\overline{X}) \in IP_S(K)$.

- Choose a *subset* K^* of K, such that for any X, $\mathrm{Id}_{K^*}(X) = \mathrm{Id}_K(X)$:
  Choose an infinite set of variables Y. Then select, for each identity $p \approx q$ in $\mathrm{Id}(Y) - \mathrm{Id}_K(Y)$ an algebra $\mathbf{A} \in K$, such that $\mathbf{A} \not\models p \approx q$.
  Now K^* is a set. So there exists an infinite upper bound m of $\{|A| : \mathbf{A} \in K^*\}$.

Large K-Free Algebras (Cont'd)

- Given X, let $\Psi_{K^*}(X) = \{\phi \in \mathrm{Con}\mathbf{T}(X) : \mathbf{T}(X)/\phi \in I(K^*)\}$.

  Then $\Psi_{K^*}(X) \subseteq \Phi_{K^*}(X)$, whence $\bigcap \Psi_{K^*}(X) \supseteq \theta_{K^*}(X)$. To prove equality for $|X| \geq m$, suppose $\langle p, q\rangle \notin \theta_{K^*}(X)$. Then $K^* \not\models p \approx q$. Hence, for some $\mathbf{A} \in K^*$, $\mathbf{A} \not\models p \approx q$. If $p = p(x_1, \ldots, x_n)$, $q = q(x_1, \ldots, x_n)$, choose $a_1, \ldots, a_n \in A$, such that $p^{\mathbf{A}}(a_1, \ldots, a_n) \neq q^{\mathbf{A}}(a_1, \ldots, a_n)$. As $|X| \geq |A|$, we can find a mapping $\alpha : X \to A$ which is onto and $\alpha(x_i) = a_i, 1 \leq i \leq n$. Then α can be extended to a surjective homomorphism $\beta : \mathbf{F}_{K^*}(\overline{X}) \to \mathbf{A}$ and $\beta(p) \neq \beta(q)$. Thus $\langle p, q\rangle \notin \ker\beta \in \Psi_{K^*}(X)$. So $\langle p, q\rangle \notin \bigcap \Psi_{K^*}(X)$. Consequently
  $$\bigcap \Psi_{K^*}(X) = \theta_{K^*}(X).$$
  As $\mathbf{F}_K(\overline{X}) = \mathbf{F}_{K^*}(\overline{X})$, it follows that $\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\bigcap \Psi_{K^*}(X)$. Then we have $\mathbf{F}_K(\overline{X}) \in IP_S(K^*) \subseteq IP_S(K)$.

Another Characterization of V

Theorem

$V = HP_S$.

- As $P_S \leq SP$, we have
$$HP_S \leq HSP \leq V.$$
Given a class K of algebras and sufficiently large X, we have $\mathbf{F}_{V(K)}(\overline{X}) \in IP_S(K)$, by the preceding theorem. Hence, $V(K) \subseteq HP_S(K)$, by a preceding result. Thus $V = HP_S$.

Subsection 4

Mal'cev Conditions

Mal'cev Conditions

- Properties of varieties characterized by the existence of certain terms involved in certain identities are referred to as **Mal'cev conditions**.

Lemma

Let V be a variety of type $\mathscr{F}$, and let $p(x_1,\ldots,x_m,y_1,\ldots,y_n)$, $q(x_1,\ldots,x_m,y_1,\ldots,y_n)$ be terms such that in $\mathbf{F}=\mathbf{F}_V(\overline{X})$, where $X=\{x_1,\ldots,x_m,y_1,\ldots,y_n\}$, we have

$$\langle p^{\mathbf{F}}(\overline{x}_1,\ldots,\overline{x}_m,\overline{y}_1,\ldots,\overline{y}_n),q^{\mathbf{F}}(\overline{x}_1,\ldots,\overline{x}_m,\overline{y}_1,\ldots,\overline{y}_n)\rangle\in\Theta(\overline{y}_1,\ldots,\overline{y}_n).$$

Then $V\models p(x_1,\ldots,x_m,y,\ldots,y)\approx q(x_1,\ldots,x_m,y,\ldots,y)$.

- The homomorphism $\alpha:\mathbf{F}_V(\overline{x}_1,\ldots,\overline{x}_m,\overline{y}_1,\ldots,\overline{y}_n)\to\mathbf{F}_V(\overline{x}_1,\ldots,\overline{x}_m,\overline{y})$, defined by $\alpha(\overline{x}_i)=\overline{x}_i$, $1\le i\le m$, and $\alpha(\overline{y}_i)=\overline{y}$, $1\le i\le n$, is such that $\Theta(\overline{y}_1,\ldots\overline{y}_n)\subseteq\ker\alpha$. So $\alpha(p(\overline{x}_1,\ldots,\overline{x}_m,\overline{y}_1,\ldots,\overline{y}_n))=\alpha(q(\overline{x}_1,\ldots,\overline{x}_m,\overline{y}_1,\ldots,\overline{y}_n))$. Thus, $p(\overline{x}_1,\ldots,\overline{x}_m,\overline{y},\ldots,\overline{y})=q(\overline{x}_1,\ldots,\overline{x}_m,\overline{y},\ldots,\overline{y})$ in $\mathbf{F}_V(\overline{x}_1,\ldots,\overline{x}_m,\overline{y})$. Hence, $V\models p(x_1,\ldots,x_m,y,\ldots,y)\approx q(x_1,\ldots,x_m,y,\ldots,y)$.

