4. Algebraic theories

4.1. General properties

Definition 4.1. Assume L is a first order language.

1. A **first order theory** in L is a subset $T \subseteq L$ such that if $T \vdash \varphi$, then $\varphi \in T$
2. An **axiomatization** of a theory T is a subset $A \subseteq T$ such that $T = \{\varphi \in L : A \vdash \varphi\}$. A is called a set of **axioms** for T. If $A \vdash \varphi$ we say that φ is a **theorem** of the theory.

Definition 4.2. Assume L is a first order language.

1. A **model** of a theory T is an L-structure M such that $M \vDash T$
2. Two theories T_1 and T_2 are **(model) equivalent** if they have the same models.

If A is an axiomatization of T, then a T-model is simply an L-structure M such that $M \vDash A$.

Definition 4.3.

1. A signature is algebraic if it only contains function symbols
2. A first order language is algebraic if it is the language with equality generated by an algebraic signature
3. A theory is algebraic if it is axiomatized by quantifier-free atomic formulas in an algebraic language.

A model of an algebraic theory is called an **algebraic structure**.

- The only atomic formulas of the language L are equalities between terms.
- The axioms of an algebraic theory can be replaced by their universal closure. In fact an L-structure M is a model for a quantifier-free formula iff it is a model for its closure.
- If T is the empty algebraic theory, then an algebraic structure is simply an L-structure as was defined in semantics of FOL.

Definition 4.4. The theory of **vector spaces** over the real numbers **R** is the algebraic theory with :

Symbol	Type	Name
0	constant	zero
$-$	unary	opposite
$+$	binary	sum
r_i	unary	multiplication by r_i

Signature

Axiom	Name
$(x+y)+z = x+(y+z)$	associativity of addition
$x+y = y+x$	commutativity of addition
$x+0 = x$	neutral element of addition
$x+(-x) = 0$	opposite
$1x = x$	neutral element of the product
$r(sx) = (rs)x$	associativity of the product
$r(x+y) = rx+ry$	additivity of the product
$(r+s)x = rx+sx$	distributivity

Axioms

There is a unary operation r (multiplication by r) for every $r \in \mathbf{R}$; the signature is infinite.

Examples of vector spaces

The set $\mathbf{R}^n$ carries a structure of vector space over **R** with operations:

- $0 = (0, \dots 0)$
- $-(x_1, \dots, x_n) = (-x_1, \dots, -x_n)$
- $(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$
- $r(x_1, \dots, x_n) = (rx_1, \dots, rx_n)$

Submodels

Definition 4.5. Let T be an algebraic theory and let M and N be two T-models such that the support of N is contained in the support of M (we will write $N \subseteq M$ in this case). We say that N is a **submodel** (or a **substructure**) of M if for every function symbol f of L the interpretation of $[\![f]\!]_N$ is the restriction to N of $[\![f]\!]_M$. That is, if $a_1, \dots, a_n \in N$,

$$[\![f]\!]_N (a_1, \dots, a_n) = [\![f]\!]_M (a_1, \dots, a_n)\,.$$

$$\begin{tikzcd}
N^n \arrow[r, tail, "i^n"] \arrow[d, "{[\![f]\!]_N}"'] & M^n \arrow[d, "{[\![f]\!]_M}"] \\
N \arrow[r, tail, "i"'] & M
\end{tikzcd}$$

Proposition 4.6. Let T be an algebraic theory and let M be a T-model. A subset $N \subseteq M$ carries a T-submodel structure if and only if for every function symbol $f \in L$ of arity n and for every tuple $(a_1, \dots, a_n) \in N^n$ we have

$$[\![f]\!]_M(a_1, \dots, a_n) \in N.$$

In this case, the T-model structure of N is unique and $[\![f]\!]_N(a_1, \dots, a_n) = [\![f]\!]_M(a_1, \dots, a_n)$ for $a \in N^n$.

Proof. $(\Rightarrow)$. Suppose N is a submodel of M. Then $[\![f]\!]_N : N^n \to N$ and hence

$$[\![f]\!]_M(a_1, \dots, a_n) = [\![f]\!]_N(a_1, \dots, a_n) \in N.$$

$(\Leftarrow)$. If N carries a submodel structure we must have $[\![f]\!]_N(a_1, \dots, a_n) = [\![f]\!]_M(a_1, \dots, a_n)$, hence $[\![f]\!]_N$ is uniquely defined and the T-structure is unique. Suppose we now define

$$[\![f]\!]_N(a_1, \dots, a_n) := [\![f]\!]_M(a_1, \dots, a_n).$$

We claim that N is a T-model. Suppose $s = t$ is an axiom of T. If $v : X \to N \subseteq M$ is a valuation, then $v(s) = v(t)$ because $M \vDash s = t$, hence $N \vDash s = t$ (notice that $v(s), v(t) \in N$). $\square$

Submodels, example

Consider the vector space $V = \mathbf{R}^3$ and let

$$U = \{x = (x_1, x_2, x_3) \in V : x_3 = 0\} = \{(x_1, x_2, 0) : x_i \in \mathbf{R}\}.$$

Then U is a subspace of V because

- $0 \in U$ because $0 = (0, 0, 0)$.
- If $x \in U$, then $-x \in U$ because $-(x_1, x_2, 0) = (-x_1, -x_2, 0)$
- If $x, y \in U$, then $x + y \in U$ because $(x_1, x_2, 0) + (y_1, y_2, 0) = (x_1 + y_1, x_2 + y_2, 0)$
- If $x \in U$ and $r \in \mathbf{R}$, then $rx \in U$ because $r(x_1, x_2, 0) = (rx_1, rx_2, 0)$

