1.1 - Definition and Examples of Ω-algebras

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Operations rise quite often in mathematics. Ever tend to notice how monoids, groups, rings, modules, lattices, etc. have similar abilities? This is because each is a set equipped with certain operations. Any such set can be treated in a generic way, which leads to the following.

Universal algebra studies morphisms, products and a lot of other topics on a generalized operation equipment on a set. To see the idea, we must stick to one batch of operation equipment which we call the *signature*.

Consider the monoid M, for instance. M is a set with an associative binary operation $*$ which has a unit 1. The binary operation $*$ should certainly belong to the signature. Now when we give a set M a binary operation $*$, do we know whether we result in a monoid? Yes, either the operation is associative or it is not, and there is at most one element 1 satisfying $1 * x = x = x * 1$ for every $x \in M$ [see Exercise 1]. So it appears that $*$ is the only operation to belong to the signature. That is not quite true, as we are about to see.

A homomorphism of monoids $f : M \to N$ satisfies $f(1) = 1$ and $f(xy) = f(x)f(y)$ for all $x, y \in M$. If only the binary operation mattered, a homomorphism would only need to satisfy $f(xy) = f(x)f(y)$. This is not sufficient, as there exist maps of monoids that preserve multiplication but do not map 1 to 1. Consider $M = N = (\mathbb{Z}, \cdot)$, for instance. Then if $f : M \to N$ is defined by $f(a) = 0$ for all a, then $f(xy) = f(x)f(y)$ [since $0 \cdot 0 = 0$] but $f(1) \neq 1$.

So both the binary operation $*$ and the unit 1 are needed to keep things in hand. Afterwards, we need only regard the identities $(xy)z = x(yz)$ and $1x = x = x1$, which don't affect homomorphisms at all.

Note that if G and H are *groups* and $f : G \to H$ satisfies $f(xy) = f(x)f(y)$, then f is a group homomorphism [see Exercise 2]. So in terms of group homomorphisms, only the binary operation needs to be regarded. But this is not so for subgroups. The subset $\mathbb{N}$ of the additive group $\mathbb{Z}$ is not a subgroup because $1 \in \mathbb{N}$, but its inverse -1 is not in $\mathbb{N}$. It is closed under addition, nevertheless.

Therefore the group's signature needs to regard the binary operation, the inverse and the identity. It is then straightforward what the requirements of a subgroup would be.

To generalize the idea, it is important to know that a set like that has two things: (1) existential operators; (2) equational identities [axioms of the form $(\dots) = (\dots)$]. Morphisms and subsets that have the equipment need to regard (1), but not (2). (1) comes in the form of *n-ary operators*, which are feed n elements of the set and return an element of the set. As of now, we will stick to only (1).

Let A be a set, and n a nonnegative integer. If ω is a map $A^n \to A$ sending $(a_1, a_2, \dots a_n)$ to $(\omega a_1 a_2 \dots a_n)$, then ω is an n-ary operator on A. An example with $n = 2$ is the binary operation on a monoid. Note that if $n = 0$, ω is just a map from the 1-element set $\{()\}$ to A, which can be thought of as an element

(ω_A) of A. An example of this is the unit 1 of a monoid, which must be regarded by the signature.

There may be many operators in the signature, but each has a certain degree. This motivates the following definitions.

DEFINITION

*A **signature** is a mathematical object Ω such that for each nonnegative integer n, $\Omega(n)$ is a set, whose elements are called n-**ary operators**. Ω can be thought of as $\uplus\Omega(n)$.*

*If Ω is a signature, an Ω-**algebra** is a set A such that for each $n \geq 0$, each $\omega \in \Omega(n)$ is associated with a map $A^n \to A$, where the output under $(a_1, a_2, \ldots a_n)$ is denoted $(\omega a_1 a_2 \ldots a_n)$. The set is called the **carrier** of the Ω-algebra.*

EXAMPLES

A vast majority of the following examples have equational identities. However, it is best that we not generalize the concept of identities until Section 9.

1. Let $\Omega = \{p, 1\}$ where p is binary and 1 is nullary. Then a monoid is an Ω-algebra satisfying the identities $(px(pyz)) = (p(pxy)z)$; $(p(1)x) = x$; $(px(1)) = x$.

2. Let $\Omega = \{p, 1, i\}$ where p is binary, 1 is nullary and i is unary. Then a group is an Ω-algebra satisfying the identities $(px(pyz)) = (p(pxy)z)$; $(p(1)x) = x$; $(px(1)) = x$; $(px(ix)) = (1)$; $(p(ix)x) = (1)$. Note that the last identity is quite redundant; it follows from the other identities.

3. Add the identity $(pab) = (pba)$ to the previous example to get an abelian group. They form a signature of their own.

4. A ring is an Ω-algebra with even more identities, where $\Omega(2) = \{s, p\}$ (s sum, p product), $\Omega(1) = \{n\}$ (additive inverse) and $\Omega(0) = \{0, 1\}$. As an exercise, write out all the necessary identities; one of them is $(px(syz)) = (s(pxy)(pxz))$.

5. A **rng** is an Ω-algebra where $\Omega(2) = \{s, p\}$, $\Omega(1) = \{n\}$ and $\Omega(0) = \{0\}$, and all the ring's identities that don't involve 1 are satisfied. A rng can be thought of as a "ring without unit."

6. A **ring with involution** is a ring R with an extra unary operator $a \to a^*$ satisfying $(a + b)^* = a^* + b^*$, $(ab)^* = b^*a^*$, $1^* = 1$ and $(a^*)^* = a$. It is easily seen that there is a signature for rings with involution.

7. If $\Omega(n) = \emptyset$ for all n, then an Ω-algebra is simply a set. You can think of this as a set equipped with no operations at all. Ω is called the **empty signature**.

8. A **pointed set** is an Ω-algebra where Ω consists of a single nullary operator for the **base point**. It can be thought of as a pair (X, x_0), where $x_0 \in X$.

9. A **set with involution** is an Ω-algebra A where Ω consists of a single unary operator * and $(a^*)^* = a$ for all $a \in A$. The operator is called an **involution**.

10. Let R be a fixed ring. Define $\Omega(2) = \{s\}$, $\Omega(0) = \{0\}$ and $\Omega(1) = R$. Then an Ω-algebra satisfying the correct identities [such as $(r(sx)) = ((rs)x)$ when $r, s \in R$] is a left R-module. Note that there is no restriction on the cardinality of operators or identities.

Warning: There is no signature for all modules. The modules *over a given ring* can be put into a signature. It is pertinent to know that there's no such thing as a module homomorphism from M to N if they are modules over entirely different rings.

11. In a similar way right R-modules and R-S-bimodules can be defined.

12. A **Lie algebra** over a commutative ring R is an R-module L with a binary operator $a, b \to [a : b]$ satisfying $[x : (y + z)] = [x : y] + [x : z]$, $[(x + y) : z] = [x : z] + [y : z]$, $[x : cy] = c[x : y] = [cx : y]$, $[x : x] = 0$ and $[x : [y : z]] + [y : [z : x]] + [z : [x : y]] = 0$. Once again, this is an Ω-algebra with identities, and they will be dealt with in Sections 9 and up.

13. An **associative algebra** over a commutative ring R is a ring A which is an R-module with the same addition, such that $(cx)y = c(xy) = x(cy)$ for all $c \in R$, $x, y \in A$. For example, the matrix ring $M_n(R)$ is an associative algebra over R.

14. A **magma** is a set equipped with a binary operation. It does not require any identities. A **semigroup** is a magma whose operation is associative; i.e. satisfies the identity $(pa(pbc)) = (p(pab)c)$. Thus a monoid is a semigroup with an identity element.

15. A **lattice** is an Ω-algebra where $\Omega(2) = \{\wedge, \vee\}$ satisfying $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$, $a \wedge b = b \wedge a$, $a \vee b = b \vee a$, $a \wedge a = a = a \vee a$, $a \wedge (a \vee b) = a = a \vee (a \wedge b)$.

16. Let M be a monoid. An M-action is an Ω-algebra X with $\Omega(1) = M$ [that is, a set X along with a map $M \times X \to X$] satisfying $1x = x$ and $(mn)x = m(nx)$ for $m, n \in M$, $x \in X$. Thus a set with involution is an M-action where M is the group $\mathbb{Z}_2$.

You should be convinced that there are loads of different kinds of Ω-algebras. This is why we should be able to give general proofs that work for all of them.

New Signatures from Old Ones

If Ω_1 and Ω_2 are signatures, Ω_2 is said to be an **extension** of Ω_1 provided that $\Omega_1(n) \subseteq \Omega_2(n)$ for all n. In this case, every Ω_2-algebra is an Ω_1-algebra.

EXAMPLES

Note that the definition of an extension can be rephrased when identities are involved. But like we said, we are not dealing with identities quite yet.

1. The group's signature is an extension of the monoid's, which is an extension of the semigroup's, which is an extension of the magma's.

2. The ring's signature is an extension of the rng's, where the identity is added. The signature for the ring with involution is an extension of the ring's

signature. The rng's signature is an extension of the signature for an abelian group (because a rng is an abelian group under addition).

3. Every signature is an extension of the empty signature for sets, because $\emptyset \subseteq \Omega(n)$ whenever Ω is a signature. This works as promised; an Ω-algebra is a set.

4. If F is a field, then associative algebras over F are an extension of rings, and also an extension of vector spaces over F. Lie algebras over F are an extension of vector spaces over F.

5. Note that a monoid is actually an extension of a pointed set, because a monoid M can have the weaker treatment as a pointed set with base point 1.

6. Abelian groups are an extension of groups, and commutative rings are an extension of rings.

New Ω-algebras from Old Ones

It is high time we stop talking about all the different signatures, and from this point, focus on a single signature Ω. Can two Ω-algebras A and B be combined, in a generic way that doesn't depend on Ω? The answer is yes: we define $A \times B$ to be the usual Cartesian product of sets, and for each $n \in \Omega(n)$, we define

$$(\omega(a_1, b_1)(a_2, b_2) \dots (a_n, b_n)) = ((\omega a_1 a_2 \dots a_n), (\omega b_1 b_2 \dots b_n))$$

For instance, if A and B are sets with involution, $A \times B$ is defined by $(a, b)^* = (a^*, b^*)$.

Now suppose A is an Ω-algebra and S is a set. [S need not be an Ω-algebra at all.] One can define an Ω-algebra structure on the set A^S of functions $S \to A$ thus: for $\omega \in \Omega(n)$ and $f_1, f_2, \dots f_n \in A^S$, $(\omega f_1 f_2 \dots f_n) : S \to A$ is defined by $(\omega f_1 f_2 \dots f_n)(s) = (\omega f_1(s) f_2(s) \dots f_n(s))$.

This is a vague introduction to Ω-algebras. It should be easy to remember in the future sections.

EXERCISES

1. If M is a set equipped with a binary operation $*$, prove that there is at most one $1 \in M$ such that $1 * x = x = x * 1$ for every $x \in M$.

2. Let G and H be groups. If $f : G \to H$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$, prove that f is a homomorphism. [You need to show that $f(e) = e$ and $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$.]

3. What is wrong with the following argument that subgroups of a group need not regard the identity element? "If H is a subgroup of G and $a \in H$, then $a^{-1} \in H$ since the inverse of an element of H is also in H. Furthermore, $aa^{-1} = e \in H$ since H is closed under multiplication. Therefore, every subset of G closed under multiplication and inverses automatically contains the identity element."

4. Let G be a semigroup.

   (a) If there exists $e \in G$ such that $ea = a$ for all a and for each $a \in G$, there exists $d \in G$ such that $da = e$, prove that G is a group.

   (b) If there exists $e \in G$ such that $ea = a$ for all a and for each $a \in G$, there exists $d \in G$ such that $ad = e$, show by example that G may not be a group.

   (c) If G is finite and nonempty, and whenever $ab = ac$ or $ba = ca$ then $b = c$, prove that G is group.

   (d) Show by example that (c) may be false if G is infinite.

   (e) If G is nonempty and for all $a, b \in G$, there exist $x, y \in G$ such that $ax = b = ya$, prove that G is a group.

5. For a Boolean algebra, what are all the operations needed in the signature?

6. Show that an associative algebra A over a commutative ring R is a Lie algebra given by $[a : b] = ab - ba$ for $a, b \in A$.

7. If L is a Lie algebra over R, prove that $[a : b] = -[b : a]$ for $a, b \in L$. [*Hint*: Expand $[(a + b) : (a + b)]$.]

8. (a) Show that every signature Ω is an extension of Ω.

   (b) Show that if Ω_3 is an extension of Ω_2 and Ω_2 is an extension of Ω_1, then Ω_3 is an extension of Ω_1.

9. Let $T(\Omega)$ be the 1-element set $\{\epsilon\}$, where for each $\omega \in \Omega(n)$, $(\omega\epsilon\epsilon \dots \epsilon) = \epsilon$. Convince yourself that $T(\Omega)$ is an Ω-algebra. It is called the **terminal** or **trivial Ω-algebra**.

1.2 - Subalgebras and Products

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Recall the Ω-algebra from last chapter. What subsets are also Ω-algebras under the operations in Ω? Well, the ones that are closed under the operations. Section 9 shows that any equational identity holding in an Ω-algebra must also hold in each subset closed under the operations. This yields the following definition.

DEFINITION

Let A be an Ω-algebra. A subset B of A is called a ***subalgebra*** *of A provided that whenever $\omega \in \Omega(n)$ and $a_1, a_2, \ldots a_n \in B$, then $(\omega a_1 a_2 \ldots a_n) \in B$. When $n = 0$, it is understood that B contains every nullary $(\omega_A) \in A$.*

Note: Most authors require every Ω-algebra to be nonempty. This yields differences in the future lessons. I personally think that an Ω-algebra should not be required to be nonempty unless it follows from the equipment. See Exercise 1.

If B is a subalgebra of A, the first pertinent thing to be able to view B as an Ω-algebra itself under the operations in A. Then it is clear that A is a subalgebra of A, and a subalgebra C of a subalgebra B of A is a subalgebra of A.

EXAMPLES

1. Let G be a group and H a subgroup of G. Then H is a group under the operation in G. The converse actually holds in this case: if H is a subset of G which is a group under the binary operation in G, then H is a subgroup of G. This is because, for example, if $a \in G$ and $ab = b$ for at least *one* $b \in G$, then $a = e$.

2. If M is a monoid, a subset of M which is a monoid under M's binary operation need not be a submonoid of M. Consider $M = (\mathbb{Z}_6, \cdot)$, for instance. Let $N = \{[0], [2], [4]\} \subseteq M$. Then N is a monoid under multiplication [with identity [4]], but N is not a submonoid of M because $[1] \notin N$. A submonoid of M must be a monoid under M's multiplication *and* identity element.

3. If Ω-algebras are pointed sets, a subalgebra of (X, x_0) is a subset of X containing x_0.

4. Yeah...let's cut the examples.

Let Sub A be the set of subalgebras of A. We claim that Sub A is a **complete lattice** under inclusion [i.e. a lattice in which every nonempty subset has a sup and an inf]. It all follows from quite a basic lemma:

LEMMA 1.1 *Let L be a partially ordered set with a largest element 1 such that every nonempty subset has an inf. Then L is a complete lattice.*

Proof of Lemma 1.1. We need to show that every nonempty subset $S \subseteq L$ has a sup. Let $\overline{S} = \{a \in L \mid s \leq a \ \forall s \in S\}$ be the set of upper bounds of S. $1 \in \overline{S}$

so $\overline{S}$ is nonempty. Therefore, by hypothesis, $\overline{S}$ has an inf u. Since each $s \in S$ is a lower bound of $\overline{S}$, $s \leq u$ and u is an upper bound of S. If v is any other upper bound of S, then $v \in \overline{S}$, and hence, $u \leq v$. Therefore, u is a sup of S. ■

THEOREM 1.2 *If A is an Ω-algebra, then Sub A is a complete lattice under inclusion.*

Proof of Theorem 1.2. Sub A is clearly a poset under inclusion. Also, $A \in$ Sub A is largest in the poset. Now let $\{A_\alpha\}$ be a nonempty family of subalgebras of A. Exercise 2 shows that the intersection $\cap A_\alpha$ is a subalgebra of A, and it is seen to be the inf of $\{A_\alpha\}$. Therefore, Sub A has a largest element and every nonempty subset has an inf. We can then apply Lemma 1.1 and conclude that Sub A is a complete lattice. ■

According to Theorem 1.2, any family $\{A_\alpha\}$ of subalgebras of A has a least upper bound. This does *not* mean the union $\cup A_\alpha$ is necessarily a subalgebra of A. Rather, it means there is a *subalgebra* of A containing the A_α that's contained in every *subalgebra* of A containing the A_α. This subalgebra is denoted as $\vee A_\alpha$.

However, there *is* a rather important case in which the union $\cup A_\alpha$ is a subalgebra; see Exercise 3.

But unions of subalgebras aren't the only things that can generate subalgebras. In fact, *any* subset of A generates a subalgebra according to the following theorem. Recall that in the proof of Lemma 1.1, we showed that the sup of a set is the inf of its upper bounds. This gives us a clue as to what to do.

For $X \subseteq A$, define the **subalgebra of A generated by X** — denoted $\langle X \rangle$ — to be the intersection of all subalgebras of A containing X. Note that at least one subalgebra of A contains X — namely A itself.

THEOREM 1.3 *Let X be a subset of an Ω-algebra A. Then:*

(1) *$\langle X \rangle$ is a subalgebra of A containing X.*

(2) *Whenever B is a subalgebra of A containing X, $\langle X \rangle \subseteq B$.*

(3) *$\langle X \rangle$ is the only subalgebra of A with properties (1) and (2).*

Proof of Theorem 1.3. (1) $\langle X \rangle$ is the intersection of subalgebras of A, which is a subalgebra of A by Exercise 2. Since X is contained in every operand set, it is contained in the intersection.

(2) If B is a subalgebra of A containing X, then B is one of the operands that $\langle X \rangle$ is the intersection of; hence, $\langle X \rangle \subseteq B$.

(3) Suppose X' is another subalgebra of A satisfying properties (1) and (2). Since X' is a subalgebra of A containing X, then $\langle X \rangle \subseteq X'$ by (2). Reversing the roles, since $\langle X \rangle$ is a subalgebra of A containing X and every such subalgebra contains X', then $X' \subseteq \langle X \rangle$. Therefore, $X' = \langle X \rangle$, and $\langle X \rangle$ is unique. ■

One can think of $\vee A_\alpha$ as $\langle \cup A_\alpha \rangle$ according to the last theorem. It is the smallest subalgebra of A containing every A_α.

Arbitrary Products

We recall the constructions of $A \times B$ and A^S from the last chapter. They are just special cases of the following.

DEFINITION

Let $\{A_\alpha\}$ be an indexed collection of Ω-algebras. Now let A be the set product ΠA_α and for $a \in A$, denote as a_α the component of a in place α. Then A becomes an Ω-algebra where $\omega \in \Omega(n)$ is defined as:

$$(\omega a^1 a^2 \dots a^n)_\alpha = (\omega a^1_\alpha a^2_\alpha \dots a^n_\alpha)$$

for each $a^1, a^2, \dots a^n \in A$ and component index α.

Note that there is no restriction on the cardinality of $\{A_\alpha\}$. The next section shows how $A \times B$ can be viewed as a product of A and B, and that A^S can be viewed as a product of as many A's as elements of S.

When $A_1, A_2, \dots A_n$ are finitely many Ω-algebras, the product is denoted ΠA_i or $A_1 \times A_2 \times \dots \times A_n$.

Note, by the way, that Section 9 shows that identities are safely preserved by the product.

EXERCISES

1. Show that every Ω-algebra is nonempty if and only if $\Omega(0)$ is nonempty [i.e. Ω has a nullary operator].

2. If $\{A_\alpha\}$ is a nonempty family of subalgebras of A, prove that the intersection $\cap A_\alpha$ is a subalgebra of A.

3. Now suppose $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ is an ascending chain of subalgebras of A. Prove that the union $\cup A_i$ is a subalgebra of A. [*Hint*: If $a_1, a_2, \dots a_n \in \cup A_i$, each of them is in one of the algebras in the chain. Why must one of the algebras contain all of them?]

4. Let $A_1, A_2, \dots A_n$ be Ω-algebras. Show that $A = A_1 \times A_2 \times \dots \times A_n$ is finite if and only if all the A_i are, and that $|A| = |A_1||A_2| \dots |A_n|$. Conclude that A is empty if and only if at least one of the A_i is.

5. (a) If $\{A_\alpha\}$ is an indexed collection of Ω-algebras and B_α is a subalgebra of A_α for every α, prove that ΠB_α is a subalgebra of ΠA_α.

   (b) Give an example to show that a subalgebra of ΠA_α need not be described like such.