Mal'cev's Theorem on Congruence Permutability

Theorem (Mal'cev)

Let V be a variety of type $\mathscr{F}$. The variety V is congruence-permutable iff there is a term $p(x,y,z)$, such that

$$V \models p(x,x,y) \approx y \quad \text{and} \quad V \models p(x,y,y) \approx x.$$

- (⇒) Suppose V is congruence-permutable. In $\mathbf{F}_V(\overline{x},\overline{y},\overline{z})$, we have $\langle \overline{x},\overline{z}\rangle \in \Theta(\overline{x},\overline{y}) \circ \Theta(\overline{y},\overline{z})$. So $\langle \overline{x},\overline{z}\rangle \in \Theta(\overline{y},\overline{z}) \circ \Theta(\overline{x},\overline{y})$. Hence, there is a $p(\overline{x},\overline{y},\overline{z}) \in F_V(\overline{x},\overline{y},\overline{z})$, such that $\overline{x}\ \Theta(\overline{y},\overline{z})\ p(\overline{x},\overline{y},\overline{z})\ \Theta(\overline{x},\overline{y})\ \overline{z}$. By the lemma, $V \models p(x,y,y) \approx x$ and $V \models p(x,x,z) \approx z$.
- (⇐) Let $\mathbf{A} \in V$ and $\phi, \psi \in \mathrm{Con}\mathbf{A}$. Suppose $\langle a,b\rangle \in \phi \circ \psi$, say $a\ \phi\ c\ \psi\ b$. Then $b = p(c,c,b)\ \phi\ p(a,c,b)\ \psi\ p(a,b,b) = a$. So $\langle b,a\rangle \in \phi \circ \psi$. Thus, $\phi \circ \psi = \psi \circ \phi$.

Examples

(1) Groups $\langle A, \cdot, ^{-1}, 1\rangle$ are congruence-permutable: Let

$$p(x,y,z) = x \cdot y^{-1} \cdot z.$$

(2) Rings $\langle R, +, \cdot, -, 0\rangle$ are congruence-permutable: Let

$$p(x,y,z) = x - y + z.$$

(3) Quasigroups $\langle Q, /, \cdot, \backslash\rangle$ are congruence-permutable: Let

$$p(x,y,z) = (x/(y\backslash y)) \cdot (y\backslash z).$$

Congruence Distributivity

Theorem

Suppose V is a variety for which there is a ternary term $M(x,y,z)$, such that

$$V \models M(x,x,y) \approx M(x,y,x) \approx M(y,x,x) \approx x.$$

Then V is congruence-distributive.

- Let $\phi, \psi, \chi \in \mathrm{Con}\mathbf{A}$, where $\mathbf{A} \in V$. Suppose $\langle a,b\rangle \in \phi \wedge (\psi \vee \chi)$. Then $\langle a,b\rangle \in \phi$ and, there exist $c_1,\ldots,c_n$, such that $a\ \psi\ c_1\ \chi\ c_2\ \cdots\ \psi\ c_n\ \chi\ b$. Since $M(a,c_i,b)\ \phi\ M(a,c_i,a) = a$, for each i, we get

$$a = M(a,a,b)\ (\phi\wedge\psi)\ M(a,c_1,b)\ (\phi\wedge\chi)\ M(a,c_2,b)\cdots \\ M(a,c_n,b)\ (\phi\wedge\chi)\ M(a,b,b) = b.$$

  So $\langle a,b\rangle \in (\phi\wedge\psi)\vee(\phi\wedge\chi)$. This suffices to show $\phi\wedge(\psi\vee\chi) = (\phi\wedge\psi)\vee(\phi\wedge\chi)$. So V is congruence-distributive.

  Example: Lattices are congruence-distributive:
  $M(x,y,z) = (x\vee y)\wedge(x\vee z)\wedge(y\vee z)$.

Arithmetical Varieties

Definition

A variety V is **arithmetical** if it is both congruence-distributive and congruence-permutable.

Theorem (Pixley)

A variety V is arithmetical iff it satisfies either of the equivalent conditions:

(a) There are a congruence permutability term p and a congruence distributivity term M.

(b) There is a term $m(x,y,z)$, such that $V \models m(x,y,x) \approx m(x,y,y) \approx m(y,y,x) \approx x$.

- If V is arithmetical, then V is congruence-permutable, so there is a term p. Let $\mathbf{F}_V(\overline{x},\overline{y},\overline{z})$ be the free algebra in V freely generated by $\{\overline{x},\overline{y},\overline{z}\}$. We have $\langle\overline{x},\overline{z}\rangle \in \Theta(\overline{x},\overline{z}) \cap [\Theta(\overline{x},\overline{y}) \vee \Theta(\overline{y},\overline{z})]$. Hence, $\langle\overline{x},\overline{z}\rangle \in [\Theta(\overline{x},\overline{z}) \cap \Theta(\overline{x},\overline{y})] \vee [\Theta(\overline{x},\overline{z}) \cap \Theta(\overline{y},\overline{z})]$.

