Předmluva

Skriptum je určeno zejména pro odborné studium matematiky a informatiky ve 3.semestru přírodovědecké fakulty Univerzity Palackého. Pokrývá příslušné partie základního kursu algebry, v mnohém však tuto základní látku přesahuje a dává tak nahlédnout do motivací resp. aplikací pojmů a výsledků základního kursu.

Cílem je ukázat, že teorie svazů, ale zvláště teorie universálních algeber v jistém smyslu "zastřešuje" pojmy a výsledky elementární teorie grup, grupoidů, okruhů a těles, které jsou předmětem prvních dvou semestrů úvodního kursu. Dále se autor snažil podat tyto teorie jako pojmotvorný proces, který vychovává v jistém druhu úsudků a myšlení, jenž je zcela nezbytný pro zvládnutí studia matematiky. Konečně bylo cílem ukázat algebru jako zdaleka neuzavřený tvůrčí proces, pro který je zamýšlené studium inspirací.

Teorie svazů je koncipována v tomto skriptu tak, aby obsahovala jednak základní výsledky této teorie, používané v jiných partiích matematiky, jednak pojmy a výsledky nutné pro výklad universální algebry. Ve vztahu k uceleným teoriím (přednášených v prvních dvou semestrech) obsahuje výklad vztahu kongruencí a ideálů na svazech. Logickým vyústěním první části, a současně přechodem k druhé, je kapitola o Booleových algebrách.

Teorie universálních algeber v rozsahu tohoto skripta má za cíl nejen výklad základních pojmů, zobecňujících výsledky známé pro grupy, grupoidy, okruhy či svazy, ale také demonstraci vnitřních zdrojů universální algebry, uplatněných zejména v teorii variet, umožňující samostatný (a mnohdy překotný) rozvoj této disciplíny, a zpětné aplikace k účelu explanace speciálních teorií jednotlivých typů algebraických struktur.

Vybrané kapitoly universální algebry obsahují jednak rozšíření 2.části (kap.13), umožňující hlubší pochopení teorie variet, jednak úvod do primálních algeber (sloužící i ke studiu vícehodnotových logik), a také některé výsledky o akceptorech a Pawlakových strojích, tvořící algebraický základ teoretického studia informatiky.

TEORIE SVAZŮ

1 USPOŘÁDANÉ MNOŽINY

1.1 Uspořádání a kvaziuspořádání

Nechť A je neprázdná množina. *Relací na* A rozumíme každou podmnožinu kartézského součinu $A \times A$.
Relace R na A je
reflexivní, jestliže $\forall x \in A$ platí: $\langle x, x \rangle \in R$
symetrická, jestliže $\forall x, y \in A$ platí: $\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R$
tranzitivní, jestliže $\forall x, y, z \in A$ platí: $\langle x, y \rangle \in R \ \wedge \langle y, z \rangle \in R \Rightarrow$
$\langle x, z \rangle \in R$
antisymetrická, jestliže $\forall x, y \in A$ platí: $\langle x, y \rangle \in A \ \wedge \langle y, x \rangle \in A \Rightarrow \ x = y$.

Relaci na množině A, která je reflexivní a tranzitivní, nazveme *kvaziuspořádání.* Relaci, která je reflexivní, tranzitivní a antisymetrická, nazveme *uspořádání*. Relaci, která je reflexivní, symetrická a tranzitivní, nazveme *ekvivalence.*

Tedy uspořádání je antisymetrické kvaziuspořádání, ekvivalence je symetrické kvaziuspořádání.

Je-li E ekvivalence na množině A, označme symbolem A/E tzv. *faktorovou množinu* A *dle* E, tj. množinu všech tříd rozkladu množiny A, indukovaného ekvivalencí E.

Je-li R uspořádání na A, pak pro zápis této relace zpravidla používáme symbol $\leq$ a místo $\langle x, y \rangle \in R$ zapisujeme $x \leq y$ nebo také $y \geq x$. Je-li $x \leq y$, $x \neq y$, zapisujeme $x < y$ nebo $y > x$. Je-li $\leq$ uspořádání na A, a jestliže pro dva prvky $x, y \in A$ neplatí ani $x \leq y$ ani $y \leq x$, zapisujeme $x \parallel y$.

Příklady:

(1) Relace "$\leq$" na množině všech čísel celých (resp. racionálních, resp. reálných) je uspořádání.

(2) Relace dělitelnosti na množině všech čísel přirozených je uspořádání.

(3) Relace inkluze $\subseteq$ na množině *Exp* M všech podmnožin neprázdné množiny M je uspořádání.

(4) Relace dělitelnosti na množině všech čísel celých je kvaziuspořádání, které není uspořádáním, neboť např. 3 dělí -3, dále -3 dělí 3, ale $-3 \neq 3$.

(5) Nechť F je množina všech reálných funkcí jedné reálné proměnné na intervalu (a, b). Položme $f \leq g$ pro $f, g \in F$, právě když $\forall x \in (a, b)$ platí $f(x) \leq g(x)$ (pro čísla $f(x), g(x) \in R$). Pak takto zavedená relace je uspořádání na F.

Je-li $\leq$ uspořádání na množině A, dvojici $(A, \leq)$ nazveme *uspořádaná množina.* Jestliže $\leq$ je uspořádání na A takové, že $\forall x, y \in A$ platí buď $x \leq y$ nebo $y \leq x$, pak se $\leq$ nazývá *úplné uspořádání* a A se nazývá *úplně uspořádaná množina* neboli *řetězec.* Je-li $\leq$ uspořádání na A takové, že $\forall x, y \in A$ platí $x \parallel y$, pak se $(A, \leq)$ nazývá *antiřetězec.*

Množiny z příkladu (1), t.j. $(\boldsymbol{Z}, \leq), (\boldsymbol{Q}, \leq), (\boldsymbol{R}, \leq)$ jsou řetězce, uspoř. množiny z příkladů (2),(3),(5) nejsou řetězce (v příkladu (3) je $(M, \subseteq)$ řetězec, právě když M je jednoprvková).

Věta 1.1. *Nechť Q je kvaziuspořádání na množině $A \neq \emptyset$. Pak $E = Q \cap Q^{-1}$ je ekvivalence na A a faktorová množina A/E je uspořádaná vzhledem k relaci $\leq_Q$, definované takto: $B, C \in A/E$,*

$B \leq_Q C$ tehdy a jen tehdy, když $\forall b \in B$, $\forall c \in C$, $\langle b, c \rangle \in Q$.

Důkaz: Jelikož Q je reflexivní, je i Q^{-1} reflexivní, t.j. také $E = Q \cap Q^{-1}$ je reflexivní. Nechť $\langle x, y \rangle \in E$, pak $\langle x, y \rangle \in Q \ \wedge \langle x, y \rangle \in Q^{-1} \Rightarrow$ $\langle y, x \rangle \in (Q^{-1})^{-1} = Q$, $\langle y, x \rangle \in Q^{-1}$, tedy $\langle y, x \rangle \in E = Q \cap Q^{-1}$, t.j. E je symetrická. Jestliže $\langle x, y \rangle \in E \wedge \langle y, z \rangle \in E$, pak $\langle x, y \rangle \in Q \wedge \langle y, z \rangle \in Q$, tedy $\langle x, z \rangle \in Q$, $\langle x, y \rangle \in Q^{-1} \wedge \langle y, z \rangle \in Q^{-1} \Rightarrow \langle x, z \rangle \in Q^{-1}$, t.j. $\langle x, z \rangle \in E$, tedy E je tranzitivní, t.j. E je ekvivalence.

Uvažujme nyní faktorovou množinu A/E s relací $\leq_Q$ definovanou výše uvedeným předpisem. Nechť $B \in A/E$. Pak $\forall b_1, b_2 \in B$ platí $\langle b_1, b_2 \rangle \in Q$, odtud $B \leq_Q B$, tedy $\leq_Q$ je reflexivní. Nechť $B, C \in A/E$ a platí $B \leq_Q C$, $C \leq_Q B$. Pak $\forall b \in B$, $\forall c \in C$ platí $\langle b, c \rangle \in Q$, $\langle c, b \rangle \in Q$, tedy b, c padnou do téže třídy rozkladu. To je však možné jen pro $B = C$, neboť různé třídy jsou vzájemně disjunktní. Tranzitivita $\leq_Q$ plyne přímo z tranzitivity relace Q, tedy $\leq_Q$ je vskutku uspořádání na A. $\square$

Označme symbolem $Exp\,M$ množinu všech podmnožin množiny M. Z příkladu (3) víme, že $(Exp\,M, \subseteq)$ je uspořádaná množina. Dokážeme, že tato uspořádaná množina je v jistém smyslu universální, t.j. každou uspořádanou množinu lze representovat jako podmnožinu takové množiny.

Nechť $(A, \leq)$, $(B, \leq)$ jsou uspořádané množiny. Řekneme, že jsou *o-izomorfní*, jestliže existuje bijekce $f : A \to B$ s vlastnostmi:

$$\forall x, y \in A, \text{ jestliže } x \leq y, \text{ pak } f(x) \leq f(y),$$

$$\forall c, d \in B, \text{ jestliže } c \leq d, \text{ pak } f^{-1}(c) \leq f^{-1}(d).$$

Věta 1.2. *Každá uspořádaná množina $(M, \leq)$ je o-izomorfní některé podmnožině uspořádané množiny $(Exp\,M, \subseteq)$.*

D ů k a z : Nechť $f : M \to Exp\, M$ je zobrazení dané předpisem $f(a) = \{x \in M; x \leq a\}$. Jestliže $a, b \in M$ a $a \leq b$, zřejmě $f(a) = \{x \in M; x \leq a\} \subseteq \{x \in M; x \leq b\} = f(b)$. Obráceně, jestliže $C, D \in f(M)$ a $C \subseteq D$, pak $\exists a, b \in M$ tak, že $C = \{x \in M; x \leq a\}$, $D = \{x \in M; x \leq b\}$, a z $C \subseteq D$ plyne $a \leq b$; ale $a = f^{-1}(C), b = f^{-1}(D)$, tedy $C \subseteq D \Rightarrow f^{-1}(C) \leq f^{-1}(D)$.

Je-li $C = D$, pak pro $a, b \in M$ splňující $f(a) = C$, $f(b) = D$ zřejmě platí $a = b$, tudíž f je injekce. Takže f je bijekce M na $f(M)$, t.j. $(M, \leq)$ a $(f(M), \subseteq)$ jsou o-izomorfní, přičemž $f(M) \subseteq Exp\, M$. □

Věta 1.3. Princip duality. *Nechť $\leq$ je uspořádání na množině A. Pak inversní relace, t.j $\leq^{-1}$ (označení $\geq$), je opět uspořádání na A.*

D ů k a z : Je ihned zřejmé, že z reflexivity, antisymetrie a tranzitivity relace $\leq$ plyne, že tyto vlastnosti má i relace $\geq$. □

1.2 Diagramy

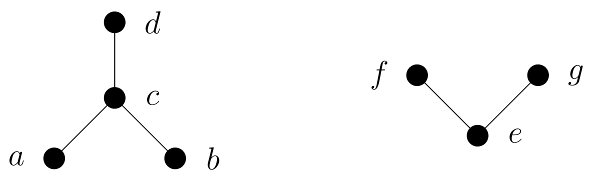
Je-li $(A, \leq)$ konečná uspořádaná množina, pak ji lze snadno znázornit v rovině i s relací uspořádání. Zavedeme následující pojem: Nechť $x, y \in A$, $x < y$. Řekneme, že prvek y *kryje* prvek x, neboli x *je pokrýván* prvkem y, jestliže $\forall z \in A$ splňující $x \leq z \leq y$ platí $x = z$ nebo $z = y$. Zapisujeme $x \prec y$. Relaci $\prec$ nazveme *relace pokrytí*.

Lemma 1.4. *Nechť $(A, \leq)$ je konečná uspořádaná množina, $x, y \in A$. Pak $x < y$ právě když existují prvky $z_0 = x, z_1, \ldots, z_{n-1}, z_n = y$ v A tak, že $z_i \prec z_{i+1}$ $\forall i = 0, 1, \ldots, n-1$.*

D ů k a z : Nechť $x < y$. Pak buď $x \prec y$ (v tom případě položme $n = 1$, $z_0 = x$, $z_1 = y$), nebo existuje $a \in A$ tak, že $x < a < y$. Jestliže $x \prec a \prec y$, pak položme $n = 2$, $x = z_0$, $a = z_1$, $y = z_2$. Jestliže neplatí $x \prec a$ pak existuje $b \in B$ tak, že $x < b < a$. Celou úvahu opakujeme. Protože A je konečná, musíme po konečném počtu kroků již dojít k prvkům, které se pokrývají; stejně pro prvky $a < y$. Tedy po konečném počtu opakování výše uvedeného kroku dostaneme existenci $z_0, z_1, \ldots, z_n$, splňujících tvrzení věty. Obráceně, nechť $x = z_0 \prec z_1 \prec \ldots \prec z_{n-1} \prec z_n = y$. Pak $x < z_1 < z_2 < \ldots < z_{n-1} < y$, tedy také $x \leq z_1 \leq z_2 \leq \ldots \leq z_{n-1} \leq y$. Avšak relace $\leq$ je tranzitivní, tedy $x \leq y$. □

Nyní popíšeme znázornění konečné uspořádané množiny diagramem: Nechť $(A, \leq)$ je konečná. Representujme každý prvek z A bodem v rovině a to tak, že je-li $a, b \in A, a < b$, pak bod b znázorníme nad bodem a (posunutí do strany tuto situaci neovlivní). Je-li $x \prec y$, pak body x, y spojíme úsečkou. Vzniklou konfiguraci nazveme *diagram uspořádané množiny* $(A, \leq)$.