Definition 4.7. Let T be an algebraic theory and let M be a T-model. A **congruence** on M is an equivalence relation $\sim$ which is compatible with all the operations, in the sense that for every function symbol $f \in L(T)$ and for all tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ of elements of M we have

$$(a_1 \sim b_1) \wedge \ldots \wedge (a_n \sim b_n) \to [\![f]\!]_M (a_1, \ldots, a_n) \sim [\![f]\!]_M (b_1, \ldots, b_n)$$

Congruences, example

Consider the vector space $V = \mathbf{R}^3$ and the subspace $U = \{(x_1, x_2, 0) : x_i \in \mathbf{R}\}$. The relation

$$x \sim y \Leftrightarrow x - y \in U$$

is a congruence on V. It is an equivalence relation:

- $x - x = 0 \in U \Rightarrow x \sim x$
- $x \sim y \Rightarrow y - x = -(x - y) \in -U \subseteq U \Rightarrow y \sim x$
- $(x \sim y) \wedge (y \sim z) \Rightarrow x - z = (x - y) + (y - z) \in U + U \subseteq U \Rightarrow x \sim z$

It is compatible with the operations:

- $0 \sim 0$
- $x \sim y \Rightarrow (-x) - (-y) = -(x - y) \in -U \subseteq U \Rightarrow -x \sim -y$
- $(x \sim y) \wedge (x' \sim y') \Rightarrow (x + x') - (y + y') = (x - y) + (x' - y') \in U + U \subseteq U \Rightarrow x + x' \sim y + y'$
- $x \sim y \Rightarrow rx - ry = r(x - y) \in rU \subseteq U \Rightarrow rx \sim ry$

Quotient models

Proposition 4.8. Let T be an algebraic theory and let M be a T-model. If E is a congruence on M then M/E is a T model for the structure

$$[\![f]\!]_{M/E}([a_1], \dots, [a_n]) = [[\![f]\!]_M(a_1, \dots, a_n)]$$

Proof. The definition is well posed:

$$\begin{aligned}
[a_i] = [b_i] &\Rightarrow a_i \sim b_i \\
&\Rightarrow [\![f]\!]_M(a_1, \dots, a_n) \sim [\![f]\!]_M(b_1, \dots, b_n) \\
&\Rightarrow [[\![f]\!]_M(a_1, \dots, a_n)] = [[\![f]\!]_M(b_1, \dots, b_n)] \\
&\Rightarrow [\![f]\!]_{M/E}([a_1], \dots, [a_n]) = [\![f]\!]_{M/E}([b_1], \dots, [b_n])
\end{aligned}$$

$M/E \models T$: if $s = t$ is an axiom, v is a valuation in M/E and u lifts v to M (i.e. $[u(x_i)] = v(x_i)$), then

$$\begin{aligned}
M \models s = t &\Rightarrow u(s) = u(t) \\
&\Rightarrow v(s) = v(t) \\
&\Rightarrow M/E \models s = t.
\end{aligned}$$

Quotient models, an example

On $\mathbf{R}^3$ consider the subspace $U = \{(x_1, x_2, 0) : x_i \in \mathbf{R}\}$ and the induced congruence

$$x \sim y \Leftrightarrow x - y \in U.$$

Set $W = \mathbf{R}^3/\sim$. An element of W is an equivalence class $[x]$ of a vector $x = (x_1, x_2, x_3) \in R^3$. Since

$$x \sim y \Leftrightarrow x - y = u \in U,$$

we have $[x] = \{x + u : u \in U\}$. This set is denoted by $x + U$, so that

$$W = \left\{x + U : x \in \mathbf{R}^3\right\}$$

is the set of planes parallel to U. The vector space structure of W is given by the formulas

- $0 = [0]$
- $-[x] = [-x]$
- $[x] + [y] = [x + y]$
- $r[x] = [rx]$

Morphisms of L-structures

Definition 4.9. If L is an algebraic language and M, N are L-structures, a **morphism** (or **homomorphism**) from M to N is a function $h : M \to N$ with the property that for every function symbol f of L of arity n,

$$h([\![f]\!]_M(x_1, \dots, x_n)) = [\![f]\!]_N(h(x_1), \dots, h(x_n))$$

$$\begin{tikzcd} M^n \arrow[r, "{[\![f]\!]_M}"] \arrow[d, "h^n"'] & M \arrow[d, "h"] \\ N^n \arrow[r, "{[\![f]\!]_N}"'] & N \end{tikzcd}$$

Morphisms of T-models

Definition 4.10. If T is an algebraic theory formulated in L and M and N are T-models , then a T-morphism (or morphism of T-models) is a morphism of L-structures. A T-morphism $h : M \to N$ is

1. a **monomorphism** if it is injective,
2. an **epimorphism** if it is surjective,
3. an **isomorphism** if it is bijective.

If T is the empty algebraic theory in a language L, then a morphism of T-models is precisely a morphism of L-structures. Therefore, without loss of generality, we can always consider morphisms of algebraic theories.