1.3 - Homomorphisms and Isomorphisms

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

A homomorphism of Ω-algebras is a map that preserves structure. These maps are more important than any maps, since structure is mostly what we care for. To get a rigorous definition of a homomorphism, we must recall the structure of an Ω-algebra.

If A is an Ω-algebra, an n-ary operator corresponds to a map $\omega : A^n \to A$ mapping $a_1, a_2, \dots a_n$ to $(\omega a_1 a_2 \dots a_n)$. Now let $f : A \to B$ be a function. It is generous to say that f *preserves* ω if whenever it maps $a_i \in A$ to $b_i \in B$, it maps $(\omega a_1 a_2 \dots a_n)$ to $(\omega b_1 b_2 \dots b_n)$. But we want a quicker way to say this.

Notice that the element of B that f maps a_i to is denoted $f(a_i)$. Taking $b_i = f(a_i)$, we have $(\omega b_1 b_2 \dots b_n) = (\omega f(a_1) f(a_2) \dots f(a_n))$. So our rule is that f maps $(\omega a_1 a_2 \dots a_n)$ to $(\omega f(a_1) f(a_2) \dots f(a_n))$, as seen in the following definition.

DEFINITION

If A and B are Ω-algebras, a map $f : A \to B$ is said to be a ***homomorphism*** *if for all $\omega \in \Omega(n)$ and $a_1, a_2, \dots a_n \in A$,*

$$f(\omega a_1 a_2 \dots a_n) = (\omega f(a_1) f(a_2) \dots f(a_n))$$

When $n = 0$ it is understood that the statement says $f(\omega_A) = (\omega_B)$. A homomorphism that is bijective is called an ***isomorphism****.*

Note that this definition does not regard any equational identities. It never will, as there is no notion of identities being preserved by maps.

EXAMPLES

1. Monoid, group and ring homomorphisms are as usual.
2. If Ω-algebras are pointed sets, a homomorphism $(X, x_0) \to (Y, y_0)$ is a map $f : X \to Y$ satisfying $f(x_0) = y_0$.
3. A homomorphism $f : M \to N$ of left R-modules satisfies $f(a+b) = f(a) + f(b)$ and $f(ka) = kf(a)$ for $a, b \in M, k \in R$. Recall that scalar multiplication is viewed as $|R|$ unary operators. In this case, our definition of a homomorphism certainly matches with this one.
4. If M and N are modules over different rings, they are not the same kind of algebra, so there's no notion of a homomorphism from M to N, except for just an abelian group homomorphism.
5. If M is a fixed monoid and X and Y are M-actions, a homomorphism $f : X \to Y$ is an **equivariant map**: it satisfies $f(mx) = mf(x)$ for $m \in M, x \in X$.

There are a few preliminary things to know about homomorphisms:

THEOREM 1.4 *Let A, B, C be Ω-algebras, $f : A \to B$ and $g : B \to C$ homomorphisms. Then:*

(1) *The composite function $gf : A \to C$ is a homomorphism.*
(2) *The identity map $1_A : A \to A$ is an isomorphism.*
(3) *If f is an isomorphism, then so is its inverse $f^{-1} : B \to A$.*

Proof of Theorem 1.4. (1) The statement follows from

$$gf(\omega a_1 a_2 \dots a_n) = g(\omega f(a_1) f(a_2) \dots f(a_n)) = (\omega gf(a_1) gf(a_2) \dots gf(a_n))$$

for all $\omega \in \Omega(n)$, $a_1, a_2, \dots a_n \in A$.

(2) It is clear that 1_A is bijective, and that $1_A(\omega a_1 a_2 \dots a_n) = (\omega a_1 a_2 \dots a_n) = (\omega 1_A(a_1) 1_A(a_2) \dots 1_A(a_n))$.

(3) Since f is a bijection, then so is f^{-1}, and $ff^{-1} = 1_B$ and $f^{-1}f = 1_A$ hold. We need only show that f^{-1} is a homomorphism:

$$f^{-1}(\omega b_1 b_2 \dots b_n) = f^{-1}(\omega ff^{-1}(b_1) ff^{-1}(b_2) \dots ff^{-1}(b_n))$$

$$= f^{-1}f(\omega f^{-1}(b_1) f^{-1}(b_2) \dots f^{-1}(b_n)) = (\omega f^{-1}(b_1) f^{-1}(b_2) \dots f^{-1}(b_n))$$

whenever $\omega \in \Omega(n)$ and $b_1, b_2, \dots b_n \in B$. ■

An Ω-algebra A is said to be **isomorphic** to an Ω-algebra B — denoted $A \cong B$ — if there exists an isomorphism $A \to B$. Notice that $A \cong A$ by Theorem 1.4(2), and if $A \cong B$ then $B \cong A$ by Theorem 1.4(3). Now suppose $A \cong B$ and $B \cong C$. Then there exist isomorphisms $f : A \to B$ and $g : B \to C$. The map $gf : A \to C$ is a homomorphism by Theorem 1.4(1) and is bijective because f and g are. Hence, gf is an isomorphism and $A \cong C$. Therefore, isomorphism is an equivalence relation.

Now let's cut the isomorphism and get to some pertinent homomorphisms. Let $\{A_\alpha\}$ be an indexed collection of Ω-algebras and $A = \Pi A_\alpha$. Define $p_\alpha : A \to A_\alpha$ by $p_\alpha(a) = a_\alpha$. Then p_α is seen to be a homomorphism because $(\omega a^1 a^2 \dots a^n)_\alpha = (\omega a^1_\alpha a^2_\alpha \dots a^n_\alpha)$ holds. p_α is called a **projection homomorphism**. Section 4 of Chapter 2 explains more about this.

Making a Homomorphism Surjective

If $f : A \to B$ is a homomorphism of Ω-algebras, its image $f(A)$ may not be all of B. However, it is readily seen to be a subalgebra of B, for if $\omega \in \Omega(n)$ and $b_1, b_2, \dots b_n \in f(A)$, each $b_i = f(a_i)$ for some $a_i \in A$. Furthermore,

$$(\omega b_1 b_2 \dots b_n) = (\omega f(a_1) f(a_2) \dots f(a_n)) = f(\omega a_1 a_2 \dots a_n) \in f(A)$$

Hence, $f(A)$ is a subalgebra of B. Conversely, every subalgebra C of B is the image of some homomorphism into B. Define $\iota : C \to B$ by $\iota(c) = c$ for all $c \in C$. [This map is seen to fix its subjects while enlarging the outside

world.] Exercise 1 shows that ι is an injective homomorphism. It is called the **canonical monomorphism** [or **injection homomorphism**] of C into B and is sometimes denoted $C \hookrightarrow B$.

The idea of surjectification is to cut the codomain down to a subalgebra containing the image. Important things to know are that, as shown in (3), injectivity is not affected, and as shown in (4), surjectivity comes from cutting the codomain down entirely to the image.

THEOREM 1.5 (SURJECTIFICATION) *Let $f : A \to B$ be a homomorphism of Ω-algebras and C a subalgebra of B. If $\iota : C \to B$ is the canonical monomorphism, then:*

(1) *There exists a homomorphism $f_1 : A \to C$ such that $f = \iota f_1$ [in other words, that $f_1(a) = f(a)$ for all $a \in A$] if and only if $f(A) \subseteq C$.*

If the equivalent conditions in (1) hold, then

(2) *f_1 is unique;*

(3) *f_1 is injective if and only if f is injective;*

(4) *f_1 is surjective if and only if $f(A) = C$.*

You're probably wondering if there's an analogue of this theorem with injectivity and surjectivity exchanged. The answer is yes, but a new concept in the next section is needed for this.

Proof of Theorem 1.5. (1) If $f(A) \subseteq C$, then $f(a) \in C$ for all $a \in A$, so one can clearly define $f_1 : A \to C$ by $f_1(a) = f(a)$. f_1 is readily seen to be a homomorphism. Conversely, if $f_1 : A \to C$ and $f_1(a) = f(a)$ for all a, then $f(a) \in C$, so that $f(A) \subseteq C$.

(2) Suppose $f_1' : A \to C$ is also a homomorphism satisfying $f = \iota f_1'$. Then $\iota f_1 = \iota f_1'$. Since ι is injective, $f_1 = f_1'$ follows, and f_1 is unique.

(3) Since $f_1(a) = f(a)$ for all $a \in A$, $f_1(a) = f_1(b)$ if and only if $f(a) = f(b)$. So if either one of these statements implies $a = b$, the other does. Furthermore, f_1 is injective if and only if f is.

(4) Note that $f_1(A) = f(A)$, because the maps agree on every element of A. Since f_1 is surjective if and only if its image $f_1(A)$ is equal to its codomain C, this statement follows. ■

An important special case of Theorem 1.5 is when f is injective and $f(A) = C$. In that case, the map f_1 is injective and surjective, so that it is an isomorphism. This gives us

COROLLARY 1.6 *If $f : A \to B$ is an injective homomorphism, then $A \cong f(A)$.*

One can think of an injective homomorphism as an embedding for that reason.

Homomorphisms play an important role in many aspects. There are many ways to think of their structure, one of which is in Exercise 3.

EXERCISES

1. Let B be a subalgebra of A and $\iota : B \to A$ the map defined by $\iota(b) = b$ for all $b \in B$. Show that ι is an injective homomorphism of Ω-algebras.

2. If A is an Ω-algebra and $d : A \to A \times A$ is defined by $d(a) = (a, a)$ for all $a \in A$, show that d is an injective homomorphism. [d is called the **diagonal map** on A.] Conclude that $A \cong \{(a, a) \mid a \in A\}$.

3. An **automorphism** of an Ω-algebra A is an isomorphism from A to A. Show that the set Aut A of all automorphisms of A is a group under the operation of function composition. *Remark*: This holds even if A is itself a group. [*Hint*: Follow the paragraph after the proof of Theorem 1.4.]

4. Let G be a group and X a set. A **group action** of G on X is said to be a map $\cdot : G \times X \to X$ satisfying $ab \cdot x = a \cdot (b \cdot x)$ and $e \cdot x = x$ for all $a, b \in G$, $x \in X$. If A is an Ω-algebra, verify that Aut A acts on A given by $\sigma \cdot a = \sigma(a)$.

5. Let A be an Ω-algebra and $T(\Omega)$ be the one-element algebra $\{\epsilon\}$ given by Exercise 9 of Section 1. Prove that there is exactly one homomorphism $A \to T(\Omega)$.

6. (a) Show that the product $A \times B$ seen in Section 1 is isomorphic to that in Section 2.

   (b) Show that $A^S \cong \prod_{s \in S} A$.

7. (a) If $A \cong B$ and $C \cong D$, prove that $A \times C \cong B \times D$.

   Then prove the following statements for Ω-algebras A, B, C:

   (b) $(A \times B) \times C \cong A \times (B \times C)$

   (c) $A \times B \cong B \times A$

   (d) $T(\Omega) \times A \cong A$

8. (a) If $f : A \to B$ is a homomorphism and A_1 is a subalgebra of A, prove that $f(A_1) = \{f(a) \mid a \in A_1\}$ is a subalgebra of B.

   (b) Now suppose B_1 is a subalgebra of B. Show that $f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}$ is a subalgebra of A.

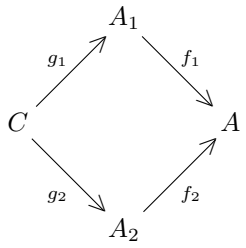
9. (a) If $f : A \to B$ and $g : A \to B$ are homomorphisms, show that $\{a \in A \mid f(a) = g(a)\}$ is a subalgebra of A.

   (b) Let $X \subseteq A$ such that $\langle X \rangle = A$. If $f : A \to B$ and $g : A \to B$ are homomorphisms with $f|X = g|X$, prove that $f = g$. Thus, a homomorphism of A is completely determined by its action on generators of A.

10. Let A_1, A_2 and A be Ω-algebras and $f_1 : A_1 \to A$ and $f_2 : A_2 \to A$ homomorphisms. Define $C = \{(a_1, a_2) \in A_1 \times A_2 \mid f_1(a_1) = f_2(a_2)\}$.

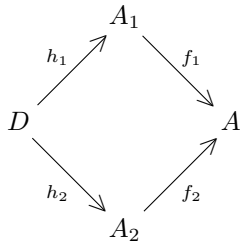
    (a) Show that C is a subalgebra of $A_1 \times A_2$.

(b) Define $g_1 : C \to A_1$ by $g_1(a_1, a_2) = a_1$ and $g_2 : C \to A_2$ by $g_2(a_1, a_2) = a_2$. Show that g_1 and g_2 are homomorphisms, and that $f_1 g_1 = f_2 g_2$; that is, the diagram



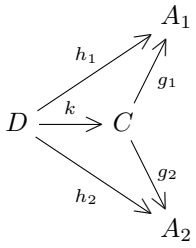
is commutative.

(c) Suppose D is an Ω-algebra and $h_1 : D \to A_1$ and $h_2 : D \to A_2$ are homomorphisms such that



is commutative. Define $k : D \to A_1 \times A_2$ by $k(d) = (h_1(d), h_2(d))$. Show that $k(D) \subseteq C$. Conclude that k can be surjectified to a homomorphism $D \to C$.

(d) Show that k is the unique homomorphism $D \to C$ such that the triangles in



are commutative.

The algebra C and the maps g_1 and g_2 from C are said to be a **pullback** of the maps f_1 and f_2.

1.4 - Congruence Relations

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Congruence relations are the seed to quotient algebras. To understand them, we first need a notion of relations [as mathematical objects]. If A is a set, then a **relation** on A hereby refers to a subset of $A \times A$. If $\Phi \subseteq A \times A$ and $a, b \in A$, one can write $a\Phi b$ if $(a, b) \in \Phi$.

Recall that a relation Φ is an *equivalence relation* if for all $a, b, c \in A$:
$a\Phi a$ [reflexivity];
$a\Phi b \implies b\Phi a$ [symmetry];
$a\Phi b, b\Phi c \implies a\Phi c$ [transitivity].

In this case, if $\overline{a}$ is the equivalence class $\{b \in A \mid b\Phi a\}$, then $\overline{a} = \overline{b}$ if $a\Phi b$, otherwise $\overline{a} \cap \overline{b} = \emptyset$. A congruence relation is even stronger than an equivalence relation. If you apply an n-ary operator to equivalence classes, you should get one equivalence class without any dependence of the operand representatives. This motivates the following definition.

DEFINITION

*A **congruence relation** [or **congruence**] on an Ω-algebra A is an equivalence relation on A which is a subalgebra of $A \times A$.*

This definition may appear to be confusing. How does one view a relation Φ as a subalgebra of $A \times A$? Well, recall that it's constructed as a subset of $A \times A$. So the definition says that whenever $n \geq 0$, $\omega \in \Omega(n)$ and $(a_1, b_1), (a_2, b_2), \ldots (a_n, b_n) \in A \times A$, we have $(\omega(a_1, b_1)(a_2, b_2) \ldots (a_n, b_n)) = ((\omega a_1 a_2 \ldots a_n), (\omega b_1 b_2 \ldots b_n)) \in A \times A$. Stated otherwise, if $a_i \Phi b_i$ for $1 \leq i \leq n$, then $(\omega a_1 a_2 \ldots a_n)\Phi(\omega b_1 b_2 \ldots b_n)$.

Notice that if $n = 0$, the previous statement says $(\omega_A)\Phi(\omega_A)$. However, that is an immediate consequence of reflexivity, so nullary operators need not be regarded in a congruence relation. Stated otherwise,

An equivalence relation Φ on an Ω-algebra A is a congruence relation if and only if whenever $n \geq 1$, $\omega \in \Omega(n)$, $a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n \in A$ and $a_i \Phi b_i$ for each $i = 1, 2, \ldots, n$, then $(\omega a_1 a_2 \ldots a_n)\Phi(\omega b_1 b_2 \ldots b_n)$.

The equivalence classes of a congruence relation are usually called **congruence classes**.

EXAMPLES

1. The identity relation/diagonal $1_A = \{(a, a) \mid a \in A\}$ is a congruence relation on A because if $a_i = b_i$ for all i, clearly $(\omega a_1 a_2 \ldots a_n) = (\omega b_1 b_2 \ldots b_n)$. The full relation $A \times A$ is also a congruence relation.

2. If Φ is a congruence relation on A and B is a subalgebra of A, then $\Phi \cap (B \times B)$ is a congruence relation on B, called the **restriction of Φ to B**.

3. If A and B are Ω-algebras, define a relation A^* by $(a_1, b_1)A^*(a_2, b_2)$ if $b_1 = b_2$. A^* is seen to be a congruence relation.

4. In general, let Φ be a congruence relation on B. Then define Φ^* by $(a_1, b_1)\Phi^*(a_2, b_2)$ if $b_1 \Phi b_2$. Φ^* is a congruence relation; the last example was a special case with $\Phi = 1_B$.

If you didn't learn about congruence relations in earlier abstract algebra lessons, that's probably because they're usually associated with special kinds of subsets. In universal algebra, however, they are relations at best, so I would recommend you read this section to get the hang of them.

EXAMPLES

1. If Φ is a congruence relation on a group G, then the congruence class $N = \{a \in G \mid a\Phi e\}$ is a normal subgroup of G. Conversely, if N is a normal subgroup, the relation $\{(a, b) \mid ab^{-1} \in N\}$ is a congruence relation. This is seen to be a one-to-one correspondence. So normal subgroups are used for congruence in a group, rather than congruence relations as previously defined.

2. Let R be a fixed ring and M a left R-module. If Φ is a congruence relation on M [ex. $a\Phi b$ implies $ka\Phi kb$ for all $k \in R$], then $N = \{a \in M \mid a\Phi 0\}$ is a submodule; and if N is a submodule then $\{(a, b) \mid a - b \in N\}$ is a congruence relation on M. Again, this is a one-to-one correspondence. So congruence relations in a module are identified with submodules.

3. If Φ is a congruence relation on a ring R, the set $I = \{a \in R \mid a\Phi 0\}$ is an ideal, and every ideal I results in a congruence relation $\{(a, b) \mid a - b \in I\}$. This is a one-to-one correspondence. Congruence relations in a ring are viewed as ideals.

4. Let Φ be a congruence relation on a Boolean algebra B. Then $F = \{a \in B \mid a\Phi 1\}$ is a filter in B. Conversely, whenever F is a filter in B, the relation $\{(a, b) \mid a \vee b' \in F \text{ and } a' \vee b \in F\}$ is the corresponding congruence. The Boolean algebra's congruence relation is thus a filter.

We recall that the subalgebras of A form a complete lattice under inclusion. The same is true for congruence relations. As subsets of $A \times A$, one would already know the notion of inclusion and intersection of relations: If Θ and Φ are congruence relations, then $\Theta \subseteq \Phi$ if and only if whenever $a\Theta b$ for $a, b \in A$, then $a\Phi b$. If $\{\Phi_\alpha\}$ are congruence relations, then $\cap\Phi_\alpha$ is the relation $a \sim b$ that $a\Phi_\alpha b$ for every α. According to the following theorem, $\cap\Phi_\alpha$ is indeed a congruence.

THEOREM 1.7 *If A is an Ω-algebra, then Con A — the set of congruence relations on A — is a complete lattice under inclusion.*

Proof of Theorem 1.7. Con A is clearly a poset under inclusion, with largest element $A \times A$ and smallest element 1_A. Now suppose $\{\Phi_\alpha\}$ are congruence relations on A; we claim that $\cap\Phi_\alpha$ is a congruence relation. In that case, we can apply Lemma 1.1 and conclude that Con A is a complete lattice.

Since every Φ_α is a subalgebra of $A \times A$, so is the intersection $\cap\Phi_\alpha$ by Exercise 2 of Section 2. We need only show that $\cap\Phi_\alpha$ is an equivalence relation on A. It is clear that for $a \in A$, (a, a) is in every Φ_α, hence in the intersection, so that $\cap\Phi_\alpha$ is reflexive. If $(a, b) \in \cap\Phi_\alpha$, then $(a, b) \in \Phi_\alpha$ for every α. Since each Φ_α is symmetric it contains (b, a), which is thus in $\cap\Phi_\alpha$. This proves symmetry. Finally, if $(a, b), (b, c) \in \cap\Phi_\alpha$, then each Φ_α contains (a, b) and (b, c), hence (a, c) by transitivity. Therefore, $(a, c) \in \cap\Phi_\alpha$, and $\cap\Phi_\alpha$ is transitive, hence an equivalence relation. ■

And now, very pertinent in many studies is a congruence relation generated by a set. As in the case of subalgebras, if $X \subseteq A \times A$, $[X]$ is the intersection of all congruence relations on A containing X. [At least one exists, namely $A \times A$.]