Příklad: Nechť $A = \{a, b, c, d, e, f, g\}$ a relace $\leq$ je na A dána takto: $a < c$, $b < c$, $c < d$, $a < d$, $b < d$, $e < f$, $e < g$. Pak $(A, \leq)$ má diagram:



Obr.1

Speciální případy:

(A) Je-li $(A, \leq)$ řetězec, pak její diagram je znázorněn na Obr.2.

(B) Je-li $(A, \leq)$ antiřetězec, pak její diagram je znázorněn na Obr.3.

(C) Je-li $(A, \leq)$ konečná uspořádaná množina a $\geq$ je inversní uspořádání, pak dle principu duality je $(A, \geq)$ rovněž uspořádaná množina, jejíž diagram je "vzhůru nohama" obrácený diagram množiny $(A, \leq)$.

Obr.2 Obr.3

1.3 Speciální prvky a množiny

Definice: Nechť $(A, \leq)$ je uspořádaná množina. Prvek $a \in A$ se nazývá

minimální, jestliže $x \leq a \Rightarrow \ x = a$;

nejmenší, jestliže $\forall x \in A$ platí $a \leq x$;

maximální, jestliže $a \leq x \Rightarrow \ x = a$;

největší, jestliže $\forall x \in A$ platí $x \leq a$.

Je ihned zřejmé, že má-li $(A, \leq)$ největší prvek, pak je jediný; má-li $(A, \leq)$ nejmenší prvek, pak je jediný. Na obr.1 je uspořádaná množina, která nemá ani nejmenší, ani největší prvek, avšak a, b, e jsou minimální prvky, d, f, g jsou maximální prvky v $(A, \leq)$.

Má-li $(A, \leq)$ největší prvek, pak tento prvek je maximální a jiné maximální prvky v $(A, \leq)$ neexistují; duálně, má-li $(A, \leq)$ nejmenší prvvek, pak je tento prvek minimální a jiné minimální prvky v $(A, \leq)$ neexistují. Každý konečný řetězec má největší a nejmenší prvek. Antiřetězec nemá ani největší, ani nejmenší prvek, ale každý jeho prvek je současně minimální i maximální.

Definice: Nechť $(A, \leq)$ je uspořádaná množina a $M \subseteq A$. Označme symbolem

$U(M) = \{x \in A; y \leq x$ pro každé $y \in M\}$

$L(M) = \{x \in A; x \leq y$ pro každé $y \in M\}$.

Množina $U(M)$ se nazývá *horní kužel* množiny M, množina $L(M)$ se nazývá *dolní kužel* množiny M. Má-li $U(M)$ nejmenší prvek, pak tento prvek se nazývá *supremum* M a značí se $sup\, M$; má-li $L(M)$ největší prvek, pak tento prvek se nazývá *infimum* M a značí se *inf* M. Jestliže $\forall a, b \in A$ je $U(\{a, b\}) \neq \emptyset$, pak $(A, \leq)$ se nazývá (*shora*) *usměrněná množina.*

Jelikož v uspořádané množině může být nejvýše jediný největší (nejmenší) prvek, je zřejmé, že pro každou $M \subseteq A$ buď *sup* A (*inf* A) neexistuje, nebo je jediné. Je-li $M = \{a_1, \ldots, a_n\}$, pak místo $sup\,(\{a_1, \ldots, a_n\})$ píšeme $sup\,(a_1, \ldots, a_n)$, místo $inf\,(\{a_1, \ldots, a_n\})$ píšeme $inf\,(a_1, \ldots, a_n)$.

Zřejmě, je-li $a \leq b$, je $sup\,(a, b) = b$, $inf\,(a, b) = a$. Je-li $(A, \leq)$ konečná uspořádaná množina, $a, b \in A$, a platí-li $a||b$, pak v diagramu $(A, \leq)$ nalezneme $sup\,(a, b)$ jako nejmenší prvek, který je spojen s prvky a, b a leží nad nimi; $inf\,(a, b)$ je pak největší prvek, který je spojen s a, b, a leží pod nimi. Např. na diagramu množiny A z předchozího Příkladu (na Obr.1) je $sup\,(a, b) = c$, $inf\,(f, g) = e$.

Cvičení: Ověřte, že pro každou uspořádanou množinu $(A, \leq)$ a pro každé dvě její podmnožiny X, Y platí:

(i) $U(\emptyset) = A$, $L(\emptyset) = A$;

(ii) $X \subseteq Y \Rightarrow\; L(Y) \subseteq L(X)$, $U(Y) \subseteq U(X)$;

(iii) má-li A největší prvek a, pak $U(A) = \{a\}$, nemá-li A největší prvek, pak $U(A) = \emptyset$; duálně, má-li A nejmenší prvek b, pak $L(A) = \{b\}$, nemá-li A nejmenší prvek, pak $L(A) = \emptyset$;

(iv) $L(U(A)) = A$, $\;U(L(A)) = A$.

1.4 Polosvazy

Definice: *Polosvazem* nazýváme komutativní idempotentní pologrupu, t.j. takový grupoid $(G, \circ)$, kde pro každé tři prvky $a, b, c \in G$ platí tyto identity:
(a) asociativita: $a \circ (b \circ c) = (a \circ b) \circ c$
(k) komutativita: $a \circ b = b \circ a$
(i) idempotence: $a \circ a = a$.

Věta 1.5. *Nechť $(G, \circ)$ je polosvaz. Relace $\leq$ definovaná na G předpisem:*

$$a \leq b \quad \textit{právě když} \quad a \circ b = b$$

je uspořádání, přičemž v uspořádané množině $(G, \leq)$ existuje pro každé $a, b \in G$ $sup\,(a, b)$ a platí $sup\,(a, b) = a \circ b$.

Důkaz: Z idempotence plyne ihned $a \leq a$ pro každé $a \in G$, tedy $\leq$ je reflexivní. Je-li $a \leq b$, $b \leq c$ pro $a, b, c \in G$, pak $a \circ b = b$, $b \circ c = c$, tedy z asociativity dostáváme $a \circ c = a \circ (b \circ c) = (a \circ b) \circ c = b \circ c = c$, tedy $a \leq c$, t.j. $\leq$ je tranzitivní. Nechť $a \leq b$ a $b \leq a$. Vzhledem ke komutativitě dostáváme $b = a \circ b = b \circ a = a$, tedy $\leq$ je antisymetrická, t.j. $\leq$ je uspořádání v G.

Z asociativity, komutativity a idempotence plyne $a \circ (a \circ b) = a \circ b$, $b \circ (a \circ b) = a \circ b$, tedy $a \leq a \circ b$, $b \leq a \circ b$, t.j. $a \circ b \in U(a, b)$. Nechť $c \in U(a, b)$, pak $a \leq c$, $b \leq c$, tedy $a \circ c = c$, $b \circ c = c$, tudíž $(a \circ b) \circ c = (a \circ b) \circ (c \circ c) = (a \circ c) \circ (b \circ c) = c \circ c = c$, t.j. $a \circ b \leq c$. Je tedy $a \circ b$ nejmenší prvek v $U(a, b)$, t.j. $a \circ b = sup\,(a, b)$. □

Věta 1.6. *Nechť $(G, \leq)$ je uspořádaná množina a pro každé $a, b \in G$ existuje $sup\,(a, b)$. Označme $a \circ b = sup\,(a, b)$; pak $(G, \circ)$ je polosvaz.*

Důkaz: Jelikož $sup\,(a, a) = a$, $sup\,(a, b) = sup\,(b, a)$, $sup\,(a, sup\,(b, c)) = sup\,(a, b, c) = sup\,(sup\,(a, b), c)$, je ihned zřejmé, že operace $\circ$ je idempotentní, komutativní a asociativní. □

Poznámka: Zaměníme-li uspořádání za tzv. duální, t.j. $\geq$, pak, dle principu duality, pojem suprema v duálním uspořádaní $\geq$ je infimem v uspořádání $\leq$. Definujeme-li v polosvazu uspořádání předpisem:

$$a \leq b \quad \text{právě když} \quad a \circ b = a,$$

pak pro každé $a, b \in G$ existuje $inf\,(a, b)$ a platí $inf\,(a, b) = a \circ b$ (viz V.1.5.). Obráceně, je-li $(G, \leq)$ uspořádaná množina, kde pro každé $a, b \in G$ existuje $inf\,(a, b)$, pak $(G, \circ)$, kde $a \circ b = inf\,(a, b)$ je polosvaz (srovnej s V.1.6.).

Příklady:

(1) Nechť $M \neq \emptyset$, pak v $(Exp\,M, \subseteq)$ existuje pro každé A, B supremum a platí $sup\,(A, B) = A \cup B$. Tedy $(Exp\,M, \cup)$ je polosvaz.

(2) Duálně, $inf\,(A, B) = A \cap B$, tedy $(Exp\,M, \cap)$ je opět polosvaz.

(3) Na množině všech přirozených čísel $\boldsymbol{N}$ zaveďme relaci dělitelnosti: $a|b$ právě když a dělí b. Pak $|$ je uspořádání na $\boldsymbol{N}$ a $\forall a, b \in \boldsymbol{N}$ je

$sup\,(a, b) =$ nejmenší společný násobek čísel a, b,

$inf\,(a, b) =$ největší společný dělitel čísel a, b;

označujeme $NSN(a, b)$, $NSD(a, b)$. Tedy $(\boldsymbol{N}, NSN)$, $(\boldsymbol{N}, NSD)$ jsou polosvazy.

Věta 1.7. *Nechť* $(G, \circ)$ *je polosvaz a* $(H, \circ)$ *je podgrupoid grupoidu* $(G, \circ)$. *Pak* $(H, \circ)$ *je opět polosvaz, tzv. podpolosvaz polosvazu* $(G, \circ)$.

Důkaz: Zřejmý. □

2 SVAZY

Definice: Nechť L je neprázná množina, nechť $\vee, \wedge$ jsou dvě binární operace na L takové, že $(L; \wedge)$ a $(L; \vee)$ jsou polosvazy a platí tzv. *zákony absorpce*:

$$(ab) \qquad a \wedge (a \vee b) = a \quad , \quad a \vee (a \wedge b) = a$$

pro každé $a, b \in L$. Pak se $(L, \vee, \wedge)$ nazývá *svaz.*

Tedy svaz je množina s dvěma binárními operacemi, které jsou asociativní, komutativní, idempotentní a splňují zákony absorpce.

Lemma 2.1. *Nechť* $L \neq \emptyset$ *je množina se dvěma binárními operacemi, které jsou asociativní, komutativní a splňují zákony absorpce. Pak* $\vee, \wedge$ *jsou idempotentní, t.j.* $(L; \vee, \wedge)$ *je svaz.*

Důkaz: Nechť $a, b \in L$. Označme $a \wedge b = c$. Dle absorpce obdržíme $a = a \vee (a \wedge b)$, tedy $a \wedge a = a \wedge (a \vee (a \wedge b)) = a \wedge (a \vee c) = a$, t.j. operace $\wedge$ je idempotentní. Duálně pro operaci $\vee$. □

Poznámka: Operaci $\vee$ ve svazu $(L; \vee, \wedge)$ nazýváme *spojení*, operaci $\wedge$ nazyváme *průsek*.

Věta 2.2. *Nechť* $(L; \vee, \wedge)$ *je svaz. Definujme relaci* $\leq$ *na* L *takto:*
$a \leq b$ *právě když* $a \vee b = b$. *Pak platí:*

(i) $\leq$ *je uspořádání na* L *(tzv. indukované uspořádání);*

(ii) $a \vee b = sup\,(a, b)$;

(iii) $a \leq b$ *právě když* $a \wedge b = a$;
(iv) $a \wedge b = inf\,(a,b)$.

D ů k a z : Tvzení (i) a (ii) plynou přímo z Věty 1.5. Dále, nechť $a \leq b$. Tato relace je ekvivalentní s $a \vee b = b$, což dle absorpce dává $a \wedge b = a \wedge (a \vee b) = a$, tedy platí (iii). Z duality (viz Poznámka za Větou 1.6.) plyne ihned (iv). □

Věta 2.3. *Nechť* $(L, \leq)$ *je uspořádaná množina, kde pro každé* $a, b \in L$ *existuje* $sup\,(a,b)$, $inf\,(a,b)$. *Označme* $sup\,(a,b) = a \vee b$, $inf\,(a,b) = a \wedge b$. *Pak* $(L; \vee, \wedge)$ *je svaz.*

D ů k a z : Z Věty 1.6. pyne, že stačí dokázat zákony absorpce pro operace $\vee, \wedge$. Jelikož

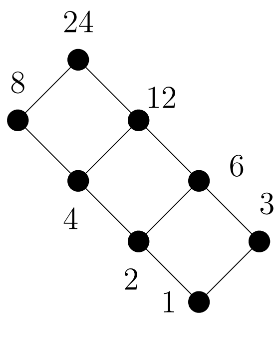
$$a \wedge b = inf\,(a,b) \leq a \leq sup\,(a,b) = a \vee b,$$

platí zřejmě

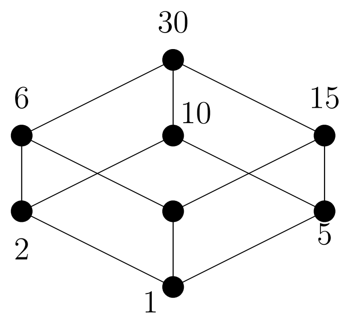
$$\begin{aligned} a \vee (a \wedge b) &= sup\,(a, inf\,(a,b)) = a, \\ a \wedge (a \vee b) &= inf\,(a, sup\,(a,b)) = a. \end{aligned}$$

□

Příklady:
(1) Každý řetězec je svaz; zřejmě $a \vee b = max\,(a,b)$, $a \wedge b = min\,(a,b)$.
(2) Nechť $M \neq \emptyset$, pak $(Exp\,M; \cup, \cap)$ je svaz.
(3) Nechť $\boldsymbol{N}$ je množina přirozených čísel, $a \vee b$ je $NSN(a,b)$, $a \wedge b$ je $NSD(a,b)$, pak $(\boldsymbol{N}; \vee, \wedge)$ je svaz.
(4) Nechť n je přirozené číslo, $P(n)$ je množina všech dělitelů čísla n. Pak $(P(n); NSN, NSD)$ je svaz. Pro $n = 24$ resp. $n = 30$ je tento svaz znázorněn diagramem na obr.4 resp obr.5 (kde uspořádání je zřejmě relace dělitelnosti).