Morphisms, an example

Suppose $V = (V, 0, -, +, r_0, r_1, \ldots)$ and $V' = (V', 0, -, +, r_0, r_1, \ldots)$ are vector spaces over **R**. Notice that we are using the same simbols for the interpretation of the signature. A morphism of vector spaces is a function $h : V \to V'$ such that

1. $h(0) = 0$
2. $h(-x) = -h(x)$
3. $h(x + y) = h(x) + h(y)$
4. $h(rx) = rh(x)$

1 and 2 are consequences of 3 and 4 which, in turn, can be combined into the single formula

$$h(rx + sy) = rh(x) + sh(y)\,.$$

Thus a morphism of vector spaces is precisely a linear function.

Theorem 4.11. Assume T is an algebraic theory and M a T-model.

1. Submodels of M are precisely the images of morphisms with codomain M
2. Congruences on M are precisely kernel pairs of morphisms with domain M. Moreover, the structure on M/E is the only one that makes the projection $p : M \to M/E$ a morphism.

Proof. We only prove 2. If E is the kernel pair of a T-morphism $h : M \to N$ it is an equivalence relation. If f is a function symbol and $a_i E b_i$ then $h(a_i) = h(b_i)$ and hence

$$h(\llbracket f \rrbracket_M (a_1, \dots, a_n)) = \llbracket f \rrbracket_N (h(a_1), \dots, h(a_n)) = \llbracket f \rrbracket_N (h(b_1), \dots, h(b_n)) = h(\llbracket f \rrbracket_M (b_1, \dots, b_n))$$

proving that $\llbracket f \rrbracket_M (a_1, \dots, a_n) \, E \llbracket f \rrbracket_M (b_1, \dots, b_n)$. Thus E is a congruence. Conversely, if $E \subseteq M^2$ is a congruence, then

$$p(\llbracket f \rrbracket_M (a_1, \dots, a_n)) = [\llbracket f \rrbracket_M (a_1, \dots, a_n)] = \llbracket f \rrbracket_{M/E} ([a_1], \dots, [a_n]) = \llbracket f \rrbracket_{M/E} (p(a_1), \dots, p(a_n)) .$$

Hence p is a T-morphism and $E = \ker(p)$

The categorical structure of morphisms

Proposition 4.12. Assume T is an algebraic theory.

1. The identity on a T-model M is a T-morphism.
2. The product of T-morphisms is a T-morphism.
3. The inverse function of a T-isomorphism is a T-isomorphism.

First isomorphism theorem

Theorem 4.13. Assume h in the diagram below is a T-morphism. Then h factors uniquely through the projection p over its kernel pair through a T-morphism g which is injective and $\mathrm{im}(g) = \mathrm{im}(h)$.

$$\begin{tikzcd} M \arrow[r, "h"] \arrow[d, "p"'] & N \\ M/E \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

By the first isomorphism theorem for functions, it suffices to prove that $g([a]) = h(a)$ is a T-morphism

$$\begin{aligned} g(\llbracket f \rrbracket_{M/E}([a_1], \dots, [a_n])) &= g(\llbracket f \rrbracket_{M/E}(p(a_1), \dots, p(a_n))) \\ &= g(p(\llbracket f \rrbracket_{M}(a_1, \dots, a_n))) \\ &= h(\llbracket f \rrbracket_{M}(a_1, \dots, a_n)) \\ &= \llbracket f \rrbracket_{N}(h(a_1), \dots, h(a_n)) \\ &= \llbracket f \rrbracket_{N}(g(p(a_1)), \dots, g(p(a_n))) \\ &= \llbracket f \rrbracket_{N}(g([a_1]), \dots, g([a_n])) \end{aligned}$$

Direct and inverse images of submodels

Proposition 4.14. Suppose $h : M \to N$ is a T-morphism.

1. If $M' \subseteq M$ is a submodel, its direct image $h_*(M') := \{h(x) : x \in M'\}$ is a submodel of N.
2. If $N' \subseteq N$ is a submodel, its inverse image $h^*(N') := \{x \in M : h(x) \in N'\}$ is a submodel of M.

1. Assume f is a function symbol of arity n and $y_i \in h_*(M')$ for $i = 1, \dots, n$. Then $y_i = h(x_i)$ with $x_i \in M'$. If $x = [\![f]\!]_M(x_1, \dots, x_n) \in M'$, then

$$[\![f]\!]_N(y_1, \dots, y_n) = [\![f]\!]_N(h(x_1), \dots, h(x_n)) = h([\![f]\!]_M(x_1, \dots, x_n)) = h(x) \in h_*(M').$$

$h_*(M')$ is closed under the operations and is therefore a submodel of N.
2. If $x_i \in h^*(N')$ for $i = 1, \dots, n$ then $y_i := h(x_i) \in N'$ and $y := [\![f]\!]_N(y_1, \dots, y_n) \in N'$. Hence

$$h([\![f]\!]_M(x_1, \dots, x_n)) = [\![f]\!]_N(h(x_1), \dots, h(x_n)) = [\![f]\!]_N(y_1, \dots, y_n) = y \in N'$$

and hence $[\![f]\!]_M(x_1, \dots, x_n) \in h^*(N')$.

4.2. Groups

Definition 4.15. The theory of **groups** is defined as follows:

Symbol	Type	Name
1	constant	one
$\times$	functional, binary	product
$(\ )^{-1}$	functional, unary	inverse

Axiom	Name
$(xy)\,z = x(yz)$	associativity
$1x = x = x1$	neutral element
$x^{-1}x = 1 = xx^{-1}$	inverse

The theory of **commutative** or **abelian** groups is obtained by adding the axiom

$$xy = yx$$

Equivalent (not algebraic) version: signature $(\times)$ and axioms

- Associativity: $(xy)\,z = x(yz)$
- $\exists y \forall x (yx = x = xy)$; prove that this y is unique and introduce a parameter for it, say e.
- $\forall x \exists y (yx = e = xy)$; prove that y is unique and write $y = x^{-1}$

The first version of the theory is essentially the skolemization of the second.

