SVAZY

Pologrupa: $(S,\cdot)$, kde S je množina a $\cdot : S\times S \to S$ asociativní binární operace.

Polosvaz (semilattice) = komutativní a idempotentní pologrupa, tj.

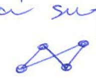
$\forall a,b,c\in S$: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$, $a\cdot b = b\cdot a$, $a\cdot a = a$.

Ukážeme si, že na polosvazy se dá dívat jako na jisté uspořádané množiny.

Definice: $(S,\le)$ uspořádaná množina, $a,b\in S$. Pokud existuje nejmenší horní závora prvků $\underline{a},\underline{b}$, nazýváme ji __supremem__ $\underline{a}$ a $\underline{b}$ a značíme $a\vee b$. (je určeno jednoznačně)

Vlastnosti definující supremum tedy jsou: $a\le a\vee b$, $b\le a\vee b$, $\forall c\in S$: $((a\le c \,\&\, b\le c) \Rightarrow a\vee b\le c)$.

opačná implikace platí automaticky

Příklad:  vs.  vs.  ($\mathbb{N}$ se dvěma ∞)

Největší dolní závora prvků a,b se nazývá __infimum__ $\underline{a}$ a $\underline{b}$ a značí $a\wedge b$.

Takže: $a\wedge b\le a$, $a\wedge b\le b$, $\forall c\in S$: $((c\le a \,\&\, c\le b)\Rightarrow c\le a\wedge b)$.

Mají-li každé 2 prvky v uspořádané množině $(S,\le)$ supremum, dostáváme binární operaci $\vee$ na S (spojení, join) a $(S,\le)$ nazýváme __spojový polosvaz__. Mají-li každé 2 prvky v $(S,\le)$ infimum, dostáváme operaci $\wedge$ (průsek, meet) a $(S,\le)$ nazýváme __průsekový polosvaz__.

Tvrzení: Je-li $(S,\le)$ spojový polosvaz, tak $(S,\vee)$ je polosvaz a platí:

$\forall a,b\in S$: $a\le b \Leftrightarrow a\vee b = b$.

Důkaz: vše zřejmé, kromě asociativity $\vee$:

$(a\vee b)\vee c\ge c$, $(a\vee b)\vee c\ge a\vee b\ge b \Rightarrow (a\vee b)\vee c\ge b\vee c$

$(a\vee b)\vee c\ge a\vee b\ge a \Rightarrow (a\vee b)\vee c\ge a\vee(b\vee c)$

Analogicky se dokáže $(a\vee b)\vee c\le a\vee(b\vee c)$. Antisymetrie $\Rightarrow (a\vee b)\vee c = a\vee(b\vee c)$.

Tvrzení: Je-li $(S,\cdot)$ polosvaz, tak předpis $a\le b :\Leftrightarrow a\cdot b = b$, pro $a,b\in S$, definuje na S uspořádání t.ž. pro všechna $a,b\in S$ je $a\cdot b$ supremem $\underline{a}$ a $\underline{b}$.

Důkaz: refl.: $a\cdot a = a \Rightarrow a\le a$

antisym.: $a\le b$, $b\le a \Rightarrow b = a\cdot b = b\cdot a = a$

tranzit.: $a\le b$, $b\le c \Rightarrow a\cdot b = b$, $b\cdot c = c \Rightarrow a\cdot c = a(b\cdot c) = (a\cdot b)\cdot c = b\cdot c = c \Rightarrow a\le c$

$a\cdot b$ je horní závora $\underline{a}$ a $\underline{b}$: $a\cdot(a\cdot b) = (a\cdot a)\cdot b = a\cdot b \Rightarrow a\le a\cdot b$

$b\cdot(a\cdot b) = b\cdot(b\cdot a) = (b\cdot b)\cdot a = b\cdot a = a\cdot b \Rightarrow b\le a\cdot b$

je nejmenší: $c\ge a$, $c\ge b \Rightarrow a\cdot c = c$, $b\cdot c = c \Rightarrow (a\cdot b)\cdot c = a\cdot(b\cdot c) = a\cdot c = c \Rightarrow c\ge a\cdot b$.

Předchozí tvrzení určují pro každou množinu S vzájemně inverzní bijekce mezi množinami $\{\le\ \subseteq S\times S \mid (S,\le)$ je spojový polosvaz$\}$ a $\{\cdot : S\times S\to S \mid (S,\cdot)$ je polosvaz$\}$.

$\le\ \longmapsto \vee \longmapsto \le'$, přičemž $a\le' b \Leftrightarrow a\vee b = b \Leftrightarrow a\le b$.

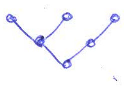
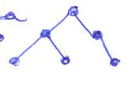
$\cdot \longmapsto \le\ \longmapsto \vee = \cdot$

Polosvazy a spojové polosvazy jsou tedy v podstatě dva různé popisy stejných struktur. Bývá výhodné používat oba popisy současně.

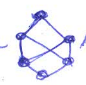
Dualita: suprema v $(S,\le)$ jsou infima v $(S,\ge)$.

Proto můžeme polosvazy chápat i jako průsekové polosvazy, kde $a\cdot b$ je infimum $\underline{a}$ a $\underline{b}$.

Polosvazy jsou vlastně abstrakce spojových i průsekových polosvazů, kde nemáme uvedeno, zda $\cdot$ reprezentuje $\vee$ nebo $\wedge$.

 $\xleftrightarrow{\text{dualita}}$  (tentýž polosvaz reprezentovaný jako průsekový a spojový polosvaz)

Definice: __Svazově uspořádaná množina__ je uspořádaná množina, v níž ke každým dvěma prvkům existuje supremum i infimum, tj. je současně spojovým a průsekovým polosvazem.

Příklady: lineárně uspořádané množiny. $(\mathbb{N}, |)$: $\vee = \mathrm{lcm}$, $\wedge = \gcd$. , ale  není.

Jako pro polosvazy, existuje algebraický popis.

Definice: __Svaz__ (lattice) je $(L,\vee,\wedge)$, kde $(L,\vee)$ a $(L,\wedge)$ jsou polosvazy a platí absorpční zákony:

$\forall a,b\in L$: $a\wedge(a\vee b) = a$, $a\vee(a\wedge b) = a$.

Tvrzení: Je-li $(L,\le)$ svazově uspořádaná množina, je $(L,\vee,\wedge)$ svaz a platí: $\forall a,b\in L$:

$a\le b \Leftrightarrow a\wedge b = a \Leftrightarrow a\vee b = b$.

Důkaz: Vše plyne z tvrzení o polosvazech, až na absorpce, které jsou jasné.

Tvrzení: Je-li $(L,\vee,\wedge)$ svaz, tak předpis $a\leq b :\Leftrightarrow a\vee b = b$, pro $a,b\in L$, definuje na L uspořádání takové, že pro všechna $a,b\in L$ je $a\vee b$ jejich supremem a $a\wedge b$ jejich infimem.

Důkaz: Pro suprema víme z tvrzení pro polosvazy.

Dokážeme, že platí $a\leq b \Leftrightarrow a\wedge b = a$:

$a\leq b \Rightarrow a\vee b = b \Rightarrow a = a\wedge(a\vee b) = a\wedge b$

$a\wedge b = a \Rightarrow b = (a\wedge b)\vee b = a\vee b \Rightarrow a\leq b$

Takže z tvrzení pro polosvazy dostáváme i tvrzení pro infima.

Takže máme 2 ekvivalentní možnosti, jak popisovat svazy. Bývá výhodné pracovat s oběma formalismy současně, tzn. používat $\leq$ i pravidla pro počítání s $\vee$ a $\wedge$.

Dualita: ~~Pokud~~ $(L,\leq)$ odpovídá $(L,\vee,\wedge)$, tak $(L,\geq)$ odpovídá $(L,\wedge,\vee)$.

Přitom užitečná vlastnost svazů kombinující $\leq$ s $\vee$ a $\wedge$ je monotonie, tj. $\forall a,b,c,d\in L: (a\leq b \,\&\, c\leq d)\Rightarrow (a\vee c\leq b\vee d \,\&\, a\wedge c\leq b\wedge d)$.

Definice: $(L,\vee,\wedge)$ svaz. Podmnožina $M\subseteq L$ je podsvaz L, jestliže $\forall a,b\in M: a\vee b\in M \,\&\, a\wedge b\in M$, tj. M je podpologrupa $(L,\vee)$ i $(L,\wedge)$.

Příklady: $\emptyset$, L, všechny jednoprvkové podmnožiny.

$\{a,b\}\subseteq L$ je podsvaz $\Leftrightarrow$ a,b jsou srovnatelné.

Uspořádaná podmnožina, která je svaz, nemusí být podsvaz: 

Tvrzení: $I\neq\emptyset$, M_i pro $i\in I$ podsvazy svazu $(L,\vee,\wedge)$. Pak $\bigcap_{i\in I} M_i$ je také jeho podsvaz.

Důkaz: $a,b\in\bigcap_{i\in I} M_i \Rightarrow \forall i\in I: a,b\in M_i \Rightarrow \forall i\in I: a\vee b, a\wedge b\in M_i \Rightarrow a\vee b, a\wedge b\in\bigcap_{i\in I} M_i$

Důsledek: $(L,\vee,\wedge)$ svaz, $K\subseteq L$ podmnožina. Potom existuje vzhledem k inkluzi nejmenší podsvaz L obsahující K, a to $\bigcap\{M \mid M \text{ podsvaz } L, K\subseteq M\}$. Nazýváme jej podsvaz generovaný K.

Generování podsvazů je divoké: $K=\emptyset$ generuje $\emptyset$, 1-prvková K generuje 1-prvkový, 2-prvková 2-prvkový nebo 4-prvkový, ale 3-prvková může generovat nekonečný.

Definice: $(L,\leq)$, $(M,\sqsubseteq)$ uspořádané množiny. Zobrazení $\varphi: L\to M$ nazýváme izotonní, jestliže $\forall a,b\in L: a\leq b \Rightarrow \varphi(a)\sqsubseteq\varphi(b)$.

Izomorfismus uspořádaných množin = izotonní bijekce φ t. ž. φ^{-1} je také izotonní.

Příklad izotonní bijekce svazů, která není izomorfismus: 

Definice: $(L,\vee,\wedge)$, $(M,\bar\vee,\bar\wedge)$ svazy. Zobrazení $\varphi: L\to M$ nazýváme homomorfismus svazů, jestliže $\forall a,b\in L: \varphi(a\vee b) = \varphi(a)\bar\vee\varphi(b)$, $\varphi(a\wedge b) = \varphi(a)\bar\wedge\varphi(b)$.

Izomorfismus svazů = bijektivní homomorfismus.

Tvrzení: Je-li $\varphi: L\to M$ izomorfismus svazů, je φ^{-1} také izomorfismus.

Důkaz: $c,d\in M$ lib. Pak $\varphi^{-1}(c\bar\vee d) = \varphi^{-1}(\varphi(\varphi^{-1}(c))\bar\vee\varphi(\varphi^{-1}(d))) = \varphi^{-1}(\varphi(\varphi^{-1}(c)\vee\varphi^{-1}(d))) = \varphi^{-1}(c)\vee\varphi^{-1}(d)$ a analog. pro $\wedge$.

Tvrzení: $\varphi: L\to M$ homomorfismus svazů, $N\subseteq L$ podsvaz. Pak $\varphi(N)$ je podsvaz M.

Důkaz: $c,d\in\varphi(N)$ lib. Pak $\exists a,b\in N: \varphi(a)=c, \varphi(b)=d$. Tedy $\varphi(N)\ni\varphi(a\vee b) = \varphi(a)\bar\vee\varphi(b) = c\bar\vee d$. analog. pro $\wedge$.

Tvrzení: Je-li $\varphi: L\to M$ homomorfismus svazů, pak je φ izotonní zobrazení přísl. uspoř. množin $(L,\leq)$ a $(M,\sqsubseteq)$.

Důkaz: $a\leq b \Rightarrow a\vee b = b \Rightarrow \varphi(a)\bar\vee\varphi(b) = \varphi(a\vee b) = \varphi(b) \Rightarrow \varphi(a)\sqsubseteq\varphi(b)$.

Viděli jsme, že opačná implikace neplatí!

Tvrzení: L, M svazy, $\varphi: L\to M$ zobrazení. Pak φ je izomorfismus svazů $\Leftrightarrow$ φ je izomorfismus uspořádaných množin.

Důkaz: "$\Rightarrow$" φ a φ^{-1} jsou homom. $\Rightarrow$ jsou izotonní.

"$\Leftarrow$" Předp., že φ je izom. uspoř. množin. Chceme ukázat $\varphi(a\vee b) = \varphi(a)\bar\vee\varphi(b)$. (pro $\wedge$ analog.)

1) $\varphi(a\vee b)$ je horní závora $\varphi(a)$, $\varphi(b)$: $a\leq a\vee b \Rightarrow \varphi(a)\sqsubseteq\varphi(a\vee b)$, $b\leq a\vee b \Rightarrow \varphi(b)\sqsubseteq\varphi(a\vee b)$.

2) je nejmenší: $c\in M$ lib. t. ž. $\varphi(a)\sqsubseteq c$, $\varphi(b)\sqsubseteq c$. Pak $a = \varphi^{-1}(\varphi(a))\leq\varphi^{-1}(c)$, $b = \varphi^{-1}(\varphi(b))\leq\varphi^{-1}(c)$, takže $a\vee b\leq\varphi^{-1}(c)$. Proto $\varphi(a\vee b)\sqsubseteq\varphi(\varphi^{-1}(c)) = c$.

(Bývá daleko jednodušší dokázat, že je to izomorfismus uspoř. množin, než izomorfismus svazů.)

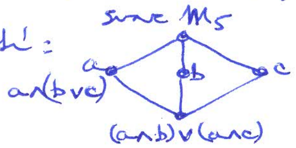
Součin svazů L a M: Na $L\times M$ operace definované po složkách, tj. pro $a,b\in L$, $c,d\in M$: $(a,c)\vee(b,d) = (a\vee b, c\vee d)$, $(a,c)\wedge(b,d) = (a\wedge b, c\wedge d)$. Takto definovaný svaz odpovídá součinu uspoř. množin $(L,\leq)$, $(M,\sqsubseteq)$, kde $(a,c)\leq(b,d) \Leftrightarrow a\leq b \,\&\, c\leq d$. Příklad: 

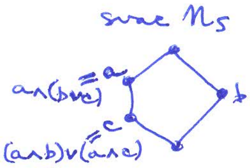
DISTRIBUTIVNÍ A MODULÁRNÍ SVAZY

Tvrzení: $(L,\vee,\wedge)$ svaz. Pak platí: $\forall a,b,c\in L$: $(a\wedge b)\vee(a\wedge c)\leq a\wedge(b\vee c)$
$(a\vee b)\wedge(a\vee c)\geq a\vee(b\wedge c)$. (distributivní nerovnosti)

Důkaz: $(a\wedge b)\vee(a\wedge c)\leq a\wedge(b\vee c) \iff (a\wedge b\leq a\wedge(b\vee c)\ \&\ a\wedge c\leq a\wedge(b\vee c)) \iff$
$\iff (a\wedge b\leq a\ \&\ a\wedge b\leq b\vee c\ \&\ a\wedge c\leq a\ \&\ a\wedge c\leq b\vee c)$, což platí. (2. nerovnost je symetrická)

Opačné nerovnosti obecně neplatí:





Definice: Svaz $(L,\vee,\wedge)$ nazýváme <u>distributivní</u>, jestliže $\forall a,b,c\in L$: $(a\wedge b)\vee(a\wedge c)=a\wedge(b\vee c)$ & $(a\vee b)\wedge(a\vee c)=a\vee(b\wedge c)$.

Tvrzení: Svaz $(L,\vee,\wedge)$ je distributivní $\iff \forall a,b,c\in L$: $(a\wedge b)\vee(a\wedge c)=a\wedge(b\vee c) \iff$
$\iff \forall a,b,c\in L$: $(a\vee b)\wedge(a\vee c)=a\vee(b\wedge c)$.

Důkaz: Stačí ukázat "$\Rightarrow$" v 2. ekvivalenci, "$\Leftarrow$" plyne z duality a zbytek je zřejmý.

$$(a\vee b)\wedge(a\vee c)=\big(\underline{(a\vee b)\wedge a}\big)\vee\big(\underline{(a\vee b)\wedge c}\big)=\underline{a\vee\big((a\wedge c)}\vee(b\wedge c)\big)=a\vee(b\wedge c).$$

Příklad: A lib. množina. Pak $(\mathcal{P}(A),\cup,\cap)$, tj. $(\mathcal{P}(A),\subseteq)$, je distrib. svaz.

Tvrzení: Pro každý svaz $(L,\vee,\wedge)$ platí: $\forall a,b,c\in L$: $c\leq a \Rightarrow (a\wedge b)\vee c\leq a\wedge(b\vee c)$.

Důkaz: plyne z 1. distrib. nerovnosti.

Definice: Svaz $(L,\vee,\wedge)$ nazýváme <u>modulární</u>, jestliže $\forall a,b,c\in L$: $c\leq a \Rightarrow (a\wedge b)\vee c=a\wedge(b\vee c)$.
(nezáleží na pořadí, v jakém děláme průsek s větším a spojení s menším)

Definiční podmínka je samoduální.

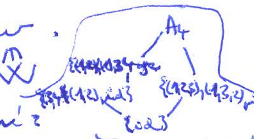
N_5 není modulární. Každý distributivní svaz je modulární, M_5 je modulární.

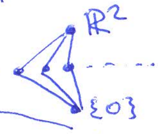
L je modulární $\iff \forall a,b,c\in L$: $(a\wedge b)\vee(a\wedge c)=a\wedge(b\vee(a\wedge c))$. (jsou tedy definovány rovností)

Příklady: Svaz všech podprostorů vektorového prostoru V je modulární, ale nemusí být distributivní: T,U,W podprostory V, $W\subseteq T$. Chceme ukázat, že $(T\cap U)+W\supseteq T\cap(U+W)$.

Buď $v\in T\cap(U+W)$ lib. Pak $v=u+w$, kde $u\in U$, $w\in W\subseteq T$. Tedy $u=v-w\in T$.

Máme tedy $v=u+w$.
$\overset{\cap}{T\cap U}\ \ \overset{\cap}{W}$





(nespočetně) nekonečně mnoho jednorozměrných podprostorů

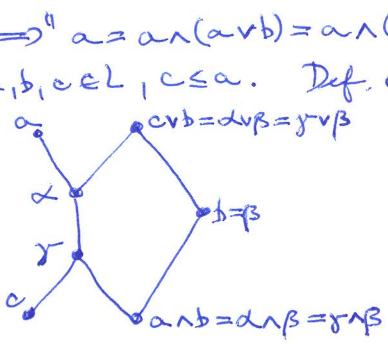
Svaz podgrup grupy S_4 není modulární:

Podsvazy, homomorfní obrazy a součiny distributivních svazů jsou distributivní, a totéž platí pro modularitu.

Tvrzení: Svaz L je modulární $\iff \forall a,b,c\in L$: $(c\leq a\ \&\ a\wedge b=c\wedge b\ \&\ a\vee b=c\vee b)\Rightarrow a=c$.

Důkaz: "$\Rightarrow$" $a=a\wedge(a\vee b)=a\wedge(b\vee c)=(a\wedge b)\vee c=(c\wedge b)\vee c=c$.

"$\Leftarrow$" $a,b,c\in L$, $c\leq a$. Def. $\alpha=a\wedge(b\vee c)$, $\beta=b$, $\gamma=(a\wedge b)\vee c$. Pak $\gamma\leq\alpha$ díky modulární nerovnosti. Z monotonie máme $\gamma\wedge\beta\leq\alpha\wedge\beta$.



Dále $\alpha\wedge\beta=\underline{(a\wedge(b\vee c))\wedge b}=a\wedge b\leq\gamma\wedge\beta$. Takže $\alpha\wedge\beta=\gamma\wedge\beta$. $\underset{a\wedge b}{\shortparallel}$

Ze symetrie máme i $\alpha\vee\beta=\gamma\vee\beta=c\vee b$.