Obr.4



Obr.5

(5) Nechť $(G, \cdot)$ je grupa. Pak množina všech normálních podgrup tvoří svaz, přičemž $A \wedge B = A \cap B$, $A \vee B = A \cdot B$, kde A, B jsou normální podgrupy.

(6) Nechť $(R, +, \cdot)$ je okruh. Množina J všech ideálů okruhu R je svaz, kde pro $I, J \in J$ je $I \wedge J = I \cap J$, $I \vee J$ je ideál, generovaný množinou $I \cup J$.

Poznámka: Princip duality se ve svazech uplatní tímto způsobem: Nahradíme-li v platném tvrzení o svazu všude symbol $\vee$ symbolem $\wedge$ a symbol $\wedge$ symbolem $\vee$, resp. symbol $\leq$ symbolem $\geq$ a naopak, dostaneme opět platné tvrzení, tzv. *duální tvrzení*. Proto v důkazech dokazujeme zpravidla jen jedno tvrzení, neboť duální z něj získáme dle principu duality výše uvedeným postupem.

Definice: Nechť $(L; \vee, \wedge)$ je svaz, nechť $\emptyset \neq A \subseteq L$. A se nazývá *podsvaz* svazu $(L; \vee, \wedge)$, jestliže $\forall a, b \in A$ platí $a \vee b \in A$, $a \wedge b \in A$.

Definice: Nechť $(A, \leq)$ je uspořádaná množina, $a, b \in A$ a platí $a \leq b$. Množina $[a, b] = \{x \in A; a \leq x \leq b\}$ se nazývá *interval* v A.

Definice: Nechť $(L; \vee, \wedge)$ je svaz a $\leq$ je indukované uspořádání. Má-li $(L, \leq)$ nejmenší prvek, nazýváme jej *nula svazu* a značíme 0; má-li $(L, \leq)$ největší prvek, nazýváme jej jednotka svazu a značíme 1.

Věta 2.4. *Nechť $(L; \vee, \wedge)$ je svaz, A_i pro $i \in I$ jeho podsvazy. Je-li $\cap\{A_i; i \in I\} \neq \emptyset$, pak je $\cap\{A_i; i \in I\}$ podsvazem svazu $(L; \vee, \wedge)$.*

Důkaz: Nechť $A = \cap\{A_i; i \in I\} \neq \emptyset$, nechť $a, b \in A$. Pak $a, b \in A_i$ $\forall i \in I$, ale A_i je podsvaz, tedy i $a \vee b \in A_i$, $a \wedge b \in A_i$ $\forall i \in I$, tedy $a \vee b \in A$, $a \wedge b \in A$, t.j. A je podsvaz. $\square$

Věta 2.5. *Nechť $(L; \vee, \wedge)$ je svaz. Pak platí:*
(i) *pro každý prvek $a \in L$ je $\{a\}$ podsvaz svazu $(L; \vee, \wedge)$;*
(ii) *každý interval svazu $(L; \vee, \wedge)$ je jeho podsvaz;*
(iii) *má-li L prvky 0 a 1, pak $L = [0, 1]$.*

Důkaz: Nejprve dokážeme (ii): Nechť $\leq$ je indukované uspořádání, $a, b \in L$ a platí $a \leq b$. Nechť $x, y \in [a, b]$. Pak $a \leq x \leq b$, $a \leq y \leq b$, tedy také $a \leq inf\,(x, y) \leq sup\,(x, y) \leq b$, t.j. $x \vee y \in [a, b]$, $x \wedge y \in [a, b]$, tedy $[a,b]$ je podsvaz svazu $(L; \vee, \wedge)$.

Jelikož $a \leq a$ pro každé $a \in L$, je $\{a\} = [a, a]$, tedy také $\{a\}$ je podsvaz $(L; \vee, \wedge)$, t.j. platí (i).

(iii): Má-li L prvky 0 a 1, pak, vzhledem k indukovanému uspořádání $\leq$ je $0 \leq x \leq 1$ pro každé $x \in L$, t.j. platí (iii). $\square$

Věta 2.6. *Má-li svaz $(L; \vee, \wedge)$ prvek 0, pak pro každé $x \in L$ platí*

$$x \wedge 0 = 0 \qquad , \qquad x \vee 0 = x.$$

Má-li svaz $(L;\vee,\wedge)$ *prvek* 1*, pak pro každé* $x \in L$ *platí*

$$x \wedge 1 = x \qquad , \qquad x \vee 1 = 1.$$

D ů k a z : Je zřejmý. □

Věta 2.7. *Nechť* $(L;\vee,\wedge)$ *je konečný svaz* (*t.j.* L *je konečná množina*). *Pak v* $(L;\vee,\wedge)$ *existují prvky* 0 *a* 1.

D ů k a z : Je-li L konečná množina, t.j. $L = \{a_1, a_2, \ldots, a_n\}$, položme $a = a_1 \wedge a_2 \wedge \ldots \wedge a_n$, $b = a_1 \vee a_2 \vee \ldots \vee a_n$. Zřejmě $a \leq a_i \leq b$ pro každý prvek $a_i \in L$, tedy a je nula, b je jednotka svazu $(L;\vee,\wedge)$. □

Věta 2.8. *Nechť* $(A;\vee,\wedge)$ *je svaz,* $\leq$ *je indukované uspořádání. Pak pro každé prvky* $a, b, c, d \in A$ *platí:*
(i) $a \wedge b \leq a \leq a \vee b$;
(ii) *jestliže* $a \leq b$, $c \leq d$, *pak*

$$a \wedge c \leq b \wedge d \qquad , \qquad a \vee c \leq b \vee d.$$

D ů k a z : (i) je zřejmé, neboť $inf\,(a,b) \leq a \leq sup\,(a,b)$. Dokážeme (ii): Jestliže $a \leq b$, $c \leq d$, pak $a \wedge b = a$, $c \wedge d = c$. Tedy

$$a \wedge c = (a \wedge b) \wedge c = (a \wedge b) \wedge (c \wedge d) = (a \wedge c) \wedge (b \wedge d),$$

odtud $a \wedge c \leq b \wedge d$. Duálně lze dokázat druhou nerovnost. □

Definice: Nechť $(A;\vee,\wedge)$ a $(B;\vee,\wedge)$ jsou svazy. Zobrazení $h : A \to B$ se nazývá *homomorfismus*, jestliže pro každé $a, b \in A$ platí:

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

Bijektivní homomorfismus se nazývá *izomorfismus*.
Ekvivalence θ na množině L se nazývá *kongruence* svazu $(L;\vee,\wedge)$, jestliže pro každé $a, b, c, d \in L$ platí implikace:

jestliže $\langle a, b\rangle \in \theta, \langle c, d\rangle \in \theta,$ pak $\langle a \vee c, b \vee d\rangle \in \theta, \langle a \wedge c, b \wedge d\rangle \in \theta.$

Úmluva: Pokud nehrozí nebezpečí nedorozumění, budeme místo zápisu: $(L;\vee,\wedge)$ je svaz, psát pouze: L je svaz; v tomto případě budou vždy operace svazu L označeny $\vee, \wedge$.

Věta 2.9. *Buďte* A, B, C *svazy,* $f : A \to B$, $g : B \to C$ *homomorfismy* (*resp. izomorfismy*). *Pak složené zobrazení* $f \circ g$ *je opět homomorfismus (izomorfismus)* $A \to C$. *Je-li* $f : A \to B$ *izomorfismus, je i* $f^{-1} : B \to A$

izomorfismus. Identické zobrazení $id\,(x) = x$ je izomorfismem svazu A. Je-li h homomorfismus svazu A do B, $a, b \in A$ a platí $a \leq b$ vzhledem k indukovanému uspořádání na A, pak $h(a) \leq h(b)$ vzhledem k indukovanému uspořádání na B.

Důkaz: Nechť $a, b \in A$, pak $f \circ g(a \vee b) = g(f(a \vee b)) = g(f(a) \vee f(b)) = g(f(a)) \vee g(f(b)) = f \circ g(a) \vee\ f \circ g(b)$, duálně pro operaci $\wedge$, tedy složení dvou homomorfismů je homomorfismus. Jelikož složení dvou bijekcí je bijekce, je složení dvou izomorfismů izomorfismem.

Je-li $f : A \to B$ izomorfismus, $x, y \in B$, pak, jelikož f je surjekce, existují $a, b \in A$ tak, že $f(a) = x, f(b) = y$. Pak $f^{-1}(x \vee y) = f^{-1}(f(a) \vee f(b)) = f^{-1}(f(a \vee b)) = a \vee b = f^{-1}(x) \vee f^{-1}(y)$, duálně pro operaci $\wedge$, tedy inversní zobrazení k izomorfismu je izomorfismus. Identita je zřejmě bijekcí a platí $id\,(x \vee y) = x \vee y = id\,(x) \vee id\,(y)$, duálně pro $\wedge$, tedy je izomorfismem.

Nechť $a, b \in A, a \leq b$. Pak $a \wedge b = a$, a pro homomorfismus h platí $h(a) = h(a \wedge b) = h(a) \wedge h(b)$, tedy $h(a) \leq h(b)$.

□

Označení: Jestliže existuje izomorfismus svazu A na svaz B, říkáme, že A,B jsou *izomorfní*, což zapisujeme $A \cong B$.

Vzhledem k Větě 2.9. platí: jsou-li A,B,C svazy, pak

$$A \cong A,$$
$$A \cong B \Rightarrow\ B \cong A,$$
$$A \cong B \text{ a } B \cong C \Rightarrow\ A \cong C,$$

tedy relace "býti izomorfní" je ekvivalencí na třídě všech svazů. □

Věta 2.10. *Necht L je svaz a θ je kongruence na L. Pak faktorová množina L/θ je svazem vzhledem k operacím definovaným takto:*

$$B, C \in L/\theta,\ \textit{pak}\ B \vee C = D\ \textit{a}\ B \wedge C = E,$$

jestliže pro každé $b \in B, c \in C$ platí $b \vee c \in D,\ \ b \wedge c \in E$.

Důkaz: Nechť $b \in B, c \in C$. Jelikož L/θ je množina všech tříd rozkladu L dle θ, existují $D \in L/\theta\,,\ E \in L/\theta$ tak, že $b \vee c \in D\,,\ b \wedge c \in E$. Nechť $b' \in B, c' \in C$. Pak $\langle b, b' \rangle \in \theta\,,\ \langle c, c' \rangle \in \theta$, tedy také $\langle b \vee c, b' \vee c' \rangle \in \theta$, t.j. $b' \vee c' \in D$, a $\langle b \wedge c\,,\ b' \wedge c' \rangle \in \theta$, t.j. $b' \wedge c' \in E$. Protože třídy rozkladu jsou vzájemně disjunktní, jsou D,E určeny jednoznačně, tedy $\vee, \wedge$ jsou skutečně binární operace na L/θ. Zbývá dokázat platnost identit (a), (k), (ab) pro tyto operace.

Nechť $x \in (B \vee C) \vee D$ pro některé $B, C, D \in L/\theta$, pak $x = (b \vee c) \vee d$ pro některé $b \in B,\ \ c \in C,\ \ d \in D$. Pak $x = b \vee (c \vee d)$, neboť operace $\vee$

je v L asociativní. Tedy je $x \in B \vee (C \vee D)$. Dokázali jsme $(B \vee C) \vee D \subseteq B \vee (C \vee D)$. Analogicky se dokáže obrácená inkluze, tedy operace $\vee$ na L/θ je asociativní. Duálně se dokáže asociativita operace $\wedge$ na L/θ. Důkaz komutativity a absorpce je obdobný. $\square$

Věta 2.11. Věta o homomorfismu.

(1) *Nechť A, B jsou svazy a $h : A \to B$ je surjektivní homomorfismus. Definujme relaci θ_h na A takto:*

$$(*) \qquad \langle a, b\rangle \in \theta_h \text{ právě když } h(a) = h(b).$$

Pak θ_h je kongruence na A a $A/\theta_h \cong B$.

(2) *Nechť θ je kongruence na svazu L. Pro $a \in L$ označme $[a]_\theta$ tu třídu L/θ, která obsahuje prvek a. Pak zobrazení $h_\theta : L \to L/\theta$ dané předpisem*

$$(**) \qquad h_\theta(a) = [a]_\theta$$

je surjektivní homomorfismus svazu L na L/θ.