Examples of groups

If T is an algebraic theory and M is a T-model, the set $\mathrm{Aut}(M)$ of all T-automorphisms of M, i.e. T-isomorphisms

$$f : M \to M$$

carries a group structure:

- 1 is the identity
- the product of T-morphisms
- the inverse T-morphism

These are operations on $\mathrm{Aut}(M)$ (▷4.12) and the axioms follow from properties of functions. Special cases:

- if X is a set, $\mathrm{Aut}(X)$ is the set of all bijective functions $f : X \to X$.
- if V is a vector space over k, $\mathrm{Aut}(V)$ is the set of all bijective linear functions $f : V \to V$.
- if $n \in \mathbf{N}$ is greater than 0, then $\mathrm{GL}_n(k)$ is a group with neutral element I and the usual matrix product and inverse (this is a rephrasing of the previous one)

Special criteria for subgroups and group morphisms

Proposition 4.16. Let G be a group. A subset $H \subseteq G$ is a subgroup if and only if:

1. $H \neq \varnothing$
2. For every pair of elements $x, y \in H$, $xy^{-1} \in H$.

Proposition 4.17. Assume G and H are groups. A function $h : G \to H$ is a morphism of groups if and only if it preserves the product.

$$h(xy) = h(x)\,h(y)$$

A subgroup of matrices

A subgroup of $G = \mathrm{GL}_2(\mathbf{R})$ is the subset

$$H = \left\{ A \in G : A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \right\}.$$

To check it, we use proposition 4.6 and prove that H is closed under all operations of G:

Neutral element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Product $\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix}$

Inverse $\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}^{-1} = \frac{1}{a_{11}a_{22}} \begin{pmatrix} a_{22} & -a_{12} \\ 0 & a_{11} \end{pmatrix} = \begin{pmatrix} \frac{1}{a_{11}} & \frac{-a_{12}}{a_{11}a_{22}} \\ 0 & \frac{1}{a_{22}} \end{pmatrix}$

A subgroup of matrices (continued)

Alternative

- $H \neq \varnothing$ because $I \in H$
- Multiplication by inverse:

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix}^{-1} = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} \frac{1}{b_{11}} & -\frac{b_{12}}{b_{11}b_{22}} \\ 0 & \frac{1}{b_{22}} \end{pmatrix} = \begin{pmatrix} \frac{a_{11}}{b_{11}} & \frac{a_{12}b_{11}-a_{11}b_{12}}{b_{11}b_{22}} \\ 0 & \frac{a_{22}}{b_{22}} \end{pmatrix}$$

Morphism example

- Binet's theorem states that if $A, B \in \mathrm{Mat}_n(\mathbf{R})$ are square matrices of order n, then

$$\det(AB) = \det(A)\det(B)\,.$$

- Therefore the determinant is a group morphism

$$\det : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$$

Normal subgroups

Definition 4.18. Let G be a group and $H \subseteq G$ a subgroup.

1. Given $g, x \in G$, the element $x^g := g^{-1}xg$ is called the **conjugate** of x by g.
2. H is **normal** in G (in symbols $H \lhd G$) if

$$\forall h \in H \ \forall g \in G (h^g \in H) .$$

Note: if G is abelian, every subgroup $H \subseteq G$ is normal:

$$h^g = g^{-1}hg = g^{-1}gh = 1h = h \in H.$$

Example of normal subgroup

The set

$$\underset{n}{\mathrm{SL}}(\mathbf{R}) = \left\{A \in \underset{n}{\mathrm{GL}}(\mathbf{R}) : \det(A) = 1\right\}$$

is a normal subgroup of $\mathrm{GL}_n(\mathbf{R})$. It is a subgroup:

- $|I| = 1 \Rightarrow I \in \mathrm{SL}_n(\mathbf{R})$
- $A, B \in \mathrm{SL}_n(\mathbf{R}) \Rightarrow |AB| = |A| \cdot |B| = 1 \cdot 1 = 1 \Rightarrow AB \in \mathrm{SL}_n(\mathbf{R})$.
- $A \in \mathrm{SL}_n(\mathbf{R}) \Rightarrow |A^{-1}| = |A|^{-1} = 1^{-1} = 1 \Rightarrow A^{-1} \in \mathrm{SL}_n(\mathbf{R})$.

It is normal: if $A \in \mathrm{SL}_n(\mathbf{R})$ and $B \in \mathrm{GL}_n(\mathbf{R})$; then

$$|B^{-1}AB| = |B^{-1}| \cdot |A| \cdot |B| = |B^{-1}| \cdot |B| = |B^{-1}B| = |I| = 1$$

and therefore $B^{-1}AB \in \mathrm{SL}_n(\mathbf{R})$.

Congruences, normal subgroups, kernels

Proposition 4.19. Normal subgroups of G classify congruences on G. More precisely, the following two constructions define inverse bijections between congruences on G and normal subgroups of G.

1. If $\sim$ is a congruence on G, then $[1]$ is a normal subgroup of G.
2. Every normal subgroup $N \subseteq G$ defines a congruence via the formula $x \sim y := xy^{-1} \in N$.