THEOREM 1.8 *Let A be an Ω-algebra and X be a subset of a $A \times A$. Then:*
(1) *$[X]$ is a congruence relation on A containing X.*
(2) *Whenever Φ is a congruence relation on A containing X, $[X] \subseteq \Phi$.*
(3) *$[X]$ is the only congruence relation on A with properties (1) and (2).*

Proof of Theorem 1.8. Copy the proof of Theorem 1.3, translating $\langle X \rangle$ to $[X]$, subalgebras of A to congruence relations on A, Exercise 2 of Section 2 to Theorem 1.7, and B to Φ. ■

If Θ and Φ are congruence relations on A, then $\Theta \cup \Phi$ need not be a congruence relation. However, by Theorem 1.7, Θ and Φ do have a least upper bound $\Theta \vee \Phi$.

Also, the correspondence between normal subgroups of a group and congruence relations actually preserves the lattice structure; if N and M are normal subgroups, $N \subseteq M$ if and only if congruence mod N is contained in congruence mod M. Same for ideals and rings, etc.

EXERCISES

From this point on, words like "show that" and "prove that" are omitted for simplification. If an exercise is in the form of a statement, you are supposed to prove it.

1. (a) If $f : A \to B$ is a homomorphism of Ω-algebras and $\Theta = \{(a, b) \in A \times A \mid f(a) = f(b)\}$, then Θ is a congruence relation on A.

   (b) If Φ is a congruence relation on B and $f : A \to B$ is a homomorphism, $\Theta = \{(a, b) \in A \times A \mid f(a)\Phi f(b)\}$ is a congruence relation on A.

2. If Φ is a congruence relation on A and B is a subalgebra of A, then B is said to be **Φ-invariant** provided that whenever $a \in B$ and $a\Phi b$, then $b \in B$.

   (a) If $\{A_\alpha\}$ is a family of Φ-invariant subalgebras of A, the intersection $\cap A_\alpha$ is Φ-invariant.

   (b) A is Φ-invariant for every congruence relation Φ on A.

   (c) Every subalgebra of A is 1_A-invariant.

3. (a) If R is a ring, I an ideal in R and S a subring of R, let Φ be the congruence relation associated with I. Then S is Φ-invariant if and only if $I \subseteq S$.

   (b) State an analogous result for groups.

4. If Φ is a congruence relation on A and B is a subalgebra of A, define $B\Phi = \{a \in A \mid a\Phi b \text{ for some } b \in B\}$.

   (a) $B\Phi$ is the smallest Φ-invariant subalgebra of A containing B.

   (b) B is Φ-invariant if and only if $B\Phi = B$.

   (c) If Φ_1 and Φ_2 are congruences on A, then $B(\Phi_1 \cap \Phi_2) \subseteq B\Phi_1 \cap B\Phi_2$.

   (d) Show by example that $B(\Phi_1 \cap \Phi_2) = B\Phi_1 \cap B\Phi_2$ may not hold.

   (e) If B_1 and B_2 are subalgebras of A, then $(B_1 \cap B_2)\Phi \subseteq B_1\Phi \cap B_2\Phi$.

   (f) Show by example that $(B_1 \cap B_2)\Phi = B_1\Phi \cap B_2\Phi$ may not hold.

5. (a) If Φ is a congruence relation on A and $\{\epsilon\}$ a one-element subalgebra of A, then $\overline{\epsilon} = \{a \in A \mid a\Phi\epsilon\}$ is a subalgebra of A. Conclude that if A has a one-element subalgebra, each congruence relation has a subalgebra of A as a congruence class.

   (b) Show by example that Φ need not be determined by $\overline{\epsilon}$.

6. (a) If G is a group, N a normal subgroup and K any subgroup, let Φ be the congruence relation associated with N. Then $K\Phi$ is the subgroup $NK = \{nk \mid n \in N, k \in K\}$.

   (b) $N \cap K$ is a normal subgroup of K, which corresponds to the congruence relation $\Phi \cap (K \times K)$ on K.

   (c) State an analogous result for rings.

7. If Θ and Φ are congruence relations on A, then $[\Theta \cup \Phi]$ is the least upper bound of Θ and Φ in the lattice of congruence relations.

8. An **ideal** in a Lie algebra L over a field F is a subalgebra I such that whenever $a \in I$ and $l \in L$, then $[a : l] \in I$ and $[l : a] \in I$. [Note that the statement $[l : a] \in I$ is superfluous because $[l : a] = -[a : l]$.] Show that there is a bijection between the ideals in L and the congruence relations on L, preserving the lattice structure.

1.5 - Quotient Algebras and Homomorphisms

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Let Φ be a congruence relation on an Ω-algebra A. Our goal is to show that the set A/Φ of congruence classes is actually an Ω-algebra.

If $a \in A$, the congruence class with a is denoted $\overline{a}_\Phi$, or $\overline{a}$ if Φ is clearly under discussion. Thus $\overline{a} = \overline{b}$ if and only if $a\Phi b$. For each $\omega \in \Omega(0)$, we take $(\omega_{A/\Phi}) = \overline{(\omega_A)}$. Now suppose $n \geq 1$ and $\omega \in \Omega(n)$. Then define ω as follows:

$$(\omega\overline{a}_1\overline{a}_2 \dots \overline{a}_n) = \overline{(\omega a_1 a_2 \dots a_n)}$$

for $a_1, a_2, \dots a_n \in A$. We need to know that ω is well-defined on A/Φ [its result does not depend on the representatives used for the operands in A/Φ]. However, this follows from the fact that Φ is a congruence relation, thus a subalgebra of $A \times A$. So if $\overline{b}_i = \overline{a}_i$ for $i = 1, 2, \dots n$, then $\overline{(\omega a_1 a_2 \dots a_n)} = \overline{(\omega b_1 b_2 \dots b_n)}$.

Section 9 shows that all identities that hold for A also hold for A/Φ. Right now, we think of A as a set equipped with operations without any identities required. It is called the **quotient algebra of A given by Φ**.

NOTE You should take the time to verify that if Ω-algebras are groups, and N is the normal subgroup in G corresponding to the congruence relation Φ, then the quotient group G/N is the same as G/Φ just defined. Same for R-modules and submodules; rings and ideals; and Boolean algebras and filters.

The definition of A/Φ may appear to resemble a homomorphism. Well, it does. If Φ is a congruence relation on A, define $\pi : A \to A/\Phi$ by $\pi(a) = \overline{a}$ for all $a \in A$. Then π is a homomorphism:

$$\pi(\omega a_1 a_2 \dots a_n) = \overline{(\omega a_1 a_2 \dots a_n)} = (\omega\overline{a}_1\overline{a}_2 \dots \overline{a}_n) = (\omega\pi(a_1)\pi(a_2)\dots\pi(a_n))$$

and is clearly surjective, because every element of A/Φ can be represented by an element of A. π is called the **canonical epimorphism [natural homomorphism] of A into A/Φ**. Notice that $a\Phi b$ in A if and only if $\overline{a} = \overline{b}$ in A/Φ, that is, $\pi(a) = \pi(b)$. This leads to the following definition.

DEFINITION *If $f : A \to B$ is a homomorphism of Ω-algebras, the **kernel** of f is defined to be the relation $\{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$.*

It is clear that f is injective if and only if its kernel is 1_A. The kernel informally measures how far f is from being injective.

Take another look at the canonical epimorphism $\pi : A \to A/\Phi$. What is its kernel? Well, (a, b) is in the kernel of π if and only if $\pi(a) = \pi(b)$, which is true if and only if $a\Phi b$, as we saw before the definition. So the kernel of π is Φ. This means that every congruence relation on A is the kernel of some homomorphism from A. Conversely, a kernel is always a congruence relation:

THEOREM 1.9 *If $f : A \to B$ is a homomorphism of Ω-algebras, then the kernel Θ of f is a congruence relation on A.*

Notice that if $f : G \to H$ is a homomorphism of groups, its kernel [as a relation] corresponds to the normal subgroup $N = \{a \in G \mid f(a) = e\}$, which is also called its kernel.

Proof of Theorem 1.9. Θ is obviously an equivalence relation on A. Now suppose $\omega \in \Omega(n)$ and $a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n \in A$ with $a_i \Theta b_i$ for $1 \leq i \leq n$. Then $f(a_i) = f(b_i)$ for all i, and hence,

$$f(\omega a_1 a_2 \ldots a_n) = (\omega f(a_1) f(a_2) \ldots f(a_n)) = (\omega f(b_1) f(b_2) \ldots f(b_n)) = f(\omega b_1 b_2 \ldots b_n)$$

therefore, $(\omega a_1 a_2 \ldots a_n) \Theta (\omega b_1 b_2 \ldots b_n)$, and Θ is a congruence relation. ■

An Ω-algebra B is said to be a **homomorphic image** of an Ω-algebra A if there exists a surjective homomorphism $A \to B$. The canonical epimorphism shows that A/Φ is a homomorphic image of A, for every congruence relation Φ. To see that every homomorphic image actually looks like one of those, we develop the dual of Theorem 1.5, where injectivity and surjectivity are exchanged.

THEOREM 1.10 (INJECTIFICATION) *Let $f : A \to B$ be a homomorphism of Ω-algebras and Φ a congruence relation on A. If $\pi : A \to A/\Phi$ is the canonical epimorphism, then:*

(1) *There exists a homomorphism $\overline{f} : A/\Phi \to B$ such that $f = \overline{f}\pi$ [in other words, that $\overline{f}(\overline{a}) = f(a)$ for all $a \in A$] if and only if $\Phi \subseteq \ker f$.*

If the equivalent conditions in (1) hold, then

(2) *$\overline{f}$ is unique;*

(3) *$\overline{f}$ is injective if and only if $\Phi = \ker f$;*

(4) *$\overline{f}$ is surjective if and only if f is surjective.*

Here's the idea: $\ker f$ tells how much information is lost through f. By changing the domain to A/Φ, some of the information ends up never existing in the first place. (4) shows that surjectivity is not affected, and (3) shows that injectivity comes from dividing the domain by the whole kernel.

Proof of Theorem 1.10. (1) Suppose $\Phi \subseteq \ker f$. Now define $\overline{f} : A/\Phi \to B$ by $\overline{f}(\overline{a}) = f(a)$. This map is well-defined because $\Phi \subseteq \ker f$, and hence, if $\overline{a} = \overline{b}$ in A/Φ, then $f(a) = f(b)$. $\overline{f}$ is a homomorphism because

$$\overline{f}(\omega \overline{a}_1 \overline{a}_2 \ldots \overline{a}_n) = \overline{f}(\overline{\omega a_1 a_2 \ldots a_n}) = f(\omega a_1 a_2 \ldots a_n)$$

$$= (\omega f(a_1) f(a_2) \ldots f(a_n)) = (\omega \overline{f}(\overline{a}_1) \overline{f}(\overline{a}_2) \ldots \overline{f}(\overline{a}_n))$$

for $\omega \in \Omega(n)$ and $a_1, a_2, \ldots a_n \in A$. Also, $f(a) = \overline{f}(\overline{a}) = \overline{f}\pi(a)$, so that $f = \overline{f}\pi$. Conversely, if $\overline{f} : A/\Phi \to B$ is a homomorphism such that $f = \overline{f}\pi$, then whenever $a \Phi b$, $\pi(a) = \pi(b)$, so that $f(a) = \overline{f}\pi(a) = \overline{f}\pi(b) = f(b)$ and $(a, b) \in \ker f$. Thus $\Phi \subseteq \ker f$.

(2) Suppose $\overline{f}' : A/\Phi \to B$ is also a homomorphism satisfying $f = \overline{f}'\pi$. Then $\overline{f}\pi = \overline{f}'\pi$. Since π is surjective, $\overline{f} = \overline{f}'$ follows, and $\overline{f}$ is unique.

(3) Suppose $\overline{f}$ is injective. We already know that $\Phi \subseteq \ker f$, so let $(a, b) \in \ker f$, and we show that $a\Phi b$. Well, $f(a) = f(b)$ by definition. Hence, $\overline{f}\pi(a) = \overline{f}\pi(b)$, so that $\pi(a) = \pi(b)$ since $\overline{f}$ is injective. This implies $a\Phi b$. Hence $\ker f \subseteq \Phi$ and $\Phi = \ker f$. Conversely, if $\Phi = \ker f$ and $\overline{f}(\overline{a}) = \overline{f}(\overline{b})$, then $f(a) = \overline{f}\pi(a) = \overline{f}\pi(b) = f(b)$. Thus $(a, b) \in \ker f$, which is Φ, by hypothesis, hence $a\Phi b$ and $\overline{a} = \overline{b}$. Therefore $\overline{f}$ is injective.

(4) For each $b \in B$, there exists $a \in A$ such that $f(a) = b$ if and only if there exists $a \in A$ such that $\overline{f}(\overline{a}) = b$, that is, if there exists $\overline{a} \in A/\Phi$ such that $\overline{f}(\overline{a}) = b$. So the images of f and $\overline{f}$ are the same subalgebra of B, and of course, one is surjective if and only if the other is. ■

If f is surjective and $\Phi = \ker f$, then the map $\overline{f}$ given by Theorem 1.10 is injective and surjective, so that it is an isomorphism. Hence:

COROLLARY 1.11 (FIRST ISOMORPHISM THEOREM) *If $f : A \to B$ is a surjective homomorphism with kernel Θ, then $A/\Theta \cong B$.*

Thus every homomorphic image of A is actually isomorphic to A/Θ, for some congruence relation Θ.

Note that the identity map $1_A : A \to A$ is surjective with kernel 1_A. [It should not be ambiguous when 1_A refers to the identity map, and when it refers to the identity relation.] By the First Isomorphism Theorem, $A/1_A \cong A$ follows.

What is $A/(A \times A)$, on the other hand? If $A = \emptyset$, this quotient is empty, of course. Now suppose $A \neq \emptyset$. Since $A \times A$ is the relation that holds for all pairs of elements of A, there is a single congruence class in $A/(A \times A)$. It follows that $A/(A \times A) \cong T(\Omega)$.

Subalgebras and Quotient Algebras of Quotient Algebras

What can be said about subalgebras of A/Φ? Let C be a subalgebra of A/Φ and $B = \{a \in A \mid \overline{a} \in C\}$ be the union of the congruence classes in C. It is clear that B is a Φ-invariant subalgebra of A. Now define $f : B \to C$ by $f(a) = \overline{a}$. For each $\overline{a} \in C$, $a \in B$ by definition and $\overline{a} = f(a)$ so f is surjective. Clearly f is a homomorphism.

What's the kernel of f? Well, $f(a_1) = f(a_2)$ if and only if $\overline{a_1} = \overline{a_2}$, which holds if and only if $a_1\Phi a_2$ in A [because C consists of congruence classes of Φ]. So $f(a_1) = f(a_2)$ for $a_1, a_2 \in B$ if and only if $a_1\Phi a_2$ in A. Furthermore, the kernel of f is $\Phi \cap (B \times B)$ [or $\Phi \cap B^2$], the restriction of Φ to B. By Corollary 1.11, $B/(\Phi \cap B^2) \cong C$. In fact, $B/(\Phi \cap B^2)$ *is* C, because B is Φ-invariant, and hence, $B/(\Phi \cap B^2)$ consists of the congruence classes of Φ contained in B.

So, the subalgebras of A/Φ are of the form $B/(\Phi \cap B^2)$ with B a Φ-invariant subalgebra of A. What can we say about $B/(\Phi \cap B^2)$ if B is *any* subalgebra of A? The idea is to "complete" the half-full congruence classes. Recall that

$B\Phi = \{a \in A \mid a\Phi b \text{ for some } b \in B\}$ is the union of the congruence classes of Φ that meet B. Exercise 4(a) of the last section shows that $B\Phi$ is a Φ-invariant subalgebra of A. Hence, $B\Phi/(\Phi \cap (B\Phi)^2)$ is a subalgebra of A/Φ. Since all we did to $B/(\Phi \cap B^2)$ was add to the congruence classes, we expect the Ω-algebra structure to remain unchanged. This is indeed the case:

THEOREM 1.12 (SECOND ISOMORPHISM THEOREM) *Let B be a subalgebra of A and Φ a congruence relation on A. Then $B/(\Phi \cap B^2)$ is isomorphic to the subalgebra $B\Phi/(\Phi \cap (B\Phi)^2)$ of A/Φ.*

Since $B\Phi$ is Φ-invariant, one could abbreviate $B\Phi/(\Phi \cap (B\Phi)^2)$ as $B\Phi/\Phi$.

Proof of Theorem 1.12. Define $f : B \to B\Phi/(\Phi \cap (B\Phi)^2)$ by $f(b) = \overline{b}_\Phi$. Then clearly f is a homomorphism. Every element of $B\Phi/(\Phi \cap (B\Phi)^2)$ is of the form $\overline{c}_\Phi$ with $c \in B\Phi$. By definition, there exists $b \in B$ with $b\Phi c$, and hence $\overline{c}_\Phi = \overline{b}_\Phi = f(b)$. Therefore, f is surjective.

We claim that $\ker f = \Phi \cap B^2$, so that the statement $B/(\Phi \cap B^2) \cong B\Phi/(\Phi \cap (B\Phi)^2)$ will follow from Corollary 1.11. If $f(a) = f(b)$, then $\overline{a}_\Phi = \overline{b}_\Phi$, and hence, $a\Phi b$. However, a and b must be in B for $f(a)$ and $f(b)$ to exist. Therefore, $(a, b) \in \Phi \cap B^2$. Conversely, if $(a, b) \in \Phi \cap B^2$, then $(a, b) \in \Phi$, so that $\overline{a}_\Phi = \overline{b}_\Phi$ and $f(a) = f(b)$. Therefore, $\ker f = \Phi \cap B^2$. ■

Now to ask about quotient algebras of A/Φ. To do this, suppose Φ and Θ are congruence relations on A with $\Phi \subseteq \Theta$. Then define

$$\Theta/\Phi = \{(\overline{a}_\Phi, \overline{b}_\Phi) \in A/\Phi \times A/\Phi \mid a\Theta b\}$$

Since $\Phi \subseteq \Theta$, it turns out that whether an element of $A/\Phi \times A/\Phi$ is in Θ/Φ doesn't depend on the choice of congruence class representatives. It is also clear that Θ/Φ is a congruence relation on A/Φ. Now consider the map from congruence relations on A containing Φ to congruence relations on A/Φ, sending each Θ containing Φ to the relation Θ/Φ just defined. Exercise 6 shows that this is a bijective map.

Hence, every congruence relation on A/Φ is of the form Θ/Φ. What is the structure of the quotient $(A/\Phi)/(\Theta/\Phi)$? Well, we have basically glued Φ's congruence classes together to result in Θ's, so we should end up with A/Θ. We certainly do, which yields the third isomorphism theorem.

THEOREM 1.13 (THIRD ISOMORPHISM THEOREM) *Let Φ and Θ be congruence relations on A with $\Phi \subseteq \Theta$. Then $(A/\Phi)/(\Theta/\Phi) \cong A/\Theta$.*

Proof of Theorem 1.13. Let $\pi : A \to A/\Theta$ be the canonical epimorphism. Since Θ is the kernel of π and $\Phi \subseteq \Theta$ by hypothesis, π can be injectified to a surjective homomorphism $f : A/\Phi \to A/\Theta$ by Theorem 1.10, sending $\overline{a}_\Phi \to \overline{a}_\Theta$. If $(\overline{a}_\Phi, \overline{b}_\Phi) \in \ker f$, then $\overline{a}_\Theta = \overline{b}_\Theta$, hence $a\Theta b$ which means $(\overline{a}_\Phi, \overline{b}_\Phi) \in \Theta/\Phi$. The converse can be traced easily. Hence, Θ/Φ is the kernel of f, from which it

follows that $(A/\Phi)/(\Theta/\Phi) \cong A/\Theta$ by Corollary 1.11. ■

EXERCISES

In general, all maps in the following exercises are homomorphisms.

1. (a) A is a homomorphic image of A.

   (b) If C is a homomorphic image of B and B is a homomorphic image of A, then C is a homomorphic image of A.

2. Consider $p : A \times B \to A$ given by $p(a, b) = a$. What is the kernel of p?

3. Suppose Θ is a congruence relation on A and Φ a congruence relation on B. Describe the kernel of the map $f : A \times B \to A/\Theta \times B/\Phi$ defined by $f(a, b) = (\overline{a}_\Theta, \overline{b}_\Phi)$.

4. If Φ and Θ are congruence relations on A and $f : A \to A/\Phi \times A/\Theta$ is defined by $f(a) = (\overline{a}_\Theta, \overline{a}_\Phi)$, what is the kernel of f?

5. (a) If $f : A \to B$ has kernel Θ, then for every subalgebra C of B, $f^{-1}(C)$ is Θ-invariant. [A subalgebra of A is said to be **saturated** if it's $(\ker f)$-invariant.]

   (b) If $f : A \to B$ is surjective, there exists a bijection between the subalgebras of B and the saturated subalgebras of A.

