ORDERED ALGEBRAIC STRUCTURES
SYNOPSIS OF A COURSE AT OU, WINTER SEMESTERS 2017/2018 AND 2018/2019

PASHA ZUSMANOVICH

CLASS 1. ALGEBRAIC STRUCTURES, SUBSTRUCTURES, AUTOMORPHISMS. ORDERS (OCTOBER 4, 2018)

Literature: [BS, Chap.I,§1, Chap.II,§§1,2]; [B, §§1.1,1.2,2.1]; [M, §§1.4,1.5,2.2,2.3].

The basic structures in mathematics are: algebraic, topological, and ordered structures. Combinations of these leads to various branches of mathematics.

Definition of an algebraic structure. Notion of a substructure of an algebraic structure.

Definition of order; partial and total (= linear) orders.

Examples: $(\mathbb{N},\le)$, $(\mathbb{Z},\le)$, $P(X)$ (set of subsets of the given set X). The latter order is total if an only if $|X| \le 1$.

Cartesian product of orders: if $(X_i,\le)$ are orders, $i = 1,\dots,n$, then the order $X_1 \times \dots \times X_n$ is defined as $(x_1,\dots,x_n) \le (y_1,\dots,y_n)$ iff $x_i \le y_i$ for any $i = 1,\dots,n$. This order is not total except degenerate cases ($|X_i| \le 1$). For example, complex numbers, considered as pairs of real numbers, may be ordered this way.

Examples of algebraic structures:

(i) $(\mathbb{N},\mapsto)$, where $\mapsto$ is the unary function $n \mapsto n+1$. All substructures are of the form $\{n, n+1, n+2, \dots\}$ for some n.
(ii) A dynamical system: (X, f), for unary $f : X \to X$.
(iii) $(C^\infty(\mathbb{R}), \frac{d}{dx}, +, \cdot)$, where $+$ and $\cdot$ are pointwise addition and multiplication of functions. Examples of substructures: polynomials; functions of the form $a_1e^{b_1x} + \dots + a_ne^{b_nx}$, where $a_i, b_i \in \mathbb{R}$.
(iv) $(M_n(\mathbb{R}), t)$, where $t(A,B,C) = ABC$.
(v) A "circular" variant of (i): $(\{1,2,3,4\},\mapsto)$, where $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$. There are no proper substructures.
(vi) Small structures with operations of small arity can be given by "multiplication" tables.

Theorem 1.1. *The intersection of any number of substructures of an algebraic structure is a substructure.*

Notions of homomorphism, isomorphism, automorphism.

Example of isomorphism: $(\mathbb{R},+) \simeq (\mathbb{R}_{>0},\cdot)$, where isomorphism is provided by $x \mapsto e^x$.

Theorem 1.2. *Automorphisms of an algebraic system form a group.*

Example: automorphisms of the structure from Example (v) form the cyclic group $\mathbb{Z}/4\mathbb{Z}$.

CLASS 2. CONGRUENCES. HOMOMORPHISM THEOREMS (OCTOBER 11, 2018)

Literature: [BS, Chap.II, §§5,6]; [B, §§1.5,3.1]; [M, §§2.4,3.3,4.1].

Refresher: equivalence relation, equivalence classes.

Definition of congruence. Congruences for groups amount to normal subgroups, and congruences for rings amount to ideals.

Any algebraic structure X has trivial congruences: the minimal one – the diagonal $\Delta(X) = \{(x,x) \mid x \in X\}$, and the maximal one – the whole Cartesian product $X \times X$.

Date: last modified December 28, 2018.

Definition 2.1. If $\varphi : X \to Y$ is a homomorphism of algebraic structures (of the same signature), then its kernel, denoted by $\operatorname{Ker}\varphi$, is defined as $\{(a,b) \in X \mid \varphi(a) = \varphi(b)\}$.

Theorem 2.1. *A kernel of homomorphism is a congruence.*

Example. The only nontrivial congruence of the structure (v) from Class 1 is:
$\Delta(x) \cup \{(1,3),(3,1),(2,4),(4,2)\}$.

