# MSe1

## The aim of these lectures.

**(1)** Recapitulation of structures the students have met so far and pointing out their similarities and differences.

**(2)** Introduction to study of some[1] structures the students will need later: partially ordered sets and related structures, basics of universal algebra and basics of topology.

## Examples.

1. Reals $\mathbb{R}$ (in particular, in analysis) were endowed with several structures simultaneously:
   (a) there are algebraic operations: $a + b$, $ab$,
   (b) there is order: $a \leq b$
   (c) $\mathbb{R}$ is also viewed as a space (real line): we consider the distance $d(x, y) = |x - y|$, convergence, continuity.

2. Vector spaces (and linear algebra): a system of operations allowing a rich calculus.

3. Graphs, variously described: vertices and edges, sets and systems of two-elemented subsets, binary relations.

4. Metric spaces, convergence, continuity, special subsets.

**Note** that in mathematical theories we often (in fact, typically) encounter

structures on sets **plus** associated suitable mappings.

These "suitable mappings" are somehow associated with the structure in question. Sometimes it may seem that they are (uniquely) determined by the structure (homomorphisms of algebras as respecting the operations); but they may differ according to needs of that or other problem (homomorphisms

[1] In particular we will consider those that appear as data on a carrier set; this is not always so, of course: one may have several sets linked by a structure – e.g. multigraphs, or automata.

and strong homomorphism of graphs, choosing continuity, uniform continuity or perhaps contractivity of maps between metric spaces, etc.).

# Notation, basic terminology, conventions.

**A mapping** $f : X \to Y$ : the information on the domain $X$ and range $Y$ is included. In set theory, a mapping is usually understood as a subset

$$f \subseteq X \times Y$$

such that for every $x \in X$ there exists precisely one $y \in Y$ such that $xfy$. From such a set $f$ we cannot reconstruct the $Y$ in question, and of course we know nothing about the structures on the $X$ and $Y$ we have in mind. We think, rather, of a situation where there are two objects $X$ and $Y$, with $f$ a symbol replacing a formula assigning elements $y$ of $Y$ to elements $x$ of $X$.

> **Note** that we speak of objects $X, Y$, not just of sets. The structure is included: otherwise we would not be able to speak of properties of maps – consider $X_i$ resp. $Y_i$ metric spaces carried by the sets $X$ resp. $Y$; the same mapping $f : X \to Y$ can be continuous as $f : X_1 \to Y_1$ and discontinuous as $f : X_2 \to Y_2$.

**One-to-one mappings**: mappings for which $x \neq y \;\Rightarrow\; f(x) \neq f(y)$
and **onto mappings**: mappings such that $\forall y \in Y \exists x \in X,\ y = f(x)$.
Both properties are important.

Composition of mappings: the $g \circ f : X \to Z$ defined for $f : X \to Y$ and $g : Y \to Z$ by setting $(g \circ f)(x) = g(f(x))$. We also write $g \cdot f$ or $gf$.

The inverse (mapping) $f^{-1}$: such $g$ that $f \circ g$ and $g \circ f$ are identities.

**Image and preimage:**
For $f : X \to Y$, $A \subseteq X$ and $B \subseteq Y$ we have

$$\begin{aligned} &\text{the } \textit{image} \;\; f[A] = \{f(x) \,|\, x \in A\} \text{ and} \\ &\text{the } \textit{preimage} \;\; f^{-1}[B] = \{x \,|\, f(x) \in B\}. \end{aligned}$$

One obviously always has

$$f[f^{-1}[B]] \subseteq B \quad \text{and} \quad f^{-1}[f[A]] \supseteq A.$$

**Relation:** unary, binary, ternary

$$R \subseteq X,\ X \times X,\ X \times X \times X,$$

etc., $n$-ary, and also relations with infinite arities.

**Convention.** If $R$ is a binary operation we often (and in some cases, for example if $R = \leq$ is an order, typically) write

$$xRy \quad \text{for} \quad (x, y) \in R.$$

A very expedient notation, and a convention:

$$X^A = \{\xi \,|\, \xi : A \to X\}$$

and an *$A$-ary relation*

$$R \subseteq X^A$$

This includes the above mentioned finitary relations:
For instance for binary relations we can view $X \times X$ as $X^{\{0,1\}}$ identifying the mappings $x : \{0, 1\} \to X$ with their "tables" $(x_0, x_1) = (x(0), x(1))$. Similarly in the ternary case we view $X \times X \times X$ as $X^{\{0,1,2\}}$ where $(x_0, x_1, x_2)$ describes the mapping $x(i) = x_i$, etc..

**Homomorphisms** preserve (respect) relations, that is, for instance in the binary case

$f : (X, R) \to (Y, S)$ satisfies the condition

$$(x_0, x_1) \in R \ \Rightarrow\ (f(x_0), f(x_1)) \in S. \qquad (*)$$

Note that if we view the $(x_0, x_1)$ as the mapping $x = (i \mapsto x_i)$ (hence, $x(i) = x_i$) the $(f(x_0), f(x_1))$ represents the map $f \circ x$, and the condition $(*)$ transforms to the expedient

$$\xi \in R \ \Rightarrow\ f \circ \xi \in S$$

which suits well for *homomorphisms* of arbitrary arities $A$ (that is, for $R \subseteq X^A$ and $S \subseteq Y^A$).

A homomorphism $f$ is an *isomorphism* if it has an inverse $f^{-1}$ which is also a homomorphism.

Homomorphisms (resp. isomorphisms) $(X, R) \to (X, R)$ are termed *endomorphisms* (resp. *automorphisms*).

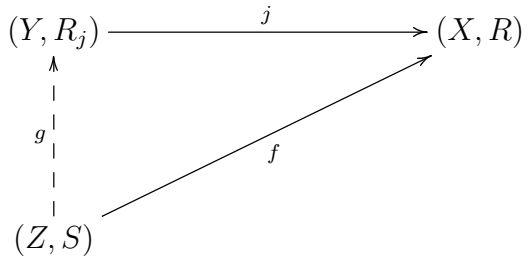
**Subobject.** Let $(X, R)$ be a set with an $A$-ary relation, and $Y \subseteq X$ a subset. The subobject $(Y, R_Y)$ carried by this subset in $(X, R)$ is endowed by the relation

$$R_Y = \{\beta : A \to Y \mid j\beta \in R\};$$

it is the largest $A$-ary relation on $Y$ such that $j : Y \subseteq X$ is a homomorphism.

More generally, a subobject $j : (Y, R_j) \to (X, R)$ is a one-to-one mapping with the relation $R_j = \{\beta : A \to Y \mid j\beta \in R\}$.

**Proposition.** *Let in a commutative diagram*

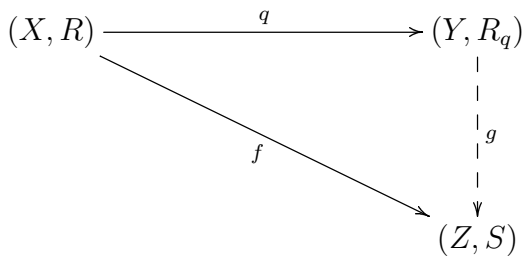



*$j$ is a subobject and $f$ is a homomorphism. Then $g$ is a homomorphism.*

*Proof.* Take an $\alpha : A \to Z$ in $S$. Then $j(g\alpha) = (jg)\alpha = f\alpha \in R$ and hence $g\alpha$ is in $R_j$.

**Quotient (factorobject).** Dually, for $(X, R)$ and an onto mapping $q : X \to Y$ we define $R_q = \{q\alpha \mid \alpha \in R\}$ on $Y$ and obtain the smallest $A$-ary relation on $Y$ such that $q$ is a homomorphism. We speak on $(Y, q)$ as of a quotioent, or a factorobject.

**Proposition.** *Let in a commutative diagram*




*$g$ be a quotient and $f$ a homomorphism. Then $g$ is a homomorphism.*

*Proof.* If $\beta$ (that is, a $q\alpha$ with $\alpha \in R$) is in $R_q$, we have $g\beta = g(q\alpha) = (gq)\alpha = f\alpha$ in $S$.

**Products.** For $(X_i, R_i)$, $i \in J$, define

$$\prod_i (X_i, R_i) = (\prod X_i, R)$$

with $R = \{\alpha : A \to X \mid \forall i, p_i\alpha \in R_i\}$.

Finite products are usually written as $(X_1, R_1) \times (X_2, R_2)$ etc., and the product of a system of the same $(X, R)$ repeated $J$ times is written as power, $(X, R)^J$.

In the standard description, say with two $R_i \subseteq X_i \times X_i$, we have the product relation

$$R = \{((x_1, x_2), (y_1, y_2)) \mid (x_1, y_1) \in R_1, (x_2, y_2) \in R_2\}.$$

This may seem to be more transparent, but it is easier to work with the $X^A$ convention; in bigger arities it is particularly comfortable.

The $R$ in the definition of product is the largest relation on the cartesian product $\prod_J X_i$ such that the mappings

$$p_j : (\prod_J X_i, R) \to (X_j, R_j)$$

are homomorphisms for every $j$. This is important for

**Proposition.** *For every system of homomorphisms $f_i : (Y, S) \to (X_i, R_i)$ there exists precisely one homomorphism*

$$f : (Y, S) \to \prod_J (X_i, R_i)$$

*such that $p_i f = f_i$ for all $i$.*

*Proof.* First we see that there is precisely one *mapping* $f : Y \to \prod_J X_i$ such that $\forall i$, $p_i f = f_i$: if $f$ has this property we have for $f(y) = (x_i)_i$, $x_j = p_j((x_i)_i) = p_j f(y) = f_j(y)$, hence the unicity, and the $f$ defined by $f(y) = (f_i(y))_i$ satisfies the equations $p_i f = f_i$.

Hence we have to prove that this $f$ is a homeomorphism. If $\alpha : A \to Y$ is in $S$ then we have $f_i \alpha \in R_i$ for all $i$, and since $p_i(f\alpha) = (p_i f)\alpha = f_i \alpha$, $f\alpha$ is in $R$.

## Relational systems and objects.

A *type* is a system

$$\Delta = (A_t)_{t \in T}$$

A *relational system of* type $\Delta$ on a set $X$ is a system

$$R = (R_t)_{t \in T} \quad \text{of } A_t\text{-nary relations } R_t \text{ on } X.$$

The pair $(X, R)$ is said to be a relational object (of the type $\Delta$).

Everything that was introduced for individual relations is extended to relational systems considering the individual relations simultaneously for all the indices $t \in T$.

Hence in particular,

- $f : (X, R) \to (Y, S)$ is a homomorphism if all the $f : (X, R_t) \to (Y, S_t)$ are homomorphisms,
- $j : (X, R) \to (Y, S)$ is a subobjects if all the $j : (X, R_t) \to (Y, S_t)$ are subobjects,
- $q : (X, R) \to (Y, S)$ is a quotient if all the $q : (X, R_t) \to (Y, S_t)$ are quotients, and
- in the product $\prod_i (X_i, R^i) = (\prod X_i, R)$ we have $R = (R_t)_{t \in T}$ where the $R_t$ come from the products $\prod_i (X_i, R^i_t) = (\prod X_i, R_t)$ in which the $R^i_t$ constitute the $R^i = (R^i_t)_{t \in T}$ .

**Note.** The students have so far met mostly binary relations, in particular when working with graphs or order. Other arities are also important, though, and relational systems with non-trivial types as well – remember the Constraint Satisfaction Problem which is the task to find, or at least prove the existence or non-existence of, a suitable homomorphism between relational objects of a particular type.

**Next week** we will start to discuss (partially) ordered sets, that is, sets endowed with a special sort of binary relations called (partial) orders.

We will consider *preorders*: relations $R \subseteq X \times X$ that are

- reflexive, that is, one has $xRx$ for all $x \in X$,
- and transitive, that is, $xRy$ and $yRz$ imply $xRz$,

and in particular *(partial) orders* where, moreover,

- $xRy$ and $yRx \quad \Rightarrow \quad x = y$.

The pair $(X, \leq)$ is then termed a (partially) ordered set, briefly a *poset*.

# MSe2

## Preorder and order

A *preorder* is a relation $R \subseteq X \times X$ which is

- reflexive, that is, $xRx$ for all $x \in X$, and
- transitive, that is, $xRy$ and $yRz \;\Rightarrow\; xRz$.

For a *(partial) order* we assume, moreover, that

- $xRy$ and $yRx \quad \Rightarrow \quad x = y$.

A set together with an order $(X, \leq)$ is called a *(partially) ordered set*, briefly a *poset*.
In a *linear order* we assume that :

- $\forall xy$, $xRy$ or $yRx$,

A linearly ordered set is often called a *chain*.

> **Preorders viewed as orders.** On a preordered set $(X, \leq)$ define the equivalence
>
> $$x \sim y \quad \text{iff} \quad x \leq y \text{ and } y \leq x.$$
>
> Then the set of equivalence classes $X/\sim$ ordered by $[x] \leq [y]$ iff $x \leq y$ is a poset. One often works with the $(X, \leq)$ as with a poset tacitly assuming that one has in fact in mind the equivalence classes instead of the elements of $X$.

**A note on terminology.** We will often say just "order" resp. "ordered set" (but never "oset" – "poset" is well established) for the partial case. The linearity, however, will be always emphasized.

The **opposite (dual) order** $\leq^{\mathrm{op}}$ is defined by

$$a \leq^{\mathrm{op}} b \quad \text{iff} \quad b \leq a$$

and we write $X^{\mathrm{op}} = (X, \leq)^{\mathrm{op}} = (X, \leq^{\mathrm{op}})$ for the dually ordered set.

**Notation.** If there is no danger of confusion one often uses the same symbol, usually $\leq$, also for distinct orders (see the definition of monotonicity below). In specific context one uses specific symbols, like the $\subseteq$ for inclusion, or $|$ for divisibility in the examples below. Sometimes it is just necessary to express a distinction, say, using

$$\leq_1, \ , \sqsubseteq, \ \preceq \quad \text{etc.}$$

**Examples.** 1. Numbers (that is, natural numbers, integers, rationals or reals, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$) with the standard order.

2. The set $\mathfrak{P}(X)$ of all subsets of $X$ ordered by inclusion $\subseteq$.

> **Note.** This is a sort of a universal order in the sense that each partially ordered set can be represented as a system of subsets of a set $X$ (typically not as the whole of $\mathfrak{P}(X)$, of course). For $(X, \leq)$ set $\downarrow x = \{y \,|\, y \leq x\}$. Then
>
> $$\downarrow = (x \mapsto \downarrow x) : (X, \leq) \to (\mathfrak{P}(X), \subseteq)$$
>
> is a representation of the poset in which $x \leq y$ iff $\downarrow x \subseteq \downarrow y$.

3. Divisibility: $a|b$ for "$a$ divides $b$": In $\mathbb{N}$ it is an order, in $\mathbb{Z}$ just a preorder; in the system of all real or complex polynomials it is again a preorder, with equivalence classes more complicated than the $\{n, -n\}$ in $\mathbb{Z}$.

4. In the set of words in an alphabet: $w \leq w'$ iff $wv = w'$ for a suffix $v$.

**Monotone maps** $f : (X, \leq) \to (Y, \leq)$ [1] satisfy the condition

$$x \leq y \quad \Rightarrow \quad f(x) \leq f(y).$$

An *isomorphism* (in agreement with the terminology of general relations) is a monotone $f$ such that there is a monotone $g$ such that $fg = \mathrm{id}$ a $gf = \mathrm{id}$.

**Remark.** Do not get confused by the different terminology in calculus where one includes the $f$ with

$$x \leq y \quad \Rightarrow \quad f(x) \geq f(y).$$

Here we will speak in such a case about *antitone* maps.

# Suprema and infima.

An element $x \in (X, \leq)$ is a *lower* (resp. *upper*) *bound* of a subset $M \subseteq X$ if $M \subseteq \uparrow x$ (resp. $M \subseteq \downarrow x$).
The least upper bound of $M$ (if it exists) is called the *supremum* of $M$, denoted

$$\sup M;$$

the largest lower bound of $M$ is called the *infimum* of $M$ and denoted by

$$\inf M.$$

Thus, $s = \sup M$ if

(1) $\forall m \in M,\ m \leq s$ and

(2) $(\forall m \in M, m \leq x) \Rightarrow\ s \leq x.$

**Notes.** 1. A supremum resp. infimum does not have to exist, but if it does, it is uniquely determined.

2. The students may remember that in analysis when dealing with suprema (and similarly with infima) in $\mathbb{R}$ they had the condition (2) replaced by

(2') If $x < s$ then there is an $m \in M$ such that $m > x$.

This is correct in the linearly ordered $\mathbb{R}$, but not generally. See Homework.

[1] Just for getting used to it we use here the convention of the same symbol $\leq$ for possibly, and typically, distinct orders.

**Remarks on notation.** One often writes $\bigvee M$ for $\sup M$, and $\bigwedge M$ for $\inf M$, in particular in posets where the suprema resp. infima generally exist; for finite subsets (again, in particular in posets where *finite* suprema resp. infima exist) we write

$$a \vee b,\ a \wedge b,\ a_1 \vee \cdots \vee a_n, \quad \text{etc.}$$

Sometimes one uses other specific symbols.[2]

**Bottom and top.** A poset may have the least or the largest element. Note that the least element is the same as $\sup \emptyset$; it is often denoted by $\bot$, 0.

Similarly $\inf \emptyset$ is the same as the largest element (which is often denoted by $\top$ or 1).

**Minimal and maximal elements.** An element $x \in (X, \leq)$ is minimal if $y \leq x$ implies that $y = x$. Similarly, $x$ is maximal if $x \leq y$ implies that $x = y$.

This is not to be confused with the least and largest elements. The least element is minimal, but a minimal element is not necessarily the least one. See Homework.

**Examples.** 1. Suprema and infima of sets of real numbers in analysis.

2. In $(\mathfrak{P}(X), \subseteq)$ we have for $\mathcal{A} = \{A_i \,|\, i \in J\}$

$$\sup \mathcal{A} = \bigcup_i A_i, \quad \inf \mathcal{A} = \bigcap_i A_i.$$

3. In the set of all vector subspaces of a vector space $V$, infima are intersections again, suprema are the subspaces generated by the unions.

> Note that the suprema differ from those in $\mathfrak{P}(V)$ althought the order is the same.

4. In $\mathbb{N}$ with $a|b$ ("$a$ divides $b$"), $\sup\{a, b\}$ is the least common multiple of $a$ and $b$ and $\inf\{a, b\}$ is the largest common divisor.

[2] And terminology as well: one speaks of joins resp. meets, or, when in $\mathfrak{P}(X)$, one (naturally) speaks of unions and intersections.

**Observations.** 1. Provided the indicated suprema or infima exist,

$$M \subseteq N \;\Rightarrow\; \sup M \leq \sup N \text{ and } \inf M \geq \inf N.$$

(WHY: every upper resp. lower bound of $N$ is an upper resp. lower bound of $M$.)

2. $M$ is said to be confinal in $N$ if $M \subseteq N$ and for every $x \in N$ there is a $y \in M$ such that $x \leq y$. In such a case, $\sup M$ exists iff $\sup N$ exists, and if they exist they coincide.
(WHY: $M$ and $N$ have the same upper bounds.)

**Proposition.** *We have*

$$\sup\{\sup M_j \,|\, j \in J\} = \sup(\bigcup_{j\in J} M_j),$$
$$\inf\{\inf M_j \,|\, j \in J\} = \inf(\bigcup_{j\in J} M_j)$$

*whenever the left hand sides make sense.*

*Proof.* (Very simple, just to see the role of the left hand side.) We have $s = \sup\{\sup M_j \,|\, j \in J\} \geq \sup M_i \geq m$ for any $m \in \bigcup_{j\in J} M_j$, hence $s$ is an upper bound of $\bigcup_{j\in J} M_j$.

Let $x$ be an upper bound of $\bigcup_{j\in J} M_j$. Then it is an upper bound of each $M_j$, hence for every $j$, $x \geq \sup M_j$, hence it is an upper bound of $\{\sup M_j \,|\, j \in J\}$ and hence $x \geq \sup\{\sup M_j \,|\, j \in J\}$. Thus $\sup\{\sup M_j \,|\, j \in J\}$ is the least upper bound of $\bigcup_{j\in J} M_j$.