   (c) Let $\pi : A \to A/\Phi$ be the canonical epimorphism and B a subalgebra of A. Then $B\Phi = \pi^{-1}(\pi(B))$.

6. (a) Every congruence relation on A/Φ is of the form Θ/Φ, with Θ a congruence relation on A containing Φ. For example, $1_{A/\Phi} = \Phi/\Phi$.

   (b) If $\Theta_1/\Phi = \Theta_2/\Phi$ then $\Theta_1 = \Theta_2$.

   (c) There exists a bijection between the congruence relations on A/Φ and the congruence relations on A containing Φ.

7. If $f : A \to B$ is a homomorphism with kernel Θ and Φ is a congruence relation on A such that $\Phi \subseteq \Theta$, the homomorphism $\overline{f} : A/\Phi \to B$ resulting from injectification [Theorem 1.10] has kernel Θ/Φ.

8. If Θ is a congruence relation on B, then $f^{-1}(\Theta) = \{(a_1, a_2) \in A \times A \mid f(a_1)\Theta f(a_2)\}$ is a congruence relation on A containing the kernel of f.

9. An Ω-algebra A is said to be **simple** if $|A| \geq 2$ and the only congruence relations on A are 1_A and $A \times A$. If A is simple, $|B| \geq 2$ and $f : A \to B$ is a surjective homomorphism, then f is an isomorphism.

10. Let B be a subalgebra of A and Φ a congruence relation on A, such that $B\Phi = A$ and $\Phi \cap (B \times B) = 1_B$. [$B$ and Φ are said to be **complementary** in this case.] Assume $\iota : B \hookrightarrow A$ is the canonical monomorphism, and $\pi : A \to A/\Phi$ is the canonical epimorphism.

(a) Every congruence class of Φ contains exactly one element of B. Stated otherwise, the map $f = \pi\iota : B \to A/\Phi$ is bijective, so it's an isomorphism. Conclude that any two subalgebras of A complementary to Φ are isomorphic.

(b) $g = \iota f^{-1} : A/\Phi \to A$ is a homomorphism such that $\operatorname{im} g = B$ and $\pi g = 1_{A/\Phi}$. [Such a homomorphism g is said to be a **section**.]

(c) If $g : A/\Phi \to A$ is any homomorphism such that $\pi g = 1_{A/\Phi}$, then $\operatorname{im} g$ and Φ are complementary.

(d) $h = f^{-1}\pi : A \to B$ is a homomorphism such that $\ker h = \Phi$ and $h\iota = 1_B$. [Such a homomorphism h is said to be a **retraction**.]

(e) If $h : A \to B$ is any homomorphism such that $h\iota = 1_B$, then B and $\ker h$ are complementary.

(f) Now suppose $e = \iota f^{-1}\pi : A \to A$; show that $e^2 = e$, $\ker e = \Phi$ and $\operatorname{im} e = B$. e is said to be **the projection through the congruence relation Φ onto the subalgebra B**.

(g) If $e : A \to A$ is any homomorphism such that $e^2 = e$, $\operatorname{im} e$ and $\ker e$ are complementary, and e is the projection through $\ker e$ onto $\operatorname{im} e$.

(h) If G is a group, N a normal subgroup of G corresponding to a congruence relation Φ, and K any subgroup, then K and Φ are complementary if and only if $NK = G$ and $N \cap K = \langle e \rangle$ — so that $G = N \rtimes K$. [*Hint*: Use Exercise 6 of Section 4 to translate the definition of complements.]

1.6 - Subdirect Products

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Only section 10 will use this material, and the theorems used will be stated in the section.

The subdirect product cuts down on congruence relations in the strongest way. To illustrate this, let G be a group and N_1, N_2, N_3 be normal subgroups of G such that $N_1 \cap N_2 \cap N_3 = \langle e \rangle$. That last statement shows that no information is lost in all of G/N_1, G/N_2 and G/N_3. But does that mean we can get G back from them somehow?

The answer is yes, but it's not all that algorithmic. Define $f : G \to G/N_1 \times G/N_2 \times G/N_3$ by $f(a) = (N_1a, N_2a, N_3a)$. f is clearly a group homomorphism. Now if $a \in \ker f$, then $f(a) = (N_1e, N_2e, N_3e)$, whence $a \in N_1$, $a \in N_2$ and $a \in N_3$. Therefore $a \in N_1 \cap N_2 \cap N_3 = \langle e \rangle$, and $a = e$, from which it follows that $\ker f = \langle e \rangle$ and f is injective. Hence, *G is isomorphic to a subgroup of $G/N_1 \times G/N_2 \times G/N_3$* [namely, the image of f]. If we can find all subgroups of the direct product, we can get G.

Now we generalize this to universal algebra, with an arbitrary — *possibly infinite* — batch of congruence relations. Let A be an Ω-algebra and $\{\Phi_\alpha\}$ a batch of congruence relations on A such that $\cap\Phi_\alpha = 1_A$. Then there is no information in A that gets lost in all of the A/Φ_α.

Define $f : A \to \Pi A/\Phi_\alpha$ by $f(a)_\alpha = \overline{a}_{\Phi_\alpha}$. Then for $\omega \in \Omega(n)$, $a^1, a^2, \ldots a^n \in A$ and component index α,

$$f(\omega a^1 a^2 \ldots a^n)_\alpha = \overline{(\omega a^1 a^2 \ldots a^n)}_{\Phi_\alpha} = (\omega \overline{a^1}_{\Phi_\alpha} \overline{a^2}_{\Phi_\alpha} \ldots \overline{a^n}_{\Phi_\alpha})$$

$$= (\omega f(a^1)_\alpha f(a^2)_\alpha \ldots f(a^n)_\alpha) = (\omega f(a^1) f(a^2) \ldots f(a^n))_\alpha$$

hence f is a homomorphism. Now suppose $f(a) = f(b)$. Then for every α, $f(a)_\alpha = f(b)_\alpha$, hence $\overline{a}_{\Phi_\alpha} = \overline{b}_{\Phi_\alpha}$ and $a \Phi_\alpha b$. This means (a, b) is in every Φ_α, hence $(a, b) \in \cap\Phi_\alpha = 1_A$ and $a = b$. Therefore, f is injective. Note that if $p_\alpha : \Pi A/\Phi_\alpha \to A/\Phi_\alpha$ is the projection homomorphism $a \to a_\alpha$, then $p_\alpha f$ is the canonical epimorphism $A \to A/\Phi_\alpha$, and is hence surjective. This motivates the following definition.

DEFINITION

*If $\{A_\alpha\}$ is a batch of Ω-algebras, a **subdirect product** of the A_α is an Ω-algebra A along with an injective homomorphism $f : A \to \Pi A_\alpha$ such that for each projection $p_\alpha : \Pi A_\alpha \to A_\alpha$, the map $p_\alpha f$ is surjective.*

You can think of a subdirect product of the A_α's as a subalgebra of the product, such that for each component index α, every element of A_α lies in index α of some element.

As we have seen, if $\cap\Phi_\alpha = 1_A$, A is a subdirect product of the A/Φ_α's. If we aren't given $\cap\Phi_\alpha = 1_A$, then what? This is answered in Exercise 1.

Recall that whenever p is a prime integer and $p = nm$ with n and m integers, then $p = \pm n$ or $p = \pm m$. Subdirect irreducibility is defined similarly:

DEFINITION

An Ω-algebra A is said to be ***subdirectly irreducible*** *provided that $|A| \geq 2$ and whenever A is a subdirect product of $\{A_\alpha\}$ given by $f : A \to \Pi A_\alpha$, there exists a component index α such that $p_\alpha f : A \to A_\alpha$ is an isomorphism.*

Stated otherwise, for each $a \in A_\alpha$, there is exactly one $t \in f(A)$ with $t_\alpha = a$. Hence, A is simply isomorphic to the operand A_α.

Is there an easier way to think about this? When A is a subdirect product of $\{A_\alpha\}$, each A_α is a homomorphic image of A, with the kernels intersecting to 1_A. This fails when you cannot intersect congruence relations of A and result in 1_A, unless one of the operands itself is 1_A.

THEOREM 1.15 *An Ω-algebra A with $|A| \geq 2$ is subdirectly irreducible if and only if the intersection of all nonidentity congruence relations on A is not 1_A.*

Proof of Theorem 1.15. If A is subdirectly irreducible, let $\{\Phi_\alpha\}$ be the set of nonidentity congruence relations on A. We want to show that $\cap\Phi_\alpha \neq 1_A$. If $\cap\Phi_\alpha = 1_A$, define $f : A \to \Pi A/\Phi_\alpha$ by $f(a)_\alpha = \overline{a}_{\Phi_\alpha}$ as before. We have already seen this to be a subdirect product. By subdirect irreducibility, $p_\alpha f : A \to A/\Phi_\alpha$ is an isomorphism for some α. This means that $\ker(p_\alpha f) = 1_A$. But $\ker(p_\alpha f) = \Phi_\alpha$, since $p_\alpha f$ is the canonical epimorphism. Hence $\Phi_\alpha = 1_A$, contrary to $\{\Phi_\alpha\}$ being the set of *nonidentity* congruence relations. Therefore, $\cap\Phi_\alpha \neq 1_A$. Conversely, suppose the intersection of all nonidentity relations on A is not 1_A, and $f : A \to \Pi A_\alpha$ gives a subdirect product. It is clear that the kernel of f, which is 1_A, is the intersection of the kernels of $p_\alpha f$ for every α. Since nonidentity congruence relations never intersect to 1_A, $\ker(p_\alpha f) = 1_A$ for some α. Hence $p_\alpha f : A \to A_\alpha$ is injective, but it is also surjective by definition of a subdirect product, so that it is an isomorphism. Hence, A is subdirectly irreducible. ■

Exercise 4 shows that an Ω-algebra with at least two elements is a subdirect product of subdirectly irreducible algebras.

EXERCISES

1. Let $\{\Phi_\alpha\}$ be any batch of congruence relations on A, and let $\Phi = \cap\Phi_\alpha$. A/Φ is a subdirect product of the A/Φ_α's. [*Hint*: Define $f : A \to \Pi A/\Phi_\alpha$ by $f(a)_\alpha = \overline{a}_{\Phi_\alpha}$ as before. Find the kernel of f and injectify.]

2. (a) Use Theorem 1.15 to show that if $n \geq 2$, the cyclic group $\mathbb{Z}_n$ is subdirectly irreducible if and only if $n = p^k$ with p prime.

   (b) The ring $\mathbb{Z}_n$ is also subdirectly irreducible if and only if $n = p^k$ with p prime.

3. If $\Phi_1 \subseteq \Phi_2 \subseteq \Phi_3 \subseteq \dots$ is an ascending chain of congruence relations on A, the union $\cup\Phi_i$ is a congruence relation. [*Hint*: Exercise 3 of Section 2.]

4. Assume that there is a maximal element in every nonempty poset in which every chain subset has an upper bound. This is **Zorn's Lemma**, but the proof of this requires the Axiom of Choice.

   (a) If $a, b \in A$ with $a \neq b$, then there exists a congruence relation $\Phi_{a,b}$ on A with $(a, b) \notin \Phi_{a,b}$ such that whenever Φ is another congruence relation with $\Phi_{a,b} \subsetneqq \Phi$, $(a, b) \in \Phi$.

   (b) $A/\Phi_{a,b}$ is subdirectly irreducible. [*Hint*: Recall Exercise 6(c) of Section 5. What can be said about nonidentity congruence relations on $A/\Phi_{a,b}$? Use Theorem 1.15.]

   (c) Every Ω-algebra A with $|A| \geq 2$ is a subdirect product of subdirectly irreducible algebras. [*Hint*: Consider $A/\Phi_{a,b}$ for all $a \neq b$ in A.]

1.7 - The Ultraproduct

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

This section is not a prerequisite of any other and may be skipped if desired.

Isn't it saddening that some objects just fail the product? For example, if F and G are fields, the ring product $F \times G$ is *not* a field: $(1, 0)$ is a nonzero element of $F \times G$ which doesn't have an inverse. Thing is, the multiplicative inverse isn't really a unary operator, it's a *partial* unary operator because 0^{-1} is not defined.

That's just an ordinary product all right, it's not meant to preserve much. But what kind of a product would preserve *all* the logic there is? The ultrafilter is what brightens our day at this very moment. Let's just start out with the filter, which was mentioned in Section 4.

A filter in a Boolean algebra B is a nonempty subset F satisfying the following two properties:

(1) Whenever $x \in F$ and $y \in F$, $x \wedge y \in F$;

(2) Whenever $x \in F$ and $x \leq y$ then $y \in F$.

Theoretically, every filter F contains $1 \in B$, but if $0 \in F$ then $F = B$. This bears a similarity to ideals in a ring: every ideal contains 0, but if 1 is in there, it's the whole ring.

LEMMA 1.16 *Let F be a proper filter in a Boolean algebra B. Then F is maximal in the poset of proper filters in B if and only if whenever $a \in B$, either $a \in F$ or $a' \in F$.*

A proper filter satisfying either of the equivalent conditions in Lemma 1.16 is called an **ultrafilter**. Note, by the way, that we can't have *both* a and a' in F, because that would cause $a \wedge a' = 0 \in F$ and $F = B$. Hence an ultrafilter contains a if and only if it doesn't have a'.

Proof of Lemma 1.16. Suppose that F is maximal in the lattice of proper filters and $a \in B$. We want to show that $a \in F$ or $a' \in F$. If $a \in F$, there is nothing to prove. If $a \notin F$, define

$$G = \{x \in B \mid a \wedge u \leq x \text{ for some } u \in F\}.$$

Then G is seen to be a filter in B: $a \wedge u \leq 1$ for all $u \in F$, so $1 \in G$ and G is nonempty. If $x, y \in G$, then there exist $u, v \in F$ such that $a \wedge u \leq x$ and $a \wedge v \leq y$. Furthermore, $u \wedge v \in F$ and $a \wedge u \wedge v \leq a \wedge u \leq x$ and $a \wedge u \wedge v \leq a \wedge v \leq y$, so that $a \wedge u \wedge v \leq x \wedge y$. This means $x \wedge y \in G$. If $x \in G$ and $x \leq y$, then $a \wedge u \leq x$ for some $u \in F$; since $a \wedge u \leq x \leq y$, we have $a \wedge u \leq y$ and $y \in G$. Therefore, G is a filter in B.

Furthermore, $F \subseteq G$, because if $x \in F$, then $a \wedge x \leq x$ so $a \wedge u \leq x$ for some $u \in F$, thus $x \in G$. Also, $a \in G$ because $1 \in F$ and $a \wedge 1 \leq a$, but we are given $a \notin F$. Therefore, $F \neq G$. Since F is maximal we must have $G = B$.

In particular, $0 \in G$, so that $a \wedge u \leq 0$ for some $u \in F$. Since 0 is smallest in B, this basically says that $a \wedge u = 0$; hence, $u \wedge a' = (u \wedge a') \vee 0 = (u \wedge a') \vee (u \wedge a) = u \wedge (a' \vee a) = u \wedge 1 = u$ and $u \leq a'$. Since $u \in F$, $a' \in F$ follows, completing the proof of this implication.

Conversely, if $a \in F$ or $a' \in F$ for all $a \in B$, suppose G is a filter in B with $F \subsetneqq G$. Then there exists $a \in G$ such that $a \notin F$. Since $a \notin F$, $a' \in F$ by hypothesis, hence $a' \in G$. Therefore $a \wedge a' = 0 \in G$ and $G = B$. Thus, F is maximal. ■

For the remainder of this section, we deal with filters in the power set $\mathcal{P}(I)$ [the subsets of I under inclusion] where I is a set of indices. If $\{A_\alpha\}$ is an indexed set of Ω-algebras and F is a filter in $\mathcal{P}(I)$, let Φ be the relation on the product ΠA_α given by

$$a \Phi b \text{ if } \{\alpha \in I \mid a_\alpha = b_\alpha\} \in F.$$

Stated otherwise, a and b are congruent if F "has the set of their shared components." We show that Φ is truly a congruence relation on ΠA_α. For $a \in A$, $\{\alpha \in I \mid a_\alpha = a_\alpha\} = I \in F$, hence, $a \Phi a$ and Φ is reflexive. If $a \Phi b$, then $\{\alpha \in I \mid b_\alpha = a_\alpha\} = \{\alpha \in I \mid a_\alpha = b_\alpha\} \in F$, so $b \Phi a$ easily follows. Now suppose $a \Phi b$ and $b \Phi c$. Then $A_1 = \{\alpha \in I \mid a_\alpha = b_\alpha\}$ and $A_2 = \{\alpha \in I \mid b_\alpha = c_\alpha\}$ are in F. To show that Φ is transitive, we need to show that $A_3 = \{\alpha \in I \mid a_\alpha = c_\alpha\}$ is in F, so that $a \Phi c$. Well, if $\alpha \in A_1 \cap A_2$, then $a_\alpha = b_\alpha = c_\alpha$ and $\alpha \in A_3$. Therefore, $A_1 \cap A_2 \subseteq A_3$. Yet, $A_1 \cap A_2 \in F$ and $A_3 \in F$ follow since F is a filter. Consequently, Φ is an equivalence relation.

Now suppose $\omega \in \Omega(n)$, $a^1, a^2, \ldots a^n, b^1, b^2, \ldots b^n \in \Pi A_\alpha$ and $a^i \Phi b^i$ for every i. Then for each i, form the set $A_i = \{\alpha \in I \mid a^i_\alpha = b^i_\alpha\}$. We are given that F contains all the A_i's, and need to show that F contains $A = \{\alpha \in I \mid (\omega a^1 a^2 \ldots a^n)_\alpha = (\omega b^1 b^2 \ldots b^n)_\alpha\}$. It is seen that $A_1 \cap A_2 \cap \cdots \cap A_n \subseteq A$, by reasoning similar to the last paragraph, from which $A \in F$ follows. Therefore, Φ is indeed a congruence relation on ΠA_α.

The special moment comes from the ultrafilter.

DEFINITION

*Let $\{A_\alpha\}$ be an indexed collection of Ω-algebras with indices in I, and U an ultrafilter in $\mathcal{P}(I)$. If Φ is defined as before [$a \Phi b \iff \{\alpha \in I \mid a_\alpha = b_\alpha\} \in U$], the quotient algebra $(\Pi A_\alpha)/\Phi$ is called an **ultraproduct** of the A_α's.*

Fields fail the product, as previously seen. But they don't fail the ultraproduct — and almost nothing fails this. Let's practice a proof.

THEOREM 1.17 *An ultraproduct of fields is a field.*

Proof of Theorem 1.17. Let $\{A_\alpha\}$ be an indexed collection of fields and $(\Pi A_\alpha)/\Phi$ the ultraproduct of the A_α's involving ultrafilter U. It is clear that $(\Pi A_\alpha)/\Phi$ is a commutative ring, because commutative rings are closed under homomorphic images and products.

Now suppose $\overline{a} \neq \overline{0}$ in $(\Pi A_\alpha)/\Phi$. We show that $\overline{a}\overline{b} = \overline{1}$ for some $\overline{b}$. $\overline{a} \neq \overline{0}$ implies that $\{\alpha \in I \mid a_\alpha = 0\} \notin U$, so its complement, $N = \{\alpha \in I \mid a_\alpha \neq 0\}$ *is* in U. Consider b given by $b_\alpha = a_\alpha^{-1}$ if $a_\alpha \neq 0$, and 0 if $a_\alpha = 0$. Then $(ab)_\alpha = a_\alpha b_\alpha$ is 1 if $a_\alpha \neq 0$ and 0 if $a_\alpha = 0$. We claim that $\overline{a}\overline{b} = \overline{ab} = \overline{1}$; to show this, we see that $\{\alpha \in I \mid (ab)_\alpha = 1\} = \{\alpha \in I \mid a_\alpha \neq 0\} = N \in U$. Therefore, $\overline{a}\overline{b}$ is indeed $\overline{1}$, and $(\Pi A_\alpha)/\Phi$ is a field. ■

An ultraproduct of integral domains is an integral domain by the same token [see Exercise 1]. This can be generalized.

What are examples of filters in $\mathcal{P}(I)$? Well, a lot can be said about them.

EXAMPLES

1. A subset S of I is said to be **cofinite** in I if $I - S$ is finite. It is easily seen that the set $\mathcal{F}$ of cofinite subsets of I is a filter in $\mathcal{P}(I)$. It is not an ultrafilter; for example, if $I = \mathbb{Z}$, $\mathcal{F}$ contains neither the set of even integers, nor its complement, the set of odd integers. $\mathcal{F}$ is called the **Fréchet filter**.

2. If $\sigma \in I$, then the set of subsets of I containing σ is an ultrafilter in $\mathcal{P}(I)$. It is called **the principal ultrafilter given by** σ.