Proposition 4.20. The normal subgroups of G are the **kernels** of group morphisms $h : G \to G'$, i.e.

$$\ker(h) = \{g \in G : h(g) = 1 \in G'\}.$$

Normal subgroups via kernels, example

The determinant

$$\det : \underset{n}{\mathrm{GL}}(\mathbf{R}) \to \mathbf{R}^{\times}$$

is a morphism of groups by the Binet theorem. Its kernel is

$$\ker(\det) = \left\{ A \in \underset{n}{\mathrm{GL}}(\mathbf{R}) : \det(A) = 1 \right\} = \underset{n}{\mathrm{SL}}(\mathbf{R}) \,.$$

hence

$$\underset{n}{\mathrm{SL}}(\mathbf{R}) \lhd \underset{n}{\mathrm{GL}}(\mathbf{R}) \,.$$

Notation for quotient groups

- If $H \lhd G$ and $\sim$ is the associated congruence, one writes G/H instead of $G/{\sim}$.
- The equivalence class of x is

$$[x] = \{y \in G : y \sim x\} = \left\{y \in G : yx^{-1} = h \in H\right\} = \{y \in G : y = hx\} = Hx.$$

Hx is called the **right coset** of H in G represented by x. Thus,

$$G/H = \{Hx : x \in G\}.$$

- Operations in G/H can be described using cosets:

$$1 = [1] = H1 = H$$

$$(Hx)^{-1} = [x]^{-1} = [x^{-1}] = Hx^{-1}$$

$$(Hx)\,(Hy) = [x]\,[y] = [xy] = Hxy$$

4.3. Rings

Definition 4.21. The **theory of rings** is the algebraic theory whose language and axioms are given below.

Symbol	Type	Name
0	constant	zero
1	constant	one
$-$	unary	opposite
$+$	binary	sum
$\times$	binary	product

Axiom	Name
$(x+y)+z = x+(y+z)$	associativity
$x+y = y+x$	commutativity
$0+x = x$	neutral element
$x+(-x) = 0$	opposite
$(xy)z = x(yz)$	associativity
$1x = x$	left neutral element
$x1 = x$	right neutral element
$x(y+z) = xy+xz$	distributivity
$(x+y)z = xz+yz$	distributivity

If the product is commutative, i.e. if $xy = yx$, we obtain the theory of **commutative rings**.

Examples of rings

- Many familiar numeric sets are rings: **Z**, **Q**, **R**, **C**.

- If V is a vector space over **R**, the set $\mathrm{End}(V)$ of all linear functions $V \to V$ is a (non commutative) ring with addition and multiplication defined by

$$(f+g)(v) = f(v) + g(v), \qquad (f \circ g)(x) = f(g(x))$$

- The set $\mathrm{Mat}_n(k)$ of $n \times n$ matrices with coefficients in k with the usual sum and product. This ring is not commutative when $n > 1$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Special rings

Definition 4.22. A ring R is:

- **integral** (or an **integral domain**) if $R \vDash xy = 0 \to x = 0 \vee y = 0$.
- a **field** if it is commutative and $R \vDash \forall x(x \neq 0 \to \exists y(xy = 1))$

Neither the theory of integral domains nor the theory of fields is algebraic.

- Every field is an integral domain: if $xy = 0$ and $x \neq 0$, then there exists $z \in R$ such that $zx = 1$. But then

$$y = 1y = (zx)y = z(xy) = z0 = 0.$$

- **Z** is integral and commutative, but not a field.
- $\mathrm{Mat}_2(\mathbf{Q})$ is not integral (and hence not a field):

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- **Q**, **R**, **C** are fields

Proposition 4.23. The following formulas are valid in every ring:

1. $-0 = 0$
2. $-(-x) = x$
3. $-(x + y) = (-x) + (-y)$
4. $0x = 0 = x0$
5. $x(-y) = -(xy) = (-x)\,y$
6. $(-x)\,(-y) = xy$

Special criteria for subrings and ring morphisms

Proposition 4.24. Let R be a ring. A subset $S \subseteq R$ is a subring if and only if:

1. $1 \in S$
2. For every pair of elements $x, y \in S$, $x - y \in S$
3. For every pair of elements $x, y \in S$, $xy \in S$

Proposition 4.25. Assume R and S are rings. A function $h : R \to S$ is a morphism of rings if and only if

1. $h(x + y) = h(x) + h(y)$
2. $h(xy) = h(x)\,h(y)$
3. $h(1) = 1$

Subrings, example

Consider the ring $R = \mathrm{Mat}_2(\mathbf{R})$ of 2×2 matrices with real coefficients. The subset $S \subseteq R$ below is a subring:

$$S = \left\{ A \in \underset{2}{\mathrm{Mat}}(\mathbf{R}) : A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \right\}$$

1. S is closed under the neutral element of the product:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2. S is closed under differences:

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} - \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ 0 & a_{22} - b_{22} \end{pmatrix}$$

3. S is closed under products

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix}$$

Ring morphisms, an example

If $S \subseteq \mathrm{Mat}_2(\mathbf{R})$ is the subring of matrices of type

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}$$

and **R** is the field of real numbers, the function $h : S \to \mathbf{R}$ defined by the formula $h(A) = a_{11}$ is a ring morphism:

$$h(A+B) = h\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ 0 & a_{22}+b_{22} \end{pmatrix} = a_{11}+b_{11} = h(A)+h(B)$$

$$h(AB) = h\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12}+a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix} = a_{11}b_{11} = h(A)\,h(B)$$

$$h(I) = 1$$

Definition 4.26. Let R be a (unitary) ring. An **ideal** of R is a subset $\mathfrak{a} \subseteq R$ satisfying the following conditions:

1. $0 \in \mathfrak{a}$
2. If $x \in \mathfrak{a}$, then $-x \in \mathfrak{a}$.
3. If $x, y \in \mathfrak{a}$, then $x + y \in \mathfrak{a}$.
4. If $x \in \mathfrak{a}$ and $y \in R$, then $xy, yx \in \mathfrak{a}$.