Podle předpokladu platí $\alpha=\gamma$, což je definiční podmínka modularity.

Věta: Svaz je modulární $\iff$ neobsahuje podsvaz izomorfní N_5. (modulární svazy mají potřebnou strukturu respektovanou $\wedge$ a $\vee$. (dimenze podprostorů))

Důkaz: "$\Rightarrow$" N_5 není modulární, takže není podsvazem modulárního.

"$\Leftarrow$" Není-li L modulární, tak existují $a,b,c\in L$ t.ž. $c\leq a$, $a\wedge b=c\wedge b$, $a\vee b=c\vee b$, $a\neq c$.

Pak $\{a,b,c,a\wedge b,a\vee b\}$ je podsvaz izomorfní N_5.

Věta: Pro svaz L je ekvivalentní:
1) L je distributivní.
2) $\forall a,b,c\in L$: $(a\wedge b=c\wedge b\ \&\ a\vee b=c\vee b)\Rightarrow a=c$.
3) L neobsahuje podsvaz izomorfní M_5 nebo N_5.

Důkaz: Podobný jako pro modularitu, jen o dost složitější.

Ukážeme, jak zkonstruovat všechny konečné distributivní svazy.

Definice: $(L,\leq)$ svaz. Prvek $a\in L$ nazýváme <u>$\vee$-nedosažitelný</u>, jestliže $\forall b,c\in L:\ a=b\vee c \Rightarrow (a=b \text{ nebo } a=c)$. Množinu všech $\vee$-nedosažitelných prvků v L označme $K(L,\leq)$.

Lemma: $(L,\leq)$ konečný svaz, $a\in L$, $b_1,\dots,b_m$ všechny $\vee$-nedosažitelné prvky v L menší nebo rovné $\underline{a}$. Pak $a=b_1\vee\dots\vee b_m$.

Důkaz: Indukcí vzhledem k počtu prvků menších než $\underline{a}$ dokážeme, že existují $c_1,\dots,c_m\in L$ ($\vee$-nedosažitelné prvky) t.ž. $a=c_1\vee\dots\vee c_m$. Protože platí $a\geq b_1\vee\dots\vee b_m\geq c_1\vee\dots\vee c_m$, tak potom $a=b_1\vee\dots\vee b_m$.

Zákl. kroky: a je $\vee$-nedosažitelný $\Rightarrow$ stačí brát $m=1$, $c_1=a$.

Ind. krok: a je $\vee$-dosažitelný $\Rightarrow a=d\vee e$, kde $d<a$, $e<a$, takže pro d a e platí indukční předpoklad, tj. $d=d_1\vee\dots\vee d_k$, $e=e_1\vee\dots\vee e_\ell$, d_i,e_j $\vee$-nedosažitelné. Proto $a=d_1\vee\dots\vee d_k\vee e_1\vee\dots\vee e_\ell$.

Definice: $(M,\leq)$ uspořádaná množina. Podmnožina $P\subseteq M$ se nazývá <u>dědičná</u>, jestliže $\forall a\in P\ \forall b\in M:\ b\leq a \Rightarrow b\in P$.

Množinu všech (neprázdných) dědičných podmnožin v $(M,\leq)$ označme $H(M,\leq)$.

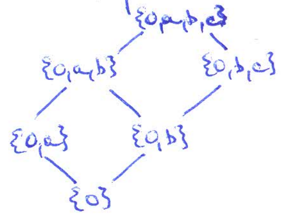
$(H(M,\leq),\subseteq)$ podsvaz v $(\mathcal{P}(M),\cup,\cap)$, protože průnik i sjednocení dědičných množin je dědičná množina, a neprázdnost průniku plyne z existence nejmenšího prvku v $(M,\leq)$. (Má-li $(M,\leq)$ nejmenší prvek, je.)

Příklad:

distr. svaz $(L,\leq)$

$(K(L,\leq),\leq)$:

$(H(K(L,\leq),\leq),\subseteq)$



Věta (reprezentace konečných distributivních svazů):
Je-li $(L,\leq)$ konečný distributivní svaz, tak $(L,\leq)\cong(H(K(L,\leq),\leq),\subseteq)$.

Důkaz: $\varphi: L\longrightarrow H(K(L))$ $\qquad \psi: H(K(L))\longrightarrow L$

$a\longmapsto\{b\in K(L)\mid b\leq a\}$ $\qquad \{a_1,\dots,a_m\}\longmapsto a_1\vee\dots\vee a_m$ (dědičná množina $\vee$-nedosažitelných prvků)

φ je izotonní: $a\leq b\Rightarrow\varphi(a)\subseteq\varphi(b)$ $\qquad$ ψ je izotonní: $\{a_1,\dots,a_m\}\subseteq\{b_1,\dots,b_m\}\Rightarrow a_1\vee\dots\vee a_m\leq b_1\vee\dots\vee b_m$.

Lemma říká, že $\forall a\in L:\ \psi(\varphi(a))=a$.

Zbývá ukázat, že $\varphi\circ\psi=id_{H(K(L))}$.

$\varphi(\psi(\{a_1,\dots,a_m\}))=\underbrace{\{c\in K(L)\mid c\leq a_1\vee\dots\vee a_m\}}_{J}$. Triviálně platí $\{a_1,\dots,a_m\}\subseteq J$.

Zbývá ukázat $J\subseteq\{a_1,\dots,a_m\}$. Buď $c\in K(L)$ takové, že $c\leq a_1\vee\dots\vee a_m$.

Pak $c=c\wedge(a_1\vee\dots\vee a_m)\overset{\uparrow}{=}(c\wedge a_1)\vee\dots\vee(c\wedge a_m)$. Jelikož $c\in K(L)$, (jediné použití distributivity)

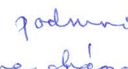
existuje $i\in\{1,\dots,m\}$ t.ž. $c=c\wedge a_i$, tzn. $c\leq a_i$. Protože $\{a_1,\dots,a_m\}$ je dědičná, tak $c\in\{a_1,\dots,a_m\}$.

Důsledek: Konečné distributivní svazy jsou až na izomorfismus právě podsvazy svazů $(\mathcal{P}(A),\cup,\cap)$ pro konečné množiny A.

Pozn.: Pomocí axiomu výběru lze dokázat, že (všechny) distr. svazy jsou až na izomorfismus právě podsvazy $(\mathcal{P}(A),\cup,\cap)$ pro libov. množiny A.

BOOLEOVY ALGEBRY

Definice: $(L,\le)$ svaz s nejmenším prvkem 0 a největším prvkem 1, $a\in L$.
Prvek $b\in L$ se nazývá komplement a, jestliže $a\vee b=1$, $a\wedge b=0$.
Komplementární svaz je svaz, v němž má každý prvek komplement.
Být komplementem je symetrická relace.
Příklady: 0 je komplement 1.
V lineárně uspořádané množině mají komplement jen prvky $0,1$.
Tvrzení: Každý prvek distributivního svazu má nejvýše jeden komplement.
Důkaz: b,c komplementy $a \Rightarrow a\wedge b=0=a\wedge c$, $a\vee b \overset{=1}{=} a\vee c \Rightarrow b=c$.
Příklad: ~~Pro~~ M_5 a N_5 tvrzení neplatí.
Definice: Booleova algebra = distributivní a komplementární svaz.
V Bool. algebře máme unární operaci $a\mapsto a'$, která každému prvku přiřazuje jeho jediný komplement.
Jako strukturu s 5 operacemi $(L,\underbrace{\vee,\wedge}_{\text{binární}},\underbrace{0,1}_{\text{nulární}},\underbrace{'}_{\text{unární}})$ lze Bool. algebru definovat pomocí rovností: pro $\vee$ a $\wedge$ komutativita, asociativita, idempotence, absorpce, distrib.
$\forall a\in L$: $\underbrace{a\wedge 0=0,\ a\vee 1=1}_{\text{plynou z následujících dvou}}$, $a\vee a'=1$, $a\wedge a'=0$
Příklad: A lib. množina. Pak $(\mathcal{P}(A),\cup,\cap,\emptyset,A,A\setminus -)$ je Bool. algebra.
Tvrzení: V každé Bool. algebře platí $\forall a,b\in L: (a\vee b)'=a'\wedge b'$, $(a\wedge b)'=a'\vee b'$ (de Morganovy zákony)
Důkaz: $(a\vee b)\vee(a'\wedge b') \overset{(L,\le)}{=} (a\vee b\vee a')\wedge(a\vee b\vee b')=1\wedge 1=1$, $(a\vee b)\wedge(a'\wedge b')=0$ a 2. zákon symetricky.
Booleova podalgebra je podmnožina Bool. algebry uzavřená na všech 5 operací.
Homomorfismus Bool. algeber $\varphi: L\to M$ je homomorfismus svazů splňující
$\varphi(0)=0$, $\varphi(1)=1$, $\forall a\in L: \varphi(a')=(\varphi(a))'$.
Poslední podmínka v definici homomorfismu je nadbytečná: $\varphi(a')\vee\varphi(a)=\varphi(a'\vee a)=\varphi(1)=1$, $\varphi(a')\wedge\varphi(a)\overset{0}{=}$ symetricky.
Izomorfismus = bijektivní homomorfismus.
~~Tvrzení: Každý izomorfismus svazů $\varphi: L\to M$ je izomorfismus Bool. algeber.~~
~~Důkaz: $\exists a\in L$~~
Tvrzení: Jsou-li L,M Bool. algebry, pak každý ~~...~~ izomorfismus svazů $\varphi: L\to M$ je izomorfismus Bool. algeber.
Důkaz: $\exists a\in L: \varphi(a)=1 \Rightarrow \varphi(1)\ge\varphi(a)=1 \Rightarrow \varphi(1)=1$. Analog. $\varphi(0)=0$.
Definice: Atom = prvek Bool. algebry, který pokrývá 0, tzn. $a\in L$ je atom, jestliže $a>0$ & $\forall b\in L: b<a \Rightarrow b=0$.
Věta: Každá konečná Booleova algebra $(L,\vee,\wedge,0,1,')$ je izomorfní algebře $(\mathcal{P}(A),\cup,\cap,\emptyset,A,A\setminus -)$, kde A je množina všech atomů L.
Důkaz: Ukážeme, že $a\in L$ je $\vee$-nedosažitelný $\Leftrightarrow$ je atom nebo 0.
"$\Leftarrow$" zřejmé
"$\Rightarrow$" a $\vee$-nedosažitelný. Sporem předpokládejme, že a není atom ani 0.
Pak $\exists b\in L: 0<b<a$, z čehož plyne $(a\wedge b')\vee b=(a\vee b)\wedge(\underbrace{b'\vee b}_{1})=a\vee b=a$.
(lokalizace inverze k b' do intervalu $\langle 0,a\rangle$: $a\wedge b'$ je inverze k b v $\langle 0,a\rangle$.)

Protože a je $\vee$-nedosažitelný a $b\ne a$, tak $a\wedge b'=a$, a tedy $b'\ge a\ge b$, spor.
Takže $(K(L),\le)\cong$  ... atomy L, a proto neprázdné dědičné podmnožiny $K(L)$ přesně odpovídají podmnožinám A, tj. $L\cong H(K(L))\cong\mathcal{P}(A)$.
Každý prvek $\mathcal{P}(A)$ můžeme chápat jako pravdivostní tabulku nějakého tvrzení o prvcích množiny A. Potom $\cup$ odpovídá OR, $\cap$ odpovídá AND, 0 je FALSE, 1 je TRUE a komplement je negace.

Věta neplatí pro nekonečné Bool. algebry:

Nejmenší nekonečná Bool. algebra tvaru $P(A)$ má mohutnost kontinua (pro A spočetnou), ale existují spočetné Bool. algebry, např.

$\{P \subseteq \mathbb{N} \mid P$ je konečná nebo $\mathbb{N} \setminus P$ je konečná$\}$ je spočetná Bool. podalgebra $P(\mathbb{N})$, která je generovaná atomy $P(\mathbb{N})$, tj. jednoprvkovými množinami $\{n\}$, $n \in \mathbb{N}$.

(Odpovídá to tomu, že pomocí výrokových formulí používajících jako elementární formule "$x=n$" pro $n \in \mathbb{N}$ lze zapsat tvrzení "$x \in P$" pouze pro konečné a kokonečné $P \subseteq \mathbb{N}$.)

Pomocí axiomu výběru lze dokázat, že Booleovy algebry jsou až na izomorfismus právě Bool. podalgebry $P(A)$ pro libovolné množiny A.

<u>Booleův okruh</u> = okruh $(R,+,\cdot)$, kde $\cdot$ je idempotentní.

V Bool. okruhu platí: $2 = 2\cdot 2 = 4 \Rightarrow 0 = 2$, takže má charakteristiku 2 nebo 1.

$a+a = 2\cdot a = 0 \Rightarrow -a = a$.

$a+b = (a+b)\cdot(a+b) = a^2+ab+ba+b^2 = a+b+ab+ba \Rightarrow ab = -ba = ba$, takže je komutativní.

Existuje vzájemně jednoznačná korespondence mezi Bool. algebrami a Bool. okruhy:

L Bool. algebra. Def. $a+b = (a \wedge b') \vee (a' \wedge b)$. Pak $(L,+,\wedge)$ je Bool. okruh.

R Bool. okruh. Def. $a \vee b = a\cdot b + a + b$, $a' = a+1$. Pak $(R, \vee, \cdot, 0, 1, ')$ je Bool. algebra.

Odpovídá logickým operacím: $\vee$ je OR, $\wedge$ je AND, $+$ je XOR.

ÚPLNÉ SVAZY

Definice: $(L,\leq)$ uspořádaná množina, $K \subseteq L$. Řekneme, že prvek $a \in L$ je <u>supremem</u> množiny K, jestliže je nejmenší horní závora K, tj.:

$$(\forall b \in K : b \leq a) \,\&\, (\forall c \in L : (\forall b \in K : b \leq c) \Rightarrow a \leq c).$$

Příklady: $\sup \emptyset$ je nejmenší prvek, $\sup L$ je největší prvek.
v $(\mathbb{R},\leq)$ je supremem množiny $K = \{-\frac{1}{n} \mid n \in \mathbb{N}\}$ číslo 0, v $(\mathbb{R}\setminus\{0\},\leq)$ supremum K neexistuje.

<u>Infimum</u> K = největší dolní závora K.

(pokud supremum či infimum existuje, je určeno jednoznačně)

<u>Úplný svaz</u> = uspořádaná množina, v níž pro každou podmnožinu existuje supremum i infimum.

Každý úplný svaz je ohraničený svaz, tj. má největší prvek 1 a nejmenší prvek 0.

Příklad: $(\mathbb{R},\leq)$ je svaz, ale není úplný.

V každém svazu $(L,\leq)$ existují suprema a infima všech neprázdných konečných podmnožin: $\sup\{a_1,\dots,a_n\} = a_1 \vee \dots \vee a_n$.

$\sup \emptyset = \inf L$, $\inf \emptyset = \sup L$.

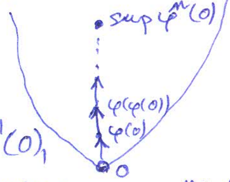
Z předchozích 2 pozorování plyne, že každý neprázdný konečný svaz je úplný.

(úplné svazy nejsou algebraické struktury, ale vyskytují se v algebře všude)

Příklad: A lib. množina. Pak $(\mathcal{P}(A),\subseteq)$ je úplný svaz, přičemž pro lib. $\mathcal{R} \subseteq \mathcal{P}(A)$ platí $\sup \mathcal{R} = \bigcup \mathcal{R} = \bigcup_{P \in \mathcal{R}} P$ a $\inf \mathcal{R} = \bigcap \mathcal{R} = \bigcap_{P \in \mathcal{R}} P$, kde pro $\mathcal{R} = \emptyset$ zavádíme konvenci $\bigcap \emptyset = A$.

Definice: <u>Pevný bod</u> zobrazení $\varphi : L \to L$ je prvek $a \in L$ t.ž. $\varphi(a) = a$.

Věta o pevném bodě: $(L,\leq)$ úplný svaz, $\varphi : L \to L$ zobrazení t.ž. pro každou neprázdnou lineárně uspořádanou podmnožinu K v $(L,\leq)$ platí $\varphi(\sup K) = \sup(\varphi(K))$.
Potom $\sup_{n \in \mathbb{N}_0} \varphi^n(0)$ je nejmenší pevný bod φ.



Důkaz: Je-li $a \leq b$, tak $\varphi(b) = \varphi(\sup\{a,b\}) = \sup\{\varphi(a),\varphi(b)\}$, takže $\varphi(a) \leq \varphi(b)$.
Proto φ je izotonní.

Z $0 \leq \varphi(0)$ opakovanou aplikací φ indukcí dostaneme $\forall n \in \mathbb{N}_0 : \varphi^n(0) \leq \varphi^{n+1}(0)$, takže $\{\varphi^n(0) \mid n \in \mathbb{N}\}$ je lineárně uspořádaná. Proto $\varphi(\sup_{n \in \mathbb{N}_0} \varphi^n(0)) = \sup_{n \in \mathbb{N}_0} \varphi^{n+1}(0) = \sup_{n \in \mathbb{N}_0} \varphi^n(0)$, takže $\sup_{n \in \mathbb{N}_0} \varphi^n(0)$ je pevný bod. Ukážeme, že je nejmenší. Buď $a \in L$ lib. pevný bod φ.
Indukcí ověříme, že $\forall n \in \mathbb{N}_0 : \varphi^n(0) \leq a$: 1) $0 \leq a$ 2) $\varphi^n(0) \leq a \Rightarrow \varphi^{n+1}(0) \leq \varphi(a) = a$.
Takže $\sup_{n \in \mathbb{N}_0} \varphi^n(0) \leq a$.

Příklad užití v denotačních sémantikách: Sémantika sekvence příkazů P je parc. fce $[\![P]\!]$ z S do S.
S množina všech stavů počítače. L = množina všech parc. fcí z S do S uspořádaná předpisem $f \leq g \Leftrightarrow f = g|\operatorname{dom} f$.
Pak $(L,\leq)$ je úplný svaz s odebraným největším prvkem.
$[\![\text{while } C \text{ do } P]\!]$ = nejmenší pevný bod fce $\varphi : L \to L$ definované pro $s \in S$ předpisem

$$(\varphi(f))(s) = \begin{cases} f([\![P]\!](s)), & \text{pokud } [\![C]\!](s) = \text{True} \\ s, & \text{pokud } \underbrace{[\![C]\!](s)}_{\text{platnost podmínky } C \text{ ve stavu } s} = \text{False} \end{cases}$$

Vysvětlení:
Nejmenší prvek L je prázdná fce $\emptyset$.

$$\varphi(\emptyset)(s) = \begin{cases} \text{nedef.}, & \text{pokud } [\![C]\!](s) = \text{True} \\ s, & \text{pokud } [\![C]\!](s) = \text{False} \end{cases}$$

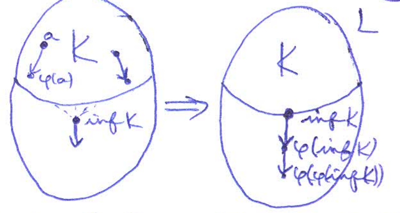
(výsledky, které lze určit jediným testem platnosti C)

$$\varphi(\varphi(\emptyset))(s) = \begin{cases} \text{nedef.}, & \text{pokud } [\![C]\!](s) = [\![C]\!]([\![P]\!](s)) = \text{True} \\ [\![P]\!](s), & \text{pokud } [\![C]\!](s) = \text{True} \,\&\, [\![C]\!]([\![P]\!](s)) = \text{False} \\ s, & \text{pokud } [\![C]\!](s) = \text{False} \end{cases}$$

(výsledky, které lze určit nejvýše dvěma testy platnosti C)

$\vdots$

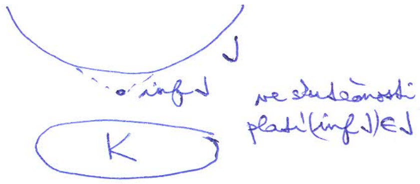
Věta o pevném bodě (Tarski): $(L,\le)$ úplný svaz, $\varphi: L\to L$ izotonní zobrazení.
Pak existuje nejmenší pevný bod φ.