Arithmetical Varieties (Cont'd)

- Hence, $\langle\overline{x},\overline{z}\rangle \in [\Theta(\overline{x},\overline{z})\cap\Theta(\overline{x},\overline{y})]\circ[\Theta(\overline{x},\overline{z})\cap\Theta(\overline{y},\overline{z})]$. Choose $M(\overline{x},\overline{y},\overline{z})\in F_V(\overline{x},\overline{y},\overline{z})$, such that $\overline{x}\ [\Theta(\overline{x},\overline{z})\cap\Theta(\overline{x},\overline{y})]\ M(\overline{x},\overline{y},\overline{z})\ [\Theta(\overline{x},\overline{z})\cap\Theta(\overline{y},\overline{z})]\ \overline{z}$. Then $V\models M(x,x,y)\approx M(x,y,x)\approx M(y,x,x)\approx x$.

  If (a) holds, let $m(x,y,z):=p(x,M(x,y,z),z)$. Verify that $V\models m(x,y,x)\approx m(x,y,y)\approx m(y,y,x)\approx x$.

  If (b) holds, let $p(x,y,z):=m(x,y,z)$ and $M(x,y,z):=m(x,m(x,y,z),z)$. Verify that $V\models p(x,x,y)\approx y$, $V\models p(x,y,y)\approx x$ and $V\models M(x,x,y)\approx M(x,y,x)\approx M(y,x,x)\approx x$.

  Examples:

  (1) Boolean algebras are arithmetical: Let $m(x,y,z)=(x\wedge z)\vee(x\wedge y'\wedge z')\vee(x'\wedge y'\wedge z)$.

  (2) Heyting algebras are arithmetical: Let $m(x,y,z)=[(x\to y)\to z]\wedge[(z\to y)\to x]\wedge[x\vee z]$.

Congruence-Distributivity

Theorem (Jónsson)

A variety V is congruence-distributive iff there is a finite n and terms $p_0(x,y,z),\ldots,p_n(x,y,z)$, such that V satisfies:

$$\begin{array}{ll} p_i(x,y,x) \approx x & 0 \le i \le n \\ p_0(x,y,z) \approx x; \quad p_n(x,y,z) \approx z & \\ p_i(x,x,y) \approx p_{i+1}(x,x,y) & \text{for } i \text{ even} \\ p_i(x,y,y) \approx p_{i+1}(x,y,y) & \text{for } i \text{ odd.} \end{array}$$

($\Rightarrow$) We have

$$\Theta(\overline{x},\overline{z}) \wedge [\Theta(\overline{x},\overline{y}) \vee \Theta(\overline{y},\overline{z})] = [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{x},\overline{y})] \vee [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{y},\overline{z})].$$

Thus, in $\mathbf{F}_V(\overline{x},\overline{y},\overline{z})$,

$$\langle \overline{x},\overline{z}\rangle \in [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{x},\overline{y})] \vee [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{y},\overline{z})].$$

Congruence-Distributivity (Cont'd)

Thus, for some $p_1(\overline{x},\overline{y},\overline{z}),\ldots,p_{n-1}(\overline{x},\overline{y},\overline{z}) \in F_V(\overline{x},\overline{y},\overline{z})$, we have

$$\begin{array}{rcl} \overline{x} & [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{x},\overline{y})] & p_1(\overline{x},\overline{y},\overline{z}) \\ p_1(\overline{x},\overline{y},\overline{z}) & [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{y},\overline{z})] & p_2(\overline{x},\overline{y},\overline{z}) \\ & \vdots & \\ p_{n-1}(\overline{x},\overline{y},\overline{z}) & [\Theta(\overline{x},\overline{z}) \wedge \Theta(\overline{y},\overline{z})] & \overline{z}. \end{array}$$

From these the desired equations fall out.

($\Leftarrow$) For $\phi,\psi,\chi \in \mathrm{Con}\mathbf{A}$, $\mathbf{A} \in V$, we need $\phi \wedge (\psi \vee \chi) \subseteq (\phi \wedge \psi) \vee (\phi \wedge \chi)$. Let $\langle a,b\rangle \in \phi \wedge (\psi \vee \chi)$. Then $\langle a,b\rangle \in \phi$, and, for some $c_1,\ldots,c_t$, we have $a \ \psi \ c_1 \ \chi \ \cdots \ c_t \ \chi \ b$. From these, we get, for $0 \leq i \leq n$, $p_i(a,a,b) \ \psi \ p_i(a,c_1,b) \ \chi \ \cdots \ p_i(a,c_t,b) \ \chi \ p_i(a,b,b)$. Hence, $p_i(a,a,b) \ (\phi \wedge \psi) \ p_i(a,c_1,b) \ (\phi \wedge \chi) \ \cdots \ p_i(a,c_t,b) \ (\phi \wedge \chi) \ p_i(a,b,b)$. So $p_i(a,a,b) \ [(\phi \wedge \psi) \vee (\phi \wedge \chi)] \ p_i(a,b,b)$, $0 \leq i \leq n$. Then in view of the given equations, $a \ [(\phi \wedge \psi) \vee (\phi \wedge \chi)] \ b$.