The First Homomorphism Theorem. *If $\varphi : X \to Y$ is a surjective homomorphism of algebraic structures, then $X/\operatorname{Ker}\varphi \simeq Y$.*

Definition 2.2. If $\alpha \subseteq \beta$ are congruences on an algebraic structure X, then

$$\beta/\alpha \overset{df}{=} \{(x/\alpha, y/\alpha) \in X/\alpha \times X/\alpha \mid (x,y) \in \beta\}.$$

Lemma 2.1. *β/α is a congruence on X/α.*

The Second Homomorphism Theorem. *If $\alpha \subseteq \beta$ are congruences on an algebraic structure X, then $(X/\alpha)/(\beta/\alpha) \simeq X/\beta$.*

Proof. Establish a map $X/\alpha \to X/\beta$, and use the First Homomorphism Theorem. □

Lemma 2.2. *If X is a substructure of, and α is a congruence on an algebraic structure Y, then $\alpha \cap (X \times X)$ is a congruence on X.*

The Third Homomorphism Theorem. *If X is a substructure of, and α is a congruence on an algebraic structure Y, then $X/(\alpha \cap (X \times X))$ is isomorphic to a substructure of Y/α.*

Proof. Establish a map $X/(\alpha \cap (X \times X)) \to Y/\alpha$, prove that it is injective, and use the First Homomorphism Theorem. □

CLASS 3. LATTICES (OCTOBER 18, 2018)

Literature: [BS, Chap.I,§1, Chap.II,§5]; [B, §§1.4,2.1]; [M, §§2.3,5.1]; Wikipedia: *Lattice (order)*.

Notions of supremum and infimum of a subset of an ordered set.

Definition 3.1. A lattice is an ordered set in which any two elements have supremum and infimum (called join and meet, respectively).

Definition 3.2. A lattice is an algebraic structure of the form $(X, \wedge, \vee)$, where $\wedge$ and $\vee$ are binary operations satisfying the following axioms:

(1) both $\wedge$ and $\vee$ are commutative and associative;
(2) (absorption) $a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$.

Equivalence of these two definitions: $1 \Rightarrow 2$: $a \vee b = sup(a,b)$, $a \wedge b = inf(a,b)$.
$2 \Rightarrow 1$: $a \le b$ iff $a = a \vee b$ iff $b = a \wedge b$.

Idempotency in lattices: $a \wedge a = a$, $a \vee a = a$. Follows from absorption, for example: $a \vee a = a \vee (a \wedge (a \vee a)) = a$.

Intersection of congruences on an algebraic structure is a congruence (had to be earlier, when talking about congruences).

Notions of substructure of and congruence on algebraic structure generated by a subset (had to be earlier, when talking about substructures and congruences in arbitrary algebraic structures).

Examples: in an arbitrary lattice, every element generates an one-element sublattice. Every two element generate either two-element totally ordered sublattice, or 4-element "diamond" sublattice D_4, depending whether they are comparable or not.

Any lattice consisting of ≤ 4 elements isomorphic to one of the 5 lattices: a linear order L_1, L_2, L_3, L_4 (consisting of 1, 2, 3, 4 elements respectively), or D_4.

Hasse diagram of a lattice.

Examples: $P(X)$ (the set of all subsets of a set X) forms a lattice; for any $A \subseteq X$, $P(A)$ is a sublattice. The lattice $(\mathbb{N}, |)$ ($|$ means "divides") is isomorphic (through the prime numbers decomposition) to the countable direct power of the lattice $(\mathbb{N}, \leq)$.

Substructures of and congruences on a given algebraic structure form lattices.

Example: the lattice of substructures of the "circular" structure from Class 1, Example (v) is isomorphic to the one-element lattice L_1, and the lattice of its congruences is isomorphic to L_3.

Lattice of congruences of a totally ordered set.

CLASS 4. DISTRIBUTIVE AND MODULAR LATTICES (OCTOBER 25, 2018)

Literature: [BS, Chap.I,§3]; [B, §2.2]; [M, §5.2].

Exercise: Find lattices of sublattices of and congruences on the 4-element diamond lattice D_4.

Answer: Sublattices form a certain 12-element lattice, $Con(D_4) \simeq D_4$.

The question about congruences on the lattice $P(X)$ (for arbitrary X) is a difficult one.

Dual lattice.

Definition 4.1. A lattice L is called distributive if one of the following three equivalent condition holds:

(i) Distributivity of $\vee$ with respect to $\wedge$: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for any $x, y, z \in L$;
(ii) Distributivity of $\wedge$ with respect to $\vee$: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ for any $x, y, z \in L$;
(iii) $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$ for any $x, y, z \in L$;
(iv) $x \vee (y \wedge z) \geq (x \vee y) \wedge (x \vee z)$ for any $x, y, z \in L$.

Lemma 4.1. *In any lattice L, the following holds for any $x, y, z \in L$:*

(i) $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$
(ii) $(x \vee y) \wedge (x \vee z) \geq x \vee (y \wedge z)$

Proof. (i) Since $x \wedge y \leq x$, we have $(x \wedge y) \vee (x \wedge z) \leq x \vee (x \wedge z) = x$ (by absorption). Since $x \wedge y \leq y$ and $x \wedge z \leq z$, we have $(x \wedge y) \vee (x \wedge z) \leq y \vee z$. Hence $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$, as required.

