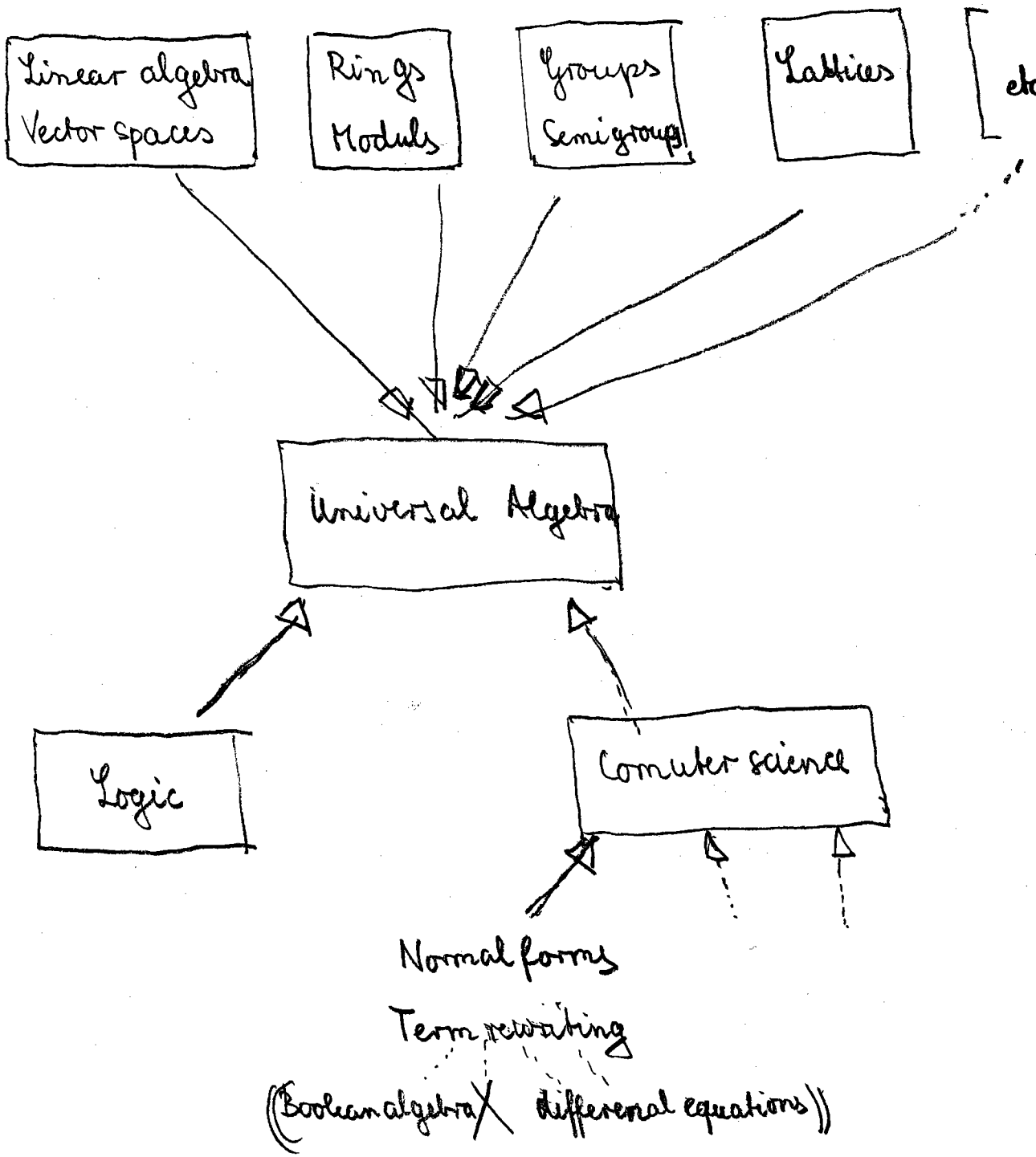
D. Schweigert WS2003/2004

Universal Algebra

Introduction



Introduction

The algebra is divided into many subjects:

Linear algebra Vector spaces	Rings Moduls	Groups (Semigroups)	Lattices

We consider the algebra under a general view
The universal algebra is mostly influenced by the logic (and specially model theory)
Whitehead and Russel have founded the theory of the universal algebra in the book "Principia Mathematica" (1910)

The applications of the universal algebra is given by the computer science. We will only study term writing (see the book: Baader, Nipkow)
An example of the application is normal forms of Boolean algebra

§1 Order and sets

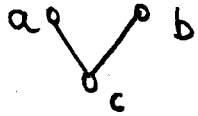
1A Order relations

Def. 1.1 A binary relation "$\leq$" on a set A is a partialy ordered if for all $x, y, z \in A$ holds

i) $x \leq x$ reflexive
ii) $x \leq y$ and $y \leq x$ implies $x = y$ antisymmetric
iii) $x \leq y$ and $y \leq z$ implies $x \leq z$ transitive

A partialy ordered set $\underline{A} = (A; \leq)$ is a non-empty set A with an order relation $\leq$ and is called also poset

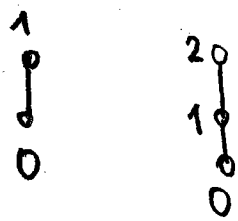
Hasse diagram.
How do we draw the diagram of a finite poset $(A; \leq)$?
Example

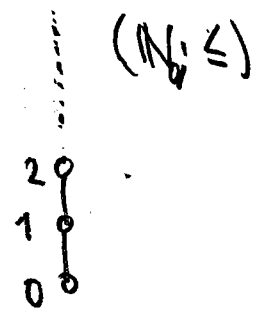


$a < a$ presents "lower" in the plane

Def. 1.2 A poset $(A; \leq)$ is called linear ordered or a chain if for all elements x, y holds either $x \leq y$ or $y < x$

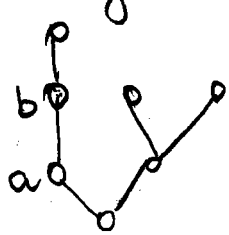
Examples





Def. 1.3 An element a is called lower neighbor of b if we have for all $c \in A$ with $a \leq c \leq b$ then it follows $a = c$ or $c = b$

An upper neighbor is defined in dual way



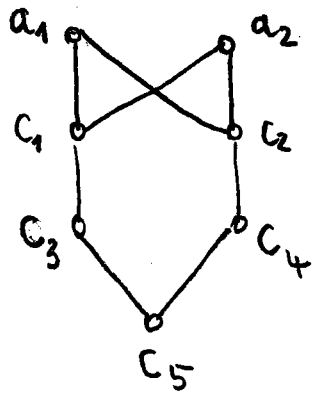
Def 1.4 Let $(A; \leq)$ be a poset. An element m is a maximal element of the set $C \subseteq A$ if it holds

i) $m \in C$

ii) for all $a \in C$ and $m \leq a$ it holds $a = m$

Minimal elements are defined in a dual way

Example



$A = \{a_1, a_2, c_1, c_2, \ldots, c_5\}$

$C = \{c_1, \ldots, c_5\}$

c_1, c_2 are maximal elements

Def. 1.5 Let $(A; \leq)$ be a poset and C be a subset. An element b is an upper bound of c if it holds $c \leq b$ for all $c \in C$

An element s is a supremum (: least upper bound) of C if it holds

i) s is an upper bound

ii) if b is an upper bound of C then follows $s \leq b$

(The supremum need not to contain C)

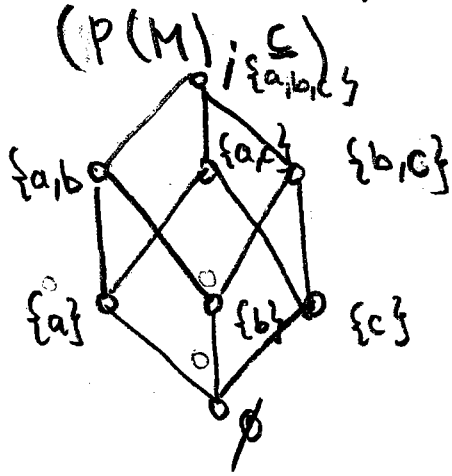
Dual way: infimum := greatest lower bound

Example: C has two upper bounds a_1, a_2 but not there is no supremum.
C has an infimum c_5 which is also minimal,

Proposition 1.6 Let $(A; \leq)$ be a poset with $C \subseteq A$ If C has a supremum then the supremum is unique.

Proof. We assume that there two supremas s, t of C. Then s, t are upper bounds of C As s is a least upper bound of C we have $s \leq t$. In the otherwise we have $t \leq s$ and therefore $s = t$ $\square$

Example Power set of $M = \{a, b, c\}$



$\{a\}$ and $\{b\}$ is the supremum $\{a,b\}$. In this poset: Every pair x, y of the elements has a supremum $x \wedge y$ and an infimum $x \vee y$

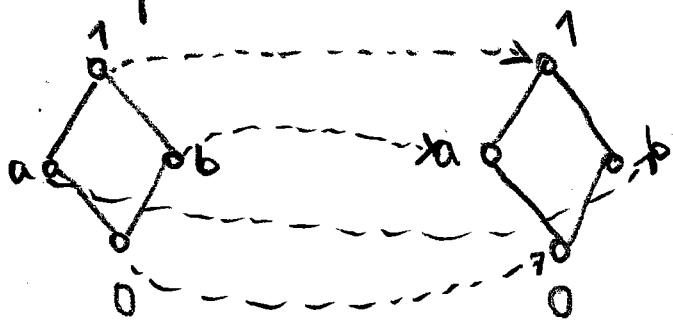
supremum $\{x,y\} := x \vee y$ (join, union)

infimum $\{x,y\} := x \wedge y$ (meet, intersection)

Def. 1.7 Let $\underline{A} = (A; \leq_\alpha)$ and $\underline{B} = (B; \leq_\beta)$ be posets. A mapping $f: A \longrightarrow B$ is called monoton (or an order-homomorphism) if for all $a_i \leq_\alpha c_i$, $i = 1, \dots, n$ holds that $f(a_1, \dots, a_n) \leq_\beta f(c_1, \dots, c_n)$

If f is bijective then f is an order isomorphism

Example



We write only $\leq$ instead of $\leq_\alpha$ and $\leq_\beta$

1 B Well ordered sets

Def. 1.8 A linear ordered set (= chain) $(A; \leq)$ is called well-ordered if every non-empty subset of A has a minimal element

(This minimal element is also the infimum)

Let $(A; \leq)$ be linear ordered set. We denote

$P(a) = \{b \mid b \in A, b < a\}$

Thm 1.9 (Principle of the transfinite induction)

Let $(A; \leq)$ be a well order and let B be a subset of A. We assume that for all $a \in A$ it holds:

* If $P(a) \subseteq B$ then $a \in B$

Then we have $A = B$

Proof. Assume that $A \neq B$. Let a be a minimal element of $A \setminus B$. Then it holds $P(a) \subseteq B$

If (*) holds then we have $a \in B$

Remark. We compare with the usual induction

We consider $(\mathbb{N}; \leq)$ and a subset $M \subseteq \mathbb{N}$

If for all $n \in \mathbb{N}$ implies

(**) $P(n) = \{m \mid m \in T, m \leq n\} \subseteq M$

then we have $M = \mathbb{N}$

With other words:

(***) If a proposition $\varphi(m)$ is true for all $m < n$

then the proposition is true for all $\varphi(n)$

If (***) holds and $\varphi(k)$ is true then
it holds for all $k \in \mathbb{N}$

1C Axiom of choice

1.10 (Axiom of choice)

For a given set M there exists a function φ

which maps every non-empty subset A of M
into on a element $\varphi(A)$ of its subset

It means that we can choose an element from a non-empty subset A of the set M. It seems trivial but there mathematicians who do not believe this axioms

The axiom of choice is equivalent to the theorem of Zermelo

Thm 1.11 Every set can be well ordered

(Without proof (See Kurosch)

The most important application of the axiom of choice is the lemma of Zorn.

Lemma of Zorn 1.12 Let $(A;\leq)$ be a non-empty poset in which every chain has an upper bound. Then the poset $(A;\leq)$ has a minimal element

Axiom of choice $\leftrightarrow$ Well order $\leftrightarrow$ Lemma of Zorn

*1D On ordinal numbers

We understand an ordinal number as a set with some properties. Idea:

$\{\emptyset\} := 1$

$\{\emptyset, \{\emptyset\}\} := 2$

$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} := 3$ ...

We observe that $2 = 1 \cup \{1\}$, $3 = 2 \cup \{2\}$, ...

Def. 1.13 (v. Neumann)

A set ξ is a ordinal number if ξ fulfilles the conditions

i) If $\eta \in \xi$ then $\eta \subseteq \xi$

ii) If $\eta, \mu \in \xi$ then either $\mu = \eta$ or $\mu \in \eta$ or $\eta \in \mu$

iii) If A is a non-empty set of ξ then there is a $\eta \in A$ with $\eta \cap A \in \emptyset$

The most important properties of ordinals are (without proofs)

1.14 If ξ is an ordinal number then $(\xi; \leq)$ is well ordered set

1.15 An ordinal number is the set of all smaller ordinal numbers

Def. 1.16 An ordinal number ξ is not a limes ordinal number, if $\xi = \gamma \cup \{\gamma\}$ for some ordinal γ. In other cases ξ is a limes ordinal number

ϕ is a limes ordinal ($\phi := 0$)

We called an ordinal number γ^+ as a sucessor if $\gamma^+ = \gamma \cup \{\gamma\}$

Remark 1.17 There exists a limes ordinal which is not 0.

Def. 1.18 ω is the least limes ordinal which is not 0. The elements of ω are called natural numbers (or also finite ordinal numbers)

*1E On cardinal numbers

Def. 1.19 Let ξ be an ordinal. ξ is a cardinal number if for every ordinal γ with $\gamma < \xi$ there exists no bijective map between γ and ξ

Remark. Obviously the finite ordinals $0, 1, 2, 3, \ldots$ and ω are also cardinals. But $\omega + 1$ is not a cardinal

Def. 1.20 The cardinality $|A|$ of a set A is the least ordinal number α such that there exists a bijective map between A and α

Remark. Let $|A|$ be a cardinal number.
A set A is finite if $|A| < \omega$
A is countable if $|A| \leq \omega$
A is infinite if $|A| \geq \omega$

Remark. For sets A, B the following are equivalent
i) $|A| \leq |B|$
ii) There exists an injective map from A to B
iii) There exists a surjective map from B to A

Theorem 1.21 Let α and β be infinite cardinalities
It holds
$$\max\{\alpha,\beta\} = \alpha+\beta = \alpha\cdot\beta$$

Thm. 1.22 For all cardinalities holds:
$$\alpha < 2^{\alpha}$$

Def. 1.23 Let α be a cardinal number.
α^+ is the least cardinal number β with $\alpha<\beta$ (successor)
(α^+ is successor)
Remark. α^+ exists because $\alpha < 2^{\alpha}$
and because the set of the cardinalities $\leq 2^{\alpha}$
are well ordered.

For ordinal numbers ξ holds:
$|\xi| = \alpha$ if and only if $\alpha \leq \xi < \alpha^+$

Remark 1.24 A cardinal number α is not a limes number if $\alpha = \beta^+$ for some cardinal number β. If not then α is a limes number

Def 1.25 The statement $\omega^+ = 2^\omega$ is called continuum hypothesis

The statement $\alpha^+ = 2^\alpha$ for all infinite cardinality α is called the general continuum hypothesis

Historical remarks

The theory of sets is created by Cantor 1845 - 1918
The continuum hypothesis was formulated by him. He tried to prove that with out sucess.

Does it exist a cardinal number between $\mathbb{N}$ and $\mathbb{R}$?

The proposition of not being contradiction is called consistent

The consistence of the Zermelo - Fraenkel - set theory with axiom of choice and the continuum hypothesis was proved by Gödel.

The most important results are from
Cohen, Tarski, Erdős, Rado, Hausdorff,
v. Neumann, Kuratowski, König, Cauchy
and naturally Cantor
Shelah is most important researcher nowadays

$$0 < 1 < 2 < 3 \ldots < \omega < \omega+1 < \ldots < \aleph_1 < \aleph_{1+1} < \ldots$$

$$0 < 1 < 2 < 3 \ldots < \aleph_0 < \aleph_1 < \ldots < \aleph_\alpha < \ldots$$

$\aleph_\alpha$ = the least infinite cardinal different from $\aleph_\beta$ for every β than α

Def 1.25 The statement $\omega^+ = 2^\omega$ is called continuum hypothesis

The statement $\alpha^+ = 2^\alpha$ for all infinite cardinality α is called the general continuum hypothesis

Historical remarks

The theory of sets is created by Cantor 1845 - 1918

The continuum hypothesis was formulated by him. He tried to prove that with out success.

Does it exist a cardinal number between $\mathbb{N}$ and $\mathbb{R}$?

The proposition of not being contradiction is called consistent

The consistence of the Zermelo - Fraenkel - settheory with axiom of choice and the continuum hypothesis was proved by Gödel.

The most important results are from Cohen, Tarski, Erdös, Rado, Hausdorff, v. Neumann, Kuratowski, König, Cauchy and naturally Cantor

Shelah is most important researcher nowadays

$$0 < 1 < 2 < 3 \ldots < \omega < \omega+1 < \ldots < \aleph_\alpha < \aleph_{\alpha+1} < \ldots$$

$$0 < 1 < 2 < 3 \ldots < \aleph_0 < \aleph_1 < \ldots < \aleph_\alpha < \ldots$$

$\aleph_\alpha$ = the least infinite cardinal different from $\aleph_\beta$ for every β than α

Def 1.25 The statement $\omega^+ = 2^\omega$ is called continuum hypothesis

The statement $\alpha^+ = 2^\alpha$ for all infinite cardinality α is called the general continuum hypothesis

Historical remarks

The theory of sets is created by Cantor 1845 - 1918

The continuum hypothesis was formulated by him. He tried to prove that with out sucess.

Does it exist a cardinal number between $\mathbb{N}$ and $\mathbb{R}$?

The proposition of not being contradiction is called consistent

The consistence of the Zermelo - Fraenkel - settheory with axiom of choice and the continuum hypothesis was proved by Gödel.

The most important results are from Cohen, Tarski, Erdös, Rado, Hausdorff, v. Neumann, Kuratowski, König, Cauchy and naturally Cantor

Shelah is most important researcher nowadays

$0 < 1 < 2 < 3 \ldots < \omega < \omega+1 < \ldots < \aleph_1 < \aleph_{1+1} < \ldots$

$0 < 1 < 2 < 3 \ldots < \aleph_0 < \aleph_1 < \ldots < \aleph_\alpha < \ldots$

$\aleph_\alpha$ = the least infinite cardinal different from $\aleph_\beta$ for every β than α

Def 1.25 The statement $\omega^+ = 2^\omega$ is called continuum hypothesis

The statement $\alpha^+ = 2^\alpha$ for all infinite cardinality α is called the general continuum hypothesis

Historical remarks

The theory of sets is created by Cantor 1845 - 1918

The continuum hypothesis was formulated by him. He tried to proove that with out sucess.

Does it exist a cardinal number between $\mathbb{N}$ and $\mathbb{R}$?

The proposition of not being contradiction is called consistent

The consistence of the Zermelo - Fraenkel - settheory with axiom of choice and the continuum hypothesis was proved by Gödel.

The most important results are from Cohen, Tarski, Erdös, Rado, Hausdorff, v. Neumann, Kuratowski, König, Cauchy and naturally Cantor

Shelah is most important researcher nowadays

$0 < 1 < 2 < 3 \ldots < \omega < \omega+1 < \ldots < \aleph_1 < \aleph_{1+1} < \ldots$

$0 < 1 < 2 < 3 \ldots < \aleph_0 < \aleph_1 < \ldots < \aleph_\alpha < \ldots$

$\aleph_\alpha$ = the least infinite cardinal different from $\aleph_\beta$ for every β than α

§2 Lattices

Def. 2.1 A lattice (Verband) $\underset{\sim}{L} = (L; \wedge, \vee)$ is a pair consisting of a non-empty set L and two operations $\wedge$ (cut, intersection; Schnitt) and $\vee$ (join, union; Verbindung, Vereinigung) such that ~~for all~~ $x, y, z \in L$ holds

L1 $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ $\qquad x \vee (y \vee z) = (x \vee y) \vee z$

associativity

L2 $x \wedge y = y \wedge x$ $\qquad x \vee y = y \vee x$

Commutativity

L3 $x \wedge x = x$ $\qquad x \vee x = x$

idempotence

L4 $x \wedge (x \vee y) = x$ $\qquad x \vee (x \wedge y) = x$

adsorption

(Remark. The axioms can also be written with a single axiom of the length of 1000 letters)

Thm 2.2 For every lattice $\underset{\sim}{L} = (L; \wedge, \vee)$ there corresponds a poset $\underset{\approx}{L} = (L; \leq)$ in which the infimum $\inf\{a,b\}$ and the supremum $\sup\{a,b\}$ exists forall elements $a, b \in L$.

Proof. Let $\underset{\sim}{L} = (L; \wedge, \vee)$ be a lattice. We define a binary relation "$\leq$" on L by

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

Obviously $\leq$ is reflexive because $a \wedge a = a$ we have $a \leq a$ for all $a \in L$.

Now $\leq$ is antisymmetric because it follows from $a \leq b$ and $b \leq a$ by $a = a \wedge b = b \wedge a = b$

For the transitivity we have for $a \leq b$ and $b \leq c$ that $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$

We show that $\inf\{a,b\} = a \wedge b$

That means we have to show that $a \wedge b$ is the greatest lower bound.

We have $(a \wedge b) \wedge a = a \wedge b$ and $(a \wedge b) \wedge b = a \wedge b$

It follows $a \wedge b \leq a$ and $a \wedge b \leq b$. Therefore $a \wedge b$ is a lower bound for a, b. Assume that $a \wedge b \leq c \leq a$ and $a \wedge b \leq c \leq b$.

Then we have $c \wedge a = c$ and $c \wedge b = c$

Altogether we have $c \wedge (a \wedge b) = (c \wedge a) \wedge (c \wedge b)$

$= c \wedge c = c$ and $a \wedge b$ is the infimum

For the supremum we use the dual argument.

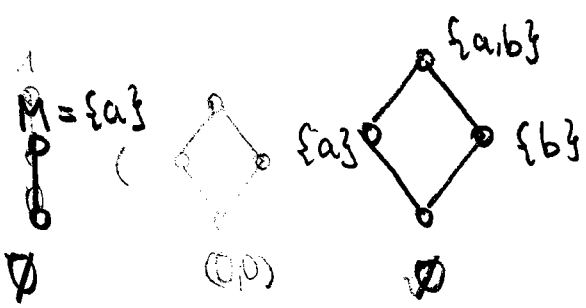
Thm. 2.3 For every poset $(L; \leq)$ there corresponds a lattice $(L; \wedge, \vee)$ in which infimum and supremum exists for all $a, b \in L$.

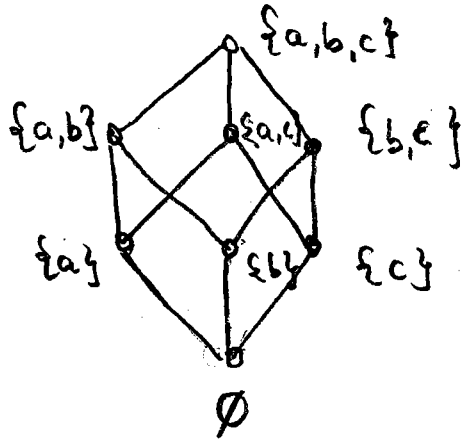
Proof. We define $a \wedge b := \inf\{a, b\}$ and $a \vee b := \sup\{a, b\}$ and we have to show

the axioms L1 - L4. This is trivial in the case L2 because $a \wedge b = \inf\{a,b\} = \inf\{b,a\} = b \wedge a$ and also L3. In the case L1 and L4 is lengthy.

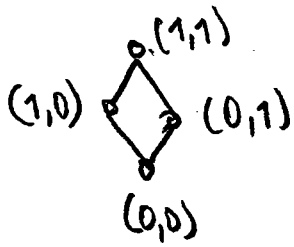
Examples of lattices given by the Hasse diagrams

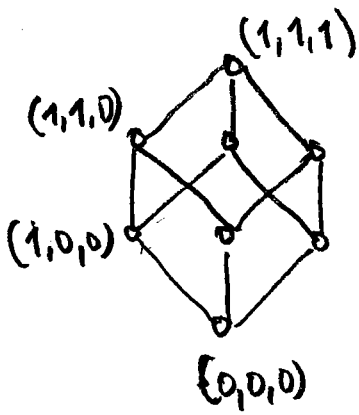
2.4 Power set $M = \{a,b,c\}$

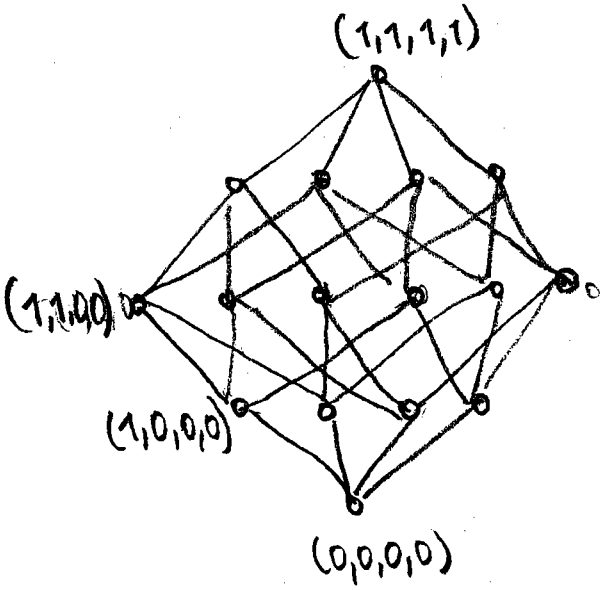




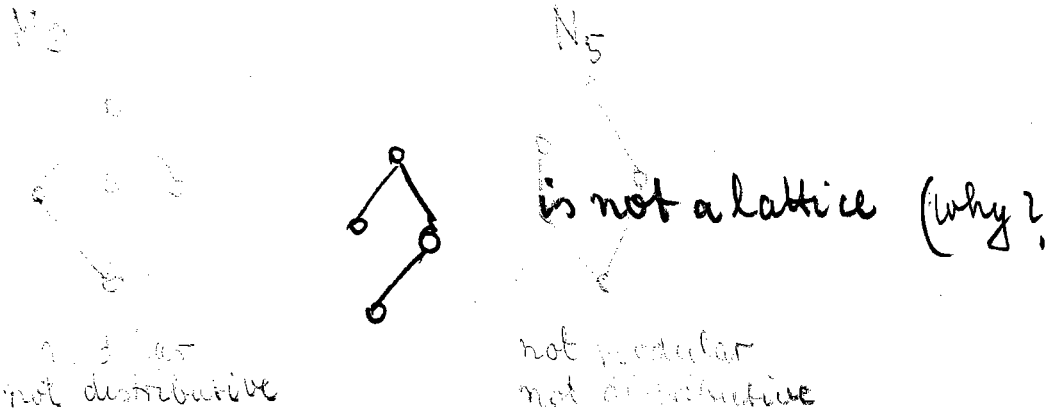
2.5 Switching algebra







2.6



is not a lattice (why?

2.5

is <u>not</u> lattice (why?)

2.7 Let V be a K-vector space and let $L(V)$ be the set of all subspaces of V. The lattice $(L(V); \wedge, \vee)$ of all subspaces is defined by $U_1 \wedge U_2 := U_1 \cap U_2$ and $U_1 \vee U_2 := \text{span}\{U_1, U_2\}$ for all subspaces.

Def. 28 A distributive lattice is a lattice which satisfies the distributive laws

D1 $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

D2 $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Remark D1 is equivalent to D2

Def. 29 A modular lattice fulfills the modular law

M $x \leq y \longrightarrow x \vee (y \wedge z) = y \wedge (x \vee z$

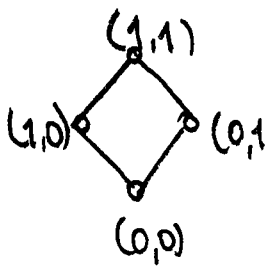
Observe:

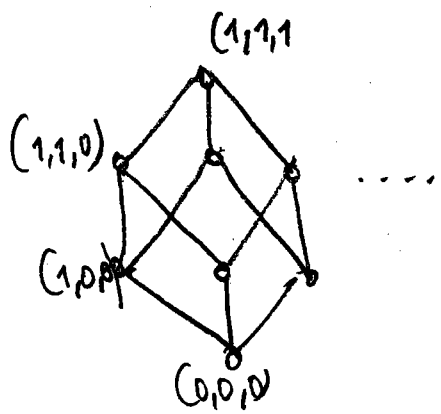
If $x \leq y$ then $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

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

Hasse diagrams

2.10

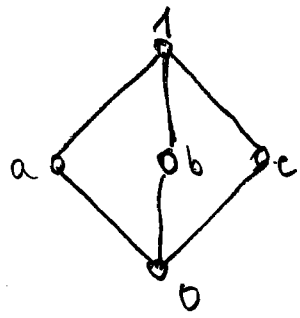




....

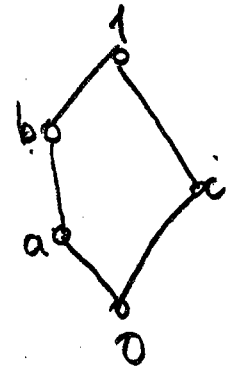
are distributive

2.11



M_3

The smallest modular lattice which is not distributive



N_5

The smallest non-modular lattice

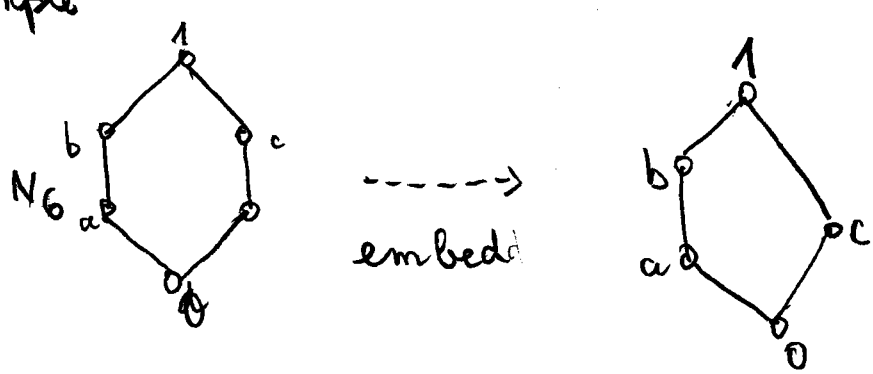
Remark 2.12

Every distributive lattice is a modular lattice

Thm 2.13 (Dedekind) A lattice L is not modular if and only if N_5 can be embedded to L

(We will postpone for later)

Example



Thm. 2.14 (Birkhoff) L is a non-distributive lattice if and only if M_3 or N_5 can be embedded into L.