Důkaz: Def. $K=\{a\in L \mid \varphi(a)\le a\}$. Ukážeme, že K má nejmenší prvek, a ten je pevným bodem. Platí $\forall a\in K: a\ge \inf K$, takže $\forall a\in K: a\ge\varphi(a)\ge\varphi(\inf K)$. Takže $\varphi(\inf K)$ je dolní závora K, a tedy $\varphi(\inf K)\le \inf K$ (tj. $(\inf K)\in K$).
Potom $\varphi(\varphi(\inf K))\le\varphi(\inf K)$, takže $\varphi(\inf K)\in K$, a proto $\varphi(\inf K))\ge \inf K$. Celkem $\varphi(\inf K)=\inf K$.

Příklady aplikací věty:
– k důkazu Schröderovy–Bernsteinovy věty: $|A|\le|B| \,\&\, |B|\le|A| \Longrightarrow |A|=|B|$
(z existence injekcí oběma směry plyne existence bijekce)
– k důkazu existence rovnovážných situací v supermodulárních hrách
(hry, kde zvýší-li jeden hráč sázku, vyplatí se zvýšit sázku i ostatním)

Tvrzení: $(L,\le)$ je úplný svaz $\iff$ každá podmnožina L má infimum $\iff$
L má největší prvek a každá neprázdná podmnožina L má infimum.
(díky dualitě platí analogické tvrzení i pro suprema)



Důkaz: Předp., že každá podmnožina L má infimum.
Buď $K\subseteq L$ lib. Označme $J=\{a\in L\mid \forall b\in K: a\ge b\}$ množinu všech horních závor K. Ukážeme, že $\inf J$ je nejmenší prvek J, takže $\inf J=\sup K$. K tomu stačí ověřit, že $(\inf J)\in J$, tj. že $\inf J$ je horní závora K. Ovšem pro všechna $b\in K$ platí $\forall a\in J: a\ge b$, tj. b je dolní závora J, a tedy $b\le \inf J$.

(popíšeme, jak úplné svazy vznikají)

Definice: A množina. Podmnožina $\mathcal U\subseteq \mathcal P(A)$ se nazývá <u>uzávěrový systém</u> na A, jestliže $A\in\mathcal U$ a $\forall\, \emptyset\ne \mathcal R\subseteq\mathcal U: \bigcap\mathcal R\in\mathcal U$. (při konvenci $\bigcap\emptyset = A$ stačí psát $\forall \mathcal R\subseteq\mathcal U: \bigcap \mathcal R\in\mathcal U$)
(termín uzávěrový systém není standardizovaný)

Je-li $\mathcal U$ uzávěrový systém na A, pak $(\mathcal U,\subseteq)$ je úplný svaz, kde $\forall\mathcal R\subseteq\mathcal U: \inf\mathcal R=\bigcap\mathcal R$
a $\sup\mathcal R = \inf\{P\in\mathcal U\mid \forall Q\in\mathcal R: Q\subseteq P\} = \bigcap\{P\in\mathcal U\mid \bigcup\mathcal R\subseteq P\}$.

Příklady: A pologrupa, $\mathcal U=\{P\subseteq A\mid P$ je podpologrupa $A\}$

grupa	podgrupa
okruh	podokruh
těleso	podtěleso
svaz	podsvaz
vekt. prostor	podprostor
okruh	ideál
grupa	norm. podgrupa
množina	podmnožina ($\mathcal U=\mathcal P(A)$)
$A=\mathbb R^n$	konvexní v A
$A=\mathbb R^n$	uzavřená v A
$A=B\times B$	relace ekvivalence

(ve všech případech je ~~vlastnost~~ požadovaná množin P definovaná podmínkou, že když tam nějaké prvky patří, tak tam jistý prvek patří také)

Nejsou uzávěrové systémy:
$\mathcal U=\{P\subseteq\mathbb R^n\mid P$ je otevřená$\}$: např. $\bigcap_{n\in\mathbb N}(-\frac1n,\frac1n)=\{0\}\notin\mathcal U$
(s každým bodem patří do P nějaké jeho okolí, ale není řečeno jaké)
$\mathcal U=\{\le\,\subseteq B\times B\mid \le$ je relace uspořádání$\}$: sice $\bigcap_{i\in I}\le_i$ je uspořádání pro lib. $I\ne\emptyset$,
ale $B\times B\notin\mathcal U$. (kvůli antisymetrii)

Lemma (tvrdejme mu reprezentační): $(L,\leq)$ uspoř. množina, $K\subseteq L$ podmnožina t.ž. $\forall a\in L: a=\sup\{c\in K \mid c\leq a\}$. (a jde zrekonstruovat ze znalosti prvků K pod ním) Pak zobrazení $\varphi: L\to P(K)$ definované předpisem $\varphi(a)=\{c\in K\mid c\leq a\}$ je izotonní vložení $(L,\leq)$ do $(P(K),\subseteq)$. (Tuhle myšlenku už jsme použili k reprezentaci konečných distributivních svazů) Přitom pro všechny podmnožiny $J\subseteq L$, které mají v L infimum, platí $\varphi(\inf J)=\bigcap_{a\in J}\varphi(a)$.

Důkaz: $a\leq b \Rightarrow \varphi(a)\subseteq\varphi(b)$: $c\in\varphi(a)\Rightarrow c\in K$, $\Rightarrow c\leq a\leq b$ $\Rightarrow c\in\varphi(b)$

$\varphi(a)\subseteq\varphi(b)\Rightarrow a\leq b$: $a=\sup(\varphi(a))\leq\sup(\varphi(b))=b$

Tedy φ je izotonní vložení, protože injektivita plyne z předchozího:
$\varphi(a)=\varphi(b)\Rightarrow(\varphi(a)\subseteq\varphi(b)\ \&\ \varphi(b)\subseteq\varphi(a))\Rightarrow(a\leq b\ \&\ b\leq a)\Rightarrow a=b$

Nechť $J\subseteq L$ je t.ž. $\inf J$ existuje. Pak $\varphi(\inf J)=\{c\in K\mid c\leq\inf J\}=$
$=\{c\in K\mid\forall a\in J: c\leq a\}=\bigcap_{a\in J}\{c\in K\mid c\leq a\}=\bigcap_{a\in J}\varphi(a)$.

Věta: Každý úplný svaz $(L,\leq)$ je izomorfní nějakému svazu $(\mathcal{U},\subseteq)$, kde $\mathcal{U}$ je uzávěrový systém na L. (porovnat s reprezentací distrib. svazů)

Důkaz: Zvolíme v reprezentačním lemmatu $K=L$, tj. $\varphi(a)=\downarrow a=\{c\in L\mid c\leq a\}$.
Pak $(L,\leq)\cong_{\varphi}(\varphi(L),\subseteq)$. Přitom pro všechna $J\subseteq L$ existuje $\inf J$ a tedy
$\bigcap_{a\in J}\varphi(a)=\varphi(\inf J)\in\varphi(L)$, takže $\varphi(L)$ je uzavřená na průniky.

Definice: A množina. <u>Uzávěrovým operátorem</u> na A myslíme zobrazení $C: P(A)\to P(A)$ splňující podmínky:
1) $\forall P\subseteq A: P\subseteq C(P)$ (extenzivita) (přidává, neubírá)
2) $\forall P\subseteq A: C(C(P))=C(P)$ (idempotence) (co C uzavřel, je uzavřené)
3) $\forall P,Q\subseteq A: P\subseteq Q\Rightarrow C(P)\subseteq C(Q)$ (monotonie)

Podmnožina $P\subseteq A$ se nazývá <u>C-uzavřená</u>, jestliže $C(P)=P$.
C-uzavřené množiny jsou právě množiny tvaru $C(Q)$ pro $Q\subseteq A$.
(ukázat na dřívějších příkladech)

Věta: Je-li C uzávěrový operátor na množině A, tak množina $\mathcal{U}_C$ všech C-uzavřených podmnožin A je uzávěrový systém na A t.ž. $\forall P\subseteq A: C(P)=\bigcap\{Q\in\mathcal{U}_C\mid P\subseteq Q\}$
(speciálně, v $(\mathcal{U}_C,\subseteq)$ platí $\forall\mathcal{R}\subseteq\mathcal{U}_C: \sup\mathcal{R}=C(\bigcup\mathcal{R})$). (volíme $P=\bigcup\mathcal{R}$)

Důkaz: 1) $\mathcal{U}_C$ je uzávěrový systém: $C(A)=A\Rightarrow A\in\mathcal{U}_C$
Buď $\emptyset\neq\mathcal{R}\subseteq\mathcal{U}_C$. Chceme ukázat, že $\bigcap\mathcal{R}\in\mathcal{U}_C$, tj. $C(\bigcap\mathcal{R})=\bigcap\mathcal{R}$:
"$\supseteq$" z definice C
"$\subseteq$" Nechť $R\in\mathcal{R}$ je libovolná. Protože $\bigcap\mathcal{R}\subseteq R$ a R je C-uzavřená, tak
$C(\bigcap\mathcal{R})\subseteq C(R)=R$. Takže $C(\bigcap\mathcal{R})\subseteq\bigcap\mathcal{R}$.

2) $C(P)=\bigcap\{Q\in\mathcal{U}_C\mid P\subseteq Q\}$: "$\subseteq$" $P\subseteq Q\Rightarrow C(P)\subseteq C(Q)=Q$, protože Q je C-uzavřená
"$\supseteq$" plyne z toho, že $C(P)$ je jedním z Q.

Věta: Je-li $\mathcal{U}\subseteq P(A)$ uzávěrový systém na A, tak předpis $C_{\mathcal{U}}(P):=\bigcap\{Q\in\mathcal{U}\mid P\subseteq Q\}$, pro $P\subseteq A$, definuje uzávěrový operátor $C_{\mathcal{U}}$ na A t.ž. $C_{\mathcal{U}}$-uzavřené množiny jsou právě prvky $\mathcal{U}$.

Důkaz: Jelikož $A\in\mathcal{U}$, je $C_{\mathcal{U}}(P)\subseteq A$ korektně definováno.
$C_{\mathcal{U}}$ je uzávěrový operátor: 1) $P\subseteq\bigcap\{Q\in\mathcal{U}\mid P\subseteq Q\}$
2) $\mathcal{U}$ je uzávěrový systém, takže $C_{\mathcal{U}}(P)\in\mathcal{U}$. Proto $C_{\mathcal{U}}(C_{\mathcal{U}}(P))=\bigcap\{Q\in\mathcal{U}\mid C_{\mathcal{U}}(P)\subseteq Q\}=$
$=C_{\mathcal{U}}(P)$.
3) $P\subseteq R\Rightarrow\{Q\in\mathcal{U}\mid P\subseteq Q\}\supseteq\{Q\in\mathcal{U}\mid R\subseteq Q\}\Rightarrow C_{\mathcal{U}}(P)\subseteq C_{\mathcal{U}}(R)$

$C_{\mathcal{U}}(P)=P\Leftrightarrow P\in\mathcal{U}$: "$\Rightarrow$" $P=\bigcap\{Q\in\mathcal{U}\mid P\subseteq Q\}\in\mathcal{U}$, protože $\mathcal{U}$ je uzávěrový systém.
"$\Leftarrow$" $\bigcap\{Q\in\mathcal{U}\mid P\subseteq Q\}=P$

Dohromady: Existuje vzájemně jednoznačná korespondence mezi uzávěrovými operátory na A a uzávěrovými systémy na A:

$C \mapsto \mathcal{U}_C$, $\mathcal{U} \mapsto C_{\mathcal{U}}$

$$C_{\mathcal{U}_C}(P) \overset{\text{def.}}{=} \bigcap\{Q \in \mathcal{U}_C \mid P \subseteq Q\} \overset{\text{bylo dokázáno}}{=} C(P)$$

$$P \in \mathcal{U}_{C_{\mathcal{U}}} \overset{\text{def.}}{\iff} C_{\mathcal{U}}(P) = P \overset{\text{bylo dokázáno}}{\iff} P \in \mathcal{U}$$

(je výhodné pracovat s oběma pojmy současně)

(každý úplný svaz tedy vzniká z nějakého uzávěrového operátoru)

Věta: Každá uspořádaná množina $(L,\le)$ lze izotonně vložit do úplného svazu tak, aby byla zachována existující suprema a infima.

Příklad: $(\mathbb{Q},\le) \hookrightarrow (\mathbb{R}\cup\{-\infty,\infty\},\le)$ pomocí Dedekindových řezů.

(teď zobecníme na libovolnou uspořádanou množinu)

Důkaz: $\mathcal{U} := \{P \subseteq L \mid P$ je $\underbrace{\text{dědičná}}_{\forall a\in P,\, b\in L:\ b\le a \Rightarrow b\in P}$ a $\underbrace{\text{uzavřená na existující suprema}}_{\forall J\subseteq P:\ \sup J \text{ v } (L,\le) \text{ existuje} \Rightarrow \sup J\in P}\}$

$\mathcal{U}$ je uzávěrový systém na L, takže $(\mathcal{U},\subseteq)$ je úplný svaz, kde infima jsou průniky.

$\varphi: L \to \mathcal{U}$ definujeme předpisem $\varphi(a) = \downarrow a$. Přitom $\downarrow a \in \mathcal{U}$, protože pro $J \subseteq \downarrow a$ t.ž. $\sup J$ existuje, platí $\sup J \le a$ (protože a je horní závora J), takže $\sup J \in \downarrow a$.

Podle reprezentačního lemmatu je φ izotonní vložení, přičemž pokud pro $J \subseteq L$ existuje $\inf J$, tak $\varphi(\inf J) = \bigcap_{a\in J}\varphi(a) = \inf(\varphi(J))$.

Předpokládejme, že pro $J \subseteq L$ existuje $\sup J$. Chceme dokázat, že $\varphi(\sup J) = \sup(\varphi(J))$, tj. $\downarrow(\sup J) = \sup_{b\in J}(\downarrow b)$.

1) $\downarrow(\sup J)$ je horní závora $\{\downarrow b \mid b\in J\}$, protože $\forall b\in J: b \le \sup J$.

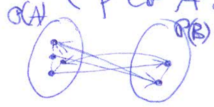
2) Je-li $P\in\mathcal{U}$ horní závora $\{\downarrow b \mid b\in J\}$, tak $(\forall b\in J: \downarrow b \subseteq P) \Rightarrow J \subseteq P \overset{P\in\mathcal{U}}{\Longrightarrow} \sup J \in P \overset{P\in\mathcal{U}}{\Longrightarrow} \downarrow(\sup J) \subseteq P$.

GALOISOVY KORESPONDENCE

Definice: A, B množiny. <u>Galoisova korespondence</u> (konexe) mezi $\mathcal{P}(A)$ a $\mathcal{P}(B)$ je dvojice zobrazení $\varphi: \mathcal{P}(A) \to \mathcal{P}(B)$ a $\psi: \mathcal{P}(B) \to \mathcal{P}(A)$ t.ž.

1) $\forall P \subseteq A: P \subseteq \psi(\varphi(P))$ 2) $\forall Q \subseteq B: Q \subseteq \varphi(\psi(Q))$ (podmínky jsou symetrické pro A a B)

3) $\forall P \subseteq R \subseteq A: \varphi(P) \supseteq \varphi(R)$ 4) $\forall Q \subseteq S \subseteq B: \psi(Q) \supseteq \psi(S)$

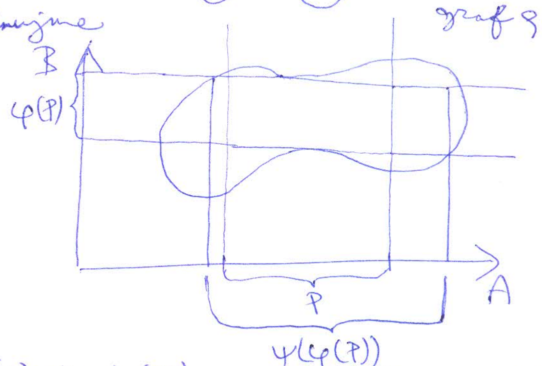


Jak takové korespondence vznikají?

Buď $\rho \subseteq A \times B$ libovolná binární relace. Definujme

$\varphi(P) = \{b \in B \mid \forall a \in P: (a,b) \in \rho\}$

$\psi(Q) = \{a \in A \mid \forall b \in Q: (a,b) \in \rho\}$



Příklady: 1) A = množina všech formulí dané logiky

B = množina (třída) všech realizací této logiky

Pro $\Phi \in A$ a $S \in B$ definujme

$(\Phi, S) \in \rho :\Longleftrightarrow S \models \Phi$

Pak pro lib. teorii $T \subseteq A$ máme $\varphi(T) = \mathrm{Mod}(T)$ a pro realizací (třídu) $Q \subseteq B$ je $\psi(Q)$ množina všech formulí platných ve všech realizacích v Q.

2) $A = B = V$ konečněrozměrný vektorový prostor, $(u,v) \in \rho :\Longleftrightarrow \langle u,v \rangle = 0$ (tj. $u \perp v$).
(vektorové podprostory obvykle popisujeme jako $\varphi(\{v_1, \dots, v_n\})$)

3) Původní Galoisova korespondence: A je těleso, B je grupa všech automorfismů A.
Pro $a \in A$, $f \in B$: $(a,f) \in \rho :\Longleftrightarrow f(a) = a$.

Pro každou Galoisovu korespondenci platí: $\forall P \subseteq A: \varphi(\psi(\varphi(P))) = \varphi(P)$ a $\forall Q \subseteq B: \psi(\varphi(\psi(Q))) = \psi(Q)$.

Důkaz: "$\supseteq$" z 2) "$\subseteq$" 1) $\Rightarrow P \subseteq \psi(\varphi(P)) \overset{3)}{\Rightarrow} \varphi(P) \supseteq \varphi(\psi(\varphi(P)))$.

Proto $C := \psi \circ \varphi$ je uzávěrový operátor na A a $D := \varphi \circ \psi$ je uzávěrový operátor na B.

Důkaz: 1) $\psi(\varphi(P)) \supseteq P$ 2) $\psi(\varphi(\psi(\varphi(P)))) = \psi(\varphi(P))$ 3) $P \subseteq R \Rightarrow \psi(\varphi(P)) \subseteq \psi(\varphi(R))$

Pokračování příkladů: 1) Pro $T \subseteq A$ je $\psi(\varphi(T))$ uzávěr teorie na sémantické důsledky.
Uzavřené třídy v B jsou právě třídy definovatelné v dané logice.

2) $\psi \circ \varphi$ i $\varphi \circ \psi$ je generování podprostoru.

3) Za určitých podmínek je $\psi \circ \varphi$ generování podtělesa a $\varphi \circ \psi$ generování podgrupy.

Úplné svazy $(\mathcal{U}_C, \subseteq)$ a $(\mathcal{U}_D, \supseteq)$ jsou izomorfní:

Důkaz: Ukážeme, že φ a ψ (zúžené) jsou vzáj. inverzní bijekce mezi $\mathcal{U}_C$ a $\mathcal{U}_D$:

Je-li $P \in \mathcal{U}_C$, tak $P = \psi(\varphi(P))$ a tedy $\psi \circ \varphi|\mathcal{U}_C$ je identita. Analog. $\varphi \circ \psi|\mathcal{U}_D = \mathrm{id}$.

Izotonie φ, ψ plyne z 3), 4).

Pokračování příkladů: 1) Izomorfismus mezi teoriemi uzavřenými na důsledky a definovatelnými třídami.

2) Izomorfismus zobrazuje každý podprostor na jeho ortogonální doplněk.