So V is congruence-distributive.

Additional Characterizations and Terminology

Theorem

A variety V is congruence permutable (respectively, congruence distributive) iff $\mathbf{F}_V(\overline{x},\overline{y},\overline{z})$ has permutable (respectively, distributive) congruences.

- This follows by looking at the proofs of the corresponding Mal'cev conditions.

Definition

- A ternary term p satisfying the congruence-permutability conditions for a variety V is called a **Mal'cev term** for V;
- A ternary term M satisfying the congruence-distributivity conditions is a **majority term** for V;
- A ternary term m satisfying the arithmeticity conditions is a $\frac{2}{3}$**-minority term** for V.

Subsection 5

Equational Logic and Fully Invariant Congruences

Fully Invariant Congruences

Definition

A congruence θ on an algebra $\mathbf{A}$ is **fully invariant** if, for every endomorphism α on $\mathbf{A}$,

$$\langle a,b\rangle \in \theta \quad \Rightarrow \quad \langle \alpha(a),\alpha(b)\rangle \in \theta.$$

Let $\mathrm{Con}_{\mathrm{FI}}(\mathbf{A})$ denote the set of fully invariant congruences on $\mathbf{A}$.

Lemma

$\mathrm{Con}_{\mathrm{FI}}(\mathbf{A})$ is closed under arbitrary intersection.

- First, note, that $\nabla^{\mathbf{A}}$ is invariant.

  Now, suppose $\{\theta_i : i \in I\} \subseteq \mathrm{Con}_{\mathrm{FI}}(\mathbf{A})$ and α is an endomorphism of $\mathbf{A}$. Then $\langle a,b\rangle \in \bigcap_{i\in I}\theta_i$ implies $\langle a,b\rangle \in \theta_i$, $i \in I$, implies $\langle \alpha(a),\alpha(b)\rangle \in \theta_i$, $i \in I$, implies $\langle \alpha(a),\alpha(b)\rangle \in \bigcap_{i\in I}\theta_i$.

Fully Invariant Congruence Generated by a Set of Pairs

Definition

Given an algebra **A** and $S \subseteq A \times A$ let $\Theta_{\mathrm{FI}}(S)$ denote the least fully invariant congruence on A containing S.
The congruence $\Theta_{\mathrm{FI}}(S)$ is called the **fully invariant congruence generated by** S.

The Fully Invariant Congruence Θ_{FI}

Lemma

If we are given an algebra $\mathbf{A}$ of type $\mathscr{F}$ then Θ_{FI} is an algebraic closure operator on $A \times A$. Indeed, Θ_{FI} is 2-ary.

- Construct $\mathbf{A} \times \mathbf{A}$. To the fundamental operations of $\mathbf{A} \times \mathbf{A}$ add the following:

$$\begin{array}{rcll} & & \langle a, a \rangle & \text{for } a \in A \\ s(\langle a, b \rangle) & = & \langle b, a \rangle & \\ t(\langle a, b \rangle, \langle c, d \rangle) & = & \begin{cases} \langle a, d \rangle, & \text{if } b = c \\ \langle a, b \rangle, & \text{otherwise} \end{cases} & \\ e_\sigma(\langle a, b \rangle) & = & \langle \sigma(a), \sigma(b) \rangle & \sigma \text{ endomorphism of } \mathbf{A} \end{array}$$

  Then θ is a fully invariant congruence on $\mathbf{A}$ iff θ is a subuniverse of the new algebra we have just constructed. Thus, Θ_{FI} is an algebraic closure operator.

The Fully Invariant Congruence Θ_{FI} (Cont'd)

- We show that Θ_{FI} is 2-ary. Define a new algebra $\mathbf{A}^*$ by replacing each n-ary fundamental operation f of $\mathbf{A}$ by the set of all unary operations of form $f(a_1,\ldots,a_{i-1},x,a_{i+1},\ldots,a_n)$, $a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n \in A$.

  Claim: $\mathrm{Con}\mathbf{A} = \mathrm{Con}\mathbf{A}^*$.

  Clearly $\theta \in \mathrm{Con}\mathbf{A} \Rightarrow \theta \in \mathrm{Con}\mathbf{A}^*$. For the converse suppose that $\theta \in \mathrm{Con}\mathbf{A}^*$ and $f \in \mathscr{F}_n$. Then, for $\langle a_i, b_i\rangle \in \theta$, $1 \le i \le n$, we have:

$$\begin{gathered}\langle f(a_1,\ldots,a_{n-1},a_n), f(a_1,\ldots,a_{n-1},b_n)\rangle \in \theta\\ \langle f(a_1,\ldots,a_{n-1},b_n), f(a_1,\ldots,b_{n-1},b_n)\rangle \in \theta\\ \vdots\\ \langle f(a_1,b_2,\ldots,b_2), f(b_1,b_2,\ldots,b_n)\rangle \in \theta.\end{gathered}$$

  Hence $\langle f(a_1,\ldots,a_n), f(b_1,\ldots,b_n)\rangle \in \theta$. Thus, $\theta \in \mathrm{Con}\mathbf{A}$.