**Remark.** The fact is sometimes referred to as the *associative rule* for suprema resp. infima: Note the removal of brackets in

$$a \vee (b \vee c) = a \vee b \vee c = (a \vee b) \vee c.$$

Hence, if in a poset all the $\sup\{a, b\} = a \vee b$ exist, $\vee$ is an associative operation.

## Some special posets.

**Semilattices.** A *lower resp. upper semilattice* has infima resp. suprema of all pairs of its elements. One speaks of a *bounded* semilattice if it has a bottom and top.

> **Observation.** From the associative rule it immediately follows that a lower semilattice has infima of all non-empty finite subsets, and a bounded lower semilattice has infima of all finite subsets.

**Lattices.** A *lattice* has infima and suprema of all pairs of its elements. One speaks of a *bounded* lattice if it has a bottom and top.

> **Observation.** From the associative rule it immediately follows that a lattice has infima and suprema of all non-empty finite subsets, and a bounded lattice has infima and suprema of all finite subsets. similarly for semilattices.

**Complete lattices.** A *a complete lattice* has infima and suprema of all of its subsets.

> **Remark.** Note that unlike in semilattices and lattices this condition includes also the void suprema and infima, that is, the existence of the least and the largest element.

**Theorem.** *A poset is a complete lattice iff each subset has a supremum. Similarly with infima.*

*Proof.* Let us have in $(X, \leq)$ all suprema. We will determine the infimum of an $M \subseteq X$. Set

$$N = \{x \mid M \subseteq \uparrow x\},\ i = \sup N.$$

For every $y \in M$ we have $N \subseteq \downarrow y$ and hence $i \leq y$; thus, $i$ is a lower bound of the set $M$. If $M \subseteq \uparrow x$ then $x \in N$ and hence $x \leq i$ so that $i = \inf M$.

**Directed sets and subsets.** $D \subseteq (X, \leq)$ is *directed*, if every finite $K \subseteq D$ has an upper bound in $D$. Note that in particular it has to be non-void.

(More precisely, one should speak of *up-directed* sets as opposed to the *down-directed* defined with lower bounds, but in applications the up-directed ones somehow prevail.)

**DCPOs.** A DCPO is a poset in which each directed subset has a supremum. This is the fundamental structure of domain theory.

## Dedekind-MacNeille completion.

We have already mentioned the representation of $(X, \leq)$ (replacing $x \in X$ by $\downarrow x \in \mathfrak{P}(X)$) as a subobject of the complete $\mathfrak{P}(X)$.
In fact we have more: if $M \subseteq X$ had an infimum $i$ then $\downarrow i = \bigcap\{\downarrow x \,|\, x \in M\}$ which is the infimum of $\{\downarrow x \,|\, x \in M\}$ in $\mathfrak{P}(X)$; thus, this extension preserves all the existing infima. Typically, however, suprema are in this representation not preserved.

The question naturally arises whether we can extend a poset to a complete lattice so that all the already existing infima and all the already existing suprema are preserved. This can be done by the *Dedekind-MacNeille construction*.

For a subset $M$ of a poset $X$ consider the sets of all upper resp. lower bounds

$$\begin{aligned} &\mathsf{ub}(M) = \{y \,|\, M \subseteq \downarrow y\}, \\ &\mathsf{lb}(M) = \{y \,|\, M \subseteq \uparrow y\}, \text{ and set} \\ &\nu(M) = \mathsf{lb}(\mathsf{ub}(M)). \end{aligned}$$

We will show that

$$\mathsf{DMN}(X, \leq) = (\{M \subseteq X \,|\, \nu(M) = M\}, \subseteq)$$

is a complete lattice and $\downarrow = (x \mapsto \downarrow x) : (X, \leq) \to \mathsf{DMN}(X, \leq)$ preserves all the existing suprema and infima.

**Lemma.**(1) *If* $M \subseteq N$ *then* $\mathsf{ub}(M) \supseteq \mathsf{ub}(N)$ *and* $\mathsf{lb}(M) \supseteq \mathsf{lb}(N)$.
(2) $M \subseteq \nu(M) = \mathsf{lb}(\mathsf{ub}(M))$ *and* $M \subseteq \mathsf{ub}(\mathsf{lb}(M))$.
(3) $\mathsf{ub}(\downarrow a) = \uparrow a$ *and* $\mathsf{lb}(\uparrow a) = \downarrow a$.
(4) $\nu$ *is monotone.*
(5) $\nu\nu(M) = \nu(M)$.

*Proof.* (1) through (4) are immediate observations. Now by (1) and (2) we have $\mathsf{lb}(M) \subseteq \mathsf{lb}(\mathsf{ub}(\mathsf{lb}(M))) \subseteq \mathsf{lb}(M)$ and $\mathsf{ub}(M) \subseteq \mathsf{ub}(\mathsf{lb}(\mathsf{ub}(M))) \subseteq \mathsf{ub}(M)$ so that $\mathsf{lb}(M) = \mathsf{lb}(\mathsf{ub}(\mathsf{lb}(M)))$ and $\mathsf{ub}(M) = \mathsf{ub}(\mathsf{lb}(\mathsf{ub}(M)))$ and finally $\mathsf{lb}(\mathsf{ub}(M)) = \mathsf{lb}(\mathsf{ub}(\mathsf{lb}(\mathsf{ub}(M))))$.

**Theorem.** (Dedekind – MacNeille completion) (1) $L = \mathsf{DMN}(X)$ *is a complete lattice. Suprema in* $L$ *are given by the formula* $\bigvee_{j\in J} M_j = \nu(\bigcup_{j\in J} M_j)$.

(2) *The mapping* $a \mapsto{\downarrow}a$ *is an embedding of a subobject (that is, it is a one-to-one mapping such that* $a \leq b$ *iff* ${\downarrow}a \subseteq{\downarrow}b$*), and it preseves all the already existing suprema and infima.*

*Proof.* (1): If $\nu(M) = M$ and $M \supseteq M_j$ for all $j \in J$ we have $M \supseteq \bigcup M_j$ and hence $M = \nu(M) \supseteq \nu(\bigcup M_j)$.

(2): By the Lemma we have $\nu({\downarrow}a) = \mathsf{lb}(\mathsf{ub}({\downarrow}a)) = \mathsf{lb}({\uparrow}a) = {\downarrow}a$ so that indeed ${\downarrow}a \in \mathsf{DMN}(X)$; obviously $a \leq b$ iff ${\downarrow}a \subseteq{\downarrow}b$ and moreover we have for $a = \inf a_j$, ${\downarrow}a = \bigcap {\downarrow}a_j$, and hence it is the infimum already in $\mathfrak{P}(X)$ and consequently in $\mathsf{DMN}(X)$. Finally we have

$$\bigvee_j {\downarrow}a_j = \nu(\bigcup_j {\downarrow}a_j) = \mathsf{lb}(\mathsf{ub}(\bigcup {\downarrow}a_j)) =$$
$$= \mathsf{lb}\{x \mid \forall j,\ x \geq a_j\} = \mathsf{lb}({\uparrow}a) = {\downarrow}a.$$

**Note.** Students may have seen a construction of real numbers extending rationals by special divisions $(A, B)$ of $\mathbb{Q}$ with $A \cup B = \mathbb{Q}$ and $a \leq b$ for any $a \in A$ and $b \in B$. This well-known Dedekind's procedure is a special case of the construction above.

# Two fixed-point theorems.

**Theorem.** (Bourbaki) *Let $(X, \leq)$ have $\perp$ and let every chain in $X$*

$$x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots$$

*have a supremum. Let $f : X \to Y$ preserve suprema of chains. Then $f$ has a fixed point.*
*Proof.* Start with $x_0 = \perp$ and define $x_n$ by setting $x_{n+1} = f(x_n)$. As $x_0 = \perp \leq x_1$ we obtain inductively that $x_{n+1} = f(x_n) \leq f(x_{n+1}) = x_{n+2}$ so that $x_0 \leq x_1 \leq \cdots \leq x_n \leq \cdots$. Consider $y = \sup x_n$. Then $f(y) = \sup f(x_n) = \sup x_{n+1} = y$ and $y$ is a fixed point.

**Note** that the $y$ from the proof is the *least fixed point of $f$*. If $f(z) = z$ we have $\perp \leq z$, $f(\perp) \leq f(z) = z$, and by induction $f(x_n) \leq z$.

**Application: the First Kleene Recursion Theorem.**
Consider the set

$$X = \{f \mid f \colon A \rightharpoonup B\}$$

of all partial maps from a set $A$ into a set $B$ and order it by the relation of extension, that is,

$$f \sqsubseteq g \quad \begin{array}{l}\text{iff the domain } D(f) \text{ of the function } f \text{ is contained in} \\ \text{the domain } D(g) \text{ of } g, \text{ and on } D(f) \text{ one has } f(x) = g(x).\end{array}$$

A *continuous functional* $F : X \to X$ is a monotone map such that

$$\textit{if } F(f)(a) = b \textit{ there is a finite } g \sqsubseteq f \textit{ such that } F(g)(a) = b.$$

(For instance: $A = B = \mathbb{N}$ and $F$ a recursion rule.) One has

**Theorem.** (Kleene) *For every continuous functional $F$ there exists a least $f$ such that $F(f) = f$.*
*Proof.* We will prove that $F$ preserves the suprema of chains. For a chain

$$f_1 \sqsubseteq f_2 \sqsubseteq \cdots \sqsubseteq f_n \sqsubseteq \cdots ,$$

the supremum is obviously the mapping $f$ defined on $\bigcup_{n\in\mathbb{N}} D(f_n)$ by the formula $f(x) = f_n(x)$ for $x \in D(f_n)$.

Trivially $\sup F(f_n) \sqsubseteq F(f)$. On the other hand, if $F(f)(a) = b$ we have $F(g)(a) = b$ for some finite $g \sqsubseteq f$. Because of the finiteness we have $g \sqsubseteq f_k$ for sufficiently large $k$; hence $F(f_k)(a) = b$. Thus also $(\sup F(f_n))(a) = b$.

**Theorem.** (Tarski – Knaster) *Every monotone mapping of a complete lattice into itself has a fixed point.*
*Proof.* Set $M = \{x \,|\, x \leq f(x)\}$ and $s = \sup M$. For $x \in M$, $x \leq s$, hence $x \leq f(x) \leq f(s)$, hence $f(s)$ is an upper bound of $M$, so that $s \leq f(s)$. Now, $f(s) \leq f(f(s))$ so that $f(s) \in M$. Therefore also $f(s) \leq s$.

**Application: Cantor-Bernstein Theorem.** *Let there exist one-to-one $\alpha : X \to Y$ and $\beta : Y \to X$. Then there exists a one-to-one onto $\phi : X \to Y$.*
*Proof.* Define $f : \mathfrak{P}(X) \to \mathfrak{P}(X)$ by $f(M) = X \setminus \beta[Y \setminus \alpha[M]]$, let $f(A) = A$ so that $X \setminus A = \beta[Y \setminus \alpha[A]]$. Set

$$\phi(x) = \begin{cases} \alpha(x) \text{ for } x \in A, \\ \beta^{-1}(x) \text{ for } x \in X \setminus A. \end{cases}$$

$\phi$ is onto: if $y \notin \phi[A] = \alpha[A]$ then $\beta(y) \in X \setminus A$ and $y = \phi(\beta(y))$.

$\phi$ is one-to-one: $x \in A$ and $z \in X \setminus A$ makes $\phi(x) \in \alpha[A]$ and $\phi(z) \in \beta^{-1}\beta[Y \setminus \alpha[A]] = Y \setminus \alpha[A]$.

**Another application:**

**Stability of two-person games with full information.**

A *two-person game* consists of a set $X$ (set of *states*) and relations $A \subseteq X \times X$ (the first player's rules) and $B \subseteq X \times X$ (the second player's rules), and an initial state $x_0 \in X$. A *play* in the game $(X, A, B, x_0)$ is a sequence

$$x_0 A x_1 B x_2 A x_3 \ldots \quad \text{(finite or infinite)}$$

($x_i A x_{i+1}$ are *moves* of the first player, $x_i B x_{i+1}$ are the moves of the second one). A player *loses* if on move and cannot proceed. An infinite play is evaluated as a *draw*.

A *strategy* of the first resp. second player is a subset $S \subseteq A$ resp. $S \subseteq B$. A strategy $S$ is *persistent* if it allows proceeding in $S$ after whatever move of the adversary, that is, say for the first player,

$$\text{whenever } \; xSy \; \text{ and } \; yBz \; \text{ there is a } \; u \; \text{ such that } \; zSu.$$

The existence of a persistent strategy does not yet make sure that the player cannot lose. For that, moreover, the player has to reach a state from which the strategy can be used. Thus, a *non-losing* strategy of the first player is a persistent strategy $S$ for which $x_0 S \neq \emptyset$, and for the second one it has to be such that $yS \neq \emptyset$ for every $y$ such that $x_0 A y$.

A variant of the following theorem was proved, first, by Kalmár (1928).

**Theorem.** *At least one of the players has a non-losing strategy. Consequently, if the game admits finite plays only, this player has a winning strategy.*
*Proof.* For $P \subseteq X \times X$ set $r(P) = \{(x, y) \,|\, yP = \emptyset\}$ and for fixed $A, B \subseteq X \times X$ define a (monotone)

$$\phi_{AB} : \mathfrak{P}(X \times X) \to \mathfrak{P}(X \times X)$$

by the formula

$$\phi_{AB}(P) = A \cap r(B \cap r(P)).$$

Take the relations $A, B$ from the definition of game above and choose a fixed point $S_{II}$ of $\phi_{BA}$ (hence

$$S_{II} = B \cap r(A \cap r(S_{II}))\ )$$

and set $S_I = A \cap r(S_{II})$. Then, $S_I$ is a fixed point of $\phi_{AB}$: we have

$$\phi_{AB}(S_I) = A \cap r(B \cap r(A \cap r(S_{II}))) = A \cap r(S_{II}) = S_I.$$

> **Claim.** *$S_I$ resp. $S_{II}$ is a persistent strategy of the first resp. second player.*
>
> (For $S_{II}$: let $xS_{II}y$ and $yAz$. If we had $zS_{II} = \emptyset$ there were $(y, z) \in A \cap r(S_{II})$. But $(x, y) \in S_{II} \subseteq r(A \cap r(S_{II}))$ and hence $y(A \cap r(S_{II}))$ would be void.)

Now assume that the second player has to lose. Hence the first player can prevent him to move in $S_{II}$, that is, there is a first move $x_0Ax_1$ with $x_1S_{II} = \emptyset$. Hence, $(x_0, x_1) \in A \cap r(S_{II}) = S_I$ and $S_I$ is a non-losing strategy of the first player.

# Appendix:

## Another fixed point theorem and Zorn's Lemma.

A very important proof principle is the Axiom of Choice, the claim that

*for every onto map $f : X \to Y$ there is a $g : Y \to X$ such that $fg = \mathrm{id}_Y$.*

It is non-constructive and therefore one mostly tries to avoid it. Nevertheless, there are important and interesting facts in which it is necessary. Often it is used as an application of an equivalent statement. A very expedient equivalent is the Zorn's Lemma we will also use later, and which we will discuss now. It is very easy to prove if we have established the theory of cardinals, but we will present here a proof that will not need it. Instead, we will use one more fixed-point theorem.

Let a set $X$ be ordered by $\leq$. A map $f : X \to X$ is said to be *inflationary* if $x \leq f(x)$ for all $x \in X$.

**Proposition.** (Witt's Lemma) *Let $f : (X, \leq) \to (X, \leq)$ be an inflationary map. Then the smallest $D \subseteq X$ closed under $f$ and existing suprema is a chain.*[3]

*Proof.* Let $\mathcal{D}$ be the set of all the $A \subseteq X$ such that

- $f[A] \subseteq A$, and
- if $B \subseteq A$ has a supremum in $X$ then $\sup B \in A$.

Obviously any intersection of elements of $\mathcal{D}$ is in $\mathcal{D}$ and hence in particular $D = \bigcap \mathcal{D}$ satisfies the two properties above, that is, $D$ is the smallest subset of $X$ closed under $f$ and existing suprema. We will prove that $D$ is a chain.

Set

$$C = \{c \in D \,|\, x \in D, x < c \;\Rightarrow\; f(x) \leq c\}.$$

Then for any $c \in C$,

$$D_c = (\downarrow c \cup \uparrow f(c)) \cap D \in \mathcal{D} \quad \text{and hence} \quad D = D_c.$$

Indeed, if $x \in D_c$ then either $x < c$ and then $f(x) \leq c$, or $x = c$ and then $f(x) = f(c) \geq f(c)$, or $x \geq f(c)$ and then $f(x) \geq x \geq f(c)$; if $B \subseteq D_c$ has a supremum then either $B \subseteq \downarrow c$ and $\sup B \leq c$ or $B \cap \uparrow f(c) \neq \emptyset$ and $\sup B \geq f(c)$.

[3] This is a very important fact on which Ernst Witt based his proof to be reproduced below.

Consequently, each $c \in C$ is comparable with all the elements of $D$, and in particular, as $C \subseteq D$,

$$C \text{ is a chain.}$$

Hence it suffices to prove that $C \in \mathcal{D}$, which will make $D = C$.

Let $c \in C$ and $x \in D = D_c$. If $x < f(c)$ then $x \not\geq f(c)$ and hence $x \leq c$. Then either $x < c$ and hence $f(x) \leq c \leq f(c)$ or $x = c$ and then $f(x) = f(c) \leq f(c)$.

Let $s = \sup B$ for some $B \subseteq C$. If $x < s$ then, since $C$ is a chain, $x < b$ for some $b \in B$ and hence $f(x) \leq b \leq s = \sup B$.

**Corollary.** (Bourbaki-Witt Fixed Point Theorem) *Let $(X, \leq)$ be a poset in which every chain has a supremum. Then each inflationary $f\colon X \to X$ has a fixed point.*

*Consequently, if every chain in a poset $(X, \leq)$ has a supremum, then there is no $f : X \to X$ such that $x < f(x)$ for all $x$.*

*Proof.* Let $s = \sup D$ for the $D$ from the previous lemma. Then $f(s) \in D$ and hence $f(s) \leq s \leq f(s)$.

**Theorem.** (Zorn's Lemma) *Let $(X, \leq)$ be a poset in which every chain has an upper bound. Then for every $x_0$ in $X$ there exists a maximal $y \in X$ such that $x_0 \leq y$.*

*Proof.* Suppose the statement does not hold. Then there is an $x_0$ such that none of the $y \geq x_0$ is maximal.

Let $Y$ be the poset of all chains in $X$ with minimum element $x_0$, ordered by inclusion. Obviously the union of a chain $\mathcal{C}$ in $Y$ is a chain in $X$ and we have $\bigcup \mathcal{C} = \sup \mathcal{C}$. For each $C \in Y$ choose an upper bound $b$. By the assumption $b$ cannot be maximal in $X$, and hence there is an $x_C > b$. Defining $f\colon Y \to Y$ by $f(C) = C \cup \{x_C\}$ we obtain a contradiction.

Zorn's Lemma is often used in the form of the

**Maximality principle.** *Let $(X, \leq)$ be a poset. Let $\mathcal{A} \subseteq \mathfrak{P}(X)$ be such that for every chain $\mathcal{C} \subseteq \mathcal{A}$ there is an $A \in \mathcal{A}$ such that $\bigcup \mathcal{C} \subseteq A$. Then for every $A \in \mathcal{A}$ there exists a $B$ maximal (in the inclusion) in $\mathcal{A}$ such that $A \subseteq B$.*

**Choice from Zorn.** Finally, we will show that the Axiom of Choice follows from the Zorn's Lemma, that is, that these two statements are equivalent.

Let $f\colon X \to Y$ be an onto map between sets. Consider

$$F = \{g\colon D(g) \to X \mid D(g) \subseteq Y, \text{ and } \forall y \in D(g), f(g(y)) = y\}$$

ordered by

$$g_1 \leq g_2 \quad \text{iff} \quad D(g_1) \subseteq D(g_2) \text{ and } \forall y \in D(g_1),\ g_1(y) = g_2(y).$$

For a chain $G$ in $F$ set $D = \bigcup_{g \in G} D(g)$. Since $G$ is a chain, we can define a mapping $h\colon D \to X$ by $h(y) = g(y)$ for $y \in D(g)$, $g \in G$, and obviously this $h$ is an upper bound of $G$. By Zorn's lemma there is a $g$ maximal in $F$. Suppose $D(g) \neq Y$; this is a contradiction: we can take a $y_0 \in Y \setminus D(g)$ and extend the $g$ to a larger $g'\colon D(g) \cup \{y_0\} \to X$ by choosing for $g'(y_0)$ any element of $f^{-1}[\{y_0\}]$.