(ii) By duality. □

Proof of equivalences in Definition 4.1. (i) ⇒ (ii)

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee (x \wedge z)) \vee (y \wedge z) \text{ (by absorption)} \\ &= x \vee ((x \wedge z) \vee (y \wedge z)) \text{ (by associativity)} \\ &= x \vee ((z \wedge x) \vee (z \wedge y)) \text{ (by commutativity)} \\ &= x \vee (z \wedge (x \vee y)) \text{ (by (i))} \\ &= x \vee ((x \vee y) \wedge z) \text{ (by commutativity)} \\ &= (x \wedge (x \vee y)) \vee ((x \vee y) \wedge z) \text{ (by absorption)} \\ &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \text{ (by commutativity)} \\ &= (x \vee y) \wedge (x \vee z) \text{ (by (i))}. \end{aligned}$$

(ii) ⇒ (i) By duality.

(i) ⇔ (iii) follows from Fact 4.1(i).

(ii) ⇔ (iv) follows from Fact 4.1(ii) (or by duality). □

Example of distributive lattices: linear orders, $P(X)$.

Example of non-distributive lattice: M_5.

Definition 4.2. A lattice is called modular if one of the following equivalent conditions holds:

(i) $x \leq y \Rightarrow y \wedge (x \vee z) = x \vee (y \wedge z)$;
(ii) $(x \wedge y) \vee (z \wedge y) = ((x \wedge y) \vee z) \wedge y$.

Proof of equivalence in this definition. (i) $\Rightarrow$ (ii) We have $x \wedge y \le y$, hence $y \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (y \wedge z)$, what, up to commutativity, is (ii).

(ii) $\Rightarrow$ (i) If $x \le y$, then $x = x \wedge y$, and the identity (ii) becomes $x \vee (z \wedge y) = ((x \vee z) \wedge y$, what, up to commutativity, is implication in (i). □

Theorem 4.1. *Any distributive lattice is modular.*

Proof. If $x \le y$, then $x \vee y = y$, and $y \wedge (x \vee z) = (x \vee y) \wedge (x \vee z) = x \vee (y \wedge z)$ (by distributivity). □

When checking a lattice for distributivity or modularity, it is enough to consider triples of elements which are all different, and not contain 0 and 1 (the minimal and maximal elements), if they exist.

Exercise: check that the lattice M_5 is modular, and N_5 is not distributive and not modular.

Theorem 4.2. *Let V be a vector space. Then the lattice of subspaces of V is modular.*

Question: whether it is distributive?

Class 5. Distributive and modular lattices (cont.). Complemented lattices. Boolean algebras (November 1, 2018)

Literature: [BS, Chap.I,§3, Chap.IV,§1]; [B, §2.2]; [M, §5.2].

Theorem 5.1. *Let V be a vector space. Then the lattice of subspaces of V is distributive iff* $\dim V = 0$ *or* 1.

Proof. The cases of $\dim V = 0$ or 1 are obvious. Assume $\dim V \ge 2$.

Case 1. The characteristic of the ground field is $\ne 2$. Choose two linearly independent vectors u and v. Then the three one-dimensional vector spaces $\langle u \rangle$, $\langle u+v \rangle$, $\langle u-v \rangle$ provide counterexample to the distributivity:

$$(\langle u-v \rangle + \langle u+v \rangle) \cap \langle u \rangle = \langle u,v \rangle \cap \langle u \rangle = \langle u \rangle,$$

but

$$\langle u-v \rangle \cap \langle u \rangle + \langle u+v \rangle \cap \langle u \rangle = 0+0 = 0.$$

Case 2. The characteristic of the ground field is 2. Over $GF(2)$, the lattices of subspaces of a 2-dimensional space is isomorphic to M_5 which is not distributive. Since enlargement of the vector space, and enlargement of the ground field lead to a bigger lattice, it will be also not distributive, and we are done. □

Dedekind's and Birkhoff's theorems about characterization of modular and distributive lattices in terms of (not) containment of N_5 and M_5.

Proof of the Dedekind theorem.

Another proof of Theorem 4.2 using the Dedekind theorem.

Complemented lattices: definition.

Exercise: Which of the following lattices are complemented: $P(X)$, total order, M_5, N_5. (the latter two lattices show that complement does not have to be unique).

Definition 5.1. A Boolean algebra is a distributive complemented lattice.

