Algebras

We use the term "algebra" to mean an algebraic system—a set with operations.

1. Examples

(1) A group $\langle G; \cdot, {}^{-1}, e\rangle$.

(2) A ring $\langle R; +, \cdot, -, 0\rangle$; or a ring with 1 $\langle R; +, \cdot, -, 0, 1\rangle$.

(3) A Boolean algebra $\langle \mathrm{B}; \vee, \wedge, 0, 1, ' \rangle$.

(4) A lattice $\langle L; \vee, \wedge\rangle$; the lattice $\langle \mathbf{R}; \max, \min\rangle$.

(5) A vector space $\langle V; +, -, 0, \text{mult by } r \text{ for each } r \in \mathbf{R}\rangle$ (if V is over the reals).

(6) Perkins' semigroup $\langle S; \cdot\rangle$, with elements
$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$

(7) The 1-unary algebra $\langle A; f\rangle$ with diagram

(8) The tournament $\langle T; \vee, \wedge\rangle$ with diagram

(9) The Heyting algebra $\langle \{0, a, 1\}; \vee, \wedge, \to, 0, 1\rangle$.

(10) The Murskii 1-binary algebra $\langle M; \cdot\rangle$ with table

	0	a	b
0	0	0	0
a	0	0	a
b	0	b	b

(11) Tarski's high-school-algebra algebra $\langle \omega; +, \cdot, \uparrow, 1\rangle$.

(12) Shallon's graph algebra $\langle G \cup \{0\}; \cdot\rangle$, $\quad G =$

(13) The relation algebra $\langle \mathrm{Pow}(S \times S); \cup, \cap, \emptyset, 1, ', \circ, {}^{\cup}, \Delta \rangle$ (S any set).

(14) The implication algebra $\langle \mathbf{2}; \to \rangle$.

(15) The lattice-ordered group $\langle \mathbf{Z}; \wedge, \vee, +, -, 0 \rangle$.

(16) The set algebra $\langle S; \rangle$ (set S with no operations).

(17) The 1-binary algebra $\langle \{0,1,2\}; \cdot \rangle$ with table

	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

2. Some sets of laws

[1] Defining laws for groups: A *group* is an algebra ... satisfying the laws ...

[2] Defining laws for lattices: A *lattice* is an algebra ... satisfying the laws ...

[3] Defining laws for relation algebras: A *relation algebra* is an algebra $\langle R; \vee, \wedge, 0, 1, ', \circ, {}^{\cup}, \Delta \rangle$ such that

(i) $\langle R; \vee, \wedge, 0, 1 \rangle$ is a Boolean algebra;

(ii) $\circ$ is associative;

(iii) $\Delta \circ x = x \circ \Delta = x$;

(iv) ${}^{\cup}$ is a Boolean automorphism, $x^{\cup\cup} = x$, and $(x \circ y)^{\cup} = y^{\cup} \circ x^{\cup}$;

(v) $(x \circ y) \wedge z \leq x \circ (y \wedge (x^{\cup} \circ z))$.

[4] Defining laws for Heyting algebras: A *Heyting algebra* is an algebra $\langle H; \vee, \wedge, \to, 0 \rangle$ such that

(i) $\langle H; \vee, \wedge, 0 \rangle$ is a lattice with 0;

(ii) $x \wedge (x \to y) = x \wedge y$;

(iii) $x \wedge (y \to z) = x \wedge ((x \wedge y) \to (x \wedge z))$;

(iv) $z \wedge ((x \wedge y) \to x) = z$.

[5] Defining laws for implication algebras: An *implication algebra* is an algebra $\langle A; \to \rangle$ such that

(i) $(x \to y) \to x = x$;

(ii) $(x \to y) \to y = (y \to x) \to x$;

(iii) $x \to (y \to z) = y \to (x \to z)$.

[6] Tarski's "high-school identity problem": Do these laws imply all laws of $\langle \omega; x+y, xy, x^y, 1 \rangle$? This was solved; the answer is negative.

$x + y = y + x$	$xy = yx$	$x+(y+z) = (x+y)+z$	$x(yz) = (xy)z$
$x(y + z) = xy + xz$	$x^{y+z} = x^y x^z$	$(xy)^z = x^z y^z$	$(x^y)^z = x^{(yz)}$
$x \cdot 1 = x$	$x^1 = x$	$1^x = 1$	

[7] Robbins' Problem: Do these laws define Boolean algebras? The answer is "yes"; the proof was found by computer in 1996.

(i) $\vee$ is commutative;

(ii) $\vee$ is associative;

(iii) $((x \vee y)' \vee (x \vee y')')' = x$.

Erratum: A different version of (iii) was quoted in Handout H; it was not the one Robbins asked about.

3. Some definitions

3.1 A function $f : A^n \to A$ is an *n-ary operation* on A; n is its "arity."

(For $n = 0, 1, 2, 3$ we say "nullary", "unary", "binary", "ternary".)

3.2 An *algebra* is a set A with a given family of operations f_γ ($\gamma \in \Gamma$), called the "basic operations" of A. Officially, the algebra is $\langle A; f_\gamma, \gamma \in \Gamma \rangle$. Texts often use a separate letter to distinguish the algebra from the set, but we'll follow the informal practice of group theory and use A for both.

3.3 The *type* of $\langle A; f_\gamma, \gamma \in \Gamma \rangle$ is the function $\tau : \Gamma \to \omega$ given by $\tau(\gamma) = n_\gamma$, the arity of f_γ. Two algebras of the same type are *similar*. In discussions involving more than one algebra, we'll normally assume that all the algebras are similar. Usually Γ will be finite; if $|\Gamma| = m$, then it is simplest to choose $\Gamma = 0, \ldots, m-1$ and write the n_γ as a sequence.

For example, the type of a Boolean algebra $\langle B; \vee, \wedge, 0, 1, ' \rangle$ can be written $\langle 2, 2, 0, 0, 1 \rangle$.

3.4 The *terms* (formal expressions) in variable symbols $x_1, \ldots, x_n$ for type τ are the strings of symbols obtained recursively from these conditions:

(a) Each x_i is a term, and

(b) if $t_1, \ldots, t_{n_\gamma}$ are terms, so is $\mathbf{f}_\gamma(t_1, \ldots, t_{n_\gamma})$, where $\mathbf{f}_\gamma$ and the commas and parentheses are symbols and $\gamma \in \Gamma$.

A term t in variable symbols $x_1, \ldots, x_n$ is often described by $t(x_1, \ldots, x_n)$. For algebras with familiar notations we use those notations instead; for example, a group term might be written as $x_1(x_2^{-1}x_3)$.

3.5 Evaluation: If $t(x_1, \ldots, x_n)$ is a term for type τ and A is an algebra of type τ, and if $a_1, \ldots, a_n \in A$ are given, $t(x_1, \ldots, x_n)$ can be regarded as a recipe for calculating a *value* in A, called $t(a_1, \ldots, a_n)$. Thus t induces a function on $A^n \to A$. The functions so induced are called the *n-ary term functions* on A.

This is similar to the case of of polynomials over a commutative ring R, where we distinguish between a formal polynomial $f(X)$ and a polynomial function. Indeed, if R is finite, there are only finitely many one-variable polynomials functions on R, but $R[X]$ is infinite.

3.6 A sentence $(\forall x_1) \ldots (\forall x_n) t(x_1, \ldots, x_n) = u(x_1, \ldots, x_n)$ is called a *law* or *identity* in n variables. We often suppress $\forall x_i$ or even write $t = u$. Also, many authors write $t \approx u$, to distinguish this formal situation from actual equality of two elements. If $t(a_1, \ldots, a_n) = u(a_1, \ldots, a_n)$ for all $a_1, \ldots, a_n \in A$, then $t = u$ is *satisfied* by A (written $A \models t = u$), or *holds* in A, or that A is a *model* of $t = u$.

3.7 A *variety* is a class of algebras definable by laws, i.e., the class of all algebras that satisfy some particular set of laws. An *equational theory* is the set of all laws satisfied by some one class of similar algebras.