# MSe3

## Adjunction (Galois connection)

Monotone maps $f : X \to Y$, $g : Y \to X$ are said to be (*Galois*) *adjoint*, or to be in a *Galois connection*, $f$ to the left and $g$ to the right, if

$$\forall x, y \quad f(x) \leq y \quad \Leftrightarrow \quad x \leq g(y).$$

**Note.** The original Galois connection concerned antitone maps.

If a right (resp. left) adjoint map for $f$ (resp. $g$) exists then

*it is uniquely determined.*

**Examples.** (a) Mutually inverse isomorphisms.

(b) *"Almost inverse functions* $\mathbb{N} \to \mathbb{N}$": Suppose a mapping $f : \mathbb{N} \to \mathbb{N}$ can be extended to an increasing real function $\widetilde{f} : \langle 1, +\infty) \to \mathbb{R}$ with inverse $\phi$. Denote by $\lceil x \rceil$ the least integer $\geq x$ and by $\lfloor x \rfloor$ the largest integer $\leq x$. Then

$$\lceil \phi(-) \rceil \text{ is a left adjoint of } f, \text{ and}$$
$$\lfloor \phi(-) \rfloor \text{ is a right adjoint of } f.$$

(Thus for instance $\lceil \log_2 \rceil$ and $\lfloor \log_2 \rfloor$ are the left and the right adjoint of the exponentiation $2^n$.)

(c) Let $f : X \to Y$ be an arbitrary map. We have

$$f[A] \subseteq B \quad \text{if and only if} \quad A \subseteq f^{-1}[B].$$

Thus the maps $f[-] : \mathfrak{P}(X) \to \mathfrak{P}(Y)$ and $f^{-1}[-] : \mathfrak{P}(Y) \to \mathfrak{P}(X)$ are adjoint, the image to the left, and the preimage to the right.

(d) *Concatenation of words.* Let $M$ be a set ("an alphabet"), let $M^+$ be the semigroup of words in this alphabet $M$, and $X = \mathfrak{P}(M^+)$. Denote for $A, B, C \in X$

$$A \cdot B = \{ab \,|\, a \in A, b \in B\},$$
$$C/B = \{w \,|\, \forall b \in B,\ wb \in C\},$$
$$A\backslash C = \{w \,|\, \forall a \in A,\ aw \in C\}.$$

Then we have

$$A \cdot B \subseteq C \quad \text{iff} \quad A \subseteq C/B \quad \text{iff} \quad B \subseteq A\backslash C.$$

The maps $(A \mapsto A \cdot B) : X \to X$ resp. $(B \mapsto A \cdot B) : X \to X$ are, hence, left adjoints to $C \mapsto C/B$ resp. $C \mapsto A\backslash C$.

(e) *Supremum as a left adjoint.* Let $(X \leq)$ be a complete lattice. By the definition of supremum we have

$$\sup M \leq x \quad \text{iff} \quad M \subseteq {\downarrow}x.$$

Thus,

$$\sup : (\mathfrak{P}(X), \subseteq) \to (X, \leq)$$

is a left adjoint to the embedding

$$\downarrow : (X, \leq) \to (\mathfrak{P}(X), \subseteq).$$

## An equivalent description of adjunction.

**Proposition.** *Monotone maps $f : X \to Y$ and $g : Y \to X$ are adjoint ($f$ to the left, $g$ to the right) if and only if there holds*

$$f(g(y)) \leq y \quad \textit{and} \quad x \leq g(f(x)),$$
$$\textit{in short} \quad fg \leq \mathrm{id} \ \textit{and} \ \ gf \geq \mathrm{id}.$$

> **Note.** This description does not seem to be of much advantage (and one rather thinks of it as of the weaker
>
> **Proposition.** *If $f, g$ are adjoit then $fg \leq \mathrm{id}$ and $\mathrm{id} \leq gf$,*
>
> but it is in fact very expedient in generalizations where dealing with two conditions each in one variable is much simpler then dealing with two variables. Anyway, in the original definition there is no trouble remembering what is right and what is left.

Hence $f \leq f(gf) = (fg)f \leq f$ and similarly for $gfg$ and we have an often used

**Corollary.** *If $f, g$ are adjoint then*

$$fgf = f \quad \textit{and} \quad gfg = g.$$

**Example.** Recall the adjunctions concerning the images and preimages $f[-]$ and $f^{-1}[-]$ above and the well known formulas

$$f[f^{-1}[A]] \subseteq A \quad \text{and} \quad A \subseteq f^{-1}[f[A]],$$

and also that

$$f[f^{-1}[f[A]]] = f[A],$$
$$f^{-1}[f[f^{-1}[A]]] = f^{-1}[A]$$

**Theorem.** *Left Galois adjoints preserve (all the existing) suprema, and the right ones preserve infima.*
*Proof.* Consider $f$ left adjoint to $g$. Take $s = \sup M$. Then obviously $f(s)$ is an upper bound of $f[M]$. The point is in proving that it is the least one. Let for all $m \in M$, $f(m) \leq b$. Then for all $m \in M$, $f(m) \leq b$, hence $m \leq g(b)$. Thus, $g(b)$ is an upper bound of $M$ and we have $s \leq g(b)$ and finally $f(s) \leq b$.

Can this implication be reversed? If existing suprema resp. infima would be scarce we could not expect much: the assumption would be too weak.
**BUT IF SUPREMA and INFIMA EXIST IN ABUNDANCE** it works. We have
**Theorem.** *If $X, Y$ are complete lattices then a monotone map $f : X \to Y$ is a left (resp. right) adjoint*

$$\underline{\textit{if and only if}}$$

*it preserves all suprema (resp. infima).*

*Proof.* Let $f$ preserve suprema. Define $g : Y \to X$ by setting

$$g(y) = \sup\{x \mid f(x) \leq y\}.$$

Trivially, $f(x) \leq y$ implies $x \leq g(y)$. But if $x \leq g(y) = \sup\{z \mid f(z) \leq y\}$ and $f$ preserves the supremum, we also obtain

$$f(x) \leq \sup\{f(z) \mid f(z) \leq y\} \leq y.$$

However easy, this is a fundamental and standardly used fact (and a special case of a much more general phenomenon).

## Semilattices and lattices as algebras

**Lower (resp. upper) semilattices:** We have here

$$a \wedge b \quad (\text{resp.} \quad a \vee b)$$

for any $a, b$. Let us view the $\wedge$ resp. $\vee$ as an *operation*. We immediately see that

$$\begin{aligned} &a \wedge (b \wedge c) = (a \wedge b) \wedge c, \\ &a \wedge b = b \wedge a, \qquad (\wedge\text{-eq}) \\ &a \wedge a = a. \end{aligned}$$

If a semilattice has a largest element, we have, moreover,

$$1 \wedge a = a. \qquad (1\text{-eq})$$

**Theorem.** *Let us have on $X$ an operation satisfying ($\wedge$-eq). Then there is precisely one order $\leq$ on $X$ such that $a \wedge b = \inf\{a, b\}$.*
*Proof.* There is at most one such order, because if it exists it follows from the formula $\inf\{a, b\} = a \wedge b$: we have to have $x \leq y$ iff $x = \inf\{x, y\} = x \wedge y$. Thus, we have to show that if $\wedge$ is satisfies (1-eq) then the relation defined by

$$x \leq y \quad \equiv_{\text{df}} \quad x \wedge y = x.$$

will do the job.

And indeed it does: we have $x \leq x$ since $x \wedge x = x$; if $x \leq y \leq z$ then $x \wedge y = x$ and $y \wedge z = y$ and hence $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$ and consequently $x \leq z$; and if $x \leq y \leq x$ then $x = x \wedge y = y \wedge x = y$.

Finally, in thus defined order, $x \wedge y = \inf\{x, y\}$: first of all $x \wedge y$ is a lower bound of the set $\{x, y\}$ since $(x \wedge y) \wedge x = (x \wedge x) \wedge y = x \wedge y$ and $(x \wedge y) \wedge y = x \wedge y$; it is the largest lower bound since if $z \wedge x = z = z \wedge y$ then $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$ and hence $z \leq x \wedge y$.

Similarly, **upper semilattices** are characterized by the obviously modified equations

$$\begin{aligned} &a \vee (b \vee c) = (a \vee b) \vee c, \\ &a \vee b = b \vee a, \\ &a \vee a = a \end{aligned} \qquad (\vee\text{-eq})$$

and if there is a smallest element 0, we have, moreover,

$$0 \vee a = a. \qquad (0\text{-eq})$$

**Lattices** are characterized by the system of equations
($\wedge$-eq), ($\vee$-eq) and ($\wedge\vee$-eq)

where ($\wedge\vee$-eq) stands for

$$a \wedge (a \vee b) = a \quad \text{and} \quad a \vee (a \wedge b) = a. \qquad (\wedge\vee\text{-eq})$$

The extra equation ($\wedge\vee$-eq) makes sure that the orders associated with $\vee$ and $\wedge$ coincide:

If we have $x \wedge y = x$ then $y = y \vee (x \wedge y) = y \vee x$, and if $y = y \vee x$ then $x = x \wedge (y \vee x) = x \wedge y$.

The least and largest elements, if they exist, are characterized by equations

$$0 \vee a = a, \quad 1 \wedge a = a.$$

The theories of semilattices and lattices **as posets and as algebras differ:** The difference is, first of all, in the preferred mappings.

In case of posets we think of *monotone* maps.

In case of algebras we think of *homomorphisms*, that is, maps such that

$$\begin{aligned} &h(x \vee y) = h(x) \vee h(y), \text{ and} \\ &h(x \wedge y) = h(x) \wedge h(y) \end{aligned}$$

which in the monotone case does not have to hold.

But also the preferred subobjects differ. A subalgebra should be closed under operations; a subset of a, say, lower semilattice can be a semilattice again (with the same order) but with other infima (the sets of lower bounds are not the same).

Note that the rule ($\wedge\vee$-eq)

$$a \wedge (a \vee b) = a, \quad a \vee (a \wedge b) = a.$$

binding the *operations* $\vee$ and $\wedge$ can be viewed as a very weak step towards distributivity that we have for instance in the complete lattice $\mathfrak{P}(X)$ of all subsets of a set.

In this lattice one is used to think of the union $A \cup B$ as of a sort of addition, and (in a somewhat lesser degree) of the intersection as of a multiplication. One has the unit $1 = X$ with $1 \cap A = A$ for all $A$, and the distributive law $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and hence one may view $\mathfrak{P}(X)$ as a sort of an algebraic ring, and a similar phenomenon can be observed more generally, with various "degrees of distributivity".

We have a step towards distributivity in the *modular* lattices, the lattices in which holds the implication

$$a \leq c \quad \Rightarrow \quad a \vee (b \wedge c) = (a \vee b) \wedge c.$$

**Notes.**1. Realize that the implication

$$a \leq c \quad \Rightarrow \quad a \vee (b \wedge c) \leq (a \vee b) \wedge c. \qquad \text{(mod)}$$

holds always. Thus, modularity concerns the reverse inequality.

2. Exchanging in the formula the role of $a$ and $c$ we immediately see that if $L$ is modular than also the dual $L^{\mathrm{op}}$ is. This will be also obvious from the characterization of modularity by prohibited configuration below.

**Examples.** 1. The lattice of all vector subspaces of a vector space $V$ is modular. Indeed, let $A, B, C$ be vector subspaces of a vector space $V$, let $A \subseteq C$, and let $x$ be in $(A \vee B) \cap C$. Then $x = \alpha a + \beta b = c \in C$ with $\alpha, \beta \in \mathbb{R}$, $a \in A \subseteq C$ and $b \in B$; hence $\beta b = c - \alpha a \in C \cap B$ and $x = \alpha a + \beta b \in A \vee (B \cap C)$.

Note that in these lattices $\cap$ does not have to distribute over $\vee$: consider, e.g., $V = \mathbb{R}\times\mathbb{R}$ with the standard vector structure, $A = \mathbb{R}\times\{0\}$, $B = \{0\}\times\mathbb{R}$ and $C = \{(x,x) \mid x \in \mathbb{R}\}$. Then $A \vee B = V$ and hence $C \cap (A \vee B) = C$ while $(C \cap A) \vee (C \cap B) = \{0\}$.

2. Similarly, and even simpler, we see that the lattice of all subgroups of an abelian group is modular, and, again, that it is not distributive (consider $\mathbb{Z} \times \mathbb{Z}$ and $A = \mathbb{Z} \times \{0\}$, $B = \{0\} \times \mathbb{Z}$ and $C = \{(x,x) \mid x \in \mathbb{Z}\}$).

3. On the other hand, the lattice of all subgroups of a general group is not necessarily modular. However, the lattice of all the *normal* subgroups is.

> **Note.** Modular lattices play an important role in algebra. The third example above indicates an interesting feature of modularity. Normal subgroups are in a natural one-to-one correspondence with congruences on groups; when we return to the two first examples we see that they are the rare cases where the lattices of subgroups and lattices of congruences are naturally isomorphic. One of the fundamental facts of general algebra is that *congruence lattices* of algebras are modular (while modularity of lattices of subalgebras is rare).

**Theorem.** *A lattice $L$ is modular if and only if it does not contain a sublattice isomorphic with the lattice $C_5$ described in the Hasse diagram in figure 1.*

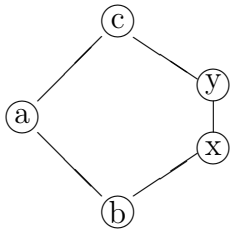



Figure 1: $C_5$, the configuration prohibited in modular lattices.

*Proof.* I. Let $L$ contain $C_5$. Then, in the notation from the picture, we have

$$x \vee (a \wedge y) = x \vee b = x < y = c \wedge y = (x \vee a) \wedge y$$

although $x \leq y$. Thus, $L$ is not modular.

II. Let $L$ not be modular. Then there exist $u, v, w$ such that $u \leq w$ and $u \vee (v \wedge w) < (u \vee v) \wedge w$. Consequently, $v$ is incomparable with any of $u \vee (v \wedge w)$ and $(u \vee v) \wedge w$: if we had $v \leq (u \vee v) \wedge w$ there would be $v \leq w$ and $u \vee (v \wedge w) = (u \vee v) \wedge w = u \vee v$; if we had $v \geq u \vee (v \wedge w)$ there would be $v \geq u$ and hence $u \vee (v \wedge w) = (u \vee v) \wedge w = v \wedge w$.

We have $v \vee u \vee (v \wedge w) = v \vee u$, and since also $(u \vee v) \wedge w \leq v \vee u$ we see that $v \vee u \geq v \vee ((u \vee v) \wedge w)$. Similarly $v \wedge (u \vee (v \wedge w) = v \wedge (u \vee v) \wedge w = v \wedge w$. Now we obtain a copy of $C_5$ in $L$ setting $a = v$, $b = v \wedge w$, $c = v \vee w$, $x = u \vee (v \wedge w)$ and $y = (u \vee v) \wedge w$.

A lattice $L$ is said to be *distributive* if for any $a, b, c \in L$,

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{distr}$$

This is reminiscent of the relation between the addition and multiplication you know from arithmetic. But there is also something that is in a strong contrast with the addition-multiplication relation: in lattices the distributivity works also with the role of the operations reversed. We have

**Proposition.** *A lattice $L$ is distributive if and only if $L^{\mathrm{op}}$ is distributive, that is, if and only if there holds the equality*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{distr'}$$

*Proof.* Suppose (distr) holds. Then we have $(a \vee b) \wedge (a \vee c) = ((a \wedge (a \vee c)) \vee (b \wedge (a \vee c))) = a \vee (b \wedge a) \vee (b \wedge c) = a \vee (b \wedge c)$.

**Note.** Since $a \leq c$ implies $a \vee c = c$ we immediately see that

*each distributive lattice is modular.*

**Lemma.** *A modular lattice is distributive if and only if there holds the equality*

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c).$$

**Note.** The inequality

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) \wedge (b \vee c).$$

is trivial. Hence, the point is in the reverse one.

*Proof.* I. If a lattice is distributive then $(a \vee b) \wedge (a \vee c) \wedge (b \vee c) = (a \vee (b \wedge (a \vee c))) \wedge (b \vee c) = (a \wedge (b \vee c)) \vee (b \wedge (a \vee c)) = (a \wedge b) \vee (a \wedge c) \vee (b \wedge a) \vee (b \wedge c)$.

II. Let the equality hold. Then we have

$$(a \vee b) \wedge c = (a \vee b) \wedge (a \vee c) \wedge (b \vee c) \wedge c = ((a \wedge b) \vee ((a \wedge c) \vee (b \wedge c)) \wedge c.$$

If, moreover, the lattice is modular we further obtain, using $(a \wedge c) \vee (b \wedge c) \leq c$,

$$\cdots = (a \wedge c) \vee (b \wedge c) \vee (a \wedge b \wedge c) = (a \wedge c) \vee (b \wedge c).$$

**Theorem.** *A lattice $L$ is distributive if and only if it contains no sublatice isomorphic with the $C_5$ in Fig.1 and no sublattice isomorphic with the $D_3$ in Fig.2.*

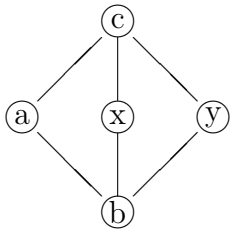



Figure 2: $D_3$, another configuration prohibited in a distributive lattice.

*Proof.* I. If the $L$ contains the configuration $C_5$ it is not even modular. If it contains $D_3$, the distributivity is violated by the inequality $(a \wedge x) \vee (a \wedge y) = b \neq a = a \wedge c = a \wedge (x \vee y)$.

II. Let the lattice not be distributive. If it is not modular it contains $C_5$. Thus, let $L$ be modular but not distributive. By Lemma there exist $a, b, c \in L$ such that

$$d = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) < h = (a \vee b) \wedge (a \vee c) \wedge (b \vee c).$$

Set

$$\begin{aligned} u &= (a \vee (b \wedge c)) \wedge (b \vee c), \\ v &= (b \vee (a \wedge c)) \wedge (a \vee c), \\ w &= (c \vee (a \wedge b)) \wedge (a \vee b). \end{aligned}$$

We will prove that

$$u \wedge v = u \wedge w = v \wedge w = d \quad \text{and} \quad u \vee v = u \vee w = v \vee w = h. \qquad (*)$$

For this it suffices to show that $u \wedge v = d$ (the rest will follow by permuting the elements $a, b, c$ and the interchange of $\wedge$ with $\vee$ which is correct since from the definition of the elements $u, v, w$ we obtain, using modularity,

$$\begin{aligned} u &= (a \wedge (b \vee c)) \vee (b \wedge c), \\ v &= (b \wedge (a \vee c)) \vee (a \wedge c), \\ w &= (c \wedge (a \vee b)) \vee (a \wedge b). \quad ) \end{aligned}$$

Using modularity again we obtain

$$\begin{aligned} u \wedge v &= (a \vee (b \wedge c)) \wedge (b \vee c) \wedge (b \vee (a \wedge c)) \wedge (a \vee c) = \\ &= (a \vee (b \wedge c)) \wedge (b \vee (a \wedge c)) = (a \wedge (b \vee (a \wedge c))) \vee (b \wedge c) = \\ &= (a \wedge b) \vee (a \wedge c) \vee (b \wedge c). \end{aligned}$$

Since $d \neq h$ we now obtain from $(*)$ the diagram $D_3$ represented by the incomparable elements $u, v, w$, the common infimum of the pairs $d$ and the common supremum of the pairs $h$. $\square$

**Theorem.** *A lattice $L$ is distributive if and only if each pair of equations*

$$\begin{aligned} a \wedge x &= b \\ a \vee x &= c \end{aligned}$$

*has at most one solution $x$.*
*Proof.* I. Let $L$ be distributive and let

$$a \wedge x = b,\ a \vee x = c,\ a \wedge y = b \text{ and } a \vee y = c.$$

Then $x = x \wedge (a \vee x) = x \wedge (a \vee y) = (x \wedge a) \vee (x \wedge y) = (y \wedge a) \vee (x \wedge y) = y \wedge (a \vee x) = y \wedge (a \vee y) = y$.

II. Let $L$ not be distributive. Then in any of the configurations $C_5$ or $D_3$, both the $x$ and $y$ solve the equations above.