So yeah, a basic example of an ultrafilter is there. However, if U is the principal ultrafilter given by $\sigma \in I$, the ultraproduct $(\Pi A_\alpha)/\Phi$ is either empty or isomorphic to the operand A_σ [Exercise 4]. So of course it satisfies everything all the operands satisfy. So principal ultrafilters don't really produce much. Now, does there exist a nonprincipal ultrafilter? Well, the Fréchet filter $\mathcal{F}$ allows us to answer this.

THEOREM 1.18 *An ultrafilter U in $\mathcal{P}(I)$ is nonprincipal if and only if $\mathcal{F} \subseteq U$.*

Proof of Theorem 1.18. Suppose U is the principal ultrafilter given by $\sigma \in I$. Then the set $I - \{\sigma\}$ is in $\mathcal{F}$ but not in U, hence $\mathcal{F}$ isn't contained in U. Thus if $\mathcal{F} \subseteq U$ then U is nonprincipal [we just proved the contrapositive]. Conversely, suppose $\mathcal{F}$ isn't contained in U; we are to show that U is principal. In this case, there exists $A \in \mathcal{F}$ such that $A \notin U$. Since $A \notin U$ and U is an ultrafilter, the complement $I - A \in U$. Since $A \in \mathcal{F}$, $I - A$ is finite by definition. Hence U contains a finite set. Let n be the smallest positive integer such that U contains a set with n elements. If $n \geq 2$, say $\{\alpha_1, \ldots \alpha_n\} \in U$, then $\{\alpha_1\} \notin U$ [otherwise U would contain a set with fewer than n elements]. Therefore, $I - \{\alpha_1\} \in U$ since U is an ultrafilter. Intersecting this set with $\{\alpha_1, \ldots \alpha_n\}$ yields $\{\alpha_2, \ldots \alpha_n\}$, which is hence a set in U with $n - 1$ elements. This contradicts the hypothesis that n is the smallest integer such that U has a set with n elements. Therefore $n = 1$, hence U contains $\{\sigma\}$ for some $\sigma \in I$, and is easily seen to be the principal ultrafilter given by σ. ■

Therefore, the only question that remains is whether there's an ultrafilter containing $\mathcal{F}$. If I is finite, $\mathcal{F} = \mathcal{P}(I)$ so this is impossible [in other words, every ultrafilter in $\mathcal{P}(I)$ is principal if I is finite!]. So suppose I is infinite. Then

$\mathcal{F}$ doesn't contain $\emptyset$ and is hence proper in $\mathcal{P}(I)$. If we assume the Axiom of Choice, we can use Zorn's Lemma [see Exercise 4 of Section 6] to show that an ultrafilter containing $\mathcal{F}$ [hence nonprincipal] exists.

Let S be the set of proper filters in $\mathcal{P}(I)$ containing $\mathcal{F}$. Assuming I is infinite, $\mathcal{F} \in S$ so that S is nonempty. If $F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$ is a chain of filters containing $\mathcal{F}$, their union is also a filter containing $\mathcal{F}$, and is proper if all the F_i's are [because a filter's proper if and only if it doesn't contain $\emptyset$]. Therefore, every chain in S has an upper bound in S, so S has a maximal element by Zorn's Lemma. Lemma 1.16 shows that this is an ultrafilter in $\mathcal{P}(I)$. And it clearly contains $\mathcal{F}$.

The conclusion is, therefore, that $\mathcal{P}(I)$ has a nonprincipal ultrafilter if and only if I is infinite.

EXERCISES

1. An ultraproduct of integral domains is an integral domain.

2. A monoid M is said to be **cancellative** provided that whenever $a, b, c \in M$ and $ab = ac$ or $ba = ca$, then $b = c$.

   (a) If monoids M and N are cancellative, it so happens that $M \times N$ is cancellative.

   (b) Why doesn't this imply that the product of integral domains is an integral domain?

   (c) A submonoid of a cancellative monoid M is cancellative.

   (d) If M is cancellative and Φ is a congruence relation on M, show by example that M/Φ need not be cancellative.

3. Let U be an ultrafilter in a Boolean algebra B, and $a, b \in B$. Then:

   (a) $a \wedge b \in U$ if and only if $a \in U$ and $b \in U$,

   (b) $a \vee b \in U$ if and only if either a or b is in U.

4. Let $\sigma \in I$ and U the principal ultrafilter in $\mathcal{P}(I)$ given by σ. Assume the A_α's are nonempty Ω-algebras.

   (a) The kernel of the projection homomorphism $p_\sigma : \Pi A_\alpha \to A_\sigma$ is the congruence relation Φ on ΠA_α given by the U in the definition of the ultraproduct.

   (b) In conclusion, the ultraproduct $(\Pi A_\alpha)/\Phi$ is isomorphic to A_σ.

5. An ultrafilter U in $\mathcal{P}(I)$ is principal if and only if the intersection of a [possibly infinite] batch of sets in U is in U.

1.8 - Ω-expressions and Free Ω-algebras

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Have you ever attempted to treat a job fairly, and not regard any rules? If so, you'd realize how tough it is. Well, that's one of the many important concepts when it comes to universal algebra.

The free algebra will bring light to many of the future lessons. It takes symbols and shells them with operators, disregarding what they could possibly mean. Having done so, the symbols can map to any elements of a particular Ω-algebra, and this gives rise to a homomorphism.

First, we define Ω-expressions on a set X. We also add a notion of *length* so the expressions stay finite.

DEFINITION

If X is a set and Ω a universal algebra template, an **Ω-expression in** *X is recursively defined as follows.*

1. If α is an element of X, then α is an Ω-expression in X with length 1.

2. If $\omega \in \Omega(n)$ and $\alpha_1, \alpha_2, \ldots \alpha_n$ are Ω-expressions with lengths $k_1, k_2, \ldots k_n$ respectively, the expression $(\omega\alpha_1\alpha_2 \ldots \alpha_n)$ is an Ω-expression whose length is $1 + k_1 + k_2 + \cdots + k_n$.

In particular, if $\omega \in \Omega(0)$, (ω) is an Ω-expression with length 1.

For example, if s and p are the sum and product in a ring, $(px(syz))$ is an Ω-expression in $\{x, y, z\}$ of length 5; whereas $(s(pxy)(pxz))$ — which is supposed to be the same thing — is an Ω-expression of length 7.

We let $F(\Omega, X)$ be the set of Ω-expressions in X, and define its Ω-algebra structure as follows: if $\omega \in \Omega(n)$ and $\alpha_1, \alpha_2, \ldots \alpha_n \in F(\Omega, X)$, then $(\omega\alpha_1\alpha_2 \ldots \alpha_n)$ is the element of $F(\Omega, X)$ given by part 2 of the definition. We then define $i : X \to F(\Omega, X)$ mapping each element of X to itself as an Ω-expression [part 1 of the definition]. $F(\Omega, X)$ is called the **free Ω-algebra** given by X.

The first important thing to realize is this: let $A = \langle i(X) \rangle \subseteq F(\Omega, X)$. We show that $A = F(\Omega, X)$. For each $a \in F(\Omega, X)$, we induct on the length of a to show that $a \in A$. If a has length 1, it is either an element of X or a nullary operator (ω), and in either case $a \in A$, because A is generated by the set $i(X)$ of elements of X seen as Ω-expressions, and it contains all nullary operators due to being a subalgebra. Now suppose a has length $n \geq 2$ and every expression with length $< n$ is in A. Then $a = (\omega a_1 a_2 \ldots a_k)$ with $\omega \in \Omega(k)$. Each a_i has length less than that of a, hence is in A by the inductive hypothesis. Since A is a subalgebra, $a \in A$ follows. Hence,

The free algebra $F(\Omega, X)$ is generated by the set $i(X)$ of symbols in X.

Now suppose that A is an Ω-algebra and $f : X \to A$ a set map. Define $f_1 : F(\Omega, X) \to A$ by assigning expressions in increasing order of length: map $x \in X$ to $f(x)$, and $(\omega a_1 a_2 \ldots a_n)$ to $(\omega f_1(a_1) f_1(a_2) \ldots f_1(a_n))$ [Once

you get to $(\omega a_1 a_2 \dots a_n)$, the $f_1(a_i)$'s already exist]. Then $f_1(\omega a_1 a_2 \dots a_n) = (\omega f_1(a_1) f_1(a_2) \dots f_1(a_n))$ is immediate from the definition, and $f_1 i = f$, because for each $x \in X$, $f_1 i(x)$ is f_1's assignment of the expression x, which is $f(x)$.

It is also seen that f_1 is uniquely determined by being a homomorphism $F(\Omega, X) \to A$ satisfying $f_1 i = f$, since $i(X)$ generates $F(\Omega, X)$; hence if $f_1' : F(\Omega, X) \to A$ is also a homomorphism satisfying $f_1' i = f$, then $f_1(x) = f_1'(x)$ for all $x \in i(X)$, hence $f_1 = f_1'$ by Exercise 10(b) of Section 3. This illustrates the following definition.

DEFINITION

Let $\mathcal{C}$ be a class of Ω-algebras. If X is a set, $F \in \mathcal{C}$ and $i : X \to F$ is a set map, (F, i) is said to constitute ***a free algebra for $\mathcal{C}$ given by*** *X provided that whenever $A \in \mathcal{C}$ and $f : X \to A$ is a set map, there is a unique homomorphism $f_1 : F \to A$ such that $f_1 i = f$.*

In particular, we have just seen that $F(\Omega, X)$ along with i is a free algebra for all Ω-algebras given by X. It is in fact the only one, as the following theorem shows.

THEOREM 1.19 *Let $\mathcal{C}$ be a class of Ω-algebras. Assume (F, i) constitutes a free algebra given by a set X, and (F', i') constitutes a free algebra given by a set X'. If $|X| = |X'|$ then $F \cong F'$.*

Basically, if there's a free algebra given by a set with a given cardinality, it is unique up to isomorphism.

Proof of Theorem 1.19. Let $\sigma : X \to X'$ be the bijection which is hypothesized to exist. Consider the map $i'\sigma : X \to F'$; since F is free given by X, there is a homomorphism $f : F \to F'$ satisfying $fi = i'\sigma$. Now reverse the roles and consider $i\sigma^{-1} : X' \to F$: since F' is free given by X', there is a homomorphism $f' : F' \to F$ satisfying $f'i' = i\sigma^{-1}$. The map $f'f : F \to F$ satisfies $f'fi = f'i'\sigma = i\sigma^{-1}\sigma = i1_X = i$. Since F is free, however, 1_F is the *unique* homomorphism $F \to F$ satisfying $1_F i = i$. Therefore, $f'f = 1_F$ by uniqueness. By the same argument, $ff' = 1_{F'}$. Hence, f and f' are isomorphisms which are inverses of each other, and $F \cong F'$. ■

EXERCISES

1. Let $\mathcal{C}$ be a class of Ω-algebras, X a set, and $F \in \mathcal{C}$ with $i : X \to F$ a free algebra for $\mathcal{C}$ given by X.

   (a) If any subalgebra of an algebra in $\mathcal{C}$ is in $\mathcal{C}$, then $i(X) \subseteq F$ generates F. [*Hint*: Let $A = \langle i(X) \rangle \subseteq F$. The map $X \to A$ sending $x \to i(x)$ extends to a homomorphism $\lambda : F \to A$ sending $i(x) \to i(x)$, since F is free. But there's also the canonical monomorphism $\iota : A \hookrightarrow F$. What can you say about $\iota\lambda : F \to F$?]

   (b) If $\mathcal{C}$ contains an algebra with at least two elements, then i is injective.

2. Let $I(\Omega) = F(\Omega, \emptyset)$.

   (a) For each Ω-algebra A, there is exactly one homomorphism $I(\Omega) \to A$. [$I(\Omega)$ is called the **initial Ω-algebra**.]

   (b) $I(\Omega) \neq \emptyset$ if and only if $\Omega(0) \neq \emptyset$.

3. The relation in $F(\Omega, X)$ of having the same length is a congruence relation.

4. If $X' \subseteq X$, then the subalgebra $\langle i(X') \rangle$ of $F(\Omega, X)$ is isomorphic to $F(\Omega, X')$.

5. Describe the congruence relation on $F(\Omega, X)$ generated by $\{(i(x), i(y)) \mid x, y \in X\}$. If $X \neq \emptyset$, what is the quotient algebra?

6. Let Φ be an equivalence relation on the set X and Φ_1 the congruence relation on $F(\Omega, X)$ generated by $\{(i(x), i(y)) \mid x \Phi y \text{ in } X\}$. Then $F(\Omega, X)/\Phi_1 \cong F(\Omega, X/\Phi)$. [*Hint*: Consider the map $X \to F(\Omega, X/\Phi)$ sending each $x \in X$ to $\overline{x}_\Phi$ as an expression in the free algebra. Then extend its domain, and injectify.]

7. In the class of pointed sets, the free algebra given by a set X is the set $X \uplus \{x_0\}$ with base point x_0. Conclude that every pointed set is actually free.

8. In the class of all sets, what's the free algebra given by a set X?

9. If X is a set and $f : X \to A$ a set map, then the resulting extension $F(\Omega, X) \to A$ has image $\langle f(X) \rangle \subseteq A$.

10. An element $a \in A$ is said to be **derivable** from $X \subseteq A$ provided that there exists an Ω-expression in X which evaluates to a in A. Show that $\langle X \rangle$ is the set of elements of A derivable from X. [*Hint*: Exercise 9.]

1.9 - Varieties and Coproducts

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

We finally have enough tools to deal with the presence of identities! Recall that an identity indicates what expressions in variables must be equal for all substitutions. Expressions are, though, elements of $F(\Omega, X)$, which leads to the following definition.

DEFINITION

*A pair $(w_1, w_2) \in F(\Omega, X)^2$ is called an **identity** for Ω. An Ω-algebra A is said to **satisfy** the identity (w_1, w_2) if $f(w_1) = f(w_2)$ for every homomorphism $f : F(\Omega, X) \to A$.*

For the rest of this chapter, we let X_0 be the countably infinite set $\{x_0, x_1, x_2, \dots\}$. For example, suppose Ω has a single binary operation [written multiplicatively] and A is an Ω-algebra. Then $((x_0x_1)x_2, x_0(x_1x_2))$ is an identity. What does it mean to say that A satisfies that identity? Well, suppose that for every homomorphism $f : F(\Omega, X_0) \to A$, $f((x_0x_1)x_2) = f(x_0(x_1x_2))$. This says $(f(x_0)f(x_1))f(x_2) = f(x_0)(f(x_1)f(x_2))$ for every homomorphism $f : F(\Omega, X_0) \to A$. Since there exists a homomorphism $F(\Omega, X_0) \to A$ with any given action on the $x_0, x_1, \dots$, it turns out that $(ab)c = a(bc)$ for *all* $a, b, c \in A$. The argument can be traced both ways. Hence, A satisfies $((x_0x_1)x_2, x_0(x_1x_2))$ if and only if $(ab)c = a(bc)$ for all $a, b, c \in A$. It all makes sense! An identity (w_1, w_2) can sometimes be referred to as $w_1 = w_2$.

This rigorates the definition of a monoid: suppose $\Omega(0) = \{1\}$ and $\Omega(2) = \{p\}$. Then an Ω-algebra A is a monoid if and only if it satisfies the identities:

1. $((p(px_0x_1)x_2), (px_0(px_1x_2)))$ [associativity];
2. $((p(1)x_0), x_0)$ [left identity];
3. $((px_0(1)), x_0)$ [right identity].

These can be rewritten as follows: $(x_0x_1)x_2 = x_0(x_1x_2)$, $1x_0 = x_0$, $x_01 = x_0$.

To generalize the idea, suppose $S \subseteq F(\Omega, X_0)^2$ is a set of identities. Let $\mathcal{V}(S)$ be the class of all Ω-algebras satisfying every identity in S. Then $\mathcal{V}(S)$ is called a **variety**. For example, the groups form a variety, as do the rings [Exercises 1 and 2]. $\mathcal{V}(S)$ has some interesting closure properties, as we now see. If $X' \subseteq X$, recall how $F(\Omega, X')$ is a subalgebra of $F(\Omega, X)$ from Exercise 4 of Section 8.

LEMMA 1.20 (1) *For each $w \in F(\Omega, X)$, there exists a finite subset X' of X such that $w \in F(\Omega, X')$.*

(2) *If $w_1, w_2 \in F(\Omega, X)$, there exists a finite subset X' of X such that $F(\Omega, X')$ contains both w_1 and w_2.*

Be careful: (1) does *not* imply that there's a finite subset $X' \subseteq X$ such that $F(\Omega, X') = F(\Omega, X)$! It says that each $w \in F(\Omega, X)$ is in $F(\Omega, X')$ for some finite subset X' of X. The finite subsets, no matter how chosen, are widely

different depending on which $w \in F(\Omega, X)$ we deal with. You can picture the theorem in one sentence: *expressions and identities are finite.* They only use finitely many symbols, due to the notion of length.

Proof of Lemma 1.20. (1) Let A be the set of $w \in F(\Omega, X)$ with the property stated in (1). We claim that $A = F(\Omega, X)$. To show this, we show that A is a subalgebra of $F(\Omega, X)$ containing $i(X)$. Each $i(x) \in i(X)$ is in $F(\Omega, \{x\})$ and $\{x\}$ is a finite subset of X, so every element of $i(X)$ satisfies the property and $i(X) \subseteq A$. If $\omega \in \Omega(0)$, then $(\omega) \in F(\Omega, \emptyset)$ [because it's in every subalgebra of $F(\Omega, X)$] and $\emptyset$ is finite, so $(\omega) \in A$. Now suppose $n \geq 1$, $\omega \in \Omega(n)$ and $a_1, a_2, \ldots a_n \in A$. Then there are finite subsets $X_1, X_2, \ldots X_n \subseteq X$ such that $a_i \in F(\Omega, X_i)$ for every i. The union $U = X_1 \cup X_2 \cup \cdots \cup X_n$ is a finite subset of X and $a_i \in F(\Omega, U)$ for every i. Hence, $(\omega a_1 a_2 \ldots a_n) \in F(\Omega, U)$, which means $(\omega a_1 a_2 \ldots a_n)$ satisfies the property and is in A. Hence, A is a subalgebra of $F(\Omega, X)$ containing $i(X)$, and is therefore $F(\Omega, X)$ since the algebra is generated by $i(X)$.

(2) If $w_1, w_2 \in F(\Omega, X)$, there exist finite subsets $X_1, X_2 \subseteq X$ with $w_i \in F(\Omega, X_i)$ for $i = 1, 2$ by part (1). $X_1 \cup X_2$ is a finite subset of X and $F(\Omega, X_1 \cup X_2)$ contains both w_1 and w_2. ■

THEOREM 1.21 (1) $\mathcal{V}(S)$ *contains the terminal algebra* $T(\Omega)$.

(2) *If* $A \in \mathcal{V}(S)$, *every subalgebra of* A *is in* $\mathcal{V}(S)$.

(3) *If* $A \in \mathcal{V}(S)$, *every homomorphic image of* A *is in* $\mathcal{V}(S)$.

(4) *If* $\{A_\alpha\}$ *is a batch of [not necessarily distinct] algebras in* $\mathcal{V}(S)$, *the product* $\Pi A_\alpha \in \mathcal{V}(S)$.

Note that if $A \cong B$, the isomorphism $A \to B$ is surjective, and hence, B is a homomorphic image of A. So part (3) implies that every isomorphic copy of an algebra in $\mathcal{V}(S)$ is in $\mathcal{V}(S)$ — and you don't need to worry over relabeling elements of an algebra.

Also, the fields do *not* form a variety. For one thing, property (4) fails: the product of fields is not a field.

Proof of Theorem 1.21. (1) There is only one homomorphism $f : F(\Omega, X_0) \to T(\Omega)$ and it maps every expression to the unique element of $T(\Omega)$. Hence, $f(w_1) = f(w_2)$ for every $(w_1, w_2) \in S$, and $T(\Omega) \in \mathcal{V}(S)$.

(2) Suppose B is a subalgebra of A, $f : F(\Omega, X_0) \to B$ is a homomorphism and $(w_1, w_2) \in S$. If $\iota : B \hookrightarrow A$ is the canonical monomorphism, $\iota f : F(\Omega, X_0) \to A$ is a homomorphism, hence $\iota f(w_1) = \iota f(w_2)$ since $A \in \mathcal{V}(S)$. Therefore, $f(w_1) = f(w_2)$ since ι is injective. Consequently, $B \in \mathcal{V}(S)$.