Example of varieties are those of rings, of groups, of abelian groups, of lattices, of distributive lattices, and of the other classes of algebras whose defining laws are given in §**??**.

4. Problems

Problem A-1. For each of these algebras K, find (i) a 1-variable law of the algebra that does not hold in *all* algebras of the same type, and (ii) (if you can) a law in 2 or more variables that is not an obvious consequence of a 1-variable law of the algebra. No proofs are required.

(a) Perkins' semigroup;

(b) Murskii's 1-binary algebra;

(c) Shallon's graph algebra [note: the operation is idempotent];

(d) the permutation group S_3.

(e) the tournament (8).

(A *tournament* is a directed graph in which every two vertices are joined by a single edge oriented one way or the other. It can be envisioned as a

record of who won each match in a "round-robin" tournament, where each player has played every other player once—the arrow points towards the player who won. A tournament can be made into an algebra by letting $x \vee y$ be the winner and $x \wedge y$ the loser of the game between x and y.)

Problem A-2. For the 1-unary algebra $\langle A; f \rangle$ of Example (7), find its equational theory (the set of all laws that hold). You'll need to consider the possibilities $f^n(x) = f^m(y)$ and $f^n(x) = f^m(x)$ $(m \geq n \geq 0)$. Sketch your reasoning.

Problem A-3. For the two-element group $C_2 = \{e, a\}$, invent a procedure for telling whether a given group law holds in C_2. (For example, $((xy)z^{-1})^{-1} = x^{-1}(zy)$?)

Problem A-4. For each of the algebras of examples (4)(for **R**), (6), (7), (8), (10), (12), (15), (16), (17) in §**??**, comment on its subalgebras. If there are just a couple, say what they are; if there are many, either describe them all or describe a typical one. No proofs are required.

Problem A-5. Of the binary operations involved in the examples from §**??**, list those that are *not* commutative.

Concepts for algebras

1. Definitions

- A *term* t or $t(x_1, \ldots, x_n)$ of type τ is a formal expression as a string of symbols, defined recursively as follows, starting from variable symbols $x_1, \ldots, x_n$ for τ:

  (a) Each x_i is a term, and

  (b) if $t_1, \ldots, t_{n_\gamma}$ are terms, so is $\mathbf{f}_\gamma(t_1, \ldots, t_{n_\gamma})$, where $\mathbf{f}_\gamma$ and the commas and parentheses are symbols and $\gamma \in \Gamma$.

- For elements $a_1, \ldots, a_n$ of an algebra A, the *value* $t(a_1, \ldots, a_n)$ is the element of A obtained by using $t(x_1, \ldots, x_n)$ as a recipe.

- A *term relation* $t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n)$ is an equation holding for a *particular* n-tuple of elements of A.

- A *law* is a formal equation $t_1 = t_2$ or $t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)$, with $(\forall x_1) \ldots (\forall x_n)$ understood. The law $t_1 = t_2$ *holds* in A when *all* n-tuples $a_1, \ldots, a_n$ from A satisfy the term relation $t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n)$.

  We also say A satisfies $t_1 = t_2$, or A is a model of $t_1 = t_2$, or write $A \models t_1 = t_2$.

- A *variety* of algebras of a given type is the class of all models of some set of laws. Examples are the varieties of all groups, of all abelian groups, of all lattices, and of all distributive lattices.

  If A is an algebra we write $\mathrm{Var}(A)$ for the variety determined by all laws holding in A, which is the smallest variety containing A.

- A *subalgebra* of an algebra A is a subset $S \subseteq A$ that is closed under all the basic operations of A.

- An algebra A is said to be *generated* by its elements $g_1, \ldots, g_n$ if the smallest subalgebra of A that contains all the g_i is A itself.

- A *homomorphism* $\phi : A \to B$ between similar algebras is a map compatible with the basic operations of A and B.

- The *direct product* of a family of similar algebras, $A_1 \times A_2$ or more generally $\prod_{\gamma \in \Gamma} A_\gamma$, is the set-theoretic cartesian product with operations computed coordinatewise.

- A *congruence relation* on A is an equivalence relation θ on A that is compatible with the basic operations of A.
- For a congruence relation θ on A, the blocks of θ form an algebra A/θ of the same type, with a natural surjective homomorphism $\eta : A \to A/\theta$.

2. Some theorems

Familiar theorems from group theory all generalize, except that in groups we focus on normal subgroups, but for algebras in general we focus on congruence relations, a generalization of the coset decomposition of a normal subgroup. The reason is that in groups the whole coset decomposition is determined by knowing the block containing the identity element, while for algebras in general no one block determines the rest.

- The subalgebra of A generated by $g_1, \ldots, g_n$ is the set of elements of the form $t(g_1, \ldots, g_n)$ for some term t in n variables.
- The image of a homomorphism is a subalgebra.
- The set $\mathrm{Con}(A)$ of all congruence relations on A is a lattice, the *congruence lattice* of A.
- If $\phi : A \to B$ is a homomorphism, then the equivalence relation on A induced by ϕ is a congruence relation, which we call $\ker \phi$, the *kernel* of ϕ.

  Observe that if $\theta \in \mathrm{Con}(A)$ and $\eta : A \to A/\theta$ is the natural surjection, then $\ker \eta = \theta$.
- If $\phi : A \to B$ is a surjective homomorphism, then $B \cong A/\ker \phi$ (the **first isomorphism theorem**).

  Thus we have an "internal description" of all the homomorphic images of A, up to isomorphism.
- If $\phi : A \to B$ is a surjective homomorphism, then the congruence relations on B correspond one-to-one to the congruence relations on A that contain $\ker \phi$ (the **correspondence theorem**).
- For a direct product $P = \prod_{\gamma \in \Gamma} A_\gamma$, for each $\gamma \in \Gamma$ the coordinate projection $\pi_\gamma : P \to A_\gamma$ is a surjective homomorphism.

Free algebras

1. The concept

Definition. Let V be a variety. The algebra F is *free* in V on $g_1, \ldots, g_n$ if

(i) $F \in V$,

(ii) F is generated by $g_1, \ldots, g_n$, and

(iii) the *only* term relations holding between $g_1, \ldots, g_n$ are those that hold for *all* n-tuples in *all* algebras in V, i.e., are the laws holding in V.

(In examples generators may also be labeled g, h, k or a, b, c, etc.)

2. Examples

#1. In a diagram of the free distributive lattice FDL(3) (Figure **??**), if the generators are g_1, g_2, g_3 you can see that

$$(g_1 \vee g_2) \wedge (g_1 \vee g_3) \wedge (g_2 \vee g_3) = (g_1 \wedge g_2) \vee (g_1 \wedge g_3) \vee (g_2 \wedge g_3).$$

Once it is known that this lattice is indeed a free distributive lattice on three generators, then it follows that this law holds in all distributive lattices:

$$(x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge (x_2 \vee x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$$

#2. The free Boolean algebra FBA(3), corresponding to a Venn diagram with three circles. It has 8 atoms and 256 elements.

#3. The free modular lattice FML(3) shown in Figure **??**. It has 28 elements.

#4. The free lattice FL(3) shown in Figure **??**. It is infinite. Dashed lines represent infinitely many elements not shown.

#5. The free abelian group on n generators is $\mathbf{Z}^n$.

#6. The free group FG(2) consists of all finite expressions such as $g^2h^{-3}gh^2$, with appropriate equalities.

#7. Every vector space is free, with generators being any basis.

#8. For a given type τ, the *term algebra* $T_\tau(n)$ is the set of all n-ary terms of type τ, with operations being formal compositions. The generators are the variable symbols $x_1, \ldots, x_n$.

Figure 1: FDL(3)

3. The universal mapping property

Proposition. If F is free in V on $g_1, \ldots, g_n$ and A is any algebra in V and $a_1, \ldots, a_n \in A$, then there is a unique homomorphism $\phi : F \to A$ with $f(g_i) = a_i$ for each i. (In other words, you can aim the generators of F at any elements of any algebra in V and find a homomorphism that takes the generators there.)