3) Izomorfismus svazu podtěles a svazu podgrup.

Příklad: Automorfismy $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ jsou 4: $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$ (kořeny $x^2 - 2$, $x^2 - 3$)

Galoisova grupa je izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_2$

Svaz podtěles $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

(ukázat odpovídající automorfismy)

ALGEBRAICKÉ SVAZY

Uzávěrové operátory, se kterými se potkáváme v algebře, mají ještě další společnou vlastnost.

Definice: A množina. Uzávěrový operátor C na A se nazývá <u>algebraický</u>, jestliže $\forall P \subseteq A: C(P) = \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\}$.

Příklady: Všechny, které jsme si uváděli u uzávěrových systémů, s výjimkou uzavřených množin v $\mathbb{R}^n$: např. v $\mathbb{R}$ platí $C((0,1)) = \langle 0,1 \rangle$, ale pro každou $Q \subseteq (0,1)$ konečnou platí $C(Q) = Q$.

Důvod: v algebře vždy příslušnost prvku do uzávěru plyne z existence konečně mnoha prvků, ale $0 \in C((0,1))$, protože k ní konverguje nekonečná posloupnost z $(0,1)$.

Tvrzení: Uzávěrový operátor C na A je algebraický $\iff$ $\forall P \subseteq A: P \in \mathcal{U}_C \iff (\forall \text{konečnou } Q \subseteq P: C(Q) \subseteq P)$. (ekvivalentně: $P \in \mathcal{U}_C \iff P = \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\}$)

Důkaz: "$\Rightarrow$" "$\Rightarrow$" $Q \subseteq P \Rightarrow C(Q) \subseteq C(P) = P$.

"$\Leftarrow$" $C(P) = \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\} \subseteq P$.

"$\Leftarrow$" Chceme ukázat, že $C(P) = \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\}$. Platí $P \subseteq \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\} \subseteq C(P)$. Stačí tedy ověřit, že $\bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\} \in \mathcal{U}_C$. Buď $R \subseteq \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\}$ konečná podmnožina. Pak existují $Q_1, \dots, Q_n \subseteq P$ konečné t.ž. $R \subseteq C(Q_1) \cup \dots \cup C(Q_n)$. Tedy $C(R) \subseteq C(C(Q_1) \cup \dots \cup C(Q_n)) = C(\underbrace{Q_1 \cup \dots \cup Q_n}_{\text{kon.}}) \subseteq \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\}$.

Definice: Podmnožina J uspořádané množiny $(L, \leq)$ se nazývá <u>usměrněná</u>, jestliže $J \neq \emptyset$ a $\forall a, b \in J\ \exists c \in J: a \leq c \ \&\ b \leq c$.
(Ekvivalentně: pro každou konečnou podmnožinu $K \subseteq J$ existuje $c \in J$ t.ž. $\forall a \in K: a \leq c$.)

Definice: Uzávěrový systém $\mathcal{U}$ na množině A se nazývá <u>algebraický</u>, jestliže pro každou usměrněnou podmnožinu $\mathcal{R}$ v $(\mathcal{U}, \subseteq)$ platí $\bigcup \mathcal{R} \in \mathcal{U}$.

Příklad: $\mathcal{R} = \{\langle \frac{1}{n}, 1 - \frac{1}{n} \rangle \mid n \in \mathbb{N}\}$ je usměrněná množina uzavřených intervalů, ale $\bigcup \mathcal{R} = (0,1)$ uzavřená není.

Věta: Uzávěrový operátor C je algebraický $\iff$ uzávěrový systém $\mathcal{U}_C$ je algebraický.

Důkaz: "$\Rightarrow$" $\mathcal{R} \subseteq \mathcal{U}_C$ usměrněná. Chceme ukázat, že $\bigcup \mathcal{R} \in \mathcal{U}_C$, tj. že pro každou konečnou $Q \subseteq \bigcup \mathcal{R}$ platí $C(Q) \subseteq \bigcup \mathcal{R}$. Pro takovou Q ovšem existuje konečná podmnožina $\mathcal{S} \subseteq \mathcal{R}$ t.ž. $Q \subseteq \bigcup \mathcal{S}$. Díky usměrněnosti $\mathcal{R}$ existuje $R \in \mathcal{R}$ t.ž. $\bigcup \mathcal{S} \subseteq R$, a tedy $C(Q) \subseteq C(\bigcup \mathcal{S}) \subseteq C(R) = R \subseteq \bigcup \mathcal{R}$.

"$\Leftarrow$" Ukážeme, že $\forall P \subseteq A: (\forall \text{konečnou } Q \subseteq P: C(Q) \subseteq P) \Rightarrow P \in \mathcal{U}_C$. Pokud totiž platí předpoklad, tak $P = \bigcup \{C(Q) \mid Q \subseteq P \text{ konečná}\}$, přičemž $\mathcal{R} = \{C(Q) \mid Q \subseteq P \text{ konečná}\}$ je usměrněná množina, protože $C(\emptyset) \in \mathcal{R}$ a $\forall Q, Q' \subseteq P$ konečné platí $C(Q) \cup C(Q') \subseteq C(Q \cup Q') \in \mathcal{R}$. Proto $P = \bigcup \mathcal{R} \in \mathcal{U}_C$.

Ukážeme, že algebraičnost lze popsat i jako abstraktní vlastnost úplného svazu, bez znalosti, jakými množinami jsou jeho prvky reprezentovány.
(je třeba popsat konečně generované ~~pod~~ podmnožiny v algebraickém systému nějakou abstraktní vlastností)

Definice: Prvek $a \in L$ úplného svazu $(L, \leq)$ se nazývá <u>kompaktní</u>, jestliže pro každou podmnožinu $J \subseteq L$ t.ž. $a \leq \sup J$ existuje konečná podmnožina $N \subseteq J$ t.ž. $a \leq \sup N$.

<u>Algebraický svaz</u> je úplný svaz, v němž každý prvek je supremem nějaké množiny kompaktních prvků.

Věta: Je-li $\mathcal{U}$ algebraický uzávěrový systém na množině A, pak $(\mathcal{U},\subseteq)$ je algebraický svaz, jehož kompaktními prvky jsou právě množiny $C_{\mathcal{U}}(P)$ pro konečné množiny P.

Důkaz: 1) $P\subseteq A$ konečná. Ukážeme, že $C_{\mathcal{U}}(P)$ je kompaktní v $(\mathcal{U},\subseteq)$.

Předp. $C_{\mathcal{U}}(P)\subseteq \sup\mathcal{R}$, kde $\mathcal{R}\subseteq\mathcal{U}$. Pak $P\subseteq C_{\mathcal{U}}(P)\subseteq\sup\mathcal{R}=C_{\mathcal{U}}(\bigcup\mathcal{R})=$
$=\bigcup\{C_{\mathcal{U}}(Q)\mid Q\subseteq\bigcup\mathcal{R}$ konečná$\}$, takže pro všechna $a\in P$ existuje konečná $Q_a\subseteq\bigcup\mathcal{R}$ t.ž. $a\in C_{\mathcal{U}}(Q_a)$. Protože $\bigcup_{a\in P}Q_a$ je konečná podmnožina $\bigcup\mathcal{R}$, tak existuje konečná $\mathcal{S}\subseteq\mathcal{R}$ t.ž. $\bigcup_{a\in P}Q_a\subseteq\bigcup\mathcal{S}$. Potom $P\subseteq C_{\mathcal{U}}(\bigcup_{a\in P}Q_a)\subseteq$
$\subseteq C_{\mathcal{U}}(\bigcup\mathcal{S})=\sup\mathcal{S}\in\mathcal{U}$. Takže $C_{\mathcal{U}}(P)\subseteq\sup\mathcal{S}$.

2) Předp., že $Q\in\mathcal{U}$ je kompaktní v $(\mathcal{U},\subseteq)$. Pak $Q=\bigcup\{C_{\mathcal{U}}(R)\mid R\subseteq Q$ kon.$\}=$
$=\sup\{C_{\mathcal{U}}(R)\mid R\subseteq Q$ konečná$\}=C_{\mathcal{U}}(R_1)\vee\dots\vee C_{\mathcal{U}}(R_n)=C_{\mathcal{U}}(\underbrace{R_1\cup\dots\cup R_n}_{\text{konečná}})$.

$\boxed{Q \text{ komp.} \Rightarrow \exists R_1,\dots,R_n\subseteq Q \text{ kon. t.ž. } Q=}$

3) $Q\in\mathcal{U}$ lib. Pak $Q=\bigcup\{C_{\mathcal{U}}(R)\mid R\subseteq Q$ konečná$\}=\sup\{C_{\mathcal{U}}(R)\mid R\subseteq Q$ kon.$\}$.

(Ve svazu všech podgrup dané grupy jsou kompaktními prvky právě konečně generované podgrupy a každá podgrupa je usměrněným sjednocením konečně generovaných. (analog. pro ostatní struk.))

Věta: Každý algebraický svaz $(L,\leq)$ je izomorfní $(\mathcal{U},\subseteq)$ pro nějaký algebraický uzávěrový systém $\mathcal{U}$.

Důkaz: Buď K množina všech kompaktních prvků L. Pak $\forall a\in L: a=\sup\{c\in K\mid c\leq a\}$, takže podle reprezentačního lemmatu je zobrazení $\varphi: L\to\mathcal{P}(K)$ definované předpisem $\varphi(a)=\{c\in K\mid c\leq a\}$ izomorfismus $(L,\leq)$ na uzávěrový systém $\varphi(L)$ na množině K. Zbývá ukázat, že pro každou usměrněnou podmnožinu J v $(L,\leq)$ platí $\bigcup\varphi(J)\in\varphi(L)$. Ukážeme, že $\bigcup\varphi(J)=\varphi(\sup J)$.

"$\subseteq$" plyne z monotonie φ.

"$\supseteq$" Předp. $c\in\varphi(\sup J)$, tj. $c\in K$, $c\leq\sup J$. Protože c je kompaktní, tak existují $a_1,\dots,a_n\in J$ t.ž. $c\leq a_1\vee\dots\vee a_n$. Jelikož J je usměrněná, tak existuje $a\in J$ t.ž. $a_1\vee\dots\vee a_n\leq a$. Tedy $c\in\varphi(a)\subseteq\bigcup\varphi(J)$.

Exkurz:

Scottovy domény jsou algebraické svazy, z nichž je případně odebraný největší prvek, pokud není dosažitelný jako supremum usměrněné podmnožiny.

Ekvivalentně: Jsou splněny podmínky
1) každá podmnožina buď nemá žádnou horní závoru nebo má supremum.
2) každá usměrněná podmnožina má supremum.

Každý prvek Scottovy domény představuje nějakou množinu konzistentních informací – je dosažitelný pomocí usměrněného suprema kompaktních prvků, což odpovídá aproximovatelnosti konečnými informacemi.

Infima = společné informace (vždy existují).

Suprema nemusejí existovat všechna, protože nelze dávat dohromady nekonzistentní informace. Každá nekonzistence ovšem vzniká už z konečně mnoha informací (věta o kompaktnosti v logice), takže suprema usměrněných množin existují.

UNIVERZÁLNÍ ALGEBRA

<u>Typ algeber</u> je množina τ, jejíž prvky se nazývají <u>operační symboly</u>, spolu se zobrazením $ar: \tau \to \mathbb{N}_0$, které každému operačnímu symbolu přiřazuje jeho <u>aritu</u>.

Budeme stručně mluvit o typu τ a o $f \in \tau$ t.ž. $ar(f)=n$ budeme mluvit jako o n-árním operačním symbolu.

<u>Algebra</u> $\mathcal{A}=(A,(f^{\mathcal{A}})_{f\in\tau})$ typu τ (stručně <u>τ-algebra</u>) je množina A (nazývaná <u>nosič</u> nebo <u>univerzum</u> $\mathcal{A}$) spolu s $ar(f)$-ární operací $f^{\mathcal{A}}: A^{ar(f)} \to A$ pro každý operační <u>symbol $f\in\tau$.</u> ($f^{\mathcal{A}}$ je realizace operačního symbolu f v $\mathcal{A}$)

Příklady: $\boxed{\text{Typ množin}: \tau = \{\}}$ Typ pologrup: $\tau=\{\cdot\}$, $ar(\cdot)=2$.

Typ grup: $\tau=\{\cdot,{}^{-1},1\}$, $ar(\cdot)=2$, $ar({}^{-1})=1$, $ar(1)=0$.

Příklad grupy: $\mathcal{A}=(\mathbb{Z},+,-,0)$, tj. $+=\cdot^{\mathcal{A}}$, $-={}^{-1\mathcal{A}}$, $0=1^{\mathcal{A}}$.

Typ Bool. algebry: $\tau=\{\vee,\wedge,0,1,'\}$, $ar(\vee)=ar(\wedge)=2$, $ar(0)=ar(1)=0$, $ar(')=1$.

Typ vektorových prostorů nad $\mathbb{R}$: $\tau=\{+,-,0\}\cup\{r\cdot \mid r\in\mathbb{R}\}$, $ar(+)=2$, $ar(-)=ar(r\cdot)=1$, $ar(0)=0$.

Typ det. automatů nad abecedou Σ bez koncových stavů: $\tau=\{\delta_\sigma \mid \sigma\in\Sigma\}\cup\{q_0\}$, $ar(\delta_\sigma)=1$, $ar(q_0)=0$.

(je to predikátová logika, kde nemáme relační symboly)

Symboly arity nula, tj. zobrazení z $A^0=\{\emptyset\}$ do A, představují <u>konstanty</u>, ale dá se s nimi pracovat stejně jako s ostatními symboly.

V každém typu τ existují jednoprvkové algebry.

Prázdná algebra v typu τ existuje $\iff$ τ neobsahuje konstanty.

(zdůraznit, že vždy uvažujeme pouze algebry 1 typu)

Definice: $\mathcal{A}=(A,(f^{\mathcal{A}})_{f\in\tau})$ algebra, $B\subseteq A$ podmnožina. Říkáme, že B je <u>nosičem podalgebry</u> algebry $\mathcal{A}$, jestliže pro každý n-ární symbol $f\in\tau$ a pro všechny prvky $a_1,\dots,a_n\in B$ platí $f^{\mathcal{A}}(a_1,\dots,a_n)\in B$.

Je-li B nosičem podalgebry $\mathcal{A}$, tak $\mathbb{B}=(B,(f^{\mathbb{B}})_{f\in\tau})$, kde $\forall a_1,\dots,a_n\in B: f^{\mathbb{B}}(a_1,\dots,a_n)=f^{\mathcal{A}}(a_1,\dots,a_n)$ (zúžení operace) je τ-algebra a říkáme jí <u>podalgebra</u> algebry $\mathcal{A}$. (ukázat na předch. příkladu)

Definice: $\mathcal{A}=(A,(f^{\mathcal{A}})_{f\in\tau})$, $\mathbb{B}=(B,(f^{\mathbb{B}})_{f\in\tau})$ lib. τ-algebry. Zobrazení $\varphi: A\to B$ se nazývá <u>homomorfismus</u> algebry $\mathcal{A}$ do algebry $\mathbb{B}$, jestliže pro každý n-ární symbol $f\in\tau$ a pro libovolné prvky $a_1,\dots,a_n\in A$ platí $\varphi(f^{\mathcal{A}}(a_1,\dots,a_n))=f^{\mathbb{B}}(\varphi(a_1),\dots,\varphi(a_n))$. (respektuje ~~zachovává~~ operace)

(pro konstantní symboly takto podmínka znamená zachování konstant: $\varphi(f^{\mathcal{A}})=f^{\mathbb{B}}$)

Příklady: $\varphi: (\mathbb{Z},+,-,0) \longrightarrow (\mathbb{Q}\setminus\{0\},\cdot,\frac{1}{-},1)$

$z \longmapsto 2^z$ je homomorfismus grup

$\varphi(z+t)=2^{z+t}=2^z\cdot 2^t=\varphi(z)\cdot\varphi(t)$

$\varphi(-z)=2^{-z}=\frac{1}{2^z}=\frac{1}{\varphi(z)}$

(všimnout si, že u binárních symbolů používáme infixovou notaci)

$\varphi(0)=2^0=1$

Homomorfismus vektorových prostorů = lineární zobrazení.

Např. $\varphi(r\cdot a)=r\cdot\varphi(a)$ pro všechny operace $r\cdot\in\tau$.

Konvence: $\mathcal{A}$ bude vždy značit algebru $(A,(f^{\mathcal{A}})_{f\in\tau})$, a analogicky pro $\mathbb{B},\mathbb{C},\mathbb{D}$.

Tvrzení: $\mathcal{A},\mathbb{B},\mathbb{C}$ τ-algebry. Pak $id: A\to A$ je homomorfismus $\mathcal{A}$ na $\mathcal{A}$.

Jsou-li $\varphi: A\to B$, $\psi: B\to C$ homomorfismy $\mathcal{A}$ do $\mathbb{B}$ a $\mathbb{B}$ do $\mathbb{C}$, tak $\psi\circ\varphi$ je homomorfismus $\mathcal{A}$ do $\mathbb{C}$.

Důkaz: $f\in\tau$ n-ární symbol, $a_1,\dots,a_n\in\mathcal{A}$.

1) $id(f^{\mathcal{A}}(a_1,\dots,a_n))=f^{\mathcal{A}}(id(a_1),\dots,id(a_n))$.

2) $\psi\circ\varphi(f^{\mathcal{A}}(a_1,\dots,a_n))=\psi(\varphi(f^{\mathcal{A}}(a_1,\dots,a_n)))=\psi(f^{\mathbb{B}}(\varphi(a_1),\dots,\varphi(a_n)))=f^{\mathbb{C}}(\psi(\varphi(a_1)),\dots,\psi(\varphi(a_n)))=$
$=f^{\mathbb{C}}(\psi\circ\varphi(a_1),\dots,\psi\circ\varphi(a_n))$.

Tvrzení: Je-li $\varphi: A \to B$ homomorfismus τ-algeber $\mathcal{A}$ a $\mathcal{B}$, $C \subseteq A$ nosič podalgebry $\mathcal{A}$ a $D \subseteq B$ nosič podalgebry $\mathcal{B}$, potom $\varphi(C)$ je nosič podalgebry $\mathcal{B}$ a $\varphi^{-1}(D)$ je nosič podalgebry $\mathcal{A}$. (2 obrázky)

Důkaz: 1) $f \in \tau$ n-ární, $b_1, \dots, b_n \in \varphi(C)$. Pak existují $c_1, \dots, c_n \in C$ t.ž. $\varphi(c_1) = b_1, \dots, \varphi(c_n) = b_n$.
Proto $f^{\mathcal{B}}(b_1, \dots, b_n) = f^{\mathcal{B}}(\varphi(c_1), \dots, \varphi(c_n)) = \varphi(f^{\mathcal{A}}(c_1, \dots, c_n)) \in \varphi(C)$.

2) $f \in \tau$ n-ární, $a_1, \dots, a_n \in \varphi^{-1}(D)$. Pak $\varphi(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(\underbrace{\varphi(a_1)}_{\in D}, \dots, \underbrace{\varphi(a_n)}_{\in D}) \in D$,
takže $f^{\mathcal{A}}(a_1, \dots, a_n) \in \varphi^{-1}(D)$.

<u>Izomorfismus</u> = homomorfismus, který je bijekce. Příklad: id_A je izom. $\mathcal{A}$ na $\mathcal{A}$.

Tvrzení: Inverze k izomorfismu je izomorfismus.

Důkaz: $\varphi: A \to B$ izomorfismus $\mathcal{A}$ na $\mathcal{B}$, $f \in \tau$ n-ární, $b_1, \dots, b_n \in B$.
Pak $\varphi^{-1}(f^{\mathcal{B}}(b_1, \dots, b_n)) = \varphi^{-1}(f^{\mathcal{B}}(\varphi(\varphi^{-1}(b_1)), \dots, \varphi(\varphi^{-1}(b_n)))) = \varphi^{-1}(\varphi(f^{\mathcal{A}}(\varphi^{-1}(b_1), \dots, \varphi^{-1}(b_n)))) =$
$= f^{\mathcal{A}}(\varphi^{-1}(b_1), \dots, \varphi^{-1}(b_n))$.