Důkaz: (1) Nechť A, B jsou svazy a $h : A \to B$ je homomorfismus. Pak zřejmě relace θ_h definovaná předpisem $(*)$ je reflexivní, symetrická a tranzitivní, tudíž ekvivalence. Nechť $\langle a, b\rangle \in \theta_h$, $\langle c, d\rangle \in \theta_h$. Pak $h(a) = h(b)$ a $h(c) = h(d)$, tedy

$$h(a \vee c) = h(a) \vee h(c) = h(b) \vee h(d) = h(b \vee d),$$

t.j. $\langle a \vee c, b \vee d\rangle \in \theta_h$. Duálně se dokáže $\langle a \wedge c, b \wedge d\rangle \in \theta_h$, tedy θ_h je kongruence na A. Dle Věty 2.10. je A/θ_h faktorový svaz. Zobrazení $[a]_{\theta_h} \to h(a)$ je zřejmě injekce, neboť $h(a) = h(b) \Rightarrow \langle a, b\rangle \in \theta_h$, t.j. $[a]_{\theta_h} = [b]_{\theta_h}$. Je zřejmě surjekce, jelikož h je surjekce, a je homomorfismem, neboť $[a]_{\theta_h} \vee [b]_{\theta_h} = [a \vee b]_{\theta_h} \to h(a \vee b) = h(a) \vee h(b)$, duálně pro $\wedge$, tedy toto zobrazení je izomorfismus $A/\theta \to B$.

(2) Nechť θ je kongruence na svazu L. Dle Věty 2.10. je L/θ faktorový svaz. Definujeme $h_\theta : L \to L/\theta$ předpisem $(**)$. Zřejmě h_θ je surjekce. Dále pro $a, b \in L$ máme

$$h_\theta(a \vee b) = [a \vee b]_\theta = [a]_\theta \vee [b]_\theta = h_\theta(a) \vee h_\theta(b),$$

což plyne z vlastností kongruence a z definice operace na faktorovém svazu, viz Věta 2.10. Duálně se dokáže $h_\theta(a \vee b) = h_\theta(a) \vee h_\theta(b)$, tedy h_θ je surjektivní homomorfismus. $\square$

Věta 2.12. *Bijekce svazu A na svaz B je izomorfismus tehdy a jen tehdy, jestliže $a \leq b$ právě když $h(a) \leq h(b)$.*

D ů k a z : Je-li h izomorfismus, pak dle Věty 2.9. jsou h i h^{-1} izotonní. Obráceně, nechť h i h^{-1} jsou izotonní bijekce. Pak

$$h(a) \wedge h(b) = \mathit{inf}\,(h(a), h(b)) = h(\mathit{inf}\,(a, b)) = h(a \wedge b),$$

duálně $h(a) \vee h(b) = h(a \vee b)$. □

3 ÚPLNÉ SVAZY

Podle Věty 2.3. je svazem každá uspořádaná množina $(A, \leq)$, ve které existují *sup*(a,b) a *inf*(a,b) pro každé dva prvky $a, b \in A$. Indukcí lze snadno dokázat, že je-li $(A, \leq)$ svazem, pak existují *sup* a *inf* pro každou *konečnou* podmnožinu $B \subseteq A$. Nelze odtud však odvodit žádné tvrzení o *sup* a *inf* nekonečných podmnožin. Například ve svazu z Příkladu (3) (str.9) je $\mathit{sup}\,(a, b) = a \vee b = NSN(a, b)$, $\mathit{inf}\,(a, b) = a \wedge b = NSD(a, b)$, ale pro žádnou nekonečnou podmnožinu $M \subseteq \boldsymbol{N}$ zřejmě *sup* M neexistuje.

Na druhé straně, existují svazy, ve kterých *sup* a *inf* existují i pro nekonečné podmnožiny, např. svaz $(\mathit{Exp}\ M; \cup, \cap)$ pro nekonečnou množinu M. Zavedeme proto následující pojem.

Definice: Uspořádaná množina $(L, \leq)$ se nazývá *úplný svaz*, jestliže pro každou $S \subseteq L$ existuje *sup* S a *inf* S v L.

Je zřejmé, že každý úplný svaz je svazem, neboť podle této definice existují *sup* a *inf* i pro dvouprvkové podmnožiny (viz Věta 2.3.). Dále každý úplný svaz $(L, \leq)$ má vždy největší a nejmenší prvek, jsou to prvky $1 = \mathit{sup}\, L$ a $0 = \mathit{inf}\, L$. Dále, v úplném svazu lze předpokládat existenci jen jednoho z prvků *sup* resp. *inf* pro libovolnou podmnožinu, druhý prvek pak lze již zkonstruovat, viz:

Věta 3.1. *Nechť* $(L, \leq)$ *je uspořádaná množina, v níž existuje* $\mathit{inf}\, S$ *pro každou* $S \subseteq L$. *Pak* $(L, \leq)$ *je úplný svaz.*

D ů k a z : Nechť $S \subseteq L$ a nechť $U(S)$ je horní kužel množiny S. Zřejmě $U(S) \neq \emptyset$, neboť $1 = \mathit{inf}\, \emptyset$, $1 \in U(S)$. Označme $x = \mathit{inf}\ \ U(S)$. Zřejmě $s \leq x$ pro každé $s \in S$ a dále, je-li $s \leq y$ pro každé $s \in S$, pak $y \in U(S)$, tedy $x = \mathit{inf}\ \ U(S) \leq y$, tedy $x = \mathit{sup}\ S$. □

Poznámka: Dle principu duality lze Větu 3.1. vyslovit i v tomto tvaru: má-li každá podmnožina S uspořádané množiny $(L, \leq)$ supremum, pak je $(L, \leq)$ úplný svaz.

Příklad: Nechť $M \neq \emptyset$ je množina (např. nekonečná). Pak množina všech ekvivalencí na M uspořádaná množinovou inkluzí je úplný svaz. Dle Věty 3.1. totiž stačí dokázat, že pro libovolnou množinu I a libovolnou množinu ekvivalencí E_i $(i \in I)$ na M je $\cap\{E_i; i \in I\}$ opět ekvivalence. Důkaz tohoto jednoduchého tvrzení si čtenář ověří jako cvičení.

Analogicky se dokáže, že množina všech kongruencí *Con* A na grupoidu (grupě, okruhu, svazu) A uspořádaná vzhledem k $\subseteq$ je úplný svaz.

Nechť $(A, \leq), (B, \leq)$ jsou dvě uspořádané množiny. Zobrazení $f : A \to B$ se nazývá *izotonní zobrazení*, jestliže pro každé $a, b \in A$ platí:

$$\text{jestliže } a \leq b, \text{ pak } f(a) \leq f(b).$$

Věta 3.2. Věta o pevném bodu. *Nechť $(L, \leq)$ je úplný svaz a nechť f je izotonní zobrazení L do L. Pak existuje prvek $x \in L$ takový, že $f(x) = x$ (tzv. pevný bod zobrazení f).*

D ů k a z: Nechť $(L, \leq)$ je úplný svaz a $f : L \to L$ je izotonní zobrazení. Nechť $S = \{v \in L; v \leq f(v)\}$. Zřejmě $S \neq \emptyset$, neboť nejmenší prvek $0 \in S$. Položme $x = sup\ S$. Pak pro každé $s \in S$ je $s \leq x$, tedy $s \leq f(s) \leq f(x)$. Tedy $f(x)$ je větší nebo rovno každému $s \in S$, je tedy větší nebo rovno i sup $S = x$, t.j. $x \leq f(x)$. Ale f je izotonní zobrazení, tedy $f(x) \leq f(f(x))$, t.j. $f(x) \in S$. Ale $x = sup\ S$, tedy $f(x) \leq x$. Odtud $f(x) = x$. □

Dokážeme, že každý svaz je možné považovat za podsvaz úplného svazu. Nejprve definujme:

Definice: Nechť $(L; \vee, \wedge)$ je svaz, $\emptyset \neq I \subseteq L$. I se nazývá *ideál* svazu $(L; \vee, \wedge)$, pokud splňuje následující podmínky:
(i) jestliže $x, y \in I$, pak $x \vee y \in I$;
(ii) jestliže $x \in I, a \in L$, pak $x \wedge a \in I$.

Věta 3.3. *Nechť $(L; \vee, \wedge)$ je svaz, J_0 je množina všech ideálů svazu L a $J = J_0 \cup \{\emptyset\}$. Pak $(J, \subseteq)$ je úplný svaz.*

D ů k a z: Nechť $\boldsymbol{J} \subseteq J_0$, t.j. $\boldsymbol{J}$ je některá množina ideálů svazu L. Je-li $\cap\boldsymbol{J} = \emptyset$, pak $\cap\boldsymbol{J} \in J$. Nechť $\cap\boldsymbol{J} \neq \emptyset$, označme $\cap\boldsymbol{J} =$ J. Nechť $x, y \in$ J, $a \in L$. Pak $\forall I \in \boldsymbol{J}$ je $x, y \in I$, tudíž $x \vee y \in I$ a $x \wedge a \in I$ pro každé $I \in \boldsymbol{J}$, tedy i $x \vee y \in \cap\boldsymbol{J} =$ J, $x \wedge a \in$ J, t.j. J je ideál, tedy $\cap\boldsymbol{J} =$ J$\in J_0 \subseteq J$. Tedy pro každou $\boldsymbol{J} \subseteq J$ je $inf\ \boldsymbol{J} = \cap\boldsymbol{J}$ prvkem J, t.j. dle Věty 3.1. je $(J, \subseteq)$ úplný *svaz.* □

Lemma 3.4. *Nechť L je svaz, $a \in L$. Pak $I(a) = \{x \in L; x \leq a\}$ je ideál svazu L.*

Důkaz: Nechť $x, y \in I(a)$. Pak $x \leq a$, $y \leq a$, tedy dle Věty 2.8. je $x \vee y \leq a \vee a = a$, t.j. $x \vee y \in I(a)$. Je-li $b \in L$, pak $x \wedge b \leq x \leq a$, tedy $x \wedge b \in I(a)$, t.j. $I(a)$ je ideál svazu L. $\square$

Věta 3.5. *Každý svaz je izomorfní s podsvazem úplného svazu.*

Důkaz: Nechť L je svaz. Definujme zobrazení f svazu L do množiny všech ideálů J svazu L (viz Věta 3.3) takto:

$$f(a) = I(a).$$

Pak zřejmě f je injekce, neboť $I(a) = I(b) \Rightarrow a = b$. Tedy f je bijekce na množinu $\{I(a); a \in L\} \subseteq J$. Dokážeme, že f je svazový homomorfismus. Pro každé $a, b \in L$ zřejmě platí $a \wedge b \in I(a)$, $a \wedge b \in I(b)$, tedy $a \wedge b \in I(a) \cap I(b) \Rightarrow I(a \wedge b) \subseteq I(a) \cap I(b)$. Jestliže $x \in I(a) \cap I(b)$, pak $x \leq a$, $x \leq b$, tedy $x \leq a \wedge b \Rightarrow x \in I(a \wedge b)$, tedy $I(a) \cap I(b) \subseteq I(a \wedge b)$. Dohromady dostáváme

$$f(a \wedge b) = I(a \wedge b) = I(a) \cap I(b) = f(a) \cap f(b).$$

Dle důkazu Věty 3.3. je $I(a) \vee I(b)$ rovno průniku všech ideálů z J, obsahujících $I(a) \cup I(b)$. Avšak $I(a) \subseteq I(a \vee b)$, $I(b) \subseteq I(a \vee b)$, t.j. $I(a) \cup I(b) \subseteq I(a \vee b)$, tedy i $I(a) \vee I(b) \subseteq I(a \vee b)$. Je-li však $I \in J$ takový, že $I(a) \cup I(b) \subseteq I$, pak $a \in I, b \in I$, tedy i $a \vee b \in I$, t.j. $I(a \vee b) \subseteq I$. Neboli $I(a) \vee I(b) = I(a \vee b)$, odkud

$$f(a \vee b) = I(a \vee b) = I(a) \vee I(b) = f(a) \vee f(b),$$

tedy f je homomorfismus L do úplného svazu $(J, \subseteq)$, neboli f je izomorfismus L na podsvaz $\{I(a); a \in L\}$. $\square$

Poznámka: je-li svaz L konečný, I jeho ideál, pak zřejmě $I = I(a)$, kde $a = sup\ I$. Tedy $(\{I(a); a \in L\}, \subseteq)$ je svaz všech ideálů konečného svazu L, t.j. zobrazení $f : a \to I(a)$ je izomorfismus L na $(J, \subseteq)$.

Pojem ideálu lze zobecnit i pro polosvazy: Je-li $(G, \circ)$ polosvaz, je dle Věty 1.5. relace $a \leq b$ právě když $a \circ b = b$ uspořádáním, vzhledem ke kterému je $a \circ b = sup\,(a, b)$. Budeme tedy, ve shodě s označením pro svazy, značit polosvazovou operaci symbolem $\vee$. Nyní definujme:

Definice: Nechť $(F, \vee)$ je polosvaz. $\emptyset \neq I \subseteq F$ se nazývá *ideál polosvazu* $(F, \vee)$, jestliže pro každé $a, b \in F$ platí

$$a \vee b \in I \text{ tehdy a jen tehdy, když } a \in I, b \in I.$$

Označme $J(F)$ množinu všech ideálů polosvazu F. Má-li F nejmenší prvek 0, pak lze dokázat stejně jako ve Větě 3.3., že $(J(F), \subseteq)$ je úplný svaz (jelikož $0 \in F$, zřejmě průnik libovolné podmnožiny $J(F)$ je neprázdný, neboť obsahuje 0).

