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.

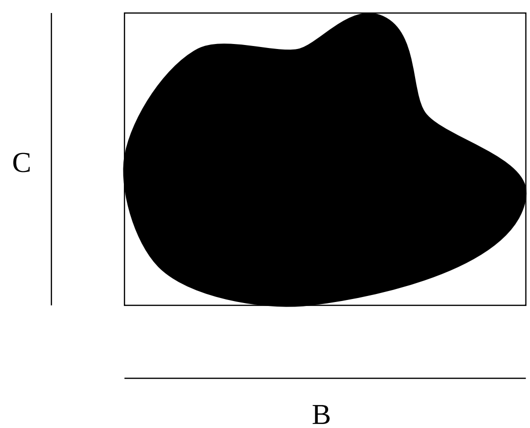

Figure 1: A subdirect product, heuristically

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.

[1]Such a basis argument requires the Axiom of Choice, but there are similar examples that do not. See Problem AA-8 and Problem AA-9.

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 2.

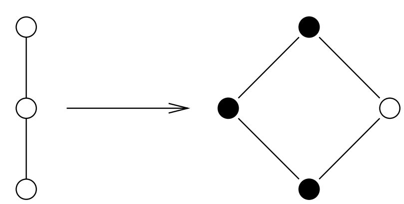

Figure 2: Subdirect representation of a 3-element chain

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 7.1 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 5.1.

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 $a \not\equiv b$ (θ).

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 $\operatorname{con}(a, b)$, 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 $\theta \not\geq \operatorname{con}(a, b)$.

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

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

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

Proof of the Representation Theorem. By Observation 6.4 we have $\mathcal{A} \hookrightarrow \prod_{a\neq b} \mathcal{A}/\theta_{ab}$, and by Observation 6.3 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 $\mathbf{2}$. Consequences:

(i) Every distributive lattice is a subdirect product of copies of $\mathbf{2}$.

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

(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 AA-1. Prove Proposition 5.3.

Problem AA-2. Represent the 1-unary algebra $\langle \mathcal{A}; f\rangle$ explicitly as a subdirect product of SI algebras, where $\mathcal{A}$ has the diagram of Figure 3.

Problem AA-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.)

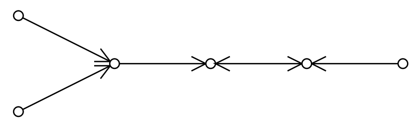

Figure 3: A 1-unary algebra

(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 AA-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 AA-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) Show that the group $\mathbf{Z}$ of integers is not SI.

(c) Show that every nontrivial subgroup of an SI abelian group, finite or finite, is also SI.

(d) Show that any infinite SI abelian group G is isomorphic for some prime p to $\mathbf{Z}_{p^\infty}$, which can be described up to isomorphism as the subgroup of the circle group (the group of complex numbers of absolute value 1) consisting of elements $\{e^{2\pi r} : r = \frac{k}{p^n}\}$.

Problem AA-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 $\mathrm{Subgroup}(\mathbf{Z}_n)$.)

Problem AA-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 AA-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 AA-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 AA-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 (and in fact, simple if $n \neq 2$).

(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 $\mathrm{Var}(\mathcal{A}_3)$?

Problem AA-11. In the proof of Lemma 6.6.1, θ_{ab} is maximal with respect to not identifying a and b. Does every completely meet-irreducible congruence have this form? In other words, if θ is c.m.i. in $\mathrm{Con}(A)$, do there exist $a, b \in A$ with $a \neq b$ such that θ is maximal with respect to not identifying a and b? (As usual, the top element is not considered c.m.i.)