  Go back to the beginning of the proof. Take $\mathbf{A}^*$ instead of $\mathbf{A}$. Keep the e_σ's the same. Then Θ_{FI} is the closure operator Sg of an algebra all of whose operations are of arity at most 2. Tus, Θ_{FI} is 2-ary.

From Identities to Congruences

Definition

Given a set of variables X and a type $\mathscr{F}$, let $\tau : \mathrm{Id}(X) \to T(X) \times T(X)$ be the bijection defined by $\tau(p \approx q) = \langle p, q \rangle$.

Lemma

For K a class of algebras of type $\mathscr{F}$ and X a set of variables, $\tau(\mathrm{Id}_K(X))$ is a fully invariant congruence on $\mathbf{T}(X)$.

- Let $p, q, r \in T(X)$.
  - $p \approx p \in \mathrm{Id}_K(X)$. Hence, $\langle p, p \rangle \in \tau(\mathrm{Id}_K(X))$.
  - Suppose $\langle p, q \rangle \in \tau(\mathrm{Id}_K(X))$. Then $p \approx q \in \mathrm{Id}_K(X)$. Thus, $q \approx p \in \mathrm{Id}_K(X)$. Hence, $\langle q, p \rangle \in \tau(\mathrm{Id}_K(X))$.
  - Suppose $\langle p, q \rangle, \langle q, r \rangle \in \tau(\mathrm{Id}_K(X))$. Then $p \approx q, q \approx r \in \mathrm{Id}_K(X)$. Thus, $p \approx r \in \mathrm{Id}_K(X)$. Hence, $\langle p, r \rangle \in \tau(\mathrm{Id}_K(X))$.

  Therefore, $\tau(\mathrm{Id}_K(X))$ is an equivalence relation on $T(X)$.

From Identities to Congruences (Cont'd)

- Let $f \in \mathscr{F}_n$, $p_1,\ldots,p_n,q_1,\ldots,q_n \in T(X)$, such that $\langle p_i,q_i\rangle \in \tau(\mathrm{Id}_K(X))$, $1 \le i \le n$. Then $p_i \approx q_i \in \mathrm{Id}_K(X)$, $1 \le i \le n$. Thus, $f(p_1,\ldots,p_n) \approx f(q_1,\ldots,q_n) \in \mathrm{Id}_K(X)$. Hence, $\langle f(p_1,\ldots,p_n), f(q_1,\ldots,q_n)\rangle \in \tau(\mathrm{Id}_K(X))$. So $\tau(\mathrm{Id}_K(X))$ is a congruence relation on $\mathbf{T}(X)$.
- Finally, let α be an endomorphism of $\mathbf{T}(X)$ and $p = p(x_1,\ldots,x_n)$, $q = q(x_1,\ldots,x_n) \in T(X)$, such that $\langle p,q\rangle \in \tau(\mathrm{Id}_K(X))$. Then $p(x_1,\ldots,x_n) \approx q(x_1,\ldots,x_n) \in \mathrm{Id}_K(X)$. Thus, $p(\alpha(x_1),\ldots,\alpha(x_n)) \approx q(\alpha(x_1),\ldots,\alpha(x_n)) \in \mathrm{Id}_K(X)$. It follows that $\alpha(p(x_1,\ldots,x_n)) \approx \alpha(q(x_1,\ldots,x_n)) \in \mathrm{Id}_K(X)$, i.e., $\langle \alpha(p),\alpha(q)\rangle \in \tau(\mathrm{Id}_K(X))$. Hence, $\tau(\mathrm{Id}_K(X))$ is fully invariant.

Freeness of $\mathbf{T}(X)/\theta$

Lemma

Given a set of variables X and a fully invariant congruence θ on $\mathbf{T}(X)$, we have, for $p \approx q \in \mathrm{Id}(X)$,

$$\mathbf{T}(X)/\theta \models p \approx q \quad \Leftrightarrow \quad \langle p, q \rangle \in \theta.$$

Thus, $\mathbf{T}(X)/\theta$ is free in $V(\mathbf{T}(X)/\theta)$.

($\Rightarrow$) If $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n)$, then

$$\begin{array}{ll} \mathbf{T}(X)/\theta \models p(x_1,\ldots,x_n) \approx q(x_1,\ldots,x_n) & \\ \Rightarrow & p(x_1/\theta,\ldots,x_n/\theta) = q(x_1/\theta,\ldots,x_n/\theta) \\ \Rightarrow & p(x_1,\ldots,x_n)/\theta = q(x_1,\ldots,x_n)/\theta \\ \Rightarrow & \langle p(x_1,\ldots,x_n), q(x_1,\ldots,x_n) \rangle \in \theta \\ \Rightarrow & \langle p, q \rangle \in \theta. \end{array}$$

Freeness of $\mathbf{T}(X)/\theta$ (Converse)

($\Leftarrow$) Given $r_1,\ldots,r_n \in T(X)$, we can find an endomorphism ε of $\mathbf{T}(X)$ with $\varepsilon(x_i) = r_i$, $1 \le i \le n$. Hence,

$$\begin{array}{ll} & \langle p(x_1,\ldots,x_n), q(x_1,\ldots,x_n)\rangle \in \theta \\ \Rightarrow & \langle \varepsilon(p(x_1,\ldots,x_n)), \varepsilon(q(x_1,\ldots,x_n))\rangle \in \theta \\ \Rightarrow & \langle p(r_1,\ldots,r_n), q(r_1,\ldots,r_n)\rangle \in \theta \\ \Rightarrow & p(r_1/\theta,\ldots,r_n/\theta) = q(r_1/\theta,\ldots,r_n/\theta). \end{array}$$

Thus, $\mathbf{T}(X)/\theta \models p \approx q$.