Proposition 4.27. Let R be a (unitary) ring. Ideals in R classify classify congruences on R. More precisely:

1. If $\sim$ is a congruence on R, then $[0]$ is an ideal of R.
2. Every ideal $\mathfrak{a} \subseteq R$ defines a congruence via the formula

$$x \sim y := x - y \in \mathfrak{a}.$$

The constructions define inverse bijections between the set of congruences on R and the set of ideals of R.

Examples of ideals and congruences

If **Z** is the ring of integers and n is a positive natural number, the subset

$$(n) = \{kn : k \in \mathbf{Z}\}$$

of multiples of n is an ideal, the **principal ideal** generated by n:

- $0 \in (n)$ because $0 = 0n$
- If $x \in (n)$, then $x = kn$ for some k. hence $-x = (-k)\,n$ and $-x \in (n)$
- If $x, y \in (n)$, then $x = hn$ and $y = kn$. Therefore, $x + y = (h + k)\,n$ and $x + y \in (n)$.
- If $x \in (n)$, then $x = kn$. Therefore, $xy = (ky)\,n$ and $xy \in (n)$.

The congruence generated on **Z** by (n) is the congruence modulo n:

$$x \sim y \Leftrightarrow x - y \in (n) \Leftrightarrow n \mid x - y \Leftrightarrow x \underset{n}{\equiv} y.$$

How operations in $\mathbf{Z}/5 = \{[0], [1], [2], [3], [4]\}$ work:

$$[3] + [4] = [7] = [2], \qquad [3]\,[4] = [12] = [2], \qquad -[3] = [-3] = [2]\,.$$

When is Z/n a field?

1. If p is prime, then $\mathbf{Z}/p$ is a field. Reason: if $x \neq 0$ then x and p are coprime, hence $yx + zp = 1$ for some $y, z \in \mathbf{Z}$ by the euclidean algorithm. This means that, in $\mathbf{Z}/p$, we have

$$[1] = [yx + zp] = [y]\,[x] + [z]\,[p] = [y]\,[x] + [z]\,0 = [x]\,[y]\,.$$

2. If n is not prime, then $\mathbf{Z}/n$ is not integral: suppose $n = rs$ with r and s proper divisors of n. Then $[r], [s] \neq 0$ and

$$[r]\,[s] = [n] = 0.$$

Ideals are kernels

Definition 4.28. If $h : R \to S$ is a ring morphism, the **kernel** of h is the preimage of the neutral element for the sum $0 \in S$.

$$\ker(h) = h^*(\{0\}) = \{x \in G : h(x) = 0\}$$

Proposition 4.29. Ideals on R are precisely the kernels of ring morphisms from R.

The structure of the quotient ring

If $\sim$ is the congruence generated by an ideal $\mathfrak{a} \subseteq R$, one writes $R/\mathfrak{a}$ instead of $R/\sim$ for the quotient ring. Notice that, given $x \in R$,

$$[x] = \{y \in R : y \sim x\} = \{y \in R : y - x = a \in \mathfrak{a}\} =$$
$$\{y \in R : y = a + x, a \in \mathfrak{a}\} = \{a + x, a \in \mathfrak{a}\} = \mathfrak{a} + x.$$

The subset $\mathfrak{a} + x$ is called the right coset of $\mathfrak{a}$ represented by x. Thus, the elements of $R/\mathfrak{a}$ are the right cosets of $\mathfrak{a}$. The operations on the quotient ring are usually described in terms of ideals:

$$0 = \mathfrak{a} + 0$$
$$1 = \mathfrak{a} + 1$$
$$-(\mathfrak{a} + x) = -[x] = [-x] = \mathfrak{a} + (-x)$$
$$(\mathfrak{a} + x) + (\mathfrak{a} + y) = [x] + [y] = [x + y] = \mathfrak{a} + (x + y)$$
$$(\mathfrak{a} + x)(\mathfrak{a} + y) = [x][y] = [xy] = \mathfrak{a} + (xy)$$

4.4. Lattices

The theory of lattices

Definition 4.30. The theory of **lattices** is the algebraic theory with:

1. Language: generated by the binary function symbols $\wedge$ (meet) and $\vee$ (join).
2. Axioms:

$x \wedge y = y \wedge x$	$x \vee y = y \vee x$	commutativity
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	$(x \vee y) \vee z = x \vee (y \vee z)$	associativity
$x \wedge (x \vee y) = x$	$x \vee (x \wedge y) = x$	absorption

Finitely complete PO-sets

Definition 4.31. The theory of **finitely complete posets** is the first order theory with:

1. Language: generated by a single relation symbol $\leq$ of arity two.
2. Axioms:
   1. $\forall x(x \leq x)$
   2. $\forall xyz((x \leq y) \wedge (y \wedge \leq z) \to (x \leq z))$
   3. $\forall xy((x \leq y) \wedge (y \leq x) \to x = y)$
   4. $\forall xy \exists z((x \leq z) \wedge (y \leq z) \wedge \forall w((x \leq w) \wedge (y \leq w) \to (z \leq w)))$
   5. $\forall xy \exists z((x \geq z) \wedge (y \geq z) \wedge \forall w((x \geq w) \wedge (y \geq w) \to (z \geq w)))$

1. The models of the theory of finitely complete posets are partially ordered sets in which every pair (and hence every positive finite number) of elements has a least upper bound (supremum) and greatest lower bound (infimum)
2. The theory, as formulated, is not algebraic.