(3) Let $\eta : A \to B$ be the surjective homomorphism which is hypothesized to exist, $f : F(\Omega, X_0) \to B$ a homomorphism and $(w_1, w_2) \in S$. By Lemma 1.20(2), there exists a finite set $X' \subseteq X_0$ such that $F(\Omega, X')$ contains w_1 and w_2. For each $x_k \in X'$, choose $a_k \in A$ so that $\eta(a_k) = f(x_k)$ [since η is surjective, this is possible; and no Axiom of Choice is needed since X' is finite]. Pick one random element of A [what does this proof become if $A = \emptyset$?] to be

a_k whenever $x_k \in X_0 - X'$. The map $x_k \to a_k$ from X_0 to A extends to a homomorphism $g : F(\Omega, X) \to A$. We know that $f(x_k) = \eta g(x_k)$ for all $x_k \in i(X')$, because $\eta g(x_k) = \eta(a_k) = f(x_k)$. Hence $f(w) = \eta g(w)$ for all $w \in F(\Omega, X')$ by Exercise 10(a) of Section 3. In particular, $f(w_1) = \eta g(w_1)$ and $f(w_2) = \eta g(w_2)$. But $g(w_1) = g(w_2)$, since $A \in \mathcal{V}(S)$, therefore, applying η to both sides, $f(w_1) = f(w_2)$. Therefore, B satisfies all identities in S and hence is in $\mathcal{V}(S)$.

(4) Suppose $f : F(\Omega, X_0) \to \Pi A_\alpha$ is a homomorphism and $(w_1, w_2) \in S$. For each α, recall the projection $p_\alpha : \Pi A_\alpha \to A_\alpha$ and consider $p_\alpha f : F(\Omega, X_0) \to A_\alpha$. Since $A_\alpha \in \mathcal{V}(S)$, $p_\alpha f(w_1) = p_\alpha f(w_2)$. Hence, $f(w_1)_\alpha = f(w_2)_\alpha$ for all indices α, so that $f(w_1) = f(w_2)$. It follows that $\Pi A_\alpha \in \mathcal{V}(S)$. ■

Do you realize what we've done? We've just given a general proof that applies to monoids, groups, rings, lattices, Boolean algebras, R-modules for a fixed ring R, and so much more! Don't get overpumped; next chapter will be even better!

You probably asked whether free algebras exist in $\mathcal{V}(S)$. They certainly do, and we take the following approach to find them. If X is a set, define $\Phi(X, S)$ to be the congruence relation on $F(\Omega, X)$ generated by the set

$$\{(\varphi(w_1), \varphi(w_2)) \mid (w_1, w_2) \in S, \varphi \text{ a homomorphism } F(\Omega, X_0) \to F(\Omega, X)\}$$

Note that we took all *images* of the identities. For example, the distributive law $a(b + c) = ab + ac$ in a ring, after substituting into b the expression $x + yz$, yields $a((x + yz) + c) = a(x + yz) + ac$, and that must hold in a ring. By closing the relation into a congruence, we also regarded complicated results like $1x + (ab)c = x + a(bc)$.

Now put $F_S(\Omega, X) = F(\Omega, X)/\Phi(X, S)$. We show:

THEOREM 1.22 *The Ω-algebra $F_S(\Omega, X)$ along with the map $j : X \to F_S(\Omega, X)$ sending $x \to \overline{x}$ is a free algebra for $\mathcal{V}(S)$ given by X.*

Proof of Theorem 1.22. First we show that $F_S(\Omega, X) \in \mathcal{V}(S)$. Suppose $f : F(\Omega, X_0) \to F_S(\Omega, X)$ is a homomorphism and $(w_1, w_2) \in S$. X has a finite subset X' such that $w_1, w_2 \in F(\Omega, X')$ by Lemma 1.20(2). For each $x_k \in X'$, choose $a_k \in F(\Omega, X)$ so that $\overline{a_k} = f(x_k)$. Pick one random element of $F(\Omega, X)$ to be a_k for each $x_k \in X_0 - X'$. The map $x_k \to a_k$ from X_0 to $F(\Omega, X)$ extends to a homomorphism $g : F(\Omega, X_0) \to F(\Omega, X)$. Notice that if $\pi : F(\Omega, X) \to F_S(\Omega, X)$ is the canonical epimorphism, $f(x_k) = \pi g(x_k)$ for $x_k \in X'$, and hence, $f(w_1) = \pi g(w_1)$ and $f(w_2) = \pi g(w_2)$ by Exercise 10(a) of Section 3. However, $(g(w_1), g(w_2)) \in \Phi(X, S)$ by definition, whence $\pi g(w_1) = \pi g(w_2)$, since $\Phi(X, S)$ is the kernel of π. Furthermore, $f(w_1) = f(w_2)$, so that $F_S(\Omega, X) \in \mathcal{V}(S)$.

Now let $A \in \mathcal{V}(S)$ and $f : X \to A$ a set map. This yields an Ω-algebra homomorphism $f_1 : F(\Omega, X) \to A$ such that $f_1 j = f$. We claim that $\Phi(X, S) \subseteq \ker f_1$: to show this, we need only show that $(\varphi(w_1), \varphi(w_2)) \in \ker f_1$ whenever $(w_1, w_2) \in S$ and $\varphi : F(\Omega, X_0) \to F(\Omega, X)$ is a homomorphism. This is because $\Phi(X, S)$ is generated by the pairs of that form, hence *any* congruence relation

containing them — in particular, $\ker f_1$ — contains $\Phi(X, S)$. The claim follows from $f_1\varphi$ being a homomorphism $F(\Omega, X_0) \to A$; hence $f_1\varphi(w_1) = f_1\varphi(w_2)$ since $(w_1, w_2) \in S$ and $A \in \mathcal{V}(S)$. Thus $(\varphi(w_1), \varphi(w_2))$ is in the kernel of f_1. Therefore, $\Phi(X, S) \subseteq \ker f_1$.

By Theorem 1.10, there is a homomorphism $\overline{f}_1 : F_S(\Omega, X) \to A$ such that $\overline{f}_1\pi = f_1$ with π the canonical epimorphism. Also, notice that $j = \pi i$. Hence $\overline{f}_1 j = \overline{f}_1\pi i = f_1 i = f$.

Now suppose $\overline{f}'_1 : F_S(\Omega, X) \to A$ is also a homomorphism satisfying $\overline{f}'_1 j = f$. Put $f'_1 = \overline{f}'_1\pi$. Then $f'_1 i = \overline{f}'_1\pi i = \overline{f}'_1 j = f$. But f_1 is the *unique* homomorphism $F(\Omega, X) \to A$ such that $f_1 j = f$, so we must have $f_1 = f'_1$. Hence $\overline{f}_1\pi = \overline{f}'_1\pi$. Since π is surjective, $\overline{f}_1 = \overline{f}'_1$ follows, and $\overline{f}'_1$ is unique. ■

EXAMPLE

The free group given by X_0 consists of strings made up of elements of X_0 and their formal inverses. For example, $x_1x_3^{-1}x_0x_2x_0^{-1}$ is in the free group; however, $x_2x_2^{-1}$ simplifies to e.

We have shown that if $\{A_\alpha\}$ is a family of $\mathcal{V}(S)$ algebras, then $A = \Pi A_\alpha \in \mathcal{V}(S)$. If $p_\alpha : A \to A_\alpha$ is defined by $p_\alpha(a) = a_\alpha$, recall that the following holds [see Section 3]:

Whenever $f_\alpha : B \to A_\alpha$ is a homomorphism for each α, there is a unique homomorphism $f : B \to \Pi A_\alpha$ such that $f_\alpha = p_\alpha f$ for all α.

The coproduct comes from reversing the arrows. It can be seen to combine algebras together, and can always be found due to the existence of free algebras.

DEFINITION

*If $\{A_\alpha\}$ is a batch of $\mathcal{V}(S)$ algebras, a **coproduct** [or **sum**] of the A_α's is defined to be an algebra $A \in \mathcal{V}(S)$ along with homomorphisms $i_\alpha : A_\alpha \to A$ such that whenever $B \in \mathcal{V}(S)$ and $f_\alpha : A_\alpha \to B$ for each α, there is a unique homomorphism $f : A \to B$ such that $fi_\alpha = f_\alpha$ for all α. The i_α are called **injection maps**.*

EXAMPLES

1. Coproducts in the variety of sets are disjoint unions, because any two maps $A \to C, B \to C$ combine to a unique map $A \uplus B \to C$.

2. If the $\{A_\alpha\}$ are R-modules, then their coproduct [normally called their direct sum] is the set ΣA_α of $a \in \Pi A_\alpha$ such that $a_\alpha \neq 0$ for finitely many α's. The injection map $i_\alpha : A_\alpha \to \Sigma A_\alpha$ is defined by $i_\alpha(a)_\alpha = a$, $i_\alpha(a)_\beta = 0$ when $\beta \neq \alpha$.

3. Exercise 14 shows that a coproduct of groups is a free product. If the G_α are groups, every nonidentity element of $\coprod G_\alpha$ can be written uniquely in the form $x_1x_2 \ldots x_n$ where each $x_i \in G_\alpha$ for some α, $x_i \neq e$ and x_i, x_{i+1} are never in the same operand group.

LEMMA 1.23 *Every $\mathcal{V}(S)$ algebra is a homomorphic image of a free $\mathcal{V}(S)$ algebra.*

Proof of Lemma 1.23. If A is a $\mathcal{V}(S)$ algebra, the identity map $A \to A$ [where the domain is regarded as a set] extends to a homomorphism $f : F_S(\Omega, A) \to A$ satisfying $f(\overline{x}) = x$ for all $x \in A$. Each $a \in A$ is equal to $f(\overline{a})$, so f is surjective. Hence, A is a homomorphic image of $F_S(\Omega, A)$. ■

THEOREM 1.24 *Any $\mathcal{V}(S)$ algebras have a coproduct in $\mathcal{V}(S)$, which is unique up to isomorphism.*

The proof yields a legitimate recipe for finding coproducts in $\mathcal{V}(S)$. However, this recipe is deferred to Section 2.4, because it [sadly] makes this section too long.

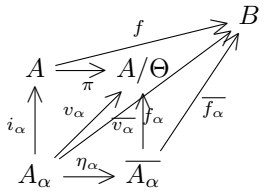
Proof of Theorem 1.24. We claim that $\mathcal{V}(S)$ algebras which possess coproducts include all free algebras and are closed under homomorphic images. Then since every algebra is a homomorphic image of a free algebra by Lemma 1.23, it will follow that all algebras have coproducts.

First suppose A is a coproduct of the A_α given by homomorphisms $i_\alpha : A_\alpha \to A$ and for each α, $\eta_\alpha : A_\alpha \to \overline{A_\alpha}$ is a surjective homomorphism. Now let $\Theta_\alpha = \ker \eta_\alpha$, $i_\alpha\Theta_\alpha = \{(i_\alpha(a), i_\alpha(b)) \mid (a, b) \in \Theta_\alpha\}$ and Θ the congruence relation on A generated by $\bigcup i_\alpha\Theta_\alpha$. [This constitutes our first trick!] We claim that A/Θ is a coproduct of the $\overline{A_\alpha}$.

Let π be the canonical epimorphism $A \to A/\Theta$ and $v_\alpha = \pi i_\alpha : A_\alpha \to A/\Theta$. We claim that $\Theta_\alpha \subseteq \ker v_\alpha$. To show this, suppose $(a, b) \in \Theta_\alpha$. Then $(i_\alpha(a), i_\alpha(b)) \in i_\alpha\Theta_\alpha \subseteq \Theta$. Hence, $\pi i_\alpha(a) = \pi i_\alpha(b)$ by definition of π, and $v_\alpha(a) = v_\alpha(b)$, which means that $(a, b) \in \ker v_\alpha$. Therefore, there is a unique homomorphism $\overline{v_\alpha} : \overline{A_\alpha} \to A/\Theta$ such that $v_\alpha = \overline{v_\alpha}\eta_\alpha$.

So we have a homomorphism from each $\overline{A_\alpha}$ to A/Θ. Now suppose $B \in \mathcal{V}(S)$ and $\overline{f_\alpha} : \overline{A_\alpha} \to B$ are homomorphisms. Let $f_\alpha = \overline{f_\alpha}\eta_\alpha : A_\alpha \to B$. Then since A is a coproduct of the A_α's, there is a unique homomorphism $f : A \to B$ such that $f_\alpha = fi_\alpha$ for all α.

The statements $v_\alpha = \pi i_\alpha, v_\alpha = \overline{v_\alpha}\eta_\alpha, f_\alpha = \overline{f_\alpha}\eta_\alpha, f_\alpha = fi_\alpha$ are organized in the following commutative diagram.



We claim that $\Theta \subseteq \ker f$: since Θ is *generated* by $\bigcup i_\alpha\Theta_\alpha$, we need only show that $i_\alpha\Theta_\alpha \subseteq f$ for every α to prove our claim. Whenever $(a', b') \in i_\alpha\Theta_\alpha$, there exists $(a, b) \in \Theta_\alpha$ such that $a' = i_\alpha(a)$ and $b' = i_\alpha(b)$. Furthermore,

$\eta_\alpha(a) = \eta_\alpha(b)$ so that $f(a') = fi_\alpha(a) = f_\alpha(a) = \overline{f_\alpha}\eta_\alpha(a) = \overline{f_\alpha}\eta_\alpha(b) = f_\alpha(b) = fi_\alpha(b) = f(b')$, and $(a', b') \in \ker f$. Therefore, $\Theta \subseteq \ker f$.

Consequently, f injectifies to a homomorphism $\overline{f} : A/\Theta \to B$ such that $f = \overline{f}\pi$, where π is the canonical epimorphism $A \to A/\Theta$. We also have $\overline{f}\,\overline{v_\alpha} = \overline{f_\alpha}$ because $\overline{f}\,\overline{v_\alpha}\eta_\alpha = \overline{f}v_\alpha = \overline{f}\pi i_\alpha = fi_\alpha = f_\alpha = \overline{f_\alpha}\eta_\alpha$, and η_α can be cancelled off the right due to surjectivity.

To show that $\overline{f}$ is unique, suppose $\overline{f}' : A/\Theta \to B$ also satisfies $\overline{f}'\,\overline{v_\alpha} = \overline{f_\alpha}$. Then $f' = \overline{f}'\pi$ satisfies $f'i_\alpha = \overline{f}'\pi i_\alpha = \overline{f}'v_\alpha = \overline{f}'\,\overline{v_\alpha}\eta_\alpha = \overline{f_\alpha}\eta_\alpha = f_\alpha$. Since f is the *unique* homomorphism $A \to B$ such that $fi_\alpha = f_\alpha$, we must have $f = f'$. Therefore, $\overline{f}\pi = \overline{f}'\pi$, hence $\overline{f} = \overline{f}'$ since π is surjective. Therefore, $\overline{f}$ is unique, and A/Θ is a coproduct of the $\overline{A_\alpha}$'s.

Now we show that free $\mathcal{V}(S)$ algebras have a coproduct. Let X_α be sets and $A_\alpha = F_S(\Omega, X_\alpha)$. Now let $X = \biguplus X_\alpha$ and we show that $A = F_S(\Omega, X)$ is a coproduct of the A_α's, with $i_\alpha : A_\alpha \to A$ mapping each element of X_α to the corresponding element of X.

Suppose B is an Ω-algebra and $f_\alpha : A_\alpha \to B$ for each α. Define $\overline{f} : X \to B$ mapping each $x \in X_\alpha$ to $f_\alpha(x)$. Then since $A = F_S(\Omega, X)$, there is a unique $f : A \to B$ such that $\overline{f} = f|X$. $f_\alpha = fi_\alpha$ for each α follows from $f_\alpha|X_\alpha = fi_\alpha|X_\alpha$, and $f|X$ is uniquely determined by this property, making f unique. This concludes the proof of the coproduct's existence.

The uniqueness of the coproduct is similar to Theorem 1.19 and is left to the reader. ■

EXERCISES

1. If $\Omega(0) = \{e\}$, $\Omega(1) = \{i\}$, $\Omega(2) = \{p\}$ and

   $$S = \{((p(px_0x_1)x_2), (px_0(px_1x_2))), ((p(e)x_0), x_0), ((p(ix_0)x_0), (e))\}$$

   then $\mathcal{V}(S)$ is the class of groups. [*Hint*: Exercise 4(a) of Section 1.]

2. Suppose $\Omega(0) = \{0, 1\}$, $\Omega(1) = \{n\}$, $\Omega(2) = \{s, p\}$ and S consists of the following pairs:

   $((s(sx_0x_1)x_2), (sx_0(sx_1x_2)))$
   $((sx_0x_1), (sx_1x_0))$
   $((s(0)x_0), x_0)$
   $((sx_0(nx_0)), (0))$
   $((p(px_0x_1)x_2), (px_0(px_1x_2)))$
   $((px_0(sx_1x_2)), (s(px_0x_1)(px_0x_2)))$
   $((p(sx_0x_1)x_2), (s(px_0x_2)(px_1x_2)))$
   $((p(1)x_0), x_0)$
   $((px_0(1)), x_0)$

   (a) Rewrite the operators and identities so they are easier to read.

   (b) Convince yourself that $\mathcal{V}(S)$ is the class of rings.

3. Express the class of rings with involution as a variety.

4. There are no axioms for the pointed set — it's just a set with a nullary operator. Does this prevent the pointed sets from being a variety?

5. The free monoid given by a set X consists of the strings made up of elements of X, including the empty string. For example, if $X = X_0$, one of the elements is $x_1x_4x_2x_2x_5x_1$.

6. (a) The commutative monoids form a variety.

   (b) Describe the free commutative monoid given by a set.

7. Every element of the free ring given by a set X is a formal sum of strings made up of elements of X and their formal negatives. For example, $x_1x_3 - x_2 + x_4x_6x_4$ is in the free ring given by X_0; and $(x_1 + x_4)(x_2x_3 + x_2)$ can be changed to $x_1x_2x_3 + x_4x_2x_3 + x_1x_2 + x_4x_2$ so it doesn't have parentheses.

8. If M is a fixed monoid, the free M-action given by a set X is $M \times X$ given by $m(a, x) = (ma, x)$ for $m, a \in M, x \in X$, and $i : X \to M \times X$ sending $x \to (1, x)$.

9. Let $X' = \{x_1, x_2, \ldots x_n\}$ and $v_1, v_2, \ldots v_k, w_1, w_2, \ldots w_k$ be expressions in X'. Then

$$A = \langle x_1, x_2, \ldots x_n \mid v_1 = w_1, v_2 = w_2, \ldots, v_k = w_k \rangle$$

   is defined to be the result of taking the free $\mathcal{V}(S)$ algebra given by X', and then dividing out the congruence relation generated by the (v_j, w_j)'s. [This is usually done in the variety of groups.] If B is a $\mathcal{V}(S)$ algebra, show that a map $f : X' \to B$ extends to a homomorphism $A \to B$ if and only if substituting each x_i for $f(x_i)$ in any statement $v_j = w_j$ yields a true statement in B.

10. Let $I_S(\Omega) = F_S(\Omega, \emptyset)$. $I_S(\Omega)$ is called the **initial algebra for the variety** $\mathcal{V}(S)$.

    (a) $I_S(\Omega)$ is nonempty if and only if Ω contains a nullary operator.

    (b) If $\mathcal{V}(S)$ is the class of rings, $I_S(\Omega) \cong \mathbb{Z}$. [*Hint*: Exercise 7.]

    (c) For each $A \in \mathcal{V}(S)$, there is exactly one homomorphism $I_S(\Omega) \to A$, and its image is the smallest subalgebra of A.

    (d) A $\mathcal{V}(S)$ algebra is a homomorphic image of $I_S(\Omega)$ if and only if it has no subalgebra except itself.

11. Assume $A \coprod B$ denotes a coproduct of A and B in $\mathcal{V}(S)$.

    (a) If $A \cong C$ and $B \cong D$, then $A \coprod C \cong B \coprod D$

    (b) $(A \coprod B) \coprod C \cong A \coprod (B \coprod C)$

    (c) $A \coprod B \cong B \coprod A$

    (d) $I_S(\Omega) \coprod A \cong A$

12. If $S \subseteq T \subseteq F(\Omega, X_0)$, every Ω-algebra in $\mathcal{V}(T)$ is in $\mathcal{V}(S)$. [$\mathcal{V}(T)$ is said to be a **subvariety** of $\mathcal{V}(S)$ in this case.]

13. Suppose $\mathcal{V}(S)$ is a variety in which $I_S(\Omega) \cong T(\Omega)$. Then every $\mathcal{V}(S)$ algebra has a unique one-element subalgebra. Furthermore, for all $A, B \in \mathcal{V}(S)$, there exists a homomorphism $A \to B$. [If the initial algebra is isomorphic to the terminal algebra, it can be called a **zero algebra**.]