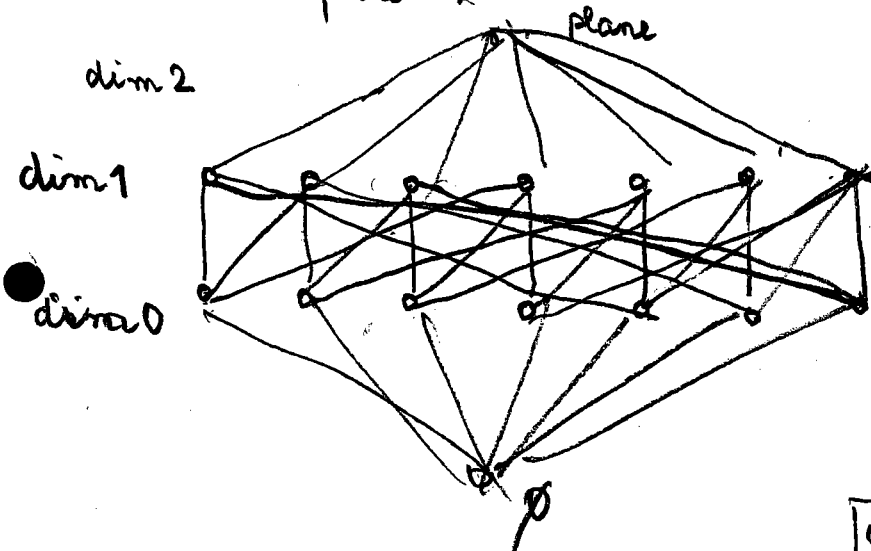
(Postpone for later)

Remark. The modular lattice play an important role for projective geometry and vector spaces

Example

K Vectorspace

Smallest projective plane



$K = \{0,1\}$ vector space

Idea of Decartes

Geometry

Algebra

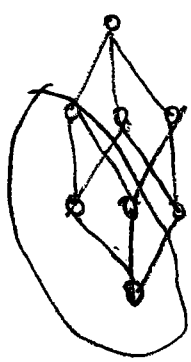
Def. 2.9 Let $(L; \wedge, \vee)$ be a lattice.
$(K; \wedge, \vee)$ is called a sublattice if it holds i) $\emptyset \neq K \subseteq L$

ii) for all $a, b \in K$ it holds $a \wedge b \in K$

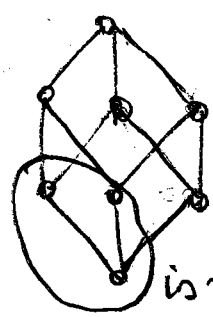
iii) for all $a, b \in K$ it holds $a \vee b \in K$

Examples:

2.



is a sublattice



is not a sublattice because it is not closed under join $\vee$

§3 Algebras and subalgebras

3.1 Algebras

Def. 3.1 An algebra $\underset{\sim}{A} = (A; \Omega)$ is an ordered pair (A, Ω) where A is a non empty set and Ω be a family of finitary operations on A.

The mapping $f_\gamma : A^{n_\gamma} \to A$ is a n_γ-arity operation (also: n_γ-place)

The type of the algebra $(A; \Omega)$ is a sequence $(n_0, n_1, \dots, n_\gamma, \dots)$ of not negative numbers $\gamma < o(\tau)$ where $o(\tau)$ is an ordinal number.

Examples

3.2 Groups

A group $\underset{\sim}{G}$ is an algebra $(G; \cdot, {}^{-1}, 1)$ is an binary, a unary and a nullary operations in which the following identities are true

G1 $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

G2 $x \cdot 1 = 1 \cdot x = x$

G3 $x \cdot x^{-1} = x^{-1} \cdot x = 1$

A group $\underset{\sim}{G}$ is Abelian (or commutative) if it holds

G4 $x \cdot y = y \cdot x$

3.3 Rings

A ring is an algebra $(R; +, -, \cdot, 0)$ where $+$ and $\cdot$ are binary, $-$ is unary and 0 is nullary if it holds

R1 $(R; +, -, 0)$ is an Abelian group

R2 $(R; \cdot)$ is a semigroup, i.e. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

R3 $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$

3.4 Modules

Let R be a given ring. A (left) R-module $\underset{\sim}{M}$ is an algebra $(M; +, -, 0, (f_r)_{r \in R})$ of the type $(2, 1, 0, 1, \ldots 1, \ldots)$

M1 $(M; +, -, 0)$ is an abelian group

M2 $f_r(x+y) = f_r(x) + f_r(y)$ for $r \in R$

M3 $f_{r+s}(x) = f_r(x) + f_s(y)$ for $r, s \in R$

M4 $f_r(f_s(x)) = f_{rs}(x)$ for $r, s \in R$

A unitary R-Modul is an algebra of M1 – M4 and

M5 $f_1(x) = x$

(Compare ~~a~~ vector spaces)

3.5 Boolean algebra

A Boolean algebra $\mathfrak{B}$ is an algebra $(B; \wedge, \vee, ', 0, 1)$ of type $(2, 2, 1, 0, 0)$ with the axioms

B1 $(B; \wedge, \vee)$ is a distributive lattice

B2 $x \wedge 0 = 0$, $x \vee 1 = 1$

B3 $x \wedge x' = 0$ $x \vee x' = 1$

3B Subalgebras, subgroups

Def. 3.6 Let $\underset{\sim}{A}, \underset{\sim}{B}$ be algebras of the same type.
Then $\underset{\sim}{B}$ is sub-algebra of $\underset{\sim}{A}$ if $A \subseteq B$
and every operation of $\underset{\sim}{B}$ is the restriction
to the corresponding operation A

This means that B is closed under the
operations of A

It requires : $a_1, \dots, a_n \in B \Longrightarrow f(a_1, \dots, a_n) \in B$

for every n-ary operation f

3.7 Sub-groups

Let H be a non-empty set which is contained
of a group $\underset{\sim}{G} = (G; \cdot, ^{-1}, e)$
H is a sub-group of G if it holds
i) if $h_1, h_2 \in H$ then $h_1 \cdot h_2 \in H$
ii) if $h \in H$ then $h^{-1} \in H$

A set of elements in a group is called a complex. We use the complex products

for instance $H_1 \cdot H_2$ for subgroups H_1, H_2

or $x^{-1} \cdot H\, x$

Def. 3.8 A sub-group $\underset{\sim}{H}$ of a group $\underset{\sim}{G}$ is a normal subgroup (Normalteiler) if it holds

$$x^{-1} \cdot H \cdot x = H$$

Every subgroup H of an abelian group is again abelian and H is a normal group

Def. 3.9 The order of a group G is a cardinal number of the sets of G

3.10 The list of distinct groups of each order from 1 till 10

order	1	2	3	4	5	6	7	8	9	10
number	1	1	1	2	1	2	1	5	2	2

Klein dihedral

We present the (small) groups as tables

1

	e
e	e

;

2

	e	a
e	e	a
a	a	e

;

3

	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

4

	e	a	a^2	a^3
e				
a				
a^2				
a^3				

a

Klein

	e	a	b	a·b
e	e	a	b	a·b
a	a	e	a·b	b
b	b	b·a	e	
a·b	a·b			

$a \cdot a \cdot b = b$

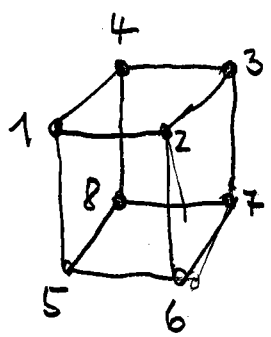
$b \cdot a = a \cdot b$

Example 3.11 Symmetries of a cube

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

rotation

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 8 & 5 & 2 & 3 & 7 & 6 \end{pmatrix}$$



reflection

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix}$$

3 C Lattice of subalgebras

3.12 The set of all subalgebra of an algebra $\mathcal{A}$ forms a lattice

The lattice $(L_A ; \wedge, \vee)$ of all subalgebras is defined by $U_1 \wedge U_2 := U_1 \cap U_2$ for all subalgebras U_1, U_2

$U_1 \vee U_2 := \langle U_1, U_2 \rangle$ for all subalgebra U_1, U_2

$\langle U_1, U_2 \rangle$ is the smallest subalgebra which contains U_1 and U_2

Example. Consider the Kleinian group

	e	a	b	a·b
e	e	a	b	a·b
a	a	e	a·b	b
b	b	a·b	e	
a·b	a·b	b		e

Subgroupps are

e	e
e	e

,

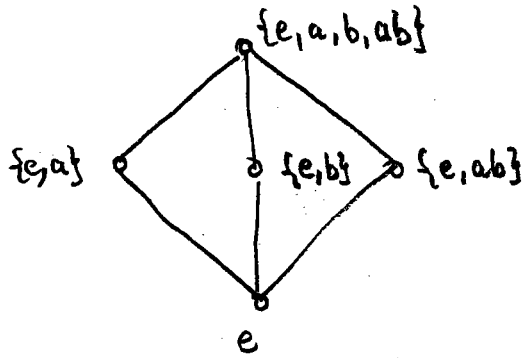
e	e	a
e	e	a
a	e	e

,

e	e	b
e		
b		

e	e	ab
e		
ab		

Hassediagram



Def 3.13 Let G be a group and $L_N(G)$ be set of all normal subgroups of G. The lattice $(L_N(G); \wedge, \vee)$ of all normal subgroups is defined by

$N_1 \wedge N_2 := N_1 \cap N_2$ for normal subgroups N_1, N_2

$N_2 \vee N_2 := N_1 \cdot N_2$

Observe that for normal subgroups we have

$$N_1 \cdot N_2 = N_2 \cdot N_1$$

Def. 3.14 K Vectorspaces

$U_1 \wedge U_2 := U_1 \cap U_2$

$U_1 \vee U_2 := \operatorname{span}\{U_1, U_2\}$

Def.ple 3.15 Modulln

The lattice of the sub-moduls is defined by

$U_1 \wedge U_2 := U_1 \cap U_2$, $U_1 \vee U_2 := \langle U_1, U_2 \rangle$

the smallest sub-modul which generates by U_1, U_2

Def. 3.16 Let $\underset{\sim}{R}$ be a ring.

A non-empty subset m of R is ideal
if it holds
i) from $a \in m$ and $b \in m$ it implies $a - b \in m$
ii) from $a \in m$, $r \in R$ it implies $a \cdot r \in m$ for all $r \in R$

Examples: 1) The zero ideal consists only the zero element
2) The unity ideal consists the all ring elements

Two elements a, b is called congruent with the ideal m
if $a - b \in m$

Notation $a \equiv b \mod m$

Def. 3.17 Let R be a ring

The lattice $(L_I ; \wedge, \vee)$ of all ideals on the ring R is defined by

$I \wedge J := I \cap J$ for every ideals I, J

$I \vee J := \langle I, J \rangle$ is smallest ideal which generates by I, J

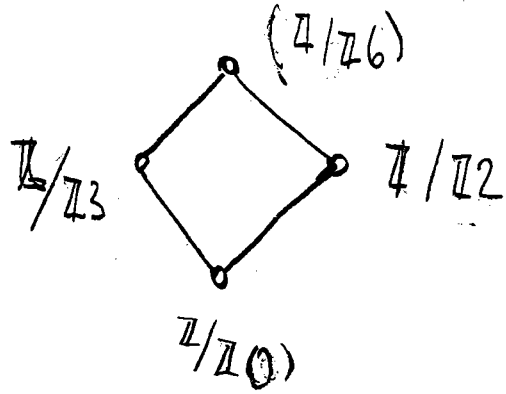
The lattice of a field or the lattice of a vector space are similarly defined.

(Example 3.18 We consider the ring

$$(\mathbb{Z}/\mathbb{Z}6 \; ; +, -, 0, \cdot)$$

There are ideals for instance

$a \equiv b \bmod(3)$ and $a \equiv b \bmod(2)$



§4 Homomorphisms, Terms and Polynomials

4A Homomorphisms

Def. 4.1 Let $\underset{\sim}{A}$ and $\underset{\sim}{B}$ be algebras of the same type. A function $\alpha : A \to B$ is homomorphism from $\underset{\sim}{A}$ to $\underset{\sim}{B}$ if for every n-arity operation $f \in \Omega$ and for every $a_1, \dots, a_n \in A$ it holds

$$\alpha(f_A(a_1, \dots, a_n)) = f_B(\alpha(a_1, \dots, a_n))$$

(We drop the indices)

If a homomorphism is bijective then it is called an isomorphism

An isomorphism $\alpha : A \to A$ is called an automorphism.

Def. 4.2 Let $\underset{\sim}{A} = (A; \wedge, \vee)$ and $\underset{\sim}{B} = (B; \wedge, \vee)$ be lattices. A function $f: A \to B$ is called a lattice homomorphism if it holds

$$f(x \wedge y) = f(x) \wedge f(y)$$

$$f(x \vee y) = f(x) \vee f(y) \quad (\text{for all } x, y \in A)$$

We make a difference between

$\wedge$- homomorphism

$\vee$- homomorphism

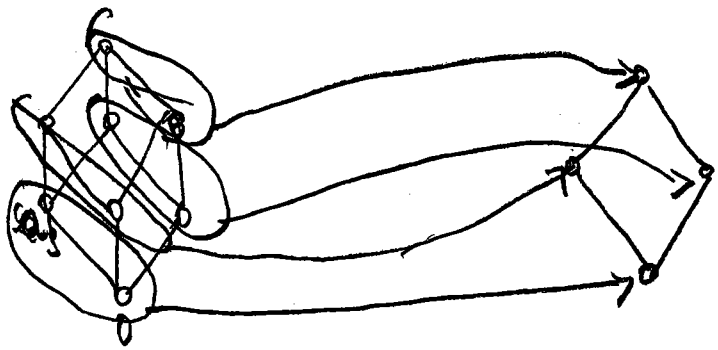
Prop. 4.3 Every $\wedge$-homomorphism $f: A \to B$ from a lattice $\underset{\sim}{A}$ to the lattice $\underset{\sim}{B}$ is monotone (= preserves the order relation)

Proof: For all $c, d \in A$ let it be $c \leq d$

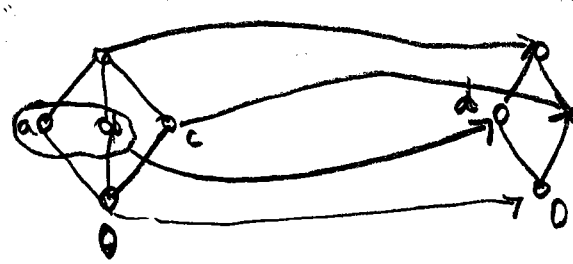
Then it holds $c = c \wedge d$ and $f(c) = f(c \wedge d)$

$= f(c) \wedge f(d) \leq f(d)$. It follows $f(c) \leq f(d)$ □

Example lattice homomorphism



function f



e is not a lattice homomorphism

because $f(a \wedge b) \neq f(a) \wedge f(b)$ $((0 \neq d \wedge d = d))$

4B Terms

Def. 4.4 Let an algebra $\mathbb{A}$ be given. The set T_m of the m-ary terms of the algebra $\mathbb{A}$ is defined by recursion:

i) x_i , $i = 1, \dots, m$ is a variable

ii) If $t_1(x_1, \dots, x_m) \in T_m, \dots, t_n(x_1, \dots, x_m) \in T_m$ are m-ary terms and f_σ is a n-ary operation then $f_\sigma(t_1(x_1, \dots, x_m), \dots, t_n(x_1, \dots, x_m))$ is m-ary term

Remark. The steps ii) can be applied only finite times

Notation 4.5 For lattices it holds

ii) If $t(x_1,\dots,x_m) \in T_m$ and $s(x_1,\dots,x_m) \in T_m$ are m-ary terms then

$$t(x_1,\dots,x_m) \wedge s(x_1,\dots,x_m)$$

$$t(x_1,\dots,x_m) \vee s(x_1,\dots,x_m)$$ are m-ary terms.

Example 4.6 The 3-ary term $m(x_1,x_2,x_3)$ is called majority term

$$m(x,y,z) = (x \wedge y) \vee (y \wedge z) \vee (z \vee x)$$

because $m(x,x,z) = m(x,z,x) = m(z,x,x) = x$

(Apply the axioms of a lattice)

Def. 4.7 For every n-ary term we can define a n-ary term function $t: A^n \longrightarrow A$ by $(a_1, \dots, a_n) \longmapsto t(a_1, \dots, a_n)$

for all $a_i \in A$, $i = 1, \dots, n$

Notation 4.8 The term function $\pi_i: A^n \longrightarrow A$ with $\pi_i(x_1, \dots, x_n) = x_i$ is called the i-the projection.

Notation 4.9

$$T := \bigcup_{n \in \mathbb{N}} T_n \qquad \text{Term}$$

Examples 4.10

1) Lattices of terms

$x \wedge (y \vee z)$ $\qquad$ $(x \wedge y) \vee (x \wedge z)$

2) Rings

$x \cdot (y + z)$ $\qquad$ $(x \cdot y) + (x \cdot z)$

3) Groups

$x^{-1} y x$ $\quad$ $x \cdot x \cdot x$ we write x^3

$x^3 \cdot y \cdot x \cdot y^2$

4) Boolean algebras

$x' \wedge y \wedge x$ $\quad$ $x \wedge x \wedge x$

Def 4.11 Let $\underset{\sim}{A} = (A; \Omega)$ be an algebra

An identity (or equality) is a pair

$(t(x_1, \dots, x_k), s(x_1, \dots, x_m)) \in T \times T$ of terms

We write $t(x_1, \dots, x_k) = s(x_1, \dots, x_m)$

An identity $t(x_1, \dots, x_k) = s(x_1, \dots, x_m)$ satisfies an algebra $\underset{\sim}{A}$ if for all $a_1, \dots, a_k, \dots, a_m \in A$ holds

$$t(a_1, \dots, a_k) = s(a_1, \dots, a_m)$$

We write also $\underset{\sim}{A} \models (t(x_1, \dots, x_k) = s(x_1, \dots, x_m))$

Examples

1) Lattices: Let $\underset{\sim}{L}$ be a distributive lattice

$$\underset{\sim}{L} \models (x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z))$$

2) Ring

$$\underset{\sim}{R} \models (x \cdot (y+z) = (x \cdot y) + (x \cdot z))$$

3) Groups $\underset{\sim}{G}$ an abelian algebra

$$\underset{\sim}{R} \models x^3 \cdot y \cdot x\, y^2 = x^4 \cdot y^{-1}$$

4) Boolean algebra

$$\underset{\sim}{B} \models (x \wedge x \wedge x = x)$$

4C Polynomials

Def 4.12 Let $\underset{\sim}{A} = (A; \Omega)$ be an algebra

The set $P_m(\underset{\sim}{A})$ of m-ary polynomials is defined by recursion.

i) x_i, $i = 1, \dots, m$ is a variable

ii) a is a constant (for all $a \in A$)

iii)

iii) If $p_1(x_1,\dots,x_m) \in P_n(\underset{\sim}{A}), \dots, p_n(x_1,\dots,x_m) \in P_n(\underset{\sim}{A})$ are m-arity polynomials and f_γ is a n-ary operation then

$$f_\gamma(p_1(x_1,\dots,x_m),\dots,p_n(x_1,\dots,x_m))$$

is an m-ary polynomial

In the same way we have the concept of a

polynomial function

$$(a_1,\dots,a_n) \longmapsto p(a_1,\dots,a_n)$$

We denote $P(\underset{\sim}{A}) := \bigcup_{n\in\mathbb{N}} P_n(\underset{\sim}{A})$

Examples 4.13

1) Let $\underset{\sim}{K} = (K; +, -, 0, \cdot, 1)$ be a field

Then $p(x) = a_n x_n + a_{n-1} x_{n-1} + \dots + a_1 x + a_0$

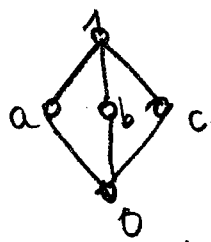
is a polynomial function in a

"normal form"

2) Let $G=(G;\cdot,^{-1},e)$ be a group

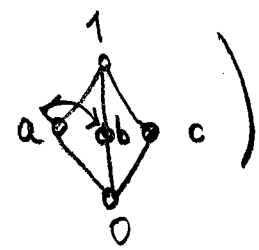
Then $p(x)=x^{-1}ax$ for some $a\in G$ is a polynomial function, namely an inner automorphism.

3) We consider the lattice M_3



$$p(x)=((x\wedge a)\vee c)\wedge b)\vee((x\wedge b)\vee c)\wedge a)\vee(x\wedge c)$$

is a polynomial function. (it is a lattice-automorphism



)

4) Boolean algebra

$$p(x,y)=(x\wedge y')\wedge(x'\wedge y)\wedge 1$$

$$(=x+y \bmod 2)$$

Proposition 4.14 Every term function of a lattice L is a monotone function.

Proof. Terms are constructed recursively. Hence we prove the statement by induction. Let $a_i \leq b_i$, $i = 1, \dots, n$ in L. For every projection $\pi_i(x_1, \dots, x_n)$ we have $\pi(a_1, \dots, a_n) = a_i \leq b_i = \pi_i(b_1, \dots, b_n)$. Let $t(x_1, \dots, x_n) = r(x_1, \dots, x_n) \vee s(x_1, \dots, x_n)$. By hypothesis r and s are monotone and hence $r(a_1, \dots, a_n) \leq r(b_1, \dots, b_n)$ and $s(a_1, \dots, a_n) \leq s(b_1, \dots, b_n)$.

Therefore $[r(a_1, \dots, a_n) \vee s(a_1, \dots, a_n)] \wedge [(r(b_1, \dots, b_n) \vee s(b_1, \dots, b_n)]$

$\leq [r(a_1, \dots, a_n) \wedge \{r(b_1, \dots, b_n) \vee s(b_1, \dots, b_n)\}] \vee$

$[s(a_1, \dots, a_n) \wedge \{r(b_1, \dots, b_n) \vee s(b_1, \dots, b_n)\}]$

$= r(a_1, \dots, a_n) \vee s(a_1, \dots, a_n)$.

The case $t = r \wedge s$ is proved dually

Proposition 4.15 Every polynomial function of a lattice $\underset{\sim}{L}$ is a monotone function.

Proof. Obviously the constant functions $c_a(x_1, \dots, x_n) = a$, $a \in L$, are monotone. Then we proceed by induction as in the proof of 3.4

4D Pre-fixed and fixed point

Def. 4.16 The element $c \in L$ is called fixed point of a monotone function $f: L \to L$ if $f(c) = c$. c is called an upper (lower) pre-fixed point of f if $f(c) \geq c$ $(f(c) \leq c)$

Theorem 4.17 Every polynomial function $p: L \to L$ of a lattice $\underset{\sim}{L}$ has a lower pre-fixed point.

Proof. We show that for any polynomial function p of a lattice there exists an element c_p such that for every c with $c_p \leq c$ it follows that $p(c) \leq c$. We proceed by induction.

If $p(x) = x$ then we choose an arbitrary

element $c_p \in L$. If $p(x) \equiv a$ then we put $c_p = a$. If $p(x) = q(x) \wedge r(x)$ then we put $c_p = c_q \wedge c_r$ and have for $c_p \leq c$ that $p(c) = q(c) \wedge r(c) \leq q(c) \leq c$. If $p(x) = q(x) \vee r(x)$ we put $c_p = c_q \vee c_r$. Let $c \geq c_q \vee c_r$. Then $p(c) = q(c) \vee r(c) \leq c$ by induction.

Def. 4.18 A lattice $\underset{\sim}{L} = (L; \wedge, \vee)$ has a greatest element 1 if $a \leq 1$ for every $a \in L$, and $\underset{\sim}{L}$ has a least element 0 if $0 \leq a$ for every $a \in L$.
A lattice $\underset{\sim}{L}$ with 0, 1 is called also a bounded lattices

Prop Remark 4.19 A lattice $\underset{\sim}{L}$ has a greatest (least) element iff each monotone function $f: L \to L$ has a lower (upper) prefixed point [ ]

Def. 4.20 A lattice $\underset{\sim}{L}$ is complete if for every subset $H \subseteq L$ the infimum $\bigwedge H$ and the supremum $\bigvee H$ exists.

Theorem 4.21 (Tarski) Let L be a complete lattice and f a monotone function $f: L \to L$. Then $f(c) = c$ for some $c \in L$

Proof. Consider the set S of all upper pre-fixed points. As $0 \in L$ and $0 \leq f(0)$ the set S is not empty. For $c := \sup S$ it follows from $x \leq c$ that $f(x) \leq f(c)$ and hence $x \leq f(x) \leq f(c)$ for all $x \in S$. Therefore $c = \sup S \leq f(c)$ and $c \in S$. As f is monotone we have $f(c) \leq ff(c))$ and hence $f(c) \in S$. Then $f(c) \leq c$ and altogether we have $f(c) = c$

Remark 4.24 A lattice $\underset{\sim}{L}$ is complete if and only if every monotone function $f: L \to L$ has a fixed point [Anne Davis]

Remark 4.25 Fixed points play an important role in a theory of the partial correctness of computer programs. [Dana Scott]

§5 Distributive and modular lattices

5A Distributive lattices

Proposition 5.1 The following inequalities hold for every lattice:

(5.1.1) $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$

(5.1.2) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

Proof. We have $x \wedge y \leq x$ and $x \wedge z \leq x$ and therefore $(x \wedge y) \vee (x \wedge z) \leq x$. Furthermore we have $x \wedge y \leq y$ and $x \wedge z \leq z$ and therefore $(x \wedge y) \vee (x \wedge z) \leq y \vee z$. Together we have $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. 5.1.2 is left to the reader.

Definition 5.2 A lattice L is distributive if the following identity holds.

(D) $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$ (distributive law)

Remark. The above identity is equivalent to the dual identity $(x \vee y) \wedge (x \vee z) = x \vee (y \wedge z)$

5B Modular lattices

Definition 5.5 A lattice $\underset{\sim}{L}$ is modular if the modular law (M) holds for every $x,y,z \in L$

(M) $x \leq z$ implies $x \vee (y \wedge z) = (x \vee y) \wedge z$

Remark. The modular law can be formulated as an identity. As $x \wedge z \leq x$ we have the identity

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

Proposition 5.6 Every distributive lattice is modular.

Proof. $(x \wedge z) \vee (y \wedge z) = [(x \wedge z) \vee y] \wedge [(x \wedge z) \vee z]$

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

Theorem 5.7 Let G be a group and $\widetilde{L(G)} = (L(G); \wedge, \vee)$ the lattice of all normal subgroups of G. Then $L(G)$ is modular

We use both of these distributive laws for calculations

Furthermore a lattice is distributive if and only if the following median identity holds

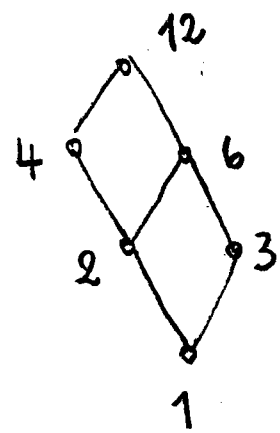
$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$$

Example 5.3 The lattice $(P(M); \cap, \cup)$ is distributive

Example 5.4 The lattice $(D(n); \wedge, \vee)$ of all divisors of the number n is distributive.

Let k_1, k_2 be divisors of n then $k_1 \vee k_2$ is defined as the least common multiple of k_1, k_2 and $k_1 \wedge k_2$ as the greatest common divisor of k_1, k_2

Illustration $n = 12$



Proof. Let N_1, N_2, N_3 be normal subgroups of G and let $N_1 \subseteq N_3$. Then we have to show that $N_1 \vee (N_2 \wedge N_3) = (N_1 \vee N_2) \wedge N_3$. According to (4.1.2) it is sufficient to show $N_1 \vee (N_2 \wedge N_3) \geq (N_1 \vee N_2) \wedge N_3$. Using complex multiplication we have to prove $(N_1 \cdot N_2) \wedge N_3 \subseteq N_1 \cdot (N_2 \cap N_3)$.

If $n \in N_1 \cdot N_2 \cap N_3$ then $n = n_1 \cdot n_2$ for some $n_1, n_2 \in N_1 \cdot N_2$ and $n_1 \cdot n_2 \in N_3$. We have $n_1 \in N_1 \subseteq N_3$ and hence we conclude $n_2 \in N_3$. Therefore $n_2 \in N_2 \cap N_3$ and hence $n_1 \cdot n_2 \in N_1 \cdot (N_2 \cap N_3)$

Thm. 5.8 Let V be a K-vector space and $\underset{\sim}{L}(V) = (L(V); \wedge, \vee)$ be the lattice of all subspaces. Then $\underset{\sim}{L}(V)$ is modular

Proof. (This proof deliver the same arguments as in 5.7)

We have to show that $(U_1 \vee U_2) \wedge U_3 \subseteq U_1 \vee (U_2 \wedge U_3)$

for $U_1 \subseteq U_3$

$U_1 \wedge U_2 = U_1 \cap U_2$

$U_1 \vee U_2 = \operatorname{span}(U_1, U_2)$

Let $v \in (U_1 \vee U_2) \wedge U_3$ and therefore $v \in \operatorname{span}(U_1, U_2)$ and $v \in U_3$. Then there are vectors $u_1 \in U_1$ $u_2 \in U_2$ such that $v = u_1 + u_2 \in \operatorname{span}(U_1, U_2)$ and $u_1 + u_2 \in U_3$. Now $u_1 \in U_1 \subseteq U_3$ and also $u_1 \in U_3$. It follows $u_2 = \underbrace{u_1 + u_2}_{\in U_3} - u_1 \in U_3$ $\in U_3$

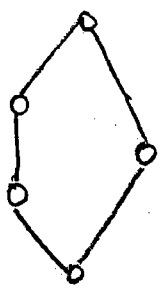
Also we have $u_2 \in U_2 \cap U_3$

$u_1 + u_2 \in \operatorname{span}(U_1, U_2 \cap U_3)$ □

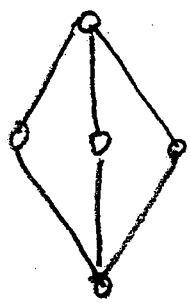
Remark. The above results hold also for the lattice of all ideals of a commutative ring and also for the lattice of all submodules of a module. The above result is also

called Dedekind's theorem on modules.