Lattices are finitely complete posets

Theorem 4.32. The theory of lattices is equivalent to the theory of finitely complete posets.

- If S is a lattice define

$$x \leq y := x \wedge y = x$$

- Conversely, if S is a finitely complete poset, define

$$x \wedge y := \inf(x, y), \qquad x \vee y := \sup(x, y)$$

Examples of lattices

1. $(\mathbf{Z}, \leq)$ is a finitely complete poset. In fact it is totally ordered, the least upper bound between x and y is the largest between x and y and the greatest lower bound is the smallest. Hence **Z** is a lattice with

$$x \wedge y := \min(x, y), \qquad\qquad x \vee y := \max(x, y),$$

2. $(\mathbf{N}, |)$ is a finitely complete poset. Divisibility on $\mathbf{N}$ is a partial order relation, the least upper bound of x and y is their least common multiple, their greatest lower bound is their greatest common divisor. Thus $\mathbf{N}$ is a lattice with

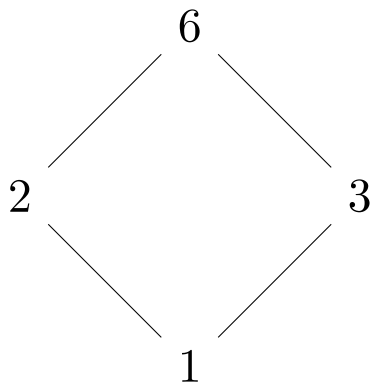
$$x \wedge y := \gcd(x, y), \qquad\qquad x \vee y := \mathrm{lcm}(x, y),$$

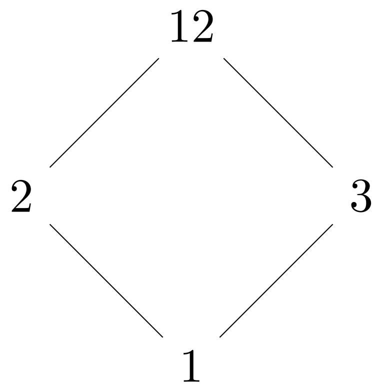
3. As a special case, the set $(D(n), |)$ of natural divisors of $n \in \mathbf{N}$, is a finitely complete poset and hence a lattice with the same operations.
4. For every set X, the powerset $(PX, \subseteq)$ is a finitely complete poset. The corresponding lattice structure is given by

$$x \wedge y := x \cap y \qquad\qquad x \vee y := x \cup y.$$

Sublattices, examples

Consider the lattice $L = (\mathbf{N}, \wedge, \vee)$ of natural numbers, where $x \wedge y = \gcd(x, y)$ and $x \vee y = \operatorname{lcm}(x, y)$. The posets represented by Hasse diagrams





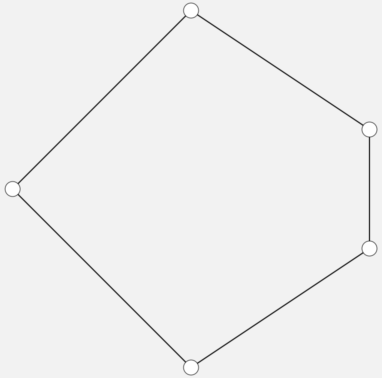
are both are lattices which are subsets of $\mathbf{N}$, but only the first is a sublattice of L.

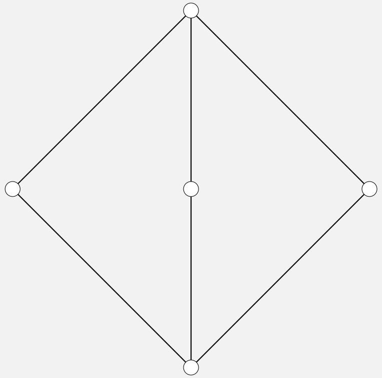
Definition 4.33. A lattice L is **distributive** if it satisfies the formulas

$$\forall xyz(x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)), \qquad \forall xyz(x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z))$$

A lattice L satisfies the first distributivity formula if and only if it satisfies the second.

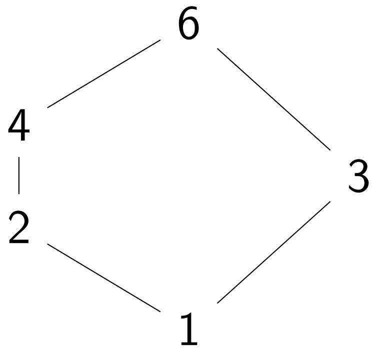
Proposition 4.34. (Dedekind's distributivity criterion) A lattice L is distributive if and only if it does not contain any sublattice isomorphic to either of the following:

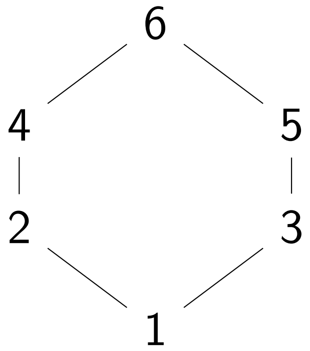




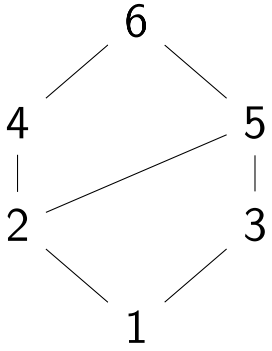
Distributive lattices, examples

- The lattice on the right below is not distributive by the Dedekind criterion, because there is an embedding of the lattice below on the left (which preserves node labels).