14. A coproduct $\coprod A_\alpha$ of $\mathcal{V}(S)$ algebras is said to be a **free product** if every $i_\alpha : A_\alpha \to \coprod A_\alpha$ is injective. If a homomorphism $A_\alpha \to A_\beta$ exists for all α, β, then $\coprod A_\alpha$ is a free product. [*Hint*: For each α, let $f_\beta : A_\beta \to A_\alpha$ be any homomorphisms, subject to the condition that $f_\alpha = 1_{A_\alpha}$. There is a homomorphism $f : \coprod A_\alpha \to A_\alpha$ such that $fi_\beta = f_\beta$ for all β. Use this to show that i_α is injective.]

15. (a) If $\mathcal{V}(S)$ is a variety in which all operators are nullary, when is a $\mathcal{V}(S)$ algebra free?

    (b) If $\mathcal{V}(S)$ is a variety in which all operators are unary, show that $\mathcal{V}(S)$ is the variety of M-actions for some fixed monoid M. Conclude that coproducts in $\mathcal{V}(S)$ are disjoint unions, and subalgebras of a $\mathcal{V}(S)$ algebra include the empty set and are closed under unions.

1.10 - Birkhoff's Theorem

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

An interesting thing about varieties is this: If you use identities to restrict the Ω-algebras in a class, the products and coproducts both exist, but the product stays the same, whereas the coproduct changes. Likewise, the terminal algebra $T(\Omega)$ stays as its 1-element self, but the initial algebra $I_S(\Omega)$ may be different. So we can claim that a variety $\mathcal{V}(S)$ can be closed under products, but "closed under coproducts" doesn't really make sense.

Let's have another look at the variety's properties in Theorem 1.21.

(1) $\mathcal{C}$ contains the terminal algebra $T(\Omega)$.
(2) If $A \in \mathcal{C}$, every subalgebra of A is in $\mathcal{C}$.
(3) If $A \in \mathcal{C}$, every homomorphic image of A is in $\mathcal{C}$.
(4) If $\{A_\alpha\}$ is a batch of [not necessarily distinct] algebras in $\mathcal{C}$, the product $\Pi A_\alpha \in \mathcal{C}$.

Our main goal is to show the converse of Theorem 1.21: every class $\mathcal{C}$ of Ω-algebras satisfying conditions (1)-(4) is a variety. This is known as the **HSP theorem** [homomorphic-image subalgebra product] in universal algebra. Note that (4) states $\mathcal{V}(S)$ is closed under *arbitrary* products — even if there are infinitely many factors. [Otherwise, the theorem would not hold; see Exercise 1.] We bring two statements from Section 6 here for our proof:

Fact 1. A subdirect product of A_α's is isomorphic to a subalgebra of their product. [definition]
Fact 2. If Φ_α's are congruence relations on A and $\Phi = \cap\Phi_\alpha$, then A/Φ is a subdirect product of the A/Φ_α's. [Exercise 1 of Section 6]

Now suppose $\mathcal{C}$ satisfies conditions (1)-(4). To begin with, condition (3) implies that $\mathcal{C}$ is closed under isomorphic copies.

Now let X be a set. If $A \in \mathcal{C}$ is nonempty, there exists a homomorphism $F(\Omega, X) \to A$. Let $\mathrm{Id}(X, A)$ be the intersection of all kernels of homomorphisms $F(\Omega, X) \to A$. Then $\mathrm{Id}(X, A)$ is the congruence relation consisting of the identities satisfied by A. We claim that $F(\Omega, X)/\mathrm{Id}(X, A) \in \mathcal{C}$. This is because for each homomorphism $f : F(\Omega, X) \to A$, surjectification and injectification together show that $F(\Omega, X)/\ker f \cong \mathrm{im}\ f$. $\mathrm{im}\ f$ is a subalgebra of A, hence is in $\mathcal{C}$ by condition (2). By closure under isomorphic copies, $F(\Omega, X)/\ker f \in \mathcal{C}$.

So $\mathcal{C}$ contains $F(\Omega, X)/\ker f$ for every homomorphism $f : F(\Omega, X) \to A$. Since $\mathrm{Id}(X, A)$ is the intersection of these $\ker f$'s, $F(\Omega, X)/\mathrm{Id}(X, A)$ is a subdirect product of the algebras of the form $F(\Omega, X)/\ker f$ by Fact 2. Since a subdirect product of algebras is a subalgebra of the product, conditions (2) and (4) show that $\mathcal{C}$ contains any subdirect product of algebras in $\mathcal{C}$. This is why $F(\Omega, X)/\mathrm{Id}(X, A) \in \mathcal{C}$.

Now let $\mathrm{Id}(X,\mathcal{C}) = \bigcap \mathrm{Id}(X,A)$ where the intersection is taken over all nonempty $A \in \mathcal{C}$ [there is at least one such algebra, namely $T(\Omega)$]. $\mathrm{Id}(X,\mathcal{C})$ is the set of identities satisfied by all algebras in $\mathcal{C}$ and is called the **congruence relation of identities for** $\mathcal{C}$. Since $F(\Omega,X)/\mathrm{Id}(X,A) \in \mathcal{C}$ for all nonempty $A \in \mathcal{C}$, the closure of $\mathcal{C}$ under subdirect products [seen in the previous paragraph] implies $F(\Omega,X)/\mathrm{Id}(X,\mathcal{C}) \in \mathcal{C}$. We claim this:

LEMMA 1.25 *If $\mathcal{C}$ is a class of Ω-algebras satisfying conditions (1)-(4) in Theorem 1.21, and X is a set, $F(\Omega,X)/Id(X,\mathcal{C})$ along with the map $i : X \to F(\Omega,X)/Id(X,\mathcal{C})$ sending $x \to \overline{x}$ is a free algebra for $\mathcal{C}$ given by X.*

Proof of Lemma 1.25. Assume π refers to the canonical epimorphism $F(\Omega,X) \to F(\Omega,X)/\mathrm{Id}(X,\mathcal{C})$, and $j : X \to F(\Omega,X)$ is the usual injection into the free algebra. Then $i = \pi j$.

Let $A \in \mathcal{C}$ and $f : X \to A$ a set map. f extends to a homomorphism $g : F(\Omega,X) \to A$ with $gj = f$. Furthermore, $\mathrm{Id}(X,\mathcal{C}) \subseteq \mathrm{Id}(X,A) \subseteq \ker g$ [since $\mathrm{Id}(X,\mathcal{C})$ is the intersection of the $\mathrm{Id}(X,A)$'s, and similarly for each $\mathrm{Id}(X,A)$], so g can be injectified to $\overline{g} : F(\Omega,X)/\mathrm{Id}(X,\mathcal{C}) \to A$ with $\overline{g}\pi = g$. We see that $\overline{g}i = \overline{g}\pi j = gj = f$.

Now suppose $\overline{g}' : F(\Omega,X)/\mathrm{Id}(X,\mathcal{C}) \to A$ also satisfies $\overline{g}'i = f$. Take $g' = \overline{g}'\pi$; then $g'j = \overline{g}'\pi j = \overline{g}'i = f$. But g is the *unique* homomorphism $F(\Omega,X) \to A$ satisfying $gj = f$ [since $F(\Omega,X)$ is free in the class of all Ω-algebras], hence $g = g'$. Furthermore, $\overline{g}\pi = \overline{g}'\pi$ and $\overline{g} = \overline{g}'$ since π is surjective. Therefore $\overline{g}$ is unique, and $(F(\Omega,X)/\mathrm{Id}(X,\mathcal{C}), i)$ constitutes a free algebra for $\mathcal{C}$ given by X. ■

Now here's our main result!

THEOREM 1.26 (BIRKHOFF'S THEOREM) *A class $\mathcal{C}$ of Ω-algebras is a variety if and only if it satisfies conditions (1)-(4) above.*

Proof of Theorem 1.26. If $\mathcal{C}$ is a variety, it satisfies conditions (1)-(4) by Theorem 1.21. Conversely, suppose $\mathcal{C}$ is a class of Ω-algebras satisfying conditions (1)-(4). Let $S = \mathrm{Id}(X_0,\mathcal{C})$. Then S is the set of identities satisfied by every algebra in $\mathcal{C}$; furthermore, $\mathcal{C}$ is contained in the variety $\mathcal{V}(S)$. We show that $\mathcal{V}(S) \subseteq \mathcal{C}$, so that $\mathcal{C} = \mathcal{V}(S)$ is a variety.

Suppose $A \in \mathcal{V}(S)$. Let $X \subseteq A$ be a set of generators of A. The injection map $X \to A$ extends to a homomorphism $f : F(\Omega,X) \to A$ sending each expression in X to its value in A. Since $X \subseteq \mathrm{im}\, f$ and generates A, f is surjective. We claim that $\mathrm{Id}(X,\mathcal{C}) \subseteq \ker f$: let $(w_1,w_2) \in \mathrm{Id}(X,\mathcal{C})$. By Lemma 1.20(2), X has a finite subset X' such that w_1, w_2 are in $F(\Omega,X')$. Exercise 2 shows that there exist maps $\lambda : X \to X_0$, $\zeta : X_0 \to X$ satisfying $\zeta\lambda(x) = x$ for all $x \in X'$. The map $i\zeta : X_0 \to F(\Omega,X)$ extends to a homomorphism $\zeta_1 : F(\Omega,X_0) \to F(\Omega,X)$ sending $x \in X_0$ to $\zeta(x)$. Likewise, λ extends to a homomorphism $\lambda_1 : F(\Omega,X) \to F(\Omega,X_0)$ sending $x \in X$ to $\lambda(x)$. Furthermore, $\zeta_1\lambda_1(x) = x$ when x is a symbol in $F(\Omega,X)$ from X'. Since those symbols

generate $F(\Omega, X')$, $\zeta_1\lambda_1$ fix all elements of $F(\Omega, X')$, in particular, w_1 and w_2. Thus $\zeta_1\lambda_1(w_1) = w_1$ and $\zeta_1\lambda_1(w_2) = w_2$. Consider $f\zeta_1 : F(\Omega, X_0) \to A$. Since $A \in \mathcal{V}(S)$, $S = \mathrm{Id}(X_0, \mathcal{C})$ is contained in the kernel of $f\zeta_1$, so it can be injectified into a homomorphism $f_1 : F(\Omega, X_0)/\mathrm{Id}(X_0, \mathcal{C}) \to A$ such that $f_1\pi = f\zeta_1$, with π the canonical epimorphism as usual. Since $F(\Omega, X_0)/\mathrm{Id}(X_0, \mathcal{C}) \in \mathcal{C}$ though [by the discussion preceding Lemma 1.25], $\pi\lambda_1 : F(\Omega, X) \to F(\Omega, X_0)/\mathrm{Id}(X_0, \mathcal{C})$ has kernel containing $\mathrm{Id}(X, \mathcal{C})$. In particular, $\pi\lambda_1(w_1) = \pi\lambda_1(w_2)$. Furthermore, $f(w_1) = f\zeta_1\lambda_1(w_1) = f_1\pi\lambda_1(w_1) = f_1\pi\lambda_1(w_2) = f\zeta_1\lambda_1(w_2) = f(w_2)$ and $(w_1, w_2) \in \ker f$. Therefore, $\mathrm{Id}(X, \mathcal{C}) \subseteq \ker f$.

As a consequence, f can be injectified into a homomorphism which maps $F(\Omega, X)/\mathrm{Id}(X, \mathcal{C}) \to A$ by Theorem 1.10, which is surjective because f is. Therefore, A is a homomorphic image of $F(\Omega, X)/\mathrm{Id}(X, \mathcal{C})$. By the discussion preceding Lemma 1.25, $F(\Omega, X)/\mathrm{Id}(X, \mathcal{C}) \in \mathcal{C}$; hence $A \in \mathcal{C}$ by condition (3). Therefore, $\mathcal{C} = \mathcal{V}(S)$. ■

Recall Theorem 1.24: in the variety, coproducts always exist and are unique up to isomorphism. The conclusion is that if conditions (1)-(4) are satisfied, there is a "slight closure" under coproducts: any indexed collection of Ω-algebras in $\mathcal{V}(S)$ have *some coproduct in* $\mathcal{V}(S)$ *unique up to isomorphism*, but it may not be isomorphic to their coproduct in all Ω-algebras.

Likewise, $\mathcal{V}(S)$ contains an initial algebra $I_S(\Omega)$, but it doesn't have the same meaning as $I(\Omega)$. It turns out that since $I_S(\Omega)$ has no subalgebra except itself, it's a homomorphic image of $I(\Omega)$ by Exercise 9(d) of Section 9.

EXERCISES

1. If a class of Ω-algebras satisfies conditions (1)-(3) of a variety and is closed under *finite* products, show by example that it need not be a variety.

2. If $X_0 = \{x_0, x_1, \dots\}$, X is a set and X' a finite subset of X, show without using the Axiom of Choice that there exist maps $\lambda : X \to X_0$, $\zeta : X_0 \to X$ satisfying $\zeta\lambda(x) = x$ for all $x \in X'$.

3. (YONEDA'S THEORY) Let $\mathcal{C}$ be a class of Ω-algebras [which may not be a variety]. For $A, B \in \mathcal{C}$, let $\hom(A, B)$ denote the set of homomorphisms from A to B. Fix $A \in \mathcal{C}$. A **natural transformation** for A is an object η which assigns each $B \in \mathcal{C}$ a map $\eta_B : \hom(A, B) \to B$ satisfying

   $$\eta_{B'}(kf) = k(\eta_B(f))$$

   for all homomorphisms $f : A \to B$, $k : B \to B'$.

   (a) If $\omega \in \Omega(0)$, then $[\omega]$ is a natural transformation for A when defined by $[\omega]_B(f) = (\omega_B)$ whenever $B \in \mathcal{C}, f : A \to B$.

   (b) If $n \geq 1$, $\omega \in \Omega(n)$ and $\eta^1, \eta^2, \dots \eta^n$ are natural transformations for A, then $(\omega\eta^1\eta^2 \dots \eta^n)$ given by

   $$(\omega\eta^1\eta^2 \dots \eta^n)_B(f) = (\omega\eta^1_B(f)\eta^2_B(f) \dots \eta^n_B(f))$$

for $B \in \mathcal{C}, f : A \to B$ is also a natural transformation for A.

We have established an Ω-algebra structure for the set N of natural transformations for A. We show that N is actually isomorphic to A.

(c) If $a \in A$, define $[a]_B(f) = f(a)$ for $B \in \mathcal{C}, f : A \to B$. Then $[a]$ is a natural transformation for A.

(d) The map $\varphi : A \to N$ sending $a \to [a]$ is an isomorphism, whose inverse is the map $\varphi^{-1} : N \to A$ sending $\eta \to \eta_A(1_A)$.

1.11 - Takeoffs and Universals

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

This section is not a prerequisite of any other and may be skipped if desired. It may be referenced later though.

Now that varieties are characterized, one must ask how you can go from one to another. We have briefly discussed extension signatures in the first section, but this section generalizes the idea.

To begin with, every group G is a monoid, because it has an associative binary operation with an identity. That's not all the group needs, but it still has it. The monoid structure on G is part of the group structure, with some details missing. This structure takes off algebraically, in the sense that every group homomorphism of groups is also a monoid homomorphism of the monoids.

Also, every ring R is a rng when you disregard the identity element, and a ring homomorphism of rings is automatically a rng homomorphism. [Note that a rng homomorphism can have rings for the domain and codomain without being a ring homomorphism — take the zero map $\mathbb{Z} \to \mathbb{Z}$, for example. However, a monoid homomorphism of groups is always a group homomorphism.]

Another interesting idea is this: Let R be a fixed ring, U its group of units. If M is an R-module, then U acts on M by assigning ux for $u \in U, x \in M$ to ux given by the R-module structure for M. Thus every R-module is a U-action in such a way that every homomorphism of R-modules is a homomorphism of the U-actions.

However, suppose some mathematics alien assigns every group G a ring structure in a random way. Then it's nearly impossible for every group homomorphism to be a homomorphism of the rings. We're not interested in that idea.

In each of the preceding examples, we formed variety by leaving certain operations and forgetting others. But here's a more nontrivial example: If A is an associative algebra over a commutative ring R, A becomes a Lie algebra by defining $[a : b] = ab - ba$. This operation isn't freshly one of the associative algebra's operations, but it is derived from the structure. Every homomorphism of associative algebras is evidently a homomorphism of the Lie algebras, because $f(ab - ba) = f(ab) - f(ba) = f(a)f(b) - f(b)f(a)$.

So the basic idea is to take the operations in one signature and define them using expressions from the other, but that's not good enough. Remember that to be in a variety, an algebra need not only have operations, but it must also satisfy identities. If the identities aren't satisfied in the first legitimate algebra, tough luck changing the structure.

Here's the rigorous definition of a takeoff of varieties:

DEFINITION

*Let Ω_1, Ω_2 be signatures, $\mathcal{V}(S_1)$ and $\mathcal{V}(S_2)$. A **takeoff** from $\mathcal{V}(S_1)$ to $\mathcal{V}(S_2)$ is a mathematical object T with the following structure:*

(1) *For each $\omega \in \Omega_2(n)$, $T\omega$ is some element of $F_{S_1}(\Omega_1, \{x_1, x_2, \ldots x_n\})$.*

(2) *Suppose* $h : F(\Omega_2, X_0) \to F_{S_1}(\Omega_1, X_0)$ *is the set map sending each symbol in* X_0 *to itself in the codomain, and each expression* $(\omega a_1 a_2 \dots a_n) \in F(\Omega_2, X_0)$ *to* $\varphi(T\omega)$ *with* $\varphi : F_{S_1}(\Omega_1, \{x_1, x_2, \dots, x_n\}) \to F_{S_1}(\Omega_1, X_0)$ *the homomorphism satisfying* $\varphi(x_i) = h(a_i)$ *for* $1 \le i \le n$. *Then* $h(w_1) = h(w_2)$ *for all* $(w_1, w_2) \in S_2$.

To make this definition less confusing, recall that $F_{S_1}(\Omega_1, \{x_1, x_2, \dots x_n\})$ consists of congruence classes of Ω_1-exrpessions in $x_1, x_2, \dots x_n$ given by the identities in S_1. Hence, $T\omega$ is one of these congruence classes, giving an expression to define ω as done with the Lie algebra.

If $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ is a takeoff and $A \in \mathcal{V}(S_1)$, then for each $\omega \in \Omega_2(n)$, $a_1, a_2, \dots a_n \in A$, define $(\omega a_1 a_2 \dots a_n)$ to equal $\varphi(T\omega)$ where

$$\varphi : F_{S_1}(\Omega_1, \{x_1, x_2, \dots, x_n\}) \to A$$

is the $\mathcal{V}(S_1)$ homomorphism sending $x_i \to a_i$. Taking $F_{S_1}(\Omega_1, X_0)$ for A, the map h in Condition (2) of the definition is then basically a homomorphism of Ω_2-algebras, and the condition says that the identities in S_2 are satisfied for $F_{S_1}(\Omega_1, X_0)$.

The fundamental theorem about takeoffs is this:

THEOREM 1.27 *Let* $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ *be a takeoff of varieties. Then:*

(1) *Every* $A \in \mathcal{V}(S_1)$ *becomes an algebra in* $\mathcal{V}(S_2)$ *when defined as above.*

(2) *Every* Ω_1*-homomorphism of algebras in* $\mathcal{V}(S_1)$ *is also an* Ω_2*-homomorphism of the algebras in* $\mathcal{V}(S_2)$ *[i.e. it preserves the operators in* Ω_2*].*

Remarkably, the converse of this theorem holds; see Exercise 3. The $\mathcal{V}(S_2)$ structure defined above is called the **derived structure** from the takeoff.

Proof of Theorem 1.27. (1) The definition above defines each $\omega \in \Omega_2(n)$ for A. We need only show that A satisfies every identity in S_2. Let $f : F(\Omega_2, X_0) \to A$ be a homomorphism, $h : F(\Omega_2, X_0) \to F_{S_1}(\Omega_1, X_0)$ be the homomorphism given by Condition (2) in the definition of a takeoff. Since $A \in \mathcal{V}(S_1)$, the map $X_0 \to A$ sending $x_i \to f(x_i)$ extends to a homomorphism $j : F_{S_1}(\Omega_1, X_0) \to A$, and evidently $jh = f$. If $(w_1, w_2) \in S_2$, $h(w_1) = h(w_2)$ by definition of a takeoff, hence $f(w_1) = jh(w_1) = jh(w_2) = f(w_2)$ and $(w_1, w_2) \in \ker f$. Therefore, $S \subseteq \ker f$ for every homomorphism $f : F(\Omega_2, X_0) \to A$, which means that $A \in \mathcal{V}(S_2)$.