In the following we present the lattices N_5 and M_3 by their Hasse-diagrams.



N_5



M_3 {Birkhoff / Dedekind}

Proposition 5.9 Every non-modular lattice L has a sublattice which is isomorphic to N_5

Proof. Let $a,b,c \in L$ with $a < c$ and $a \vee (b \wedge c) < (a \vee b) \wedge c$
We put $A := a \vee (b \wedge c)$, $B := b$, and $C := (a \vee b) \wedge c$
$D := b \wedge c$ and $E := a \vee b$. It is obvious that
$D < A < C < E$ and $D < B < E$. We have
$A \vee B = E$ and hence $C \vee B = E$. We have $C \wedge B = D$
and hence $A \wedge B = D$. $(\{A, B, C, D, E\}; \wedge, \vee)$ is
a sublattice of L isomorphic to N_5

Proposition 5.10 Every modular lattice $\underline{L}$ which is not distributive has a sublattice which is isomorphic to M_3

Proof. If $\underline{L}$ is not distributive then the median identity does not hold and we have the following proper inequality for some elements $d, e, f \in L$

$$l := (d \wedge e) \vee (e \wedge f) \vee (f \wedge d) < (d \vee e) \wedge (e \vee f) \wedge (f \vee d) =: r$$

We denote the element on the left hand side with l and on the right hand side with r and have $l < r$.

Furthermore we put $a := (d \wedge r) \vee l$, $b := (e \wedge r) \vee l$ and $c := (f \wedge r) \vee l$.

Then we have

$$d \wedge r = d \wedge [(d \vee e) \wedge (e \vee f) \wedge (f \vee d)] = d \wedge (e \vee f) \text{ and}$$

$$e \wedge r = e \wedge (f \vee d)$$

$$f \wedge r = f \wedge (d \vee e)$$

~~From this follows~~

$$a \vee b = [(d \wedge r) \vee l] \vee [(e \wedge r) \vee l]$$

$$= [d \wedge (e \vee f)] \vee [[e \wedge (f \vee d)] \vee l]$$

Now we have $d \wedge (e \vee f) \leq f \vee d$ and by modularity

$a \vee b = \langle \{[d \wedge (e \vee f)] \vee e\} \wedge (f \vee d) \rangle \vee l$

We have $e \leq e \vee f$ and by modularity

$a \vee b = \langle (e \vee f) \wedge (d \vee e) \wedge (f \vee d) \rangle \vee l$

$= r \vee l = r$

In a similar way one gets $b \vee c = r$ and $a \vee c = r$

Furthermore we have $a = (d \vee l) \wedge r$ because of $l < r$ and $(l \vee d) \wedge r = l \vee (d \wedge r) = a$ and in the same way

$b = (e \vee l) \wedge r$ and $c = (f \vee l) \wedge r$

By duality (or calculation) we get $a \wedge b = l$ $b \wedge c = l$ and $a \wedge c = l$. $(\{a, b, c, r, l\}; \wedge, \vee)$ is isomorphic to M_3.

Theorem 5.11 A lattice $\underset{\sim}{L}$ is distributive if and only if L has neither a sublattice isomorphic to M_3 nor to N_5

The proof follows from the lemma above.

5C Boolean algebras

Definition 5.12 The algebra $\underset{\sim}{B} = (B; \wedge, \vee, ', 0, 1)$ is a Boolean algebra if the following holds.

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

2) $x \wedge y = y \wedge x$ commutativity $x \vee y = y \vee x$

3) $x \wedge x = x$ idempotency $x \vee x = x$

4) $x \wedge (x \vee y) = x$ absorption $x \vee (x \wedge y) = x$

5) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ distributivity $x \vee (y \wedge z) = (x \vee y) \wedge (x$

6) $(x \wedge y)' = x' \vee y'$ De Morgan law $(x \vee y)' = x' \wedge y'$

7) $x \wedge x' = 0$ complement $x \vee x' = 1$

8) $x'' = x$

Example of Boolean algebras

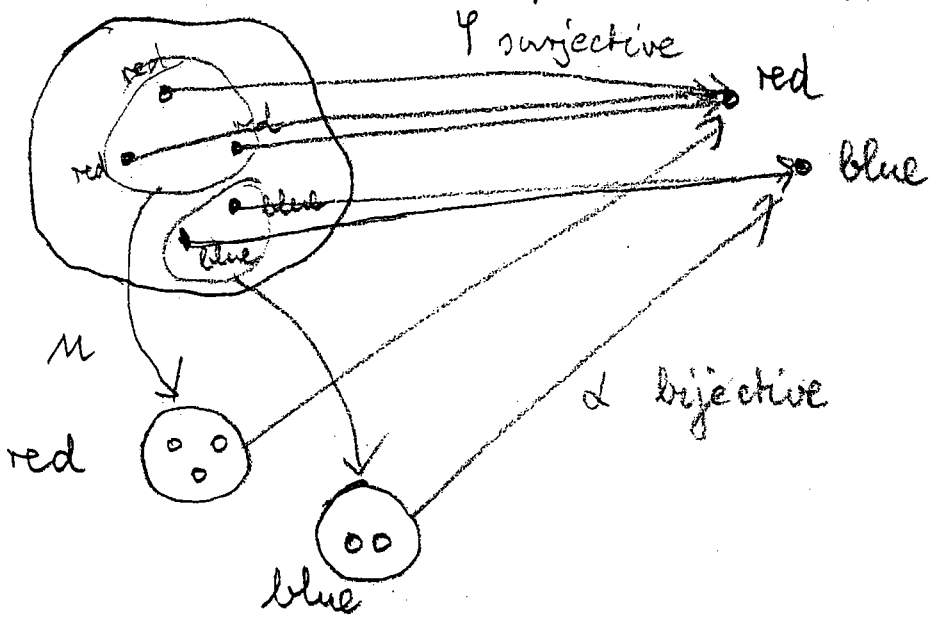
1) The two-element Boolean algebra
$\underset{\sim}{B} = (\{0,1\}; \wedge, \vee, ', 0, 1)$

2) Power set algebra
$\underset{\sim}{P} = (P(M); \cap, \cup, ^c, \emptyset, M)$

§6 Homomorphisms and congruence relations

6A Homomorphism Theorem

Remark 6.1 A boy owns a set of colored marbles. He sorts the marbles into classes of the same color, and takes from every class one marble as a representative. He has as many classes of marbles of different colors as representatives.



Definition 6.2 An n-ary relation ρ on A is a (non-empty) subset $\rho \subseteq A^n = \{(a_1, \dots, a_n) \mid a_i \in A\}$

A binary relation ρ on A is an equivalence relation of A if the following hold for every $a, b, c \in A$

(i) $(a,a) \in \rho$ (reflexivity)

(ii) If $(a,b) \in \rho$ then $(b,a) \in \rho$ (symmetry)

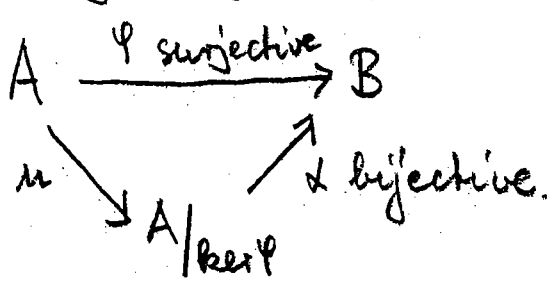
(iii) If $(a,b) \in \rho$ and $(b,c) \in \rho$ then $(a,c) \in \rho$ (transitivity)

We often write $\left[\begin{array}{l} a \rho b \\ a \equiv b \bmod \rho \end{array}\right]$ instead of $(a,b) \in \rho$.

Definition 6.3 If ρ is an equivalence relation of A then $[a]_\rho = \{ b \mid (a,b) \in \rho, b \in B \}$ is called the equivalence class of A.
$A/\rho = \{ [a]_\rho \mid a \in A \}$ is called the factor set in respect to ρ.

Definition 6.4 Let $\varphi : A \to B$ a surjective function. The equivalence relation $\ker \varphi$ is defined by $(a,b) \in \ker \varphi$ if and only if $\varphi(a) = \varphi(b)$

Remark. It is obvious that $\ker \varphi$ is an equivalence relation because $\ker \varphi$ is defined via an equality.
The above situation in 6.1 can be described in the following way.



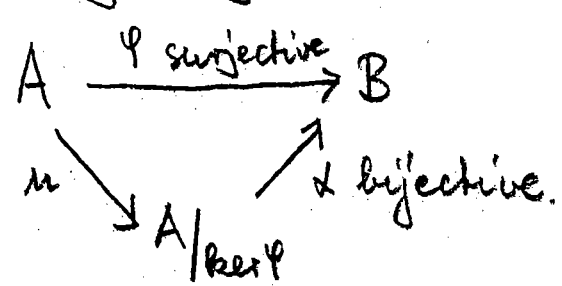
$\mu : A \longrightarrow A/\ker\varphi$ is defined by $\mu(a) = [a]_{\ker\varphi}$

We often write $\left[\begin{array}{l} a \varrho b \\ a \equiv b \bmod \varrho \end{array}\right]$ instead of $(a,b) \in \varrho$.

Definition 6.3 If ϱ is an equivalence relation of A then $[a]_\varrho = \{ b \mid (a,b) \in \varrho, b \in B \}$ is called the equivalence class of A.
$A/\varrho = \{ [a]_\varrho \mid a \in A \}$ is called the factor set in respect to ϱ.

Definition 6.4 Let $\varphi : A \to B$ a surjective function. The equivalence relation $\ker \varphi$ is defined by $(a,b) \in \ker \varphi$ if and only if $\varphi(a) = \varphi(b)$

Remark. It is obvious that $\ker \varphi$ is an equivalence relation because $\ker \varphi$ is defined via an equality.
The above situation in 6.1 can be described in the following way.



$u : A \longrightarrow A/\ker\varphi$ is defined by $u(a) = [a]_{\ker\varphi}$

Definition 6.5 Let $\underset{\sim}{A} = (A, \Omega)$ be an algebra. The equivalence relation ϱ on A is a congruence relation of the algebra if for every n-ary operation $f_\sigma \in \Omega$ and every pairs $(a_1, b_1) \in \varrho, \dots, (a_n, b_n) \in \varrho$ it follows $(f_\sigma(a_1, \dots, a_n), f_\sigma(b_1, \dots, b_n)) \in \varrho$

$\underset{\sim}{A}/\varrho = (A/\varrho, \Omega)$ is called factor algebra (or quotient algebra). The operations f_σ are defined for $\underset{\sim}{A}/\varrho$ by

$$f_\sigma([a_1]_\varrho, \dots, [a_n]_\varrho) = [f_\sigma(a_1, \dots, a_n)]_\varrho$$

Remark. The operations for $\underset{\sim}{A}/\varrho$ are well defined because ϱ is compatible with the operation of $\underset{\sim}{A}$.

Example 6.6 Let $(\mathbb{Z}; +, -, 0, \cdot, 1)$ be the ring of integers. We define

$(a, b) \in \varrho$ if and only if m multiple of $(a-b)$

Then ϱ is congruence relation. (Proof left to the reader.)

$\mathbb{Z}/\varrho = \mathbb{Z}/m\mathbb{Z}$ the ring of residue classes mod m

Definition 6.7 Let $\underset{\sim}{A} = (A, \Omega)$ and $\underset{\sim}{B} = (B, \Omega)$ be algebras of the same type τ. $\varphi : A \to B$ is a homomorphism if for every $a_1, \dots, a_n \in A$ and every n-ary operation f_σ it follows $\varphi(f_\sigma(a_1, \dots, a_n)) = f_\sigma(\varphi(a_1), \dots, \varphi(a_n))$

Example 6.8 Let $(G; \cdot, ^{-1}, e)$ cyclic group of order n. Let m be a divisor of n Then $\varphi(x) = x^m$ is a homomorphism $\varphi : G \to G$
We have $\varphi(x \cdot y) = (x \cdot y)^m = x^m \cdot y^m = \varphi(x) \cdot \varphi(y)$
Further more $\varphi(x^{-1}) = (x^{-1})^m = x^{-m} = (x^m)^{-1}$ $= \varphi(x)^{-1}$ and $\varphi(e) = e^m = e$.

Remark 6.9 If $\varphi : G \to H$ is a homomorphism from the group $(G; \cdot, ^{-1}, e)$ into the group $(H; \cdot, ^{-1}, e)$ then $(a, b) \in \ker \varphi$ if and only if $\varphi(ab^{-1}) = e$
If $(a, b) \in \ker \varphi$ then $\varphi(a) = \varphi(b)$ and hence $e = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a \cdot b^{-1})$ and vice versa

Remark 6.10 The K-vector space V can be considered as an universal algebra $\underset{\sim}{V} = (V; +, -, 0, \lambda_{K(k \in K)})$ of type $\tau = (2, 1, 0, 1, \ldots, 1, \ldots)$. The scalar multiplication is understood as $|K|$ unary operations $\lambda_k : V \to V$ with $v \longmapsto \lambda_k$

Let $\varphi : V_1 \to V_2$ be a homomorphism from the K-vector space V_1 into the K-vector space. Then $(v, w) \in \ker \varphi$ if and only $\varphi(v - w) = 0$

If $(v, w) \in \ker \varphi$ then $\varphi(v) = \varphi(w)$ and hence $0 = \varphi(v) - \varphi(w) = \varphi(v - w)$ and vice versa

Proposition 6.11 Let $\underset{\sim}{A} = (A, \Omega)$ and $\underset{\sim}{B} = (B, \Omega)$ be algebras of the same type (2.11.1). If $\varphi : A \to B$ a homomorphism then $\ker \varphi$ is a congruence relation. (2.11.2) If ρ is a congruence relation then $\mu : A \to A/\rho$ ($\mu(a) = [a]_\rho$) is a surjective homomorphism.

Proof of 6.11.1 We have already noted that $\ker \varphi$ is an equivalence relation. Let $(a_1, b_1) \in \ker \varphi, \ldots, (a_n, b_n) \in \ker \varphi$ and f_δ an n-ary operation. It follows that $\varphi(a_i) = \varphi(b_i)$ for $i = 1, \ldots, n$. We have

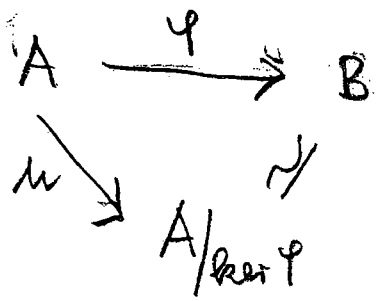
$$\varphi(f_\delta(a_1, \ldots, a_n)) = f_\delta(\varphi(a_1), \ldots, \varphi(a_n))$$
$$= f_\delta(\varphi(b_1), \ldots, \varphi(b_n)) = \varphi(f_\delta(b_1, \ldots, b_n))$$

and hence $(f_\delta(a_1, \ldots, a_n), f_\delta(b_1, \ldots, b_n)) \in \ker \varphi$.

6.11.2 We have $\mu(f_\delta(a_1, \ldots, a_n))$.

$$= [f_\delta(a_1, \ldots, a_n)]_\rho = f_\delta([a_1]_\rho, \ldots, [a_n]_\rho)$$
$$= f_\delta(\mu(a_1), \ldots, \mu(a_n)).$$ μ is surjective.

Theorem 6.12 (Homomorphism Theorem)
If $\varphi: A \to B$ is a surjective homomorphism from the algebra $\underset{\sim}{A}$ into the algebra $\underset{\sim}{B}$ then there is an isomorphism $\alpha: A/\ker\varphi \to B$



Proof. We define $\alpha: A/\ker\varphi \to B$
$\alpha([x]_{\ker\varphi}) := \varphi(x)$. If we have $[a_1]_{\ker\varphi} = [a_2]_{\ker\varphi}$ then $(a_1, a_2) \in \ker\varphi$ and hence $\varphi(a_1) = \varphi(a_2)$
Therefore α is well-defined.
α is surjective. If $b \in B$ then there is $a \in A$ with $\varphi(a) = b$ because φ is surjective
We have $\alpha[a]_{\ker\varphi} = \varphi(a) = b$.
α is injective. If $\alpha([c]_{\ker\varphi}) = \alpha([d]_{\ker\varphi})$ then $\varphi(c) = \varphi(d)$ and hence $(c, d) \in \ker\varphi$
It follows $[c]_{\ker\varphi} = [d]_{\ker\varphi}$.

α is a homomorphism. We consider

$$\alpha(f_\sigma([a_1]_{\ker\varphi}, \dots [a_n]_{\ker\varphi}) =$$

$$= \alpha([f_\sigma(a_1, \dots, a_n)]_{\ker\varphi})$$

$$= \varphi(f_\sigma(a_1, \dots, a_n))$$

$$= f_\sigma(\varphi(a_1), \dots, \varphi(a_n))$$

$$= f_\sigma(\alpha([a_1]_{\ker\varphi}), \dots, \alpha([a_n]_{\ker\varphi}))$$

6 B Congruence lattices

6B Modular congruence lattices

Notation. Let ς be a congruence relation of an algebra (A, Ω). We will say ς is a congruence and write $a \varsigma b$ instead of $(a,b) \in \varsigma$

Definition 6.13 Let θ, ς be congruences of (A, Ω). We define

$a(\theta \wedge \varsigma) b$ if and only if $a \theta b$ and $a \varsigma b$

$a(\theta \vee \varsigma) b$ if and only if there is a finite sequence of elements $z_1, \dots, z_n \in A$ such that $a \eta_1 z_1, \dots, z_{i-1} \eta_i z_i, \dots, z_n \eta_{n+1} b$ with $\eta_i \in \{\theta, \varsigma\}$ $i = 1, \dots, n+1$.

The set of congruences of the algebra A is denoted by $\underset{\sim}{\mathrm{Con}} A$. The least congruence is the identity relation Δ and the greatest congruence is the all relation ∇
$(a,b) \in \Delta$ iff $a = b$, $(a,b) \in \nabla$ for all $a, b \in A$

Proposition 6.14 $(\underset{\sim}{\mathrm{Con}} A; \wedge, \vee)$ with the operation declared in .1 is a lattice with a least element Δ and greatest element ∇

The proof is rather technically and left to the reader.

Lemma 6.15 Every congruence relation of a group G corresponds to a normal subgroup of G and vice versa

Proof (A) Let ϱ be a congruence of G. We show that $N_\varrho = \{g \mid g \in G, (g,e) \in \varrho\}$ is a normal subgroup of G.

Let $a, b \in N_\varrho$. We have $(a,e) \in \varrho$ and $(b,e) \in \varrho$

As ϱ is a congruence it follows that $(b^{-1}, e^{-1}) \in \varrho$

and hence $(b^{-1}, e) \in \varrho$ and $(a \cdot b^{-1}, e \cdot e) \in \varrho$

It follows that N_ϱ is a subgroup because $a \cdot b^{-1} \in N_\varrho$

It remains to show that $g N_\varrho g^{-1} \subseteq N_\varrho$ for every $g \in G$.

We have $(n, e) \in \varrho$ for every $n \in N_\varrho$ and $(g^{-1}, g^{-1}) \in \varrho$, $(g, g) \in \varrho$ because ϱ is reflexive. It follows that $(gng^{-1}, geg^{-1}) \in \varrho$ and $(gng^{-1}, e) \in \varrho$.

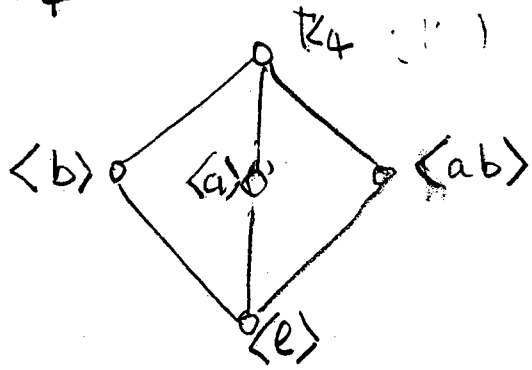
Therefore $gng^{-1} \in N_\varrho$ and we are done with the first direction.

(B) Let N be a normal subgroup of G, It is left for the reader to show that $(a,b) \in \xi$ if and only if $a.b^{-1} \in N$ defines a congruence on G.

Remark 6.116 The above correspondence is a lattice isomorphism.

Example 6.5 We consider the four-group of Klein $K_4 = \{e, a, b, ab\}$ with $a^2 = b^2 = e$ and $ab = ba$

Every subgroup of an abelian group is a normal subgroup. We have the congruence lattice $\mathrm{Con}\, K_4$



Lemma 6.117 Let $\underset{\sim}{R} = (R; +, -, 0, \cdot, 1)$ be a commutative ring with 1. Every congruence of $\underset{\sim}{R}$ corresponds to an ideal of R and vice-versa

The proof is similar as above.

Overview and example 6

1) ς is a congruence on the algebra $\underset{\sim}{A}$

if i) ς is equivalence relation

(reflexive, symmetric, transitive)

ii) $(a_1, b_1) \in \varsigma, \ldots, (a_n, b_n) \in \varsigma$

$\Longrightarrow (f_\sigma(a_1, \ldots, a_n), f_\sigma(b_1, \ldots, b_n))$

for every operation f_σ of $\underset{\sim}{A}$

2) Example $(\mathbb{Z}; +, -, 0, \cdot, 1)$

We define: $(a,b) \in \varsigma \Leftrightarrow a \equiv b \bmod m$

i) ς is an equivalence:

$(a,a) \in \varsigma$ is reflexive because $a \equiv a \bmod m$

$(a,b) \in \varsigma$ we have $a \equiv b \bmod m$

$\Rightarrow b \equiv a \bmod m$ therefore $(b,a) \in \varsigma$ is symmetric

$(a,b) \in \varsigma$ and $(b,c) \in \varsigma$. we have

$a \equiv b \bmod m$

$b \equiv c \bmod m$

and therefore $a \equiv c \bmod m$, therefore $(a,c) \in \varsigma$ transitive

The following is Dedekind's theorem on modules in another form

Theorem 6.18 The congruence lattice of a group (a vector space or a commutative ring respectively) is modular.

Proof. The theorem follows from [illegible] and the above correspondence.

6B Permutable congruences

Definition 6.19 Let θ_1, θ_2 be binary relations on a set A. The product $\theta_1 \circ \theta_2$ is defined in the following way
$(a,b) \in \theta_1 \circ \theta_2$ if and only if there exists $c \in A$ with
$(a,c) \in \theta_1$ and $(c,b) \in \theta_2$

Definition 6.20 The congruence relations θ_1, θ_2 of an algebra are called permutable if and only if $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$

Theorem 6.21. The congruence relations of a groups are permutable.

Proof. We consider a group $\underset{\sim}{G} = (G; \cdot, ^{-1}, e)$ and $(a,b) \in \theta_1 \circ \theta_2$ for congruences θ_1, θ_2 of $\underset{\sim}{G}$
Then we have $c \in G$ with $(a,c) \in \theta_1$ and $(c,b) \in \theta_2$
As θ_2 is a congruence we have $(a,a) \in \theta_2$
and from $(c,b) \in \theta_2$ it follows $(ac, ab) \in \theta_2$
and hence $(a, abc^{-1}) \in \theta_2$

ii) operations is compatible

$(a_1, b_1) \in \mathfrak{S}$ and $(a_2, b_2) \in \mathfrak{S}$

We have $a_1 \equiv b_1 \bmod m$ and $a_2 \equiv b_2 \bmod m$

We use the calculations of congruences (see van der Waerden page 60)

$a_1 + a_2 \equiv b_1 + b_2 \bmod m$

Therefore we have $(a_1 + a_2, b_1 + b_2) \in \mathfrak{S}$

For the other operation we use again the calculations of the congruences of a ring

$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \bmod m$ and so on

As θ_1 is a congruence we have $(b, b) \in \theta_1$ and from $(a, c) \in \theta_1$ it follows that $(ab^{-1}, cb^{-1}) \in \theta_1$ and furthermore $(abc^{-1}, b) \in \theta_1$. Hence $(a, b) \in \theta_2 \circ \theta_1$.

Remark. Theorem 3.10 reflects the property of groups that normal subgroups N_1, N_2 are permutable, i.e. $N_1 \cdot N_2 = N_2 \cdot N_1$. Of course 3.10 can be also formulated for vector spaces and rings.

Theorem 6.22 If an algebra $\underset{\sim}{A}$ has permutable congruence then the congruence lattice $\mathrm{Con}(\underset{\sim}{A})$ is modular.

Proof. First of all we like to note that if $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ then we have $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$

We consider $\theta, \Psi, \eta \in Con(\underset{\sim}{A})$ with $\theta > \eta$. Then it is enough to show that $\theta \wedge (\Psi \vee \eta) \leq (\theta \wedge \Psi) \vee \eta$

Let $(a,b) \in \theta \wedge (\Psi \vee \eta)$. Then $(a,b) \in \theta$ and there is $c \in A$ with $(a,c) \in \Psi$ and $(c,b) \in \eta$

As $\eta < \theta$ we have $(c,b) \in \theta$ and hence $(a,c) \in \theta$

Altogether we have $(a,c) \in \theta \wedge \Psi$, $(c,b) \in \eta$ and hence $(a,b) \in (\theta \wedge \Psi) \vee \eta$.

For the next proposition we need the concept of a relatively complemented lattice $\underset{\sim}{L}$. Let $a < c < b$ be in L. $c' \in L$ is called a relative complement of c if $c \wedge c' = a$ and $c \vee c' = b$. $\underset{\sim}{L}$ is called relatively complemented if for every $a, b, c \in L$ with $a < c < b$ there exists a relative complement c'.

Theorem 6.23 The congruence relations of a relatively complemented lattice are permutable.

Proof. Let $a,b,c \in L$ and let θ, Ψ be congruence of L with $(a,b) \in \theta$ and $(b,c) \in \Psi$. Let a_1 be a relative complement of $a \vee b$ in the sublattice (interval) $[a, a \vee b \vee c] = \{d \mid a \leq d \leq a \vee b \vee c, d \in L\}$. and c_1 a complement of $b \vee c$ in the sublattice $[c, a \vee b \vee c]$. Put $d := a_1 \wedge c_1$. We have $(a \vee b, a \vee b \vee c) \in \Psi$ and $((a \vee b) \wedge a_1, (a \vee b \vee c) \wedge a_1) \in \Psi$ and hence $(a, a_1) \in \Psi$.

In similar way we get $(c_1, c) \in \theta$. We have $(a \vee b, a) \in \theta$ and $(a \vee b \vee a_1, a_1) \in \theta$ and hence $(a \vee b \vee c, a_1) \in \theta$.

Now we have $a_1 \leq a_1 \vee c_1 \leq a \vee b \vee c$ and hence $(a_1 \vee c_1, a_1) \in \theta$. Furthermore $(c_1, a_1 \wedge c_1) \in \theta$ and hence $(c, d) \in \theta$

In a similar way we show $(a, d) \in \Psi$ and we have $(a, c) \in \Psi \circ \theta$.

C Distributive congruence lattices.

Theorem 6.24 (Funayama and Nakayama) The congruence lattice of a lattice is distributive

Proof. For the congruences θ, Φ, Ψ of the congruence lattice $Con(L)$ of a lattice we have to show $\theta \wedge (\Phi \vee \Psi) \leq (\theta \wedge \Phi) \vee (\theta \wedge \Psi)$ as the other direction holds in all lattices.

Let $(a,b) \in \theta \wedge (\Phi \vee \Psi)$. Then $(a,b) \in \theta$ and $(a,b) \in \Phi \vee \Psi$. Now $(a,b) \in \Phi \vee \Psi$ if and only if $(a \wedge b, a \vee b) \in \Phi \vee \Psi$. Hence there exist a sequence $a \wedge b = z_0 \leq z_1 \leq \dots \leq z_n = a \vee b$ where $(z_k, z_{k+1}) \in \Phi$ or $(z_k, z_{k+1}) \in \Psi$, $k = 0, \dots, n-1$,

(The sequence can be ordered in such a chain. Namely from $(z_0, z_1) \in \Phi$ it follows $(z_0, z_1 \vee z_0) \in \Phi$ and we proceed in such a way till we have $(z_1 \vee \dots \vee z_{n-1}, z_1 \vee \dots \vee z_n) \in \Phi$ (or Ψ). In the case of $z_1 \vee \dots \vee z_n \notin a \vee b$ we use the meet of

every member of the sequence with $a \vee b$.)

We have $(a,b) \in \theta$ and hence $(a \wedge b, a \vee b) \in \theta$ and furthermore $(z_k, z_{k+1}) \in \theta$. Altogether we have $(z_k, z_{k+1}) \in \theta \wedge \Phi$ or $(z_k, z_{k+1}) \in \theta \wedge \Psi$ and hence $(a \wedge b, a \vee b) \in (\theta \wedge \Phi) \vee (\theta \wedge \Psi)$.

Example 15. A Boolean algebra $\underset{\sim}{B} = [B; \wedge, \vee, ', 0, 1]$ has a distributive congruence lattice, because a Boolean algebra is also a lattice. Furthermore $(B; \wedge, \vee)$ is relatively complemented. Let $a < c < b$ in B. Then $d = (c' \vee a) \wedge b$ is a relative complement: $d \wedge c = c \wedge (c' \vee a) \wedge b = c \wedge (c' \vee a) = (c \wedge c') \vee (c \wedge a) = a$, $d \vee c = ((c' \vee a) \wedge b) \vee c = (c' \vee a \vee c) \wedge (b \vee c) = b$.