Nyní zavedeme důležitý pojem pro další algebraické zkoumání:

Definice: Nechť $(L, \leq)$ je úplný svaz. Prvek $a \in L$ se nazývá *kompaktní*, jestliže pro každou $X \subseteq L$ platí: jestliže $a \leq sup\ X$, pak existuje konečná podmnožina $\{y_1, \ldots, y_n\} \subseteq X$ tak, že $a \leq sup\,(y_1, \ldots y_n) = y_1 \vee \ldots \vee y_n$. Úplný svaz $(L, \leq)$ se nazývá *algebraický* (nebo též *kompaktně generovaný*), je-li každý prvek z L supremem kompaktních prvků.

Poznámka: Je-li $(L, \leq)$ úplný svaz, budeme pro stručnost označovat *sup* X symbolem $\vee X$, symbol *inf* X budeme označovat $\wedge X$ pro každou $X \subseteq L$, což je ve shodě s označením $\vee$ a $\wedge$ pro *sup* a *inf* v případě konečných podmnožin.

Nyní lze dokázat důležitou representační větu pro algebraické svazy:

Věta 3.6. *Svaz L je algebraický tehdy a jen tehdy, je-li izomorfní svazu všech ideálů některého polosvazu $(F, \vee)$ s nejmenším prvkem 0.*

Důkaz: (1) Nechť $(F, \vee)$ je polosvaz s 0. Dokážeme, že svaz $(J(F), \subseteq)$ všech ideálů polosvazu $(F, \vee)$ je algebraický. Víme, že $(J(F), \subseteq)$ je úplný svaz (viz poznámka za definicí ideálu polosvazu). Dokážeme, že každý ideál $I(a) = \{x \in F; x \leq a\}$ je kompaktní prvek tohoto svazu (čtenář si dle definice snadno ověří, že $I(a)$ je skutečně ideál polosvazu $(F, \vee)$). Nechť $I(a) \leq \vee\{I_\alpha; I_\alpha \in X\}$ pro některou $X \subseteq J(F)$. Položme $J = \{y \in F; y \leq h_1 \vee \ldots \vee h_n$, kde $h_i \in I_{\alpha_i}$ pro $I_{\alpha_i} \in X\}$. Zřejmě $J \subseteq \vee\{I_\alpha; I_\alpha \in X\}$. Avšak J je zřejmě ideál polosvazu $(F, \vee)$ a pro každé $h \in I_\alpha$ (kde $I_\alpha \in X$) je $h \in J$, tedy $\vee\{I_\alpha; I_\alpha \in X\} \subseteq J$, t.j. $J = \vee\{I_\alpha; I_\alpha \in X\}$. Tedy $I(a) = J$, t.j. $a \in J$, neboli dle definice J, $a \leq h_1 \vee \ldots \vee h_n$ pro některé $h_i \in I_{\alpha_i},\ I_{\alpha_i} \in X$. Odtud

$$I(a) \leq\ I_{\alpha_1} \vee \ldots \vee\ I_{\alpha_n},$$

tedy $I(a)$ je kompaktní prvek svazu $(J(F), \subseteq)$. Jelikož pro každý ideál $I \in J(F)$ platí

$$I = \vee\{I(a); a \in I\},$$

je každý prvek z $(J(F), \subseteq)$ supremem kompaktních prvků, tedy $(J(F), \subseteq)$ je algebraický svaz.

(2) Nechť L je libovolný algebraický svaz. Označme F množinu jeho kompaktních prvků. Zřejmě $0 \in F$. Nechť $a, b \in F$ a platí $a \vee b \leq\ \vee X$ pro některou $X \subseteq L$. Pak $a \leq\ a \vee b \leq\ \vee X$, odkud $a \leq\ \vee X_0$ pro některou konečnou $X_0 \subseteq X$. Analogicky $b \leq\ X_1$ pro některou konečnou $X_1 \subseteq X$.

Tedy $a \vee b \leq \ \vee(X_0 \cup X_1)$, kde zřejmě $X_0 \cup X_1$ je konečná podmnožina X. Neboli, F je uzavřená na $\vee$, t.j. $(F, \vee)$ je polosvaz s 0.

Nyní definujme zobrazení $f : L \to J(F)$ takto:

$$f(a) = \{x \in F; x \leq a\}.$$

Zřejmě $a = sup\{x \in F; x \leq a\} = \vee f(a)$, t.j. $f(a) = f(b) \Rightarrow\ a = \vee f(a) = \vee f(b) = b$, tedy f je injekce. Dokážeme, že f je surjekce. Nechť $I \in J(F)$ a $a = \vee I$. Pak $f(a) \supseteq I$. Obráceně, nechť $x \in f(a)$, pak $x \leq \vee I$, avšak $x \in F$, t.j. je kompaktní, tedy existuje konečná $I_1 \subseteq I$ tak, že $x \leq \vee I_1$. Odtud $x \in I$, tedy $f(a) \subseteq I$. Dohromady $f(a) = I$, tedy f je surjekce. Zřejmě

$$f(a \vee b) = \{x \in F; x \leq a \vee b\} = \{x \in F; x \leq a\} \vee \{x \in F; x \leq b\} = f(a) \vee f(b),$$

$$f(a \wedge b) = \{x \in F; x \leq a \wedge b\} = \{x \in F; x \leq a\} \wedge \{x \in F; x \leq b\} = f(a) \vee f(b),$$

tedy f je izomorfismus. □

4 MODULÁRNÍ, DISTRIBUTIVNÍ A KOMPLEMENTÁRNÍ SVAZY

Věta 4.1. *Nechť L je svaz. Pak pro každé $a, b, c \in L$ platí tzv. distributivní nerovnosti, t.j.*

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

Pro každé $a, b, c \in L$ splňující $a \leq c$ platí tzv. modulární nerovnost, t.j.

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

D ů k a z: Jelikož $a \leq a \vee b$, $a \leq a \vee c$, je také $a \leq \ (a \vee b) \wedge (a \vee c)$. Dále $b \wedge c \leq b \leq a \vee b$, $b \wedge c \leq c \leq a \vee c$, tedy $b \wedge c \leq \ (a \vee b) \wedge (a \vee c)$. Odtud již dostaneme nerovnost

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

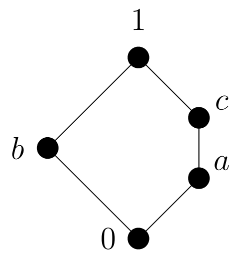
Duálně se dokáže druhá distributivní nerovnost.

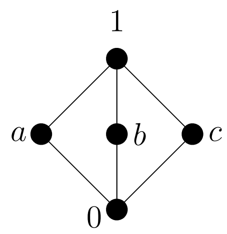
Nechť nyní $a \leq c$. Jelikož $a \leq \ a \vee b$, dostaneme $a \leq \ (a \vee b) \wedge c$. Podobně $b \wedge c \leq b \leq a \vee b$, $b \wedge c \leq c$ implikují $b \wedge c \leq (a \vee b) \wedge c$, tedy dohromady

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

□

Poznámka: Obrácené nerovnosti obecně ve svazu neplatí. Je-li např. $L = N_5$ (viz obr.6), tzv *pentagon*, pak $a \leq c$, ale $a \vee (b \wedge c) = a \vee 0 = a$, prvek a však není větší než prvek $c = (a \vee b) \wedge c$, tedy nerovnost obrácená k modulární nerovnosti v tomto svazu neplatí. Je-li $L = M_3$ (viz obr. 7), pak $a \vee (b \wedge c) = a$ není větší než $1 = (a \vee b) \wedge (a \vee c)$, dále $(a \wedge b) \vee (a \wedge c) = 0$ není větší než $a = a \wedge (b \vee c)$, tady ani jedna z nerovností obrácených k distributivním nerovnostem v tomto svazu neplatí.





Obr.6 Obr.7

Definice: Svaz L se nazývá *distributivní*, jestliže pro každé $a, b, c \in L$ platí

$$\text{(D)} \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Svaz L se nazývá *modulární*, jestliže pro každé $a, b, c \in L$ splňující $a \leq c$ platí

$$\text{(M)} \qquad a \vee (b \wedge c) = (a \vee b) \wedge c.$$

Věta 4.2. *Svaz L je distributivní, právě když pro každé $a, b, c \in L$ platí rovnost duální k rovnosti* (D)*, t.j.*

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

Důkaz: Nechť L je distributivní. Pak platí:

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

tedy platí identita z Věty 4.2. Obrácené tvrzení lze dokázat duálně. □

Věta 4.3. *Každý distributivní svaz je modulární.*

Důkaz: Nechť L je distributivní, $a, b, c \in L$ a platí $a \leq c$. Pak

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

$\square$

Věta 4.4. *Každý podsvaz a každý homomorfní obraz distributivního svazu je distributivní svaz.*

D ů k a z : Je zřejmý. $\square$

Příklady distributivních svazů:

(1) Každý řetězec je distributivní svaz.

(2) Nechť $M \neq \emptyset$, pak $(Exp\ M; \cup, \cap)$ je distributivní svaz.

(3) Svaz všech podgrup cyklické grupy je distributivní.

D ů k a z : Každá podgrupa cyklické grupy je normální, tedy pro dvě podgrupy A,B cyklické grupy $(G, \circ)$ platí $A \wedge B = A \cap B$, $A \vee B = A \circ B$. Dle Věty 4.1. stačí ověřit platnost inkluze

$$A \cap (B \circ C) \subseteq \ (A \cap B) \circ (A \cap C).$$

Nechť tedy $a \in A \cap (B \circ C)$. Pak $a \in A$ a existují $b \in B, c \in C$ tak, že $a = b \circ c$. Nechť d je generátor $(G, \circ)$. Pak $b = d^m$, $c = d^n$ pro některá $m, n \in \boldsymbol{Z}$. Tedy $a = d^{m+n}$. Nechť $m' = NSN(m+n, m)$, $n' = NSN(m+n, n)$. Pak $d^{m'} \in A \cap B$, $d^{n'} \in A \cap C$. Nechť $h = NSD(m', n')$. Pak $h = xm' + yn'$ pro některá $x, y \in \boldsymbol{Z}$, tedy

$$d^h = (d^{m'})^x \circ (d^{n'})^y \in \ (A \cap B) \circ (A \cap C).$$

Avšak $h = NSD(m', n') = NSD(NSN(m+n, m)\, , NSN(m+n, n)) = NSN(m+n, NSD(m, n)) = m+n$, tedy

$$d^h = d^{m+n} = a \quad , \text{ t.j. } a \in (A \cap B) \circ (A \cap C).$$

$\square$

Příklady modulárních svazů:

(4) Svaz všech normálních podgrup libovolné grupy $(G, \circ)$ je modulární.

D ů k a z : Nechť A,B,C jsou normální podgrupy grupy $(G, \circ)$ a nechť $A \subseteq C$. (Zřejmě $A \wedge B = A \cap B, A \vee B = A \circ B$). Dle Věty 4.1 stačí ověřit nerovnost $(A \circ B) \cap C \subseteq A \circ (B \cap C)$. Nechť $a \in (A \circ B) \cap C$. Pak $a \in C$ a existují $d \in A, b \in B$ tak, že $a = d \circ b$. Tedy $d \in A \subseteq C$, ale C je podgrupa, tedy $d^{-1} \in C$, t.j. $b = d^{-1} \circ a \in C$. Tedy $b \in B \cap C$, t.j. $a = d \circ b \in \ A \circ (B \cap C)$.
$\square$

(5) Množina všech ideálů okruhu R tvoří modulární svaz.

D ů k a z: Zřejmě pro dva ideály I, J okruhu R je $I \cap J = inf\,(I, J)$ vzhledem k uspořádání inkluzí, a dále $I + J = \{i + j;\ i \in I, j \in J\}$ je nejmenší ideál okruhu R, obsahující současně I i J, tedy $I + J$ je $sup\,(I, J)$. Tedy množina všech ideálů je svaz, $\vee = +$, $\wedge = \cap$. Nechť I, J, K jsou ideály okruhu R takové, že $I \subseteq K$, a nechť $k \in (I + J) \cap K$. Pak $k \in K$, $k = i + j$, kde $i \in I, j \in J$. Ale $I \subseteq K$, tedy $i \in K$, a také $j = k - i \in K$, tedy $j \in J \cap K$. Odtud $k = i + j \in I + (J \cap K)$; dokázali jsme inkluzi

$$(I + J) \cap K \subseteq I + (J \cap K).$$

Z Věty 4.1. plyne platnost obrácené inkluze, tedy svaz všech ideálů okruhu R je modulární. □

Věta 4.5. *Svaz L je modulární, právě když pro každé $a, b, c \in L$ platí*

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

D ů k a z: Nechť L je modulární. Jelikož $a \leq a \vee c = c'$, platí dle (M)

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

Obráceně, nechť pro libovolné $a, b, c \in L$ platí identita z Věty 4.5. a nechť $a \leq c$. Pak $a \vee c = c$, a tato identita přechází ihned v axiom (M). □

Poznámka: Dle Věty 4.5. lze tedy i modulární svazy charakterizovat pouze identitami. Nyní však ukážeme, že jak distributivní, tak i modulární svazy lze charakterizovat pomocí tzv. *zakázaných podsvazů*.