Definition 5.2. A Boolean algebra is an algebraic system with two binary operations $\vee$ and $\wedge$, one unary operation $\neg$, and two distinguished elements 0 and 1, satisfying the (highly redundant) system of axioms:

(1) $\neg 0 = 1$, $\neg 1 = 0$;
(2) $\neg\neg x = x$;
(3) $0 \vee x = x$, $0 \wedge x = 0$, $1 \vee x = 1$, $1 \wedge x = x$;
(4) $x \wedge x = x$, $x \vee x = x$;
(5) $\wedge$ and $\vee$ are commutative, associative, and distributive with respect to each other;

(6) (de Morgan laws) $\neg(x \wedge y) = (\neg x) \vee (\neg y)$, $\neg(x \vee y) = (\neg x) \wedge (\neg y)$.

Equivalence of two definitions of Boolean algebras (in a complemented distributive lattice, complements are unique).

Significance of Boolean algebras.

Class 6. Boolean algebras (cont). Direct product (November 8, 2018)

Literature: [BS, Chap.II,§7, Chap.IV,§1]; [B, §§1.3,3.2]; [M, §2.5].

Examples of Boolean algebras: two-element Boolean algebra **2**, P(X).

Exercise: find a 3-element Boolean algebra.

Answer: such Boolean algebras do not exist, because each 3-element lattice is a total order, and

Proposition 6.1. *A Boolean algebra is a total order iff it is isomorphic to* **2**.

Direct product of algebraic systems. In general, unlike in the group case, factors are not necessary subsystems in their direct product. Properties of direct product: commutativity and associativity.

Direct product of linear orders is not a linear order. Direct product of Boolean algebras is a Boolean algebra.

Homomorphism of direct product to factors.

Notion of directly indecomposable algebraic system.

Examples: 4-element "diamond" decomposes as $\mathbf{2} \times \mathbf{2}$; linear orders are directly indecomposable; simple algebraic systems are directly indecomposable.

$P(X) \simeq \mathbf{2}^X$.

Notion of restriction $B|a$ for a Boolean algebra B and $a \in B$.

Homomorphism $B \to B|a$.

Lemma 6.1. *For any Boolean algebra B, and any $a \in B$, $B \simeq B|a \times B|\neg a$.*

Class 7. The Stone theorems. Subdirect irreducibility (November 15, 2018)

Literature: [BS, Chap.II,§§7,8, Chap.IV,§1]; [B, §3.3]; [M, §5.2].

Corollary 7.1. *A Boolean algebra is directly indecomposable iff it is isomorphic to* **2**.

Theorem 7.1 ("The Little Stone Theorem")**.** *Any finite Boolean algebra is isomorphic to $P(X)$ for a finite set X.*

Proof is by induction, using Corollary 7.1 and the fact that $P(X) \simeq \mathbf{2}^X$.

Corollary 7.2. *For two finite Boolean algebras B_1 and B_2, $B_1 \simeq B_2$ iff $|B_1| = |B_2|$.*

Theorem 7.2 ("The Big Stone Theorem")**.** *Any Boolean algebra is a subalgebra of $P(X)$ for some set X.*

An example of an (infinite) Boolean algebra not isomorphic to $P(X)$: the set of all finite and all cofinite subsets of an infinite set X (to finish the proof is a Homework).

Notion of subdirect product.

An equivalent formulation of the Big Stone Theorem: any Boolean algebra is a subdirect power of **2**.

Notion of subdirect irreducibility of an algebraic structure.

Examples of subdirectly irreducible algebraic structures: 2-element structures, simple structures.

A vector space is subdirectly irreducible iff it is of dimension 0 or 1.

A finite abelian group is subdirectly irreducible iff it is isomorphic to a cyclic group of a prime power order.

CLASS 8. PROOF OF THE BIG STONE THEOREM. BOOLEAN RINGS

Literature: [BS, Chap.II,§§6,8, Chap.IV,§§1,2]; [B, §§2.1,3.1,3.3,3.4].

Notion of the interval $[a,b]$ in a lattice.

Theorem: for any algebraic structure A, and any $\theta \in Con(A)$, $[\theta, \nabla_A] \simeq Con(A/\theta)$. Corollary: a quotient of an algebraic structure by a maximal proper congruence is simple.

Criterion of subdirect irreducibility: an algebraic structure A is subdirectly irreducible iff there is a smallest element in $Con(A)\backslash\{\Delta_A\}$. Corollary: any simple algebraic structure is subdirectly irreducible.

Theorem 8.1 (Birkhoff)**.** *Any algebraic structure is a substructure of a direct product of subdirectly irreducible structures.*

Zorn's lemma.