Corollary 1. Up to isomorphism, there is only one free algebra in V on n generators.

Let us call this algebra $F_V(n)$.

Corollary 2. Every n-generated algebra of V is a homomorphic image of $F_V(n)$.

Corollary 3. If $F_V(n)$ is finite, then it is the largest n-generated algebra in V, and the only one of its size (up to isomorphism).

Figure 2: FML(3)

$M_+ = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$

M_+

a b c

M_-

$M_- = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c)$

Figure 3: FL(3)

4. Existence of free algebras in $V = \mathbf{Var}(A)$

Let the free algebra on n generators in $\mathrm{Var}(A)$ be denoted $F_A(n)$.

Theorem (Birkhoff) $F_A(n)$ can be constructed as follows:

Let Δ be the set of all functions $\delta : \{1, \ldots n\} \to A$, and let $P = A^\Delta$.

For $i = 1, \ldots, n$ let $g_i \in P$ be the element whose δ-th coordinate is $\delta(i)$.

Let F be the subalgebra of P generated by $g_1, \ldots, g_n$.

Then $F = F_A(n)$.

Example. To generate $F_{\mathbf{2}}(3)$ (= FDL(3)), where **2** is the 2-element lattice, proceed as shown in Figure **??**.

Row	coordinate values								using	expression
1:	0	1	0	1	0	1	0	1	gen	g
2:	0	0	1	1	0	0	1	1	gen	h
3:	0	0	0	0	1	1	1	1	gen	k
4:	0	0	0	1	0	0	0	1	$2 \wedge 1$	$g \wedge h$
5:	0	1	1	1	0	1	1	1	$2 \vee 1$	$g \vee h$
6:	0	0	0	0	0	1	0	1	$3 \wedge 1$	$g \wedge k$
7:	0	1	0	1	1	1	1	1	$3 \vee 1$	$g \vee k$
8:	0	0	0	0	0	0	1	1	$3 \wedge 2$	$h \wedge k$
9:	0	0	1	1	1	1	1	1	$3 \vee 2$	$h \vee k$
10:	0	0	0	0	0	0	0	1	$4 \wedge 3$	$g \wedge h \wedge k$
11:	0	0	0	1	1	1	1	1	$4 \vee 3$	$(g \wedge h) \vee k$
12:	0	0	0	0	0	1	1	1	$5 \wedge 3$	$(g \vee h) \wedge k$
13:	0	1	1	1	1	1	1	1	$5 \vee 3$	$g \vee h \vee k$
14:	0	0	1	1	0	1	1	1	$6 \vee 2$	$(g \wedge k) \vee h$
15:	0	0	0	1	0	1	0	1	$6 \vee 4$	$(g \wedge h) \vee (g \wedge k)$
16:	0	0	0	1	0	0	1	1	$7 \wedge 2$	$(g \vee k) \wedge h$
17:	0	1	0	1	0	1	1	1	$7 \wedge 5$	$(g \vee h) \wedge (g \vee k)$
18:	0	0	0	1	0	1	1	1	$11 \wedge 5$	$((g \wedge h) \vee k) \wedge (g \vee h)$

Figure 4: Construction of FDL(3) as $F_{\mathbf{2}}(3)$

As another example, Figure **??** shows the table obtain for $A = \mathbf{Z}_3$ under subtraction and for $n = 2$:

The rows form the free algebra $F_A(2)$ inside A^9. Of course, this example is really a disguised version of an additive group.

row	9-tuple	from?	expr
R1	0 1 2 0 1 2 0 1 2	gen	g
R2	0 0 0 1 1 1 2 2 2	gen	h
R3	0 0 0 0 0 0 0 0 0	R1–R1	$g - g$
R4	0 1 2 2 0 1 1 2 0	R1–R2	$g - h$
R5	0 2 1 1 0 2 2 1 0	R2–R1	$h - g$
R6	0 2 1 2 1 0 1 0 2	R1–R5	$g - (h - g)$
R7	0 2 1 0 2 1 0 2 1	R3–R1	$(g - g) - g$
R8	0 0 0 2 2 2 1 1 1	R3–R2	$(g - g) - h$
R9	0 1 2 1 2 0 2 0 1	R4–R2	$(g - h) - h$

Figure 5: Construction of $F_{\mathbf{Z}_3}(2)$ under subtraction

5. Existence of free algebras in arbitrary varieties

Proposition. For every variety V and every n there exists a free algebra in V with n generators. In other words, $F_V(n)$ always exists.

Outline of proof #1: The method of saving term relations in common.

This is a generalization of the "table" method (above) for a single algebra: We start by considering all functions $\delta : \{1, \ldots, n\} \to A$ where A runs through all algebras in V. Since V is too large to be a set, there are also too many δ's, so we restrict our attention to cases where the image of δ generates A, and we remark that up to isomorphism there is only a set (rather than a class) of ways in which an image of such a δ can sit inside the A it generates. Let Δ consist of one δ from each isomorphism class. Then inside A^Δ, for $i = 1, \ldots n$ let g_i be the element whose δ-th coordinate is $\delta(i)$, and let F be the subalgebra of A^Δ generated by $g_1, \ldots, g_n$. Then we remark that F has the Universal Mapping Property (UMP), so is free. I call this the method of "saving relations in common", because the only relations $t = u$ between the g_i are those true in every factor, and the factors account for all ways that n elements of an algebra in V can be related. As you see, there are two elements in this proof: choosing the isomorphism types and taking the subalgebra of a product.

Outline of proof #2: The method of overshooting.

For $T = T_\tau(n)$ (the algebra of all terms in n variables), let $F_V(n) = T/\theta_0$, where $\theta_0 = \cap\{\theta \in \mathrm{Con}(T) : T/\theta \in V\}$. Here θ_0 is the least congruence relation θ on t such that $T/\theta \in V$. One can show that $F_V(n)$ inherits the UMP from T, which is free in the variety of all algebras of type τ. I call this the "overshooting" method: Since T is free but much too big, you have overshot, and you must trim T down to where it fits in V, by taking T modulo a congruence relation.

6. Infinite generating sets

Everything discussed above works for the case of infinite generating sets $g_i, i \in \alpha$, where α represents any cardinal number. For example, we can make $F_V(\aleph_0)$. Even for infinitely many generators, though, every term t still involves only finitely many of the variables.

7. Application to construction of varieties

For a class $\mathcal{K}$ of similar algebras, let $\mathbf{S}(\mathcal{K})$, $\mathbf{P}(\mathcal{K})$, and $\mathbf{H}(\mathcal{K})$ denote the classes constructed from $\mathcal{K}$ by taking respectively subalgebras, products, and homomorphic images of members of $\mathcal{K}$.

Theorem (G. Birkhoff) A class $\mathcal{V}$ of similar algebras is a variety if and only if $\mathcal{V}$ is closed under $\mathbf{S}$, $\mathbf{P}$, and $\mathbf{H}$.

Corollary (Birkhoff-Tarski) For any class $\mathcal{K}$ of similar algebras, $\mathrm{Var}(\mathcal{K})$ (the smallest variety containing $\mathcal{K}$) is obtainable as $\mathrm{Var}(\mathcal{K}) = \mathbf{HSP}(\mathcal{K})$, meaning $\mathbf{H}(\mathbf{S}(\mathbf{P}(\mathcal{K})))$.

8. The free 2-generated group in the quaternion group variety (to be discussed in lecture)

Let $F = F_V(2)$ for $V = \mathrm{Var}(D_8) = \mathrm{Var}(Q_8)$.

Laws determining V are $x^4 = e$, $x^2y = yx^2$.

Let a, b be generators of F and let $c = (ab)^{-1}$.

Every element of F has the form $a^i b^j a^{2k} b^{2\ell} c^{2m}$, where $0 \leq i, j, k, \ell, m \leq 1$.

F is the semidirect product of $\mathbf{Z}_2 \times \mathbf{Z}_4$ by $\mathbf{Z}_4$ via powers of $\sigma(u, v) = (u+v, v)$.