- The lattice below is distributive by the Dedekind criterion.



Complemented lattices

Definition 4.35. Assume L is a lattice.

1. A **zero element** for L is an element 0 such that $L \vDash x \vee 0 = x$. A **one** (or unit) for L is an element $1 \in L$ such that $L \vDash x \wedge 1 = x$.
2. A **complement** for x is an element $x' \in L$ such that $x \wedge x' = 0$ and $x \vee x' = 1$.
3. L is **complemented** if every $x \in L$ has a complement.

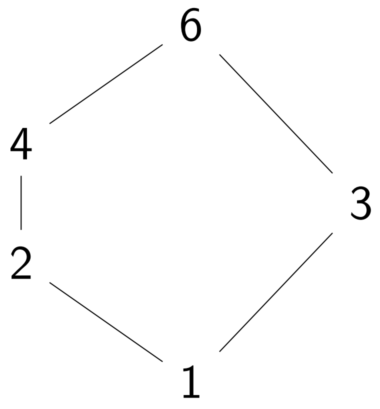
Some remarks:

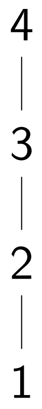
- The zero element, if it exists, is unique: if 0 and $0'$ are zeros, then $0 = 0 \vee 0' = 0'$. Similarly the element 1, if it exists, is unique.
- 0 is the minimum and 1 the maximum of the induced order: from the proof of 4.32 we have

$$x \vee 0 = x \Leftrightarrow 0 \leq x \Leftrightarrow x \wedge 0 = 0 \qquad x \wedge 1 = x \Leftrightarrow x \leq 1 \Leftrightarrow x \vee 1 = 1$$

Examples

The element 3 in the lattice on the left below has two complements: 2 and 4.





The element 3 in the lattice on the right has no complements.

Uniqueness of the complement

Proposition 4.36. Suppose L is a distributive lattice with 0 and 1. If $x \in L$ has a complement, this complement is unique.

Proof. Suppose y and z are complements of x. Then

$$y = 0 \vee y = (z \wedge x) \vee y = (z \vee y) \wedge (x \vee y) = (z \vee y) \wedge 1 = z \vee y$$
$$z = 0 \vee z = (y \wedge x) \vee z = (y \vee z) \wedge (x \vee z) = (y \vee z) \wedge 1 = y \vee z$$

Hence $y = z \vee y = y \vee z = z$. □

Definition 4.37. A **Boolean algebra** is a lattice with 0 and 1 which is distributive and complemented.

By proposition 4.36, the complement is unique and thus a unary operation on a Boolean algebra. Thus, boolean algebras can be regarded as models of the algebraic theory whose language is generated by the signature $(\wedge, \vee, ', 0, 1)$ with axioms

$$
\begin{aligned}
&x \wedge y = y \wedge x && x \vee y = y \vee x \\
&(x \wedge y) \wedge z = x \wedge (y \wedge z) && (x \vee y) \vee z = x \vee (y \vee z) \\
&x \wedge (x \vee y) = x && x \vee (x \wedge y) = x \\
&x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) && x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \\
&x \vee 0 = x && x \wedge 1 = x \\
&x \wedge x' = 0 && x \vee x' = 1
\end{aligned}
$$

The Boolean algebra of a powerset

For every set S, the powerset $\mathcal{P}(S)$ carries a boolean algebra structure as follows:

1. $x \wedge y = x \cap y$
2. $x \vee y = x \cup y$
3. $0 = \varnothing$
4. $1 = S$
5. $x' = S \setminus x$.

Meet is defined by a conjunction:

$$z \in x \cap y \Leftrightarrow (z \in x) \wedge (z \in y)\,.$$

Join is defined by a disjunction and complement by negation. The axioms follow from the properties of propositional calculus. For example, commutativity of meet follows from commutativity of conjunction:

$$\begin{aligned} z \in x \cap y &\equiv (z \in x) \wedge (z \in y) \\ &\equiv (z \in y) \wedge (z \in x) \\ &\equiv z \in y \cap x \end{aligned}$$

By extensionality, $x \cap y = y \cap x$.

Atoms

Definition 4.38. Let B be a boolean algebra. An alement $x \in B$ is an **atom** is $0 < x$ and there is no y such that $0 < y < x$.
If $x \in B$, the set

$$A_x = \{y \in B : y \leq x \text{ and } y \text{ is an atom}\}$$

of all atoms of B below x is called the set of **atoms of x**.

Example If X is any set, the atoms of the boolean algebra $\mathcal{P}(X)$ are the singletons $\{x\}$.

Characterizing finite BA

Theorem 4.39. Every finite boolean algebra B is isomorphic to the powerset of its set of atoms.

1. Every $x \neq 0$ in B has at least one atom.
2. Every $x \in B$ is the join of its atoms: $x = \bigvee A_x$.
3. If A is the set of atoms of B, there is an isomorphism of boolean algebra

$$h : B \to \mathcal{P}(A)$$

defined by $h(x) = A_x$

Corollary 4.40. If B is a finite boolean algebra, then $|B| = 2^n$ for some $n \in \mathbf{N}$.