It follows that a Boolean algebra has permutable congruences.

§7 Direct and subdirect products

Remark. Human beings like to decompose an object into parts and then reconstruct the object from the parts. A chemist decomposes matter into its elements and construct new connections from the elements. A physicist decomposes matter in molecules, the molecules into atoms and the atoms into elementary particles. The experience shows that a lot of indecomposable or simple parts are not so simple but only need finer tools for an additional decomposition, or for an adequate description.

Definition 7.1 The algebra $\underset{\sim}{A}$ is called simple if the congruence lattice $\mathrm{Con}\,\underset{\sim}{A}$ consists only of the trivial congruences namely the identity relation Δ and the all relation ∇.

Example 7.2 Simple abelian groups are of prime order. Non-abelian simple groups are for instance the alternating groups A_n, $n \geq 5$. There exist "complicated" simple groups like the sporadic groups

Repetition:

ϱ is a congruence of the algebra $\underset{\sim}{A}$

i) ϱ is an equivalence

ii) ϱ is compatible with operations Ω

---

lattice of congruences

$(\mathrm{Con}\,\underset{\sim}{A}\,;\wedge,\vee)$

$a\,(\theta\wedge\varrho)\,b \iff a\theta b$ and $a\varrho b$

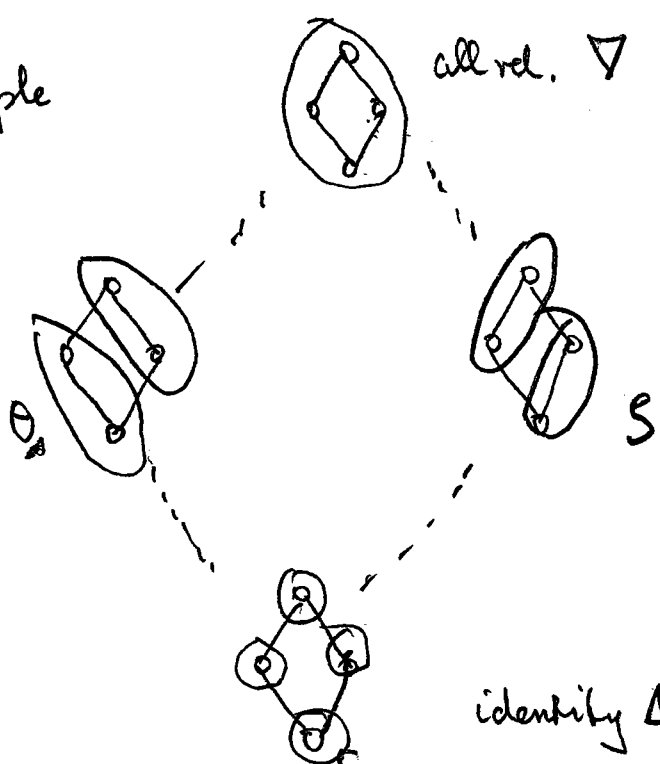
$a\,(\theta\vee\varrho)\,b \iff$ finite sequence

of elements $z_1,\dots,z_n$ such that

$a\,\eta_1 z_1, z_1\,\eta_2 \dots, z_n\,\eta_n b$

with $\eta_i \in \{\theta,\varrho\}$ $\quad i=1,\dots,n$

Example



7.3

Definition 7.3 Let $\underset{\sim}{A} = (A, \Omega)$, $\underset{\sim}{B} = (B, \Omega)$ be algebras of the same type. On the cartesian product $A \times B$ the operations are defined in the following way.

If $(a_1, b_1) \in A \times B, \dots, (a_n, b_n) \in A \times B$ then we have

$$f((a_1, b_1), \dots, (a_n, b_n)) := (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in A \times B$$

for every n-ary operation $f \in \Omega$.

$\underset{\sim}{A} \times \underset{\sim}{B} = (A \times B, \Omega)$ is called direct product of $\underset{\sim}{A}, \underset{\sim}{B}$

Example, $(\mathbb{R}^2, +)$ where we define

$$(a, b) + (c, d) = (a + c, b + d)$$

Definition 7.4 The map $\pi_i : A_1 \times A_2 \to A_i$ for $i = 1, 2$ is defined by

$$\pi_i(a_1, a_2) = a_i$$

and is called the ith projection

It is obvious that π_i is a homomorphism

The congruence relation which belongs to π_i is called factor congruence.

Definition 7.5 The congruence ϱ of an algebra $\underset{\sim}{A}$ is called a factor congruence if there is a congruence ϱ^* of $\underset{\sim}{A}$ such that

(i) $\varrho \wedge \varrho^* = \Delta$

(ii) $\varrho \vee \varrho^* = \nabla$

(iii) $\varrho \circ \varrho^* = \varrho^* \circ \varrho$

Thm 7.6 If ϱ, ϱ^* is a pair of factor congruences then

$$A \cong A/\varrho \times A/\varrho^*$$

The isomorphism α is defined by

$$\alpha(a) = ([a]_\varrho, [a]_{\varrho^*})$$

where $[a_\varrho] = \{b \mid (a,b) \in \varrho, b \in A\}$ and $[a_{\varrho^*}] = \dots$ is given.

Proof. We have to show that α is an isomorphism

1) α is injective

If $\alpha(a) = \alpha(b)$ then $([a]_\varrho, [a]_{\varrho^*}) = ([b]_\varrho, [b]_{\varrho^*})$

and therefore $[a]_\varrho = [b]_\varrho$ and $[a]_{\varrho^*} = [b]_{\varrho^*}$

It follows $(a,b) \in \varrho$ and $(a,b) \in \varrho^*$

By 7.5(i) it follows $\varrho \cap \varrho^* = \Delta$ (identity)

Therefore $a = b$

2) α is surjective

Let $([a]_\varrho, [b]_{\varrho^*}) \in A/\varrho \times A/\varrho$ be arbitrary

Then we have $(a,b) \in \zeta \vee \zeta^*$ namely the all relation ∇. Also there exist $c_1, \dots, c_n \in A$ with $(c_1, c_2) \in \theta_1, \dots, (c_{n-1}, c_n) \in \theta_n$ where $\theta_i \in \{\zeta, \zeta^*\}$ with $c_1 = a$ and $c_n = b$. By changing of 7,5 iii we get $(a,b) \in \zeta \circ \zeta^*$. Therefore there is $c \in A$ with $(a,c) \in \zeta$ and $(c,b) \in \zeta^*$

c is the element with the property

$$\alpha(c) = ([c]_\zeta, [c]_{\zeta^*}) = ([a]_\zeta, [b]_{\zeta^*})$$

3) α is a homomorphism

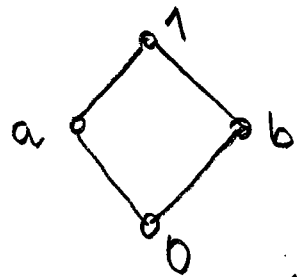
Let $f \in \Omega$ be a n-ary operation. Then we have:

$$\begin{aligned}
\alpha(f(a_1, \dots, a_n)) &= ([f(a_1, \dots, a_n)]_\zeta, [f(a_1, \dots, a_n)]) \\
&= (f([a_1]_\zeta, \dots, [a_n]_\zeta), f([a_1]_{\zeta^*}, \dots, [a_n]_{\zeta^*}) \\
&= f((([a_1]_\zeta, [a_1]_{\zeta^*}), \dots, [a_n]_\zeta, [a_n]_{\zeta^*})) \\
&= f(\alpha(a_1), \dots, \alpha(a_n))
\end{aligned}$$

□

Example 7.7.

Let $\underline{L} = (L; \wedge, \vee)$ be the lattice given by the Hasse diagram



Statement: $\varrho = \{(0,0), (a,a), (b,b), (1,1), (b,1), (1,b), (0,a), (a,0)\}$ is a factor congruences

Proof. Put $\varrho^* = \{(0,0), (a,a), (b,b), (1,1), (b,0), (0,b), (1,a), (a,1)\}$

1) $\varrho \wedge \varrho^* = \{(0,0), (a,a), (b,b), (1,1)\} = \Delta$

3) $\varrho \circ \varrho^* = \varrho \cup \varrho^* \cup T$ (transitive pairs)

$(a,0) \in \varrho, (0,b) \in \varrho^* \Rightarrow (a,b) \in \varrho \circ \varrho^*$

similar:

$(b,a) \in \varrho \circ \varrho^*$

$(0,a) \in \varrho \; (a,1) \in \varrho^* \Rightarrow (0,1) \in \varrho \circ \varrho^*$

similar $(1,0) \in \varrho \circ \varrho^*$

$\Rightarrow \varsigma \circ \varsigma^* \in \nabla$

and similar by $\varsigma^* \circ \varsigma = \nabla$

Therefore $\varsigma \circ \varsigma^* = \varsigma^* \circ \varsigma$.

2) $\varsigma \vee \varsigma^* = \nabla$

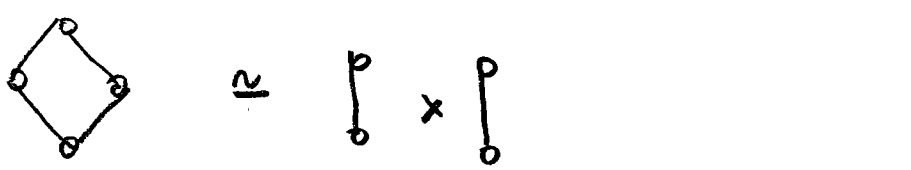
$\mathrm{L}/\varsigma =$ 

where $[1]_\varsigma = \{1, b\}$ $[0]_\varsigma = \{0, a\}$

$\mathrm{L}/\varsigma^* =$ 

where $[1]_{\varsigma^*} = \{1, a\}$ - $[0]_{\varsigma^*} = \{0, b\}$

$\mathrm{L} \cong \mathrm{L}/\varsigma \times \mathrm{L}/\varsigma^*$



□

The generalization of many factors:

Def. 7.8 Let $\{A_i \mid i \in I\}$ be a family of non-empty sets. The cartecian product $\prod_{i \in I} A_i$ is the set of all functions

$f: I \longrightarrow \bigcup_{i \in I} A_i$ with $f(i) \in A_i$ for all $i \in I$

Motivation:

$A_1 = \{a_1, a_2\}$, $A_2 = \{b_1, b_2\}$, $I = \{1,2\}$

$f_{ij}: I \longrightarrow A_1 \cup A_2$

f_{11} , f_{12} , f_{21} , f_{22} with

$f_{11}(1) = a_1 \quad f_{11}(2) = b_1 \qquad f_{11} \longleftrightarrow (a_1, b_1)$

$f_{12}(1) = a_1 \quad f_{12}(2) = b_2$

$f_{21}(1) = a_2 \quad f_{21}(2) = b_1$

$f_{22}(1) = a_2 \quad f_{22}(2) = b_2$

Def. 7.9 Let $\{A_i \mid i \in I\}$ be a family of algebras of the same type. The direct product $\prod_{i \in I} \underset{\sim}{A}_i$ is the algebra $\underset{\sim}{A}$

$\underset{\sim}{A} = (\prod_{i \in I} A_i ; \Omega)$ where the operations are defined componentwise

Let f be an n-ary operation of Ω

$f(a_1, \dots, a_n)(i) := f(a_1(i), \dots, a_n(i))$

The projections $e_j : A \to A_j$ with $e_j(a) = a(j)$ are surjective homomorphisms

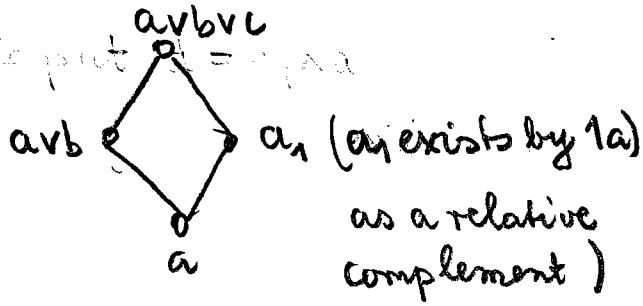
Def. 7.10 An algebra $\underset{\sim}{A}$ is called directly indecomposable if $\underset{\sim}{A}$ is not isomorphic to a direct product $\underset{\sim}{A}_1 \times \underset{\sim}{A}_2$ with $|A_1| \neq 1$ and $|A_2| \neq 1$

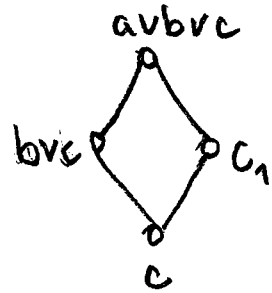
Example 7.11 Every finite algebra $\underset{\sim}{A}$ with $|A| = p$, p a prime number, is directly indecomposable.

Thm 7.12 Every finite algebra $\underset{\sim}{A}$ is either directly indecomposable or isomorphic to a direct product of directly indecomposable algebras

We consider $(a,c) \in \varrho_1 \circ \varrho_2$ where at exists

$(a,b) \in \varrho_1$ and $(b,c) \in \varrho_2$





Put $d := a_1 \wedge c_1$. Then we have

$(b,c) \in \varrho_2 \;,\; (a,a) \in \varrho_2 \Rightarrow (avb, avc) \in \varrho_2$

$(b,b) \in \varrho_2 \Rightarrow (avbvb, avcvb) \in \varrho_2$

$(a_1,a_2) \in \varrho_2 \Rightarrow ((avb)\wedge a_1, (avbvc)\wedge a_2) \in \varrho_2$

We have $(a,a_1) \in \varrho_2$

In the same way we have $(c_1,c) \in \varrho_1$

$(a,b) \in \varrho_1 \Rightarrow (a, avb) \in \varrho_1 \Rightarrow (ava_1, avbvc) \in \varrho_1$

From $(a_1, avbvc) \in \varrho_1$ and $(a_1 \vee c_1, avbvc) \in \varrho_1$

it follows by the transitivity

$(a_1 \vee c_1, a_1) \in \varrho_1 \Rightarrow ((a_1 \vee c_1)\wedge c_1, a_1 \wedge c_1) \in \varrho_1$

also $(c_1,d) \in \varrho_1$

In the same way we have $(a,d) \in \varrho_2$

and $(a,c) \in \varrho_2 \circ \varrho_1$. It holds $\varrho_1 \circ \varrho_2 \subseteq \varrho_2 \circ \varrho_1$

In the same way $\varrho_2 \circ \varrho_1 \subseteq \varrho_1 \circ \varrho_2$

Example 7.13 Every finite Boolean algebra $\underline{B} = (B; \wedge, \vee, ', 0, 1)$ is isomorphic to a direct product of the two-element Boolean algebra $\underline{B}_2 = (\{0,1\}; \wedge, \vee, ', 0, 1)$

Step 1: Every non-trivial congruence of $\underline{B}$ is a **factor-congruence**

Step 2: Only $\underline{B}_2$ is directly incomposable.

The statement follows from the steps 1 and 2

Step 1

1a) Let $u \leq t \leq v$ be
(it is $u \leq t$ iff $u \wedge t = u$)
Then there exist relative complement s
with $t \wedge s = u$ and $t \vee s = v$

Put $s = u \vee (t' \wedge v)$ then it holds

$$t \wedge s = t \wedge (u \vee (t' \wedge v))$$
$$= (t \wedge u) \vee (t \wedge t' \wedge v')$$
$$= u \vee 0 = u \text{ and}$$
$$t \vee s = t \vee u \vee (t' \wedge v) =$$
$$= t \vee (t' \wedge v)$$
$$= (t \vee t') \wedge (t \vee v) = 1 \wedge v = v$$

1b) $\varrho_1 \circ \varrho_2 = \varrho_2 \circ \varrho_1$ for all congruences ϱ_1, ϱ_2

Step 2 : Statement:

A Boolean algebra $\underset{\sim}{B}$ is exactly indecomposable if $|\underset{\sim}{B}| = 2$ i.e $B = \{0,1\}$

Proof. If B has more then two elements then there exists an element d with $0 < d < 1$

We define a congruence by

$$(a,b) \in \zeta \Leftrightarrow a \wedge d = b \wedge d$$

1) ζ is an equivalence relation because " = "

2) ζ is compatible by the operations $\wedge, \vee, '$

Let $(a,b) \in \zeta$, $(c,e) \in \zeta$. Then $a \wedge d = b \wedge d$

$c \wedge d = e \wedge d$ and $a \wedge c \wedge d = b \wedge e \wedge d$

therefore $(a \wedge c, b \wedge e) \in \zeta$

Consider $(a \vee c) \wedge d = (a \wedge d) \vee (c \wedge d)$

$= (b \wedge d) \vee (e \wedge d) = (b \vee e) \wedge d$. Also $(a \vee c, b \vee e) \in \zeta$

From $(a,b) \in \zeta$ it follows $a \wedge d = b \wedge d$

and $(a \wedge d)' = (b \wedge d)' \Rightarrow a' \vee d' = b' \vee d'$

also $a' \leq b' \vee d' \Rightarrow a' \wedge d \leq (b' \vee d') \wedge d$

$a' \wedge d \leq (b' \wedge d) \vee (d' \wedge d) \Rightarrow a' \wedge d \leq b' \wedge d$

Similarly $a' \wedge d \geq b' \wedge d$, also $(a', b') \in \zeta$

3) ς is factor congruence

because there exists a ς^* namely

$(h,k) \in \varsigma^* \iff h \wedge d' = k \wedge d'$

It holds $\varsigma \circ \varsigma^* = \varsigma^* \circ \varsigma$ as we have shown.

$\varsigma \wedge \varsigma^* = \Delta$ because from $(a,b) \in \varsigma \wedge \varsigma^*$

$a \wedge d = b \wedge d$ and $a \wedge d' = b \wedge d'$

$\Rightarrow (a \wedge d) \vee (a \wedge d') = (b \wedge d) \vee (b \wedge d')$

$\Rightarrow a \wedge (d \vee d') = b \wedge (d \vee d') \Rightarrow$

$a = b$

$\varsigma \vee \varsigma^* = \nabla$ because $(0,d') \in \varsigma$ then

$0 \wedge d = d' \wedge d$ and $(d',1) \in \varsigma^*$

$d' \wedge d' = 1 \wedge d'$. It follows $(0,1) \in \varsigma \vee \varsigma^*$

We have $(0,1) \in \varsigma \vee \varsigma^*$ and $(a,a) \in \varsigma \vee \varsigma^*$

$\Rightarrow (0,a) \in \varsigma \vee \varsigma^*$

Similarly $(0,b) \in \varsigma \vee \varsigma^*$. Therefore $(a,b) \in \varsigma \vee \varsigma^*$

$\Rightarrow \varsigma \vee \varsigma^* = \nabla$.

We have the results:

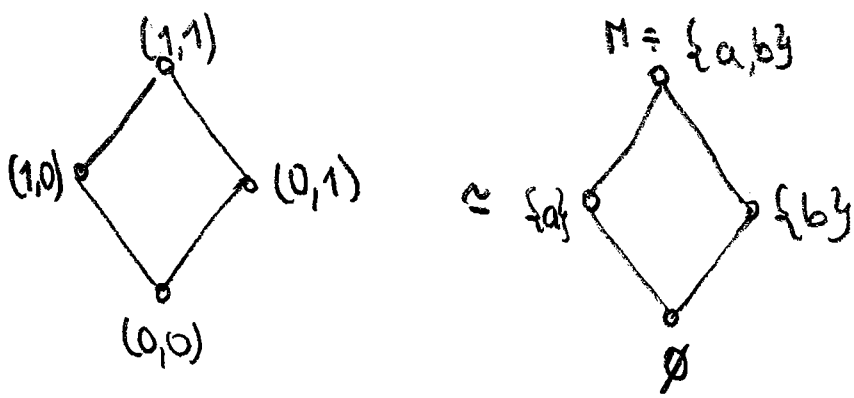
7.14 Every finite Boolean algebra $\underset{\sim}{B}$ is isomorphic to a direct product of the Boolean algebra $\underset{\sim}{B}_2 = (\{0,1\}; \wedge, \vee, ', 0, 1)$

7.15 Every finite Boolean algebra is isomorphic to $(\{0,1\}^n; \wedge, \vee, ', 0, 1)$ for some $n \in \mathbb{N}$

7.16 A finite Boolean algebra has 2^n elements for some $n \in \mathbb{N}$

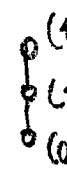
7.17 Every finite Boolean algebra $\underset{\sim}{B}$ is isomorphic to a power order algebra $(P(M); \cap, \cup, ', \emptyset, M)$

Illustration



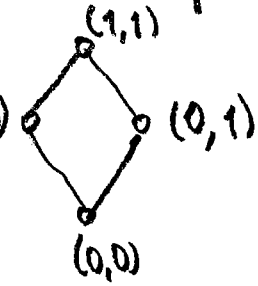
7 B Subdirect products

Def. 7.18 Let $\{\underset{\sim}{A}_i \mid i \in I\}$ be a family of algebras of the same type. Let $\underset{\sim}{A}$ be a subalgebra of the direct product $\prod_{i \in I} \underset{\sim}{A}_i$. The algebra $\underset{\sim}{A}$ is a subdirect product of the algebras $\underset{\sim}{A}_i$, $i \in I$, if all projections e_i, $i \in I$, are surjective (i.e $e_i(A) = A_i$)

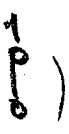
Example The lattice $L = (\;$  $;\wedge,\vee)$ is a subdirect product of

$L_1 = (\;$  $;\wedge,\vee)$ and $L_2 = (\;$  $;\wedge,\vee)$

1) L is a sublattice of

$L_1 \times L_2 =$ 

2) The projections are surjective

$e_1($  $) =$ and $e_2($  $) =$

Lemma 7.19 Let $\underset{\sim}{A} = (A; \Omega)$ be an algebra and let $\{\theta_i \mid i \in I\}$ be the set of all congruences of $\underset{\sim}{A}$ without of Δ. If $\bigwedge \{\theta_i \mid i \in I\} = \Delta$ then $\underset{\sim}{A}$ is isomorphic to a subdirect product of algebras $\{\underset{\sim}{A}/\theta_i \mid i \in I\}$

Proof. For every element $a \in A$ we define an element $f_a \in \prod_{i \in I} A/\theta_i$ in the following way

$$f_a(i) = [a]_{\theta_i}$$

We consider the subset $A' = \{f_a \mid a \in A\} \subseteq \prod_{i \in I} A/\theta_i$

We have to show 1) $\underset{\sim}{A'}$ is a subalgebra of $\prod_{i \in I} \underset{\sim}{A}/\theta_i$

2) $\underset{\sim}{A'}$ is isomorphic to $\underset{\sim}{A}$

1) Let $\omega \in \Omega$ be a n-ary operation
We consider $\omega(f_{a_1}, \dots, f_{a_n})$ in the place i

$$\omega(f_{a_1} \dots f_{a_n})(i) = \omega(f_{a_1}(i), \dots, f_{a_n}(i))$$
$$= f_{\omega(a_1, \dots, a_n)}(i)$$

Now $f_{\omega(a_1, \dots, a_n)}(i) \in A'$ beause $\omega(a_1, \dots, a_n) \in A$

2) $\varphi : A \to A'$ defined by $\varphi(a) = f_a$ is an isomorphism

a) φ is surjective by definition of f_a

b) φ is injective

Let $f_a \neq f_b \Rightarrow f_a(i) = f_b(i)$ for all $i \in I$

$\Rightarrow [a]_{\theta_i} = [b]_{\theta_i}$ for all $i \in I$

$\Rightarrow (a,b) \in \theta_i$ for all $i \in I$

$\Rightarrow (a,b) \in \bigwedge_{i \in I} \theta_i = \Delta \Rightarrow a = b$

c) φ is homomorphism if you check that !

Remark The lemma 7.19 holds also the other direction !

Def. 7.20 Let $\underset{\sim}{A}$ be an algebra with the set $\{\theta_j \mid j \in J\}$ of congruences of $\underset{\sim}{A}$

$\underset{\sim}{A}$ is subdirectly indecomposable = irreducible if for every subset $I \subseteq J$ it holds

If $\bigwedge_{i \in I} \theta_i = \Delta$ then there exists a $i \in I$ with $\theta_i = \Delta$

Illustration. If $\underset{\sim}{A}$ is an algebra with congruence lattice

then $\underset{\sim}{A}$ is subdirectly irreducible

Examples 1) Every simple algebra is subdirectly irreducible (has only ∇ and Δ as congruences)
$(\{0,1\}; \wedge, \vee, ', 0, 1)$ is simple, simple groups and so on

2) The congruence lattice of the symmetric group S_n for $n \geq 5$ is the following:

corresponds to normal group A_n (alternative group)

Thm 7.21 (G. Birkhoff) ~(1938):

Every algebra $\underset{\sim}{A} = (A, R)$ with $|A| > 1$ is isomorphic to subdirect product of subdirectly irreducible algebras

Proof. Let $a, b \in \Delta$ $(a \neq b)$. We consider the maximal congruence θ_{ab} with the property $(a,b) \notin \theta_{ab}$

1) The congruence θ_{ab} exists because:

Let $P = \{\varphi \mid (a,b) \notin \varphi$, φ congruence of $\underline{A}\}$

P is not-empty because $\Delta \in P$ if $(a,b) \notin \Delta$

P is a poset because P is a subset of congruence lattice

Let C be a chain in P and let $\Psi = \bigcup_{\varphi \in C} \varphi$

$(a,b) \in \Psi$ if and only if there exists a $\varphi \in C$ with $(a,b) \in \varphi$. We conclude that $(a,b) \notin \Psi$

Also $\Psi \in P$ and P is inductive ordered

By the Lemma of Zorn P has maximal elements

θ_{ab} is such one

2) It holds $\bigwedge \{\theta_{ab} \mid a,b \in A, a \neq b\} = \Delta$

If we assume that $\bigwedge \{\theta_{ab}\} \neq \Delta$ with $c \neq d$ and $(c,d) \in \bigwedge \{\theta_{ab}\}$ we have $(c,d) \in \theta_{cd}$. Contradiction

3) $\underline{A}/\theta_{ab}$ is subdirectly irreducible

Let Ψ the smallest congruence $\neq \Delta$ with $(a,b) \in \Psi$ and let θ be a congruence $\neq \Delta$ of A/θ_{ab}. Then $\theta \geq \theta_{ab}$ and $\theta \geq \Psi$

It follows that Ψ is the smallest non-trivial congruence in A/θ_{ab} □

Remark. This theorem is equivalent to the axiom of choice!

§8 Theorem of Birkhoff

8A Varieties

We make a difference of classes and sets to avoid the difficulties of set-of-sets.
We introduce operators of classes of algebras

Def. 8.1 Let K be a class of algebras of the same type.

$\underset{\sim}{A} \in I(K)$ iff $\underset{\sim}{A}$ is isomorphic to some member of K

$\underset{\sim}{A} \in S(K)$ iff $\underset{\sim}{A}$ is a subalgebra of some member of K

$\underset{\sim}{A} \in H(K)$ iff $\underset{\sim}{A}$ is a homomorphic image of some member of K

$\underset{\sim}{A} \in P(K)$ iff $\underset{\sim}{A}$ is a direct product of a non-empty family of algebras in K

$\underset{\sim}{A} \in P_s(K)$ iff $\underset{\sim}{A}$ is a subdirect product of a non-empty family of algebras in K

Example. The class of all abelian groups is closed under the operators S, H and P

Def. 8.2 A class K of algebras of a type τ is called a variety if $P(K) \subseteq K$, $S(K) \subseteq K$ and $P(K) \subseteq K$

Remark. H, S, P generate a semigroup of class operators of a given type.
A description can be found in the paper of [Pigozzi]

Lemma 8.3 The following inequalities holds

$$SH \subseteq HS \,, \quad PS \subseteq SP \,, \quad PH \subseteq HP$$

The operators S, H and P are idempotent (that means $SS = S$, $HH = H$ and $PP = P$

Proof. Suppose $\underset{\sim}{A} \in SH$. Then for some algebra $\underset{\sim}{B} \in K$ and onto homomorphism $\alpha : \underset{\sim}{B} \longrightarrow \underset{\sim}{C}$

we have $\underset{\sim}{A} \leq \underset{\sim}{C}$

(that means $\underset{\sim}{A}$ is a subalgebra of $\underset{\sim}{C}$: $\underset{\sim}{A} \leq \underset{\sim}{C}$)

Thus $\alpha^{-1}(\underset{\sim}{A}) \leq \underset{\sim}{B}$ and as $\alpha(\alpha^{-1}(\underset{\sim}{A}) = \underset{\sim}{A}$

we have $A \in HS(K)$.

The other statements are an exercise (Stan Burris, Sanka A Course in Universal Algebra page 61)

Examples for varieties

1) The class of all groups is a variety

because it is closed under subgroups,

homomorphic images and direct products

of groups

Abelian groups, nilpotent groups, solvable

groups; and so on

2) The class of all distributive lattices is a variety

because: a sublattice of a distributive lattice

is again distributive

a homomorphism image is again distributive

a direct product of distributive lattice is again distributive

3) and so

Def. 8.4 Let $V(K)$ be denote the smallest variety containing K. We say that $V(K)$ is the variety generated by K.

Thm. 8.5 $V = HSP$

(that means: If $H(V) \subseteq V$, $S(V) \subseteq V$, $P(V) \subseteq V$ then $HSP(V) \subseteq V$)

(without proof)

Thm 8.6 If K is a variety then every member of K is isomorphic to a subdirect product of subdirectly irreducible member of K

§8 Free algebras

Remark. In some class K there may exist a free algebra $F_K(X)$ such that all other algebras with $|X|$ generators are homomorphic images of $F_K(X)$. In a certain sense $F_K(X)$ is the most general algebra in K and the other algebras are special cases of $F_K(X)$

In order to stress the general nature of the free algebra one denotes the generating elements like variables by $x_1, x_2, x_3, \ldots$

Def 8.7: Let K be a class of algebras of type τ and let $F_K(X) \in K$ be an algebra generated by $X = \{x_i \mid i \in I\}$. $F_K(X)$ is called a free algebra with the generating system X in the

8.7

in the class K if for every algebra $\underset{\sim}{A} \in K$ and every map $\psi : I \longrightarrow A$ there exists a homomorphism $\varphi : F_K(X) \longrightarrow A$ with $\varphi(x_i) = \psi(i)$

Remarks 8.8

8.8.1 The homomorphism φ is unique

8.8.2 In the the case $X = \{x_1, \ldots, x_n\}$ we will write $F_K(n)$

8.8.3 If $|X| = |Y|$ then $F_K(X) \cong F_K(Y)$.

8.9 Construction of the free algebra $F_K(X)$

(i) Every variable $x \in X$ and every nullary operation symbol are terms

(ii) If $t_1, \ldots, t_n$ are terms and f_σ is an n-ary operation symbol then $f_\sigma(t_1, \ldots, t_n)$ is a term

We allow only finitary application of (ii) and denote the set of terms by $T(X)$.