(2) Suppose $A, B \in \mathcal{V}(S_1)$ and $f : A \to B$ is a Ω_1-homomorphism. Let $\omega \in \Omega_2(n)$, we wish to show that $f(\omega a_1 a_2 \dots a_n) = (\omega f(a_1) f(a_2) \dots f(a_n))$ for $a_1, a_2, \dots a_n \in A$. Let $\varphi_A : F_{S_1}(\Omega, \{x_1, x_2, \dots x_n\}) \to A$ be the homomorphism sending $x_i \to a_i$, and $\varphi_B : F_{S_1}(\Omega, \{x_1, x_2, \dots x_n\}) \to B$ the homomorphism sending $x_i \to f(a_i)$. Evidently $\varphi_B = f\varphi_A$ because $f\varphi_A$ sends $x_i \to f(a_i)$ and φ_B is unique for this property. However, by definition of ω in A and B,

$$\varphi_A(T\omega) = (\omega a_1 a_2 \dots a_n)$$

$$\varphi_B(T\omega) = (\omega f(a_1)f(a_2)\dots f(a_n))$$

Applying f to the first of these,

$$f\varphi_A(T\omega) = f(\omega a_1 a_2 \dots a_n)$$

Therefore, since $f\varphi_A = \varphi_B$, it follows that f preserves ω and is an Ω_2-homomorphism, completing the proof. ■

The takeoffs act a lot like homomorphisms of algebras in a single variety. The reader is left to do Exercises 1-7 and make discoveries.

Universals

The notion of a free algebra given by a set can be generalized to any takeoff. Recall the takeoff from rings to rngs, for instance; we shall find a fundamental ring enveloping any rng R. Define the ring $\overline{R} = \mathbb{Z} \times R$ as follows:

$$(n, r) + (n', r') = (n + n', r + r')$$

$$(n, r)(n', r') = (nn', nr' + n'r + rr')$$

$$0 = (0, 0), 1 = (1, 0), -(n, r) = (-n, -r)$$

Direct verification shows that $\overline{R}$ is a ring under these operations, and that $i : R \to \overline{R}$ given by $i(r) = (0, r)$ is a rng homomorphism.

Now suppose S is any *ring* and $f : R \to S$ is a rng homomorphism. Define $h : \overline{R} \to S$ by $j(n, r) = n1 + f(r)$. Then h is readily seen to be a *ring* homomorphism, and of course, $f = hi$. In fact, h is unique for this property, because if $f = h'i$ where h' is another ring homomorphism $\overline{R} \to S$,

$$h'(n, r) = h'(n(1, 0) + (0, r)) = h'(n1 + i(r)) = nh'(1) + h'i(r) = n1 + f(r)$$

Hence, $h' = h$.

Notice that even if R is already a ring, $\overline{R}$ may be larger than R. This is because of a basic property failed by the takeoff from rings to rngs; see Exercise 8. Summarizing this to any takeoff, we have:

DEFINITION

Let $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ be a takeoff of varieties. If $A \in \mathcal{V}(S_2)$, a ***universal $\mathcal{V}(S_1)$-algebra enveloping A for the takeoff*** *is a pair (U, i) where $U \in \mathcal{V}(S_1)$ and $i : A \to U$ is an Ω_2-homomorphism, such that whenever (U', f) is another pair with $U' \in \mathcal{V}(S_1)$ and $f : A \to U'$ an Ω_2-homomorphism, there exists a unique Ω_1-homomorphism $h : U \to U'$ such that $f = hi$.*

The foregoing example shows that $\overline{R}$ is a universal ring enveloping the rng R. Also, if $\mathcal{V}(S_2)$ is the variety of sets and T is the unique takeoff [Exercise 4(a)], the universal U is the free $\mathcal{V}(S_1)$-algebra given by the set A.

It can be shown that a universal is unique up to isomorphism, and in fact exists with a subtle and interesting recipe:

THEOREM 1.28 *Let $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ be a takeoff of varieties, and $A \in \mathcal{V}(S_2)$. If (U, i) and (U', i') are both universal $\mathcal{V}(S_1)$-algebras enveloping A, there exists a unique isomorphism $\sigma : U \to U'$ such that $i' = \sigma i$.*

Proof of Theorem 1.28. Since (U', i') is a pair with $U' \in \mathcal{V}(S_1)$ and $i' : A \to U'$ a Ω_2-homomorphism, but (U, i) is universal for this property, there exists a unique Ω_1-homomorphism $\sigma : U \to U'$ such that $i' = \sigma i$. Reversing the roles of (U', i') and (U, i) shows that since (U, i) has a property (U', i') is universal for, there is an Ω_1-homomorphism $\sigma' : U' \to U$ such that $i = \sigma' i'$. Furthermore, $\sigma'\sigma i = \sigma' i' = i$. Since (U, i) is universal though, 1_U is the *unique* homomorphism $U \to U$ such that $1_U i = i$, and hence, $\sigma'\sigma = 1_U$ by uniqueness. Likewise, $\sigma\sigma' = 1_{U'}$. Therefore, σ is an isomorphism with inverse σ'. ■

THEOREM 1.29 *Let $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ be a takeoff of varieties, and $A \in \mathcal{V}(S_2)$. Then there exists a universal (U, i) enveloping A.*

Proof of Theorem 1.29. Let $F = F_{S_1}(\Omega_1, A)$ where A is regarded as a *set*, and let $j : A \to F$ be the canonical set map into the free algebra. Then, let Θ be the congruence relation on F generated by tuples of the form

$$(j(\omega a_1 a_2 \dots a_n), (\omega j(a_1) j(a_2) \dots j(a_n)))$$

with $\omega \in \Omega_2(n)$ and $a_1, a_2, \dots a_n \in A$. [The latter of these expressions used the derived Ω_2-structure for F.] Finally, let $\pi : F \to F/\Theta$ the canonical epimorphism, $i = \pi j$. We claim that $(F/\Theta, i)$ is a universal enveloping A.

To begin with, $i : A \to F/\Theta$ is an Ω_2-homomorphism because whenever $\omega \in \Omega_2(n)$ and $a_1, a_2, \dots a_n \in A$, $j(\omega a_1 a_2 \dots a_n)\Theta(\omega j(a_1) j(a_2) \dots j(a_n))$, so that

$$\pi j(\omega a_1 a_2 \dots a_n) = \pi(\omega j(a_1) j(a_2) \dots j(a_n)) = (\omega \pi j(a_1) \pi j(a_2) \dots \pi j(a_n))$$

by virtue of π. Hence, $\pi j = i$ is a homomorphism.

Now suppose $B \in \mathcal{V}(S_1)$ and $f : A \to B$ is a Ω_2-homomorphism. Since $B \in \mathcal{V}(S_1)$, the set map f extends to an Ω_1-homomorphism $\overline{f} : F \to B$ such that $f = \overline{f} j$. It turns out that $\Theta \subseteq \ker \overline{f}$ because f is a homomorphism, and hence,

$$\overline{f} j(\omega a_1 a_2 \dots a_n) = f(\omega a_1 a_2 \dots a_n) = (\omega f(a_1) f(a_2) \dots f(a_n))$$

$$= (\omega \overline{f} j(a_1) \overline{f} j(a_2) \dots \overline{f} j(a_n)) = \overline{f}(\omega j(a_1) j(a_2) \dots j(a_n))$$

Thus $\ker \overline{f}$ contains all tuples of the form $(j(\omega a_1 a_2 \dots a_n), (\omega j(a_1) j(a_2) \dots j(a_n)))$, and hence, Θ since it's generated by those tuples. By Theorem 1.10, a homomorphism $h : F/\Theta \to B$ satisfying $\overline{f} = h\pi$ exists. Meanwhile, $f = hi$ since $f = \overline{f} j = h\pi j = hi$.

To show that h is unique, suppose $h' : F/\Theta \to B$ is also an Ω_1-homomorphism satisfying $f = h'i$. Then $f = h'i = h'\pi j = \overline{f}' j$, where $\overline{f}' = h'\pi$. However, $\overline{f}$ is the *unique* homomorphism $F \to B$ satisfying $f = \overline{f}j$, so that $\overline{f} = \overline{f}'$ by uniqueness. Finally, $h\pi = h'\pi$, and hence, $h = h'$ since π is surjective. Therefore, h is unique and the proof is concluded. ■

The proof of the existence of universals outlined a "recipe" for finding them: Let $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ be a takeoff of varieties, and $A \in \mathcal{V}(S_2)$.

1. First, take the free $\mathcal{V}(S_1)$-algebra F given by the set A. This induces a set map $A \to F$ with a universal mapping property.

2. To make that map a homomorphism, take each expression in F using one operator in Ω_2 as taken from Ω_1's operators, and identify that expression with its value in A, by factoring out the generated congruence relation. Make *no more identifications than that*, so the map is universal for all homomorphisms from A to any Ω_1-algebra.

3. Compose the set map in Step 1 with the canonical epimorphism $F \to F/\Theta$ and you get an Ω_2-homomorphism $A \to F/\Theta$. F/Θ with that map is the desired universal.

Remember, any two universals are isomorphic by Theorem 1.27, so don't expect to have different choices for the results.

To try the recipe, let M be a fixed monoid, N a submonoid of M. Then every M-action X becomes an N-action if we restrict the actors in the monoid, and this is clearly a takeoff. Now let X be an N-action; we wish to find the universal M-action enveloping X. Step 1 tells us to start with the free M-action given by X, which we know is $M \times X$, along with the map $x \to (1, x)$ from $X \to M \times X$.

To do Step 2, we must take each *expression* in $M \times X$ [given by the free M-action] resulting in scalarly multiplying a symbol in X by an element of N, and identify it with its actual value in the N-action X. If $x \in X$ and $n \in N$, the former of these is (n, x), whereas the latter is $nx \to (1, nx)$. So if Θ is the congruence relation on $M \times X$ generated by $\{((n, x), (1, nx)) \mid x \in X, n \in N\}$, then $(M \times X)/\Theta$ is the desired universal M-action. Step 3 tells us that the corresponding map $X \to (M \times X)/\Theta$ is given by $x \to \overline{(1, x)}$.

A more difficult example is the group enveloping a monoid M. Knowing what a free group is, one can easily apply Steps 1-3. The resulting group G consists of expressions of the form $[m_1]m_2^{-1}m_3m_4^{-1}\ldots m_{n-1}^{-1}[m_n]$, where $m_i \neq 1$ and $m_i \neq m_{i+1}$ in the reduced case.

EXERCISES

1. Let $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ be a takeoff of varieties and $A \in \mathcal{V}(S_1)$.

   (a) If B is a subalgebra of the Ω_1-algebra A, then B is also a subalgebra of A as an Ω_2-algebra, and the Ω_2-subalgebra structure on B is the same as the derived structure from the Ω_1-subalgebra structure. [*Hint*: Consider the canonical monomorphism.]

(b) If Φ is a congruence relation on the Ω_1-algebra A, then Φ is also a congruence relation of A as an Ω_2-algebra, and the Ω_2-quotient structure on A/Φ is the same as the derived structure from the Ω_1-quotient structure. [*Hint*: Consider the canonical epimorphism.]

(c) If $\{A_\alpha\}$ is a collection of algebras in $\mathcal{V}(S_1)$, then the derived Ω_2-structure of ΠA_α is the same as the structure for the product of the A_α's each with the derived structure. [*Hint*: Consider the projections from the product.]

2. An **affine** is a set X with a ternary operator $a\bar{b}c$ and the identities $(a\bar{b}c)\bar{d}f = a\bar{b}(c\bar{d}f)$ and $a\bar{b}b = a = b\bar{b}a$. Show that a group G is an affine when defined by $a\bar{b}c = ab^{-1}c$, and that this is a takeoff from the groups to the affines.

3. Let $\mathcal{V}(S_1)$ and $\mathcal{V}(S_2)$ be varieties. Suppose every algebra in $\mathcal{V}(S_1)$ is given a structure for an algebra in $\mathcal{V}(S_2)$, such that an Ω_1-homomorphism of algebras in $\mathcal{V}(S_1)$ is also an Ω_2-homomorphism. For each $\omega \in \Omega_2(n)$, define $T\omega = (\omega x_1 x_2 \dots x_n) \in F_{S_1}(\Omega_1, \{x_1, x_2, \dots x_n\})$. Show that T is the unique takeoff $\mathcal{V}(S_1) \to \mathcal{V}(S_2)$ in which the ensuing structures are the derived structures.

4. (a) Let $\mathcal{S}$ be the variety of sets, i.e. Ω-algebras with no operations in Ω whatsoever. Then there is a unique takeoff $\mathcal{V} \to \mathcal{S}$ where $\mathcal{V}$ is any variety.

   (b) Let $\mathcal{K}$ be the variety given by one nullary operator ϵ and one identity, $x = (\epsilon)$. Convince yourself that every $\mathcal{K}$-algebra is the one-element set $\{(\epsilon)\}$. [It is called the "King variety", if you insist.] Show that there's a unique takeoff $\mathcal{K} \to \mathcal{V}$ where $\mathcal{V}$ is any variety.

5. Let $T_1 : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ and $T_2 : \mathcal{V}(S_2) \to \mathcal{V}(S_3)$ be takeoffs of varieties. Define the **composite takeoff** $T_2T_1 : \mathcal{V}(S_1) \to \mathcal{V}(S_3)$ as follows: For each $\omega \in \Omega_3(n)$, $T_2T_1\omega = \varphi(T_2\omega)$ where $\varphi : F_{S_2}(\Omega_2, \{x_1, x_2, \dots x_n\}) \to F_{S_1}(\Omega_1, \{x_1, x_2, \dots x_n\})$ is the Ω_2-homomorphism sending each $x_i \to x_i$ [it exists because $F_{S_1}(\Omega_1, \{x_1, x_2, \dots x_n\}) \in \mathcal{V}(S_2)$].

   (a) T_2T_1 is a takeoff from $\mathcal{V}(S_1)$ to $\mathcal{V}(S_3)$, and for every $A \in \mathcal{V}(S_1)$, the derived Ω_3-structure given by T_2 of A as an Ω_2-algebra given by T_1's derived structure is the same as the derived Ω_3-structure of A given by T_2T_1.

   (b) If $T_3 : \mathcal{V}(S_3) \to \mathcal{V}(S_4)$ is another takeoff, $(T_3T_2)T_1 = T_3(T_2T_1)$. [*Hint*: Exercise 3 may help.]

   (c) Define the **identity takeoff** $1_{\mathcal{V}(S_1)} : \mathcal{V}(S_1) \to \mathcal{V}(S_1)$ by $T\omega = (\omega x_1 x_2 \dots x_n)$ for $\omega \in \Omega_1(n)$. Then the derived structure for an Ω_1-algebra A given by $1_{\mathcal{V}(S_1)}$ is simply its original structure.

   (d) If $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ is any takeoff, then $T1_{\mathcal{V}(S_1)} = T = 1_{\mathcal{V}(S_2)}T$.

6. A takeoff $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ is said to be an **isomorphism** [of varieties] if there exists another takeoff $T^{-1} : \mathcal{V}(S_2) \to \mathcal{V}(S_1)$ [called the **inverse** of T] such that $T^{-1}T = 1_{\mathcal{V}(S_1)}$ and $TT^{-1} = 1_{\mathcal{V}(S_2)}$.

   (a) Isomorphism of varieties is an equivalence relation.

   (b) The variety of abelian groups is isomorphic to the variety of $\mathbb{Z}$-modules. [*Hint*: Show that an abelian group, written additively, has a unique $\mathbb{Z}$-module structure.]

   (c) Let $1 \leq k \leq n$ be fixed positive integers. Suppose $\mathcal{V}$ is a variety given by one n-ary operator ω, and one identity, $(\omega x_1 x_2 \dots x_n) = x_k$. Then *every* set map of $\mathcal{V}$-algebras is a homomorphism, and $\mathcal{V}$ is isomorphic to the variety of sets.

   (d) The variety of groups is isomorphic to the variety of pointed affines [that is, affines with a nullary operator for the base point]. [*Hint*: Treat the base point as the group's identity element.]

   (e) A **Boolean ring** is a ring R satisfying $x^2 = x$ for all $x \in R$. Show that R is commutative and $1 + 1 = 0$ in R. Then, show that the takeoff from Boolean rings to Boolean algebras given by

   $$a \vee b = a + b - ab, a \wedge b = ab, 1 = 1, 0 = 0, a' = 1 - a$$

   is an isomorphism with inverse

   $$a + b = (a \wedge b') \vee (a' \wedge b), ab = a \wedge b, 1 = 1, 0 = 0, -a = a$$

   from the Boolean algebras to the Boolean rings.

   (f) Informally, what can you say about isomorphic varieties?

7. An **automorphism** of a variety is an isomorphism from the variety to itself.

   (a) The automorphisms of a variety form a group under takeoff composition. [You may assume that they form a set.]

   (b) Give examples of automorphisms of order 2 of the variety of monoids, of groups, of rings, of lattices, and of Boolean algebras. [*Hint*: If M is a monoid, define M^{op} by reversing the operands, $a * b = ba$.]

8. A takeoff $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ is said to be **full** if every Ω_2-homomorphism of algebras in $\mathcal{V}(S_1)$ [with derived structure] is an Ω_1-homomorphism. For example, the takeoff from groups to monoids is full, but the takeoff from rings to rngs is not, because a rng homomorphism of rings need not map 1 to 1.

   (a) The composition of full takeoffs is full, and every isomorphism of varieties is full.

   (b) If $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ is a full takeoff and A is an Ω_1-algebra, then $(A, 1_A)$ is the universal enveloping A [as an Ω_2-algebra with the derived structure] for T.

   (c) Show by example that part (b) may be false if T is not full.

9. (a) Suppose $T_1 : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ and $T_2 : \mathcal{V}(S_2) \to \mathcal{V}(S_3)$ are takeoffs, and let $A \in \mathcal{V}(S_3)$. If (U_2, i_2) is a universal enveloping A for T_2, and (U_1, i_1) is a universal enveloping U_2 for T_1, then $(U_1, i_1 i_2)$ is a universal enveloping A for $T_2 T_1$.

   (b) If $T_1 : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ is a takeoff, then a universal enveloping a free $\mathcal{V}(S_2)$-algebra given by a set X is a free $\mathcal{V}(S_1)$-algebra given by X. [*Hint*: Apply part (a) with $\mathcal{V}(S_3)$ the variety of sets.]

   (c) Under the takeoff from rings to monoids taking only the multiplication and 1 of a ring, the universal ring envelopping a monoid M is the direct sum $\sum_{m \in M} \mathbb{Z}$ with multiplication defined using the monoid operation and the distributive laws.

   (d) Using parts (b) and (c), figure out the free ring given by a set.

10. (a) Consider the takeoff from abelian groups to groups which forgets the commutativity requirement. The universal abelian group enveloping a group G is then $G/[G, G]$, where $[G, G]$ is the commutator subgroup of G.

    (b) Now consider the takeoff from commutative rings to rings. What's the universal commutative ring enveloping a ring R?

11. Let R be a fixed commutative ring, and consider the takeoff from associative algebras over R to Lie algebras over R given by $[a : b] = ab - ba$. Use the above recipe to find the universal associative algebra enveloping a Lie algebra L. [*Hint*: The free associative algebra given by a set is a bit similar to the free ring given by a set.]

12. Let $\mathcal{V}(S)$ be a variety. Define a new variety $\mathcal{V}(S')$ by adding a unary operator η which must be a homomorphism from the algebra to itself; that is, $(\eta(\omega a_1 a_2 \dots a_n)) = (\omega(\eta a_1)(\eta a_2) \dots (\eta a_n))$ for $\omega \in \Omega(n)$, $a_i \in A$. [This is called a $\mathcal{V}(S)$ **algebra with operator**.] Now consider the takeoff $\mathcal{V}(S') \to \mathcal{V}(S)$ which forgets the operator η and takes all other operators. Show that if $A \in \mathcal{V}(S)$, the universal $\mathcal{V}(S')$-algebra enveloping A is $\coprod_{n \in \mathbb{N}} A$, with η shifting up the operands of the coproduct.

13. Let $\mathcal{V}(S)$ be a variety. Define a new variety $\mathcal{V}(S')$ by adding a nullary operator ϵ for a base point. [This is called a **pointed** $\mathcal{V}(S)$ **algebra**.] Now consider the takeoff $\mathcal{V}(S') \to \mathcal{V}(S)$ which forgets the operator ϵ and takes all other operators. If $A \in \mathcal{V}(S)$, describe the universal $\mathcal{V}(S')$-algebra enveloping A.

14. Let $T : \mathcal{V}(S_1) \to \mathcal{V}(S_2)$ be a takeoff, $\{A_\alpha\}$ a family of $\mathcal{V}(S_2)$-algebras. For each α, let U_α be a universal Ω_1-algebra enveloping A_α. Show that the universal preserves coproducts: $\coprod U_\alpha$ is a universal Ω_1-algebra enveloping $\coprod A_\alpha$. Then determine the map. [*Caution*: $\coprod U_\alpha$ takes the coproduct in $\mathcal{V}(S_1)$, not in $\mathcal{V}(S_2)$.]