Věta 4.6. *Svaz L je modulární, právě když neobsahuje podsvaz izomorfní s N_5. Svaz L je distributivní, právě když neobsahuje podsvaz izomorfní s N_5 nebo M_3* (viz obr.6.,7.).

D ů k a z:

(a) Z Věty 4.5. vyplývá, že každý podsvaz modulárního svazu je modulární. Dle Poznámky za Větou 4.1. tedy modulární svaz nemůže obsahovat podsvaz izomorfní s N_5. Je-li L distributivní, pak dle Věty 4.4. je každý jeho podsvaz distributivní, tedy L nemůže obsahovat podsvaz izomorfní M_3, jak plyne z Poznámky za Větou 4.1. Dle Věty 4.3. je však L také modulární, tedy nemůže obsahovat ani podsvaz izomorfní s N_5, jak bylo výše dokázáno.

(b) Předpokládejme, že L není modulární. Pak obsahuje prvky a, b, c takové, že $a < c$, ale

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

Nechť $x = c \vee b$, $y = a \wedge b$. Pak z $a < c$ plyne $a \vee b \leq x$, $c \wedge b \geq y$. Je-li však např. $a \vee b < x$, pak snadno dokážeme nerovnost obrácenou k (M); stejně tak v případě $c \wedge b > y$. Musí tedy platit $a \vee b = x$, $c \wedge b = y$. Odtud

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

tedy $\{y, a, b, c, x\}$ tvoří N_5, kde x je největší a y nejmenší prvek.

Předpokládejme, že L není distributivní. Pak buď není modulární, t.j. obsahuje podsvaz izomorfní s N_5, jak bylo výše ukázáno, nebo je modulární, ale existují prvky $a, b, c \in L$ tak, že

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

Jsou-li kterékoliv dva z prvků a,b,c srovnatelné, pak z modularity L vyplývá platnost distributivní identity pro tyto tři prvky. Tedy a,b,c jsou nesrovnatelné, t.j. tvoří antiřetězec. Položme $x = a \vee b \vee c$, $y = a \wedge b \wedge c$. Je-li např. $a \vee b < x$ nebo $a \wedge b > y$, pak tyto prvky a,b,c buď neporušují distributivní identitu, nebo prvky $\{y, a \wedge b, b, c, x\}$ nebo $\{y, b, a \vee b, c, x\}$ tvoří podsvaz izomorfní s N_5, což by byl spor s modularitou svazu L. Analogicky v případě $b \vee c < x$ nebo $b \wedge c > x$ nebo $a \vee c < x$ nebo $a \wedge c > y$.

Zbývá tedy $a \vee b = b \vee c = a \vee c = x$, $a \wedge b = b \wedge c = a \wedge c = y$, tedy $\{y, a, b, c, x\}$ tvoří podsvaz izomorfní s M_3, kde y je nejmenší a x největší prvek. $\square$

Důsledek: *Svaz L je modulární tehdy a jen tehdy, když pro každé $x, y, z \in L$, $x \leq y$ platí:*

$$(*) \qquad \textit{jestliže } x \wedge z = y \wedge z \quad \textit{a} \quad x \vee z = y \vee z, \textit{ pak } x = y.$$

Svaz L je distributivní tehdy a jen tehdy, když pro každé $x, y, z \in L$ platí $(*)$.

Důkaz: Je-li L modulární, $x, y, z \in L$ a neplatí $(*)$, pak $\{x \wedge y \wedge z, x, y, z, x \vee y \vee z\}$ tvoří N_5 - spor. Jestliže L není modulární, pak obsahuje podsvaz izomorfní s N_5, jehož prvky nesplňují $(*)$. Je-li L distributivní, $x, y, z \in L$ a neplatí $(*)$, pak $\{x \wedge y \wedge z, x, y, z, x \vee y \vee z\}$ tvoří N_5 nebo M_3, jehož prvky však nesplňují $(*)$, jak se můžeme snadno přesvědčit. $\square$

Věta 4.7. *Nechť L je modulární svaz. Nechť $a, b \in L$. Pak intervaly $[a, a \vee b], [a \wedge b, b]$ jsou izomorfní podsvazy.*

Důkaz: Definujme zobrazení $f : [a, a \vee b] \to [a \wedge b, b]$ předpisem $f(x) = x \wedge b$. Pak pro každé $y \in [a \wedge b, b]$ je $a \leq a \vee y \leq a \vee b$, t.j. $a \vee y \in [a, a \vee b]$, přičemž dle (M) platí

$$f(a \vee y) = (y \vee a) \wedge b = y \vee (a \wedge b) = y.$$

Tedy f je surjekce. Nechť $x, x' \in [a, a \vee b]$. Jestliže $f(x) = f(x')$, pak $x \wedge b = x' \wedge b$, tedy dle (M) dostaneme

$$x = (a \vee b) \wedge x = a \vee (b \wedge x) = a \vee (b \wedge x') = (a \vee b) \wedge x' = x',$$

tedy f je injekce. Platí

$$f(x \wedge x') = x \wedge x' \wedge b = (x \wedge b) \wedge (x' \wedge b) = f(x) \wedge f(x').$$

Dále, jelikož $x \wedge b \leq b$, $a \leq x$, $a \leq x' \leq a \vee b$, dostaneme opakovaným použitím modulární identity (M):
$f(x) \vee f(x') = (x \wedge b) \vee (x' \wedge b) = ((x \wedge b) \vee x') \wedge b = ((x \wedge b) \vee a \vee x') \wedge b =$
$= (((a \vee b) \wedge x) \vee x') \wedge b = (x' \vee x) \wedge (a \vee b) \wedge b = (x \vee x') \wedge b = f(x \vee x')$.
Tedy f je bijektivní homomorfismus, t.j. izomorfismus. $\square$

Definice: Nechť L je svaz s 0 a 1. Prvek $b \in L$ se nazývá *komplement* prvku $a \in L$, jestliže

$$a \vee b = 1 \qquad , \qquad a \wedge b = 0.$$

Svaz L s 0 a 1 se nazývá *komplementární*, má-li každý prvek aspoň jeden komplement.

Nechť L je svaz, $a, b \in L, a \leq b$. Nechť $c \in [a, b]$. Prvek $d \in [a, b]$ se nazývá *relativní komplement* prvku c v intervalu $[a, b]$, jestliže platí

$$c \vee d = b \qquad , \qquad c \wedge d = a.$$

Svaz L se nazývá *relativně komplementární*, má-li každý prvek $c \in [a, b]$ pro libovolné $a, b \in L, a \leq b$, aspoň jeden relativní komplement v $[a,b]$.

Je-li tedy L svaz s 0 a 1 relativně komplementární, je i komplementární, neboť $L = [0, 1]$ a komplement prvku $a \in L$ je tudíž relativní komplement prvku a v intervalu [0,1]. Existují však relativně komplementární svazy, které nemají 0 resp. 1.

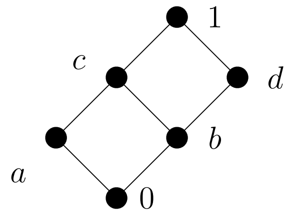
Příklady na komplementaritu:

(1) Nechť L je svaz s 0 a 1. Pak 0 je komplementem prvku 1, a obráceně 1 je komplementem prvku 0.

(2) Je-li ve svazu L prvek a komplementem prvku b, pak b je komplementem a; říkáme tedy, že a,b jsou (vzájemně) *komplementární.*

(3) Nechť C_n je n-prvkový řetězec, t.j. C_n obsahuje prvky
$0 < a_1 < a_2 < \ldots < a_{n-2} < 1$. Pak $0, 1$ jsou jediné prvky svazu C_n, které mají komplement.

(4) Ve svazu na obr.8 jsou a,d komplementární, 0,1 jsou komplementární, ale prvky b,c nemají komplementy.



Obr.8

(5) Ve svazu N_5 na obr.6 má prvek b dva komplementy, a to prvky a,c, prvek c má jediný komplement b, prvek a má rovněž jediný komplement b.

Ve svazu M_3 na obr.7 má a dva komplementy b,c, prvek b má dva komplementy a,c, prvek c má dva komplementy a,b.

(6) Ukažte, že ve svazu L na obr.5 má každý prvek právě jeden komplement.

O vztazích mezi komplementy a relativními komplementy, a o podmínce pro jednoznačnou komplementaci, vypovídají následující věty.

Věta 4.8. *Nechť L je distributivní svaz s 0 a 1. Pak každý prvek $a \in L$ má nejvýše jeden komplement.*

D ů k a z : Nechť $b, c \in L$ jsou komplementy prvku $a \in L$. Pak

$$b = b \wedge 1 = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = 0 \vee (b \wedge c) = b \wedge c,$$

$$c = c \wedge 1 = c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) = 0 \vee (c \wedge b) = b \wedge c,$$

tedy $b = c$.

□

Definice: Svaz L s 0 a 1 se nazývá *jednoznačně komplementární*, má-li každý prvek $a \in L$ právě jeden komplement.

V jednoznačně komplementárním svazu budeme komplement prvku x označovat symbolem x'.

Zřejmě tedy svaz L na obr.5 je jednoznačně komplementární.

Důsledek *Každý komplementární distributivní svaz je jednoznačně komplementární.*

Poznámka: Naskýtá se otázka, zda tento důsledek lze obrátit, t.j. zda platí tvrzení, že každý jednoznačně komplementární svaz je distributivní. Toto obrácené tvrzení obecně neplatí, což je ale obtížné dokázat; takový svaz totiž není konečný a jeho konstrukce je složitá (viz kniha [14], V.N.Salij).

Pro konečné svazy však lze dokázat obrácené tvrzení. Zaveďme následující pojmy:

Prvek a svazu L s 0 se nazývá *atom*, jestliže $0 < a$, a pro každé $x \in L$ splňující $0 < x \leq a$ platí $x = a$. Jinými slovy, atom je prvek, který kryje 0. Svaz L s 0 se nazývá *atomický*, jestliže pro každý prvek $b \in L$, $b \neq 0$ existuje atom $a \in L$ tak, že $a \leq b$.

Věta 4.9. *Každý jednoznačně komplementární atomický svaz je distributivní.*

Nástin důkazu: Nechť L je jednoznačně komplementární svaz. Označme A množinu všech atomů v L, a pro $x \in L$ označme $A(x)$ množinu všech atomů, které jsou $\leq x$. Snadno nahlédneme, že $x \leq y \Rightarrow \ A(x) \subseteq A(y)$. Předpokládejme, že $x \neq y$, avšak $A(x) = A(y)$. Nechť x' je komplement (jednoznačný) prvku x. Pak bude platit

$$A(0) = \emptyset \ = A(x) \cap A(x'),$$

$$A(1) = A = A(x) \cup A(x').$$

Je-li tedy $A(x) = A(y)$, plyne odtud, že také x' je komplement k y, t.j. $x' = y'$. Avšak $(x')' = x, (y')' = y$, tedy $x' = y' \Rightarrow \ x = y$, což je spor. Je tedy pro $x \neq y$ také $A(x) \neq A(y)$. Nechť $f : L \to A$ takové, že $f(x) = A(x)$. Pak, jak bylo výše ukázáné, f zachovává uspořádání a je bijekcí. Dle Věty 2.12. je f izomorfismus, t.j.

$$f(x \vee y) = A(x) \cup A(y),$$

$$f(x \wedge y) = A(x) \cap A(y).$$

Tedy f je izomorfismus $(L; \vee, \wedge)$ na $(Exp\, A, \cup, \cap)$. Ale, jak víme, svaz $(Exp\, A, \cup, \cap)$ je distributivní. □

Důsledek: *Každý konečný jednoznačně komplementární svaz je distributivní.*

Důkaz: Je-li L konečný svaz, $0 < x \in L$, pak buď x je atom, nebo existuje jen konečně mnoho prvků $z_1, \ldots, z_n$ tak, že $0 \prec z_1 \prec z_2 \prec \ldots \prec z_n \prec x$. Pak z_1 je atom. Tedy L je atomický a důsledek plyne ihned z Věty 4.9. □

Definice: Nechť L je jednoznačně komplementární svaz. Řekneme, že v L platí *De Morganovy zákony*, jestliže pro každé $x, y \in L$ platí

$$(x \vee y)' = x' \wedge y' \qquad \text{a} \qquad (x \wedge y)' = x' \vee y'.$$

Věta 4.10. *Nechť L je jednoznačně komplementární svaz. Pak je ekvivalentní*

(a) *pro každé* $x, y \in L$ *platí:* $x \le y \Rightarrow\ x' \ge y'$;
(b) *v* L *platí De Morganovy zákony.*

Důkaz: (a) $\Rightarrow$ (b): Nechť $x, y \in L$. Pak dle (a) platí:

$$x \le\ x \vee y \Rightarrow\ x' \ge\ (x \vee y)'$$

$$y \le\ x \vee y \Rightarrow\ y' \ge\ (x \vee y)'\ ,$$

tedy $x' \wedge y' \ge (x \vee y)'$.
Dále

$$\left.\begin{array}{l} x' \ge\ x' \wedge y' \Rightarrow\ x = (x')' \le\ (x' \wedge y')' \\ y' \ge\ x' \wedge y' \Rightarrow\ y = (y')' \le\ (x' \wedge y')' \end{array}\right\} \Rightarrow x \vee y \le (x' \wedge y')' \quad ,$$

což implikuje $(x \vee y)' \ge x' \wedge y'$. Dohromady tedy $x' \wedge y' = (x \vee y)'$. Duálně se dokáže druhý De Morganův zákon.
(b) $\Rightarrow$ (a): Nechť $x \le y$. Pak $y = x \vee y$, dle De Morganova zákona platí $y' = (x \vee y)' = x' \wedge y'$, tedy $y' \le x'$. □

Definice: Komplementární distributivní svaz nazveme *booleovský*.