We introduce operations on set in the following way.

If f_σ is an n-ary operation and $t_1, \dots, t_n$ are terms then $f_\sigma(t_1, \dots, t_n) := f_\sigma(t_1, \dots, t_n)$

$\underset{\sim}{T}(X) = (T(X), \Omega)$ is called term algebra.

Now we consider the class $\Delta(K)$ of all homomorphism δ of $\underset{\sim}{T}(X)$ into the algebras of the class K. We define the following congruence θ on $T(X)$

$(t_1, t_2) \in \theta$ if and only if $\delta(w_1) = \delta(w_2)$ for every $\delta \in \Delta(K)$

It is obvious that $\theta = \bigcap_{\delta \in \Delta(K)} \ker \delta$

We will show that $F_K(X) := T(X)/\theta$ is the free algebra.

Definition 8.10 A class K of algebras is called non-trivial if K contains an algebra with more than one element.

Theorem 8.11: If K is non trivial and $T(X)/_\theta \in K$ then $F_K(X) = T(X)/_\theta$ is the free algebra of K with the generating system X

Proof. Let $\underset{\sim}{A} \in K$ and let $\varphi: I \longrightarrow A$. We consider $\bar{\varphi}: X \longrightarrow A$ with $\bar{\varphi}(x_i) := \varphi(i)$ and define recursively $\underset{\sim}{\varphi}: T(X) \longrightarrow \underset{\sim}{A}$ by $\underset{\sim}{\varphi}(x_i) = \bar{\varphi}(x_i)$ and for $t_1, \ldots, t_n \in T(X)$ and $\underset{\sim}{\varphi}(t_1) = a_1, \ldots \underset{\sim}{\varphi}(t_n) = a_n$ by $\underset{\sim}{\varphi}(f_r(t_1, \ldots, t_n)) := f_r(\varphi(t_1), \ldots, \varphi(t_n))$
Obviously $\underset{\sim}{\varphi}$ is a homomorphism.
We consider the diagram

$$\begin{array}{ccc} T(X) & \xrightarrow{\underset{\sim}{\varphi}} & A \\ & \searrow & \uparrow \alpha \\ & & T(X)/_\theta \end{array}$$

with $\alpha([t]_\theta) := \underset{\sim}{\varphi}(t)$. α is well defined and a homomorphism.

Theorem 8.12 If K is a non-trivial variety then the free algebra $F_K(X)$ exists in K

Proof. We have to show that $I(X)/\theta \in K$

Because $\theta = \bigcap_{\delta \in \Delta(K)} \ker \delta$ for the class $\Delta(K)$ one can find a set M of congruence relation of $I(X)$ such that $\theta = \bigcap_{\delta \in M} \ker \delta$. By Birkhoff's theorem (7.21) the free algebra $I(X)/\theta$ is isomorphic to a subdirect product of algebras $I(X)/\ker\delta$. According to the homomorphism theorem (8.11) $I(X)/\ker\delta$ is isomorphic to an algebra of K.

As K is closed under homomorphic images and subdirect product the free algebra $I(X)/\theta \in K$.

Definition 8.13 An algebra $\underset{\sim}{A}$ is locally finite if every finitely generated subalgebra is finite. A variety V is locally finite if every algebra $\underset{\sim}{A}$ of V is locally finite.

Theorem 8.14 A variety V is locally finite if and only if $F_K(X)$ is finite for a finite generating set X

Proof. Let G be a finite set of generators of the algebra $\underset{\sim}{A}$. We choose X in such a way that $\varphi : X \to A$ is a bijection. We extend φ to $\underset{\sim}{\varphi} : F(X) \to A$. $\underset{\sim}{\varphi}[F(X)]$ is a subalgebra of $\underset{\sim}{A}$ containing. Hence we have $\underset{\sim}{\varphi}[F(X)] = A$. If $F(X)$ is finite then A is finite. Hence V is locally finite.

Burris

Theorem 8.15 Let K be a finite set of finite algebras. Then $V(K)$ is a locally finite algebra.

8C Birkhoff's theorem

Definition 8.16 An identity (of type τ) over X is a pair (t,s) of terms $t, s \in T(X)$

We write $t = s$

or $t(x_1,\dots,x_n) = s(x_1,\dots,x_n)$

An identity $t=s$ is true in an algebra $\underset{\sim}{A}$ if for every choice of $a_1,\dots,a_n \in A$ we have $t(a_1,\dots,a_n) = s(a_1,\dots,a_n)$

We write $A \models (t(x_1,\dots,x_n) = s(x_1,\dots,x_n))$

A class K of algebras of type τ satisfies an identity if the identity is true for every algebra $\underset{\sim}{A} \in K$

We write $K \models (t = s)$

Example. Let V be the variety of lattices.
Consider $t(x,y) := x$ and $s(x,y) := x \wedge (y \vee x)$
Then $t(x,y) = s(x,y)$ is satisfied in V

Proposition 8.17 Let K be a class of algebras of type τ and Σ be a set of identities. If $K \models \Sigma$ then $H(K) \models \Sigma$, $S(K) \models \Sigma$ and $P(K) \models \Sigma$ (i.e. $HSP(K) \models \Sigma$)

Proof. Obvious.

Lemma 8.18 Let K be a class of algebras of type τ $K \models (t=s)$ if and only if $F_K(X) \models (t=s)$

Proof. If $F_K(X) \models (t=s)$ then any homomorphic image $\underset{\sim}{A} \models (t=s)$ and hence $K \models (t=s)$

If $K \models (t=s)$ then every algebra $\underset{\sim}{A} \in HSP(K)$ satisfies $(t=s)$. As $F_K(X) \in HSP(K)$ then $F_K(X) \models t=s$

Notation 8.19 Let Σ be a set of identities of type τ. Let $M(\Sigma)$ be the class of all algebras of type τ which satisfy Σ.

$M(\Sigma)$ is a variety because of 5.11

$Id(X)$ is the set of all identities of [illegible]

$Id_K(X) := \{ s=t \mid K \models (s=t),\ s,t \in T(X) \}$
is the set of all identities of type τ which hold for K

Lemma 8.20: If V is a variety and X an infinite set of variables then $V = M(Id_V(X))$

Proof. Clearly $V \supseteq M(Id_V(X))$. Now let $F_V(X)$ be the free algebra of V with infinitely many variables. Let $F_V(X) \models (s=t)$. Then $(s=t) \in Id_V(X)$ and $F_V(X) \in M(Id_V(X))$

Hence $V \subseteq M(Id_V(X))$

(Birkhoff)

Theorem 8.21: K is variety if and only if there exists a set Σ of identities such that $K = M(\Sigma)$

Proof. If $K = M(\Sigma)$ then K is a variety because of

If K is variety then consider $\Sigma = Id_K(X)$ for X with infinitely many variables. By
$K = M(Id_K(X)) = M(\Sigma)$.

Summary 8.22

K is closed under homomorphic
- images $H(K) \subseteq K$
- sub-algebras $S(K) \subseteq K$
- direct products $P(K) \subseteq K$

$\Leftrightarrow$ $K \models (t = s)$ defined by identities

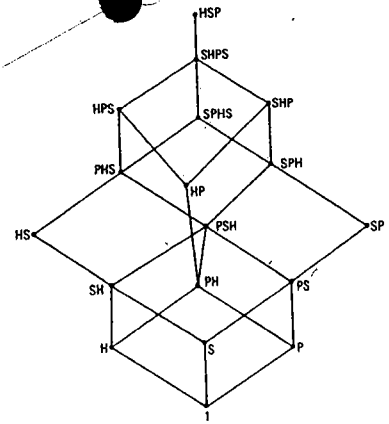
variety

Tool: Free algebras

Example

- A homomorphic image of a distributive lattice is again distributive
- A sub-lattice of a distributive lattice is again distributive $\Leftrightarrow$ $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge$
- A direct product of distributive lattices is again distributive

Chapter 8



Partial order of $\mathfrak{H}$ and $\mathfrak{S}$

COROLLARY 4 (A. Tarski [1946]). *Let* K *be a class of lattices. Then* HSP(K) *is the smallest equational class containing* K.

PROOF. We start out by observing three formulas for any class K of lattices:
(i) $\mathbf{SH}(\mathbf{K}) \subseteq \mathbf{HS}(\mathbf{K})$.
(ii) $\mathbf{PH}(\mathbf{K}) \subseteq \mathbf{HP}(\mathbf{K})$.
(iii) $\mathbf{PS}(\mathbf{K}) \subseteq \mathbf{SP}(\mathbf{K})$.

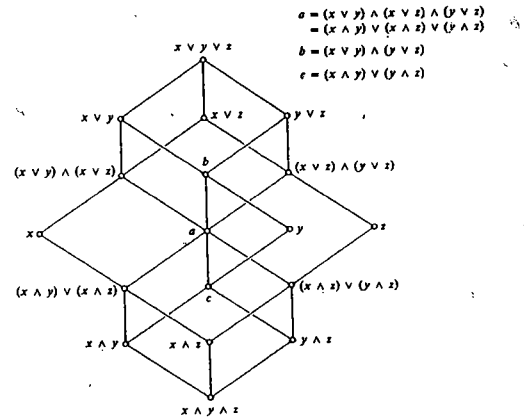
To prove (i), let $L \in \mathbf{SH}(\mathbf{K})$. Then there is an $A \in \mathbf{K}$ and a homomorphism α of A onto a lattice B containing L as a sublattice. Set $C = \{x \mid x \in A \text{ and } x\alpha \in L\}$. Then $C \in \mathbf{S}(\mathbf{K})$ and $L \in \mathbf{H}(C)$. Hence $L \in \mathbf{HS}(\mathbf{K})$, proving (i).

To prove (ii), let $L \in \mathbf{PH}(\mathbf{K})$. Then there exist $A_i \in \mathbf{K}$ and a homomorphism α_i of A_i onto B_i, for $i \in I$, such that $L = \Pi(B_i \mid i \in I)$. It is clear that L is a homomorphi[illegible] of $\Pi(A_i \mid i \in I) \in \mathbf{P}(\mathbf{K})$, proving (ii).

[illegible] of (iii) follows that of (ii) with A_i a sublattice of B_i.

[illegible] $\mathbf{SP}(\mathbf{K}) = \mathbf{K}_1$ is an equational class using Theorem 3, we have to [illegible] $\mathbf{Q}(\mathbf{K}_1) \subseteq \mathbf{K}_1$, and $\mathbf{P}(\mathbf{K}_1) \subseteq \mathbf{K}_1$. Indeed (using (i)–(iii) and that [illegible] and any class $\mathbf{K}_2$):

THEOREM 10. *A free distributive lattice on three generators,* $F_D(3)$, *has eighteen elements* (see Figure 6).



THEOREM 11. (R. Dedekind [1900]). *A free modular lattice on three generators,* $F_M(3)$, *has twenty-eight elements* (see Figure 7).

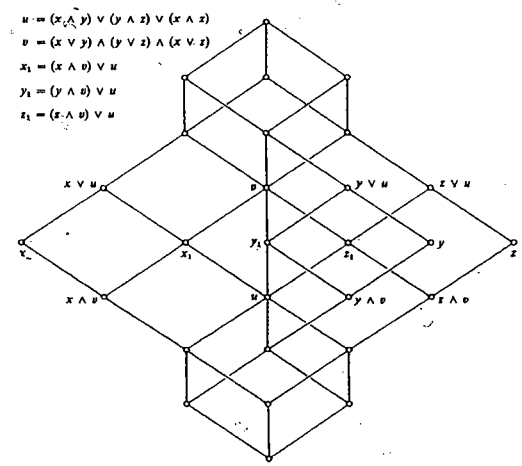
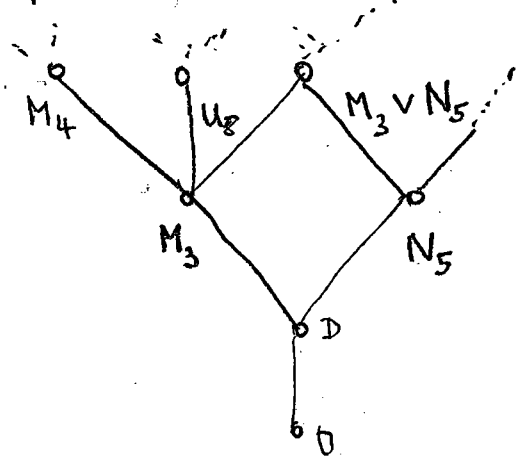


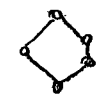
Figure 7

Don Pigozzi Algebra Universalis 2 346-353 (1972)

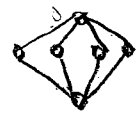
The lower part of the lattice of all subvarieties of lattices

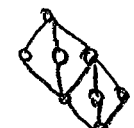


D is the variety of distributive lattices generated by [illegible]

N_5 is generated by 

M_3 is generated by 

M_4 is generated by 

U_8 is generated by 

§9 Mal'cev Type Theorems

9A Mal'cev type theorems

Thm 9.1 (A.I. Mal'cev) (Anatoliĭ Ivanovich)

A variety K is congruence-permutable

if and only if there is a term $t = t(x,y,z)$

such that the following identities holds

$$x = t(x,z,z)$$

$$z = t(x,x,z)$$

Proof. Let K be congruence-permutable and

let $F(3)$ be the free algebra with the generating

system $X = \{x,y,z\}$ in the class K

Let $\theta(a,b)$ be the smallest congruence

which contains a and b.

In $F(3)$ we have $x = z\,(\theta(x,y) \circ \theta(y,z))$

Because the congruence-permutable

we have $x = z\,(\theta(y,z) \circ \theta(x,y))$

Therefore there an element $t \in F(3)$

with $x = t(\theta(y,z)$ and $t = z\,(\theta(x,y))$

Now we have

$$F(3)/\theta(x,y) \cong F(3)/\theta(y,z) \cong F(2)$$

Therefore it holds $x = t(x,z,z)$ and $z = t(x,x,z)$ in $F(3)$

On the other hand let A be an algebra

$\theta, \varphi \in \operatorname{Con} \underset{\sim}{A}$, $a,b,c \in A$ and $a = b \bmod \theta$ and $b = c \bmod \varphi$

It holds $a = t(a,b,b) = t(a,b,c) \bmod \varphi$ because $t(x,y,z)$ is a term and terms are compatible with congruences.

It is $t(a,b,c) = t(a,a,c) \bmod \theta$ and $t(a,a,c) = c$

Therefore $a = t(a,b,c) \bmod \varphi$ and $t(a,b,c) = c \bmod \theta$

Therefore $\theta \circ \varphi = \varphi \circ \theta$ □

Examples 9.2 Congruence-permutable varieties

9.2.1 Groups

$$t(x,y,z) = x \cdot y^{-1} \cdot z \qquad (t(x,z,z) = x,\ t(x,x,z) = z)$$

9.2.2 Rings

$$t(x,y,z) = x - y + z$$

9.2.3 Boolean Algebras

$$t(x,y,z) = [(x \wedge y') \vee z] \wedge (x \vee y')$$

$$t(x,x,z) = [(x \wedge x') \vee z] \wedge (x \vee x') = [0 \vee z] \wedge 1 = z$$

$$t(x,z,z) = [(x \wedge z') \vee z] \wedge (x \vee z')$$
$$= (x \vee z) \wedge (z' \vee z) \wedge (x \vee z')$$
$$= (x \vee z) \wedge (x \vee z')$$
$$= x \vee (z \wedge z') = x$$

Def 9.3 A variety is arithmetical if it is congruence-distributive and congruence-permutable

Thm 9.4 (A.F. Pixley)

A variety V is arithmetical if and only if there is a term $p = p(x,y,z)$ with

$$V \models p(x,y,x) = p(x,y,y) = p(y,y,x) = x$$

Proof. If the variety V is arithmetical then there is a term p as V is congruence permutable. Let $F(3)$ be the free algebra

in V generated by x,y,z

Then as $(x,z) \in \theta(x,z) \wedge [\theta(x,y) \vee \theta(y,z)]$

it follows that

$$(x,z) \in [\theta(x,z) \wedge \theta(x,y)] \vee [\theta(x,z) \vee \theta(y,z)]$$

hence $(x,z) \in [\theta(x,z) \wedge \theta(x,y)] \circ [\theta(x,z) \vee \theta(y,z)]$

Choose a term $p(x,y,z) \in F(3)$ such that

$(x, p(x,y,z)) \in \theta(x,z) \wedge \theta(x,y)$ and $(p(x,y,z), z) \in \theta(x,z) \wedge \theta(y,z)$

By 9.1 $\quad V \models p(x,x,z) = p(x,z,x) = p(y,x,x) = x$

The other direction it follows from the congruence-distributive and congruence-permutable

□

Thm 9.5 B. Jonsson

A variety is congruence-distributive if and only if there exist terms $t_0, \dots, t_n$ for a number $n \geq 2$ in three variables such that it holds for $i = 0, \dots, n-1$

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

$t_n(x,y,z) = z$

$t_i(x,y,x) = x$

$t_i(x,x,z) = t_{i+1}(x,x,z)$ i even

$t_i(x,z,z) = t_{i+1}(x,z,z)$ i odd

Remark. For the variety of lattice we can take $t_0(x,y,z) = x$, $t_1(x,y,z) = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$ $t_2(x,y,z) = z$

A. Day has characterized the congruence-modular varieties. W. Taylor gives an overview in [ ]

* 9B Thm of Baker-Pixley

9.6 Remark. The chinese remaind theorem of the number theory:

Let $a_1, \dots, a_k \in \mathbb{Z}$, $m_1, \dots, m_k \in \mathbb{N}$ be given.

The equality system

$$\begin{aligned} x &= a_1 \mod m_1 \\ &\vdots \\ x &= a_k \mod m_k \end{aligned} \qquad k \text{ equalities}$$

has exactly a solution if every subsystem

$$\left.\begin{aligned} x &= a_i \mod m_i \\ x &= a_j \mod m_j \end{aligned}\right\} \; i \neq j \text{ two equalities}$$

for every $1 \leq i < j \leq k$ has a solution.

9.7 General version

An algebra $\underset{\sim}{A}$ fulfills the chinese remainder theorem for d if it holds

Every system $x = a_1 \mod \theta_1$

$\vdots$

$x = a_k \mod \theta_k$

has exactly a solution if every subsystem of d equalities has a solution

Remark: In number theory we have $d=2$

Thm 9.8 For every variety V and a number $d \geq 2$ the following conditions are equivalent

1) Every algebra of V satisfies the chinese remainder theorem

2) If the algebra $\underset{\sim}{A}$ is given as subalgebra of a direct product $B = C_1 \times \dots \times C_k$, $k \geq d$ then the algebra A is already determined by the d-placed projetions $e_{i_1}(A) \times \dots \times e_{i_d}(A)$

for $i_1 \leq \dots \leq i_d$.

Proof. 1) $\Rightarrow$ 2)

Let $\underset{\sim}{A}$ and $\underset{\sim}{B}$ two subalgebras of $C_1 \times \dots \times C_k$

such that $e_{i_1}(A) \times \dots \times e_{i_d}(A) = e_{i_1}(B) \times \dots \times e_{i_d}(B)$

for all d-placed projections

It is enough to show $A \subseteq B$.

Let $a \in A$. For every i, $1 \leq i \leq k$ we can

choose a $b_i \in B$ with $e_i(a) = e_i(b)$

Consider the k congruences

$$x = b_i \bmod \ker e_i$$

and ask a solution in the algebra $\underset{\sim}{B}$

We know that d equalities have a solution b

$$x = b_j \bmod \ker e_j$$

because $e_{j_1}(A) \times \dots \times e_{j_d}(A) = e_{j_1}(B) \times \dots \times e_{j_d}(B)$

All k equalities have a solution b as

the chinese remainder thm holds with d in $\underset{\sim}{B}$

Also we have $e_i(a) = e_i(b)$ for all $i = 1, \dots, k$

and therefore $a = b$ and therefore $a \in B$

2) $\Rightarrow$ 1)

Consider $\varphi: A \longrightarrow A/\theta_1 \times \dots \times A/\theta_k$

a is a solution for the k congruences $x = a_i \bmod \theta_i$

iff $\varphi(a) = ([a_1], \dots, [a_k])$ where $[a_i]$ is

the classes a mod θ_i

We have to show: $([a_1], \dots, [a_k]) \in \varphi(A)$

We know that every d-placed projection

of $([a_1], \dots [a_k])$ contains in the corresponding

d-placed projection of $\varphi(A)$

By $([a_1], \dots [a_k])$ and by $\varphi(A)$ generated

subalgebra it have to be in $\varphi(A)$, because

this is so for every d-placed projections

of 2)

□

Thm 9.9 (Baker - Pixley)

For a variety V and for a number $d \geq 2$ it is equivalent:

1) V has a term $m(x_0, \dots, x_d)$ with
$m(x, \dots, x, y, x, \dots, x) = x$ for every position of a single y
(near unanimity term) $y = $ (lone dissenter)

2) If two subalgebras $\underset{\sim}{A}, \underset{\sim}{B}$ of a direct product $P = C_1 \times \dots \times C_k$ $k \geq d$
and if the d-placed projections of A is equal to the corresponding d-placed projection of B
then $\underset{\sim}{A} = \underset{\sim}{B}$

(without proof)

Thm 9.10 (Baker-Pixley) (the popular version)
Let $\underset{\sim}{A}$ be a finite algebra with a majority term m.
Then for any $n \in \mathbb{N}$, an n-ary operation $f: A^n \to A$ in $\underset{\sim}{A}$ is a term operation if and only if f preserves each subalgebra of A^2

§ 10 Commutator theory and solvable algebras

10A Term condition

Def. 10.1 An algebra $\underset{\sim}{A}$ satisfies the term condition if for $n \in \mathbb{N}$, $n \geq 1$ for all term operations t of $\underset{\sim}{A}$ and for all elements $a, b, c_2, \dots, c_n, d_2, \dots, d_n \in A$ the following implication is satisfied:

$$t(a, c_2, \dots, c_n) = t(a, d_2, \dots, d_n)$$

$$\Longrightarrow t(b, c_2, \dots, c_n) = t(b, d_2, \dots, d_n)$$

An algebra $\underset{\sim}{A}$ is called abelian if it satisfies the term condition.

Examples 10.2

10.2.1 Every abelian group is an abelian algebra

$t(x_1, \dots, x_n) = x_1^{k_1} \cdot \dots \cdot x_n^{k_n}$, $k_1, \dots, k_n \in \mathbb{Z}$

(These terms are normal forms)

Now we have

$a \cdot c_2 \cdot \dots \cdot c_n = a \cdot d_2 \cdot \dots \cdot d_n \Rightarrow c_2 \cdot \dots \cdot c_n = d_2 \cdot \dots \cdot d_n$ by a^{-1}

$\Rightarrow b \cdot c_2 \cdot \dots \cdot c_n = b \cdot d_1 \cdot \dots \cdot d_n$

10.2.2 A rectangular band ist a semigroup which satisfies the identities

$$x_1 \cdot x_2 \cdot x_3 = x_1 \cdot x_3$$

and $x_1 \cdot x_1 = x_1$

Since in a rectangular band we can write

every $x_1 \cdot \dots \cdot x_n = x_1 \cdot x_n$

We can show that term condition is fulfilled

$a \cdot c_2 \cdot \dots \cdot c_n = a \cdot d_2 \cdot \dots d_n \Rightarrow a \cdot c_n = a \cdot d_n$

$\Rightarrow b \cdot a \cdot c_n = b \cdot a \cdot c_n \Rightarrow b \cdot c_n = b \cdot d_n$

$\Rightarrow b \cdot c_2 \cdot \dots \cdot c_n = b \cdot d_2 \cdot \dots \cdot d_n$

10.2.3 Zero-semigroups are semigroups satisfijing $x_1 \cdot x_2 = x_3 \cdot x_4$

10.2.4 Every algebra which has only unary fundamental operations is abelian.
Every term operation is again unary and the terms condition is satisfied.

10.2.5 Every subalgebra of an abelian algebra is abelian and every product is abelian.
(Exercise) (Quasivarieties)

Def. 10.3 Let α, β, δ be congruences of an algebra $\underset{\sim}{A}$
α centralizes β modulo δ (which is denoted by $C(\alpha, \beta, \delta)$) if for every $n > 1$, for every term operation $T_n(\underset{\sim}{A})$ and for every $(a,b) \in \alpha$ $(c_2, d_2) \in \beta, \ldots, (c_n, d_n) \in \beta$ implies

$$t(a, c_2, \ldots, c_n) \overset{\delta}{\equiv} t(a, d_2, \ldots, d_n)$$

$$\Rightarrow t(b, c_2, \ldots, c_n) \overset{\delta}{\equiv} t(b, d_2, \ldots, d_n)$$

(This is a generalization of the term condition)

Def. 10.4 The commutator $[\alpha, \beta]$ is the smallest congruence δ for which $C(\alpha, \beta, \delta)$ holds

Def. 10.5 Let α and β be congruences of an algebra $\mathbb{A}$ with $\alpha \leq \beta$.

1) β is Abelian over α iff $C(\beta, \beta, \alpha)$

2) β is solvable over α iff there exists a finite chain of congruences $\alpha_0 \leq \alpha_1 \leq \dots \leq \alpha_n$ such that $\alpha_0 = \alpha$, $\alpha_n = \beta$ and α_{i+1} is Abelian over α_i for each $i < n$

10 B Solvable groups

This approach of our commutator is abstract and general. Therefore we like to consider the commutator $[,]$ in group theory

An abelian group fulfills the identity

$$x \cdot y = y \cdot x$$

But there are many non-abelian groups like permutation groups, dihedral groups and so on

Def. 10.6 The element $x^{-1}y^{-1}xy$ of a group G is called commutator of x and y. We write

$$[x,y] := x^{-1}y^{-1}x \cdot y$$

Motivation:

$$x \cdot y = y \cdot x \, [x,y]$$

(That means $x \cdot y = y \cdot x \, [x,y] = y \cdot x \, x^{-1}y^{-1}xy = xy$)

(The commutator "measures" how much is such the group far away from being abelian)

Def. 10.7 The subgroup G' of G generated by all commutators $[x,y]$ is called the commutator subgroup or derived group

Thm 10.8 The factor group G/G' is abelian

Proof. In the mapping $G \to G/G'$ let u, v be arbitrary elements of G/G' and suppose $x \to u$, $y \to v$. Then $x^{-1}y^{-1}xy \to u^{-1}v^{-1}uv$

But $x^{-1}y^{-1}xy \in G'$ and therefore $x^{-1}y^{-1}xy \to 1 = u^{-1}v^{-1}uv$

and hence $vu = uv$ and G/G' is abelian

Def. 10.9 A group G is solvable if the sequence $G \subseteq G' \subseteq G'' \subseteq \dots \subseteq G^{(i)}$ where each group $G^{(i)}$ is the derived group, terminates in the identity in finite steps $G^{(e)} = 1$

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	b

$a^2b = ba$

$ba = a^2b$

$b \cdot a^2 = b.aa = a^2ba =$
$= a^2a^2b = ab$

$bab = a^2bb = a^2$

$ba^2b = baab$
$= a^2bab$
$= a^2a^2b^2 = a$

$ba^2 = baa =$
$= a^2ba = a^4b = ab$

$a^2b \cdot a = a^4b = ab$

$a^2ba^2 = a^2ab = b$

$a^2bb = a^2$

$a^2bab = a^2a^2b^2 = a$

$aba = aa^2b = b$

$aba^2 = aab = a^2b$

$ab \cdot ab = aa^2bb$
$= a^3b^2 = e$

Example 10.7

We consider the group of the order 6 generated by $a^3 = e$ and $b^2 = e$ and $ba = a^2b$

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	b

1) The group is not abelian!

2) There is a normal subgroup of order 3

e a a^2

3) G is solvable:

$G \trianglerighteq G' \trianglerighteq e$

Remark 10.8

The dihedral groups are defined by

$$a^n = e \quad , b^2 = e \quad \text{and} \quad ba = a^{-1}b$$

(name: Dieder gruppe (German))

We have only studied by $a^3 = e$, $b^2 = e$ and $ba = a^2b \quad (= a^{-1}b)$

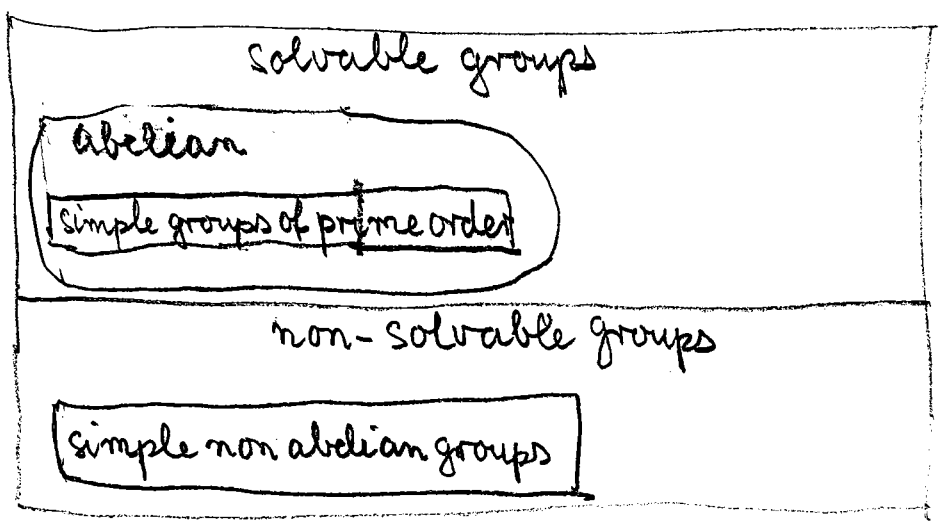
They are built by the symmetries !