See Figure **??**.

9. Problems

(Some of these problems depend on additional material from lectures.)

Problem C-1. Describe (a) the free 1-unary algebra on n generators;

(b) $F_V(2)$, where V is the variety of 1-unary algebras with $f^3(x) = f^5(x)$;

(c) the free 2-unary algebra on 1 generator;

(d) $F_S(3)$, where $S = \langle \mathbf{2}, \vee \rangle$, using the table method. (Here S is a *semilattice*—a set with a single binary operation that is associative, commutative, and idempotent. A semilattice can also be defined as a set with a partial order such that any two elements have a least upper bound. Thus one way to obtain a semilattice is to take a lattice and ignore the meet operation, as has been done to make S.)

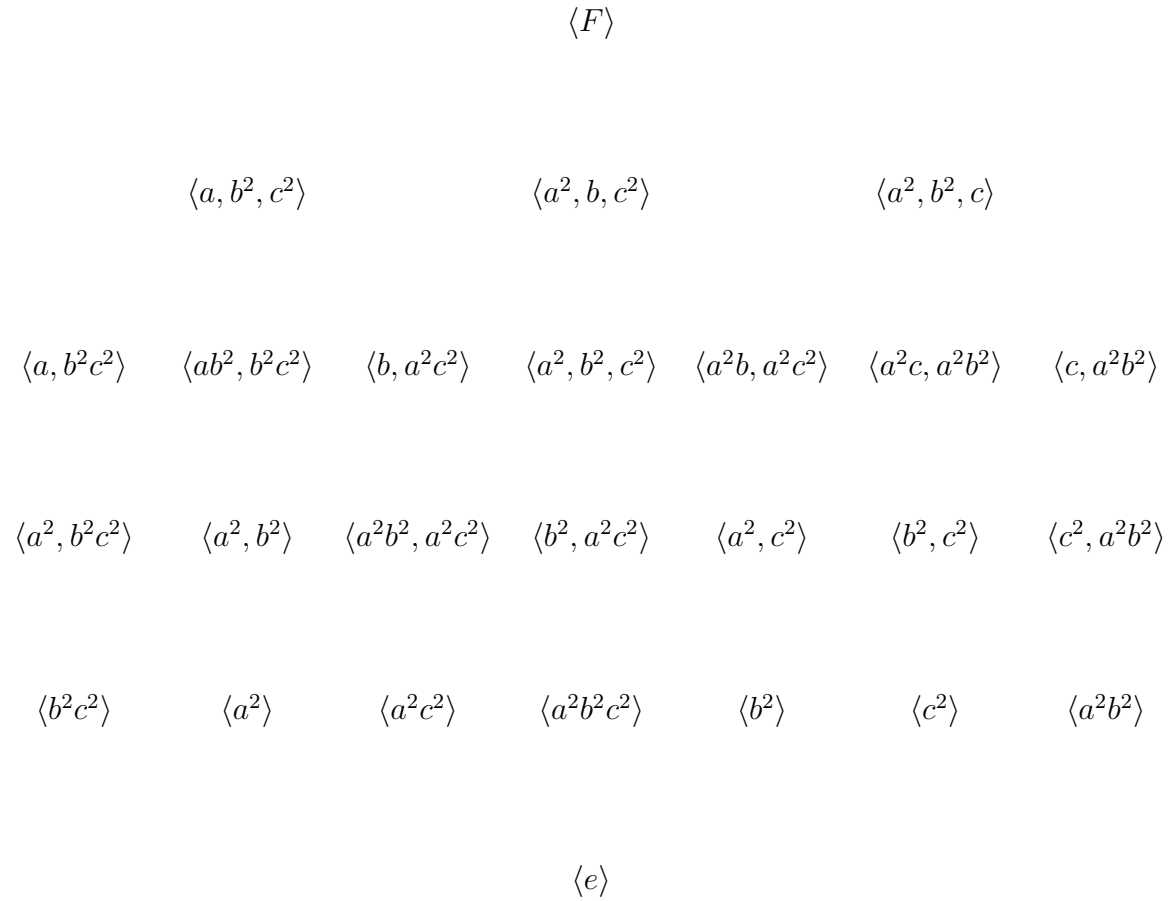

Figure 6: $\mathrm{Con}(F)$, the lattice of normal subgroups of F

Problem C-2. *Theorem.* In a group G, every commutator $a^{-1}b^{-1}ab$ is a product of squares.

Proof #1. Let $S = \{\text{products of squares}\}$. Observe that S is a normal subgroup. Moreover, G/S satisfies $x^2 = e$ and so is abelian. Then in G/S, $\overline{a}^{-1}\overline{b}^{-1}\overline{a}\overline{b} = \overline{e}$. This is the same as saying that in G, $a^{-1}b^{-1}ab \in S$.

This proof was indirect. A more direct proof would be to exhibit a law $x^{-1}y^{-1}xy = (\dots)^2(\dots)^2\dots(\dots)^2$ true in all groups, where each $(\dots)$ contains some expression in x, y.

(a) Before attempting to *give* such a proof, explain why there *must* exist a direct proof of this form.

(b) Somehow or other, find the direct proof.

Problem C-3. For Murskii's algebra M, suppose you want to compute $F_M(2)$, using the table method. (a) Show what generating rows you would use. (b) Compute new rows in some reasonable order, labeling each row with the expression in the generators that produced it, until you generate a row that is already there. What law have you found? (c) If your law was in one variable, continue further until you get a law involving two variables. (d) Actually, $F_M(2)$ has 11 elements. How many multiplications of rows would be involved in computing the whole free algebra and verifying that you are done?

Problem C-4. Two proofs of the existence of the free algebra $F_V(n)$ are described in §6 above. They sound very different. Nevertheless, they are essentially the same. The problem: Explain why, by analyzing how the two elements of the first one are really present in the second.

Problem C-5. (a) Suppose that an algebra F has a given set of generators $g_1, \dots, g_n$. Show that if F has the universal mapping property for maps into *itself*, then F is free in *some* variety V. (Thus being free is in effect an absolute property of an algebra, without having to name a variety containing it.)

(b) An achievement of recent years was the solution of the restricted Burnside problem: For any k and n, there is a largest finite group with n generators that obeys $x^k = 1$. (There could also be infinite groups fitting this description; it's just that there is a largest finite one.) Is this largest finite group necessarily free? (Discuss.)

Problem C-6. Let V be the variety of *idempotent semigroups*: 1-binary algebras whose operation is associative and obeys the law $x^2 = x$.

By experimenting with expressions, make a conjecture as to whether $F_V(3)$ is finite or infinite. Explain briefly how you arrived at your answer.

Problem C-7. The term algebra $T_\tau(n)$ is described in §3 above; in §6 it is used in the second proof of the existence of free algebras in a variety.

For the variety V of 1-unary algebras obeying the law $f^3(x) = f^5(x)$ and for $n = 1$, explicitly describe $T_\tau(1)$ and all $\theta \in \mathrm{Con}(T_\tau(1))$ giving a quotient in V. (Here $\tau = \langle 1 \rangle$.)

Problem C-8. Consider the "constructions" $\mathbf{H}, \mathbf{S}, \mathbf{P}$ on classes of algebras.

(a) Say which containment relations between pairs of constructions must hold, e.g., $\mathbf{SH}(\mathcal{K}) \subseteq \mathbf{HS}(\mathcal{K})$. (All the valid relations have easy proofs, but it is not required to write them down. Interpret $\mathbf{H}, \mathbf{S}, \mathbf{P}$ up to isomorphism.)

(b) For one such potential relation that does *not* hold, find a counterexample, with brief proof.

Problem C-9. Let $F = F_{Q_8}(2)$. Refer to Figure **??**. (a) Find a normal subgroup N of F such that $F/N \cong \mathbf{Z}_2 \times \mathbf{Z}_4$. (b) Find a normal subgroup N such that $F/N \cong D_8$. Find a normal subgroup N such that $F/N \cong Q_8$. Find the commutator subgroup F' of F. (Determine the order of each subgroup. Recall the Correspondence Theorem, which says that the subgroups of F that contain N form the same diagram as the subgroups of F/N; the same is true if just normal subgroups are considered. From the previous problem you know that for abelian 2-groups (groups whose order is a power of 2), the group can be identified from the subgroup diagram. Recall that F' is contained in every N for which F/N is abelian.)