# MSe4

Recall that a lattice $L$ is *distributive* if there holds, for any $a, b, c \in L$,

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{distr}$$

This is reminiscent of the relation between addition and multiplication from arithmetic, but we also have

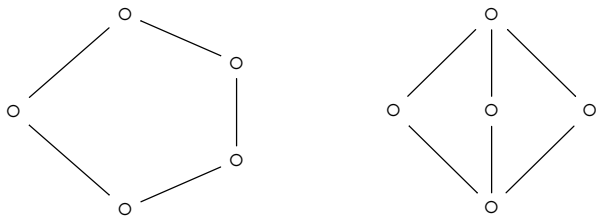
**Proposition.** *A lattice $L$ is distributive if and only if $L^{\mathrm{op}}$ is distributive, that is, if and only if there holds the equality*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{distr'}$$

.

This fact is also seen in

**Theorem.** *A lattice $L$ is distributive if and only if it does not contain any of the following two configurations*



Furthermore we learned that

**Theorem.** *In a distributive lattice, each pair of equations of the form*

$$a \wedge x = b$$
$$a \vee x = c$$

*has at most one solution $x$.*

# Ideals and filters in distributive lattices.

**Like in rings** we have *ideals*, that is, subsets $J \subseteq L$ such that

$$\begin{aligned} &0 \in J, \\ &a, b \in J \ \Rightarrow \ a \vee b \in J, \\ &a \in J \text{ and } b \text{ arbitrary } \Rightarrow \ a \wedge b \in J. \end{aligned} \tag{idl}$$

The third rule, will be used in the equivalent and handier form

$$a \in J \text{ and } b \leq a \Rightarrow \ a \wedge b \in J.$$

**Dually** we have *filters* $F \subseteq L$ satisfying

$$\begin{aligned} &1 \in F, \\ &a, b \in F \ \Rightarrow \ a \wedge b \in F, \\ &a \in F \text{ and } b \geq a \ \Rightarrow \ b \in F. \end{aligned} \tag{fltr}$$

> **Note.** This concept is not just a natural dualization. It apears for instance when describing the systems of neighbourhoods of points in a space.

An ideal $J$ resp. filter $F$ is said to be *proper* if $J \neq L$ resp. $F \neq L$ which is the same as stating that $1 \notin J$ resp. $0 \notin F$. This is often assumed without saying, but here it will mostly be explicitly stated.

A proper ideal $J$ resp. filter $F$ is *prime* if

$$a \wedge b \in J \ \Rightarrow \ \text{either } a \in J \text{ or } b \in J$$

resp.

$$a \vee b \in F \ \Rightarrow \ \text{either } a \in F \text{ or } b \in F.$$

**Note.** Complements $L \smallsetminus F$ resp. $L \smallsetminus J$ of filters resp. ideals are not necessarily ideals resp. filters.
BUT:

> *Complements $L \smallsetminus F$ resp. $L \smallsetminus J$ of <u>prime</u> filters resp. ideals are <u>prime</u> ideals resp. filters.*

A proper filter resp. ideal is *maximal* if it is not contained in a bigger proper filter resp. ideal.
Often one considers maximality with respect to a special condition added.

> **Aside.** 1. Recall the role of ideals in factorization of rings and in particular that of the prime and maximal ones:
>
> - maximal ideals are those making $R/J$ a field,
> - prime ideals are those making $R/J$ an integrity domain.
>
> 2. In the ring $\mathbb{Z}$ of integers we have the ideals $I_n = \{nx \mid x \in \mathbb{Z}\}$. Note that $I_n$ is prime iff $n$ is a prime number.

**Proposition.** *Let $J$ be a non-empty ideal and let a filter $F$ be maximal such that $F \cap J = \emptyset$. Then it is prime.*

> **Note.** This includes, of course, the plainly maximal filters: consider $J = \{0\}$.

*Proof.* Let $a \vee b \in F$ and $a, b \notin F$. Set

$$G = \{x \mid x \vee a \in F\}.$$

Then by distributivity $G$ is a filter; since $x \vee a \geq x$ one has $F \subseteq G$, and $b \in G \setminus F$. Thus, by the maximality of $F$, there has to be a $c \in G \cap J$. As $c \in G$, $c \vee a \in F$, and as $F \cap J = \emptyset$ we now have $c, a \notin F$. Set

$$H = \{x \mid c \vee x \in F\}$$

and repeat the reasoning as with the $G$ above. Now we will obtain a $d \in H \cap J$, which is a contradiction: $c \vee d \in F$, but it is also in $J$, because $J$ is closed under $\vee$.

> **Note.** For plain maximality one stops with the $c \in G \cap J$: this makes $c = 0$ and $a = 0 \vee a \in F$.

In the next proposition we will use the Axiom of Choice (in the form of Zorn's Lemma). Using a choice principle for this statement is necessary.

**Proposition.** (Birkhoff maximal filter theorem) *Let $F \subseteq L$ be a filter and $J \subseteq L$ an ideal such that $F \cap J = \emptyset$. Then there exists a maximal and hence prime filter $\overline{F}$ and a maximal and hence prime ideal $\overline{J}$ such that*

$$F \subseteq \overline{F},\ J \subseteq \overline{J} \quad \textit{and} \quad \overline{F} \cap \overline{J} = \emptyset.$$

*Proof.* Consider $\mathcal{F}$ the set of filters disjoint with $J$ ordered by $\subseteq$. Let $\mathcal{C}$ be a chain in $\mathcal{F}$. Then $\widetilde{G} = \bigvee\{G \,|\, G \in \mathcal{F}\}$ is a filter (if $a_i \in G_i$, $G_1, G_2 \in \mathcal{C}$ and $G_1 \subseteq G_2$, then $a_1 \wedge a_2 \in G_2 \subseteq \widetilde{G}$), and an upper bound of $\mathcal{C}$.

By Zorn's Lemma there is a maximal $\overline{F}$ containing $F$ such that $\overline{F} \cap J = \emptyset$.

Now we can use the fact dually for $\overline{F}$ and $J$.[1]

**Corollary.** *Let $a \not\leq b$ in a distributive lattice $L$. Then there is a prime filter $F$ and a prime ideal $J$ such that*

$$a \in F,\ b \in J \quad \textit{and} \quad F \cap J = \emptyset.$$

**Remark.** Take the lattice $\mathfrak{P}(X)$ of subsets of a set $X$ there is a lot of the obviously prime filters, namely the

$$\mathcal{F}(a) = \{U \subseteq X \,|\, a \in U\} \qquad (*)$$

for arbitrary $a \in L$. But the fact that every proper filter can be extended to a prime one is a highly non-trivial phenomenon. Birhoff's theorem guarantees, e.g., a prime filter extending the filter of all $X \subseteq \mathbb{N}$ such that $\mathbb{N} \smallsetminus X$ is finite[2] which cannot be described constructively (it is a basis of very non-trivial models in set theory – and is of importance elsewhere as well).

The filters $\mathcal{F}(a)$ from $(*)$ and more generally the filters $\mathcal{F}$ of open neighbourhoods of points $a$ in the lattice of open subsets of a metric space have in fact a stronger property. They are *completely prime*, that is, if $\bigcup_i U_i \in \mathcal{F}$ for any union (join) then there is an $U_i$ in $\mathcal{F}$. Unlike prime filters that exist (albeit assuming choice) in every distributive lattice, completely prime ones may be rare or even quite absent.

[1] For the statement on prime ideals and filters we can simply take for $\overline{J}$ the complement of $\overline{F}$

[2] The so called Fréchet filter.

# Pseudocomplements.

In the general information on pseudocomplements we will not need distributivity. But in fact we are not moving away from the topic all that far:

- the existence of pseudocomplements is in fact a week form of distributivity as we will see very soon, and
- in the next lecture we will discuss an operation that will be in a way extending the phenomenon, and that will be connected with a property stronger than distributivity.

First of all, however, pseudocomplements are important for modelling such issues as negation in logic.

An element $b$ is a *pseudocomplement* of $a$ if it is the largest element meeting $a$ in 0:

$$x \leq b \quad \text{iff} \quad x \wedge a = 0$$

A pseudocomplement does not have to exist, but if it does it is uniquely determined (the same condition for $b'$ makes $b \leq b'$ and $b' \leq b$). It will be denoted by

$$a^*.$$

Obviously

$$a \leq b \ \Rightarrow b^* \leq a^*, \tag{anti}$$

and hence the mapping $(a \mapsto a^*) : L \to L^{\mathrm{op}}$ is monotone.
It is adjoint to $(a \mapsto a^*) : L^{\mathrm{op}} \to L$: we have $x \leq y^*$ iff $x \wedge y = 0$ iff $y \leq x^*$, and hence

$$x^* \leq^{\mathrm{op}} y \quad \text{iff} \quad x \leq y^*.$$

In particular, it sends suprema from $L$ to suprema in $L^{\mathrm{op}}$, hence to infima in $L$ :

$$(\bigvee a_i)^* = \bigwedge a_i^* \tag{DM}$$

It is one of the De Morgan formulas; the student certainly knows also the dual one (concerning complements of sets, or negation in classical logic. Only (DM) holds generally, though.

**Remark.** The existence of pseudocomplements can be viewed as a weak form of distributivity: namely, it says that

$$(\bigvee a_i) \wedge b = 0 \quad \text{iff} \quad \bigvee (a_i \wedge b) = 0.$$

**Facts:** (1) $a \leq a^{**}$
(2) $a^* = a^{***}$, *hence* $x \wedge a^{**} = 0$ *iff* $x \wedge a = 0$
(3) $(a \wedge b)^{**} = a^{**} \wedge b^{**}$

*Proof.* (1) Interpret the fact that $a \wedge a^* = 0$ as $x \wedge a^* = 0$ in the definition of the pseudocomplement $(a^*)^*$ of $a^*$.

(2) By (anti) and (1) we have $(a^{**})^* \geq a^*$, by (1) $a^* \leq (a^*)^{**}$.

(3) Trivially $(a \wedge b)^{**} \leq a^{**} \wedge b^{**}$ ($(a \wedge b)^{**}$ is a lower bound of $\{a^{**}, b^{**}\}$). By (1), $a \wedge b \leq (a \wedge b)^{**}$, hence $a \wedge b \wedge (a \wedge b)^* = 0$, hence by (2) $a^{**} \wedge b \wedge (a \wedge b)^* = 0$, by (2) again, $a^{**} \wedge b^{**} \wedge (a \wedge b)^* = 0$, and hence $a^{**} \wedge b^{**} \leq (a \wedge b)^{**}$.

**Note.** In the Brouwerian (intuitionistic) logic one abandons the rule of double negation, that is, the assumption that $\neg\neg V = V$. Understanding $\neg V$ as the weakest statement that still contradicts $V$ we see that $\neg\neg V \not\leq V$ only if $V$ cannot be a negation of anything (and then of course not of the $\neg V$ either): whenever $V = \neg W$ we have $V = \neg\neg\neg W = \neg\neg V$.

A **complement** of $a$ is a $b$ such that

$$a \vee b = 1 \text{ and}$$
$$a \wedge b = 0.$$

A complement need not exist and if it exists it may not be necessarily unique.

> **Example.** Consider again the lattice $L$ of vector subspaces of the vector space $V_2 = \mathbb{R} \times \mathbb{R}$ and the subspaces
>
> $$A = \{(x, 0) \,|\, x \in \mathbb{R}\},\ B = \{(0, x) \,|\, x \in \mathbb{R}\} \quad \text{and} \quad C = \{(x, x) \,|\, x \in \mathbb{R}\}.$$
>
> Then
>
> $$A \vee B = A \vee C = V_2 \quad \text{and} \quad A \wedge B = A \wedge C = \{(0, 0)\}.$$

Recall, however, the proposition on unique solutions of the equations

$$a \vee x = b \text{ and}$$
$$a \wedge x = c$$

in distributive lattices. Consequently,

> *in a distributive lattice a complement, if it exists, is uniquely determined.*

The unicity also follows from the following

**Proposition.** *Each complement in a distributive lattice is a pseudocomplement.*
(If $x \wedge a = 0$ then $x = x \wedge (a \vee b) = x \wedge b$, hence $x \leq b$.)

**Notation.** Consequently, if there is no danger of confusion we often write the complement as a pseudocomplement $a^*$. Else one has to use some other symbol, say $a^{\mathsf{c}}$.

# MSe5

## Heyting algebras

A *Heyting algebra* is a bounded lattice with an operation $\to$ such that

$$a \wedge b \leq c \quad \text{iff} \quad a \leq b \to c. \tag{Hey}$$

Thus we have adjunctions between mappings $(-) \wedge b$ and $b \to (-)$ (check that $x \mapsto b \to x$ is monotone) and hence

- $\to$ is uniquely determined by $\wedge$, and
- we have the distributivity

$$(\bigvee_i a_i) \wedge b = \bigvee_i (a_i \wedge b)$$

for all existing suprema $\bigvee a_i$.

**Notes.** 1. Hence, the introducing the Heying operation amounts to the claim that the maps $a \wedge -$ are left adjoints. 2. If $L$ is complete then the stronger distributivity $(\bigvee_i a_i) \wedge b = \bigvee_i (a_i \wedge b)$ (because left adjoints are the precisely the maps preserving suprema (joins)) implies the existence of the Heyting operation.

3. The stronger distributivity does not carry over to the dual lattice, that is, the dual of a Heyting algebra is typicaly only distributive, but not a Heyting algebra again. Thus, in a sense, Heyting algebras are closer to rings then the plainly distributive ones.

## Heyting algebras and pseudocomplements.

In particular $x \wedge a \leq 0$ iff $x \leq a \to 0$. Thus

*Heyting algebras have pseudocomplements, namely* $a^* = a \to 0$.

We have more. Take an arbitrary $b \in L$ and the subset

$$\uparrow b = \{x \mid x \geq b\}.$$

$\uparrow b$ is a sublattice of $L$ (not a bounded sublattice allthough it is a bounded lattice: it has a different bottom, namely $b$). We have for $a, x \in \uparrow b$

$$x \wedge a = b \quad \text{iff} \quad x \wedge a \leq b \quad \text{iff} \quad x \leq a \to b$$

and since $b \wedge a \leq b$ we have $b \leq a \to b$, that is, $a \to b \in \uparrow a$. Hence,

> *if $L$ is a Heyting algebra then each $\uparrow b \subseteq L$ is pseudocomplemented, with pseudocomplements $a^{b*} = a \to b$.*

**Notes.** 1. All the $\uparrow b$ in a Heyting algebra are in fact Heyting, of course.

2. In view of the pseudocomplements $a^{b*}$ in the up-sets $\uparrow b$, the Heyting operation $\to$ is sometimes called *relative pseudocomplement*.

## Heyting algebras and complements.

We have

**Proposition.** *Let $L$ be a distributive lattice. Let $b$ have a complement $b^*$. Then $b^* \vee (-)$ is a right adjoint to $(-) \wedge b$, that is,*

$$x \wedge b \leq y \quad \textit{iff} \quad x \leq b^* \vee y.$$

*Proof.* If $x \wedge b \leq y$ then $x = x \wedge (b \vee b^*) = (x \wedge b) \vee (a \wedge b^*) \leq y \vee b^*$. If $x \leq b^* \vee y$ then $x \wedge b \leq (b^* \vee y) \wedge b = (b \wedge b^*) \vee (y \wedge b) \leq y$.

Thus in particular, **in a Heyting algebra we have that**

> *for a complemented $b$ the Heyting operation is equal to $b \to c = b^{\mathsf{c}} \vee c$.*

**Note.** This is one of the cases where we write cautiously $b^{\mathsf{c}}$ for the complement. The formula holds only for the $b^*$ that are complements: if $b \to c = b^* \vee c$ we have in particular $1 \wedge b \leq b$ implying $1 \leq b \to b = b^* \vee b$, hence $b^*$ is a complement.

## Some simple Heyting rules.

The Heyting operation is in general not quite easy to compute, but there are a few easy rules that are helpful. Let us present a few of them.

(1) $b \to \bigwedge_i c_i = \bigwedge_i (b \to c_i)$.

($b \to (-) : L \to L$ is a right adjoint.)

(2) $(\bigvee_i a_i) \to c = \bigwedge_i \to (a_i \to c)$.

($a \leq b \to c$ iff $b \leq a \to c$, hence $b \to c \leq^{\mathrm{op}} a$ iff $b \leq a \to c$ so that $(-) \to c : L \to L^{\mathrm{op}}$ is a left adjoint.)

(3) *For any $a$, $a \to a$ is the largest element 1, and $1 \to a = a$ for all $a$.*

(For any $a$ and any $x$ we have $x \leq a \to a$, hence for each $a$, $a \to a$ is the top 1. We have $x \leq 1 \to a$ iff $x = x \wedge 1 \leq a$, hence $1 \to a = a$. )

(4) $a \leq b$ *iff* $a \to b = 1$.

($1 \leq a \to b$ iff $a = 1 \wedge a \leq b$.)

(5) $a \leq b \to a$.

($a \wedge b \leq a$.)

(6) $a \to b = a \to (a \wedge b)$.

($a \to (a \wedge b) = (a \to a) \wedge (a \to b) = a \to b$ by (1) and (3).)

(7) $a \wedge (a \to b) \leq b$, *more precisely* $a \wedge (a \to b) \leq a \wedge b$.

($a \to b \leq a \to b$, hence $a \wedge (a \to b) \leq b$ and hence also $a \wedge (a \to b) \leq a \wedge b$. By (5), $b \to a \leq b$, hence $a \wedge b \leq a \wedge (a \to b)$.)

(8) *If $a \leq b$ then $a \to c \geq b \to c$.*

(If $a \leq b$ then $a \wedge (b \to c) \leq b \wedge (b \to c) \leq c$ and hence $b \to c \leq a \to c$.)

(9) $a \to b = a \to c$ *iff* $a \wedge b = a \wedge c$.

(Follows from (6) and (7).)

(10) $(a \wedge b) \to c = a \to (b \to c) = b \to (a \to c)$.

(We have $x \leq (a \wedge b) \to c$ iff $x \wedge a \wedge b \leq c$ iff $x \wedge a \leq b \to c$ iff $x \leq a \to (b \to c)$.)

(11) $a = (a \vee b) \wedge (b \to a)$.

(By distributivity, $(a \vee b) \wedge (b \to a) = (a \wedge (b \to a)) \vee (b \wedge (b \to a)) = a \vee (a \wedge b) = a$.)

(12) $a \leq (a \to b) \to b$ *and* $((a \to b) \to b) \to b = a \to b$.

(The inequality follows immediately from (7), from that then, substituting $a \to b$ for $b$, $((a \to b) \to b) \to b \leq a \to b$, and $((a \to b) \to b) \to b \geq a \to b$ by (8).)

## Heyting operation and implication.

The formula $b \to c = b^{\mathsf{c}} \vee c$ for complemented $b$ is reminiscent of the formula for the classical implication

$$B \Rightarrow C \;=\; \mathrm{non}B \vee C$$

And rightly so; one of the roles of the Heyting operation is modeling general implication.

Recall the charaterization of the adjunction $l(x) \leq y$ iff $x \leq r(y)$ as the pair of inequalities $lr \leq \mathrm{id}$ and $\mathrm{id} \leq rl$. In particular we see that the condition (Hey) is equivalent to

$$a \wedge (a \to b) \leq b \quad \text{and} \quad a \leq b \to (a \wedge b).$$

Hence if we think of a system of propositions with the (pre)order of inference $\vdash$ we see that the formula

$$(U \& V) \vdash W \quad \text{iff} \quad U \vdash (V \Rightarrow W)$$

is equivalent to the very natural assumptions

$$\begin{array}{ll} V \& (V \Rightarrow W) & \vdash \; W \quad \text{(modus ponens), and} \\ U & \vdash \; V \Rightarrow (U \& V) \quad \text{(assumed } V \text{ can be added)} \end{array}$$

and the formula $a \to b = a^* \vee b$ for complemented $a$ can be interpreted as that if $V$ has a negation $\mathrm{non}V$ such that $V \vee \mathrm{non}V$ is tautological then

$$V \Rightarrow W \quad \text{is} \quad (\mathrm{non}V) \vee W.$$

**Another observation:** In a Heyting algebra we have

$$a \leq b \quad \text{iff} \quad a \to b = 1$$

($a = 1 \wedge a \leq b$ iff $1 \leq a \to b$). This gives the relation between inference and implication:

$$U \vdash V \quad \text{iff} \quad U \Rightarrow V \text{ is true.}$$

# Boolean algebras.

A *Boolean algebra* is a distributive lattice in which each element is complemented.