Rotation $a = \begin{pmatrix} 1 & 2 & & n-1 & n \\ 2 & 3 & & n & 1 \end{pmatrix}$

Reflection $b = \begin{pmatrix} 1 & 2 & & n-1 & n \\ 1 & n & & 3 & 2 \end{pmatrix}$

Please 3.11

Remark Overview of all finite groups



Historical remark

Galois has shown that a polynomial equation

$$f(x) = 0$$

is solvable by radicals if and only if its Galois group is solvable (1832)

The general equation of the degree 1 till 4 is solvable by radicals

1) $ax + b = 0$ solution $x_1 = \frac{-b}{a}$

2) $ax^2 + bx + c = 0$ solutions $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

3) $ax^3 + bx^2 + cx + d = 0$

4) $ax^4 + bx^3 + cx^2 + dx + e = 0$

} Method of Cardano

Galois (and also Abel) have shown that the (general) polynomial equation in degree $5 \geqslant n$ is not solvable by radicals

10 C Commutator on lattices

Def. 10.9 A tolerance relation on a lattice $(L;\wedge,\vee)$ is reflexive, symmetric binary relation with the operations $\wedge,\vee$

(A transitive tolerance of L is a congruence of L).

Def. 10.10 Let L be a complete lattice. A map $[,]: L\times L \to L$ is called a lattice commutator of L if the following holds

10.10.1 $[a_1 \vee a_2, b] = [a_1, b] \vee [a_2, b]$ for all $a_1, a_2, b \in L$

10.10.2 $[a,b] = [b,a]$ for all $a,b \in L$

10.10.3 $[a,b] \leq a \wedge b$ for all $a,b \in L$

We assume that L is a complete lattice with a least element 0 and a greatest element 1

Remark. In congruence modular varieties the commutator has also these three properties (10.10.1 - 3)

The commutator was introduced by Smith from grouptheory to congruence permutable varieties in universal algebra. Furthermore Hagemann and Hermann extended this concept to congruence modular varieties.

We like to study lattice commutators.

Def 10.11 The map $[,)^i : L \times L \to L$ for $i \in \mathbb{N}$ is defined recursively by

$$[a,b)^1 = [a,b]$$

$$[a,b)^i = [[a,b)^{i-1}, b]$$

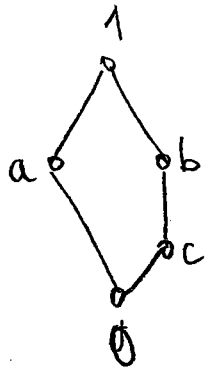
for a given commutator

Def. 10.12 A lattice $\underset{\sim}{L}A$ is nilpotent there is a number $n \in \mathbb{N}$ such that

$$[1,1)^n = 0$$

Example 10.13

We consider the lattice N_5



$[1,1] = [a \vee b, 1] = [a,1] \vee [b,1] \leq (a \wedge 1) = a$
$\leq (b,1)$

$= [a,b] \vee [b,a] \leq a \wedge b = 0$

This lattice is nilpotent because $[1,1]=0$

Characterize all distributive lattices which are nilpotent!

§ 11 Quasi varieties

11A Quasi-identities

Def. 11.1 A quasi-identity $\mathcal{E}$ is an implication of the form

$$(t_0 = s_0) \wedge \dots \wedge (t_{n-1} = s_{n-1}) \to (t_n = s_n)$$

where $t_i = s_i$ are k-ary identities of a given type, for $i = 0, \dots, n$

A quasi-identity $\mathcal{E}$ is satisfied in an algebra $\underset{\sim}{A}$ of a given type if and only if the following implication is satisfied in $\underset{\sim}{A}$:

A given a sequence $a_1, \dots, a_k$
If these elements satisfy the equations $t_i($
$t_i(a_1, \dots, a_k) = s_i(a_1, \dots, a_k)$ in $\underset{\sim}{A}$ for $i = 0, 1, \dots, n-1$
then the equation $t_n(a_1, \dots, a_k) = s_n(a_1, \dots, a_k)$ is satisfied in $\underset{\sim}{A}$

We write $\underset{\sim}{A} \models (t_0 = s_0) \wedge \cdots \wedge (t_{n-1} = s_{n-1}) \Rightarrow (t_n = s_n)$

A quasi-identity ε is satisfied in a class V of algebras of a given type if and only if it is satisfied in all algebras $\underset{\sim}{A}$ belonging to V.

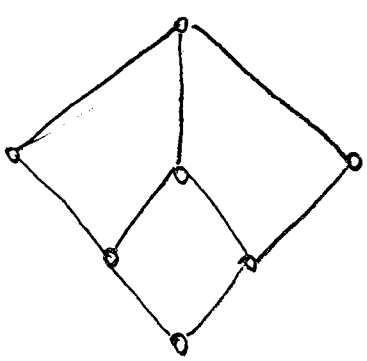
Examples 11.2

11.2.1 An algebra $\underset{\sim}{A}$ is abelian if for every $n > 1$ and every n-ary term operation f of $\underset{\sim}{A}$ and for all $u, v, x_1, \ldots, x_n, y_1, \ldots, y_n$ the following quasi-identity holds

$$f(u, x_1, \ldots, x_n) = f(u, y_1, \ldots, y_n) \rightarrow f(v, x_1, \ldots, x_n) = f(v, y_1, \ldots, y_n)$$

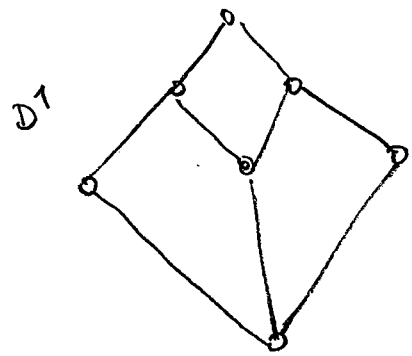
11.2.2 A lattice $(L; \wedge, \vee)$ is join semi distributive if $(SD_\vee)$ $(x \vee y = x \vee z) \rightarrow (x \vee y = x \vee (y \wedge z))$

Example



D_2

Dual version: $(SD\wedge)$



11.2.3 A semigroup $\underset{\sim}{A}$ is called cancellation semigroup if the quasi-identities is fulfilled

$$(x_1 \cdot x_2 = x_1 \cdot x_3 \longrightarrow x_2 = x_3$$

$$x_1 x_3 = x_2 x_3 \longrightarrow x_1 = x_2$$

Notation 11.3

We consider classes of algebras without predicate symbols and so identities and quasi identities have the respective forms

(11.3.1) $\forall x_1 \dots \forall x_k \; (t(x_1 \dots x_k) = s(x_1 \dots x_k)$

(11.3.2) $\forall x_1 \dots \forall x_k ((t_0 = s_0) \wedge \dots \wedge (t_{n-1} = s_{n-1})) \rightarrow (t_n = s_n)$

We consider also

(11.3.3) $\forall x_1 \dots \forall x_k \, (t_0 \neq s_0) \vee \dots \vee (t_{n-1} \neq s_{n-1})$

which is called as anti-identities $(t_0 \neq s_0 := \neg(t_0 = s_0))$

The classes of identies, quasi-identities and anti-identities are called universal Horn classes.

Them Horn classes are preserved by non-trivial (arbitrary) direct products

11 B Ultra products

Def. 11.4 Let $(B; \wedge, \vee, ', 0, 1)$ be a Boolean algebra
A subset $F \subseteq B$ is a filter if it holds

i) $1 \in F$ $(F \neq \emptyset)$

ii) If $x \in F$ and $x \leq y$ then $y \in F$

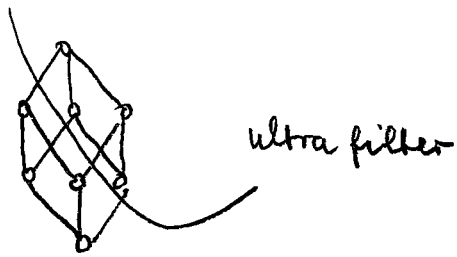
iii) If $x \in F$ and $y \in F$ then $x \wedge y \in F$

A filter F is an ultrafilter if

iv) $0 \notin F$

v) If $x \in B$ then either $x \in F$ or $x' \in F$

Example



You could also consider the dual form namely

ideal $\longleftrightarrow$ prim ideal.

Construction 11.5 Let I be a index set, and the Boolean algebra $(P(I); \wedge, \vee, \neg, \emptyset, I)$

We consider a family of algebras $\underset{\sim}{A}_i = (A_i, \Omega)$ for some types ~~varies~~ $i \in I$. $\underset{\sim}{A} = \prod \underset{\sim}{A}_i$ is the direct product. If $f \in A$ we denote its ith coordinate by $f(i)$

Let F be a collection of subsets of I. We define the relation $\sim_F$ on A by

$$f \sim_F g \quad \text{iff} \quad \{i \mid i \in I, f(i) = g(i)\} \in F$$

Lemma 11.6 If F is a filter on I then $\sim_F$ is an equivalence relation on $\prod A_i$

Proof. If F is a filter on I, $I \in F$ and therefore $\sim_F$ is reflexive. Clearly $\sim_F$ is symmetric.

Suppose $f \sim_F g$ and $g \sim_F h$. We have

$X = \{i \mid i \in I \ f(i) = g(i)\} \in F$

$Y = \{i \mid i \in I \ g(i) = h(i)\} \in F$

Because F is a filter we have $X \cap Y \in F$

But $X \cap Y \subseteq Z = \{i \mid i \in I \ f(i) = g(i)\}$

and $Z \in F$

We have $f \sim_F h$ and therefore it is transitive □

Def. 11.7 For each $f \in \Pi A_i$ let $f/_F$ be the equivalence class to which f belongs under the relation $\sim_F$. Let

$$\Pi A_i/_F = \{f/_F \mid f \in \Pi A_i\}$$

$\Pi A_i/_F$ is called reduced product of the family $\{A_i \mid i \in I\}$ over the filter F

If F is an ultra filter then $\prod \underset{\sim}{A}_i / F$

is called an ultra product

Notation 11.8

$P_r(K)$ is the class of reduced products of algebras in K

$P_u(K)$ is the class of ultra products of algebras in K

Remark Let $\underset{\sim}{A}_i$ be a non-empty family of algebras of the type τ and let F be a filter over I. If a Horn sentence φ holds in every algebra $\underset{\sim}{A}_i$ then φ holds in the reduced product $\prod_{i \in I} A_i / F$

sentences = 11.3.1 , 11.3.3 and 11.3.2

Thm. 11.9 (Mal'cev)

A class of algebras of the type t is a quasi-variety if and only if it is closed under sub-algebras and reduced products of algebras

(without proof)

§ 12 Equational logic

121 Let V be a variety of a given type τ

According to G. Birkhoff and A. Tarski we consider the following rules of derivation

1) $t = t$ for every $t \in T(X)$

2) $t_1 = t_2$ implies $t_2 = t_1$ for every terms $t_1, t_2 \in T(X)$

We write the rule in the form

$$\frac{t_1 = t_2}{t_2 = t_1}$$

3) $t_1 = t_2$ and $t_2 = t_3$ imply $t_1 = t_3$ for every term $t_1, t_2, t_3 \in T(X)$

$$\frac{t_1 = t_2 \ , \ t_2 = t_3}{t_1 = t_3}$$

4) $t_1 = s_1, \dots, t_n = s_n$ and f_σ a n-ary operation symbol of Ω imply $f_\sigma(t_1, \dots, t_n) = f_\sigma(s_1, \dots, s_n)$ for every $f_\sigma \in \Omega$, $t_1, \dots, t_n \in T(X)$ and $s_1, \dots, s_n \in T(X)$

$$\frac{t_1 = s_1, \ldots, t_n = s_n}{f_\sigma(t_1, \ldots, t_n) = f_\sigma(s_1, \ldots, s_n)}$$

5) $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$ and $\tau_1, \ldots, \tau_n \in T(X)$

imply $t(\tau_1, \ldots, \tau_n) = s(\tau_1, \ldots, \tau_n)$

$$\frac{t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n), \quad \tau_i \in T(X) \quad i = 1, \ldots, n}{t(\tau_1, \ldots, \tau_n) = s(\tau_1, \ldots, \tau_n)}$$

Def. 12.2 Let Σ be a set of identities of a type τ. An identity $s_m = t_m$ can be derived from Σ if there exists a sequence $(s_1 = t_1, \ldots, s_m = t_m)$ of identities such that either $(s_i = t_i) \in \Sigma$ or is implied by identies $(s_j = t_j)$ $j \in \{1, \ldots, i-1\}$ by the above five rules of equational logic. We write

$$\Sigma \vdash (s_m = t_m)$$

and we say $(s_m = t_m)$ can be deduced from Σ

A deduction of $s_m = t_m$ from Σ is also called a proof of the equational logic

Remark: $\vdash$ is called the syntactical implication

Def. 12.3 A congruence θ on an algebra $\underset{\sim}{A}$ is fully invariant if for every homomorphism $\alpha : A \to A$ $(a,b) \in \theta$ implies $(\alpha(a), \alpha(\beta)) \in \theta$

Notation 12.4
Let $Id(X)$ be a set of identities of type τ
Let $\theta : Id(X) \longrightarrow T(X) \times T(X)$ be the bijection defined by $\theta(s=t) = (s,t)$
$Id_K(X) :=$ the identities which hold for K

Lemma 12.5 $\theta(Id_K(X))$ is a fully invariant congruence for the class K of algebras of type τ

Proof. $(t_1 = t_1) \in Id_K(X)$ and hence $(t_1, t_1) \in \Theta(Id(X))$ is reflexive.

If $(t_1 = t_2) \in Id_K(X)$ then $(t_2 = t_1) \in Id_K(X)$ and if $(t_1, t_2) \in \Theta(Id_K(X))$ then $(t_2, t_1) \in \Theta(Id_K(X))$ is symmetric,

If $(t_1, t_2) \in \Theta(Id_K(X)$ and $(t_2, t_3) \in \Theta(Id_K(X)$
$\Rightarrow (t_1, t_3) \in \Theta(Id_K(X)$ is transitive,

If $(s_i = t_i) \in Id_K(X)$, $i = 1, \dots, n$ and $f_\sigma \in \Omega$ then $f_\sigma(s_1, \dots, s_n) = f_\sigma(t_1, \dots, t_n)$ and hence $\Theta(Id_K(X))$ is a congruence

If $s(x_1, \dots, x_n) = t(x_1, \dots, x_n) \in Id_K(X)$ and α is a homomorphism $\alpha : A \to A$

Then $\alpha(s(x_1, \dots, x_n) = \alpha(t(x_1, \dots, x_n))$

and hence $s(\alpha(x_1), \dots, \alpha(x_n)) = t(\alpha(x_1), \dots, \alpha(x_n))$

Hence $\Theta(Id_K(X))$ is fully invariant □

Def. 12.6 A subset Σ of $Id_K(X)$ of type τ is called an equational theory if there is a class K of algebras of type τ such that

$$\Sigma = Id_K(X)$$

Thm 12.7 Let Σ be a subset of $Id_\tau(X)$
There exists a class K of algebras of
type τ such that

$$\Sigma = Id_K(X)$$

if and only if $\theta(\Sigma)$ is a fully invariant
congruence of $T(X)$.

Proof. For Σ with $\Sigma = Id_K(X)$ for a class K we have
that $\theta(\Sigma)$ is fully invariant according to
Lemma 12.5. On the other hand, if $\theta(\Sigma)$
is a fully invariant congruence then
$K = HSP(T(X)/\theta(\Sigma))$
Then $K \models (s=t)$ iff $(s,t) \in \theta(\Sigma)$
(Burris, San... Page 91/92)

Corollary 12.8 The equational theories
of type τ form a lattice which is
isomorphic to the lattice of fully
invariant congruences of $T(X)$

Def. 12.9 Let Σ be a set of identies of type τ

$$\Sigma \models (s=t)$$

Σ implies semantically $s=t$ if

for every algebra $\underset{\sim}{A}$ which satisfies Σ

the algebra $\underset{\sim}{A}$ also satisfies $s=t$

Thm 12.10 (Correctness thm)

If $\Sigma \vdash (s=t)$ then $\Sigma \models (s=t)$

Without proof: We observe that every rule is correct.

Notation 12.11

If Σ is a set of identities of type τ

then the derivedive closure (Ableitungshülle) $\mathbb{D}(\Sigma)$

is the smallest subset of all identities of $Id(X)$

which can be derivedd.

$\eta(\Theta)$ is the smallest fully invariant congruence

which contains Θ.

Thm 12.12 Let Σ be a set of identies of type τ
Let $(s=t) \in Id_K(X)$ be the set of all identities of type τ

$\Sigma \models (s=t)$ if and only if $(s=t) \in \mathcal{D}(\Sigma)$

Proof. $\theta(\mathcal{D}(\Sigma)$ is a fully invariant congruence because of the derevation rules 1)–5)
As $\eta(\theta(\Sigma))$ is the smallest fully invariant congruence containing $\theta(\Sigma)$
we have $\eta(\theta(\Sigma)) \subseteq \theta(\mathcal{D}(\Sigma)$ $\quad (\Sigma \subseteq \mathcal{D}(\Sigma))$
On the other hand as the 5 rules contains also Σ
Therfore $\eta(\theta(\Sigma)) = \theta(\mathcal{D}(\Sigma))$

We have to show:

$\Sigma \models (s=t)$ if and only if $(s=t) \in \eta(\theta(\Sigma))$

(A) Let $(s=t) \in \eta(\theta(\Sigma))$. Assume $\underset{\sim}{A} \models \Sigma$
As $\theta(Id_{\underset{\sim}{A}}(X))$ a fully invariant congruence of $T(X)$, then we have $\eta(\theta(\Sigma)) \subseteq \theta(Id_{\underset{\sim}{A}}(X)$
Therefore it holds $(s,t) \in \eta(\theta(\Sigma)$ that $\underset{\sim}{A} \models (s=t)$
and from $(s=t) \in \eta(\theta(\Sigma)$ follows $\Sigma \models (s=t)$

(B) If $\Sigma \models (s=t)$ then we have $T(X)/\eta(\theta(\Sigma)) \models \Sigma$

If $\Sigma \models (s=t)$ then we have $T(X)/\eta(\theta(\Sigma)) \models (s=t)$

Therefore we have $(s=t) \in \eta(\theta(\Sigma))$ □

Thm 7.13 (Completeness thm of the equational logic)
(Birkhoff, Tarski)

$$\Sigma \models (s=t) \iff \Sigma \vdash (s=t)$$

Proof. We have to show

$$\Sigma \models (s=t) \Rightarrow \Sigma \vdash (s=t)$$

Because the 5 rules we have to show
1) If $(s=s) \in \Sigma$ then $(s=s) \in \mathbb{D}(\Sigma)$
2), 3) ....
4) If $\dfrac{s_1=t_1, \dots, s_n=t_n}{}$
5) ... $f_\sigma(s_1, \dots, s_n) = f(t_1, \dots, t_n)$ we have $f_\sigma(s_1, \dots, s_n) = f_\sigma(t_1, \dots, t_n) \in \mathbb{D}(\Sigma)$

Altogether we have

$$\mathbb{D}(\Sigma) \subseteq \{ s=t \mid \Sigma \vdash (s=t) \} \subseteq \mathbb{D}(\Sigma)$$

Now it follows by 12.12

$$\Sigma \models (s=t) \text{ iff } (s=t) \in \mathbb{D}(\Sigma)$$

□

§13 Finite bases

Question: Can the identities of a finite algebra of finite type τ be derived from finitely many the identities?

Birkhoff proved that is true if a finite bound on the number of variables.
Murskii constructed a three-element algebra whose identities are not finitely based (1965)

Def 13.1 Let X be a set of variables and K a class of algebras. The set $Id_K(X)$ is finitely based if there is a finite subset Σ of $Id_K(X)$ such that

$$\Sigma \models Id_K(X)$$

The identities of K is called finitely based

Thm 13.2 (Birkhoff)
Let $\underset{\sim}{A}$ be a finite algebra of finite type τ
and let X be a finite set of variables
Then $Id_{\underset{\sim}{A}}(X)$ is finitely based

Proof. Let θ be the congruence on $T(X)$ defined
by $(p,q) \in \theta$
iff $\underset{\sim}{A} \models (p=q)$

As A is finite there are only finitely many
equivalence classes of θ. From each equivalence
class of θ choose one term. Let this set
of representatives be $Q = \{q_1, \dots, q_n\}$

Now let Σ be the identities consisting of

$x = y$ if $x, y \in X$ and $(x,y) \in \theta$

$q_i = x$ if $x \in X$ and $(x, q_i) \in \theta$

$f(q_{i_1}, \dots, q_{i_n}) = q_{i_{n+1}}$ if $f \in \Omega$ and

$\left(f(q_{i_1} \dots q_{i_n}), q_{i_{n+1}}\right) \in \theta$

Then a proof by induction on the number on the function symbols in a term $p \in T(X)$ shows that if $(p_i, q_i) \in \theta$ then $\Sigma \models (p = q_i)$

But then $\Sigma \models (p = q)$ if $\underset{\sim}{A} \models (p = q)$

and therefore $\underset{\sim}{A} \models \Sigma$

$Id_K(X)$ is indeed finitely based. □

Theorem 13.3 (Baker)

If V is a finitely generated congruence-distributive variety of finite type then V is finitely based (without proof) (see 'Burris-Sankappanavar')

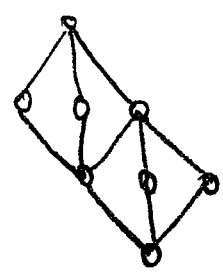
13.4 If V is a finitely generated variety of lattices then V is finitely based (McKenzie)

13.5 Any finite group has a finite basis identities (Oates-Powell)

The Russian school have found many results for finite bases of quasi-identities

13.6 A finite group G has a finite basis of quasi-identities iff
all nilpotent sub-groups of G is abelian.
(Ol'shanskii)

13.7 The lattice M_{3+3} has no finite basis of quasi-identities (Belkin)



§14 Hyperidentities

Preliminaries:

14A

An identity is a pair of terms where the variables are bound by universal quantifiers. Let us take the following medial identity as an example

$$\forall u \forall x \forall y \forall w\, (u \cdot x) \cdot (y \cdot w) = (u \cdot y) \cdot (x \cdot w).$$

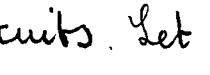
Let us look at the following hyperidentity

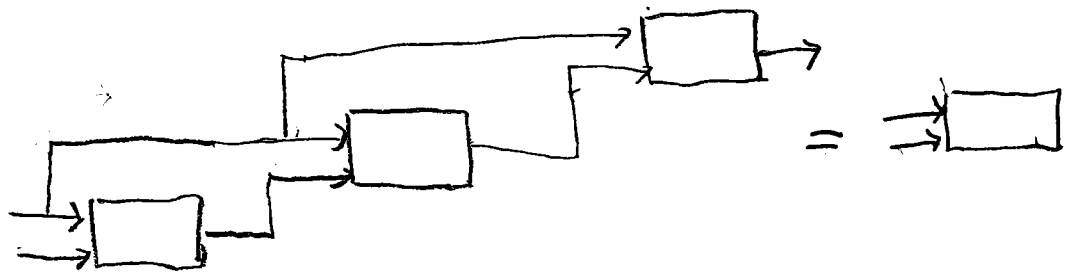
$$\forall F \forall u \forall x \forall y \forall w\, F(F(u,v), F(x,y)) = F(F(u,x), F(v,y)).$$

The hypervariable F is considered in a very specific way. Firstly every hypervariable is restricted to functions of a given arity. Secondly F is restricted to term functions of the given type. Let us take the variety $A_{n,0}$ of abelian groups of finite exponent n. Every binary term $t \equiv t(x,y)$ can be presented by $t(x,y) = ax + by$ with $a, b \in \mathbb{N}_0$. If we substitute the binary hypervariable F in the above hyperidentity by $ax + by$, leaving its variables unchanged, we get

$$a(au + bv) + b(ax + by) = a(au + bx) + b(av + by).$$

This identity holds for every term $t(x,y) = ax + by$ for the variety $A_{n,0}$. Therefore we say that the hyperidentity holds for the variety $A_{n,0}$.

14B Hyperidentities have the following interpretation in the theory of switching circuits. Let  be a symbol for a gate realizing some Boolean function $f: \{0,1\}^2 \longrightarrow \{0,1\}$. Then the two switching circuits



§ 14 Hyperidentities

14A Hyperidentities

Notation 14.1

We consider varieties of algebras of some given type τ.
For a given n_f-arity operation f_f we associate
a symbol F_f which is denoted n_f-arity hypervariable

Def. 14.2 Let V be a variety of a type τ.
The n-ary hyperterms are recursively defined
1) The variables $x_1, \dots, x_n$ are n-ary hyperterms
2) If $T_1, \dots, T_m$ are n-ary hyperterms and
F_f is a m-ary hypervariable then
$F_f(T_1, \dots, T_m)$ is a n-ary hyperterm

$H_n(\tau)$ is the smallest set which contains 1)
and is closed under finite applications of 2)
$H(\tau) = \bigcup (H_n(\tau) \mid n \in \mathbb{N})$ is called
the set of all hyperterms of type τ

A hyperidentity is a pair (T_1, T_2) of hyper terms
We write $T_1 = T_2$

Examples

14.2.1 Let V the variety of distributive lattices
The list of binary (= 2-ary) terms are

$e_1^2(x,y) = x$, $e_2^2(x,y) = y$, $x \wedge y$, $x \vee y$

Consider the following hyperidentities

$$F(F(u,x), F(y,z)) = F(F(u,y), F(x,z))$$

Then the hyperidenty for distributive lattice fulfilled

$e_1^2(e_1^2(u,x), e_1^2(y,z)) = u = e_1^2(e_1^2(u,y), e_1^2(x,z))$

$e_2^2(e_2^2 \ldots \quad = z = e_2^2(e_2^2 \quad)$

$(u \wedge x) \wedge (y \wedge z) = (u \wedge y) \wedge (x \wedge z)$

$(u \vee x) \vee (y \vee z) = (u \vee y) \vee (x \vee z)$

14.2.2 Let V be the variety of abelian groups
Every binary term can be written by

$$ax + by \qquad a, b \in \mathbb{N}_0$$

Therefore $F(F(u,x),F(y,z)) = F(F(u,y),F(x,z))$ is a hyperidentity which is fulfilled by

$$a(au+bx)+b(ay+bz) = a(au+by)+b(ax+b$$

14 B Completeness thm for hyperidentities

Def. 14.3 Derivation rules for hyperidentities

1) $T_1 = T_1$ for every hyperterm $T_1 \in H(\tau)$

2) From $T_1 = T_2$ it follows $T_2 = T_1$

3) From $T_1 = T_2$ and $T_2 = T_3$ it follows $T_1 = T_3$

4) From $S_i = T_i$, $i = 1, \dots, m$ and from the hyperterm operation F_γ it follows $F_\gamma(S_1, \dots, S_m) = F_\gamma(T_1, \dots, T_m)$

5) From $S(x_1, \dots, x_n) = T(x_1, \dots, x_n)$ for $S, T \in H(\tau)$ it follows $S(R_1, \dots, R_n) = T(R_1, \dots, R_n)$ for every $S, T, R_1, \dots, R_n \in H(\tau)$

Remark. The rules for hyperidentities consist of three rules describing reflexivity, symmetry and transitivity. Furthermore compatibility of hyper operations and finally hyper substitution.

In detail we define

Def. 14.4 A mapping $\delta : H(\tau) \to H(\tau)$ is a hypersubstitution if δ satisfies

14.4.1 $\delta(x_k) = x_k$ for every variable x_k, $1 \leq k \leq \omega$

14.4.2 To every fundamental term $f_\sigma(x_1, \dots, x_n)$ it assigns a hyper term $\delta(f_\sigma(x_1, \dots, x_n)) = F_\sigma(x_1, \dots, x_n)$

14.4.3 If $f_\sigma(x_1, \dots, x_n)$ and $F_1, \dots, F_n \in H(\tau)$ then $\delta(f_\sigma(F_1, \dots, F_n)) = F_\sigma(F_1, \dots, F_n)$

Example. Consider the hyperidentity $Q(Q(x,y,z),y,z) = Q(x,y,z)$ and hyperterm $T(x,y,z) := F(G(x,y),z)$

By hypersubstitution 14.4 we derive

$$F(G(F(G(x,y),z),y),z) = F(G(x,y),z)$$

Notation 14.5

We know that $Id_V(X)$ denotes the set of all identies which is satisfied in the variety V.

$E_\tau(V)$ denotes the set of all hyperidentities of type τ which is satisfied by the variety V

Def. 14.6 The class of all varieties K which satisfy the hyperidentities $E_\tau(K)$ of type τ is called the hypervariety of K of type τ

Completeness theorem

A set Σ of hyperidentities of type τ can be represented in the form $E_\tau(K)$ for some variety K of the type τ if and only if Σ is closed under rules 1) – 5)

This thm is a slight modification of G. Birkhoff and A. Tarski's theorem for the set of identities

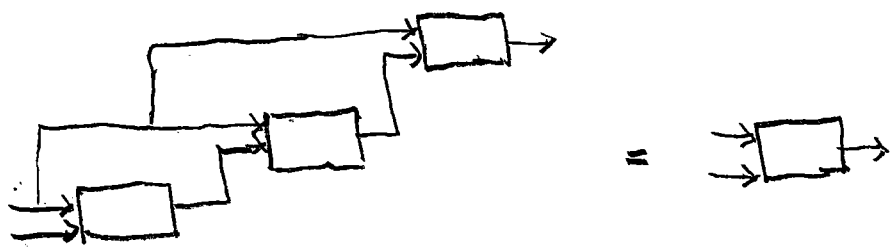
Repetition.