Finish of the proof of the Stone theorem.

Boolean rings. Correspondence Boolean rings ↔ Boolean algebras.

Exercise: Which Boolean rings are fields? Answer: $GL(2)$.

Finite Boolean rings are direct sums of copies of $GF(2)$ (follows from Stone's theorem).

CLASS 9. IDEALS, FILTERS AND ULTRAFILTERS IN BOOLEAN ALGEBRAS

Literature: [BS, Chap.IV,§3], [M, §8.1].

Ideals in Boolean rings lead to ideals in Boolean algebras.

Definition of ideal and filter in a Boolean algebra, their duality.

Examples of filters: cofinite filter in $P(X)$, principal ultrafilter.

Ultrafilters as maximal proper filters.

A filter F in a Boolean algebra B is an ultrafilter iff for any $a \in B$, either $a \in F$, or $\neg a \in F$.

Description of filters on finite Boolean algebras.

CLASS 10. STONE'S DUALITY

Literature: [BS, Chap.IV,§4].

Discussion of homeworks.

Homework 6: to prove that the lattice of normal subgroups of a group is modular is more-or-less routine task, but to describe groups for which this lattice is distributive, is more like a research problem (for example, for a group which is a direct product of n simple groups this lattice is isomorphic to lattice of subsets of an n-element set and hence is distributive).

Boolean (= Stone) topological spaces. Correspondence between Boolean algebras and Boolean spaces.

Lemma 10.1. *Let B be a Boolean algebra, X a subset of B. Then the ideal of B generated by X (= the minimal ideal of B containing X) coincides with*

$$\{b \in B \mid b \le x_1 \vee \cdots \vee x_n, x_1, \ldots, x_n \in X\} \cup \{0\}.$$

For an (easy) proof, see [BS, Chap. IV, Lemma 3.9(a)].

Proof that for a Boolean algebra B, B^* is compact. Let $\{N_a \mid a \in X\}$ be a cover of B^*. Consider the set $\mathscr{I}$ of all proper ideals of B containing X.

Case 1. $\mathscr{I} = \varnothing$. Then the ideal generated by X coincides with B, and by Lemma 10.1, $1 = x_1 \vee \cdots \vee x_n$ for some $x_1, \ldots, x_n \in X$. Let $U \in B^*$ (i.e., U is an ultrafilter of B). Since $1 \in U$, we have $x_i \in U$ for some $1 \le i \le n$, i.e. $U \in N_{x_i}$. Hence $N_{x_1}, \ldots, N_{x_n}$ is a finite (sub)cover of B^*.

Case 2. $\mathscr{I} \ne \varnothing$. Then by Zorn's lemma, X contained in some maximal ideal I of B. Then $U = \neg I$ is an ultrafilter, and $U \cap I = \varnothing$. But then for any $a \in X$, we have $a \in I$, hence $a \notin U$, and $U \notin N_a$, a contradiction with the fact that $\{N_a \mid a \in X\}$ is a cover of B^* □

Proof that the map $B \to B^{**}$, $b \mapsto N_b$, is injective. Let $a, b \in B$, $a \neq b$. Then $(a \vee b) \wedge \neg(a \wedge b) \neq 0$, and there is an ultrafilter U on B such that $(a \vee b) \wedge \neg(a \wedge b) \in U$. But since $a \vee b \geq (a \vee b) \wedge \neg(a \wedge b)$, and $a \vee b \in U$, and hence $a \in U$ or $b \in U$. Similarly, $\neg(a \wedge b) = \neg a \vee \neg b \in U$, and $\neg a \in U$ or $\neg b \in U$, what is equivalent to $a \notin U$ or $b \notin U$. Thus, exactly one of a, b belongs to U, i.e. U lies in exactly one of N_a, N_b, so $N_a \neq N_b$. □

Proof that the map $B \to B^{**}$, $b \mapsto N_b$, is surjective. Let N be a clopen subset of B^*. Then N is a union of a number of N_a's. But since N is a closed subset of a compact space, N is compact, and hence is a union of a finite number of N_a's, say, $N = N_{a_1} \cup \dots \cup N_{a_n} = N_{a_1 \vee \dots \vee a_n}$ (by the lemma proved at the previous class). □

References

[B] C. Bergman, *Universal Algebra*, CRC Press, 2012.

[BS] S. Burris and H.P. Sankappanavar, *A Course in Universal Algebra*, The Millennium Edition.

[M] A.I. Mal'cev, *Algebraic Systems*, Springer, 1973.

Email address: pasha.zusmanovich@gmail.com