Problem C-10. Figure **??** shows homomorphisms of FML(3) onto FDL(3) and M_3, determined by mapping generators to generators.

On a copy of Figure **??**, indicate $\ker \alpha$ and $\ker \beta$. (You will need to decide which elements go to which, but you need not write this information down. A congruence relation on a finite lattice is best diagrammed simply by darkening the coverings that are "collapsed", i.e., coverings between elements in the same block. Use different coloring or markings for the two congruence relations involved.)

Note. If there are surjections $A \to B$ and $A \to C$ whose kernels have intersection 0, then A is embeddable in $B \times C$, as we'll discuss in class. Since this is the case in Figure **??**, you have shown the interesting fact that FML(3) is embeddable in the direct product of FDL(3) and a single copy of M_3.

α

β

Figure 7: Two homomorphisms

Problem C-11. For the free algebra from the table shown in Figure **??**:

(a) Whenever we subtract two rows we get a relation between generators, which is then a law, usually nontrivial. What relation between generators, and so what law, comes from the computation R8-R9 = 0 2 1 1 0 2 2 1 0 = R5, where R8 means row 8, etc.?

(b) Suppose we want to use the universal mapping property to map F to A with $g \mapsto 2$, $h \mapsto 1$. Which column of the table gives the projection that achieves this, and what is the homomorphism on F?

Congruence relations

1. The concept

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

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

and of course $0 \equiv 0$.

The same definition works for algebraic systems in general:

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

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

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

2. Examples

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

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

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

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

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

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

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

(a) (b)

Figure 1: Congruence relations on lattices

3. The congruence lattice of an algebra

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

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

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

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

4. Factor algebras

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

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

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

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

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

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

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

Figure 2: The natural homomorphism

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

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

5. The first isomorphism theorem

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

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

For algebras in general, the situation is the same:

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

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

6. The correspondence theorem

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

The generalization to algebras is this:

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

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

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

7. Intersections of congruence relations

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

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

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

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

8. Congruence relations on lattices

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

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

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

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

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

8.2 **Theorems**

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

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

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

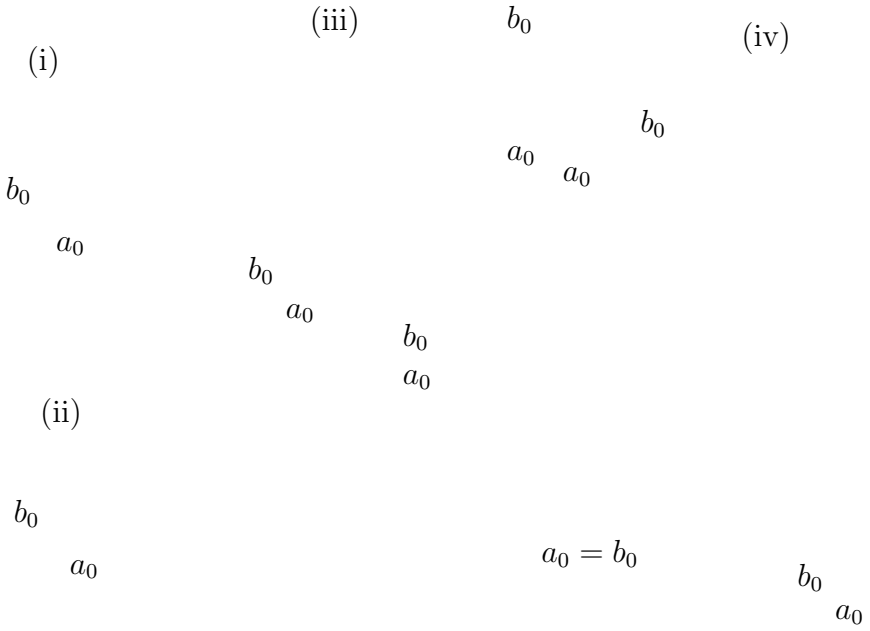

Figure 3: Some lattices for which to find congruence lattices

9. Problems

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

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

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

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

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

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

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

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

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

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

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

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

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

The subdirect representation theorem

1. Direct products

Here is an attempt at a decomposition theorem using direct products:

Define an algebra $\mathcal{A}$ to be *directly indecomposable* if $|A| > 1$ and there are no $\mathcal{B}, \mathcal{C}$ with $\mathcal{A} \equiv \mathcal{B} \times \mathcal{C}$ except with $|B| = 1$ or $|C| = 1$.

Here is the statement you might hope for: "Every algebra is the direct product of directly indecomposable algebras (possibly infinitely many)." This is certainly true for finite algebras, but is false in general. In fact, let $\mathcal{A}$ be a vector space of countable dimension over the two-element field; observe that any directly indecomposable vector space has dimension 1 by a basis argument, but $\mathcal{A}$ has the wrong cardinality to be a direct product of either finitely many or infinitely many two-element vector spaces[1].

A modified concept, that of "subdirect products of subdirectly irreducible algebras", works much better.

Figure 1: A subdirect product, heuristically

2. Subdirect products

2.1 *Definition.* A *subdirect product* of $\mathcal{B}$ and $\mathcal{C}$ is a subalgebra $\mathcal{A}_0$ of $\mathcal{B} \times \mathcal{C}$ such that the two coordinate projection maps carry $\mathcal{A}_0$ *onto* $\mathcal{B}$ and $\mathcal{C}$ respectively. In other words, every element of B is used as a coordinate in A_0 and so is every element of C. A heuristic picture is given in Figure **??**.

[1]Such a basis argument requires the Axiom of Choice, but there are similar examples that do not. See Problem E-**??** and Problem E-**??**.

More generally, the same definition applies for a subalgebra of a direct product over any index set: $\mathcal{A} \subseteq \Pi_{\gamma\in\Gamma}\mathcal{B}_\gamma$, projection onto each factor.

You can see one virtue of subdirect products: $\mathcal{A}$ is obtained from $\mathcal{B}$ and $\mathcal{C}$, but also you can get from $\mathcal{A}$ back to $\mathcal{B}$ and $\mathcal{C}$ by taking homomorphic images.

Often we say that $\mathcal{A}$ "is" a subdirect product of some other algebras when we really mean that $\mathcal{A}$ is isomorphic to such a subdirect product.

3. Subdirect representations

Usually we want to use subdirect products "up to isomorphism".

3.1 *Definition.* A *subdirect representation* of an algebra $\mathcal{A}$ is an embedding $\mathcal{A} \hookrightarrow \prod_{\gamma\in\Gamma}\mathcal{B}_\gamma$ whose image is a subdirect product.

For example, a three-element chain (as a distributive lattice) has a subdirect representation as a subdirect product of two two-element chains, as in Figure **??**.

Figure 2: Subdirect representation of a 3-element chain

4. Subdirectly irreducible algebras

A subdirect product is said to be *trivial* if one of the coordinate projections is one-to-one, so that it is an isomorphism from $\mathcal{A}_0$ onto one of the factors.

Similarly, a subdirect representation of $\mathcal{A}$ is said to be *trivial* if the image is a trivial subdirect product of the factors. In that case, the factor is isomorphic to $\mathcal{A}$.

4.1 *Definition.* An algebra $\mathcal{A}$ is *subdirectly irreducible* (SI) if $|A| > 1$ and all subdirect representations of $\mathcal{A}$ are trivial.

4.2 *Theorem* (*Subdirect Representation Theorem*) Every algebra is isomorphic to a subdirect product of subdirectly irreducible algebras.

For example, every distributive lattice is a subdirect product of two-element chains. (See Application **??** below.)