We have shown above that if $b$ is complemented in a distributive lattice then $a \wedge b \leq c$ iff $a \leq b^* \vee c$. Consequently

> *every Boolean algebra is a Heyting one and in particular it satisfies the stronger distributivity* $(\bigvee a_i) \wedge b = \bigvee (a_i \wedge b)$ *for all existing suprema* $\bigvee a_i$.

**Notes.** 1. Obviously (unlike with Heyting algebras), if $L$ is a Boolean algebra then also $L^{\mathrm{op}}$ is a Boolean algebra. Consequently, in a Boolean algebra one also has

$$(\bigwedge a_i) \vee b = \bigwedge (a_i \vee b) \qquad (*)$$

for all existing infima $\bigwedge a_i$, and both De Morgan formulas

$$(\bigvee_i a_i)^* = \bigwedge_i a_i^* \quad \text{and} \quad (\bigwedge_i a_i)^* = \bigvee_i a_i^*.$$

2. The assumption of distributivity in the definition is essential.

## Ultrafilters.

**Theorem.** *Let $F$ be a proper filter in a Boolean algebra $L$. Then TFAE*

(1) *$F$ is maximal,*

(2) *$F$ is prime,*

(3) *for every $a \in L$ either $a \in F$ or $a^{\mathsf{c}} \in F$.*

*Proof.* (1)⇒(2): holds in any distributive lattice (see previous lecture).

(2)⇒(3) follows from the fact that $a \vee a^{\mathsf{c}} = 1 \in F$.

(3)⇒(1): Let $F \subsetneq G$ for a filter $G$. Choose an $a \in G \smallsetminus F$. Since $a \notin F$ we have to have $a^{\mathsf{c}} \in F \subseteq G$, hence $a, a^{\mathsf{c}} \in G$ and finally $0 = a \wedge a^{\mathsf{c}} \in G$. Thus, the filter $G$ is not proper.

**Terminology.** Prime (≡ maximal) filters in Boolean algebras play important role in various application. They are referred to as *ultrafilters*.

## Booleanization.

Let $L$ be a pseudocomplemented meet-semilattice. Set

$$\mathfrak{B}L = \{a \in L \,|\, a = a^{**}\}.$$

**Proposition.** *$\mathfrak{B}L$ is a Boolean algebra.*
*Proof.* For $a, b \in \mathfrak{B}L$ set

$$a \sqcup b = (a^* \wedge b^*)^*.$$

It is a supremum of $a, b$ in $\mathfrak{B}L$: Since $a \wedge (a^* \wedge b^*) = 0$, $a \leq (a^* \wedge b^*)^*$ and similarly for $b$; now if $a, b \leq x \in \mathfrak{B}L$ then $x^* \leq a^*, b^*$ and hence $x^* \leq a^* \wedge b^*$ so that $x = x^{**} \geq (a^* \wedge b^*)^*$.

Further set for $b, c \in \mathfrak{B}L$

$$b \to c = (b \wedge c^*)^*.$$

Then we have

$$a \wedge b \leq c \quad \text{iff} \quad a \leq b \to c.$$

(If $a \wedge b \leq c$ then $a \wedge b \wedge c^* = 0$ and hence $a \leq (b \wedge c^*)^*$. On the other hand, if $a \leq (b \wedge c^*)^*$ then $a \wedge b \leq (b \wedge c^*)^* \wedge b$; we have $(b \wedge c^*)^* \wedge b \wedge c = 0$, hence $c^* \leq ((b \wedge c^*)^* \wedge b)^*$ and $(b \wedge c^*)^* \wedge b) \leq c^{**} = c$.)

Thus, $\mathfrak{B}L$ is Heyting and hence distributive. Finally, for $a \in \mathfrak{B}L$, $a \sqcup a^* = (a^* \wedge a^{**})^* = 0^* = 1$.

**Notes.** 1. We have not assumed the existence of joins in $L$, not to speak about distributivity. Thus the distributivity results from the pseudocomplementation at least on a part of the poset.

2. The construction $\mathfrak{B}$ together with the mapping

$$\mathfrak{b} = (a \mapsto a^{**}) : L \to \mathfrak{B}L$$

is called *booleanization* and – in particular applied to Heyting $L$ – plays a role in various areas (logic, topology).

3. In case of the lattice of open sets of a space $X$ one easily sees that $U^* = X \setminus \overline{U}$. The $U$ such that $U = U^{**} = X \setminus \overline{X \setminus \overline{U}} = \mathrm{int}\overline{U}$ are the so called *regular open sets*.

## "The law of excluded middle".

Students might wonder why one often speaks about the double negation rule

$$\neg\neg A = A$$

of classical logic as of the "law of excluded middle" (which one also otherwise interprets as

$$A \vee \neg A = \text{true. }$$

These two formulas are indeed almost the same, but not quite. This will be explained in the context of general pseudocomplemented lattices.

**Observation.** From $(x \wedge y)^* \wedge y \wedge x = 0$ we immediately obtain that in any pseudocomplemented lattice

$$(x \wedge y)^* \wedge y \leq x^*. \qquad \textbf{(PC)}$$

**Proposition.** *If $a = a^{**}$ for all $a$ in a pseudocomplemented $L$ then $L$ is Boolean.*
*Proof.* Set

$$b \to c = (c^* \wedge b)^*.$$

It is a Heyting operation in $L$: if $a \wedge b \leq c$ we have by (**PC**), $a = a^{**} \leq ((a \wedge b)^* \wedge b)^* \leq (c^* \wedge b)^*$, and if $a \leq (c^* \wedge b)^*$ then, again by (**PC**), $a \wedge b \leq (c^* \wedge b)^* \wedge b \leq c^{**} = c$.
Thus in particular $L$ is distributive. Finally, we have $a \vee a^* = (a \vee a^*)^{**} = 1$.

**Theorem.** *For a pseudocomplemented lattice $L$ the following statements are equivalent.*

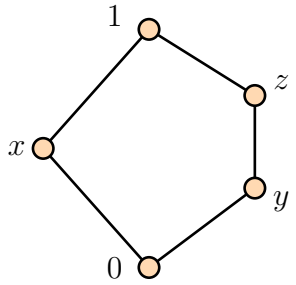
(1) *For all $a \in L$, $a^{**} = a$.*

(2) *$L$ is Boolean.*

(3) *$L$ is modular and for all $a$, $a \vee a^* = 1$.*

*Proof.* (1)⇒(2) is in the previous Proposition and (2)⇒(3 is trivial.
(3)⇒(1): Since $a \leq a^{**} = 1$ we have by modularity $a \vee (b \wedge a^{**}) = (a \vee b) \wedge a^{**}$. Setting $b = a^*$ we obtain $a = a \vee 0 = 1 \wedge a^{**} = a^{**}$.

**Note** The assumption of modularity is essential. In the pentagon below we have $z = x^*$ and $x = y^* = z^*$ so that $a \vee a^*$ is always 1, while $y^{**} = z > y$.




Thus, the two assumptions in question are indeed the same if we assume modularity (and one usually assumes distributivity without mentioning). But the double pseudocomplement rule already entails the distributivity while with the rule of excluded middle at least modularity has to be assumed.

## Aside: Prime elements.

**Completely prime filters do not have to exist.**

An element $p \neq 1$ in a distributive lattice is said to be *prime* if

$$a \wedge b \leq p \quad \text{iff} \quad a \leq p \text{ or } b \leq p.$$

**Proposition.** *Let $L$ be a complete distributive lattice. Then the formulas*

$$p \mapsto F_p = \{a \,|\, a \not\leq p\} \quad \textit{and} \quad F \mapsto p_F = \bigvee\{a \,|\, a \notin F\}$$

*provide a one-to-one correspondence between the prime elements and non-empty completely prime filters in $L$.*

*Proof.* $F_p$ is a completely prime filter: obviously $a \in F_p$ and $b \geq a$ implies $b \in F_p$, and if $a, b \in F_p$ then $a \wedge b \in F_p$ (if $a \wedge b \leq p$ then either $a \notin F_p$ or $b \notin F_p$); $F_p$ is proper because $0 \leq p$ and non-empty because $1 \not\leq p$. If $\bigvee a_i \not\leq p$ then there has to be an $a_j \not\leq p$, hence $F_p$ is completely prime.

$p_F$ is prime: Since $F$ is completely prime, $p_F = \bigvee\{a \,|\, a \notin F\}$ cannot be in $F$ so that $x \notin F$ iff $a \leq p$. Hence if $a \wedge b \leq p$ then $a \wedge b \notin F$ and hence we cannot have $a, b \in F$ and hence some of them is $\leq p$.

Finally, $p_{F_p} = \bigvee\{a \,|\, a \notin F_p\} = \bigvee\{a \,|\, a \leq p\} = p$ and $F_{p_F} = \{a \,|\, a \not\leq p_F\} = \{a \,|\, a \in F\} = F$.

**Proposition.** *If $p$ is a prime element in a Boolean algebra then it is a maximal one (that is, if $p < x$ then $x$=1).*

*Proof.* Suppose there is an $x$ with $p < x$. Since $x \wedge x^{\mathsf{c}} = 0 \leq p$, $x \not\leq p$ and $p$ is prime, we have $x^{\mathsf{c}} \leq p < x$, hence $x_c < x$, and hence finally $x = x \vee x^{\mathsf{c}} = 1$.

Let $B$ be the booleanization of the Heyting algebra $\Omega(\mathbb{R}) = \{U \subseteq \mathbb{R} \,|\, U \text{ open}\}$. Then it contains no maximal non-top element $V$ (the $V^{\mathsf{c}}$ would be minimal non-bottom element, and every open $U \subseteq \mathbb{R}$ contains a non-void open interval $(a, b)$; open intervals are obviously regular: $(a,b)^* = \mathbb{R} \smallsetminus \overline{(a,b)} = \mathbb{R} \smallsetminus \langle a, b\rangle = (-\infty, a) \cup (b, +\infty)$ and hence $(a,b)^{**} = \mathbb{R} \smallsetminus \overline{(-\infty, a) \cup (b, +\infty)} = \mathbb{R} \smallsetminus ((-\infty, a\rangle \cup \langle b, +\infty)) = (a, b)$).

Thus, there is no completely prime filter in $B$.

# MSe6

## Algebras

### Algebraic operations

An *n-ary operation* on $X$ is a mapping

$$\alpha : X^n = \overbrace{X \times \cdots \times X}^{n \text{ times}} \to X.$$

This is how one usually speaks of algebraic operations of finite arities, for more general ones we use the power notation (similarly like for relations)

$$X^M = \{\alpha \,|\, \alpha : M \to X\},$$

and $M$-ary operations are understood as mappings

$$\alpha : X^M \to X.$$

This convention is often of advantage also for the finite case.

### Algebras of type $\Delta$.

Recall that a type $\Delta = (\Delta_t)_{t\in T}$ is a system of arities $\Delta_t$.
It is said to be *finite* if $T$ and all the $\Delta_t$ are finite. In such case we usually write the arities as natural numbers, and so we do also in
*finitary types* where all the $\Delta_t$ are finite, but $T$ is not necessary so.

A typical algebra one encounters has several operations. One studies

*algebraic structures of a type* $\Delta = (\Delta_t)_{t\in T}$ *on sets* $X$,

that is

*collections* $\alpha = (\alpha_t)_{t\in T}$ *of* $\Delta_t$*-ary operations* $\alpha_t$,

and speaks of pairs $A = (X, \alpha)$ as of *algebras of type* $\Delta$.

**Notes.** 1. Speaking on an algebra of finite type as of finite algebra would be confusing, but one often speaks of algebras of finitary type as of finitary ones: there is no danger of confusion there.

2. The finiteness of the arities is of the essence, while the number of the operations hardly ever plays a role in general reasoning. The typical algebra we will discuss will be finitary ones.

3. Practically everything we will do will work simultaneously. Hence it simplifies the notation and does not reduce the information to do proofs as with single operations.

### Examples.

1. The algebras of standard arithmetic: natural numbers, or integers with addition and multiplication, rational, real and complex numbers (caution: division is not an operation in our definition, but appears as a specific property of the multiplication).

2. More generally, rings and fields.

3. Groups, semigroups and monoids.

4. Semilattices and lattices. Heyting or Boolean algebras.

5. Vector space (an algebra of finitary but not finite type); they will be often used for illustrating general phenomena).

## Homomorphisms between algebras.

A mapping $f : X \to Y$ is a *homomorphism* with respect to operations $\alpha$, $\beta$ if

$$\forall \xi : M \to X, \quad f(\alpha(\xi)) = \beta(f \cdot \xi). \qquad \text{(homom)}$$

In the finitary case this can be rewritten to the probably more transparent

$$f(\alpha(x_1, \dots, x_n)) = \beta(f(x_1), \dots, f(x_n));$$

If we use the (fairly standard) notation

$$x \Box y \quad \text{for} \quad \Box(x, y),$$

we get, of course, the even more transparent formula

$$f(x \Box y) = f(x) \Box f(y).$$

Still, even in the finitary case working with the formula (homom) may be of advantage.

A homomorphism $f$ with respect to $\alpha, \beta$ is an *isomorphism* if there exists a homomorphism $g$ with respect to $\beta, \alpha$ such that $fg = \mathrm{id}_Y$ and $gf = \mathrm{id}_X$.

*Endomorphism* resp. *automorphism* is a homomorphism resp. isomorphism $(X, \alpha) \to (X, \alpha)$.

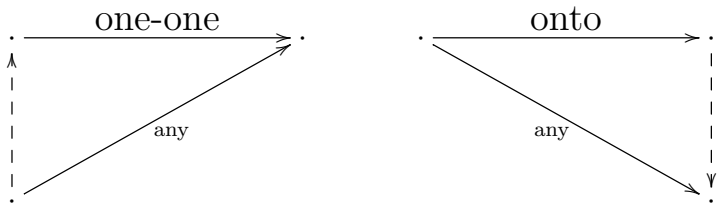
**Homomorphisms with respect to *algebraic structures*** $\alpha = (\alpha_t)_{t \in T}$, $\beta = (\beta_t)_{t \in J}$ are homomorphisms with respect to $\alpha_t$, $\beta_t$ for all $t$ simultaneously.

Obviously

> id : $(X, \alpha) \to (X, \alpha)$ *is an automorphism, and composition of homomorphisms is a homomorphism.*

**Proposition.** 1. *Let $f : (X, \alpha) \to (Y, \beta)$, $g : (Z, \gamma) \to (Y, \beta)$ be homomorphisms, $f$ one-to-one. Then a mapping $h : Z \to X$ such that $f \cdot h = g$ is a homomorphism.*

2. *Let $f : (X, \alpha) \to (Y, \beta)$, $g : (X, \alpha) \to (Z, \gamma)$ be homomorphisms, $f$ onto. Then a mapping $h : Z \to X$ such that $h \cdot f = g$ is a homomorphism.*




(The homomorphisms (indicated by full arrows) make maps (indicated by dashed arrows) homomorphisms.)

*Proof.* 1. We have $f(\alpha(\xi)) = \beta(f \cdot \xi)$ for $\xi : M \to X$ and $g(\gamma(\zeta)) = \beta(g \cdot \zeta)$ for $\zeta : M \to Z$. Thus,

$$f(h(\gamma(\xi))) = \beta(f \cdot h \cdot \xi) = f(\alpha(h \cdot \xi))$$

and since $f$ is one-to-one, $h(\gamma(\xi)) = \alpha(h \cdot \xi)$.

2. Choose a mapping $j : Y \to X$ such that $fj = \mathrm{id}$. Then

$$\begin{aligned} h(\beta(\zeta)) &= h(\beta(f \cdot j \cdot \zeta)) = h(f(\alpha(j \cdot \zeta))) = \\ &= g(\alpha(\mathrm{j} \cdot \zeta)) = \gamma(g \cdot j \cdot \zeta) = \gamma(h \cdot f \cdot j \cdot \zeta) = \gamma(h \cdot \zeta). \end{aligned}$$

**Corollary.** *A homomorphism that is one-to-one and onto is an isomorphism.*

**Remark.** This is specific for algebras. Note the contrast with with homomorphisms of relational systems: Here

every one-to-one homomorphism is a is a subobject,

and

every onto homomorphism is a quotient.

## Subalgebras.

Let $A = (X, \alpha)$, $\alpha = (\alpha_t)_{t \in T}$, be an algebra, let $Y \subseteq X$ and let $j : Y \subseteq X$ be the embedding map.

> If for every $t \in T$ and $\xi : \Delta_t \to Y$ the result $\alpha_t(j\xi)$ is in $Y$ ("$Y$ is closed under operations"),

we endow $Y$ with operations $(\alpha_t|Y)(\xi) = \alpha_t(j\xi)$ and speak of a

*subalgebra of $A$.*

In the finitary case, the condition is particularly transparent: We have

$$\forall t \in T, \quad \forall y_1, \ldots, y_{n_t} \in Y \quad \alpha_t(y_1, \ldots, y_{n_t}) \in Y.$$

Note that, unlike in a relational object, where every subset carries a subobject,

not every subset of an algebra carries a subalgebra.

Therefore there is no danger of confusion when we speak of subalgebras simply as of specific subsets of the algebra in question.

**Observations.** 1. *If $B = (Y, \alpha|Y)$ is a subalgebra of $A = (X, \alpha)$ then the embedding mapping $j : Y \subseteq X$ is a homomorphism.*

2. *For any homomorphism $f : B \to A$ the image $f[B]$ is a subalgebra of $A$.*

3. *If $f : B \to A$ is one-to-one then $f' : B \to f[B]$ defined by $f'(x) = f(x)$ is an isomorphism.*

**Proposition.** *The intersection of an arbitrary system of subalgebras is a subalgebra.*
*Proof.* Let $Y_i$, $i \in J$, be subalgebras of $A$; denote $j : Y = \bigcap Y_i \to X$, $j_i : Y_i \subseteq X$ and $k_i : Y \subseteq Y_i$. For any $i$ and $\xi : \Delta_t \to Y$ we have $\alpha_t(j\xi) = \alpha_t(j_i(k_i\xi)) \in Y_i$, and hence $\alpha_t(j\xi) \in \bigcap Y_i$.

The intersection of the void system of subalgebras is the whole of $A$ which, of course, is a subalgebra of itself.

## Subalgebra generated by a set.

For any subset $M$ of an algebra $A = (X, \alpha)$ we have, by the Proposition above, the smallest subalgebra containing $M$ namely

$$\bigcap \{Y \text{ subalgebra of } A \,|\, M \subseteq Y\}$$

This subalgebra is said to be generated by $M$ and denoted

$$\mathsf{Gen}(M).$$

If

$$\mathsf{Gen}(M) = A.$$

we say that $M$ generates the algebra $A$, and sometimes speak losely of a "set of generators of $A$."[1]

**Another description of generating.** Recall that there was another way of generating vector subspaces resp. the whole of the vector space, namely

*taking all linear combinations of the elements of $M$.*

Something like this can be done with algebras of any finitary type.
If $A = (X, \alpha)$ is an algebra of a finitary type $\Delta = (\Delta_t)_{t\in T}$, and if $M \subseteq X$ is an arbitrary subset then $\mathsf{Gen}(M) = M_\infty$ obtained as follows. Set

$$M_0 = M,$$
$$M_{k+1} = M_k \cup \{\alpha_t(x_1, \ldots, x_{n_t}) \,|\, t \in T,\ \{x_1, \ldots, x_{n_t}\} \subseteq M_k\},$$

and finally $\qquad M_\infty = \bigcup_{k=1}^{\infty} M_k$ .

[1] This is only a turn of phrase, of course. The elements of $M$ are nothing like individual generators of the $A$, only the whole of $M$ generates it.

Indeed: Obviously every subalgebra containing $M_k$ contains $M_\infty$. On the other hand, $M_\infty$ is a subalgebra since if $\{x_1, \dots, x_{n_t}\} \subseteq M_\infty$ then each of the $\xi(j)$ is in some $M_{k_j}$ and $\alpha(x_1, \dots, x_{n_t}) \in M_{k+1}$ where $k = \max k_j$.

**Note.** The procedure can stop at some finite step $M_{n+1} = M_n$. For instance for the vector spaces one has already $M_1 = M_2 = M_\infty$.