Dle Věty 4.8. je tedy každý booleovský svaz jednoznačně komplementární. Dle Důsledku Věty 4.9. je každý *konečný* jednoznačně komplementární svaz booleovský. Platí tedy:

Důsledek: *Nechť* L *je konečný svaz. Pak je ekvivalentní:*
(a) L *je booleovský,*
(b) L *je jednoznačně komplementární.*

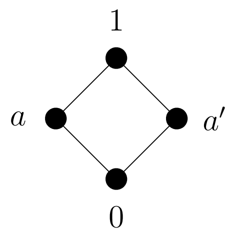
Věta 4.11. *V každém booleovském svazu platí De Morganovy zákony.*

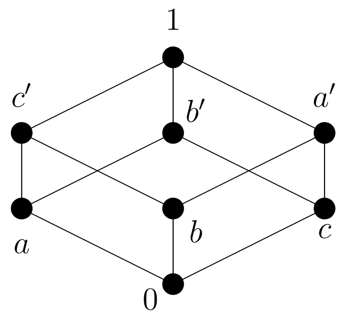
Důkaz: Nechť L je booleovský svaz. Dle Věty 4.8. je L jednoznačně komplementární. Nechť $a, b \in L, a \le b$. Pak

$$a \wedge b' = (a \wedge b) \wedge b' = a \wedge (b \wedge b') = a \wedge 0 =\ 0, \text{ tedy}$$
$$a' = 0 \vee a' = (a \wedge b') \vee a' = (a \vee a') \wedge (b' \vee a') = 1 \wedge (b' \vee a') = b' \vee a',$$

t.j. $a' \ge b'$. Dle Věty 4.10. platí v L De Morganovy zákony. □

Příklady booleovských svazů:
(1) Svaz $(Exp\, M, \cup, \cap)$ pro $M \neq \emptyset$, kde pro každou $X \subseteq M$ je $X' = M \backslash X$.
(2) Svazy na obr.9 a obr.10:





Obr.9 Obr.10

Nyní ukážeme souvislost komplementarity s relativní komplementaritou pro modulární svazy:

Věta 4.12. *Nechť L je komplementární modulární svaz. Pak L je relativně komplementární.*

D ů k a z : Nechť $x, y \in L$, $x < y$, $a \in [x, y]$. Nechť b je komplement prvku a v L. Položme

$$c = (y \wedge b) \vee x.$$

Z modularity a ze vztahu $x \leq y$ plyne $c = y \wedge (b \vee x)$, a dále

$$c \wedge a = [(x \vee b) \wedge y] \wedge a = (x \vee b) \wedge \underbrace{(y \wedge a)}_{= a} = (x \vee b) \wedge a = x \vee (b \wedge a) = x \vee 0 = x,$$

$$c \vee a = [(y \wedge b) \vee x] \vee a = (y \wedge b) \vee \underbrace{(x \vee a)}_{= a} = (y \wedge b) \vee a = y \wedge (b \vee a) = y \wedge 1 = y,$$

tedy c je relativní komplement prvku a v intervalu $[x,y]$. □

Poznámka: Jelikož každý distributivní svaz je dle Věty 4.3. modulární, dostáváme důsledek:

Každý booleovský svaz je relativně komplementární.

Nyní ukážeme, že pomocí relativních komplementů lze dokonce charakterizovat distributivitu a modularitu:

Věta 4.13. *Svaz L je distributivní tehdy a jen tehdy, když každý prvek $a \in L$ má v libovolném intervalu nejvýše jeden relativní komplement. Svaz L je modulární tehdy a jen tehdy, jestliže každý prvek $a \in L$ v libovolném intervalu nemá dva srovnatelné relativní komplementy.*

D ů k a z : Plyne ihned z Věty 4.6., neboť $a \in L$ má v některém $[x,y] \subseteq L$ dva relativní komplementy b,c, $b \neq c$, právě když $\{x,a,b,c,y\}$ tvoří podsvaz M_3; dále $b \in L$ má v $[x,y] \subseteq L$ dva srovnatelné relativní komplementy $a \leq c$, právě když $\{x,a,b,c,y\}$ tvoří N_5 (viz obr.6,7). □

5 KONGRUENCE A IDEÁLY NA SVAZECH

Ve 2.kapitole jsme definovali kongruenci na svazu a ve 3.kapitole jsme zavedli pojem svazového ideálu. Zajímáme se, zda existuje analogie vzájemného vztahu mezi ideálem a kongruencí, jaký je znám pro okruhy.

Definice: Nechť L je svaz s 0, nechť θ je kongruence na L. Množinu $K_\theta = \{x \in L; \langle x,0\rangle \in \theta\}$ nazveme *jádro kongruence θ*.

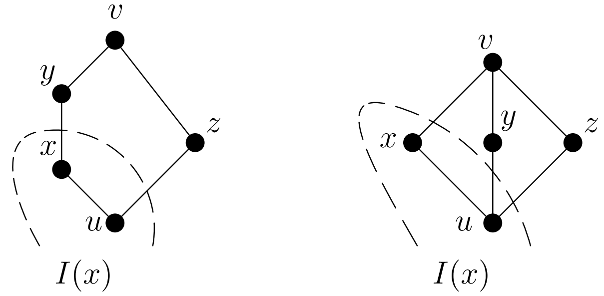
Věta 5.1. *Nechť L je svaz s 0 a θ je kongruence na L. Pak jádro K_θ je ideál svazu L.*

D ů k a z : Nechť $a,b \in K_\theta$. Pak $\langle a,0\rangle \in \theta$, $\langle b,0\rangle \in \theta$, tedy $\langle a \vee b, 0\rangle =$ $= \langle a \vee b, 0 \vee 0\rangle \in \theta$. Odtud $a \vee b \in K_\theta$. Nechť $a \in K_\theta, x \in L$. Pak $\langle a,0\rangle \in \theta$, avšak z reflexivity plyne $\langle x,x\rangle \in \theta$, tedy $\langle a \wedge x, 0\rangle = \langle a \wedge x, 0 \wedge x\rangle \in \theta$, t.j. $a \wedge x \in K_\theta$. Tedy K_θ je ideál svazu L. □

Poznámka:
(1) Je-li I ideál svazu L, $a \in I$ a $x \in L$, přičemž $x \leq a$, pak $x = a \wedge x \in I$.
(2) Je-li L svaz s 0 a $\theta = \omega$, pak $K_\theta = \{0\}$. je-li $\theta = L \times L$, pak $K_\theta = L$.

Věta 5.2. *Nechť L je svaz s 0. Pak je ekvivalentní:*
(1) *Každý ideál svazu L je jádrem aspoň jedné kongruence na L;*
(2) *L je distributivní.*

D ů k a z : (1) ⇒ (2): Nechť platí (1) a nechť L není distributivní. Dle Věty 4.6. L obsahuje aspoň jeden z podsvazů N_5, M_3, viz obr.11.



Obr.11

Předpokládejme, že ideál $I(x) = \{a \in L; a \leq x\}$ je jádrem některé kongruence θ na L. Pak $u \in I(x)$, $x \in I(x)$, tedy $\langle u, 0\rangle \in \theta$, $\langle x, 0\rangle \in \theta$, z tranzitivity relace θ dostaneme $\langle u, x\rangle \in \theta$. Jelikož θ je reflexivní, platí $\langle z, z\rangle \in \theta$, a tedy i $\langle x \vee z, u \vee z\rangle \in \theta$. Odtud $\langle y, u\rangle = \langle y \wedge (x \vee z)\, , \, y \wedge (u \vee z)\rangle \in \theta$, avšak $\langle u, 0\rangle \in \theta$, tedy z tranzitivity opět $\langle y, 0\rangle \in \theta$, t.j. $y \in K_\theta$. Avšak $y \notin I(x)$, tedy $I(x) \neq K_\theta$ – spor. Dokázali jsme (1) $\Rightarrow$ (2).

Dokážeme (2) $\Rightarrow$ (1): Nechť L je distributivní svaz s 0 a I je ideál svazu L. Definujme relaci θ na L takto:

$$\langle a, b\rangle \in \theta \text{ právě když } a \vee v = b \vee v \text{ pro některé } v \in I.$$

Pak platí

(a) θ je reflexivní, neboť pro každé $a \in L$ a pro každé $v \in I$ je $a \vee v = a \vee v$, t.j. $\langle a, a\rangle \in \theta$.

(b) Symetrie relace θ je zřejmá.

(c) Nechť $\langle a, b\rangle \in \theta$, $\langle b, c\rangle \in \theta$. Pak existují $v, w \in I$ tak, že $a \vee v = b \vee w$, $b \vee v = c \vee w$, avšak I je ideál, tedy $v \vee w \in I$, a tedy

$$a \vee v \vee w = b \vee v \vee w = c \vee v \vee w, \text{ odtud } \langle a, c\rangle \in \theta, \text{ t.j. } \theta \text{ je tranzitivní.}$$

(d) Nechť $\langle a, b\rangle \in \theta, \langle c, d\rangle \in \theta$. Pak $a \vee v = b \vee v$ a $c \vee w = d \vee w$ pro některé $v, w \in I$. Avšak $v \vee w \in I$, dále $a \vee c \vee (v \vee w) = b \vee d \vee (v \vee w)$, odtud $\langle a \vee c, b \vee d\rangle \in \theta$. Dále z distributivního zákona plyne

$$(a \vee v) \wedge (c \vee w) = [(a \vee v) \wedge c] \vee [(a \vee v) \wedge w] =$$
$$(a \wedge c) \vee (v \wedge c) \vee (a \wedge w) \vee (v \wedge w) \vee (v \wedge w) = (a \wedge c) \vee z$$
$$= w \wedge (a \vee v) \in I$$
$$= v \wedge (c \vee w) \in I$$

kde $z = [v \wedge (c \vee w)] \vee [w \wedge (a \vee v)] \in I$, neboť $w \wedge (a \vee v) \in I$ a $v \wedge (c \vee w) \in I$. Analogicky

$$(b \vee v) \wedge (d \vee w) = (b \wedge d) \vee (v \wedge d) \vee (b \wedge w) \vee (v \wedge w) \vee (v \wedge w)$$
$$= w \wedge (b \vee v)$$
$$= v \wedge (d \vee w)$$

Avšak $b \vee v = a \vee v$, $d \vee w = c \vee w$, tedy opět

$$(b \vee v) \wedge \ (d \vee w) = (b \wedge d) \vee z$$

pro totéž $z \in I$.

Odtud

$$(a \wedge c) \vee z = (a \vee v) \wedge (c \vee w) = (b \vee v) \wedge (d \vee w) = (b \wedge d) \vee z,$$

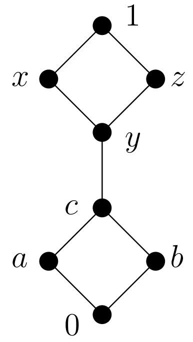
neboli

$$\langle a \wedge c, b \wedge d \rangle \in \theta.$$

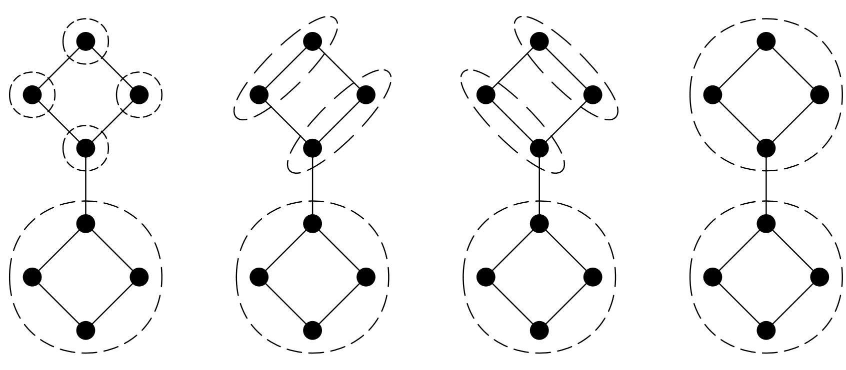
Dokázali jsme, že θ je kongruence na svazu L.

(e) Nechť $a \in K_\theta$. To je ekvivalentní s $\langle a, 0 \rangle \in \theta$, což je ekvivalentní s $a \vee v = 0 \vee v$ pro některé $v \in I$. Ale $0 \vee v = v$, t.j. $a \vee v = v$, neboli $a \leq v \in I$. Dle předchozí Poznámky platí $a \in I$, t.j. $K_\theta \subseteq I$. Obrácená inkluze je ale evidentní. Dokázali jsme $K_\theta = I$. Tedy ideál I je vskutku jádrem kongruence θ. $\square$

Příklad: Na rozdíl od okruhů, v distributivním svazu nemusí být ideál jádrem jediné kongruence. Je-li L svaz, jehož diagram je na obr.12, pak jeho ideál $I = \{0, a, b, c\}$ je jádrem 4 kongruencí, jejichž rozklady jsou na obr.13 :



Obr.12



Obr.13

Nyní budeme řešit problém, kdy je každý ideál jádrem nejvýše jedné kongruence.