Algebry se nazývají <u>izomorfní</u>, jestliže mezi nimi existuje izomorfismus.

<u>Term</u> typu τ nad množinou proměnných X je libovolná posloupnost symbolů vzniklá v konečně mnoha krocích aplikací následujících pravidel:
1) Každý prvek X je term.
2) Je-li $f \in \tau$ n-ární operační symbol a $t_1, \dots, t_n$ jsou termy, tak
$\underbrace{f(t_1, \dots, t_n)}$ je term. (spec. případ: pro $ar(f) = 0$ je f term)
(nic se nevyhodnocuje, je to posloupnost symbolů)

Množinu všech termů typu τ nad X budeme značit $T_\tau(X)$.

Příklad: $X = \{x, y\}$, $\tau = \{\cdot, {}^{-1}, 1\}$. Pak $((1 \cdot x) \cdot y^{-1})^{-1} \cdot (x \cdot y)$ je term, jehož precizní zápis podle definice by byl $\cdot({}^{-1}(\cdot(\cdot(1, x), {}^{-1}(y))), \cdot(x, y))$.

Pro lib. typ τ a množinu proměnných X definujeme <u>algebru termů</u> typu τ nad X jako $\mathcal{T}_\tau(X) = (T_\tau(X), (f^{\mathcal{T}_\tau(X)})_{f \in \tau})$, kde pro každý n-ární symbol $f \in \tau$ a termy $t_1, \dots, t_n \in T_\tau(X)$ definujeme $f^{\mathcal{T}_\tau(X)}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$.
(operaci aplikuji na termy a ona vyrobí term tak, že před ně napíše svůj symbol)

Věta: Buď $\mathcal{A}$ τ-algebra, X lib. množina a $\varphi: X \to A$ lib. zobrazení.
Potom existuje jediný homomorfismus $\overline{\varphi}: \mathcal{T}_\tau(X) \to \mathcal{A}$ takový, že $\forall x \in X: \overline{\varphi}(x) = \varphi(x)$.

$$\begin{tikzcd} X \arrow[r, hook] \arrow[dr, "\varphi"', "\text{zobrazení}"] & \mathcal{T}_\tau(X) \arrow[d, "\overline{\varphi}\ \text{homomorfismus}"] \\ & \mathcal{A} \end{tikzcd}$$

Intuice: $\overline{\varphi}$ dosadí do termu t za každou proměnnou x hodnotu $\varphi(x) \in A$ a výsledný výraz vyhodnotí v $\mathcal{A}$ na hodnotu $\overline{\varphi}(t)$. Je to induktivní rozšíření φ z X na $T_\tau(X)$.

Důkaz: Indukcí vzhledem k délce termu t dokážeme, že existuje jediná možnost, jak definovat $\overline{\varphi}(t)$: 1) $\overline{\varphi}(x) = \varphi(x)$ $\forall x \in X$.
2) $\overline{\varphi}(f(t_1, \dots, t_n)) = \overline{\varphi}(f^{\mathcal{T}_\tau(X)}(t_1, \dots, t_n)) = f^{\mathcal{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_n))$ pro lib. n-ární $f \in \tau$ a
$t_1, \dots, t_n$ termy (kratší než $f(t_1, \dots, t_n)$)

Zbývá ověřit, že výše odvozený induktivní předpis $\overline{\varphi}(x) = x$,
$\overline{\varphi}(f(t_1, \dots, t_n)) = f^{\mathcal{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_n))$ definuje homomorfismus $\mathcal{T}_\tau(X)$ do $\mathcal{A}$:
pro lib. n-ární $f \in \tau$ a $t_1, \dots, t_n \in T_\tau(X)$ máme $\overline{\varphi}(f^{\mathcal{T}_\tau(X)}(t_1, \dots, t_n)) =$
$= \overline{\varphi}(f(t_1, \dots, t_n)) = f^{\mathcal{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_n))$.

Příklad: Typ $\tau=\{f,*\}$, $ar(f)=1$, $ar(*)=0$. Pak $T_\tau(\{x\})=\{f^n(x), f^n(*) \mid n\in\mathbb{N}_0\}$,
kde $f^n(x)$ značí term $\underbrace{f(\dots(f(x))\dots)}_{n\text{-krát}}$. Buď $\mathfrak{A}=(\mathbb{N}, succ, 1)$, $\varphi:\{x\}\to\mathbb{N}$, $x\mapsto 3$.
Potom $\overline{\varphi}(f^n(x))=(f^{\mathfrak{A}})^n(\varphi(x))=succ^n(3)=3+n$, $\overline{\varphi}(f^n(*))=(f^{\mathfrak{A}})^n(*^{\mathfrak{A}})=succ^n(1)=1+n$.

Předchozí věta říká, že existuje jednoznačná korespondence mezi zobrazeními $X\to A$ a homomorfismy $T_\tau(X)\to\mathfrak{A}$ daná přiřazeními $\varphi\mapsto\overline{\varphi}$ a $\psi|X \leftarrow\!\shortmid \psi$.

Speciální případ: Zvolíme-li za X množinu A a za φ zobrazení $id: A\to A$, tak $\overline{id}: T_\tau(A)\to\mathfrak{A}$ je vyhodnocovací homomorfismus, který vyhodnocuje formálně zapsané výrazy v algebře $\mathfrak{A}$. Označme ho $eval_{\mathfrak{A}}$.

Tvrzení: $\psi:\mathfrak{A}\to\mathfrak{B}$ homomorfismus, $\varphi: X\to A$ zobrazení. Potom $\overline{\psi\circ\varphi}=\psi\circ\overline{\varphi}$.

Důkaz: $\psi\circ\overline{\varphi}$ je homomorfismus $T_\tau(X)$ do $\mathfrak{B}$ takový, že $(\psi\circ\overline{\varphi})|X=\psi\circ(\overline{\varphi}|X)=\psi\circ\varphi$.
Ovšem takový homomorfismus je jen jeden, a to $\overline{\psi\circ\varphi}$.

Intuice: Tvrzení říká, že každý homomorfismus ψ zachovává vyhodnocování termů:

$$\forall t\in T_\tau(X):\ \underbrace{\overline{\psi\circ\varphi}(t)}_{\substack{\text{dosadíme do } t \text{ za } x\\ \text{hodnotu } \psi(\varphi(x)) \text{ a}\\ \text{vyhodnotíme v } \mathfrak{B}.}} = \underbrace{\psi(\overline{\varphi}(t))}_{\substack{\text{dosadíme do } t \text{ za } x \text{ hodnotu } \varphi(x),\\ \text{vyhodnotíme v } \mathfrak{A} \text{ a výsledek zobrazíme } \psi.}}$$

Přitom definice homomorfismu vyžaduje přesně to, aby tato rovnost platila pro termy $t=f(x_1,\dots,x_n)$, kde $f\in\tau$ je n-ární a $x_1,\dots,x_n\in X$ jsou různé proměnné:

pro $a_1,\dots,a_n\in A$, volíme-li totiž $\varphi(x_i)=a_i$, tak

$$\overline{\psi\circ\varphi}(f(x_1,\dots,x_n))=f^{\mathfrak{B}}(\overline{\psi\circ\varphi}(x_1),\dots,\overline{\psi\circ\varphi}(x_n))=f^{\mathfrak{B}}(\psi(\varphi(x_1)),\dots,\psi(\varphi(x_n)))=f^{\mathfrak{B}}(\psi(a_1),\dots,\psi(a_n))$$

$$\psi(\overline{\varphi}(f(x_1,\dots,x_n)))=\psi(f^{\mathfrak{A}}(\overline{\varphi}(x_1),\dots,\overline{\varphi}(x_n)))=\psi(f^{\mathfrak{A}}(a_1,\dots,a_n))$$

Pozorování: Pro $Y\subseteq X$ je $T_\tau(Y)$ podalgebra $T_\tau(X)$.

Věta: $\mathfrak{A}$ τ-algebra. Pak nosiče podalgeber algebry $\mathfrak{A}$ tvoří algebraický uzávěrový systém na A. Proto pro každou množinu $P\subseteq A$ existuje nejmenší nosič podalgebry $\mathfrak{A}$ obsahující P; příslušnou podalgebru nazýváme podalgebrou $\mathfrak{A}$ generovanou množinou P a značíme $\langle P\rangle$. Přitom platí $\langle P\rangle = eval_{\mathfrak{A}}(T_\tau(P))=$
$=\{\overline{\varphi}(t) \mid \varphi: X\to P \text{ zobrazení}, X \text{ konečná množina}, t\in T_\tau(X)\}$.

Důkaz: Označme $\mathcal{U}=\{B\subseteq A \mid B \text{ je nosič podalgebry } \mathfrak{A}\}$. Ukážeme, že $\mathcal{U}$ je algebr. uz. systém.

1) $A\in\mathcal{U}$.
2) Předp. $I\neq\emptyset$, $B_i\in\mathcal{U}$ pro $i\in I$. Ukážeme, že $\bigcap_{i\in I}B_i\in\mathcal{U}$.
Buď $f\in\tau$ n-ární, $a_1,\dots,a_n\in\bigcap_{i\in I}B_i$. Pak $\forall i\in I: a_1,\dots,a_n\in B_i$, takže $\forall i\in I: f^{\mathfrak{A}}(a_1,\dots,a_n)\in B_i$. Proto $f^{\mathfrak{A}}(a_1,\dots,a_n)\in\bigcap_{i\in I}B_i$.
3) Předp. $I\neq\emptyset$, $B_i\in\mathcal{U}$ pro $i\in I$, přičemž $\forall i,j\in I\ \exists k\in I: B_i\cup B_j\subseteq B_k$. (usměrněná podmnožina $\mathcal{U}$)
Ukážeme, že $\bigcup_{i\in I}B_i\in\mathcal{U}$. Buď $f\in\tau$ n-ární, $a_1,\dots,a_n\in\bigcup_{i\in I}B_i$. Potom existují $i_1,\dots,i_n\in I$ t.ž. $a_1\in B_{i_1},\dots,a_n\in B_{i_n}$. Díky usměrněnosti existuje $j\in I$ t.ž. $B_{i_1}\cup\dots\cup B_{i_n}\subseteq B_j$. Takže $a_1,\dots,a_n\in B_j$, a tedy $f^{\mathfrak{A}}(a_1,\dots,a_n)\in B_j\subseteq\bigcup_{i\in I}B_i$.

Buď $\varphi: X\twoheadrightarrow P$ lib. surjektivní zobrazení. Ukážeme, že $B=\overline{\varphi}(T_\tau(X))$ je nejmenší nosič podalgebry $\mathfrak{A}$ obsahující P, tj. $C_{\mathcal{U}}(P)$.
1) B je obrazem nosiče podalgebry v homomorfismu, takže je to nosič podalgebry.
2) $P=\varphi(X)=\overline{\varphi}(X)\subseteq B$ (díky surjektivitě)
3) Je-li $C\in\mathcal{U}$ lib. t.ž. $P\subseteq C$, tak máme $\varphi: X\to C$, a proto $\overline{\varphi}$ je homomorfismus $T_\tau(X)$ do C, takže $\underset{B=}{}\overline{\varphi}(T_\tau(X))\subseteq C$.

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[d, "\varphi"'] & T_\tau(X) \arrow[d, "\overline{\varphi}"'] \arrow[dr, "\overline{\varphi}"] & \\
P \arrow[r, hook] & C \arrow[r, hook] & A
\end{tikzcd}$$

Jelikož příslušný uzávěrový operátor $C_\mathcal{U}$ je algebraický, platí:

$$\langle P\rangle = C_\mathcal{U}(P) = \bigcup_{Q\subseteq P \text{ kon.}} C_\mathcal{U}(Q) = \bigcup_{Q\subseteq P \text{ kon.}} \langle Q\rangle = \bigcup\{\varphi(T_\tau(X)) \mid \varphi: X \twoheadrightarrow Q \text{ surj. zobr.}, Q\subseteq P \text{ konečná}, X \text{ konečná}\}$$

Pozn.: Víme, že kompaktní prvky jsou právě $C_\mathcal{U}(P)$ pro $P\subseteq A$ konečnou, tj. konečněgenerované podalgebry.

Tvrzení: ~~Pro~~ Každý algebraický uzávěrový operátor C na libovolné množině A existuje algebra s nosičem A t.ž. $\forall P\subseteq A: \langle P\rangle = C(P)$. Proto každý algebraický svaz je izomorfní svazu podalgeber nějaké algebry. (Znamená to, že algebraičnost je jediná vlastnost společná všem svazům podalgeber)
Důkaz neuveden.

<u>Přímý součin</u> τ-algeber $\mathcal{A}$ a $\mathcal{B}$ je algebra $\mathcal{A}\times\mathcal{B} = (A\times B, (f^{\mathcal{A}\times\mathcal{B}})_{f\in\tau})$ s operacemi definovanými předpisem $f^{\mathcal{A}\times\mathcal{B}}((a_1,b_1),\dots,(a_n,b_n)) = (f^{\mathcal{A}}(a_1,\dots,a_n), f^{\mathcal{B}}(b_1,\dots,b_n))$ pro $f\in\tau$ n-ární, $a_1,\dots,a_n\in A$, $b_1,\dots,b_n\in B$. (po složkách)

Chceme získat popis všech homomorfismů vedoucích z dané algebry $\mathcal{A}$.

<u>Kongruence</u> algebry $\mathcal{A}$ je relace ekvivalence $\sim$ na A t.ž. pro každý n-ární symbol $f\in\tau$ a libovolné prvky $a_1,\dots,a_n, a'_1,\dots,a'_n\in A$ splňující $a_1\sim a'_1,\dots,a_n\sim a'_n$ platí $f^{\mathcal{A}}(a_1,\dots,a_n)\sim f^{\mathcal{A}}(a'_1,\dots,a'_n)$. (Znamená to, že když v libovolném výrazu nahradíme nějaké prvky prvky s nimi ekvivalentními, tak výsledky vyhodnocení původního a nového výrazu budou ekvivalentní.)

Ekvivalentně můžeme kongruenci definovat jako relaci ekvivalence, která je podalgebrou algebry $\mathcal{A}\times\mathcal{A}$:

$$(a_1,a'_1)\in\sim,\dots,(a_n,a'_n)\in\sim \implies \underset{(f^{\mathcal{A}}(a_1,\dots,a_n),\, f^{\mathcal{A}}(a'_1,\dots,a'_n))}{\underset{\parallel}{f^{\mathcal{A}\times\mathcal{A}}((a_1,a'_1),\dots,(a_n,a'_n))}}\in\sim$$

Podobně, homomorfismus $\mathcal{A}$ do $\mathcal{B}$ můžeme definovat jako zobrazení, které je podalgebrou $\mathcal{A}\times\mathcal{B}$:

$$\underbrace{(a_1,b_1)\in\varphi}_{\varphi(a_1)=b_1},\dots,\underbrace{(a_n,b_n)\in\varphi}_{\varphi(a_n)=b_n} \implies \underset{\underbrace{(f^{\mathcal{A}}(a_1,\dots,a_n),\, f^{\mathcal{B}}(b_1,\dots,b_n))}_{\varphi(f^{\mathcal{A}}(a_1,\dots,a_n)) = f^{\mathcal{B}}(b_1,\dots,b_n)}}{\underset{\parallel}{f^{\mathcal{A}\times\mathcal{B}}((a_1,b_1),\dots,(a_n,b_n))}}\in\varphi$$

Definice: $\mathcal{A},\mathcal{B}$ τ-algebry, $\varphi: A\to B$ homomorfismus. <u>Jádrem</u> φ myslíme relaci $\ker\varphi = \{(a,a')\in A\times A \mid \varphi(a)=\varphi(a')\}$.

Platí: φ je injektivní $\iff \ker\varphi = \Delta_A$.

Tvrzení: Jádro libovolného homomorfismu $\varphi:\mathcal{A}\to\mathcal{B}$ je kongruencí algebry $\mathcal{A}$.

Důkaz: $\ker\varphi$ je relace ekvivalence.

$(a_1,a'_1)\in\ker\varphi,\dots,(a_n,a'_n)\in\ker\varphi \implies \varphi(a_1)=\varphi(a'_1),\dots,\varphi(a_n)=\varphi(a'_n) \implies$

$\varphi(f^{\mathcal{A}}(a_1,\dots,a_n)) = f^{\mathcal{B}}(\varphi(a_1),\dots,\varphi(a_n)) = f^{\mathcal{B}}(\varphi(a'_1),\dots,\varphi(a'_n)) = \varphi(f^{\mathcal{A}}(a'_1,\dots,a'_n)) \implies$

$(f^{\mathcal{A}}(a_1,\dots,a_n), f^{\mathcal{A}}(a'_1,\dots,a'_n))\in\ker\varphi$.

Tvrzení: $\varphi:\mathcal{A}\twoheadrightarrow\mathcal{B}$, $\psi:\mathcal{A}\to\mathcal{C}$ homomorfismy, φ surjektivní. Pak existuje homomorfismus $\sigma:\mathcal{B}\to\mathcal{C}$ t.ž. $\sigma\circ\varphi=\psi \iff \ker\varphi\subseteq\ker\psi$. Tento homomorfismus σ je určen jednoznačně. Přitom platí: σ je surjektivní $\iff$ ψ je surjektivní. σ je injektivní $\iff \ker\varphi=\ker\psi$.

Důkaz: "$\Longrightarrow$" $(a,a')\in\ker\varphi \implies \varphi(a)=\varphi(a') \implies \psi(a)=\sigma(\varphi(a))=\sigma(\varphi(a'))=\psi(a') \implies (a,a')\in\ker\psi$.

$$\begin{tikzcd} & a\in\mathcal{A} \arrow[dl, "\varphi"'] \arrow[dr, "\psi"] & \\ b\in\mathcal{B} \arrow[rr, dashed, "\sigma"'] & & \mathcal{C}\ni\psi(a)=\sigma(b) \end{tikzcd}$$

"$\Longleftarrow$" Pro $b\in B$ buď $a\in A$ lib. t.ž. $\varphi(a)=b$. Pak musí platit $\sigma(b)=\sigma(\varphi(a))=\psi(a)$, takže σ je jednoznačně určen předpisem $\sigma(b)=\psi(a)$.

Korektnost předpisu: a,a' t.ž. $\varphi(a)=\varphi(a')=b$. Pak $(a,a')\in\ker\varphi\subseteq\ker\psi$, a tedy $\psi(a)=\psi(a')$.

σ je homomorfismus: $f\in\tau$ n-ární, $b_1,\dots,b_n\in B$, $a_1,\dots,a_n\in A$ t.ž. $\varphi(a_1)=b_1,\dots,\varphi(a_n)=b_n$. Pak $\varphi(f^{\mathcal{A}}(a_1,\dots,a_n)) = f^{\mathcal{B}}(b_1,\dots,b_n)$, a proto $\sigma(f^{\mathcal{B}}(b_1,\dots,b_n)) = \psi(f^{\mathcal{A}}(a_1,\dots,a_n)) = f^{\mathcal{C}}(\psi(a_1),\dots,\psi(a_n)) = f^{\mathcal{C}}(\sigma(b_1),\dots,\sigma(b_n))$

Protože φ je surjektivní, tak σ je surj. $\Longleftrightarrow$ $\sigma\circ\varphi$ je surj.

Je-li σ injektivní, tak pro lib. $(a,a')\in \ker\psi$ ze $\sigma(\varphi(a))=\psi(a)=\psi(a')=\sigma(\varphi(a'))$ dostáváme $\varphi(a)=\varphi(a')$, tj. $(a,a')\in\ker\varphi$.