For the last claim, given $p \approx q \in \mathrm{Id}(X)$,

$$\begin{array}{rcl} \langle p,q\rangle \in \theta & \Leftrightarrow & \mathbf{T}(X)/\theta \models p \approx q \\ & \Leftrightarrow & V(\mathbf{T}(X)/\theta) \models p \approx q. \end{array}$$

So $\mathbf{T}(X)/\theta$ is free in $V(\mathbf{T}(X)/\theta)$.

Fully Invariant Congruences and Equational Theories

Theorem

Given a subset Σ of $\mathrm{Id}(X)$, one can find a K, such that $\Sigma = \mathrm{Id}_K(X)$ iff $\tau(\Sigma)$ is a fully invariant congruence on $\mathbf{T}(X)$.

($\Rightarrow$) This was proved in a preceding lemma.

($\Leftarrow$) Suppose $\tau(\Sigma)$ is a fully invariant congruence θ. Let $K = \{\mathbf{T}(X)/\theta\}$. Then by the preceding lemma, $K \models p \approx q$ iff $\langle p, q\rangle \in \theta$ iff $p \approx q \in \Sigma$. Thus $\Sigma = \mathrm{Id}_K(X)$.

Definition

A subset Σ of $\mathrm{Id}(X)$ is called an **equational theory over** X if there is a class of algebras K, such that $\Sigma = \mathrm{Id}_K(X)$.

Corollary

The equational theories (of type $\mathscr{F}$) over X form an algebraic lattice which is isomorphic to the lattice of fully invariant congruences on $\mathbf{T}(X)$.

Validity

Definition

Let X be a set of variables and Σ a set of identities of type $\mathscr{F}$, with variables from X. For $p, q \in T(X)$, we say $\Sigma \models p \approx q$ (read: "Σ **yields** $p \approx q$", or "Σ **implies** $p \approx q$") if, given any algebra $\mathbf{A}$, $\mathbf{A} \models \Sigma$ implies $\mathbf{A} \models p \approx q$.

Theorem

If Σ is a set of identities over X and $p \approx q$ is an identity over X, then $\Sigma \models p \approx q$ iff $\langle p, q \rangle \in \Theta_{\mathrm{FI}}(\tau(\Sigma))$.

- Assume $\langle p, q \rangle \in \Theta_{\mathrm{FI}}(\tau(\Sigma))$ and let $\mathbf{A}$ be such that $\mathbf{A} \models \Sigma$. $\tau(\mathrm{Id}_{\mathbf{A}}(X))$ is a fully invariant congruence on $\mathbf{T}(X)$. Hence, $\Theta_{\mathrm{FI}}(\tau(\Sigma)) \subseteq \tau(\mathrm{Id}_{\mathbf{A}}(X))$. Thus, since $\langle p, q \rangle \in \Theta_{\mathrm{FI}}(\tau(\Sigma))$, $\mathbf{A} \models p \approx q$.

  Conversely, assume $\Sigma \models p \approx q$. But $\mathbf{T}(X)/\Theta_{\mathrm{FI}}(\tau(\Sigma)) \models \Sigma$. Hence, $\mathbf{T}(X)/\Theta_{\mathrm{FI}}(\tau(\Sigma)) \models p \approx q$. Thus, $\langle p, q \rangle \in \Theta_{\mathrm{FI}}(\tau(\Sigma))$.

Replacements and Substitutions

Definition

Given a term p, the **subterms** of p are recursively defined by:

(1) The term p is a subterm of p.

(2) If $f(p_1,\ldots,p_n)$ is a subterm of p and $f \in \mathscr{F}_n$, then each p_i is a subterm of p.

Definition

A set of identities Σ over X is **closed under replacement** if given any $p \approx q \in \Sigma$ and any term $r \in T(X)$, if p occurs as a subterm of r, then letting s be the result of replacing that occurrence of p by q, we have $r \approx s \in \Sigma$.

Definition

A set of identities Σ over X is **closed under substitution** if for each $p \approx q$ in Σ and for $r_i \in T(X)$, if we simultaneously replace every occurrence of each variable x_i in $p \approx q$ by r_i, then the resulting identity is in Σ.

Deductive Closure

Definition

If Σ is a set of identities over X, then the **deductive closure** $D(\Sigma)$ of Σ is the smallest subset of $\text{Id}(X)$ containing Σ, such that:

(1) $p \approx p \in D(\Sigma)$, for all $p \in T(X)$;

(2) $p \approx q \in D(\Sigma) \Rightarrow q \approx p \in D(\Sigma)$, for all $p, q \in T(X)$;

(3) $p \approx q, q \approx r \in D(\Sigma) \Rightarrow p \approx r \in D(\Sigma)$, for all $p, q, r \in T(X)$;

(4) $D(\Sigma)$ is closed under replacement;

(5) $D(\Sigma)$ is closed under substitution.