## A very important observation.

*If the type is finitary we obtain from the cardinality $|M|$ of $M$ the cardinality of the generated subalgebra*

$$|\mathsf{Gen}(M)| \leq \max(|M|, |T|, \omega_0).$$

*Hence for every cardinality $\alpha$ there is a cardinality $\beta$, such that the system of all distinct (up to isomorphism) algebras generated by sets of a cardinality smaller then $\alpha$ is a set of cardinality smaller than $\beta$.*

## Homomorphisms coinciding on generating sets.

**Proposition.** Let $f, g : A \to B$ be homomorphisms. Then the set

$$Z = \{x \mid f(x) = g(x)\}$$

is a subalgebra of $A$.

Proof. *Let $A = (X, \alpha)$ and $B = (Y, \beta)$. Denote by $j$ the embedding of $Z$ into $X$. Let $\xi : \Delta_t \to Z$ be arbitrary. Since $fj = gj$ we have $f(\alpha_t(j\xi)) = \beta_t(fj\xi) = \beta_t(gj\xi) = g(\alpha_t(j\xi))$ and hence $\alpha_t(j\xi) \in Z$.*

**A very important consequence.** *If $M$ generates an algebra $A$ and if homomorphisms $f, g : A \to B$ coincide on $M$ then $f = g$.*

# MSe7

## Repetition.

**Algebraic operations**: $n$-ary operations are mappings

$$\alpha : X^n = \overbrace{X \times \cdots \times X}^{n \text{ times}} \to X,$$

For general $M$-ary ones (including the finitary case when handier) we use the notation $X^M = \{\alpha \,|\, \alpha : M \to X\}$ and then $\alpha : X^M \to X$.

An **algebraic structure** of type $\Delta = (\Delta_t)_{t\in T}$ on $X$ is a system $\alpha = (\alpha_t)_{t\in T}$ of operations $\alpha_t : X^{\Delta_t} \to X$ and an algebra of type $\Delta$ is a pair $A = (X, \alpha)$.

We speak of a *finite type* if $T$ and all the $\Delta_t$ are finite, and of a *finitary type* if all the $\Delta_t$ are finite and $T$ is arbitrary.

A mapping $f : X \to Y$ is a *homomorphism* with respect to $\alpha$ and $\beta$ if

$$\forall \xi : M \to X, \quad f(\alpha(\xi)) = \beta(f \cdot \xi)$$

(in the finitary case this formula can be seen more transparently as

$$f(\alpha(x_1, \ldots, x_n)) = \beta(f(x_1), \ldots, f(x_n)).\ )$$

A *homomorphism* $f : (X, \alpha) \to (Y, \beta)$ *with respect to algebraic structures* $\alpha, \beta$ is a homomorphism with respect to the $\alpha_t, \beta_t$ for all the $t \in T$ simultaneously.

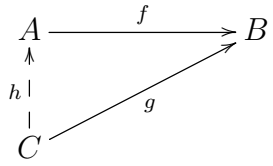
A homomorphism $f : (X, \alpha) \to (Y, \beta)$ is an *isomorphism* if there is an inverse homomorphim $g : (Y, \beta) \to (X, \alpha)$ satisfying $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$.

Homomorphisms $f : (X, \alpha) \to (X, \alpha)$ are referred to as *endomorphisms*, and if an endomorphism is an isomorphism we speak of an *automorphism*.

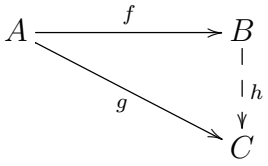
It is easy to check that,

- the identity map id : $(X, \alpha) \to (X, \alpha)$ is a homomorfism (automorphism), and that
- a composition of homomorphisms is a homomorphism.

**Specifically for algebras** (unlike for general relations) one has that if in a commutative diagram




$f$ is a one-to-one homomorphism and $g$ is any homomorphism then the mapping $h$ is a homomorphism, and if in a commutative




$f$ is a homomorphism onto and $g$ is any homomorphism then the mapping $h$ is a homomorphism.

**Corollary.** *A homomorphism that is one-to-one and onto is an isomorphism.*

**Subalgebras.** A subset $Y \subseteq (X, \alpha)$ with $\alpha = (\alpha_t)_{t\in T}$ such that

$$\forall t \in T \text{ and } \xi : \Delta_t \to Y,\ \alpha_t(j\xi) \in Y \qquad \text{(sub)}$$

can be endowed with an algebraic structure such that the embedding map $j : Y \to X$ is a homomorphism, namely with $\alpha|Y$ defined by $(\alpha_t|Y)(\xi) = \alpha_t(j\xi)$, and only on subsets satisfying (sub) there exists an algebraic structure making $j$ a homomorphism. Moreover, the $\alpha|Y$ is the only structure with this property. [1]

Hence one can work with subalgebras as special subsets (satisfying (sub)):

the suitable structure is uniquely determined.

The property (sub) is particularly transparent in a finite arity:

$$\forall t \in T, \quad \forall y_1, \ldots, y_{n_t} \in Y \quad \alpha_t(y_1, \ldots, y_{n_t}) \in Y.$$

[1] This is another strong contrast with relational systems where every subsets can be made to a subobject, and the subobject relations are not the unique ones making $j$ a homomorphisms.

We have made simple **Observations** that
*for every homomorphism $f : B \to A$, the image $f[B]$ is a subalgebra of $A$*
and that
*if a homomorphism $f : B \to A$ is one-to-one then the mapping $f' : B \to f[B]$ defined by $f'(x) = f(x)$ is an isomorphism.*

Next, an easy but important fact that

*the intersection of an arbitrary system of subalgebras is a subalgebra*

led to the definition of a **subalgebra generated by a subset** $M$,

$$\mathsf{Gen}(M) = \bigcap \{Y \text{ subalgebra} \mid M \subseteq Y\}.$$

and to the concept of *generating subset*.

Also we have proved that in case of a fintary type we can obtain $\mathsf{Gen}(M)$ as the $M_\infty$ from the following procedure:

$$\begin{aligned} &M_0 = M, \\ &M_{k+1} = M_k \cup \{\alpha_t(x_1, \ldots, x_{n_t}) \mid t \in T,\ \{x_1, \ldots, x_{n_t}\} \subseteq M_k\}, \\ &M_\infty = \bigcup_{k=1}^{\infty} M_k, \end{aligned}$$

which has **an important consequence** that for a finitary type
bounding the size of $M$ bounds the size of $\mathsf{Gen}(M)$.
Hence,

*up to isomorphism there is only a set of algebras of a given finitary type generated by sets of bounded size (cardinality).*

Finally, we have learned that

*for homomorphisms $f, g : A = (X, \alpha) \to (Y, \beta)$ the set $Z = \{x \mid f(x) = g(x)\}$ is a subalgebra of $A$.*

*Consequently, if $M$ generates $A$ and $f|M = g|M$ then je $f = g$.*

## Congruences and quotients of algebras.

Let $A = (X, \alpha = (\alpha_t)_{t\in T})$ be an algebra (of type $\Delta = (\Delta_t)_{t\in T}$). An eqiuvalence $E$ on $X$ is said to be a *congruence* on $A$ if

> for every $t \in T$, if $\xi, \eta : \Delta_t \to X$ are such that for every $d \in \Delta_t$ one has $\xi(d)E\eta(d)$, then also $\alpha_t(\xi)E\alpha_t(\eta)$.

This may be slightly confusing, hence look first at the more transparent case of finitary operations

$$\forall j, x_j E y_j \;\Rightarrow\; \alpha_t(x_1, \ldots, x_{n_t})E\alpha_t(y_1, \ldots, y_{n_t}).$$

and read the general definition again.

Denote by

$$q = (x \mapsto xE) : X \to X/E$$

the natural projection, and on $X/E$ define $\overline{\alpha}_t$

$$\overline{\alpha}_t(\xi) = q(\alpha_t(\eta)) \quad \text{where} \quad q\eta = \xi.$$

Thus obtained algebra (factoralgebra, quotient algebra, quotient) will be denoted by

$$A/E.$$

**Proposition.** 1. *$q : A \to A/E$ is a homomorphism onto.*

2. *The congruences on $A$ are precisely the relations*

$$E_h = \{(x, y) \,|\, h(x) = h(y)\}$$

*obtained from homomorphisms $h : A \to B$ to arbitrary algebras $B$.*

3. *If $h : A \to B$ is a homomorphism onto then there is an isomorphism $f : B \to A/E_h$ such that $fh = q$.*

## Products of algebras.

For a system $A_i = (X_i, \alpha^i)$, $i \in J$, of algebras of the same type $\Delta = (\Delta_t)_{t\in T}$ consider the cartesian product $X = \prod_{i\in J} X_i$ and the operations $\alpha_t$, $t \in T$ on $X$ given by

$$\alpha_t(\xi) = (\alpha_t^i(p_i\xi))_{i\in J}. \qquad (*)$$

The resulting algebra $A = (\prod_{i\in J} X_i, (\alpha_t)_{t\in T})$ is called the *product* of the system $A_i$, $i \in J$, and denoted by

$$\prod_{i\in J} A_i.$$

If the system is finite we write

$$A \times B, \quad A_1 \times \cdots \times A_n, \text{ etc.}$$

It is easy to see what is happening in the finitary case: the operations on the products are defined from the original ones coordinatewise:

$$\alpha_t((x_{1i})_{i\in J}, \ldots, (x_{nti})_{i\in J}) = (\alpha_t^i(x_{1i} \ldots, x_{nti}))_{i\in J}.$$

Unsurprisingly, very much like for general relational systems,[2] we obtain

**Theorem.** 1. *The projections* $p_j = ((x_i)_{i\in J} \mapsto x_j) : \prod_i A_i \to A_j$ *are homomorphisms.*

2. *For every system of homomorphisms*

$$f_i : B = (Y, (\beta_t)_{t\in T}) \to A_i, \quad i \in J,$$

*there exists precisely one homomorphism* $f : B \to \prod_i A_i$ *such that* $p_i f = f_i$ *for every* $i \in J$.

*Proof.* 1 follows immediately from the definition of $\alpha$.

2. We have precisely one mapping $f$ such that

$$\forall i, p_i f = f, \quad \text{namely} \quad f(y) = (f_i(y))_i.$$

Hence we have to prove that this $f$ is a homomorphism. We have, for every $i$, $f_i(\beta_t(\xi)) = \alpha_t^i(f_i\xi)$ so that

$$f(\beta_t(\xi)) = (f_i(\beta_t(\xi)))_i = (\alpha_t^i(f_i\xi))_i = (\alpha_t^i(p_i f\xi))_i = \alpha_t(f\xi).$$

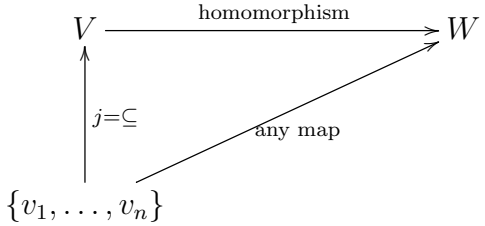
[2]Indeed there is no surprise, but nevertheless mark the recurring fact that we have observed with plain sets and plain mapings, relational objects and homomorphisms, posets and monotone maps, and may remember from metric spaces and continuous maps, that a specific important mapping is determined as a unique solution of a system of equations (namely the $f$ in $p_i f = f_i$).

# Free algebras.

In vector spaces we have something like "best" or smallest generating systems, the **bases**. They were both

- smallest in size (recall *dimension*), and
- minimal in the sense that no proper subset generated the algebra.

But the most important and characteristic property of a basis $v_1, \ldots, v_n$ of a vector space $V$ is that for any other vector space $W$ and any *mapping* $f : \{v_1, \ldots, v_n\} \to W$ there is precisely one *homomorphism* (*linear mapping*) $h : V \to W$ such that $h(v_i) = f(v_i)$.




This property is usually referred to as *freeness*: the elements of the basis are not bound by any formula that would prevent them to be sent to chosen elements (if, say, $v_3 = v_1 + 2v_2$ and $v_i$ is being sent to $x_i$ for $i = 1, 2$ then $v_3$ can be sent only to $x_1 + 2x_2$ and nowhere else).

> The fact that every vector space has a basis that is smallest and that such one is not only smallest in size, but also in the sense that they cannot be reduced, and has the extension of mappings to homomorphisms property is a specific property of these algebras. Even in so simple algebras as Abelian groups (simpler than vector spaces) this is generally lacking:
>
> E.g. in $\mathbb{Z}$ one has a minimal generating system $\{1\}$, but $M = \{6, 10, 15\}$ generates $\mathbb{Z}$ and no proper subset of $M$ does.
>
> Or, no generating subset of
>
> $$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$
>
> (addition mod $n$) has the property of extension of general mappings to homomorphisms: let $f : M \to \mathbb{Z}$ be extended to $h$. If $f(k) = x \neq 0$ we have $h(nk) = h(0) = nx \neq 0$, hence only constant 0 can be extended.

On the other hand, while the universal existence of such special generating sets is indeed a very specific property of vector spaces, we will see that in very general classes of algebras $\mathcal{A}$ we have an abundance of special objects that are thus generated.

Let $\mathcal{A}$ be a class of algebra and let $M$ be a set. A *free algebra over $M$* in $\mathcal{A}$ is an algebra $F(M) \in \mathcal{A}$ together with a mapping

$$\phi_M : M \to F(M)$$

such that

> for every algebra $A \in \mathcal{A}$ and for every *mapping* $f : M \to A$ there exists exactly one *homomorphism* $h : F(M) \to A$ such that $h \cdot \phi_M = f$.

If $\phi_M : M \to F(M)$ and $\phi_N : N \to F(N)$ are free algebras we see that

> *for every mapping $\xi : M \to N$ there is a uniquely determined homomorphism $F(\xi) : F(M) \to F(N)$ such that*
>
> $$F(\xi) \cdot \phi_M = \phi_N \cdot \xi.$$
>
> *Using the unicity we easily check that*
>
> $$F(\mathrm{id}) = \mathrm{id} \quad \textit{and} \quad F(\xi \cdot \eta) = F(\xi) \cdot F(\eta).$$

The mapping $\phi_M$ is in fact an embedding of $M$ into $F(M)$ as a generating subset. We have

**Proposition.** 1. *If $\mathcal{A}$ is a non-trivial class of algebras (that is, if there is an $A \in \mathcal{A}$ with more then one element) then $\phi_M : M \to F(M)$ is always one-to-one.*

2. *$\phi_M[M]$ generates the algebra $F(M)$.*

3. *If $F(M)$ exists then it is uniquely determined up to isomorphism.*

*Proof.* 1. Let $|A| \geq 2$. For $x \neq y$ in $M$ choose $f : M \to A$ such that $f(x) \neq f(y)$. For the asociated homomorphism we then have $h(\phi_M(x)) \neq h(\phi_M(x))$.

2. Take $k : M \subseteq \mathsf{Gen}(\phi_M[M])$ and $j : \mathsf{Gen}(\phi_M[M]) \subseteq F(M)$. Thus, $\phi_M = jk$. If $h : F(M) \to \mathsf{Gen}(\phi_M[M])$ is a homomorphism such that $h\phi_M = k$

we have $jh\phi_M = jk = \phi_M = \mathrm{id}\phi_m$ and hence, by the unicity in the definition, $jh = \mathrm{id}$ so that $j$ is a homomorphism onto and $\mathsf{Gen}(\phi_M[M]) = F(M)$.

3. Take the $h : F(M) \to F'$ and $h' : F' \to F(M)$ such that $h\phi_M = \phi'$ and $h'\phi' = \phi_M$. Thus, $h'h\phi_M = \phi_M$ and $hh'\phi' = \phi'$, and as also $\mathrm{id} \cdot \phi_M = \phi_M$ and $\mathrm{id} \cdot \phi' = \phi'$ we obtain $hh' = \mathrm{id}$ and $h'h = \mathrm{id}$ by unicity.

**Proposition.** *Let $q : A \to B$ be a homomorphism onto. Then for every homomorphism $h : F(M) \to B$ there exists a homomorphism $f : F(M) \to A$ such that $h = qf$.*

*Proof.* Choose a mapping $\xi : B \to A$ such that $q\xi = \mathrm{id}$. To $\xi h\phi_M : M \to A$ then take the homomorphism $f : F(M) \to A$ such that $f\phi_M = \xi h\phi_M$. Then $qf\phi_M = q\xi h\phi_M = h\phi_M$ and from the unicity (as both $qf$ and $h$ are homomorphisms) finally $qf = h$.

**Theorem.** *Let $\Delta = (\Delta_t)_{t\in T}$ be finitary and let $\mathcal{A}$ be a non-trivial class of algebras of type $\Delta$ closed under products,subalgebras and isomorphisms. Then for every set $M$ there is a free algebra over $M$ with respect to $\mathcal{A}$.*

*Proof.* Choose a subset $R \subseteq \mathcal{A}$ such that every $A \in \mathcal{A}$ which can be generated by a set with a cardinality $\leq |M|$ has an isomorphic copy in $R$. Set

$$U = \{u \,|\, u : M \to B_u \in R \text{ arbitrary map}\}.$$

Consider the product of algebras $p_v : \prod_{u\in U} B_u \to B_v$. It is

$$\underline{\text{also a product of the underlying sets}}$$

and hence there is a $\underline{\text{mapping}}$ $\psi : M \to \prod B_u$ determined by

$$p_u\psi = u \quad \text{for all} \quad u$$

As $\mathcal{A}$ is non-trivial there is for every $x \neq y$ in M a mapping $u \in U$ such that $u(x) \neq u(y)$ and hence $\psi$ has to be one-one. Restrict $\psi$ to

$$M \xrightarrow{\phi} F(M) = \mathsf{Gen}(\psi[m]) \xrightarrow{\iota} \prod B_u.$$

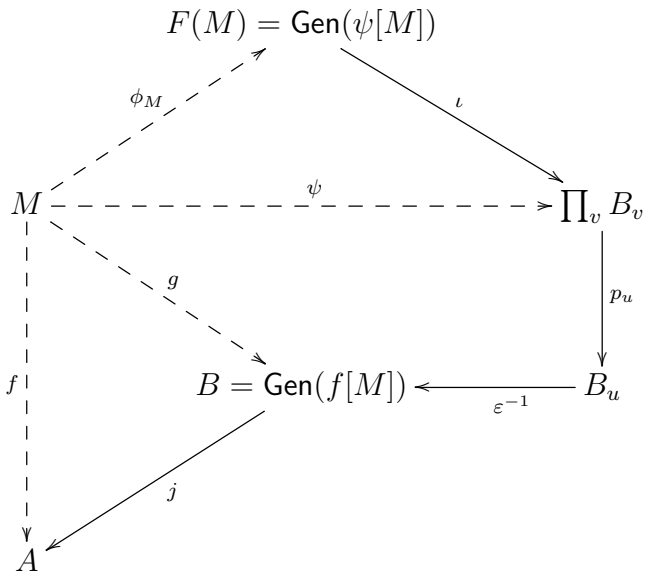
Decompose $f : M \to A \in \mathcal{A}$ to

$$M \xrightarrow{g} B \xrightarrow{j=\subseteq} A.$$

with $g$ and onto mapping, and set $B = \mathsf{Gen}(f[M])$. By the choice of $R$ there is an isomorphism $\varepsilon : B \to B' \in R$. Set

$$u = \varepsilon g \quad \text{and} \quad h = j\varepsilon^{-1}p_u\iota.$$

Now the situation is as in the diagram




where we denote by full arrows the mappings known as being homomorphisms, and where $j\phi_M = \psi$, $f = jg$ and $p_j\psi = \varepsilon g$. Now we have $h = j\varepsilon^{-1}p_u\iota$ a homomorphism and

$$h\phi_M = j\varepsilon^{-1}p_u\iota\phi_M = j\varepsilon^{-1}p_u\psi = j\varepsilon^{-1}u = j\varepsilon^{-1}\varepsilon g = jg = f.$$

The unicity follows from $F(M) = \mathsf{Gen}(\psi[m])$.

**Corollary.** *Let $\mathcal{A}$ be a non-trivial class of algebras of a finitary type closed under products, subalgebras and isomorphisms. Then each $A = (X, \alpha) \in \mathcal{A}$ is a quotient of a free algebra.*
(The $h : F(X) \to A$ such that $h\phi_X = \mathrm{id}_X$ is onto.)

# MSe8

## Repetition.

A **type** $\Delta = (\Delta_t)_{t\in T}$ is as for relational systems and we speak of a *finite type* if $J$ and all $\Delta_i$ are finite and, what is particularly important, of a *finitary type* if $\Delta_i$ are finite and $J$ is arbitrary.