Předp. $\ker\varphi=\ker\psi$. Ze $\sigma(b)=\sigma(b')$ plyne $\psi(a)=\sigma(\varphi(a))=\sigma(\varphi(a'))=\psi(a')$, kde $a,a'\in A$ jsou lib. t.ž. $\varphi(a)=b$, $\varphi(a')=b'$. Proto $(a,a')\in\ker\psi$, z čehož plyne $(a,a')\in\ker\varphi$. Tedy $b=\varphi(a)=\varphi(a')=b'$.

(injektivita je opačná inkluze ke korektnosti předpisu)

Je-li $\sim$ kongruence τ-algebry $\mathcal{A}$, můžeme na množině $A/_\sim=\{[a]_\sim \mid a\in A\}$, kde $[a]_\sim=\{a'\in A \mid a'\sim a\}$, definovat pro každý n-ární symbol $f\in\tau$ jeho realizaci předpisem $f^{\mathcal{A}/\sim}([a_1]_\sim,\dots,[a_n]_\sim)=[f^{\mathcal{A}}(a_1,\dots,a_n)]_\sim$. (pomocí reprezentantů)

Tato definice je korektní, protože z $[a_1]_\sim=[a'_1]_\sim,\dots,[a_n]_\sim=[a'_n]_\sim$ plyne $[f^{\mathcal{A}}(a_1,\dots,a_n)]_\sim=[f^{\mathcal{A}}(a'_1,\dots,a'_n)]_\sim$. (to je přesně definice kongruence)

Dostáváme tedy τ-algebru $\mathcal{A}/_\sim=(A/_\sim,(f^{\mathcal{A}/\sim})_{f\in\tau})$.

Tvrzení: $\mathcal{A}$ τ-algebra, $\sim$ kongruence $\mathcal{A}$. Potom zobrazení $\nu_\sim: A\to A/_\sim$ definované předpisem $\nu_\sim(a)=[a]_\sim$ pro $a\in A$ je surjektivní homomorfismus s jádrem $\sim$.

Důkaz: surjektivita zřejmá.

$(a,a')\in\ker\nu_\sim \Longleftrightarrow [a]_\sim=[a']_\sim \Longleftrightarrow a\sim a'$.

$\nu_\sim$ je homomorfismus: $f\in\tau$ n-ární, $a_1,\dots,a_n\in A$. Pak $\nu_\sim(f^{\mathcal{A}}(a_1,\dots,a_n))=[f^{\mathcal{A}}(a_1,\dots,a_n)]_\sim=$
$=f^{\mathcal{A}/\sim}([a_1]_\sim,\dots,[a_n]_\sim)=f^{\mathcal{A}/\sim}(\nu_\sim(a_1),\dots,\nu_\sim(a_n))$.

Takže kongruence jsou právě jádra homomorfismů.

Tvrzení: $\mathcal{A},\mathcal{B}$ τ-algebry, $\varphi: A\to B$ homomorfismus. Pak podalgebra $\varphi(A)$ algebry $\mathcal{B}$ je izomorfní $\mathcal{A}/\ker\varphi$.

Důkaz: Protože $\ker\varphi=\ker(\nu_{\ker\varphi})$ a $\nu_{\ker\varphi}$ je surjektivní homomorfismus, existuje injektivní homomorfismus $\sigma:\mathcal{A}/\ker\varphi\to\mathcal{B}$ splňující $\sigma\circ\nu_{\ker\varphi}=\varphi$, jehož obrazem je $\varphi(A)$.

$$\begin{tikzcd} & \mathcal{A} \arrow[dl, "\nu_{\ker\varphi}"'] \arrow[dr, "\varphi"] & \\ \mathcal{A}/\ker\varphi \arrow[rr, "\sigma"'] & & \mathcal{B} \end{tikzcd}$$

Každý homomorfismus φ se tedy rozkládá následovně:

$$\begin{tikzcd} \mathcal{A} \arrow[r, "\varphi"] \arrow[d, "\nu_{\ker\varphi}"', "\text{surjekt.}"] & \mathcal{B} \\ \mathcal{A}/\ker\varphi \arrow[r, "\text{izom.}", "\sigma"'] & \varphi(A) \arrow[u, "\text{vložení podalgebry}"'] \end{tikzcd}$$

V případě grup, okruhů, vektorových prostorů, apod. je celá kongruence jednoznačně určená třídou, do které patří neutrální prvek (viz cvičení).

Toto obecně neplatí: např. monoid $(\mathbb{N}_0,+)$ má pro každé $n\in\mathbb{N}_0$ kongruenci definovanou $a\sim b :\Longleftrightarrow a=b$ nebo $(a\geq n \;\&\; b\geq n)$.

Tvrzení: $\mathcal{A}$ τ-algebra, $\sim$ kongruence $\mathcal{A}$. Pak existuje vzájemně jednoznačná korespondence mezi kongruencemi $\approx$ algebry $\mathcal{A}/_\sim$ a kongruencemi $\eqsim$ algebry $\mathcal{A}$ takovými, že $\eqsim\,\supseteq\,\sim$. Tato korespondence je určená předpisem $[a]_\sim\approx[a']_\sim \Longleftrightarrow a\eqsim a'$. Přitom platí $(\mathcal{A}/_\sim)/_\approx\cong\mathcal{A}/_\eqsim$.

Důkaz: Kongruence $\mathcal{A}$ jsou právě jádra homomorfismů $\varphi:\mathcal{A}\to\mathcal{B}$ do všech možných algeber $\mathcal{B}$, a kongruence $\mathcal{A}/_\sim$ jsou jádra homomorfismů $\psi:\mathcal{A}/_\sim\to\mathcal{B}$.

Definujeme zobrazení mezi jádry homomorfismů z $\mathcal{A}/_\sim$ a jádry homomorfismů z $\mathcal{A}$ splňujícími $\ker\varphi\supseteq\sim$: $\ker\psi\mapsto\ker(\psi\circ\nu_\sim)$

$$\begin{tikzcd} & \mathcal{A} \arrow[dl, "\nu_\sim"'] \arrow[dr, "\varphi"] & \\ \mathcal{A}/_\sim \arrow[rr, "\psi"] & & \mathcal{B} \end{tikzcd}$$

korektnost: $(a,a')\in\ker(\psi\circ\nu_\sim)\Longleftrightarrow([a]_\sim,[a']_\sim)\in\ker\psi$

$\ker\varphi\mapsto\ker\psi$, kde ψ je jediný homomorfismus t.ž. $\psi\circ\nu_\sim=\varphi$ (existuje jediný, $\ker\nu_\sim=\sim\subseteq\ker\varphi$)

korektnost: $([a]_\sim,[a']_\sim)\in\ker\psi\Longleftrightarrow(a,a')\in\ker\varphi$

Obě přiřazení jsou tedy určena předpisem $[a]_\sim\approx[a']_\sim\Longleftrightarrow a\eqsim a'$, takže jde o jednoznačnou korespondenci.

Přitom $(\mathcal{A}/_\sim)/_{\ker\psi}\cong\psi(\mathcal{A}/_\sim)=\varphi(\mathcal{A})\cong\mathcal{A}/_{\ker\varphi}$.

Tvrzení: Kongruence libovolné τ-algebry $\mathcal{A}$ tvoří algebraický uzávěrový systém na množině $A\times A$. Proto pro každou podmnožinu $P\subseteq A\times A$ existuje nejmenší kongruence algebry $\mathcal{A}$ obsahující P, kterou nazýváme <u>kongruence generovaná</u> P a značíme $\langle P\rangle_{cong}$. Přitom platí:

$$\langle P\rangle_{cong} = tr\Big(\{(\overline{\varphi}(t),\overline{\psi}(t)) \mid t\in T_\tau(X),\ X \text{ konečná množina},\ x\in X,\ \varphi,\psi: X\to A \text{ zobrazení splňující } ((\varphi(x),\psi(x))\in P \text{ nebo } (\psi(x),\varphi(x))\in P)\ \&\ (\forall y\in X\setminus\{x\}: \varphi(y)=\psi(y))\}\Big) =$$

$$= tr\Big(\{\overline{\varrho}(t) \mid t\in T_\tau(X),\ X \text{ konečná množina},\ x\in X,\ \varrho: X\to A\times A \text{ t.ž. } \varrho(x)\in P\cup P^{-1}\ \&\ \forall y\in X\setminus\{x\}: \varrho(y)\in\Delta_A\}\Big)$$

(stačí v termu nahrazovat jediný prvek, protože pomocí tranzitivního uzávěru můžeme postupně nahradit všechny)

Důkaz: Protože kongruence jsou právě relace ekvivalence, které jsou podalgebry $\mathcal{A}\times\mathcal{A}$, tak jsou uzavřené na $\bigcap$ a usměrněná $\bigcup$, a tedy tvoří algebr. uzávěrový systém.
Množiny $\{(\overline{\varphi}(t),\overline{\psi}(t))\mid \dots\}$ a $\{\overline{\varrho}(t)\mid\dots\}$ jsou si rovny, protože homomorfismy $\overline{\varrho}$ do $\mathcal{A}\times\mathcal{A}$ jednoznačně odpovídají dvojicím homomorfismů $\overline{\varphi}$ a $\overline{\psi}$ do $\mathcal{A}$ (2 složky, detaily později); tuto množinu označme Q. Ukážeme, že $\langle P\rangle_{cong}=tr(Q)$.

1) Předp., že $\sim$ je lib. kongruence $\mathcal{A}$ obsahující P.
$\sim$ reflexivní a symetrická $\Rightarrow P\cup P^{-1}\cup\Delta_A\subseteq\sim$.
$\sim$ je podalgebra $\mathcal{A}\times\mathcal{A} \Rightarrow Q\subseteq\sim$. $\sim$ tranzitivní $\Rightarrow tr(Q)\subseteq\sim$.

2) Pro $(a,a')\in P$ dostáváme $(a,a')\in Q$ volbou $X=\{x\}$, $t=x$, $\varrho(x)=(a,a')$.

3) Ukážeme, že $tr(Q)$ je kongruence $\mathcal{A}$.

(i) Q je reflexivní: pro $a\in A$ lib. volíme $\varrho(y)=(a,a)$, $t=y$. Pak $\overline{\varrho}(t)=(a,a)$.

(ii) Q je symetrická: pro lib. $(\overline{\varphi}(t),\overline{\psi}(t))\in Q$ patří do Q rovněž $(\overline{\psi}(t),\overline{\varphi}(t))$, protože podmínka na φ a ψ je symetrická.

(iii) Tranzitivní obal reflexivní a symetrické relace je relace ekvivalence $\Rightarrow$
$\Rightarrow tr(Q)$ je relace ekvivalence.

(iv) $tr(Q)$ je podalgebra $\mathcal{A}\times\mathcal{A}$: $f\in\tau$ n-ární symbol, $(a_1,a_1'),\dots,(a_n,a_n')\in tr(Q)$.
Potřebujeme dokázat, že $(f^{\mathcal{A}}(a_1,\dots,a_n), f^{\mathcal{A}}(a_1',\dots,a_n'))\in tr(Q)$, k čemuž stačí ověřit, že $tr(Q)$ obsahuje páry $(f^{\mathcal{A}}(a_1,\dots,a_n), f^{\mathcal{A}}(a_1',a_2,\dots,a_n))$, $(f^{\mathcal{A}}(a_1',a_2,a_3,\dots,a_n), f^{\mathcal{A}}(a_1',a_2',a_3,\dots,a_n)),\dots,(f^{\mathcal{A}}(a_1',\dots,a_{n-1}',a_n), f^{\mathcal{A}}(a_1',\dots,a_n'))$.
Dokažme $(f^{\mathcal{A}}(a_1',\dots,a_{i-1}',a_i,a_{i+1},\dots,a_n), f^{\mathcal{A}}(a_1',\dots,a_{i-1}',a_i',a_{i+1},\dots,a_n))\in tr(Q)$.
Z $(a_i,a_i')\in tr(Q)$ plyne existence kon. množin $X_1,\dots,X_m$, proměnných $x_1\in X_1,\dots,x_m\in X_m$ a termů $t_1\in T_\tau(X_1),\dots,T_\tau(X_m)$ takových, že $a_i=\overline{\varphi_1}(t_1)$, $a_i'=\overline{\psi_m}(t_m)$ a $\forall j=1,\dots,m-1$: $\overline{\psi_j}(t_j)=\overline{\varphi_{j+1}}(t_{j+1})$, přičemž φ_j a ψ_j splňují $(\varphi_j(x_j),\psi_j(x_j))\in P\cup P^{-1}$ a $\forall y\in X_j\setminus\{x_j\}: \varphi_j(y)=\psi_j(y)$, pro $j=1,\dots,m$.
Zvolme $t_j'=f(z_1,\dots,z_{i-1},t_j,z_{i+1},\dots,z_n)$, kde $z_1,\dots,z_n$ jsou nové proměnné, a rozšiřme φ_j a ψ_j na $X_j\cup\{z_1,\dots,z_n\}$ pro všechna j předpisem
$\varphi_j(z_k)=\psi_j(z_k)=\begin{cases}a_k' & \text{pro } k<i\\ a_k & \text{pro } k>i\end{cases}$. Pak $\overline{\varphi_1}(t_1')=f^{\mathcal{A}}(a_1',\dots,a_{i-1}',a_i,a_{i+1},\dots,a_n)$,
$\overline{\psi_m}(t_m')=f^{\mathcal{A}}(a_1',\dots,a_{i-1}',a_i',a_{i+1},\dots,a_n)$ a $\overline{\psi_j}(t_j')=f^{\mathcal{A}}(a_1',\dots,a_{i-1}',\overline{\psi_j}(t_j),a_{i+1},\dots,a_n)=$
$=f^{\mathcal{A}}(a_1',\dots,a_{i-1}',\overline{\varphi_{j+1}}(t_{j+1}),a_{i+1},\dots,a_n)=\overline{\varphi_{j+1}}(t_{j+1}')$.

Důsledek: Svaz kongruencí lib. algebry $\mathcal{A}$ je úplným podsvazem svazu ekvivalencí na A.

Důkaz: Infima jsou průniky.
Buďte $\sim_i$ pro $i\in I$ kongruence algebry $\mathcal{A}$. Pak $\sup\limits_{i\in I}\sim_i=\langle\bigcup_{i\in I}\sim_i\rangle_{cong}=$
$=tr\Big(\{\overline{\varrho}(t)\mid t\in T_\tau(X),\ X \text{ konečná množina},\ x\in X,\ \varrho:X\to A\times A,\ \varrho(x)\in\underbrace{\bigcup_{i\in I}\sim_i}_{\text{je symetrická}},\ \forall y\in X\setminus\{x\}:\varrho(y)\in\Delta_A\}\Big)=$
$=tr(\bigcup_{i\in I}\sim_i)$, protože "$\subseteq$" plyne z toho, že $\varrho(x)\in\sim_i$ pro nějaké $i\in I$, a tedy $\overline{\varrho}(t)\in\langle\sim_i\rangle_{cong}=\sim_i$.
"$\supseteq$" dostáváme volbou $t=x$.

$\prod_{i\in I} A_i = \{\alpha: I \to \bigcup_{i\in I} A_i \mid \forall i\in I: \alpha(i)\in A_i\}$, přičemž prvek $\alpha \in \prod_{i\in I} A_i$ t.ž. $\alpha(i)=a_i$ pro $i\in I$ obvykle zapisujeme $(a_i)_{i\in I}$.

Přímý součin τ-algeber $\mathcal{A}_i = (A_i, (f^{\mathcal{A}_i})_{f\in\tau})$ pro $i\in I$ je algebra

$\prod_{i\in I}\mathcal{A}_i = (\prod_{i\in I} A_i, (f^{\prod_{i\in I}\mathcal{A}_i})_{f\in\tau})$, kde pro $f\in\tau$ n-ární a $a_{i,k}\in A_i$ pro $i\in I$, $k=1,\dots,n$,

je definováno $f^{\prod_{i\in I}\mathcal{A}_i}((a_{i,1})_{i\in I},\dots,(a_{i,n})_{i\in I}) = (f^{\mathcal{A}_i}(a_{i,1},\dots,a_{i,n}))_{i\in I}$. (po složkách)

Speciální případ: $I=\emptyset \Rightarrow \prod_{i\in\emptyset} A_i = \emptyset^\emptyset$ je jednoprvková algebra.

Zobrazení projekce $\pi_j: \prod_{i\in I} A_i \to A_j$ jsou homomorfismy:

$$\pi_j\left(f^{\prod\mathcal{A}_i}((a_{i,1})_{i\in I},\dots,(a_{i,n})_{i\in I})\right) = f^{\mathcal{A}_j}(a_{j,1},\dots,a_{j,n}) =$$
$$= f^{\mathcal{A}_j}(\pi_j((a_{i,1})_{i\in I}),\dots,\pi_j((a_{i,n})_{i\in I})).$$

Pokud $\forall i\in I: A_i\neq\emptyset$, tak jsou všechna π_j surjektivní (to je přesně axiom výběru), takže každá algebra $\mathcal{A}_j$ je homomorfním obrazem $\prod_{i\in I}\mathcal{A}_i$.

Pozor, $\mathcal{A}$ nemusí být podalgebrou $\mathcal{A}\times\mathcal{B}$: $(\{1\},\cdot)\times(\mathbb{N},+)\cong(\mathbb{N},+)$. (platilo pro grupy, okruhy a vekt. prostory)

Příklad: Bool. okruh $(P(A),\Delta,\cap,\emptyset,A,')$ je izomorfní $\prod_{a\in A}(\mathbb{Z}_2,+,\cdot,[0]_2,[1]_2,')$. (analog. pro Bool. algebry)

$$\{a\in A\mid t_a=[1]_2\} \longleftrightarrow (t_a)_{a\in A}$$

Směřujeme ke zjištění, kdy lze danou algebru pomocí součinu rozložit. (např. spočetně rozměrný vekt. prostor nad $\mathbb{Z}_2$ není přímým součinem přímo nerozložitelných)

Tvrzení: Jsou-li $\varphi_i:\mathcal{A}\to\mathcal{A}_i$ pro $i\in I$ lib. homomorfismy, tak zobrazení

$\varphi=(\varphi_i)_{i\in I}: A\to\prod_{i\in I}A_i$ definované předpisem $(\varphi_i)_{i\in I}(a)=(\varphi_i(a))_{i\in I}$ je

homomorfismus $\mathcal{A}$ do $\prod_{i\in I}\mathcal{A}_i$ s jádrem $\bigcap_{i\in I}\ker\varphi_i$ a splňuje $\forall j\in I: \pi_j\circ\varphi=\varphi_j$.

Přitom podmínka $\forall j\in I:\pi_j\circ\varphi=\varphi_j$ určuje φ jednoznačně.

$$\begin{tikzcd}
\mathcal{A} \arrow[rr, "(\varphi_i)_{i\in I}"] \arrow[d, "\varphi_j"'] \arrow[drr, "\varphi_k"] & & \prod_{i\in I}\mathcal{A}_i \arrow[dll, "\pi_j"'] \arrow[d, "\pi_k"] \\
\mathcal{A}_j & & \mathcal{A}_k
\end{tikzcd}$$

(speciální případ $I=\emptyset$ dává jediný homomorfismus do triviální algebry)

Důkaz: 1) $(\varphi_i)_{i\in I}(f^{\mathcal{A}}(a_1,\dots,a_n)) = (\varphi_i(f^{\mathcal{A}}(a_1,\dots,a_n)))_{i\in I} = (f^{\mathcal{A}_i}(\varphi_i(a_1),\dots,\varphi_i(a_n)))_{i\in I} =$

$= f^{\prod\mathcal{A}_i}((\varphi_i(a_1))_{i\in I},\dots,(\varphi_i(a_n))_{i\in I}) = f^{\prod_{i\in I}\mathcal{A}_i}((\varphi_i)_{i\in I}(a_1),\dots,(\varphi_i)_{i\in I}(a_n))$

2) $(a,a')\in\ker(\varphi_i)_{i\in I} \iff (\varphi_i(a))_{i\in I}=(\varphi_i(a'))_{i\in I}\iff\forall i\in I:\varphi_i(a)=\varphi_i(a')\iff(a,a')\in\bigcap_{i\in I}\ker\varphi_i$

3) $\pi_j((\varphi_i)_{i\in I}(a))=\pi_j((\varphi_i(a))_{i\in I})=\varphi_j(a)$

Podpřímý součin algeber $\mathcal{A}_i$, $i\in I$, je libovolná podalgebra $\mathcal{B}$ algebry $\prod_{i\in I}\mathcal{A}_i$ t.ž.