5. The internal point of view

5.1 *Observation.* If $\mathcal{A}$ has two congruence relations θ_1 and θ_2 with $\theta_1 \cap \theta_2 = 0$, then $\mathcal{A}$ has a subdirect representation $\mathcal{A} \hookrightarrow \mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$.

The reason is that the two natural homomorphisms of $\mathcal{A}$ onto $\mathcal{A}/\theta_i$ $(i = 1, 2)$ give a homomorphism of $\mathcal{A}$ into the direct product with kernel $\theta_1 \cap \theta_2 = 0$, so the homomorphism is an embedding. Composing with the projections gives back the natural homomorphisms, so this is a subdirect product.

More generally, if $\mathcal{A}$ has congruence relations $\theta_\gamma, \gamma \in \Gamma$ with $\cap_\gamma \theta_\gamma = 0$, then $\mathcal{A}/\cap_{\gamma\in\Gamma}\theta_\gamma \hookrightarrow \prod_{\gamma\in\Gamma} A/\theta_\gamma$.

5.2 *Observation.* Up to isomorphism, *any* subdirect representation of $\mathcal{A}$ is the same as an appropriate subdirect representation of the form given in Observation **??**.

The reason: Given a subdirect representation $\phi : \mathcal{A} \hookrightarrow \prod_{\gamma\in\Gamma} \mathcal{B}_\gamma$, let $\mathcal{A}' = \phi(\mathcal{A})$, the image of ϕ. Then for each $\gamma \in \Gamma$, the coordinate projection π_γ takes $\mathcal{A}'$ onto $\mathcal{B}_\gamma$ with some kernel θ_γ. The intersection of these kernels is the 0 congruence relation, since in any product two elements are equal when their projections on all factors are the same. Moreover, by the first isomorphism theorem, $\mathcal{B}_\gamma \cong A'/\theta_\gamma$. The mappings

$\mathcal{A} \hookrightarrow \prod_{\gamma\in\Gamma} \mathcal{B}_\gamma \stackrel{\pi_\gamma}{\to} \mathcal{B}_\gamma$

become

$\mathcal{A}' \hookrightarrow \prod_{\gamma\in\Gamma} \mathcal{A}'/\theta_\gamma \stackrel{\pi_\gamma}{\to} \mathcal{A}'/\theta_\gamma$, up to isomorphism.

5.3 *Proposition.* The following conditions are equivalent:

(1) $\mathcal{A}$ is subdirectly irreducible;

(2) $\cap_{\gamma\in\Gamma}\theta_\gamma = 0$ implies $\theta_\gamma = 0$ for some $\gamma \in \Gamma$;

(3) $0 \in \mathrm{Con}(\mathcal{A})$ is completely meet irreducible;

(4) $\mathrm{Con}(\mathcal{A})$ has a least element > 0 (the *monolith* of $\mathcal{A}$).

This gives an internal description of subdirect irreducibility.

6. The proof of the subdirect representation theorem

6.1 *Lemma.* Given $a \neq b$ in $\mathcal{A}$, there exists a congruence relation θ maximal with respect to the property $a \not\equiv b\ (\theta)$.

Proof. Let $\mathcal{S} = \{\theta \in \mathrm{Con}(\mathcal{A}) : \langle a, b\rangle \notin \theta\}$. Then $\mathcal{S}$ is not empty, since $0 \in \mathcal{S}$. Suppose $\mathcal{C}$ is a chain of members of $\mathcal{S}$, where each relation is regarded as a subset of $\mathcal{A}\times\mathcal{A}$. Then $\bigcup_{\theta\in\mathcal{C}} \theta \in \mathcal{S}$, since all aspects of being in $\mathcal{S}$ (specifically, being an equivalence relation, being compatible with the operations of $\mathcal{A}$, and

not containing $\langle a, b\rangle$) can be checked using finitely many elements at a time and so can be checked inside just one member of $\mathcal{C}$ at a time. Then by Zorn's Lemma, $\mathcal{S}$ has a maximal member. $\square$

Let θ_{ab} be one such congruence relation maximal with respect to not identifying a and b. Here θ_{ab} is in contrast to $\mathrm{con}(a, b)$, the smallest congruence relation that identifies a and b. In fact, θ_{ab} can be described as a θ maximal with respect to the property $\theta \not\geq \mathrm{con}(a, b)$.

6.2 *Observation.* For $a \neq b$ in $\mathcal{A}$, in $\mathrm{Con}(\mathcal{A})$ there is a least element $> \theta_{ab}$, namely $\theta_{ab} \vee \mathrm{con}(a, b)$.

6.3 *Observation.* $\mathcal{A}/\theta_{ab}$ is subdirectly irreducible. Indeed, by Observation 1 and the Correspondence Theorem, $\mathrm{Con}(\mathcal{A}/\theta_{ab})$ has a least element > 0 and so is subdirectly irreducible.

6.4 *Observation.* $\bigcap_{a\neq b} \theta_{ab} = 0$ in $\mathrm{Con}(\mathcal{A})$, where a, b range over $\mathcal{A}$.

Proof of the Representation Theorem. By Observation **??** we have $\mathcal{A} \hookrightarrow \prod_{a\neq b} \mathcal{A}/\theta_{ab}$, and by Observation **??** each $\mathcal{A}/\theta_{ab}$ is subdirectly irreducible.

7. An application

7.1 **Application.** It is easy to show that the only subdirectly irreducible distributive lattice is **2**. Consequences:

(i) Every distributive lattice is a subdirect product of copies of **2**.

(ii) The variety of distributive lattices is the same as $\mathrm{Var}(\mathbf{2})$.

(iii) Every distributive lattice L can be represented as a lattice of subsets of some set (perhaps not all subsets), with operations $\cup, \cap$.

8. Problems

Problem E-1. Prove Proposition **??**.

Problem E-2. Represent the 1-unary algebra $\langle \mathcal{A}; f\rangle$ explicitly as a subdirect

product of SI algebras, where $\mathcal{A}$ has diagram

Problem E-3. Let L be a distributive lattice and let $a \in L$. Define $\phi_{\wedge a} : L \to L$ by $\phi_{\wedge a}(x) = x \wedge a$ and likewise $\phi_{\vee a}$ by $\phi_{\vee a}(x) = x \vee a$. As you know, these are lattice homomorphisms.

(a) Show that $\ker \phi_{\wedge a} \cap \ker \phi_{\vee a} = 0$. (Make a one-line proof based on the absorption law for lattices.)

(b) What embedding does (a) give?

(c) Show that the only SI distributive lattice is **2**. (Thus this fact is very elementary. The subdirection representation theorem then says that every distributive lattice is a subdirect product of copies of **2**, a deeper fact that depends on the Axiom of Choice.)

Problem E-4. Say how to represent the group $F_{Q_8}(2)$ as a subdirect product of subdirectly irreducible groups, using as few factors as possible, by referring to the diagram of its normal subgroups.

Problem E-5. (a) Which finite abelian groups are SI? (Use any facts you know about finite abelian groups and their subgroup diagrams. An SI abelian group has a smallest proper subgroup.)

(b) Find all SI abelian groups, finite and infinite. (They can be described as subgroups of the circle group—the multiplicative group of all complex numbers of absolute value 1.)

Problem E-6. (a) Show that an SI 1-unary algebra has no "fork", i.e., distinct elements a, b, c with $c = f(a) = f(b)$.

(Method: Let $\langle a \rangle$ denote the subalgebra generated by a, and similarly for b. For a subalgebra S of $\mathcal{A}$ let θ_S mean the congruence relation obtained by collapsing S to a point. Show that $\theta_{\langle a \rangle} \cap \theta_{\langle b \rangle} \cap \mathrm{con}(a, b) = 0$ if a, b give a fork. You may use the fact that $\mathrm{con}(a, b)$ is obtained by first identifying $f^i(a)$ with $f^i(b)$ for each i and then seeing what equivalence relation that generates.)

(b) Using (a), try to find all finite SI 1-unary algebras whose diagram is connected.

(A useful observation: In an n-cycle, you get exactly the same congruences as for the abelian group $\mathbf{Z}_n$, so the congruence lattice of an n-cycle is isomorphic to Subgroup($\mathbf{Z}_n$).)