$\mathcal{B} = (\{0,1\}; \wedge, \vee, ', 0, 1)$

The hyper-identity satisfies every term function of $\mathcal{B}$

$$F(F(F(x,y),y),y) = F(x,y)$$

Illustration:



There are 16 term function on the Boolean algebra

We have selected one: $t(x,y) = x' \wedge y$

$$t(t(t(x,y),y),y) = ((x' \wedge y) \wedge y) \wedge y = (x' \wedge y) \wedge (y \wedge y)$$

$$= (x' \wedge y) \wedge y = x' \wedge y = t(x,y)$$

14 B. Derived algebras and solid varieties

Notation 14.7 Let K be a class of algebras of a given type $\tau = (n_0, n_1, \dots, n_\beta, \dots)$

The algebra $\underset{\sim}{B}$ is called a derived algebra of $\underset{\sim}{A} = (A; f_0, f_1, \dots, f_\alpha, \dots)$ if there exists term operations $t_0, t_1, \dots, t_\beta, \dots$ of type τ such that $\underset{\sim}{B} = (A; t_0, t_1, \dots, t_\beta, \dots)$

For a class K of algebras of type τ we denote by $D(K)$ the class of all derived algebras of type τ of K.

Def. 14.8 Let V be a class of algebras of a given type τ

V is a solid variety if V is a variety which is closed under derived algebras (that means: $D(V) \subseteq V$)

Example 14.9.

14.9.1 The variety B of semigroups of the type (2) defined by the following identities, is a solid variety

$$x \circ (y \circ z) = (x \circ y) \circ z$$

$$x \circ x = x$$

$$(u \circ x) \circ (y \circ v) = (u \circ y) \circ (x \circ v)$$

Proof. We have to show that the set of binary terms of the variety consists $\{x, y, x \circ y, y \circ x, x \circ y \circ x, y \circ x \circ y\}$

For instance $(x \circ y \circ x) \circ (y \circ x) =$

$(x \circ y) \circ (x \circ y) \circ x = (x \circ y) \circ (y \circ x) \circ x$

$= (x \circ (y \circ y)) \circ (x \circ x) = x \circ y \circ x$

Furthermore the hyperidentities holds by

$$F(x, (F(y,z)) = F(F(x,y), z)$$

$$F(x,x) = x$$

$$F(F(u,x), F(y,v)) = F(F(u,y)\ F(x,v))$$

This variety of semigroups is called regular band

14.9.2 Let V be the variety RB of rectangular bands which is defined by

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$x \cdot x = x$$

$$x \cdot (y \cdot z) = x \cdot z$$

This variety is solid. Consider all binary terms

$t_1(x,y) = x$, $t_2(x,y) = y$, $t_3(x,y) = x \cdot y$, $t_4(x,y) = y \cdot x$

We can give another definition of 14.8

Def. 14.10 Let V be a class of algebras of a given type τ. V is a solid variety if and only if V is closed under homomorphic images H, sub-algebras S direct products P and derived algebras $\mathbb{D}$, i.e

$$H(V) \subseteq V,\ S(V) \subseteq V,\ P(V) \subseteq V,\ \mathbb{D}(V) \subseteq V$$

Problem 14.11 Describe the semi group generated by the Operators $H, S, P, \mathbb{D}$ (Compare Pigozzi)

Thm 14.12 Let V be a class of algebras of a given type τ. V is a solid variety if and only if

$$V = HSP\mathbb{D}(V)$$

Proof

a) $\mathbb{D}P(V) \subseteq P\mathbb{D}(V)$

For $\underset{\sim}{B} \in \mathbb{D}P(V)$ we have $\underset{\sim}{B} = (A; t_0, t_1, \ldots, t_\beta, \ldots)$

with $\underset{\sim}{A} = (A; f_0, f_1, \ldots, f_\alpha, \ldots)$ and $\underset{\sim}{A} = \Pi A_i$,

$\underset{\sim}{A}_i = (A_i; f_0, f_1, \dots, f_\delta, \dots)$ Consider $\underset{\sim}{B}_i = (A_i; t_0, t_1, \dots, t_\rho, \dots)$

then we have $\underset{\sim}{B} = \prod_{i \in I} \underset{\sim}{B}_i$ and hence $\underset{\sim}{B} \in PD(V)$

b) $DS(V) \subseteq SD(V)$

Let $\underset{\sim}{B} = (B; t_0, t_1, \dots, t_\rho, \dots) \in DS(V)$ of the algebra $(A; f_0, f_1 \dots f_\delta$

$\underset{\sim}{C} = (B; f_0, f_1, \dots, f_\sigma, \dots)$ is a subalgebra for some algebra $\underset{\sim}{A} = (A; f_0, \dots, f_\sigma, \dots)$

As $(B; t_0, t_1, \dots, t_\rho, \dots)$ is a subalgebra of $(A; t_0, t_1, \dots t_\rho \dots)$ we have $\underset{\sim}{B} \in SD(V)$

c) $DH(V) \subseteq HD(V)$

Let $\underset{\sim}{B} = (B; t_0, t_1, \dots, t_\rho, \dots) \in DH(V)$

Then there is a homomorphic images $f[\underset{\sim}{A}] = (f[A]; f_0, f_1, \dots, f_\sigma, \dots)$ of an algebra $\underset{\sim}{A}$ with $f[A] = B$. But $(B; t_0, t_1, \dots, t_\rho, \dots)$ is also a homomorphic image of $(A, t_0, t_1, \dots, t_\rho, \dots)$ because $f[A] = B$ and $f(t_\rho(x_1, \dots, x_\delta) = t_\rho(f(x_1), \dots, f(x_\delta))$

d) $DHSP(V) \subseteq HSPD(V)$

□

14C Weak isomorphisms

14.13 Example

Let $\underset{\sim}{B} = (\{0,1\}; \wedge, \vee, ', 0, 1)$ be the Boolean algebra on the set $\{0,1\}$

Let $\underset{\sim}{R} = (\{0,1\}; +, -, 0, \cdot 1)$ be the commutative ring on the set $\{0,1\}$ where the addition is modula 2

We have the mapings a) and b) on $\{0,1\}$

a) $x \vee y \to x + y + x \cdot y$ $\quad 0 \to 0$

$x \wedge y \to x \cdot y$ $\quad 1 \to 1$

$x' \to x + 1$

b) $x + y \to (x' \wedge y) \vee (x \wedge y')$ $\quad 0 \to 0$

$x \cdot y \to x \wedge y$ $\quad 1 \to 1$

$-x \to x'$

Def. 14.14 Let $\underset{\sim}{A} = (A; \Omega_1)$ and $\underset{\sim}{B} = (B; \Omega_2)$ be algebras not necessarily of the same type and let $h: A \to B$ be a mapping

Let $\varphi \in T(\underline{A})$ and $\Psi \in T(\underline{B})$ of the same arity n

Then φ and Ψ are in relation R_n, i.e

$$h(\varphi(x_1,\dots,x_n)) = \Psi(h(x_1),\dots,h(x_n))$$

Def. 14.15 The mapping $h: A \to B$ is called a weak homomorphism of $\underline{A}$ into $\underline{B}$ iff

i) for every $\varphi \in T(\underline{A})$ there is a $\Psi \in T(\underline{B})$ with $(\varphi,\Psi) \in R_n$

ii) for every $\alpha \in T(\underline{B})$ there is a $\beta \in T(\underline{A})$ with $(\beta,\alpha) \in R_n$

Def. 14.16 A congruence θ of an algebra $\underline{A}$ is totally invariant if $(a,b) \in \theta$ implies $(h(a),h(b)) \in \theta$ for every weak endomorphism h which preserve the same type τ

We observe that $\Sigma \subseteq Id\,\tau$ is solid if and only if Σ is a totally invariant congruence of $F_\tau(X)$

Remark 14.17

The closures with respect to the deduction rules 1)-6) corresponds to properties of Σ as follow:

Σ is closed under 1)-3) $\Leftrightarrow$ Σ is an equivalence

Σ is closed under 1)-4) $\Leftrightarrow$ Σ is a congruence relation

Σ " " " 1)-5) $\Leftrightarrow$ Σ is a fully invariant congruence

Σ " " " 1)-6) $\Leftrightarrow$ Σ is a totally invariant congruence

14D Fluid varieties

Let $\sigma = \langle t_0, t_1, \ldots, t_p, \ldots \rangle$ be a fixed choice of terms of V. We denote $\underset{\sim}{A}_\sigma$ the derived algebra from $\underset{\sim}{A}$

Def. 14.18 A derived algebra $\underset{\sim}{A}_\sigma$ is called proper if $\underset{\sim}{A}_\sigma$ is not isomorphic to $\underset{\sim}{A}$

A variety V of type τ is solid if the variety V contains all derived algebras from V

A variety V of type τ is fluid if the variety V does not contain any proper derived algebra

We write the fundamental operation of a commutative of the groupoid as addition and denote terms $(\ldots((x+x)+x)+\cdots)+x$ by kx if there are k variables in this term. In the following we consider the cyclic group $(\mathbb{Z}_n; +)$ of non negative integers modulo n. Ofcourse in this case we have $x + nx = x$

Prop. 14.19 If $G = (\mathbb{Z}_n; +)$ is the semigroup, which is described as above, then G is fluid

Proof. The binary terms $t(x,y)$ of G can be presented by $t(x,y) = kx + ly$; $k, l \in \mathbb{N}_0$ $0 \leq k, l \leq n-1$

Let $G_\oplus = (\mathbb{Z}_n; \oplus)$, where $x \oplus y = kx + ly$ be a that derived groupoid. Let us assume that $G_\oplus \in HSP(G)$ then we have $x \oplus y = y \oplus x$ and therefore $kx + ly = ky + lx$

We have $k=l$ and the operation $\oplus$ is of the form $x \oplus y = kx + kl$, $0 \leq k \leq n-1$. Because the associativity we have $x \oplus (y \oplus z) = (x \oplus y) \oplus z$

hence $kx + k^2y + k^2z = k^2x + k^2y + kz$

If $k=0$ then $x \oplus nx = 0$ with $x \neq 0$

Otherwise we have $x + kz = kx + z$ for $x, y \in \mathbb{Z}_n$

From this follows $k = 1$ and $G_\sigma \simeq G$

Thm 14.20 If $\underset{\sim}{A} = (G; +, -, 0)$ is an abelian group of order n then $\underset{\sim}{G} = (G; +)$ is a fluid semigroup

Proof. $\underset{\sim}{A}$ is the direct product of cyclic groups $\underset{\sim}{A}_i = (G_i; +, -, 0)$ with an order of prime power $p_i^{n_i}$

Therefore we have $G_\sigma = \left(\prod_{i \in I} G_i\right)_\sigma = \prod_{i \in I} (G_i)_\sigma$

We assume that $G_\sigma \in HSP(G)$ then it follows that $(G_i)_\sigma \in HSP(G)$ for every $i \in I$. Especially the associative and commutative laws have to hold

From the proof of 14.19 it follows that $(\underset{\sim}{G}_i)_\sigma \in HSP(\underset{\sim}{G}_i)$ if and only if $\underset{\sim}{G}_{i\sigma} \cong \underset{\sim}{G}_i$. Hence from our assumption it follows that $\underset{\sim}{G}_\sigma \cong \underset{\sim}{G}$

Prop. 14.21 Every subvariety W is a fluid variety V is fluid

Proof. Let V be a fluid variety and let $\underset{\sim}{A} \in W \subseteq V$ be an algebra. Assume that A_σ be a proper derived algebra. Then we have the contradiction of $\underset{\sim}{A}_\sigma \subseteq V$.

Remark. The subvariety of a fluid variety V of type τ form a sublattice of the lattice of all varieties of type τ

§15 Hyperquasivarieties

15A Examples of hyper-quasi-identities

We like to repeat:

Def. 15.1 An algebra $\underset{\sim}{A}$ is called abelian if for every $n \geq 1$ and every n-ary term operation $f \in \underset{\sim}{A}$ and for all $u, v, x_1, \dots, x_n$ $y_1, \dots, y_n$ the following condition holds

$$f(u, x_1, \dots, x_n) = f(u, y_1, \dots, y_n) \rightarrow f(v, x_1, \dots, x_n) = f(v, y_1, \dots, y_n)$$

Prop 15.2 An algebra $\underset{\sim}{A}$ is abelian if and only if the following hyper-quasi-identity holds in $\underset{\sim}{A}$:

$$F(u, x_1, \dots, x_n) = F(u, y_1, \dots, y_n) \rightarrow F(v, x_1, \dots, x_n) = F(v, y_1, \dots, y_n)$$

The proof is given by the definition of the hyper-quasi-identity later on.

We like to study semidistributive lattices and we repeat:

Def. 15.3 A lattice is join semidistributive if it satisfies the following quasi-identity

$$(SD_\vee) \quad x \vee y = x \vee z \rightarrow x \vee y = x \vee y \vee z$$

meet semi distributive:

$$(SD_\wedge) \quad x \wedge y = x \wedge z \rightarrow x \wedge y = x \wedge y \wedge z$$

A lattice is semidistributive if it is simultaneously join and meet semidistributive

Thm 15.5 Let $\underset{\sim}{L} = (L; \wedge, \vee)$ is a lattice which is semidistributive. Then the following hyper quasi identity is satisfied

$$(F(x,y) = F(x,z)) \rightarrow (F(x,y) = F(x, G(y,z)))$$

Proof

Case 1 $F(x,y) := x$ then $(x = x) \rightarrow (x = x)$

Case 2 $F(x,y) := y$

Consider $G(y,z) := y, z, y \wedge z, y \vee z$

Then the following quasi-identities are satisfied

$(y = z) \rightarrow (y = y)$; $(y = z) \rightarrow (y = z)$, $(y = z) \rightarrow (y = y \wedge z)$

$(y = z) \rightarrow (y = y \vee z)$

Case 3 $F(x,y) := x \wedge y$

Consider $G(y,z) := y, z, y \wedge z, y \vee z$

Then the following quasi-identities hold

$(x \wedge y = x \wedge z) \to (x \wedge y = x \wedge y)$, $(x \wedge y = x \wedge z) \to (x \wedge y = x \wedge z)$

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

$(x \wedge y = x \wedge z) \to (x \wedge y = x \wedge (y \vee z)$ (The last one follows from the meet semi distributivity

case4 $F(x,y) := x \vee y$. Consider $G(y,z) := y,z, y \wedge z, y \vee z$

Then the following quasi-identities hold in L

$(x \vee y = x \vee z) \to (x \vee y = x \vee y)$, $(x \vee y = x \vee z) \to (x \vee y = x \vee z)$

$(x \vee y = x \vee z) \to (x \vee y = x \vee (y \wedge z))$ (by semi distributivity)

$(x \vee y = x \vee z) \to (x \vee y = x \vee (y \vee z))$

15 B Derived algebras.

We like to complete the definition of the hyper-quasi-identity

Def 15.6 A hyper-quasi-identity e^* is an implication of the form

$$(T_0 = S_0) \wedge \dots \wedge (T_{n-1} = S_{n-1}) \to (T_n = S_n)$$

where $T_i = S_i$ are hyperidentities for $i = 0, \dots, n$

If σ is a hyper substitution of type τ and the elements $a_1, \dots, a_k \in A$ satisfy the equalities $\sigma(T_i)(a_1, \dots, a_k) = \sigma(S_i)(a_1, \dots, a_k)$ for $n = 0, 1, \dots, n-1$ in $\underset{\sim}{A}$ then the equality $\sigma(T_n)(a_1, \dots, a_k) = \sigma(S_n)(a_1, \dots, a_k)$ holds in $\underset{\sim}{A}$

By other words, a hyper-quasi-identity is a universally closed Horn $\forall x \forall \sigma$-formula where x vary over all sequences of individual variables (occuring in terms of the implication) and σ vary over all hypersubstitutions of a given type.

Repetition 15.7

An algebra $\underset{\sim}{B}$ of the type τ is called a derived algebra of $\underset{\sim}{A} = (A; f_0, f_1, \dots, f_\sigma, \dots)$ if there exist term operations $t_0, t_1, \dots, t_\sigma, \dots$ such that $\underset{\sim}{B} = (A; t_0, t_1, \dots, t_\sigma, \dots)$

For a class K of algebras of typeτ we denote by $\mathbb{D}(K)$ the class of all derived algebras

Notation 15.8

For a given algebra A we denote by

$QId(A)$

the set of quasi-identities and

$HQId(A)$

the set of hyper-quasi-identities

Similary we denote

$Q(K)$

the class of all algebras satisfying all quasi-identities and

$HQ(K)$

for hyper-identities

The transformation T of an quasi-identity e into a hyper-quasi-identity e^* is defined in a natural way Similary T^{-1} transform every hyper-quasi-identity e^* into the quasi-identity e

Prop. 15.9 Let K be a class of algebras of type τ
Then it holds :

$$HQId(K) = T(QId(D(K))$$

Proof. We will show $HQId(K) \subseteq T(QId(D(K))$
Let e^* be a hyper-quasi-identity and let
$\underset{\sim}{B}$ a derived algebra from $\underset{\sim}{A}$ with $\underset{\sim}{B} = \underset{\sim}{A}^{\sigma}$
By the definition 15.6 the quasi-identity
fulfills $T^{-1}(e^*)$ in $\underset{\sim}{B}$. Therefore we have
$e^* \in T(QId(D(K))$

Now we have to show $HQId(K) \supseteq T(QId(D(K))$
Let e be quaisi identity in $D(K)$ and let $\underset{\sim}{A}$
be an algebra of K with $a_1, \dots, a_k \in A$
Let σ be a hyper substitution, and consider
$\sigma(e)$ in $\underset{\sim}{A}$. As $\underset{\sim}{A} \in D(K)$ then $\sigma(e)$ can
be consider as a quasi-identity of the
derived algebra $\underset{\sim}{A}^{\sigma}$

Assume that $p_i^{A_\sigma}(a_1,\dots,a_k) = q_i^{A_\sigma}(a_1,\dots,a_k)$.

Because of $\underset{\sim}{A} \in D(K)$ we obtain that

$P_n^{A_\sigma}(a_1,\dots,a_k) = q_n^{A_\sigma}(a_1,\dots,a_k)$.

$T(e)$ holds in K as a hyper-quasi-identity and we have $T(e) \in HQId(K)$ □

Def. 15.10 A class K of algebras of type τ is called a hyper-quasi-variety if there is a set Σ of hyper-quasi-identities such that K consists exactly of those algebras of type τ that hyper satisfy all hyper-quasi-identities of Σ

Thm 15.11 A quasi-variety K of algebras of the type τ is a hyper-quasi-variety if and only if K is closed under derived algebras D (without proof.)

§16 Hybrid identities

16A Hybrid variables

Def. 16.1 Let a variety of type τ be given.
The n-ary hybrid terms are recursively defined by

i) the variables $x_1, \dots, x_n$ are n-ary hybrid terms

ii) if $T_1, \dots, T_m$ are n-ary hybrid terms and
f is an m-ary operation symbol then
$f(T_1, \dots, T_n)$ is an n-ary hybrid term

iii) if $T_1, \dots, T_m$ are n-ary hybrid term and
F is an m-ary operation symbol then
$F(T_1, \dots, T_m)$ is an n-ary hybrid term.

$H^n(\tau)$ is the smallest set containing the variables $x_1, \dots, x_n$ which closed under finite application of ii) and iii

$H(\tau) = \bigcup \{ H^n(\tau) \mid n \in \mathbb{N} \}$ is called the set of hybrid terms of type τ

Def. 16.2 A variety V satisfies a hybrid identity $h_1 = h_2$ if for every substitution of the hyper variables by terms (of the same arity) of V leaving the variables unchanged the identities (which arise) holds in V

Example 16.3 We consider the variety CB of commutative bands

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$

$x \cdot x = x$

$x \cdot y = y \cdot x$

We consider the list of term in two variables: $x, y, x \cdot y$

We also consider the set of hybrid identities

$F(x, F(y,z)) = F(F(x,y),z)$

$F(x,x) = x$

$F(F(u,x), F(y,v)) = F(F(u,y), F(x,v))$

$F(u \cdot x, y \cdot v) = F(u,y) \cdot F(x,v)$

Notation 16.4

Let us note that there is a correspondence between hyper identities and hybrid identities. Consider a type τ^* which 'duplicates' every operation symbols. For the algebra $\underset{\sim}{A} = (A; f_i : i \in I)$ we assign the algebra $\underset{\sim}{A}^* = (A; f_i, F_i : i \in I)$. We consider the monoid M of hypersubstitutions σ of type τ^* such that $\sigma(f_i) = f_i$, $i \in I$. Then we obtain for any hybrid identity:

$$\underset{\sim}{A} \vDash (p = q) \text{ if and only if } \underset{\sim}{A}^* \vDash (\hat{\sigma}(p) = \hat{\sigma}(q))$$

for $\sigma \in M$

(Every hybrid identity of $\underset{\sim}{A}$ is a M-hyper identity of $\underset{\sim}{A}^*$ and vice versa)

Notation 16.5

The rules of the hybrid identities are

1) $$\frac{}{T_1 = T_1}$$

2) $$\frac{T_1 = T_2}{T_2 = T_3}$$

3) $$\frac{T_1 = T_2 \;,\; T_2 = T_3}{T_1 = T_3}$$ (Equivalence)

4) For every n-ary operation symbol f_i and hypervariable F_i for $i \in I$ the hybrid identities $T_i = S_i$, $i \in I$ imply

$f_i(T_1, \dots, T_n) = f_i(S_1, \dots, S_n)$ and

$F_i(T_1, \dots, T_n) = F_i(S_1, \dots, S_n)$ (Compatibility)

5) $$\frac{T(x_1, \dots, x_n) = S(x_1, \dots, x_n) \;,\; \tau_i \;,\; i = 1, \dots, n}{T(\tau_1, \dots, \tau_n) = S(\tau_1, \dots, \tau_n)}$$

(Substitution)

6) $$\frac{T(x_1,\dots,x_n) = S(x_1,\dots,x_n),\ R_i,\ i = 1,\dots,n}{T(R_1,\dots,R_n) = S(R_1,\dots,R_n)}$$

This rule is a modification of the rule of hypersubstitution which allows to substitute hypervariables by terms of same arity and will be referred as the rule of hybrid substitution.

Thm 16.6 A set Σ of hybrid identities of some type can be presented as a set of hybrid identities of the variety V if and only if Σ is closed under the rules 1) - 6)

(Without proof.)

Remarks 16.7

Every variety can be presented by a set of hybrid identities

16 B Hybrid identities for normal band

16.8 The variety NB of normal bands is defined by

NB1 $x \circ x = x$

NB2 $x \cdot (y \circ z) = (x \circ y) \circ z$

NB3 $(u \circ v) \circ (x \circ y) = (u \circ x) \circ (v \circ y)$

We consider hybrid identities of NB

NBi $F(x,x) = x$

NBii $F(x,(F(y,z)) = F(F(x,y),z)$

NBiii $F(F(u,v), F(x,y)) = F(F(u,x), F(v,y))$

NB iv $F(u \circ v, x \circ y) = F(u,x) \cdot F(v,y)$

Prop 16.9 The hybrid identities NBi – NBiv hold for the variety NB of normal bands

Proof. Because the variety NB is solid then NBi – NB iii hold for NB

The hybrid identity NBiv has to checked for all binary terms. The list of these terms consists of $\{x, y, x\cdot y, y\cdot x, x\cdot y\cdot x, y\cdot x\cdot y\}$

We show only NBiv for $y\cdot x\cdot y$

We have $[(v\cdot u\cdot v)\cdot(u\cdot v\cdot u)]\cdot[(y\cdot x\cdot y)\cdot(x\cdot y\cdot x)]$

$= [(v\cdot u\cdot v)\cdot(y\cdot x\cdot y)]\cdot[(u\cdot v\cdot u)\cdot(x\cdot y\cdot x)]$

using the axioms NBi – NBiii

Prop. 16.10 If $F(u\cdot v, x\cdot y) = F(u,x)\cdot F(v,y)$ holds for a variety W of bands then every hybrid term of W can be presented as a product of hyperterms

Proof.. The statement holds for variables $x, y, u, v, \ldots$ as these can be considered as hyperterms. It holds for all hyperterms. Let us consider a hybrid term T which is no hyperterm If $T = T_1 \circ T_2$ then by induction on the complexity of T_1, T_2 the statement holds

If $T = F(T_1, T_2)$ and T_1, T_2 are hybrid then again the statement holds. If $T_1 = S_1 \cdot S_2$ then we have

$$T = F(S_1 \cdot S_2, T_2) = F(S_1 \cdot S_2, T_2 \cdot T_2)$$
$$= F(S_1, T_2) \cdot F(S_2, T_2)$$

Now we apply induction on $F(S_1, T_2)$ and $F(S_2, T_2)$

□

Prop. 16.11 Every hyper term T can be transformed to the unique normal form in NB.

Proof. If T is a variable then is in normal form If T is not a variable then we apply the associative, the medial and idempotent hyperidentity to arrange

$$T \equiv T(x_1, \ldots, x_n) = F(F(\ldots F(F(x_{i_1}, x_{i_2}), x_{i_2}) \ldots x_{i_n})$$

in such way that $x_{i_2}, \ldots, x_{i_{n-1}}$ is lexicographically ordered and any repetition of variables is dropped. From this method it follows that the normal form is unique

□

Example

$F(F(F(x_2,x_3),F(x_1,x_3),x_1) = F(F(F(x_2,x_1)F(x_3,x_3),x_1)$

$= F(F(F(x_2,x_1),x_3),x_1) = F(F(x_2,x_1),F(x_3,x_4))$

$= F(F(x_2,x_3),F(x_1,x_1)) = F(F(x_2,x_3),x_1)$

Prop 16.12 Every product $T_1 \cdot T_2 \cdot T_3 \cdot \ldots \cdot T_m$ of hyper terms T_i, $i = 1,\ldots,m$ can be written in a normal form

Proof. At first we write every hyper term T_i $i = 1,\ldots,n$ in normal form and order $T_2,\ldots,T_{m-1}$ lexicographically. We drop repetitions of factors

Thm 16.13 The hybrid identities NB_i - NB_{10} are a base from which every hybrid identity of the variety NB can be derived by the rules 1) - 6)

Proof. We write bothsides of a hybrid identity in normal form and decide whether it holds (i.e if they are equal)

§17 Term Rewriting

17A Reduction

Example. We consider an abelian group $(\mathbb{Z}_n, +, -, 0)$ and a term $(x+y)+((x+y)+y)$

The term be transformed to a normal form after some steps

$$(x+y)+((x+y)+y) \to (x+y)+(x+2y) \to 2x+3y$$

Def. 17.1 An abstract reduction system is a pair $(A, \to)$ where the reduction $\to$ is a binary relation

We write:

x is reducible if there is y such that $x \to y$

x is in normal form (irreducible) if it is not reducible

$x \xrightarrow{n} y$ if there is a path of length n from x to y

$x \xrightarrow{*} y$ if there is some finite path from x to y

$x \xrightarrow{+} y$ if there is some finite non-empty path from x to y

y is a direct successor of x iff $x \to y$

y is a successor of x if $x \xrightarrow{+} y$

x and y are joinable if there is a z such that $x \xrightarrow{*} z \xleftarrow{*} y$

in this case we write $x \downarrow y$

Example 17.2

Let $A := \mathbb{N} \setminus \{0,1\}$ and $\to := \{(m,n) \mid m > n \text{ and } n \text{ divides } m\}$

m is in normal form if m is prime

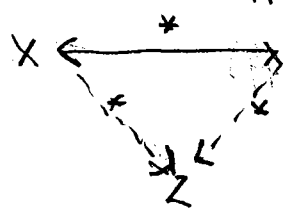
$m \downarrow n$ iff m and n are not relatively prime

$\xrightarrow{+} = \to$ because $>$ and "divides" is already transitive

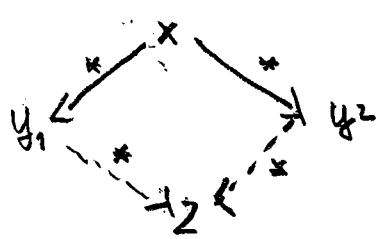
$\xleftrightarrow{*} = A \times A$

Def. 17.3 A reduction $\to$ is called

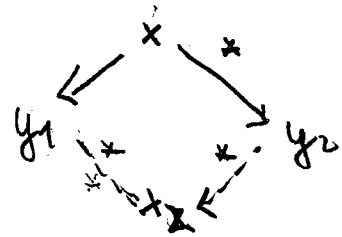
Church-Rosser iff $x \xleftrightarrow{*} y \Rightarrow x \downarrow y$



confluent iff $y_1 \xleftarrow{*} x \xrightarrow{*} y_2 \Rightarrow y_1 \downarrow y_2$



semi-fluent iff $y_1 \leftarrow x \xrightarrow{*} y_2 \Rightarrow y_1 \downarrow y_2$



Prop. 17.4

The following conditions are equivalent

1) $\rightarrow$ has the Church-Rosser property
2) $\rightarrow$ is confluent
3) $\rightarrow$ is semi-confluent

Corollary 17.5

Let $\rightarrow$ be confluent and $x \overset{*}{\leftrightarrow} y$

1) $x \xrightarrow{*} y$ if y is in normal form
2) $x = y$ if both x and y are in normal form

17B Term rewriting

Normal 17.5

17 B Term Rewriting

Notation 17.5 Let K be a class of algebras.
Let E be a set of identities and let $s = t$ be an identity
We say that $s = t$ is valid in E if
the identity $s = t$ holds in E and we write $s =_E t$

$s = t$ is satisfiable in E if there is a substitution σ
such $\sigma(s) =_E \sigma(t)$

(Both question turn out to be undecidable for
~~arbitrary~~ E)

Notation 17.6 There are the following methods:

1) term rewriting decides $=_E$ if $\to_E$ is convergent

2) syntactical unification computes σ such that
$\sigma(s) = \sigma(t)$

Def. 17.7 The word problem for E is the problem
of deciding $s =_E t$ for all $s, t \in T(X)$

17C Normal forms of hybrid terms of distributive lattices

Notation 17.18 We consider the set of hybrid identities of type (2,2) using the binary operation symbols $\wedge, \vee$ and the binary hypervariables F, G

(H1) $F(x, F(y,z)) = F(F(x,y),z)$

(H2) $F(x,x) = x$

(H3) $F(F(u,x), F(y,v)) = F(F(u,y), F(x,v))$

(H4) $F(G(x,y),z) = G(F(x,z), F(y,z))$

(H5) $F(x, G(y,z)) = G(F(x,y), F(x,z))$

(E1) $x \wedge y = y \wedge x, \quad x \vee y = y \vee x$

(E2) $x \wedge (y \vee x) = x \quad x \vee (y \wedge x) = x$

Proposition 17.19

An algebra L of type (2,2) is a distributive lattice if the hybrid identities H1 - H5 and E1, E2 hold.