$\forall j\in I: \pi_j|_B: \mathcal{B}\to\mathcal{A}_j$ je surjektivní (tj. na každé složce jsou všechny prvky použity).
(je-li některá A_i prázdná a některá neprázdná, tak žádný podpřímý součin neexistuje)

Příklad: Grupa $(\mathbb{Z},+)$ je izomorfní podpřímému součinu grup $(\mathbb{Z}_m,+)$ pro $m\in\mathbb{N}$.

$$z\longmapsto([z]_m)_{m\in\mathbb{N}}$$
$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi=(\nu_m)_{m\in\mathbb{N}}"] \arrow[dr, "\nu_m"'] & \prod\mathbb{Z}_m \arrow[d, "\pi_m"] \\
& \mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}
\end{tikzcd}$$

$\ker\varphi=\bigcap_{m\in\mathbb{N}}\ker\nu_m=\bigcap_{m\in\mathbb{N}} m\mathbb{Z}=\{0\}\Rightarrow\varphi$ je injektivní.

($\mathbb{Z}$ je tedy podpřímo rozložitelná)

Definice: τ-Algebra $\mathcal{A}$ se nazývá podpřímo nerozložitelná, jestliže pro každý injektivní homomorfismus $\varphi:\mathcal{A}\to\prod_{i\in I}\mathcal{A}_i$, t.ž. $\forall j\in I:\pi_j\circ\varphi$ je surjektivní, (kde $\mathcal{A}_i$ jsou lib. τ-algebry) existuje $j\in I$ t.ž. $\pi_j\circ\varphi:\mathcal{A}\to\mathcal{A}_j$ je izomorfismus.

(tj. při libovolném pokusu o rozklad musíme $\mathcal{A}$ na nějaké složce použít) (až na izomorfismus)

Tvrzení: $\mathcal{A}$ algebra, $\sim_i$ pro $i \in I$ kongruence $\mathcal{A}$ t.ž. $\bigcap_{i\in I} \sim_i = \Delta_A$

(tj. pro lib. $a, a' \in A$, $a \neq a'$, existuje $i \in I$ t.ž. $a \not\sim_i a'$), tj. $\sim_i$ je rozlišuje).

Pak $\varphi = (\nu_{\sim_i})_{i\in I} : \mathcal{A} \longrightarrow \prod_{i\in I} \mathcal{A}/\sim_i$ je injektivní homomorfismus t.ž. $\varphi(\mathcal{A})$ je podpřímý součin algeber $\mathcal{A}/\sim_i$ pro $i \in I$.

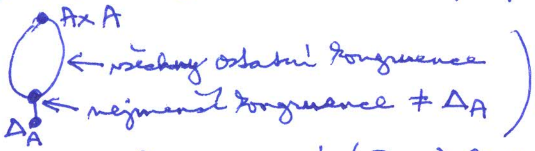
$$\begin{tikzcd}
\mathcal{A} \arrow[r, "\varphi = (\nu_{\sim_i})_{i\in I}"] \arrow[dr, "\nu_{\sim_j}"'] & \prod_{i\in I} \mathcal{A}/\sim_i \arrow[d, "\pi_j"] \\
& \mathcal{A}/\sim_j
\end{tikzcd}$$

Důkaz: $\ker((\nu_{\sim_i})_{i\in I}) = \bigcap_{i\in I} \ker \nu_{\sim_i} = \bigcap_{i\in I} \sim_i = \Delta_A \Rightarrow (\nu_{\sim_i})_{i\in I}$ je injektivní.

$\pi_j(\varphi(\mathcal{A})) = \nu_{\sim_j}(\mathcal{A}) = \mathcal{A}/\sim_j \Rightarrow \pi_j|\varphi(\mathcal{A})$ je surj.

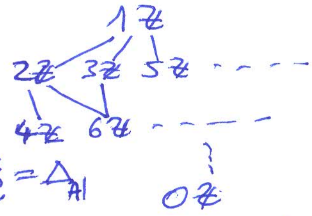
Věta: Algebra $\mathcal{A}$ je podpřímo nerozložitelná $\Longleftrightarrow$ je triviální nebo má nejmenší kongruenci různou od Δ_A.

(tj. svaz kongruencí netriv. podpřímo nerozložitelných algeber vypadá takto:



)

Příklad: svaz kongruencí $(\mathbb{Z}, +) \cong$ svaz podgrup $(\mathbb{Z}, +)$:



Důkaz: „$\Rightarrow$" Předp., že $\mathcal{A}$ není triviální a nemá nejmenší kongruenci různou od Δ_A. Pak $\bigcap \underbrace{\{\sim \mid \sim \text{kongr. } \mathcal{A}, \sim \neq \Delta_A\}}_{C} = \Delta_A$, takže podle předch. tvrzení $(\nu_\sim)_{\sim\in C}$ je injektivní homomorfismus $\mathcal{A}$ do $\prod_{\sim\in C} \mathcal{A}/\sim$, přičemž $\pi_\sim \circ (\nu_\sim)_{\sim\in C}$ jsou surjektivní, ale nejsou injektivní, neboť $\ker(\pi_\sim \circ (\nu_\sim)_{\sim\in C}) = \ker(\nu_\sim) = \sim \neq \Delta_A$.

„$\Leftarrow$" Triv. algebra $\mathcal{A}$ je nerozložitelná, protože všechny surj. homomorfismy z $\mathcal{A}$ jsou izomorfismy.

Nechť $\sim$ je nejmenší kongruence $\mathcal{A}$ různá od Δ_A a nechť $\varphi : \mathcal{A} \longrightarrow \prod_{i\in I} \mathcal{A}_i$ je injektivní homomorfismus t.ž. $\forall j \in I : \pi_j \circ \varphi$ je surjektivní a není injektivní. Potom $\ker(\pi_j \circ \varphi) \supseteq \sim$. Proto $\ker \varphi = \bigcap_{j\in I} \ker(\pi_j \circ \varphi) \supseteq \sim$, spor s injektivitou φ.

Pomocí axiomu výběru lze dokázat, že každá algebra $\mathcal{A}$ je izomorfní podpřímému součinu podpřímo nerozložitelných algeber, které jsou homomorfními obrazy $\mathcal{A}$.

Příklady: Jediný (až na izom.) netriv. podpřímo nerozložitelný distr. svaz je $\mathcal{L} = \mathbf{2} = (\{0,1\}, OR, AND)$.

Přitom $\mathcal{L}^I \cong (\mathcal{P}(I), \cup, \cap)$, takže tvrzení vlastně říká, že každý distr. svaz je izomorfní podsvazu ~~[illegible]~~ svazu $(\mathcal{P}(I), \cup, \cap)$ pro nějakou množinu I.

Totéž platí pro Bool. algebry.

Až na izomorfismus jediný (netriviální) podpřímo nerozložitelný vektorový prostor nad K je K. (právě 0- a 1-rozměrné)

Podpřímo nerozložitelné konečně generované komutativní grupy jsou právě (až na izom.) $\mathbb{Z}_{p^n}$, kde p je prvočíslo a $n \in \mathbb{N}_0$.

VARIETY A ROVNOSTNÍ LOGIKA

Def.: Identita typu τ je dvojice termů $(t,t') \in T_\tau(X) \times T_\tau(X)$ pro nějakou množinu proměnných X. Identita (t,t') je splněná v τ-algebře $\mathcal{A}$, jestliže pro všechna zobrazení $\varphi: X \to A$ platí $\overline{\varphi}(t) = \overline{\varphi}(t')$; pak píšeme $\mathcal{A} \models t = t'$.

Z pohledu logiky je identita (t,t') nad množinou proměnných $X = \{x_1, \dots, x_n\}$ formule pred. logiky 1. řádu $\forall x_1 \dots \forall x_n : t = t'$, přičemž zobrazení φ určuje dosazení za proměnné a homomorfismus $\overline{\varphi}$ do termů dosadí a vyhodnotí je.

Díky korespondenci mezi zobrazeními $X \to A$ a homomorfismy $T_\tau(X) \to \mathcal{A}$ můžeme $\mathcal{A} \models t = t'$ ekvivalentně definovat podmínkou: Pro každý homomorfismus $\varphi: T_\tau(X) \to \mathcal{A}$ platí $\varphi(t) = \varphi(t')$.

Def.: Pro lib. množinu identit $T \subseteq T_\tau(X) \times T_\tau(X)$ píšeme $\mathcal{A} \models T$, pokud $\forall (t,t') \in T: \mathcal{A} \models t = t'$, a definujeme třídu τ-algeber $\mathrm{Mod}(T) = \{\mathcal{A}\ \tau\text{-algebra} \mid \mathcal{A} \models T\}$.

Skoro všechny třídy algeber, které jsme dříve potkali, jsou tvaru $\mathrm{Mod}(T)$ pro nějakou množinu identit T, např. třída všech grup je
$\mathrm{Mod}(\{(x\cdot(y\cdot z), (x\cdot y)\cdot z), (x\cdot 1, x), (1\cdot x, x), (x\cdot x^{-1}, 1), (x^{-1}\cdot x, 1)\})$. (výjimky: tělesa, obory integrity)

Příklad: Každá grupa splňuje identitu $((x\cdot y)^{-1}, y^{-1}\cdot x^{-1})$.

Budeme se zabývat otázkou, jak zjistit důsledky daných identit.

Máme-li 2 množiny proměnných $Y \subseteq X$, tak $T_\tau(Y)$ je podalgebra $T_\tau(X)$ a homomorfismy $T_\tau(X) \to \mathcal{A}$ jsou právě rozšíření homomorfismů $T_\tau(Y) \to \mathcal{A}$ (protože každé zobrazení $Y \to A$ můžeme rozšířit na zobrazení $X \to A$).

Takže nezáleží na tom, jestli identitu $(t,t') \in T_\tau(Y) \times T_\tau(Y)$ uvažujeme nad množinou Y nebo X.

Protože každá identita nad X používá jen konečně mnoho proměnných, je ekvivalentní identitě nad nějakou konečnou množinou proměnných $Y \subseteq X$. Z toho plyne, že zvolíme-li X nekonečnou spočetnou, bude pro libovolnou identitu nad libovolnou množinou proměnných existovat v $T_\tau(X) \times T_\tau(X)$ identita s ní ekvivalentní.

Pro třídu τ-algeber $\mathcal{V}$ a množinu proměnných X značíme
$\mathrm{Id}_X(\mathcal{V}) = \{(t,t') \in T_\tau(X) \times T_\tau(X) \mid \forall \mathcal{A} \in \mathcal{V} : \mathcal{A} \models t = t'\}$.

Relace $\models$ určuje Galoisovu korespondenci: (ignorujeme, že pracujeme s vlastními třídami)
třídy τ-algeber $\underset{\mathrm{Mod}}{\overset{\mathrm{Id}_X}{\rightleftarrows}}$ množiny identit typu τ nad X, tj. $\mathcal{P}(T_\tau(X) \times T_\tau(X))$.

Cíle: Pro nekonečnou množinu X popsat uzavřené třídy algeber $\mathrm{Mod}(T)$, kde $T \subseteq T_\tau(X) \times T_\tau(X)$, tj. třídy popsatelné pomocí identit (Birkhoffova HSP věta); popsat příslušný uzávěrový operátor $\mathrm{Mod}\,\mathrm{Id}_X$. (víme, že pro všechny nekonečné množiny X dostaneme totéž)

Popsat uzavřené množiny identit a příslušný uzávěrový operátor $\mathrm{Id}_X \mathrm{Mod}$, tj. odvozovací systém pro dokazování identit.

Definice: $\mathcal{V}$ třída τ-algeber. Pak $H(\mathcal{V})$ značí třídu obsahující právě homomorfní obrazy algeber z $\mathcal{V}$, $S(\mathcal{V})$ třídu všech algeber izomorfních nějaké podalgebře algebry z $\mathcal{V}$ (ekvivalentně, $S(\mathcal{V})$ obsahuje právě vzory algeber z $\mathcal{V}$ v injektivních homomorfismech) a $P(\mathcal{V})$ třídu všech algeber izomorfních součinu nějakých algeber z $\mathcal{V}$.

Pozorování: $\mathbf{P}(\mathcal{V})$ vždy obsahuje jednoprvkové algebry: $\prod_{\emptyset} = \{\emptyset\}$.

H, S, P jsou uzávěrové operátory na třídě všech τ-algeber:

– extenzivita a monotonie jasné

$HH(\mathcal{V}) = H(\mathcal{V})$ a $SS(\mathcal{V}) = S(\mathcal{V})$, protože složení surj. homom. je surj. homom. (a složení inj. je inj.)

$PP(\mathcal{V}) = P(\mathcal{V})$, protože součin součinů je izomorfní součinu původních algeber:

$$\prod_{i\in I} \prod_{j\in J_i} \mathcal{A}_{i,j} \cong \prod_{(i,j)\in \bigcup_{i\in I}(\{i\}\times J_i)} \mathcal{A}_{i,j}$$

Tvrzení: $\mathcal{V}$ třída τ-algeber. Pak $SH(\mathcal{V}) \subseteq HS(\mathcal{V})$, $PS(\mathcal{V}) \subseteq SP(\mathcal{V})$ a $PH(\mathcal{V}) \subseteq HP(\mathcal{V})$.

Důkaz: 1) $\underset{\mathcal{A}\in\mathcal{V}}{\varphi}: \mathcal{A} \to \mathcal{B}$ surj. homom., $\mathcal{C}$ podalgebra $\mathcal{B}$. Pak $\varphi^{-1}(\mathcal{C})$ je podalgebra $\mathcal{A}$ a

$\varphi|_{\varphi^{-1}(\mathcal{C})}: \varphi^{-1}(\mathcal{C}) \to \mathcal{C}$ je surj. homom.

2) $\mathcal{B}_i$ podalgebra $\mathcal{A}_i^{\in\mathcal{V}}$ pro $i \in I$. Pak $\prod_{i\in I} \mathcal{B}_i$ je podalgebra $\prod_{i\in I} \mathcal{A}_i$.

3) $\mathcal{A}_i \in \mathcal{V}$ pro $i \in I$, $\varphi_i: \mathcal{A}_i \to \mathcal{B}_i$ surj. homom. Def. homomorfismus

$\varphi: \prod_{i\in I} \mathcal{A}_i \xrightarrow{\prod_{i\in I}\varphi_i} \prod_{i\in I} \mathcal{B}_i$ předpisem $\varphi((a_i)_{i\in I}) = (\varphi_i(a_i))_{i\in I}$. Podle AC je φ surjektiv,

Protipříklady na opačné inkluze

takže $\prod_{i\in I} \mathcal{B}_i \in HP(\mathcal{V})$.

Definice: Třída τ-algeber uzavřená současně na operátory H, S a P se nazývá <u>varieta</u> τ-algeber.

Věta: Pro lib. třídu τ-algeber $\mathcal{V}$ je $HSP(\mathcal{V})$ nejmenší varieta obsahující $\mathcal{V}$; nazýváme ji varieta <u>generovaná</u> $\mathcal{V}$ a značíme $\langle \mathcal{V} \rangle_{var}$.

Důkaz: 1) $HSP(\mathcal{V})$ je varieta: na H je uzavřená triviálně

$S(HSP(\mathcal{V})) \subseteq HSSP(\mathcal{V}) = HSP(\mathcal{V})$

$P(HSP(\mathcal{V})) \subseteq HPSP(\mathcal{V}) \subseteq HSPP(\mathcal{V}) = HSP(\mathcal{V})$

2) $\mathcal{W}$ varieta, $\mathcal{V} \subseteq \mathcal{W} \Rightarrow HSP(\mathcal{V}) \subseteq HSP(\mathcal{W}) = \mathcal{W}$.

Tvrzení: Každá varieta je generovaná svými podpřímo nerozložitelnými algebrami.

Důkaz: $\mathcal{V}$ varieta, $\mathcal{W}$ třída všech podpřímo nerozložitelných algeber ve $\mathcal{V}$.

Každá algebra $\mathcal{A} \in \mathcal{V}$ je ~~podpřímým součinem~~ jejím podpřímým součinem podpřímo nerozložitelných algeber z $H(\{\mathcal{A}\}) \subseteq \mathcal{V}$, takže patří do $SP(\mathcal{W})$. Tedy $\mathcal{V} = SP(\mathcal{W})$.

Příklad: Varieta distributivních svazů je generovaná svazem $\mathbf{2}$.

Totéž platí pro Bool. algebry.

Tvrzení: $\mathcal{A}_i$ pro $i \in I$ τ-algebry, $\mathcal{A}$ jejich libovolný podpřímý součin.

Pak $\langle \{\mathcal{A}_i \mid i \in I\} \rangle_{var} = \langle \{\mathcal{A}\} \rangle_{var}$.

Důkaz: $\subseteq$: $\forall i \in I: \mathcal{A}_i \in H(\{\mathcal{A}\})$ $\qquad$ $\supseteq$: $\mathcal{A} \in SP(\{\mathcal{A}_i \mid i \in I\})$

Důsledek: Varieta generovaná konečně mnoha konečnými algebrami je generovaná jedinou konečnou algebrou.

Tvrzení: Pro každou množinu identit $T \subseteq \mathcal{T}_\tau(X) \times \mathcal{T}_\tau(X)$ je třída $\mathrm{Mod}(T)$ varieta.

Důkaz: $(t, t') \in T$

uzavřenost na H: $\mathcal{A} \models t = t'$, $\psi: \mathcal{A} \to \mathcal{B}$ surj. homom., $\varphi: X \to B$ lib. zobrazení.

Díky surjektivitě ψ existuje zobrazení $\varrho: X \to A$ t.ž. $\psi \circ \varrho = \varphi$

(volíme lib. $\varrho(x) \in \psi^{-1}(\varphi(x))$, přičemž axiomu výběru se dá vyhnout uvažováním jen proměnných použitých v t a t').

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[d, "\varphi"'] \arrow[drr, "\varrho" near start] & \mathcal{T}_\tau(X) \arrow[dl, "\overline{\varphi}"' near start] \arrow[dr, "\overline{\varrho}"] & \\
\mathcal{B} & & \mathcal{A} \arrow[ll, two heads, "\psi"]
\end{tikzcd}$$

Pak $\overline{\varrho}(t) = \overline{\varrho}(t')$. Proto $\overline{\varphi}(t) = \overline{\psi \circ \varrho}(t) = (\psi \circ \overline{\varrho})(t) = \psi \circ \overline{\varrho}(t') = \overline{\psi \circ \varrho}(t') = \overline{\varphi}(t')$, tedy $\mathcal{B} \models t = t'$.

uzavřenost na S: $\mathcal{A} \models t = t'$, $\psi: \mathcal{B} \rightarrowtail \mathcal{A}$ injektivní homom., $\varphi: \mathcal{T}_\tau(X) \to \mathcal{B}$ homom.

Potom $(\psi \circ \varphi)(t) = (\psi \circ \varphi)(t')$, takže $\varphi(t) = \varphi(t')$ z injektivity ψ.

(vyhodnocení termu v podalgebře dopadne stejně jako v celé algebře)

uzavřenost na P: $\forall i: \mathcal{A}_i \models t = t'$, $\varphi: \mathcal{T}_\tau(X) \to \prod_{i\in I} \mathcal{A}_i$ lib. homomorfismus.

Pak $\forall i \in I$ platí $\pi_i(\varphi(t)) = (\pi_i \circ \varphi)(t) = (\pi_i \circ \varphi)(t') = \pi_i(\varphi(t'))$, takže $\varphi(t) = \varphi(t')$.