Problem E-7. Show that the finite SI 1-unary algebras are

(i) The algebra consisting of two fixed points,

(ii) the "cyclic" 1-unary algebras $\mathcal{C}_{p^k}$ of prime power order (with $k \geq 1$),

(iii) the algebras $\mathcal{D}_k, f$ where $\mathcal{D}_k = \{0, \ldots, k\}$ and $f(0) = 0$, $f(i) = i - 1$ for $i > 0$.

(iv) the two-component algebras where one component is a fixed point and the other is of kind (ii).

(In (ii), it is handy to make this observation, which you may justify very briefly: The congruence relations on an n-cycle regarded as a 1-unary algebra are exactly the same as those on the cycle regarded as the group or ring $\mathbf{Z}_n$. In all parts, you may justify briefly why these *are* SI; it is most important to explain why any finite SI must be of one of these forms.)

Problem E-8. Consider the ring $\mathcal{A} = \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \ldots$, the "direct sum" of countably many copies of the ring $\mathbf{Z}_2$, or in other words, the subring of $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \ldots$ consisting of the sequences that have only finitely many nonzero entries.

(a) Index the direct sum using $\omega = \{0, 1, 2 \ldots\}$. Show that the ideals of $\mathcal{A}$ correspond to subsets of ω.

(b) Show that if $\mathcal{A} \equiv \mathcal{B} \times \mathcal{C}$, then at least one of $\mathcal{B}$ and $\mathcal{C}$ is isomorphic to $\mathcal{A}$. (Method: $\mathcal{A}$ would be the internal direct sum of corresponding ideals I, J, so that $I \cap J = (0)$ and $I + J = A$.)

(c) Show that $\mathcal{A}$ is not the direct product of directly indecomposable algebras. (Use a cardinality argument.)

Problem E-9. (a) Show that direct-product decompositions of a commutative ring with 1 into two factors correspond to idempotents (elements e with $e^2 = e$).

(b) Let R be the ring of all ω-indexed sequences of zeros and ones that are "eventually constant", with sequences added and multiplied using the operations of Z_2 as a ring. Find all direct-product decompositions of R.

(c) In (b), does R have a direct decomposition into directly indecomposable factors? (Why or why not?)

(d) What about the Boolean algebra $\mathrm{Pow}_{fin}(X)$ for countably infinite X?

Problem E-10. Suppose that $\mathcal{A}$ is a finite algebra. An interesting question is whether $\mathrm{Var}(\mathcal{A})$ contains finite SI algebras larger than $\mathcal{A}$, or even contains an infinite SI algebra. If $\mathcal{A}$ is a lattice, for example, there are no larger SI's; if $\mathcal{A}$ is a nonabelian p-group, the answer is that there are arbitrarily large finite SI's and also infinite ones. An easy case:

(a) Show that Shallon's algebra is SI, and in fact is simple. (Method: Think about $\mathrm{con}(r, s)$ for different possible distinct elements r, s.)

More generally, Let $\mathcal{A}_n$ be the graph algebra based on a graph like Shallon's but with n nodes, so that $\mathcal{A}_n$ has $n+1$ elements and Shallon's algebra is $\mathcal{A}_3$. Show that $\mathcal{A}_n$ is SI.

(b) Show that $\mathcal{A}_n \in \mathrm{Var}(\mathcal{A}_3)$. (Suggestion: Write $\mathcal{A}_3 = \{a_1, a_2, a_3, 0\}$. Inside $\mathcal{A}_3^n$, let B be the subalgebra generated by elements whose entries are a_1's (zero or more), then one a_2, and then the rest a_3's. Let θ on B be the equivalence relation obtained by identifying all elements of B that have an entry of 0 and letting other blocks be singletons. Show that θ is a congruence relation on B. Then $B/\theta \cong \ldots$.)

(c) Can you find an infinite SI in $\mathrm{Var}(\mathcal{A}_3)$?

Mal'tsev conditions

1. The idea

Based on a theorem of Mal'tsev discussed below, a "Mal'tsev condition" is any condition on a variety that is can be characterized using the existence of terms obeying laws of some sort[1]. Some typical examples are

- V is *congruence-permutable.* In other words, for any $\mathcal{A} \in V$ and any $\theta, \psi \in \mathrm{Con}(A)$, we have $\theta\psi = \psi\theta$.

  Examples: The variety of all groups; the variety of all rings.

- V is *congruence-distributive.* In other words, for any $\mathcal{A} \in V$, $\mathrm{Con}(A)$ is a distributive lattice.

  Example: The variety of all lattices; the variety of all Boolean algebras.

- V is *congruence-modular.* In other words, for any $\mathcal{A} \in V$, $\mathrm{Con}(A)$ is a modular lattice.

  Since the distributive law implies the modular law, any congruence-distributive variety is also congruence-modular. Also, we have:

  Proposition. Any congruence-permutable variety is congruence-modular.

- V is *arithmetic* ("arithmet′ic"). This means that V is both congruence-permutable and congruence-distributive.

  Example: The variety of rings generated by a finite field.

A relevant kind of term: A ternary term $m(x, y, z)$ is said to be a *majority term* for a variety V if V has the laws

$m(x, x, y) = x$, $m(x, y, x) = x$, $m(y, x, x) = x$.

2. Some theorems showing Mal'tsev conditions

2.1 Theorem (Mal'tsev) For a variety V, the following are equivalent:

(a) V is congruence-permutable (i.e., $\theta\phi = \phi\theta$ in congruence lattices of algebras in V);

(b) there is a term $p(x, y, z)$ such that in V these laws hold:

$p(x, x, z) = z$,

$p(x, z, z) = x$.

[1] Mal'tsev, also transliterated Mal'cev, was a famous Russian algebraist.

2.2 Theorem (Pixley) For a variety V, the following are equivalent:

(a) V is arithmetic;

(b) there are terms $p(x, y, z)$ and $m(x, y, z)$ such that in V, p obeys Mal'tsev's laws of (1b) and m is a majority term;

(c) there is a term $q(x, y, z)$ such that in V,

$q(x, x, z) = z$ (minority),

$q(x, z, z) = x$ (minority),

$q(x, y, x) = x$ (majority).

2.3 Theorem (Jónsson) For a variety V, the following are equivalent:

(a) V is congruence-distributive;

(b) for some $n \geq 2$, there are terms $t_0, \ldots, t_n$ in x, y, z such that in V,

(i) $t_0(x, y, z) = x$, $t_n(x, y, z) = z$;

(ii) $t_i(x, y, x) = x$, for all i;

(iii) $t_i(x, x, z) = t_{i+1}(x, x, z)$ for i even, $t_i(x, z, z) = t_{i+1}(x, z, z)$ for i odd.

(Notice that the case $n = 2$ is equivalent to the existence of a majority term.)

2.4 Theorem (Day, Gumm) For a variety V, the following are equivalent:

(a) V is congruence-modular;

(b) for some $n \geq 0$, there are terms $t_0, \ldots, t_n$ and p in x, y, z such that in V,

(i) $t_0(x, y, z) = x$

(ii) $t_i(x, y, x) = x$, for all i;

(iii) $t_i(x, z, z) = t_{i+1}(x, z, z)$ for i even, $t_i(x, x, z) = t_{i+1}(x, x, z)$ for i odd.

(iv) $t_n(x, z, z) = p(x, z, z)$,

(v) $p(x, x, z) = z$.

3. Problems

Problem F-1. Prove Mal'tsev's theorem.

Problem F-2. Prove Pixley's theorem.

Problem F-3. (a) Another Mal'tsev condition: Show that the following are equivalent for a variety V:

• V has a majority term;

• meets of congruences distribute over composition: $\alpha \cap (\beta\gamma) = (\alpha \cap \beta)(\alpha \cap \gamma)$.

(b) Use (a) to show that a variety with a majority term is congruence-distributive (the case $n = 2$ of Jónsson's theorem).