Proof. From H1 follows the associativity

from H3 the idempotency and from H4 and H5 the distributive of the lattice operations $\wedge$ and $\vee$

Remark 17.20 The hyperidentity (H4) respectively (H5) implies:

(M1) $F(x \wedge y, z) = F(x,z) \wedge F(y,z)$
(if we hypersubstitute G by $\wedge$)

(M2) $F(x \vee y, z) = F(x,z) \vee F(y,z)$

(M3) $F(x, y \wedge z) = F(x,y) \wedge F(x,z)$

(M4) $F(x, y \vee z) = F(x,y) \vee F(x,z)$

Prop. 17.21 Every hybrid term T can be presented as a disjunction of conjunction of hyper terms

Proof. If T is a hyper term then this proposition holds. If $T = T_1 \vee T_2$ and T_1, T_2 are in dch-form then T is in dch form. If $T = T_1 \wedge T_2$ then by the distributive low T can be presented in dch-form. If $T = F(T_1, T_2)$ we apply M1-M4 to get a dch-form

Example

Consider $T = G(F(x \wedge y, z), x)$. T can be transformed in the following way:

$$G(F(x \wedge y, z), x) \xrightarrow[M1]{} G(F(x,z) \wedge F(y,z)), x)$$

$$\xrightarrow[M1]{} G(F(x,z), x) \wedge G(F(y,z), x)$$

Notation A hyper term T is called a F-hyper term respectively G-hyper term if T contains only hyper variable F or respectively G-hyper terms

Prop. 17.22 Every hyper-term T can be presented as a F-hyper-term substituted by G-hyper-term

Proof. We apply H4 and H5

Example

$$G(F(x,y), F(u,v)) \xrightarrow[H4]{} F(G(x, F(u,v)), G(y, F(u,v)))$$

$$\xrightarrow[H5]{} F(F(G(x,u), G(x,v)), F(G(y,u), G(y,v)))$$

$$\xrightarrow[H1]{} F(F(F(G(x,u), G(x,v)), G(y,u)), G(y,v))$$

Remark 17.23 As F, G are associative we write

$$F(x_1, \dots, x_n) := F(F \dots F(x_1, x_2), x_3), \dots, x_n)$$

and have

$$F(u, x_{\pi(1)}, \dots, x_{\pi(n)}, v) = F(u, x_1, \dots, x_n, v)$$

for every permutation π on $\{1, \dots, n\}$

Remark 17.24

It is clear that we can lexicographically order

the variables in F-hyperterms and G-hyper terms.
Using the lexicographic order we have a normal form for hybrid terms of distributive lattices.

17.D Unification of hybrid terms of 2-groups

Def. 17.25 A unifier of two formulas is a substitution such that the two formulas under this substitution become equal

Offcourse we consiter only terms and hybrid term

Example: A unifier of x and y is the pair of substitutions $x \to z$ and $y \to z$. We write:

$\theta := \{x \to z, y \to z\}$ or $\{x/z, y/z\}$

Def. 17.26 A hybrid substitution is a finite set $\{V_1/T_1, \dots, V_n/T_n\}$ where $V_1, \dots, V_n$ are variables or hyper variables. If V_i is a n-ary hypervariable

then T_i can be hypersubstitute by the hybrid terms.

The result θT of applying a hybrid substitution $\theta = \{V_1 | T_1, \dots, V_n | T_n\}$ to a hybrid terms can be defined recursively. We hypersubstitute the hypervariables and then substitute the variables

Example : We consider groups of exponent 2
The hybrid equation $F(x,y) + z = F(y,z)$
does not hold. We consider $\theta = \{F | *, z | 0\}$
The result is $\theta(F(x,y) * z)$ is $x * y$
and $\theta(F(y,z))$ is $y * x$

Def 17.27 A unifier of a hybrid substitution is a pair (T_1, T_2) of hybrid terms such that the hybrid identity $\theta T_1 = \theta T_2$ is satisfied

Def. 17.28 A unifier θ for a pair of hybrid terms is a most general unifier (mgu) if for each unifier σ there is a hybrid substitution λ such that $\sigma = \lambda \circ \theta$

There are only few varieties where the unification problem is explicitly solved. We use an idea of Löwenheim to study the unification in the variety of 2-groups

H1 $F(x, F(y,z)) = F(F(x,y),z)$

H2 $F^3(x,y) = F(x,y)$

H3 $F(F(u,x),F(y,v)) = F(F(u,y),F(x,v))$

M1 $F(x+y, u+v) = F(x,u) + F(y+v)$

M2 $F(0,0) = 0$

A1 $x + x = 0$

A2 $x + y = y + x$

Here we define: $F^3(x,y) := F(F(F(x,y),y),y)$

In a more general form we use $T(x_1,\dots,x_n)$ and

$\tilde{M}1$ $\quad T(x_1+y_1,\dots,x_n+y_n) = T(x_1,\dots,x_n) + T(y_1,\dots,y_n)$

$\tilde{M}2$ $\quad T(0,\dots,0) = 0$

$\tilde{H}2$ $\quad T_i^3(x_1,\dots,x_n) = T_i(x_1,\dots,x_n)$

for $T_i^3(x_1,\dots,x_n) := T(x_1,\dots,x_{i-1},T_i^2(x_1,\dots,x_n),x_{i+2},\dots,x_n)$

Instead of the unification problem for the hybrid equation $T = S$ we study the hybrid equation $T + S = 0$

These equations are equavelent:

$T = T + (S+S)$ and $(T+S)+S = 0+S = S$

Lemma 17.29 Let $T(x_1,\dots,x_n) = 0$ be a hybrid equation

Then there exists a non-trivial unifier

$$\theta = \{x_1 \mid x_1 + T_1^2(x_1,\dots,x_n), \dots, x_n \mid x_n + T_n^2(x_1,\dots,x_n)\}$$

Lemma 17.30

$\theta(\sigma)$ $\{x_i \mid x_i + \sigma T_i^2(x_1, \ldots, x_n) + \sigma T_i(0, \ldots, 0, x_i, 0, \ldots, 0)\}$

is a unifier for $\sigma T(x_1, \ldots, x_n)$

Theorem 17.31 Every unifier σ can be presented by

$$\sigma = \sigma \circ \theta(\sigma)$$

□

Prof. Dr. D. Schweigert

WS 2003/4

23.1.2004

Tutorial

Universal Algebra

Page 10

Deadline: Monday 2.2.2004

Exercise 1 Consider the variety RB of rectangular bands which is defined by $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $x \cdot x = x$, $x \cdot (y \cdot z) = x \cdot z$.

Show that this variety is solid

Exercise 2 Consider Murskii's groupoid

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

This groupoid is not finitely based

Show that this groupoid is not associative.

Exercise 3 Prove: All groupoids of two elements is finitely based (Lyndon)

Exercise 4 Is the semigroup N solid?

$N :=$ { $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $x \cdot y = x$

For a class $\mathcal{V}$ of algebras,
$\mathcal{V} \models p = q$ if $\mathcal{A} \models p = q$ for every $\mathcal{A} \in \mathcal{V}$.
For a set Σ of identities,
$\Sigma \models p = q$ if $\forall \mathcal{A}\ (\mathcal{A} \models \Sigma \Longrightarrow \mathcal{A} \models p = q)$.

Equational deduction system:

Let Σ be a set of equations;

axioms: $t = t$ and $p = q$ for $p = q \in \Sigma$;

rules:

$$\frac{p = q}{q = p}$$

$$\frac{p = q,\ q = r}{p = r}$$

$$\frac{p = q}{p(x := t) = q(x := t)}$$

$$\frac{p = q}{r(x := p) = r(x := q)}$$

For a derivable $p = q$, write $\Sigma \vdash p = q$.

COMPLETENESS THEOREM
$\Sigma \models p = q \iff \Sigma \vdash p = q$.

Prof. Dr. D. Schweigert

WS 2003/4
18.1.2004

Tutorial

Universal Algebra

Page 9

Deadline: Monday 26.1.2004

Exercise 1 Commutator on lattices

a) Show that the lattice M_3 and M_n, $n \geq 3$, (the projective line) is nilpotent

b) Show that the lattice M_{33} is nilpotent

Exercise 2

a) Show that the lattice D_2^* is join-semi-distributive

b) D_2^* is not distributive

Exercise 3 Construct an example of an ultra-product with three indices

Exercise 4 Definition: A lattice $\mathcal{L}$ is called a pappian lattice if the following condition (P) holds in $\mathcal{L}$

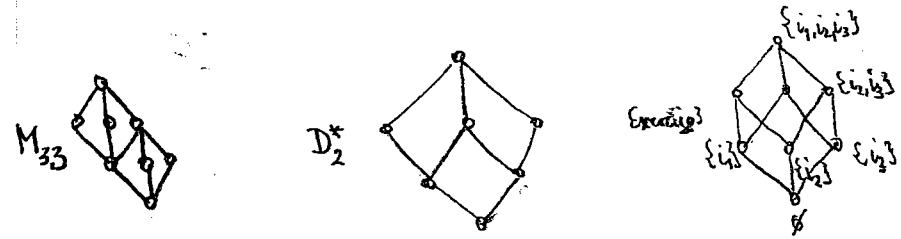
Pappos: (P):

$$[x_2 \vee (x_4 \wedge (x_5 \vee x_6))] \wedge [x_5 \vee (x_1 \wedge (x_2 \vee x_3))] \leq$$

$$\{[x_3 \vee (x_4 \wedge (x_5 \vee x_6))] \wedge [x_6 \vee (x_1 \wedge (x_2 \vee x_3))]\} \vee [(x_3 \vee x_5) \wedge (x_2 \vee x_6)]$$

Show: The lattice of Pappos is modular

Illustration



Pappos (From the book: H. Lüneburg: Die euklidische Ebene und ihre Verwandten Birkhäuser 1998)

1.1. Definition. Die projektive Ebene Π heißt *pappossch*, falls gilt: Sind a und b zwei verschiedene Geraden von Π, sind A_1, A_2, A_3 drei verschiedene Punkte auf a und B_1, B_2, B_3 drei verschiedene Punkte auf b und gilt A_i, $B_i \neq a \cap b$ für alle i, so sind die Punkte $(A_1+B_2)\cap(B_1+A_2)$, $(A_2+B_3)\cap(B_2+A_3)$, $(A_3+B_1)\cap(B_3+A_1)$ kollinear.

Fig. 20 zeigt die gegenseitige Lage der Punkte und Geraden der pappusschen Konfiguration.

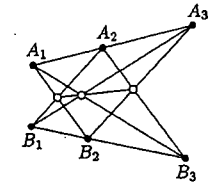


Fig. 20

Die Definition der pappusschen Ebenen wird nachträglich motiviert durch den Beweis des nun folgenden Satzes.

1.2. Satz. Ist Δ eine desarguessche projektive Ebene, so sind die folgenden Bedingungen äquivalent:

a) Der Koordinatenkörper von Δ ist kommutativ.

b) Es gibt ein nicht inzidentes Punkt-Geradenpaar (Q, h) in Δ, so daß $\Gamma(Q, h)$ abelsch ist.

c) Es ist $\Gamma(P, g)$ abelsch für alle Punkt-Geradenpaare (P, g) von Δ.

d) Δ ist pappossch.

Prof. Dr. D. Schweigert

WS 2003/4
10.1.2004

Tutorial
Universal Algebra
Page 8

Deadline: Monday, 19.1.2004

Exercise 1 Consider the dihedral group (Diedergruppe) G which is defined by $a^3 = e$, $b^2 = e$ and $ba = a^2 b$

a) Show that the group is not abelian
b) There is a normal subgroup (Normalteiler) of order 3
c) G is solvable

Exercise 2 Prove
An algebra A satisfies the term condition if and only if
A satisfies the term condition for congruences
$C(\alpha, \beta, \delta)$

Exercise 3 The even permutations on $x_1, x_2, \ldots, x_n$ forms a normal subgroup. (This group is called the alternative group A_n) (see M. Hall Theory of Groups page 59)

Exercise 4 The alternative group A_5 is simple and is not solvable

(Remark. Galois and Abel have shown that the polynomial equation in degree $5 \geq n$ is not solvable by radicals)

*The only existing authentic portrait of **Niels Henrik Abel**, drawn by Gørbitz in Paris in 1826.*

Niels Henrik Abel: A short but influential life

Niels Henrik Abel (1802-1829) had a difficult childhood. He was the second of six children where the eldest was mentally handicapped. His father died when Niels was 18 leaving the family heavily in debt, and Abel was to struggle financially throughout his life.

In Berlin, he met August Crelle, a self- taught mathematician and civil engineer. Crelle was just starting his Journal für die Reine und Angewandte Mathematik [Journal for Pure and Applied Mathematics] which gave Abel and other young, promising academics the opportunity to publish their work. Crelle was a major inspiration for Abel and became a firm friend and support. Abel wrote six pieces for the journal in three months, all of which were first class - some proved very important in the history of mathematics.

Despite being unwell when he was to visit his fiancée at Frolands Verk for the Christmas of 1828, Abel braved the cold, putting on everything he had and setting off with a horse and sleigh. He celebrated Christmas in good spirits but was confined to his bed when the time came for the return journey. He died of tuberculosis on 6 April 1829. A letter from Crelle in Berlin dated two days later contained the

following message, "The Ministry of Education has decided to call you back to Berlin and offer you employment here".

Prof. Dr. D. Schweigert

WS 2003/4

21.1.2004

Tutorial

Universal Algebra

Page 4

D

Exercise 1: Let $\underline{G} = (G; \cdot, ^{-1}, e)$ be a group

Show that the commutator $[x,y] := x^{-1}y^{-1}xy$ has the following properties:

$[y,x] = [x,y]^{-1}$

$[x \cdot y, z] = [x,z]\,[x,[z,y]]\,[y,z]$

(Remark: $[x_1,\dots,x_n] := [[x_1,\dots,x_{n-1}],x_n]$)

Exercise 2. Let V be a variety of rings generated by finitely many finite fields

Show that V is arithmetical

Exercise 3 A two-element algebra $\underline{A}$ is permutable if the operation p with $p(x,y,z) = x+y+z$ is a term operation of $\underline{A}$

Exercise 4. The following two statements are equivalent for normal subgroups $\underline{M}$ and $\underline{N}$ of a group $\underline{G}$

1) $ab = ba$ for all $a \in M$ and $b \in N$

2) $\underline{G}$ satisfies term condition with respect to (θ_M, θ_N)

Galois, Évariste (1811-1832)

French mathematician who developed new techniques to study the solubility of equations which are now called group theory. Simultaneously with Abel, he showed that the general quintic equation and polynomial equations of higher degree are not soluble in terms of a finite number of rational operations and root extractions.

Galois's life was a tragic one. His father committed suicide. Galois himself regularly failed his exams in school while he concentrated on reading Legendre's *Geometry* cover to cover.

Galois suffered the additional misfortune of having his work not only ignored, but completely misplaced by its caretakers on several occasions. When Galois gave Cauchy a paper containing his most important results to present (without keeping a copy himself), Cauchy proceeded to lose it (Infeld 1948, pp. 89-90). When Galois submitted a paper for the Académie's prize in math, Fourier took the paper home to peruse, but died shortly thereafter and this paper was also lost. Poisson returned a second paper which contained important results in group theory as incomprehensible.

Galois, always a radical, joined the National Guard, but was subsequently imprisoned in 1831 after proposing a toast interpreted as a threat to the King. On the night before his death in 1832, Galois wrote a letter to his friend Auguste Chevalier, setting forth his discovery of the connection between group theory and the solutions of polynomial equations by radicals (Galois 1959). After writing the letter, Galois was shot to death in his intestine in a gun fight. The exact circumstances of his death are not well established, and various accounts hold that he was shot by a rival in a feud over a woman, that he was challenged by a royalist who objected to his political views, or that he was killed by an agent of the police.

Prof. Dr. D. Schweigert

WS 2003/4

12.12.2003

Tutorial

Universal Algebra

Page 6

Deadline Monday 5.1.2004

Exercise 1 The free vector space $F_{V(K)}(n)$ is isomorphic to the n-dimensional vector space $(K^n; +, -, 0, K)$

Exercise 2 Every group G given as generated by a set X is the factor group of a free group F with the same number of generators

[Marshall Hall, The Theory of Groups, Macmillan, 1965 page 93]

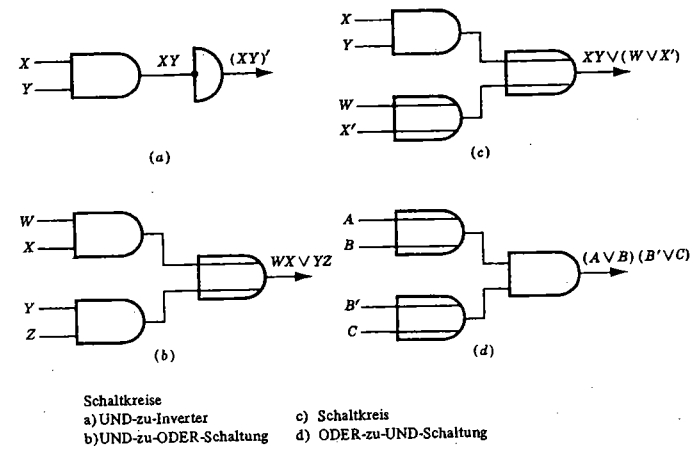
Exercise 3 Let $B_2 = (\{0,1\}; \wedge, \vee, ', 0, 1)$ the two-element Boolean algebra. Show:
Every term-function $f: \{0,1\}^n \to \{0,1\}$ and every $x_1, \dots, x_n \in \{0,1\}$

$$f(x_1, \dots, x_n) = \bigwedge \{ (x_1^{a_1} \vee \dots \vee x_n^{a_n}) \mid f(a_1, \dots, a_n) = 0 \}$$

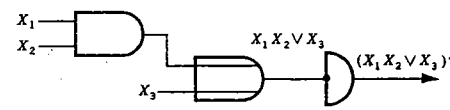
We put: $x^a := \begin{cases} x & \text{for } a = 0 \\ x' & \text{for } a = 1 \end{cases}$ $\quad (a_1, \dots, a_n) \in \{0,1\}^n$

The presentation of the term function f is called conjuntive normal form

[Birkhoff Bartee Applied Algebra]



Schaltkreise
a) UND-zu-Inverter
b) UND-zu-ODER-Schaltung
c) Schaltkreis
d) ODER-zu-UND-Schaltung



Eingangssignale

X_1	X_2	X_3	X_1X_2	$X_1X_2 \vee X_3$	$(X_1X_2 \vee X_3)'$
0	0	0	0	0	1
0	0	1	0	1	0
0	1	0	0	0	1
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	1	0
1	1	0	1	1	0
1	1	1	1	1	0

Prof. Dr. D. Schweigert

WS 2003/4

3.12.2003

Tutorial

Universal Algebra

Page 5

Deadline: Monday 15.12.2003

Exercise 1 Let $\underset{\sim}{G} = (G; \cdot, ^{-1}, e)$ be the Klein's group:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

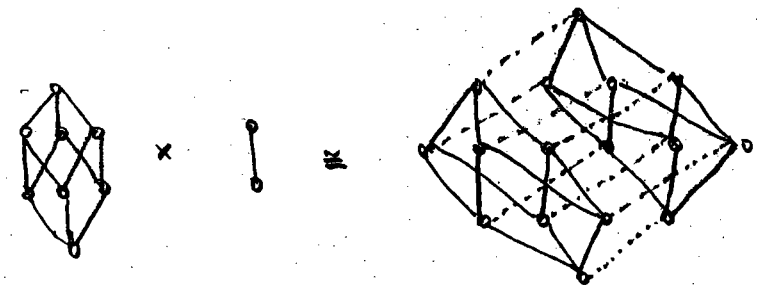
Show that $\underset{\sim}{G}$ is a direct product of $G_1 \times G_2$ with $G_1 = (\{e,a\}; \cdot, ^{-1}, e)$ and $G_2 = (\{e,b\}; \cdot, ^{-1}, e)$

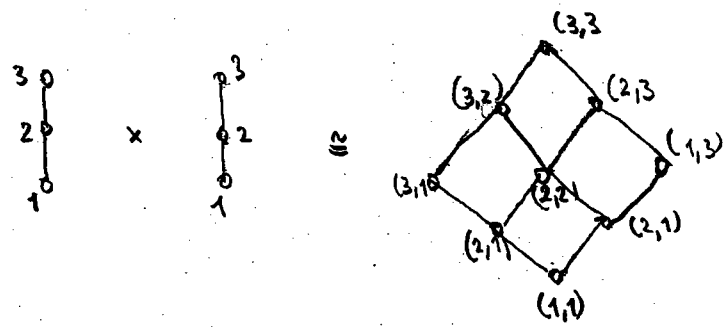
Exercise 2 Let $\underset{\sim}{G}$ be a group of order 6. Show that $\underset{\sim}{G}$ is isomorphic to a direct product of the group G_1 of order 3 and G_2 of order 2

Exercise 3 The lattice $(C_3; \wedge, \vee)$ is subdirectly irreducible

Exercise 4. Show that the ring $(\mathbb{Z}_6; +, -, 0, \cdot, 1)$ is isomorpic to a direct product of $\underset{\sim}{\mathbb{Z}}_3$ and $\underset{\sim}{\mathbb{Z}}_2$.

Examples of a direct product





Remark: There are two groups of order 6 which is not isomorphic. One is abelian, the other is not-abelian

Prof. Dr. D. Schweigert

WS 2003/4

28.11.2003

Tutorial

Universal Algebra

Page 4

Deadline: Monday 8.12.2003

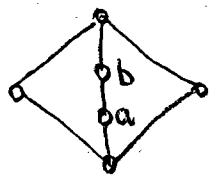
Exercise 1 Let $\underline{A}$ be an algebra with a term $t(x,y,z)$ which fulfills the equations:

$$t(x,x,z) = t(z,x,x) = t(z,x,z) = z$$

Show that the algebra $\underline{A}$ has permutable and distributive congruences

Exercise 2 Show that the pair (a,b) of the lattice $\underline{L}_4$ generates a not trivial congruence relation

$\underline{L}_4$



Exercise 3 Let $\underline{B} = (B; \wedge, \vee, ', 0, 1)$ be an Boolean algebra. Let θ be a congruence relation

(That means: $\theta \subseteq B \times B$ is an equivalence relation and is compatible by the operations $\wedge, \vee, '$)

Show that for every congruence θ

there exists a congruence ς such that

i) $\theta \vee \varsigma = \nabla$

ii) $\theta \wedge \varsigma = \Delta$

iii) $\theta \circ \varsigma = \varsigma \circ \theta$

Exercise 4 Let θ be an equivalence relation on the lattice $\underline{L}$.

Prove: θ is congruence relation if

from $(a,b) \in \theta$ it follows $(a \wedge b, a \vee b) \in \theta$

Prof. Dr. D. Schweigert

WW 2003/2004

19.11.2003

Tutorial

Universal Algebra

Page 3

Deadline: Monday 1.12.2003

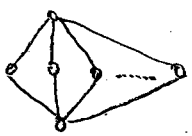
Def. 7.1 An algebra $\underset{\sim}{A}$ is simple if the congruence lattice $\mathrm{Con}\underset{\sim}{A}$ consists only the trivial congruences namely the identity relation Δ and the all relation ∇.

Exercise 1 Show that a field is a simple algebra

Exercise 2 Let V be vector-space and L(V) the lattice of subspaces. Show that L(V) is simple.

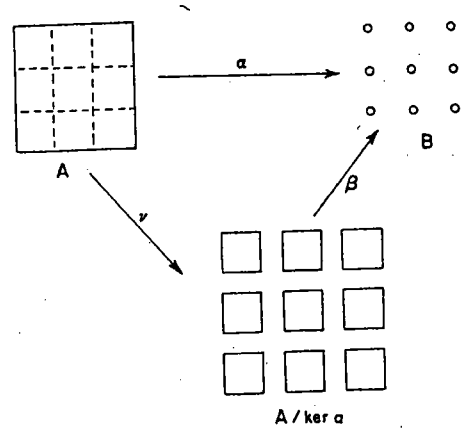
Exercise 3 Show that a cyclic group of the order of prime number is simple.

Exercise 4 The lattice M_n is simple



M_n

Theorem . (Homomorphism Theorem). *Suppose $\alpha: \mathbf{A} \to \mathbf{B}$ is a homomorphism onto B. Then there is an isomorphism β from $\mathbf{A}/\ker(\alpha)$ to $\mathbf{B}$ defined by $\alpha = \beta \circ \nu$, where ν is the natural homomorphism from $\mathbf{A}$ to $\mathbf{A}/\ker(\alpha)$.*



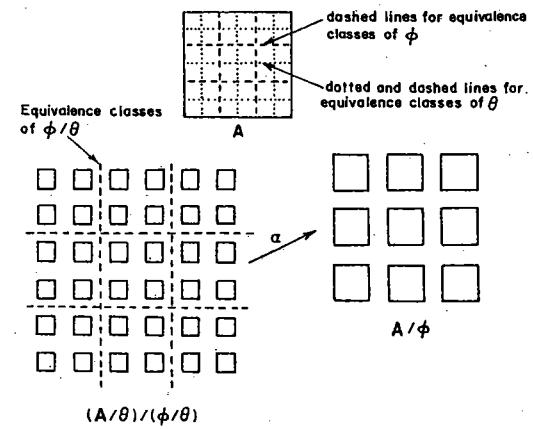
Theorem . (Second Isomorphism Theorem). *If $\phi, \theta \in \mathrm{Con}\,\mathbf{A}$ and $\theta \subseteq \phi$, then the map*

$$\alpha: (A/\theta)/(\phi/\theta) \to A/\phi$$

defined by

$$\alpha((a/\theta)/(\phi/\theta)) = a/\phi$$

is an isomorphism from $(\mathbf{A}/\theta)/(\phi/\theta)$ to $\mathbf{A}/\phi$.



Prof. Dr. D. Schweigert

WW 2003/2004

16.11.2003

Tutorial

Universal Algebra

Page 2

Deadline: Monday 24.11.2001 Mailbox: D. Schweigert or Hr. Müller

Exercise 1 Show that

a) every sublattice of a distributive lattice is again distributive

b) every sublattice of a modular lattice is again modular

c) the lattice of a chain (= linear ordered set) is distributive

Exercise 2 A group $\underset{\sim}{G} = (G; \cdot, ^{-1}, e)$ is cyclic if $\underset{\sim}{G}$ is generated only by one element

(Example

	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a_2	e	a

)

a) Present the Hasse diagram for the subgroups of cyclic group of order 4.

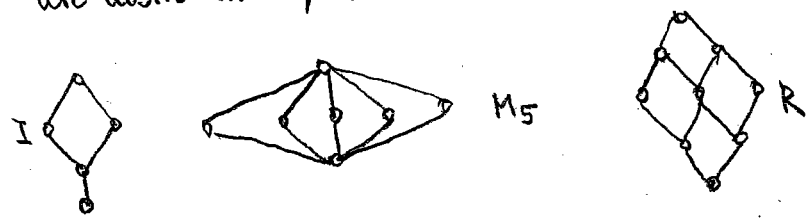
b) Present the Hasse diagram for all subgroups of a cyclic group of order p, p a prime number

Exercise 3 a) Show that there exists a homomorphic map from the ring $(\mathbb{Z}/\mathbb{Z}6; +, -, 0, \cdot, 1)$ into $(\mathbb{Z}/\mathbb{Z}3; +, -, 0, \cdot, 1)$

b) Show that there exist a homomorphism map from the Kleinean group to the group of order 2

c) Show that there exists a homorphism from the Boolean algebra $(\{0,1\}^3; \wedge, \vee, ', \bar{0}, \bar{1})$ into $(\{0,1\}; \wedge, \vee, ', \bar{0}, \bar{1})$

Exercise 4 Which lattices (given by the Hasse diagram) are distributive and which are modular?



Prof. Dr. D. Schweigert WW 2003/2004

4.11.03

Tutorial
Universal Algebra
Page 1

Deadline: Monday 17.11.2003 Mailbox D. Schweigert or Mr. Müller

Exercise 1 A distributive lattice $(L; \wedge, \vee)$ is a lattice which fulfills the distributive identity:

D1 $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Prove that D1 implies D2: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Exercise 2 The poset of all divisors of the number n is a lattice $(D(n); \wedge, \vee)$. If k_1, k_2 are divisors then $k_1 \wedge k_2$ is the greatest common divisor and $k_1 \vee k_2$ is the least common multiplies

Draw the Hasse diagram for the number 30
$(D(30); \wedge, \vee)$

Exercise 3 Let L be a lattice and $\leq$ its induced order. For $a, b, c, d \in L$ it holds

i) $a \wedge b \leq a \leq a \vee b$

ii) if $a \leq b$ then $a \wedge c \leq b \wedge c$

iii) if $a \leq b$ then $a \vee c \leq b \vee c$

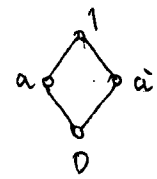
Exercise 4 Let $\underset{\sim}{L}$ be a lattice and let $\underset{\sim}{A}_i$ be sublattices of $\underset{\sim}{L}$ for $i \in I$.

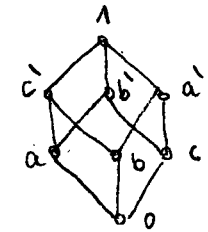
If $\cap \{A_i \mid i \in I\} = A$ then $\underset{\sim}{A}$ is also a sublattice

Remarks Let $\underset{\sim}{L}$ be a distributive lattice with 0 and 1

Then every element of L has exactly one complement.

Examples





Remark Let $\underset{\sim}{L}$ be complemented lattice. It is equivalent

i) $x \leq y$ implies $y' \leq x'$

ii) L satisfies the De Morgan laws
$x' \wedge y' = (x \vee y)'$ and $x' \vee y' = (x \wedge y)'$