Deductive Closure and Fully Invariant Congruences

Theorem

Given $\Sigma \subseteq \mathrm{Id}(X)$, $p \approx q \in \mathrm{Id}(X)$, $\Sigma \models p \approx q$ iff $p \approx q \in D(\Sigma)$.

- We first show that $\tau(D(\Sigma)) = \Theta_{\mathrm{FI}}(\tau(\Sigma))$.
  By definition $\tau(\Sigma) \subseteq \tau(D(\Sigma))$.
  By Properties (1)-(3), $\tau(D(\Sigma))$ is an equivalence relation.
  By Property (4) (closure under replacement), $\tau(D(\Sigma))$ is a congruence relation.
  By Property (5) (closure under substitution) $\tau(D(\Sigma))$ is fully invariant.
  By definition, $\Theta_{\mathrm{FI}}(\tau(\Sigma))$ is the smallest fully invariant congruence containing $\tau(\Sigma)$.
  Therefore, $\Theta_{\mathrm{FI}}(\tau(\Sigma)) \subseteq \tau(D(\Sigma))$.

Deductive Closure and Fully Invariant Congruences (Cont'd)

- We show that $\tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$ contains Σ and satisfies (1)-(5):
  - By definition $\tau(\Sigma) \subseteq \Theta_{\rm FI}(\tau(\Sigma))$. Thus, $\Sigma \subseteq \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$.
  - $\langle p,p\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$, i.e., $\tau(p \approx p) \subseteq \Theta_{\rm FI}(\tau(\Sigma))$. So $p \approx p \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$;
  - Suppose $p \approx q \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$. Then $\langle p,q\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$. Thus, $\langle q,p\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$. So $q \approx p \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$.
  - Transitivity is similar.
  - Suppose p is a term, $s \approx r \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$ and q results from substituting an occurrence of s in p by r. By hypothesis, $\langle s,r\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$. Since $\Theta_{\rm FI}(\tau(\Sigma))$ is a congruence, $\langle p,q\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$. Thus, $p \approx q \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$;
  - Let $p(x_1,\ldots,x_n) \approx q(x_1,\ldots,x_n) \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$ and $r_1,\ldots,r_n \in T(X)$. Then $\langle p,q\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$. Since $\Theta_{\rm FI}(\tau(\Sigma))$ is fully invariant, $\langle p(r_1,\ldots,r_n), q(r_1,\ldots,r_n)\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$. So $p(r_1,\ldots,r_n) \approx q(r_1,\ldots) \in \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$.

  By definition, $D(\Sigma)$ is the smallest set that contains Σ and satisfies (1)-(5). Hence $D(\Sigma) \subseteq \tau^{-1}(\Theta_{\rm FI}(\tau(\Sigma)))$. Thus, $\tau(D(\Sigma)) \subseteq \Theta_{\rm FI}(\tau(\Sigma))$. Now we get $\Sigma \models p \approx q$ iff $\langle p,q\rangle \in \Theta_{\rm FI}(\tau(\Sigma))$ iff $p \approx q \in \tau(D(\Sigma))$ iff $p \approx q \in D(\Sigma)$.

Formal Deduction and Provability

Definition

Let Σ be a set of identities over X. For $p \approx q \in \mathrm{Id}(X)$, we say $\Sigma \vdash p \approx q$, read "$\Sigma$ **proves** $p \approx q$", if there is a sequence of identities

$$p_1 \approx q_1, \ldots, p_n \approx q_n$$

from $\mathrm{Id}(X)$, such that each $p_i \approx q_i$ belongs to Σ, or is of the form $p \approx p$, or is a result of applying any of the four closure rules

$$\begin{array}{l} p \approx q \in D(\Sigma) \;\Rightarrow\; q \approx p \in D(\Sigma); \\ p \approx q,\; q \approx r \in D(\Sigma) \;\Rightarrow\; p \approx r \in D(\Sigma); \\ D(\Sigma) \text{ is closed under replacement}; \\ D(\Sigma) \text{ is closed under substitution} \end{array}$$

to previous identities in the sequence, and the last identity $p_n \approx q_n$ is $p \approx q$. The sequence $p_1 \approx q_1, \ldots, p_n \approx q_n$ is called a **formal deduction** of $p \approx q$. The number n is the **length** of the deduction.

The Completeness Theorem for Equational Logic

Theorem (Birkhoff's Completeness Theorem for Equational Logic)

Given $\Sigma \subseteq \mathrm{Id}(X)$ and $p \approx q \in \mathrm{Id}(X)$, we have $\Sigma \models p \approx q$ iff $\Sigma \vdash p \approx q$.

- In the construction of a formal deduction $p_1 \approx q_1, \ldots, p_n \approx q_n$ of $p \approx q$, only properties under which $D(\Sigma)$ is closed are used. Hence, $\Sigma \vdash p \approx q$ implies $p \approx q \in D(\Sigma)$.