Jónsson's Lemma

1. A finite version

Theorem. (Foster) Let A be a finite algebra such that $\mathrm{Var}(A)$ is congruence-distributive. Let $B \in \mathrm{Var}(A)$ be finite and subdirectly irreducible. Then $B \in \mathbf{HS}(A)$.

Corollary. Under the same hypotheses, $|B| \leq |A|$, and if $|B| = |A|$ then $B \cong A$.

Example. Each of the lattices M_3, N_5 satisfies a law that fails in the other.

Proof of the theorem: $\mathrm{Var}(A) = \mathbf{HSP}(A)$, so represent B as a homomorphic image of a subalgebra C of $A \times \cdots \times A$: $C \subseteq A \times \cdots \times A$ and $\phi : C \to B$ (a surjection). Here we know a finite product will do since B is the image of a free algebra $\mathrm{Var}_A(n)$, where $n = |B|$, and such a free algebra can be constructed by the table method. See the left-hand side of Figure **??**.

$$\begin{array}{ccccccc} C \subseteq A \times \cdots \times A & & & & & S_{i_0} \subseteq A \\ \phi \quad \pi_1 \quad \pi_n & & & \text{gives} & & \psi \\ B \quad A \quad A & & & & & B \end{array}$$

Figure 1: Mappings for the Theorem of §1.

Focus on $\mathrm{Con}(C)$. One of its elements is $\ker \phi$, which by the Correspondence Theorem is meet-irreducible. Some other elements are the kernels of the coordinate projections restricted to C: $\ker(\pi_i|_C)$. Of course $\pi_i|_C$ may not map C onto A; its image is some subalgebra S_i of A.

Observe that

$$\cap_i \ker(\pi_i|_C) = 0 \leq \ker \phi.$$

Recall that in a distributive lattice, a meet-irreducible element is meet-prime. Therefore $\ker(\pi_{i_0}|_C) \leq \ker \phi$ for some i_0. This says that $\pi_{i_0}(a) = \pi_{i_0}(a') \Rightarrow \phi(a) = \phi(a')$. Therefore a well defined map ψ of the image of S_{i_0} onto B is obtained by setting $\psi(\pi_{i_0}(a)) = \phi(a)$. This map is the desired homomorphism showing that $B \in \mathbf{HS}(A)$. See the right-hand side of Figure **??**. □

2. Ultrafilters

Consider the set $I = \omega = \{0, 1, 2, \dots\}$, the lattice $\mathrm{Pow}(I)$, and its ideals and dual ideals (filters). A principal ideal consists of the family of all subsets of some given set. Some examples to think about:

- The principal ideal generated by $I \setminus \{k\}$ is maximal, for each k.
- Its complement is the principal dual ideal ("principal ultrafilter") consisting of all subsets containing $\{k\}$.
- The ideal I_0 of all finite subsets is not principal.
- However, the ideal I_0 of all finite subsets is the intersection of maximal ideals (as is any ideal). These are the *nonprincipal* maximal ideals. There are $2^{2^{\aleph_0}}$ of them, but it is impossible to give even one explicitly!

Given a maximal ideal, we think of its members as "small" subsets of I. What is a "large" subset? There are two possible definitions:

(1) A large subset is a subset that is not small;

(2) a large subset is the complement of a small subset.

But these two definitions are equivalent! Recall that for a maximal ideal of a Boolean lattice, for each x exactly one of x or x' is in the ideal.

Question. For the principal maximal ideal generated by $I\setminus\{k\}$, which subsets of I are small and which large? (It is as if only k counts for largeness.)

To summarize,

1. Every subset of I is either large or small (not both).
2. The empty set is small. In fact, if the maximal ideal is nonprincipal, then any finite subset is small.
3. I itself is large.
4. The union of two small subsets is small.
5. The intersection of two large subsets is large.
6. A subset of a small subset is small.
7. A superset of a large subset is large.
8. The small sets form a maximal ideal.
9. The large sets form an ultrafilter.

3. Ultraproducts

An "ultraproduct" of algebras is their direct product modulo an congruence relation constructed from a nonprincipal ultrafilter. The congruence relation tends to collapse the product down to something that looks like a "generic" copy of the individual algebras, reflecting whatever features they have in common.

The construction is set-theoretic and actually works for sets with relations as well as for algebras. In detail:

Definition. Let I be an infinite index set. Let algebras $A_i, i \in I$ be given. Choose a nonprincipal ultrafilter $\mathcal{U}$ on I. On the direct product $\prod_{i\in I} A_i$, define an relation $\equiv$ by saying $\mathbf{a} \equiv \mathbf{b}$ when $\mathbf{a}$ and $\mathbf{b}$ agree on a large set of indices. The *ultraproduct* of the A_i is the direct product modulo $\equiv$:

$$A^* = (\textstyle\prod_{i\in I} A_i)/\equiv, \text{ or more simply } A^* = \prod_{i\in I} A_i/\mathcal{U}.$$

There are several things to consider here:

- Does the phrase "agree on a large set of indices" mean that there is *some* large set $J \subseteq I$ of indices such that $a_j = b_j$ for all $j \in J$, or that the set of *all* $i \in I$ with $a_i = b_i$ is large? By the properties of large sets, it doesn't matter; the meanings are the same.
- It must be checked that $\equiv$ is an equivalence relation. This follows from the properties of large sets.
- We say "the" ultraproduct even though the result does depend on the choice of $\mathcal{U}$.

Ultraproducts have some startling properties:

1. Any n-ary relation common to the A_i has a reasonable definition on their ultraproduct.
2. Any first-order sentence true in the A_i is true in their ultraproduct. (This extends to first-order formulas.)
3. An ultraproduct of fields is a field. (Why?)
4. The ultraproduct is unchanged if finitely many factors are omitted. (Why?)
5. If all the A_i are finite and isomorphic, then A^* is a copy of the same algebra. (Why?)

Examples.

(a) The ultraproduct of countably many copies of the field $\mathbf{R}$ of reals is the field $\mathbf{R}^*$ of "nonstandard reals". It is possible to do calculus using "infinitesimals" in $\mathbf{R}^*$.

(b) The ultraproduct of countably many copies of the ring $\mathbf{Z}$ of integers is the ring $\mathbf{Z}^*$ of "nonstandard integers". Some of them are "infinite".

(c) The ultraproduct $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \times \cdots / \mathcal{U}$ is a field of characteristic 0.

(d) The ultraproduct of chains $\mathbf{1} \times \mathbf{2} \times \mathbf{3} \times \cdots / \mathcal{U}$ is an infinite chain. (What does it look like?)

4. Jónsson's Lemma

"Jónsson's Lemma" would be called a theorem by most people, but it was called a lemma in the original paper and the name has stuck.

For a class $\mathcal{K}$ of similar algebras, let $\mathbf{U}(\mathcal{K})$ denote the class of algebras isomorphic to ultraproducts of algebras in $\mathcal{K}$ [1].

Theorem. (Jónsson's Lemma) Let $\mathcal{K}$ be a class of similar algebras such that $\mathrm{Var}(\mathcal{K})$ is congruence-distributive. If $B \in \mathrm{Var}(\mathcal{K})$ is subdirectly irreducible, then $B \in \mathbf{HSU}(\mathcal{K})$.

Corollary. For a finite algebra A, if $\mathrm{Var}(A)$ is congruence-distributive, then for each subdirectly irreducible algebra $B \in \mathrm{Var}(A)$ we have $B \in \mathbf{HS}(A)$.

Notice that this Corollary is a little stronger than the Theorem of §1, since it is not assumed to start with that B is finite. The conclusion is the same.

5. Problems

Problem G-1. How can we be sure that an ultraproduct of chains is a chain?

Problem G-2. Prove the Corollary of §**??** from Jónsson's Lemma.

Problem G-3. Let $\mathbf{F}_4$ be the Galois field of 4 elements. Find all the SI members of $\mathrm{Var}(\mathbf{F}_4)$, up to isomorphism.

[1] Most authors write $\mathbf{P}_U$, following Jónsson, and some omit the use of isomorphic copies.