The **subalgebra** $Y$ of an algebra $(X, \alpha)$ with $\alpha = (\alpha_t)_{t\in T}$ is a subset such that

for every $t \in T$ and $\xi : \Delta_t \to Y$ the result $\alpha_t(j\xi)$ is in $Y$.

Such $Y$ are precisely the subsets such that $j : Y \subseteq (X, \alpha)$ is a homomorphism for a suitable algebraic structure on $Y$, and there is only one such algebraic structure on $Y$, namely $(\alpha_t|Y)(\xi) = \alpha_t(j\xi)$.

We have learned that

*the intersection of an arbitrary system of subalgebras is a subalgebra.*

This further leads to the concept of the

subalgebra generated by a subset $M$, the smallest subalgebra contining $M$,

$$\mathsf{Gen}(M) = \bigcap\{Y \text{ subalgebra} \,|\, M \subseteq Y\},$$

and of the *generating set* for the whole algebra, namely such $M$ that $\mathsf{Gen}(M) = X$ – this is the case where there is no proper subalgebra containing $M$.

For finitary type, $\mathsf{Gen}(M)$ can also be obtained as the $M_\infty$ from the procedure

$$\begin{aligned} &M_0 = M,\\ &M_{k+1} = M_k \cup \{\alpha_t(x_1, \dots, x_{n_t}) \,|\, t \in T,\ \{x_1, \dots, x_{n_t}\} \subseteq M_k\},\\ &M_\infty = \bigcup_{k=1}^{\infty} M_k. \end{aligned}$$

This has a **very important consequence**: For a finitary type

> *for a fixed size $|M|$ of $M$ there is a fixed bound of the size of $\mathsf{Gen}(M)$, and consequently there exists a set of isomorphic representatives of all algebras of the type generated by sets of size $\leq |M|$.*

Finally we have learned that

> *for homomorphisms $f, g : A \to B$, $Z = \{x \,|\, f(x) = g(x)\}$ is a subalgebra of $A$.*
>
> *Consequently, if $M$ generates $A$ and $f|M = g|M$ then $f = g$.*

**Congruences.**
An equivalence $E$ on $X$ is a *congruence* on $A = (X, \alpha = (\alpha_t)_{t\in T})$ if

> for every $t \in T$, if $\xi, \eta : \Delta_t \to X$ are such that for every $d \in \Delta_t$ one has $\xi(d)E\eta(d)$, then also $\alpha_t(\xi)E\alpha_t(\eta)$.

For finitary operations, more transparently,

$$\forall j, x_j E y_j \;\Rightarrow\; \alpha_t(x_1, \ldots, x_{n_j})E\alpha_t(y_1, \ldots, y_{n_j}).$$

Denote by $q = (x \mapsto xE) : X \to X/E$ the natural projection, and on $X/E$ define $\overline{\alpha}_t(\xi) = q(\alpha_t(\eta))$ where $q\eta = \xi$.

**Proposition.** 1. *Congruences on $A$ are precisely the $E_h = \{(x, y) \,|\, h(x) = h(y)\}$ obtained from homomorphisms $h : A \to B$ to arbitrary $B$.*

2. *If $h : A \to B$ is a homomorphism onto then there is an isomorphism $f : B \to A/E_h$ such that $fh = q$.*

**Products.**
For a system $A_i = (X_i, \alpha^i)$, $i \in J$, of algebras of type $\Delta = (\Delta_t)_{t\in T}$ we consider on $X = \prod_{i\in J} X_i$ the operations $\alpha_t$, $t \in T$ by setting

$$\alpha_t(\xi) = (\alpha_t^i(p_i\xi))_{i\in J}.$$

The resulting algebra $A = (\prod_{i\in J} X_i, (\alpha_t)_{t\in T})$, denoted

$$\prod_{i\in J} A_i,$$

is called the *product* of the system $A_i$, $i \in J$. If the system is finite we write

$$A \times B, \quad A_1 \times \cdots \times A_n \ \text{ etc.}$$

> **Note.** The operations are obtained from the original ones coordinatewise. This is particularly well seen in the finitary case:
>
> $$\alpha_t((x_{1i})_{i\in J}, \ldots, (x_{n_t i})_{i\in J}) = (\alpha_t^i(x_{1i} \ldots, x_{n_t i}))_{i\in J}.$$

**Theorem.** 1. *The projections* $p_j = ((x_i)_{i\in J} \mapsto x_j) : \prod_i A_i \to A_j$ *are homomorphisms.*

2. *For every system of homomorphisms*

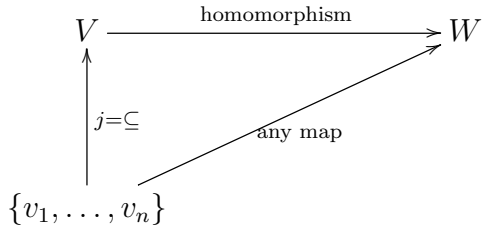
$$f_i : B = (Y, (\beta_t)_{t\in T}) \to A_i, \quad i \in J,$$

*there exists precisely one homomorphism* $f : B \to \prod_i A_i$ *such that* $p_i f = f_i$ *for every* $i \in J$.

# Free algebras.

**Bases in vector spaces.** The most important characterization of such particular generating systems (we speak of the finite ones, but the situation of infinite bases is similar) $\{v_1, \dots, v_n\} \subseteq V$ is that

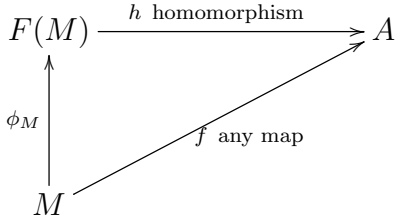
> for any other vector space $W$ and any *mapping* $f : \{v_1, \dots, v_n\} \to W$ there is precisely one *homomorphism* (*linear mapping*) $h : V \to W$ with $h(v_i) = f(v_i)$.




This we have in all vector spaces. In general classes $\mathcal{A}$ of algebras, this happens in special objects only, namely in the **free algebras.**

Let $M$ be a set. A *free algebra over $M$ with respect to $\mathcal{A}$* is

> an algebra $F(M) \in \mathcal{A}$ together with a mapping $\phi_M : M \to F(M)$ such that for every $A \in \mathcal{A}$ and every mapping $f : M \to A$ there exists exactly one homomorphism $h : F(M) \to A$ such that $h \cdot \phi_M = f$. Thus we have a commutative diagram



Let $\phi_M : M \to F(M)$ and $\phi_N : N \to F(N)$ be free algebras. We have

**Proposition.** *For every mapping $\xi : M \to N$ there is a uniquely determined homomorphism $F(\xi) : F(M) \to F(N)$ such that*

$$F(\xi) \cdot \phi_M = \phi_N \cdot \xi.$$

*One has*

$$F(\mathrm{id}) = \mathrm{id} \quad \textit{and} \quad F(\xi \cdot \eta) = F(\xi) \cdot F(\eta).$$

(Consider the map $h = \phi_N \xi$. For the second display use the unicity.)

**Proposition.** 1. *If $\mathcal{A}$ is a non-trivial class of algebras, then $\phi_M : M \to F(M)$ is always one-to-one.*

2. *$\phi_M[M]$ generates the algebra $F(M)$.*

3. *If $F(M)$ exists then it is uniquely determined up to isomorphism.*

Later we will need the following fact. It will be referred to as

## Proposition ($*$).

**Proposition.** *Let $q : A \to B$ be a homomorphism onto. Then for every homomorphism $h : F(M) \to B$ there exists a homomorphism $f : F(M) \to A$ such that $h = qf$.*

*Proof.* Choose a mapping $\xi : B \to A$ such that $q\xi = \mathrm{id}$. To $\xi h \phi_M : M \to A$ then take the homomorphism $f : F(M) \to A$ such that $f\phi_M = \xi h \phi_M$. Then $qf\phi_M = q\xi h\phi_M = h\phi_M$ and from the unicity (as both $qf$ and $h$ are homomorphisms) finally $qf = h$.

We have also proved the following

**Theorem.** *Let $\Delta$ be finitary and let $\mathcal{A}$ be a non-trivial class of algebras of type $\Delta$ closed under products, subalgebras and isomorphisms. Then for every set $M$ there is a free algebra over $M$ with respect to $\mathcal{A}$*

with

**Corollary.** *Let $\mathcal{A}$ be a non-trivial class of algebras of a finitary type closed under products, subalgebras and isomorphisms. Then each $A = (X, \alpha) \in \mathcal{A}$ is a quotient of a free algebra.*
(The $h : F(X) \to A$ such that $h\phi_X = \mathrm{id}_X$ is onto.)

## Free algebras in $\mathsf{Alg}((n_t)_{t\in T})$:

We will present an explicit description of the free algebras in the whole of $\mathsf{Alg}((n_t)_{t\in T})$.
The point is, of course, not in the existence of free algebras: this follows from the general theorem. Rather, we will describe an algebra of "names for the derived operations" which will enable us to formulate axioms of equality type.

Let $\Delta = (n_t)_{t\in T}$ be a finitary type and let $M$ be an arbitrary set. For a $t \in T$ choose distinct symbols $\sigma_t$, and add one more, say $\lambda$.[1]
Now define *terms* $w$ and their degrees $|w|$ as follows:

- $\lambda$ is a term and $|\lambda| = 1$,
- if $w_1, \dots, w_{n_t}$ are terms then $w = \sigma_t \cdot w_1 w_2 \dots w_{n_t}$ is a term and $|w| = \sum_{j=1}^{n_t} |w_j|$; if $n_t = 0$ then $\sigma_t$ is a term and $|\sigma_t| = 0$.

*Free expressions* (more precisely, *free $M$-expressions*) are

$$w[x_1 x_2 \dots x_n]$$

where $w$ is a term and $x_1 \dots x_n$ is a word of length $|w|$ in the elements of $M$; if $|w| = 0$ the word is void.

**Note:** The terms encode the derived operations in which all the entries are distinct (thus we could e.g. represent the quaternary operation $(ab)+(cd)$ but not the ternary $(ab)+(ad)$). The general derived operations are represented by the free expressions: the words $[x_1, \dots, x_n]$ indicate, roughly speaking, how, and with what repetitions the variables enter.

On the set of all free expressions define operations $\omega_t$, $t \in T$, by setting

$$\omega_t(w_1[x_1^1 \dots], \dots, w_{n_t}[x_1^{n_t} \dots]) = \sigma_t \cdot w_1 \dots w_{n_t}[x_1^1 \dots x_{|w_1|}^1 x_1^2 \dots x_{|w_2|}^2 \ \dots \ x_1^{n_t} \dots],$$

denote the obtained algebra of type $\Delta$ by $F(M)$, and consider it together with the mapping

$$\phi = (x \mapsto \lambda[x]) \colon M \to F(M).$$

[1] This is a proviso for the trivial operation of identity that plays no role in choosing homomorphisms among mappings, but does play a role in constructing derived operations.

Now let $A = (X, (\alpha_t)_t)$ be an algebra from $\mathsf{Alg}((n_t)_{t\in T})$. The *interpretations of terms $w$ in $A$* are the mappings $\overline{w}$ defined recursively by

$$\begin{aligned}\overline{\lambda} &= \mathrm{id},\\ \overline{\sigma_t.w_1\dots w_{n_t}} &= \alpha_t \circ (\overline{w}_1 \times \dots \times \overline{w}_{n_t})\end{aligned}$$

($\circ$ is here the composition of mappings and $(f \times g)(x, y) = (f(x), f(y))$).

If $f\colon M \to A$ is a mapping define

$$h\colon F(M) \to A$$

by setting

$$h(w[x_1 \dots x_m]) = \overline{w}(f(x_1), \dots, f(x_m)).$$

We will show that it is a homomorphism:

$$\begin{aligned}h(\omega_t(w_1[x_1^1\dots], w_2[x_1^2\dots], \dots)) &= h(\sigma_t \cdot w_1 \dots w_{n_t}[x_1^1 \dots x_1^2 \dots \ \dots \ x_1^{n_t} \dots])\\ &= \overline{\sigma_t \cdot w_1 \dots w_{n_t}}(f(x_1^1), \dots, f(x_1^2), \dots, \ \dots \ , f(x_1^{n_t})\dots)\\ &= \alpha_t(\overline{w}_1(f(x_1^1), \dots), \overline{w}_2(f(x_1^2), \dots), \ \dots \ , \overline{w}_{n_t}(f(x_1^{n_t}), \dots))\\ &= \alpha_t(h(w_1[x_1^1, \dots]), h(w_2[x_1^2, \dots]), \ \dots \ , h(w_{n_t}[x_1^{n_t}, \dots])).\end{aligned}$$

We have $h(\lambda[x]) = f(x)$; the algebra $F(M)$ is generated by the set $\{\lambda[x] \mid x \in M\}$ and hence this homomorphism is unique.

# Mixing products, subobjects and quotients.

**Proposition.** *Let $h : (X, \alpha) \to (Y, \beta)$ be onto, and let $j : C \subseteq B$ be an embedding of subalgebra. Then $A' = h^{-1}[C]$ is a subalgebra of $A$ and the restriction $h' : A' \to C$ of $h$ is a homomorphism onto.*
*Consequently, a subalgebra of a factoralgebra of $A$ is isomorphic with a factoralgebra of a subalgebra of $A$.*

*Proof.* Let $\iota : h^{-1}[C] \subseteq A$ be an embedding of the subset, let $t \in T$ and let $\xi : \Delta_t \to h^{-1}[C]$ be a mapping. For $jh'\xi$ we have $\beta_t(jh'\xi) \in C$. By the definition of homomorphism, $h(\alpha_t(\iota\xi)) = \beta_t(h\iota\xi) = \beta_t(jh'\xi)$ and hence $\alpha_t(\iota\xi) \in h^{-1}[C]$.

**Observation.** *If $h_i : A_i \to B_i$, $i \in J$, are onto then the $h : \prod A_i \to \prod B_i$ determined by $p_i^B h = h_i p_i^A$ is onto as well. The product $\prod A_i/E_i$ of factoralgebras is hence isomorphic with a factoralgebra of the product $\prod A_i$.*
($h$ is given by the formula $h((x_i)_{i\in J}) = (h_i(x_i))_{i\in J}$.)

**Proposition.** *A product of subalgebras of $A_i$ is a subalgebra of the product of $A_i$.*
*That is, if $j_i : B_i \to A_i$ are embeddings of subalgebras then the $j : \prod_i B_i \to \prod_i A_i$ determined by $p_i^A j = j_i p_i^B$, $i \in J$, is an embedding of a subalgebra.*
*Proof.* The equations $p_i^A j = j_i p_i^B$, $i \in J$, determine a homomorphism. Thus, it suffices to prove that it is one-to-one. Now if $(b_i)_i \neq (b'_i)_i$ then for some $k$, $b_k \neq b'_k$ and hence $p_k j((b_i)_i) = j_k(b_k) \neq j_k(b'_k) = p_k j((b'_i)_i)$ and $j((b_i)_i) \neq j((b'_i)_i)$.,

# Varieties of algebras.

In the sequel, the classes of algebras $\mathcal{A}$ will be closed under isomorphisms and the type will be finitary.

**The extensions $\mathsf{S}$, $\mathsf{P}$ and $\mathsf{H}$.** For a class of algebras $\mathcal{A}$ define

$$\mathsf{S}\mathcal{A} = \{B \mid \exists \text{ a one-to-one } j : B \to A \in \mathcal{A}\},$$
$$\mathsf{P}\mathcal{A} = \{\prod_{i\in J} A_i \mid (A_i)_{i\in J} \text{ arbitrary collection in } \mathcal{A}\}$$
$$\mathsf{H}\mathcal{A} = \{B \mid \exists \text{ an onto } h : A \to B,\ A \in \mathcal{A}\}.$$

Thus, $\mathsf{S}\mathcal{A}$ is the class $\mathcal{A}$ extended by all the subalgebras, $\mathsf{P}\mathcal{A}$ is extended by products, and $\mathsf{H}\mathcal{A}$ is extended by factoralgebras.

**Note.** This is a standard notation. $\mathsf{S}\mathcal{A}$ comes from "**S**ubalgebras", $\mathsf{P}\mathcal{A}$ from "**P**roducts", and. $\mathsf{H}\mathcal{A}$ comes from "**H**omomorphic images".

**Proposition.** $\mathsf{HSP}\mathcal{A}$ *is the smallest class of the given type containing $\mathcal{A}$ and closed under subalgebras, products and factoralgebras.*

*Proof.* Trivially

$$\mathsf{SS}\mathcal{A} = \mathsf{S}\mathcal{A},\ \mathsf{PP}\mathcal{A} = \mathsf{P}\mathcal{A} \quad \text{and} \quad \mathsf{HH}\mathcal{A} = \mathsf{H}\mathcal{A}.$$

Using the statementss above we obtain

$$\mathsf{SH}\mathcal{A} \subseteq \mathsf{HS}\mathcal{A},\ \mathsf{PH}\mathcal{A} \subseteq \mathsf{HP}\mathcal{A} \text{ and } \mathsf{PS}\mathcal{A} \subseteq \mathsf{SP}\mathcal{A}.$$

Hence

$$\begin{aligned}
&\mathsf{S}(\mathsf{HSP}\mathcal{A}) \subseteq \mathsf{HSSP}\mathcal{A} = \mathsf{HSP}\mathcal{A},\\
&\mathsf{P}(\mathsf{HSP}\mathcal{A}) \subseteq \mathsf{HPSP}\mathcal{A} \subseteq \mathsf{HSPP}\mathcal{A} = \mathsf{HSP}\mathcal{A} \ \text{ and}\\
&\mathsf{H}(\mathsf{HSP}\mathcal{A}) = \mathsf{HSP}\mathcal{A}.
\end{aligned}$$

On the other hand, if $\mathcal{B} \supseteq \mathcal{A}$ is closed under subalgebras, products and factoralgebras then obviously $\mathcal{B} \supseteq \mathsf{HSP}\mathcal{A}$.

**Axioms that are equalities.** Take classes of algebras like

groups, abelian groups, vector spaces,
semigroups, monoids,
rings of various types,
lattices, distributive lattices, Boolean algebras,
or semilattices.

What they have in common is that they are are constituted by algebras of that or other type subjected to

*axioms that are equalities between formulas.*

More precisely, there are given basic operations and some fixed derived ones, and some pairs of the latter are postulated to coincide.
Since we can encode derived operations we describe it as follows.

Take a fixed countable set

$$\Omega = \{v_1, v_2, \ldots, v_n, \ldots\} \quad (v_i \text{ distinct})$$

(tokens to be used to determine the order and repetition of variables).
An equation–axiom satisfied in an algebra $A$ can be given by fixing a pair $u, v \in F(\Omega)$ and postulating that

for every homomorphism $h : F(\Omega) \to A$ we have $h(u) = h(v)$.

**This leads to the following:**
Let $M$ be a set and $E$ an arbitrary subset of the product $F(M) \times F(M)$. Define

$$\mathcal{M}_M(E) = \{A \,|\, \forall\ h : F(M) \to A,\ \forall (u,v) \in E,\ h(u) = h(v)\}.$$

Thus, $\mathcal{M}_M(E)$ is the class of all the algebras satisfying the equalities encoded in $E$. We speak of

*varieties*, or *equational classes of algebras;*

or, sometimes one speaks of *classes of models* of (the theory) $E$.

**Proposition.** *Every variety of algebras is closed under subalgebras, products and factoralgebras.*

*Proof.* Consider an $\mathcal{A} = \mathcal{M}_M(E)$, an $A \in \mathcal{A}$ and a $(u,v) \in E$.

If $j : B \to A$ is a one-one homomorphism and $h : F(M) \to B$ a homomorphism, then $jh$ is a homomorphism to $A$, hence $jh(u) = jh(v)$ and finally $h(u) = h(v)$.

If $q : A \to B$ is a homomorphism onto and $h : F(M) \to B$ a homomorphism, take by Proposition $(*)$ on page 5 a homomorphism $f : F(M) \to A$ such that $qf = h$ to obtain $h(u) = qf(u) = qf(v) = h(v)$.

Finally take $A_i \in \mathcal{A}$ and a homomorphism $h : F(M) \to \prod_J A_i$. Then for each $i$, $p_i h(u) = p_i h(v)$ and hence $h(u) = (p_i h(u))_{i \in J} = (p_i h(v))_{i \in J} = h(v)$.