  For the converse:
  - $\Sigma \vdash p \approx q$, for $p \approx q \in \Sigma$, and $\Sigma \vdash p \approx p$, for $p \in T(X)$.
  - If $\Sigma \vdash p \approx q$, then there is a formal deduction $p_1 \approx q_1, \ldots, p_n \approx q_n$ of $p \approx q$. Now $p_1 \approx q_1, \ldots, p_n \approx q_n, q_n \approx p_n$ is a formal deduction of $q \approx p$. Hence, $\Sigma \vdash q \approx p$.
  - If $\Sigma \vdash p \approx q$, $\Sigma \vdash q \approx r$, let $p_1 \approx q_1, \ldots, p_n \approx q_n$ be a formal deduction of $p \approx q$ and let $\overline{p}_1 \approx \overline{q}_1, \ldots, \overline{p}_k \approx \overline{q}_k$ be a formal deduction of $q \approx r$. Then $p_1 \approx q_1, \ldots, p_n \approx q_n$, $\overline{p}_1 \approx \overline{q}_1, \ldots, \overline{p}_k \approx \overline{q}_k$, $p_n \approx \overline{q}_k$ is a formal deduction of $p \approx r$. Thus, $\Sigma \vdash p \approx r$.

The Completeness Theorem for Equational Logic (Cont'd)

- We continue with the remaining deduction rules:
  - If $\Sigma \vdash p \approx q$, let $p_1 \approx q_1, \ldots, p_n \approx q_n$ be a formal deduction of $p \approx q$. Let $r(\ldots, p, \ldots)$ denote a term with a specific occurrence of the subterm p. Then $p_1 \approx q_1, \ldots, p_n \approx q_n, r(\ldots, p_n, \ldots) \approx r(\ldots, q_n, \ldots)$ is a formal deduction of $r(\ldots, p, \ldots) \approx r(\ldots, q, \ldots)$.
  - Finally, if $\Sigma \vdash p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$, let $p_1 \approx q_1, \ldots, p_m \approx q_m, p \approx q$ be a formal deduction of $p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$ from Σ. Then, for terms $r_1, \ldots, r_n$, $p_1 \approx q_1, \ldots, p_m \approx q_m, p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n), p(r_1, \ldots, r_n) \approx q(r_1, \ldots, r_n)$ is a formal deduction of $p(r_1, \ldots, r_n) \approx q(r_1, \ldots, r_n)$ from Σ.

Thus, $D(\Sigma) \subseteq \{p \approx q : \Sigma \vdash p \approx q\}$. Hence, $D(\Sigma) = \{p \approx q : \Sigma \vdash p \approx q\}$. Therefore,

$$\Sigma \models p \approx q \quad \text{iff} \quad p \approx q \in D(\Sigma) \quad \text{iff} \quad \Sigma \vdash p \approx q.$$

Examples

(1) An identity $p \approx q$ is **balanced** if each variable occurs the same number of times in p as in q.

If Σ is a balanced set of identities, then, using induction on the length of a formal deduction, we can show that if $\Sigma \vdash p \approx q$, then $p \approx q$ is balanced.

This is not at all evident if one works with the notion $\models$.

(2) A famous theorem of Jacobson in ring theory says that, if we are given $n \geq 2$, if Σ is the set of ring axioms plus $x^n \approx x$, then $\Sigma \models x \cdot y \approx y \cdot x$.

However, there is no published routine way of writing out a formal deduction, given n, of $x \cdot y \approx y \cdot x$.

For special n, such as $n = 2, 3$, this is a popular exercise.

Minimal Subvarieties

Definition

A variety V is **trivial** if all algebras in V are trivial. A subclass W of a variety V which is also a variety is called a **subvariety** of V. V is a **minimal** (or **equationally complete**) variety, if V is not trivial, but the only subvariety of V not equal to V is the trivial variety.

Theorem

Let V be a nontrivial variety. Then V contains a minimal subvariety.

- Let $V = M(\Sigma)$, $\Sigma \subseteq \mathrm{Id}(X)$, with X infinite. Then $\mathrm{Id}_V(X)$ defines V. As V is nontrivial, $\tau(\mathrm{Id}_V(X))$ is a fully invariant congruence on $\mathbf{T}(X)$ which is not ∇. But $\nabla = \Theta_{\mathrm{FI}}(\langle x, y\rangle)$, for any $x, y \in X$, with $x \neq y$. Hence, ∇ is finitely generated (as a fully invariant congruence). This allows us to use Zorn's lemma to extend $\tau(\mathrm{Id}_V(X))$ to a maximal fully invariant congruence on $\mathbf{T}(X)$, say θ. Then $\tau^{-1}(\theta)$ must define a minimal variety which is a subvariety of V.

Example: Lattices

- The variety of lattices has a unique minimal subvariety, the variety generated by a two-element chain.

  To see this let V be a minimal subvariety of the variety of lattices. Let $\mathbf{L}$ be a nontrivial lattice in V. As $\mathbf{L}$ contains a two-element sublattice, we can assume $\mathbf{L}$ is a two-element lattice. Now $V(\mathbf{L})$ is not trivial, and $V(\mathbf{L}) \subseteq V$, whence $V(\mathbf{L}) = V$.