Def.: $\mathcal{V}$ třída τ-algeber, X lib. množina. Algebra $F_{\mathcal{V}}(X) \in \mathcal{V}$ se nazývá <u>volná</u> ve $\mathcal{V}$ nad X vzhledem k zobrazení $\lambda : X \to F_{\mathcal{V}}(X)$, jestliže pro každou algebru $\mathcal{A} \in \mathcal{V}$ a každé zobrazení $\varphi : X \to A$ existuje jediný homomorfismus $\hat{\varphi} : F_{\mathcal{V}}(X) \to \mathcal{A}$ t.ž. $\hat{\varphi} \circ \lambda = \varphi$.

$$\begin{tikzcd} X \arrow[r, "\lambda"] \arrow[dr, "\text{zobr. } \varphi"'] & F_{\mathcal{V}}(X) \arrow[d, "\hat{\varphi} \text{ jediný homom.}"] \\ & \mathcal{A} \end{tikzcd}$$

(Znamená to, že existuje vzájemně jednoznačná korespondence mezi zobrazeními $X \to A$ a homomorfismy $F_{\mathcal{V}}(X) \to \mathcal{A}$ daná přiřazeními $\varphi \mapsto \hat{\varphi}$, $\psi \circ \lambda \mapsfrom \psi$.)

Příklady: 1) $T_\tau(X)$ je volná nad X ve třídě všech τ-algeber vzhledem k $X \hookrightarrow T_\tau(X)$.

2) $(X^*, \cdot)$ je volný monoid nad X vzhledem k $X \hookrightarrow X^*$. Toto se používá pro konečné deterministické automaty: Přechodová fce δ je lib. zobrazení X do Q^Q, tj. $\delta(x)(q) \in Q$. Rozšířená přechodová fce $\hat{\delta}$ je příslušný homomorfismus $(X^*, \cdot)$ do $(Q^Q, \circ)$, tj. musí splňovat $\hat{\delta}(\varepsilon)(q) = q$ $(\hat{\delta}(\varepsilon) = id_Q)$ a $\hat{\delta}(uv)(q) = \hat{\delta}(v)(\hat{\delta}(u)(q))$ $(\hat{\delta}(uv) = \hat{\delta}(v) \circ \hat{\delta}(u))$. Takže automaty můžeme ekvivalentně definovat pomocí rozšířených přechodových fcí, jen na ně musíme klást příslušné podmínky, aby to byl homomorfismus.

Pozn.: Pokud $\mathcal{V}$ obsahuje nějakou netriviální algebru, tak je λ injektivní.

Intuice: Jednoznačnost $\hat{\varphi}$ říká, že v $F_{\mathcal{V}}(X)$ nejsou nadbytečné prvky, jejichž chování v homomorfismu není určeno chováním prvků $\lambda(x)$, tj. $F_{\mathcal{V}}(X)$ je generovaná $\lambda(X)$. Existence $\hat{\varphi}$ říká, že v $F_{\mathcal{V}}(X)$ jsou ztotožněny pouze ty termy, které jsou ztotožněny ve všech algebrách třídy $\mathcal{V}$.

Tvrzení: Volná algebra ve $\mathcal{V}$ nad X, pokud existuje, je určena jednoznačně až na izomorfismus.

Důkaz:

$$\begin{tikzcd} X \arrow[r, "\lambda"] \arrow[dr, "\lambda'"'] & F_{\mathcal{V}}(X) \arrow[d, shift right, "\hat{\lambda}"'] \\ & F'_{\mathcal{V}}(X) \arrow[u, shift right, "\hat{\lambda}'"'] \end{tikzcd}$$

Platí $\hat{\lambda}' \circ \widehat{\lambda'} \circ \lambda = \hat{\lambda}' \circ \lambda' = \lambda$. Takže $\hat{\lambda}' \circ \widehat{\lambda'} = \hat{\lambda} = id_{F_{\mathcal{V}}(X)}$.
analog. $\hat{\lambda}' \circ \hat{\lambda} = id_{F'_{\mathcal{V}}(X)}$

$$\begin{tikzcd} X \arrow[r, "\lambda"] \arrow[dr, "\lambda"'] & F_{\mathcal{V}}(X) \arrow[d, "id = \hat{\lambda}"] \\ & F_{\mathcal{V}}(X) \end{tikzcd}$$

Tvrzení: $\mathcal{V}$ třída τ-algeber uzavřená na S, X lib. množina proměnných.
Pak $Id_X(\mathcal{V}) = \bigcap \{ \sim \subseteq T_\tau(X) \times T_\tau(X) \mid \sim \text{ je kongruence } T_\tau(X),\ T_\tau(X)/\!\sim\ \in \mathcal{V} \}$.

Důkaz: "$\subseteq$" $(t, t') \in Id_X(\mathcal{V})$, $\sim$ kongruence $T_\tau(X)$, $T_\tau(X)/\!\sim\ \in \mathcal{V}$. Chceme dokázat $(t, t') \in \sim$.
$\nu_\sim : T_\tau(X) \to T_\tau(X)/\!\sim$ homomorfismus a $T_\tau(X)/\!\sim\ \models t = t'$, takže $\nu_\sim(t) = \nu_\sim(t')$, tj. $t \sim t'$.

"$\supseteq$" Předp., že $t \sim t'$ platí pro všechny kongruence $\sim$ algebry $T_\tau(X)$ t.ž. $T_\tau(X)/\!\sim\ \in \mathcal{V}$.
Buď $\varphi : T_\tau(X) \to \mathcal{A}$ lib. homomorfismus do nějaké algebry $\mathcal{A} \in \mathcal{V}$.
Pak $\varphi = \psi \circ \nu_{\ker\varphi}$ pro nějaký injektivní homomorfismus $\psi : T_\tau(X)/\ker\varphi \to \mathcal{A}$.
Protože $\mathcal{V}$ je uzavřená na S, tak $T_\tau(X)/\ker\varphi \in \mathcal{V}$. Podle předpokladu $(t, t') \in \ker\varphi$, takže $\varphi(t) = \varphi(t')$. Dokázali jsme $\mathcal{A} \models t = t'$.

Definice: Kongruence $\sim$ algebry $\mathcal{A}$ se nazývá <u>plně invariantní</u>, jestliže pro každý homomorfismus $\psi : \mathcal{A} \to \mathcal{A}$ a $\forall a, a' \in A$ splňující $a \sim a'$ platí $\psi(a) \sim \psi(a')$.

Příklad: Pro $\mathcal{A} = T_\tau(X)$ homomorfismy $\psi : T_\tau(X) \to T_\tau(X)$ jednoznačně odpovídají dosazování termů za proměnné, t.zn., že kongruence $\sim$ na $T_\tau(X)$ je plně invariantní $\Longleftrightarrow$ dosazením libovolných termů za proměnné dostaneme z $\sim$-ekvivalentních termů opět $\sim$-ekvivalentní termy. (tenhle případ nás bude zajímat)

Věta: Pro libovolnou varietu τ-algeber $\mathcal{V}$ a libovolnou množinu X je $Id_X(\mathcal{V})$ plně invariantní kongruencí algebry $T_\tau(X)$ a algebra $T_\tau(X)/_{Id_X(\mathcal{V})}$ je volná ve $\mathcal{V}$ nad X vzhledem k zobrazení

$$\lambda = \nu_{Id_X(\mathcal{V})} \circ \iota : X \hookrightarrow T_\tau(X) \longrightarrow T_\tau(X)/_{Id_X(\mathcal{V})}.$$

Důkaz: Podle předch. tvrzení je $Id_X(\mathcal{V})$ kongruence $T_\tau(X)$.

Buď $\psi: T_\tau(X) \longrightarrow T_\tau(X)$ homomorfismus, $(t,t') \in Id_X(\mathcal{V})$. Ukážeme $(\psi(t), \psi(t')) \in Id_X(\mathcal{V})$.

Nechť $\varphi: T_\tau(X) \longrightarrow \mathcal{A}$ je lib. homomorfismus, kde $\mathcal{A} \in \mathcal{V}$.

Pak $\varphi(\psi(t)) = (\varphi\circ\psi)(t) = (\varphi\circ\psi)(t') = \varphi(\psi(t'))$, protože $\mathcal{A} \models t = t'$ a $\varphi\circ\psi$ je homom.

Takže $Id_X(\mathcal{V})$ je plně invariantní kongruence.

Z předch. tvrzení $Id_X(\mathcal{V}) = \bigcap\{\ker \nu_\sim \mid \sim$ kongruence $T_\tau(X)$, $T_\tau(X)/_\sim \in \mathcal{V}\} = \ker((\nu_\sim)_{\sim\in I})$, kde $I = \{\sim\, \subseteq T_\tau(X)\times T_\tau(X) \mid \sim$ kongr. $T_\tau(X)$, $T_\tau(X)/_\sim \in \mathcal{V}\}$. Proto $(\nu_\sim)_{\sim\in I} = \kappa\circ\nu_{Id_X(\mathcal{V})}$ pro nějaký injektivní homomorfismus κ.

$$\begin{tikzcd}
X \arrow[r, hook, "\iota"] \arrow[rr, bend left, "\lambda"] \arrow[dr, "\varphi"'] & T_\tau(X) \arrow[r, "\nu_{Id_X(\mathcal{V})}"] \arrow[rr, bend left, "(\nu_\sim)_{\sim\in I}"] \arrow[d, "\overline{\varphi}"] \arrow[drr, "\nu_{\ker\overline{\varphi}}"] & T_\tau(X)/_{Id_X(\mathcal{V})} \arrow[r, "\kappa"] \arrow[dl, "\hat{\varphi}"] & \prod\limits_{\sim\in I} T_\tau(X)/_\sim \arrow[d, "\pi_{\ker\overline{\varphi}}"] \\
& \mathcal{A} & & T_\tau(X)/_{\ker\overline{\varphi}} \arrow[ll, "\psi"]
\end{tikzcd}$$

Mimo jiné platí $T_\tau(X)/_{Id_X(\mathcal{V})} \in \mathcal{V}$, protože je izomorfní podalgebře součinu algeber $T_\tau(X)/_\sim$.

Buď $\varphi: X \to A$ lib. zobrazení do nějaké algebry $\mathcal{A} \in \mathcal{V}$.

Protože $T_\tau(X)/_{\ker\overline{\varphi}}$ je izomorfní podalgebře algebry $\mathcal{A}$, tak $T_\tau(X)/_{\ker\overline{\varphi}} \in \mathcal{V}$, tj. $\ker\overline{\varphi} \in I$; označme ψ příslušný injektivní homomorfismus $T_\tau(X)/_{\ker\overline{\varphi}} \to \mathcal{A}$ splňující $\psi\circ\nu_{\ker\overline{\varphi}} = \overline{\varphi}$. Ukážeme, že hledaným homomorfismem

$\hat{\varphi}: T_\tau(X)/_{Id_X(\mathcal{V})} \to \mathcal{A}$ je $\psi\circ\pi_{\ker\overline{\varphi}}\circ\kappa$. Platí $(\psi\circ\pi_{\ker\overline{\varphi}}\circ\kappa)\circ\nu_{Id_X(\mathcal{V})} =$

$= \psi\circ\pi_{\ker\overline{\varphi}}\circ(\nu_\sim)_{\sim\in I} = \psi\circ\nu_{\ker\overline{\varphi}} = \overline{\varphi}$. Proto $(\psi\circ\pi_{\ker\overline{\varphi}}\circ\kappa)\circ\lambda = \overline{\varphi}\circ\iota = \varphi$.

Zbývá ukázat jednoznačnost homomorfismu $\hat{\varphi}$:

Protože $\hat{\varphi}$ splňuje $\hat{\varphi}\circ\lambda = \varphi$, tak $(\hat{\varphi}\circ\nu_{Id_X(\mathcal{V})})\circ\iota = \varphi$, z čehož plyne $\hat{\varphi}\circ\nu_{Id_X(\mathcal{V})} = \overline{\varphi} = (\psi\circ\pi_{\ker\overline{\varphi}}\circ\kappa)\circ\nu_{Id_X(\mathcal{V})}$. Ze surjektivity $\nu_{Id_X(\mathcal{V})}$ dostáváme $\hat{\varphi} = \psi\circ\pi_{\ker\overline{\varphi}}\circ\kappa$.

Existenci volných algeber $X \xrightarrow{\lambda} F_{\mathcal{V}}(X)$ ve varietě $\mathcal{V}$ lze použít k popisu algeber pomocí tzv. <u>prezentací</u>. Prezentace algebry sestává z konečné množiny generátorů X a konečné podmnožiny $M \subseteq T_\tau(X)\times T_\tau(X)$. Tato prezentace zadává algebru $F_{\mathcal{V}}(X)/_{\langle\{(\overline{\lambda}(t),\overline{\lambda}(t')) \mid (t,t')\in M\}\rangle_{cong}} =: \langle X \mid M\rangle_{\mathcal{V}}$.

Příklady: $\langle x,y \mid x\cdot y = y\cdot x,\ x\cdot x = 1\rangle_{grp} \cong \mathbb{Z}_2\times\mathbb{Z}$, $\langle x,y \mid x\cdot y = y^{-1}\cdot x,\ x\cdot x = 1,\ y^n = 1\rangle_{grp} \cong D_n$.

Existují ovšem prezentace (například pologrup a grup) takové, že v jimi popsané algebře není možné algoritmicky počítat.

Birkhoffova HSP věta: X nekonečná množina proměnných, $\mathcal{V}$ třída τ-algeber.

Pak existuje $T \subseteq T_\tau(X)\times T_\tau(X)$ t.ž. $\mathcal{V} = Mod(T) \iff \mathcal{V}$ je varieta.

Důkaz: "$\Rightarrow$" bylo dokázáno.

"$\Leftarrow$" Buď $\mathcal{V}$ varieta. Ukážeme, že $\mathcal{V} = Mod(Id_X(\mathcal{V}))$. "$\subseteq$" zř.

"$\supseteq$" Nechť $\mathcal{A} \in Mod(Id_X(\mathcal{V}))$. Protože X je nekonečná, je každá identita nad libovolnou množinou ekvivalentní nějaké identitě nad X, takže $\mathcal{A} \in Mod(Id_A(\mathcal{V}))$. Protože $eval_{\mathcal{A}}: T_\tau(A) \to \mathcal{A}$ je homomorfismus a $\mathcal{A} \models Id_A(\mathcal{V})$, tak $\forall (t,t') \in Id_A(\mathcal{V})$: $eval_{\mathcal{A}}(t) = eval_{\mathcal{A}}(t')$. Tedy $Id_A(\mathcal{V}) \subseteq \ker(eval_{\mathcal{A}})$. Z toho plyne, že existuje homomorfismus $\psi: T_\tau(A)/_{Id_A(\mathcal{V})} \to \mathcal{A}$ t.ž. $\psi\circ\nu_{Id_A(\mathcal{V})} = eval_{\mathcal{A}}$. Přitom ψ je surjektivní, neboť $eval_{\mathcal{A}}$ je surjektivní. Protože $T_\tau(A)/_{Id_A(\mathcal{V})} \in \mathcal{V}$, tak $\mathcal{A} \in H(\mathcal{V}) = \mathcal{V}$.

Věta o úplnosti rovnostní logiky:
Podmnožiny $T_\tau(X)\times T_\tau(X)$ tvaru $Id_X(V)$ pro nějakou třídu τ-algeber V jsou právě plně invariantní kongruence algebry $T_\tau(X)$.

Důkaz: Víme, že $Id_X(V)$ je plně invariantní kongruence.
Opačně, buď T plně invariantní kongruence $T_\tau(X)$. Ukážeme, že $Id_X(Mod(T))=T$, ~~přičemž~~ inkluze "$\supseteq$" je zřejmá.

"$\subseteq$" Nejprve ukážeme, že $T_\tau(X)/_T\in Mod(T)$. (používáme, že T je kongruence).
Buď $\varphi: X\to T_\tau(X)/_T$ lib. zobrazení a $(t,t')\in T$. Chceme ukázat, že $\bar\varphi(t)=\bar\varphi(t')$.
Vezměme libovolné zobrazení $\psi: X\to T_\tau(X)$ t.ž. $\varphi=\nu_T\circ\psi$. (Pro X konečnou nebo spočetnou a konečný nebo spočetný typ jde bez axiomu výběru)

$$\begin{tikzcd} X \arrow[r, hook] \arrow[d, "\varphi"'] \arrow[dr, "\psi"' near start] & T_\tau(X) \arrow[d, "\bar\psi"] \arrow[dl, "\bar\varphi" near start] \\ T_\tau(X)/_T & T_\tau(X) \arrow[l, "\nu_T"] \end{tikzcd}$$

Pak $\nu_T\circ\bar\psi=\overline{\nu_T\circ\psi}=\bar\varphi$. Jelikož T je plně invariantní, tak $(\bar\psi(t),\bar\psi(t'))\in T$. Proto $\bar\varphi(t)=\nu_T(\bar\psi(t))=\nu_T(\bar\psi(t'))=\bar\varphi(t')$.

~~[illegible]~~ Nechť $(t,t')\in Id_X(Mod(T))$. Potom $T_\tau(X)/_T\models t=t'$, a tedy homomorfismus $\nu_T: T_\tau(X)\to T_\tau(X)/_T$ je libovolné splňuje $\nu_T(t)=\nu_T(t')$, tj. $(t,t')\in T$.

Galoisova korespondence $\underset{Mod}{\overset{Id_X}{\rightleftarrows}}$ pro $X=\{x_n \mid n\in\mathbb{N}\}$ spočetnou množinu proměnných nám tedy zadává antiizomorfismus úplného svazu všech variet τ-algeber a úplného svazu všech plně invariantních kongruencí algebry $T_\tau(X)$.

Poznámka: Variety lze zadávat různými způsoby, mezi kterými není možné algoritmicky převádět, např. 1) definovat identitami; 2) popsat algoritmus rozhodující, které identity v dané varietě platí, což je ekvivalentní algoritmickému počítání v algebře $F_V(X)$; 3) zadat generující množinu algeber.

Příklad: Varieta všech distributivních svazů je generovaná svazem $\mathbf{2}$; pomocí identit jsme ji původně definovali; rozhodovat platnost identit lze třeba převodem do DNF (viz cvičení).

Poznámka: Každá varieta je generovaná jednou algebrou, a to $F_V(X)$ $(=T_\tau(X)/Id_X(V))$ pro X nekonečnou, protože tato algebra splňuje právě identity platné v celé varietě.

Vysvětlení věty o úplnosti:
$Id_X(Mod(T))$ ~~jsou~~ je právě množina všech identit, které jsou sémantickým důsledkem T. ~~[illegible]~~ Z věty plyne, že $Id_X(Mod(T))$ je plně invariantní kongruence $T_\tau(X)$ generovaná množinou T. To znamená, že všechny důsledky identit z množiny T lze získat pomocí následujícího odvozovacího systému:

$\vdash t=t$ pro $t\in T_\tau(X)$ (reflexivita)

$t=t'\vdash t'=t$ pro $t,t'\in T_\tau(X)$ (symetrie)

$t=t',\ t'=t''\vdash t=t''$ pro $t,t',t''\in T_\tau(X)$ (tranzitivita)

$t_1=t_1',\dots,t_n=t_n'\vdash f(t_1,\dots,t_n)=f(t_1',\dots,t_n')$ pro $t_1,\dots,t_n,t_1',\dots,t_n'\in T_\tau(X)$, $f\in\tau$ n-ární (kongruence)

$t(x_1,\dots,x_n)=t'(x_1,\dots,x_n)\vdash t(t_1,\dots,t_n)=t'(t_1,\dots,t_n)$ $t,t',t_1,\dots,t_n\in T_\tau(X)$ (plná invariance)

Tak jako celá logika 1. řádu je ovšem rovnostní logika pouze rekurzivně vyčíslitelná, nikoli rekurzivní, například ve varietě všech modulárních svazů není možné algoritmicky rozhodovat platnost identit; existují i ~~[illegible]~~ variety pologrup a grup zadané konečně mnoha identitami, které mají tuto vlastnost.