Going in the opposite direction, for an arbitrary class of algebras $\mathcal{A} \subseteq \mathsf{Alg}(\Delta)$ set

$$\mathcal{E}_M(\mathcal{A}) = \{(u,v) \in F(M) \times F(M) \,|\, \forall\ h : F(M) \to A \text{ with } A \in \mathcal{A},\ h(u) = h(v)\}.$$

The following facts are immediate.

$$\begin{aligned} \mathcal{A} \subseteq \mathcal{B} \quad &\Rightarrow \quad \mathcal{E}_M(\mathcal{A}) \supseteq \mathcal{E}_m(\mathcal{B}), \\ E_1 \subseteq E_2 \quad &\Rightarrow \quad \mathcal{M}_M(E_1) \supseteq \mathcal{M}_M(E_2), \\ \mathcal{A} \subseteq &\mathcal{M}_M(\mathcal{E}_M(\mathcal{A})), \\ E \subseteq &\mathcal{E}_M(\mathcal{M}_M(E)). \end{aligned}$$

Thus, the operators $\mathcal{M}_M$ and $\mathcal{E}_M$ are in a something like a "contravariant Galois adjunction" (we ignore set theoretical troubles, of course).

Given a class of algebras $\mathcal{A}$, we obtain (an encoding of) the system of all the equalities satisfied by all the algebras from $\mathcal{A}$: $\mathcal{E}_\Omega(\mathcal{A})$ is the system of the

equalities that generally hold in $\mathcal{A}$. ($\Omega$ is a countable set containing enough tokens to indicate the order and repetitions of the entries in the operations; for technical reasons one uses in proofs other sets $M$ as well).
Roughly speaking, if the class is nice enough, it is then determined by this system of equalities. There holds

**Theorem.** (Birkhoff's theorem on varieties.) *A class of algebras $\mathcal{A} \subseteq \mathsf{Alg}(\Delta)$ is a variety if and only if it is closed under isomorphisms, subalgebras, products and factoralgebras.*

**Corollary.** *Let $\mathcal{A} \subseteq \mathsf{Alg}(\Delta)$ be a class of algebras. Then $\mathsf{HSP}\mathcal{A}$ is the smallest variety containing $\mathcal{A}$.*

## Appendix I: Proof of Birkhoff Theorem.

**1. Lemma.** *Let $F(M)$ be a free algebra in $\mathsf{Alg}((n_t)_{t\in T})$. Let $X$ be a finite subset of $F(M)$. Then there is a finite $K \subseteq M$ such that $X \subseteq F(K)$.*

*Proof.* It suffices to take the set of all the elements $x$ that appear in among the $x_j$ in $w[x_1, \dots x_n] \in X$.

**2. Lemma.** *Let $\mathcal{A}$ be a class of algebras closed under subalgebras (that is, $\mathcal{A} = \mathsf{S}\mathcal{A}$). Then $\mathcal{E}_M\mathcal{A}$ is the intersection of all the congruences $E$ on $F(M)$ such that $F(M)/E$ is in $\mathcal{A}$.*

*Proof.* By the definition, $(u, v) \in \mathcal{E}_M(\mathcal{A})$ iff

$$\forall\ h : F(X) \to A,\ A \in \mathcal{A},\ (u, v) \in E_h.$$

Obviously we can restrict ourselves to the homomorphisms that are onto and hence

$$\mathcal{E}_M(\mathcal{A}) = \bigcap\{E_h \,|\, h : F(M) \to A,\ A \in \mathcal{A},\ \text{ is a homomorphism onto}\}.$$

**3. Lemma.** *Let $E_i$, $i \in J$, be a system of congruences on an algebra $A$. Then $A/\bigcap_i E_i$ is isomorphic with a subalgebra of the product $\prod_J A/E_i$.*

*Proof.* Represent $E_i$ as $E_{h_i}$ with onto homomorphisms $h_i : A \to A_i = A/E_i$ and consider the product $\prod A_i$ and the homomorphism $h : A \to \prod A_i$ defined by $p_i h = h_i$. Then

$$h(x) = h(y) \quad \text{iff} \quad \forall i, h_i(x) = h_i(y)$$

and hence $h$ maps $A$ onto a subalgebra of $\prod_J A_i$.

From 2 and 3 we immediately obtain

**4. Corollary.** *Let $\mathcal{A}$ be a class of algebras closed under subalgebras and products. Then $F(M)/\mathcal{E}_M\mathcal{A}$ is in $\mathcal{A}$.*

**5. Proposition.** *Let $A \in \mathcal{M}_\Omega\mathcal{E}_\Omega\mathcal{A}$ and let there exist an onto homomorphism $h : F(M) \to A$. Then $A \in \mathcal{M}_M\mathcal{E}_M\mathcal{A}$.*

*Proof.* For $(u, v) \in \mathcal{E}_M(\mathcal{A})$ we can choose a finite subset $K \subseteq M$ such that $u, v \in F(K)$. Choose $K_0 \subseteq \Omega$ and mappings $\gamma : \Omega \to M$ and $\overline{\gamma} : M \to \Omega$ the restrictions of which to $K_0$ and $K$ are mutually inverse. Set

$$f = F(\gamma) : F(\Omega) \to F(M) \quad \text{and} \quad \overline{f} = F(\overline{\gamma}) : F(M) \to F(\Omega).$$

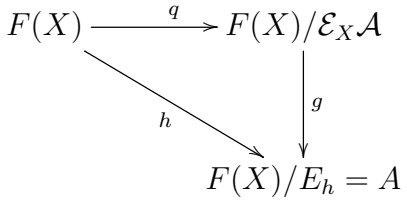
For $x \in F(K_0)$ and $y \in F(K)$ we then easily see that

$$\overline{f}f(x) = x \quad \text{and} \quad f\overline{f}(y) = y$$

Thus for $u_0 = \overline{f}(u)$ and $v_0 = \overline{f}(v)$ and an arbitrary homomorphism $h : F(\Omega) \to B \in \mathcal{A}$ one has $h(u_0) = h\overline{g}(u) = h\overline{f}(v) = h(v_0)$ so that $(u_0, v_0) \in \mathcal{E}_\Omega\mathcal{A}$.

Now let $A$ be an arbitrary algebra from $\mathcal{M}_\Omega\mathcal{E}_\Omega\mathcal{A}$ and let $h : F(M) \to A$ be an arbitrary homomorphism. For a $(u, v) \in \mathcal{E}_M\mathcal{A}$ take the $u_0, v_0$ and $f$ as above. Then we have $(u_0, v_0) \in \mathcal{E}_\Omega\mathcal{A}$ and hence $hf(u_0) = hf(v_0)$. This means, however, that $h(u) = hf\overline{f}(u) = hf(u_0) = hf(v_0) = hf\overline{f}(v) = h(v)$ and hence finally $A \in \mathcal{M}_M\mathcal{E}_M\mathcal{A}$.

**Proof of Birkhoff theorem on varieties.**
Let $\mathcal{A} = \mathsf{HSP}\mathcal{A}$. We will prove that $\mathcal{A} = \mathcal{M}_\Omega E$ where $E = \mathcal{E}_\Omega\mathcal{A}$. Suppose $A \in \mathcal{M}_\Omega\mathcal{E}_\Omega\mathcal{A}$. Since $A$ is in $\mathcal{A} \subseteq \mathsf{Alg}((n_t)_{t\in T})$ there exists a homomorphism $h$ mapping $F(X)$ onto $A$ and hence by 5 we have $A \in \mathcal{M}_X\mathcal{E}_X\mathcal{A}$ and hence by 3 we have $\mathcal{E}_X\mathcal{A} \subseteq E_h$ and hence a composition of onto maps




(with $q : F(X) \to F(X)/\mathcal{E}_X\mathcal{A}$ sending $x$ to $x\mathcal{E}_X\mathcal{A}$). By 4 we have $F(X)/\mathcal{E}_X\mathcal{A} \in \mathcal{A}$, and since $g$ is onto, $A \in \mathsf{H}\mathcal{A} = \mathcal{A}$.

We have proved that $\mathcal{M}_\Omega\mathcal{E}_\Omega\mathcal{A} \subseteq \mathcal{M}_\Omega\mathcal{E}_\Omega\mathcal{A} \subseteq \mathcal{A}$; the inclusion $\mathcal{A} \subseteq \mathcal{M}_M(\mathcal{E}_M(\mathcal{A}))$ is a general fact.

## Appendix II: Notes on some everyday-life algebras.

**1.** We will point out some particular features of the *associative law*

$$\begin{aligned} &\alpha(a,\alpha(b,c)) = \alpha(\alpha(a,b),c) \quad \text{that is,} \\ &a\cdot(b\cdot c) = (a\cdot(b\cdot c) \quad (\text{or just} \quad a(bc) = (ab)c\ ) \end{aligned} \tag{assoc}$$

in the representation of a binary operation as $\alpha(x,y) = x\cdot y$ or simply by juxtaposition $xy$.

An algebra $(X,\cdot)$ of type (2) with an associative operation is called a *semigroup*; if there is, moreover, a unit $e$ with

$$x\cdot e = e\cdot x = x \quad \text{for all} \quad x$$

we speak of the algebra $(X,\cdot,e)$ of type (2,0) as of a *monoid*.

**1.1. Extending a semigroup to a monoid.** *Every semigroup $(X,\cdot)$ can be extended to a monoid $(X_1,\cdot,e)$.*
(It suffices to take an $e\notin X$ and define on $X_1 = X\cup\{e\}$ the operation as $a\cdot b$ for $a,b\in X$ and $a\cdot e = e\cdot a = a$ for all $a$. Obviously (assoc) holds generally.)

**1.2. Proposition.** *Every monoid $M$ is isomorphic to a monoid of maps $\widetilde{M}\subseteq M^M$ with composition $\circ$ as the binary operation and the identity map as the unit.*
*Proof.* For $a\in M$ define $\widetilde{a}\colon M\to M$ by setting $\widetilde{a}(x) = ax$. Then we have $\widetilde{a}(\widetilde{b}(x)) = \widetilde{a}(bx) = a(bx) = (ab)x = \widetilde{ab}(x)$, hence $\widetilde{(ab)} = \widetilde{a}\circ\widetilde{b}$. Obviously $\widetilde{e} = \mathrm{id}$. For $a\neq b$ we have $\widetilde{a}(e) = a\neq b = \widetilde{b}(e)$ and hence $a\mapsto\widetilde{a}$ is one-to-one.

**Notes.** 1. Combining 1.1 with 1.2 we see that every semigroup is isomorphic to a semigroup of maps $X\to X$ with composition $\circ$ as the binary operation.

2. Thus, composition is a universal associative binary operation. Compare this phenomenon with the fact that every relation of order can be represented as the inclusion relation on a suitable system of sets.

3. Students have probably encountered a special case of this fact, namely that

*every group is (isomorphic to) a group of permutations.*

**2. Cayley representation.** We have seen that every monoid is isomorphic to *some* monoid of maps $X\to X$ with the operation of composition. In fact it can be represented as the monoid of *precise all endomorphisms* of an algebra.

For a monoid $M$ and $a \in M$ define *left shifts* $L_a\colon M \to M$ and *right shifts* $R_a\colon M \to M$ by setting

$$L_a(x) = ax \quad \text{and} \quad R_a(x) = xa.$$

**2.1. Proposition.** *A mapping $f\colon M \to M$ is a left shift iff for every $a \in M$, $f \circ R_a = R_a \circ f$.*
*Proof.* Obviously $L_b(R_a(x)) = bxa = R_a(L_b(x))$.

Now let $f \circ R_a = R_a \circ f$ for all $a$. Then in particular for $b = f(e)$,

$$f(a) = f(ea) = f(R_a(e)) = R_a(f(e)) = f(e)a = L_b(a).$$

**Note.** Hence, the $L_b$ (that is, the $\widetilde{b}$ from 1.2) are precisely the endomorphisms $M \to M$ with respect to the system of unary operations $(R_a)_{a\in M}$. This (perhaps not very surprising) statement is a part of a much more involved theory showing, a.o. that each monoid is for any type $\Delta$ with sum at least 2 (hence for instance (2) or (1,1)) isomorphic to an endomorphism monoid of an algebra $(X, \alpha) \in \mathsf{Alg}(\Delta)$. There holds much more than that with other than algebraic structures, too.

**3. Distributivity in rings.** Rings are an extremely important kind of algebras $(X, +, \cdot, \iota, 0)$ of type (2,2,1,0) where

- $(X, +, \iota, 0)$ is an abelian group,
- $(X, \cdot)$ is a semigroup,
- and the operations $+$ and $\cdot$ satisfy the *distributive laws*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

It is of some interest that the two distributive laws have <u>distinct</u> natural interpretations in the mappings $\widetilde{a}\colon X \to X$ associated with the elements $a \in X$ as in 1.2.
The former one says that

$$\widetilde{a}(x + y) = \widetilde{a}(x) + \widetilde{a}(y),$$

that is, that each $\widetilde{a}$ is a homomorphism with respect to the operation $+$[2], while the other,

$$\widetilde{(a+b)}(x) = \widetilde{a}(x) + \widetilde{b}(x),$$

does not say much of the nature of the individual maps $\widetilde{a}$ (the left shifts $L_a$ from 10.1.4), but does say that they naturally add following the addition in $X$.

**4. A few remarks on fields.** An everyday algebraic system one is encountered with is a ring with unit that allows, besides the subtraction $a - b$ (associated with the addition) also a division (associated similarly with the multiplication). That is, a system of numbers in which one assumes that

$$\text{for every } a \neq 0, \text{ there is a } b \text{ such that } ab = ba = 1. \tag{div}$$

Rings with this property are called *fields*.[3] The reader certainly recalls the fields of

*rational numbers, reals* or *complex numbers.*

The element $b$ with the property indicated above is uniquely determined: indeed, if $c$ also satisfies (div) we have

$$c = c(ab) = (ca)b = b.$$

Nevertheless, the correspondence $a \mapsto a^{-1}$ cannot be thought of as an operation because it is not defined for every $a$: since $0 \cdot x = 0$ for every $x$, (div) can be never satisfied for $a = 0$.
Moreover,

> *the system of fields cannot be made to a variety of algebras by a formal definition of* $0^{-1}$

for the simple reason that products of fields are obviously typically not fields — property (div) is very seldom preserved by products. However, it is a very important class of algebras, and we will add a few notes about it.

**4.1. Euclidean spaces as fields.** It is a very useful fact that the Euclidean line $\mathbb{E}_1$ can be treated as the "real line" $\mathbb{R}$, that is, enriched by the structure

[2]Which makes it in fact an endomorphism of the abelian group.

[3]Often one also assumes general commutativity of the multiplication; non-commutative rings with (div) are usually called *skew fields* or *division rings*.

of a field. When one recalls that also the Euclidean plane $\mathbb{E}_2$ can be viewed as the field $\mathbb{C}$ of complex numbers, and realizes the usefulness of complex analysis based on computing in this field, so different from the real one, one becomes eager to know whether something like this can be done with other Euclidean spaces.

More exactly, one considers the $\mathbb{E}_n$ as a vector space

$$V_n = \{(x_1, \ldots, x_n) \,|\, x_i \in \mathbb{R}\}$$

with the standard addition and vector multiplication by reals, and asks whether its structure can be completed by an operation of multiplication $m(a, b)$ that is bilinear as a mapping $m : V_n \times V_n \to V_n$. The bilinearity, of course, amounts to

- distributivity, and
- the condition $m(ra, sb) = (rs)m(a, b)$ for reals $r, s$.

Thus extended vector spaces over a field are termed *associative division algebras* [4] *over* $F$. Thus, the question amounts to asking about *finite-dimensional associative division algebras over the field of reals.*[5]

The answer to our question is that finite dimensional division algebras over $\mathbb{R}$ are very rare. By the celebrated Frobenius Theorem (1878) there are only

- the field of reals $\mathbb{R}$ (dimension 1),
- the field of complex numbers $\mathbb{C}$ (dimension 2), and
- the (noncommutative) field of *quaternions* $\mathbb{H}$ (dimension 4).

The last one can be described as follows: similarly like in $\mathbb{C}$ where we have basis

$$1, \mathbf{i} \quad \text{and complex numbers} \quad a + b\mathbf{i},$$

[4]The term "algebra" is indeed overburdened: it is used for the whole mathematical discipline, or for a set equipped with an algebraic structure, and here for very special algebraic objects.

[5]Note that the vector structure in $\mathbb{R}$ resp. $\mathbb{C}$ does not add much to the field one: in $\mathbb{R}$ it coincides with the a multiplication, and in $\mathbb{C}$ it can be expressed by the multiplication because of $r(a, b) = m((r, 0), (a, b))$. Similarly in the quaternions mentioned later.

in $\mathbb{H}$ one has a basis

$$1, \mathbf{i}, \mathbf{j}, \mathbf{k} \quad \text{and quaternions} \quad a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

subjected to the multiplication rules

$$\mathbf{ij} = \mathbf{k},\ \mathbf{ik} = -\mathbf{j},\ \mathbf{ki} = \mathbf{j},\ \mathbf{ji} = -\mathbf{k} \ \text{ and } \ \mathbf{kj} = -\mathbf{i}.$$

**Notes.** 1. Quaternions have a number of applications. In computer science they are used e.g. in 3-dimensional computer graphics and vision.

2. If we resign on distributivity of the multiplication and settle for so called *alternativity*

$$x(xy) = (xx)y \quad \text{and} \quad (yx)x = y(xx)$$

(which still allows some computing procedures) we can go one step more, namely to so called *Cayley numbers* (or *octonions*) in dimension 8.

3. Note the loss of nice properties with increasing dimension:

– dimension 1: a linearly ordered commutative field,

– dimension 2: a commutative field that cannot be linearly ordered,

– dimension 4: a field that is not commutative, and

– dimension 8: an algebra that is not any more fully associative.

**4.2. Finite, or Galois fields.** Those are fields with a finite number of elements[6], called the *order* of the field. One has that

- a finite field of order $q$ exists iff $q = p^n$ for some prime $p$, and
- the field of order $q$ is unique up to isomorphism.

The construction of Galois fields of orders $p^n$ with $n > 1$ is not quite straightforward, but those of prime orders are very easy: they are the fields

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}, \quad \text{where} \ \ p\mathbb{Z} \text{ is the ideal } \{px \,|\, x \in \mathbb{Z}\},$$

[6]Finite fields are fundamental in a number of areas of mathematics and computer science, including number theory, algebraic geometry, Galois theory, finite geometry, cryptography and coding theory.

of integers mod $p$, that is, of the integers $x, y$ identified if $x - y$ is a multiple of $p$. The fact that these rings are ideals follows from 11.2, because the $p\mathbb{Z}$ are precisely the maximal ideals of $\mathbb{Z}$ (and at the same time the prime ones; here, exceptionally, the two concepts coincide). But it may be of interest to show it as a consequence of the following (also otherwise useful) fact.

**4.2.1. Lemma.** *Let $a, b$ be natural numbers and let*

$$c = x_0 a + y_0 b \quad \textit{with} \quad x_0, y_0 \in \mathbb{Z}$$

*be the smallest positive number among the $xa + yb$ with $x, y \in \mathbb{Z}$. Then $c$ is the largest common divisor of $a$ and $b$.*

*Proof.* Obviously $c$ is a multiple of every common divisor of $a, b$. Hence we have to prove that $c$ divides both $a$ and $b$. Let, say, $c$ does not divide $a$. Then we have, dividing $a$ by $c$ with remainder,

$$a = zc + r = zx_0 a + zy_0 b + r$$

with $r$ positive and $< c$. But then $(1 - zx_0)a - zy_0 b = r < c$, a contradiction.

**4.2.2.** Now let $a$ not be equivalent with 0 in $\mathbb{Z}/p\mathbb{Z}$, that is, let $a$ not be divisible by $p$. Then by the lemma there are $x_0, y_0$ such that $x_0 a + y_0 p = 1$, hence $x_0 a - 1$ is divisible by $p$ and the class of $x_0$ is the inverse of that of $a$.

**4.2.3.** The smallest Galois field that is not of prime order is, of course, that of order 4. It looks as follows:

We have four elements

$$0, 1, a, b$$

with the addition table

| $+$ | $1$ | $a$ | $b$ |
|---|---|---|---|
| $1$ | $0$ | $b$ | $a$ |
| $a$ | $b$ | $0$ | $1$ |
| $b$ | $a$ | $1$ | $0$ |

and multiplication

| $\cdot$ | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $1$ |
| $b$ | $1$ | $a$ |