Lemma 5.3. *Nechť θ je kongruence na svazu L a $x, y \in L$. Pak $\langle x, y\rangle \in \theta$, právě když $\langle x \wedge y, x \vee y\rangle \in \theta$.*

Důkaz: Nechť $\langle x, y\rangle \in \theta$. Pak

$$\left.\begin{array}{l}\langle x, x \wedge y\rangle = \langle x \wedge x, x \wedge y\rangle \in \theta \\ \langle y, x \wedge y\rangle = \langle y \wedge y, y \wedge x\rangle \in \theta\end{array}\right\} \overset{\vee}{\Rightarrow} \langle x \vee y, x \wedge y\rangle \in \theta.$$

Obráceně, nechť $\langle x \wedge y, x \vee y\rangle \in \theta$. Pak

$$\begin{array}{l}\langle x, x \wedge y\rangle = \langle x \wedge (x \vee y),\ x \wedge (x \wedge y)\rangle \in \theta, \\ \langle y, x \wedge y\rangle = \langle y \wedge (x \vee y),\ y \wedge (x \wedge y)\rangle \in \theta,\end{array}$$

z tranzitivity relace θ plyne $\langle x, y\rangle \in \theta$. □

Lemma 5.4. *Nechť L je relativně komplementární svaz s 0 a nechť θ je kongruence na L. Pak $\langle x, y\rangle \in \theta$, právě když každý relativní komplement prvku $x \wedge y$ v intervalu $[0, x \vee y]$ leží v K_θ.*

Důkaz: Nechť z je relativní komplement $x \wedge y$ v intervalu $[0, x \vee y]$. Jestliže $\langle x, y\rangle \in \theta$, pak dle Lemma 5.3.

$$\langle z, 0\rangle = \langle (x \vee y) \wedge z,\ (x \wedge y) \wedge z\rangle \in \theta,\ \text{tedy } z \in K_\theta.$$

Obráceně, nechť $z \in K_\theta$. Pak $\langle z, 0\rangle \in \theta$, tedy $\langle (x \wedge y) \vee z, (x \wedge y) \vee 0\rangle \in \theta$, ale z je relativní komplement prvku $x \wedge y$ v $[0, x \vee y]$, tedy $(x \wedge y) \vee z = x \vee y$, t.j. dostáváme $\langle x \vee y, x \wedge y\rangle \in \theta$. Dle Lemma 5.3. platí $\langle x, y\rangle \in \theta$. □

Věta 5.5. *Nechť L je relativně komplementární svaz s 0. Pak každý ideál svazu L je jádrem nejvýše jedné kongruence.*

Důkaz: Nechť I je ideál relativně komplementárního svazu L, a nechť I je jádrem kongruencí θ_1, θ_2, t.j. $K_{\theta_1} = K_{\theta_2}$. Dle Lemma 5.4.

$\langle x, y\rangle \in \theta_1$ právě když relativní komplement $x \wedge y$ v intervalu $[0, x \vee y]$ leží v K_{θ_1},

$\langle x, y\rangle \in \theta_2$ právě když relativní komplement $x \wedge y$ v intervalu $[0, x \vee y]$ leží v K_{θ_2}.

Ovšem $K_{\theta_1} = K_{\theta_2}$, tedy $\langle x, y\rangle \in \theta_1$ právě když $\langle x, y\rangle \in \theta_2$, t.j. $\theta_1 = \theta_2$. □

Věta 5.6. *Nechť L je distributivní svaz, $a, b, x, y \in L$ a nechť $a \le b$. Nechť θ je nejmenší kongruence obsahující $\langle a, b\rangle$. Pak $\langle x, y\rangle \in \theta$ právě když*

$$x \wedge a = y \wedge a \qquad , \qquad x \vee b = y \vee b\,. \tag{H}$$

D ů k a z : Nechť Φ je binární relace na L taková, že $\langle x, y\rangle \in \Phi$ právě když platí (H). Zřejmě Φ je ekvivalence na L. Nechť $\langle x, y\rangle \in \Phi$ a nechť $z \in L$. Pak

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

$$(x \vee z) \vee b = z \vee (x \vee b) = z \vee (y \vee b) = (y \vee z) \vee b\,,$$

tedy $\langle x \vee z, y \vee z\rangle \in \Phi$. Duálně se dokáže $\langle x \wedge z, y \wedge z\rangle \in \Phi$.

Nechť nyní $\langle x, y\rangle \in \Phi$, $\langle z, w\rangle \in \Phi$. Dle výše dokázaného tvrzení platí

$$\langle x \vee z, y \vee z\rangle \in \Phi \qquad , \qquad \langle y \vee z, y \vee w\rangle \in \Phi\,,$$

z tranzitivity plyne $\langle x \vee z, y \vee w\rangle \in \Phi$. Duálně se dokáže $\langle x \wedge z, y \wedge w\rangle \in \Phi$, tedy Φ je kongruence na L. Zřejmě $\langle a, b\rangle \in \Phi$, a tedy $\theta \subseteq \Phi$.

Nechť Ψ je libovolná kongruence na L taková, že $\langle a, b\rangle \in \Psi$. Nechť $\langle x, y\rangle \in \Phi$. Pak $x \wedge a = y \wedge a$, $x \vee b = y \vee b$, a dále $\langle x \vee a, x \vee b\rangle \in \Psi$, $\langle x \wedge b, x \wedge a\rangle \in \Psi$. Tedy
$x = x \vee (x \wedge a) = x \vee (y \wedge a) = [(x \vee y) \wedge (x \vee a)]\Psi\ [(x \vee y) \wedge (x \vee b)] =$
$= (x \vee y) \wedge (y \vee b) = [y \vee (x \wedge b)]\Psi\ [y \vee (x \wedge a)] = y \vee (y \wedge a) = y,$
t.j. $\langle x, y\rangle \in \Psi$. Odtud $\Phi \subseteq \Psi$, tedy Φ je nejmenší kongruence obsahující $\langle a, b\rangle$, t.j. $\Phi = \theta$. □

Následující věta charakterizuje svazy, pro které je analogie vztahu ideálů a kongruencí pro okruhy úplná:

Věta 5.7. *Nechť L je svaz s* 0. *Pak je ekvivalentní:*
(1) *Každý ideál svazu L je jádrem právě jedné kongruence na L.*
(2) *Svaz L je relativně komplementární distributivní svaz.*

D ů k a z : (2) $\Rightarrow$ (1) ihned dle Věty 5.2. a Věty 5.5.

Dokážeme (1) $\Rightarrow$ (2): Nechť každý ideál svazu L je jádrem právě jedné kongruence θ na L. Dle Věty 5.2. je L distributivní. Zbývá tedy dokázat, že L je relativně komplementární. Nechť $a, b \in L, a \leq b$. Nechť θ je nejmenší kongruence na L obsahující dvojici $\langle a, b\rangle$, a nechť $I = [0]_\theta$. Dle Věty 5.1. je I ideál v L.

Dle druhé části důkazu Věty 5.2. existuje prvek $w \in I$ tak, že $a \vee w = b \vee w$. Položme $v = b \wedge w$. Pak $v \leq b$, avšak $v = b \wedge w \in I$. Pak platí

$$a \vee v = a \vee (b \wedge w) = (a \vee b) \wedge (a \vee w) = b \wedge (a \vee w) = b \wedge (b \vee w) = b\,.$$

Tedy existuje prvek $v \in I$ splňující $a \vee v = b$. Jelikož $v \in I = [0]_\theta$, platí $\langle v, 0\rangle \in \theta$, a dle Věty 5.6. platí

$$v \vee b = 0 \vee b = b = a \vee v$$

$$v \wedge a = 0 \wedge a = 0\,,$$

tedy v je relativní komplement prvku a v intervalu $[0, b]$.

Jelikož a, b byly vybrány libovolně, plyne odtud, že $[0,b]$ je komplementární pro každé $b \in L$. Jelikož L je distributivní, je i podsvaz $[0,b]$ distributivní, tedy i modulární. Protože $[0,b]$ je modulární komplementární svaz, je dle Věty 4.12. relativně komplementární, t.j. pro každý prvek x jeho podsvazu $[a,b]$ existuje komplement x v $[a,b]$, neboli L je relativně komplementární. $\square$

6 BOOLEOVY ALGEBRY

Definice: Nechť $A \neq \emptyset$. *Booleovou algebrou* nazveme šestici $(A; \vee, \wedge,', 0, 1)$ takovou, že $0 \neq 1$ a

(i) $(A; \vee, \wedge)$ je distributivní svaz,

(ii) 0 resp. 1 je nejmenší resp. největší prvek tohoto svazu,

(iii) symbol $'$ označuje operaci komplementace, t.j. pro každé $a \in A$ je a' komplement prvku a ve svazu $(A; \vee, \wedge)$.

Je-li tedy A booleovský svaz, je-li 0 resp. 1 nejmenší resp. největší prvek tohoto svazu a' označuje komplementaci v A, pak $(A; \vee, \wedge,', 0, 1)$ je Booleova algebra. Konečnou Booleovu algebru lze tedy opět znázornit diagramem. Na obr.9 resp. 10 je diagram čtyřprvkové resp. osmiprvkové Booleovy algebry.

Příklady:

(1) Pro každou $M \neq \emptyset$ je $(Exp\ M; \cup, \cap, \setminus, \emptyset, M)$ Booleova algebra, přičemž symbol $\setminus$ označuje pro $X \subseteq M$ podmnožinu $M \setminus X$, t.j. komplement v množinovém svazu.

(2) Nechť $P(n)$ je množina všech dělitelů přirozeného čísla n, pak $(P(30); NSN, NSD, \frac{30}{x}, 1, 30)$ je Booleova algebra (viz obr.5), kde pro $x \in P(30)$ označuje $\frac{30}{x}$ aritmetický podíl.

(3) Každý dvouprvkový svaz (t.j. dvouprvkový řetězec) $(\{a, b\}, \vee, \wedge)$ lze chápat jako Booleovu algebru. Je-li $a < b$, pak tato Booleova algebra je $(\{a, b\}; \vee, \wedge,', a, b)$, kde $a' = b,\ b' = a,\ x \vee y = max\,(x, y),\ x \wedge y = min\,(x, y)$.

Definice: Nechť $\mathcal{A} = (A; \vee, \wedge,', 0, 1)$ je Booleova algebra, $\emptyset \neq B \subseteq A$. Jestliže pro každé $a, b \in B$ platí:

(i) $a \vee b \in B, a \wedge b \in B$

(ii) $a' \in B$

(iii) $0 \in B, 1 \in B$,

pak se B nazývá *podalgebra Booleovy algebry* $\mathcal{A}$.

Nechť $\mathcal{C} = (C; \vee, \wedge,', 0, 1)$ je také Booleova algebra a $h : A \to C$ je zobrazení splňující

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

$$h(a') = h(a)' \quad , \quad h(0) = 0 \quad , \quad h(1) = 1.$$

Pak h se nazývá *homomorfismus* Booleových algeber. Je-li h navíc bijekcí, nazývá se *izmorfismus*. Relace θ na Booleově algebře $\mathcal{A}$ je *kongruence*, je-li kongruencí na svazu $(A; \vee, \wedge)$, t.j. je-li ekvivalence, a pro každé $a, b, c, d \in \mathcal{A}$ platí:

Jestliže $\langle a, b\rangle \in \theta$, $\langle c, d\rangle \in \theta$, pak

$$\langle a \vee c, b \vee d\rangle \in \theta \quad , \quad \langle a \wedge c, b \wedge d\rangle \in \theta.$$

Poznámka: Nechť $\mathcal{A} = (L; \vee, \wedge, ', 0, 1)$ je Booleova algebra, a nechť θ je kongruence na svazu $(L; \vee, \wedge)$. Pak θ je kongruence na Booleově algebře $\mathcal{A}$. Nechť platí $\langle a, b\rangle \in \theta$. Pak z reflexivity θ plyne $\langle a', a'\rangle \in \theta$, $\langle b', b'\rangle \in \theta$, a tedy také

$$\begin{aligned} \langle a', a' \wedge b'\rangle &= \langle a' \wedge 1, a' \wedge (a \vee b')\rangle = \langle a' \wedge (b \vee b'), a' \wedge (a \vee b')\rangle \in \theta \\ \langle b', a' \wedge b'\rangle &= \langle b' \wedge 1, b' \wedge (b \vee a')\rangle = \langle b' \wedge (a \vee a'), b' \wedge (b \vee a')\rangle \in \theta, \end{aligned}$$

a ze symetrie a tranzitivity relace θ plyne $\langle a', b'\rangle \in \theta$. Neboli, každá kongruence svazu $(L; \wedge, \vee)$ má substituční podmínku i vzhledem k operaci komplementace. Proto nezavádíme nový pojem "booleovské kongruence".

Poznámka: Nechť L je booleovský svaz, nechť $\mathcal{A} = (L; \vee, \wedge, ', 0, 1)$ je odpovídající Booleova algebra. Pak každá podalgebra Booleovy algebry $\mathcal{A}$ je zřejmě podsvazem svazu L, avšak obrácené tvrzení neplatí. Je-li např. $L = \{0, a, a', 1\}$ svaz (viz obr.9), pak $(L; \vee, \wedge, ', 0, 1)$ je Booleova algebra. Pak $S = \{0, a, 1\}$ je podsvaz svazu L, avšak není podalgebrou Booleovy algebry $(L; \vee, \wedge, ', 0, 1)$, neboť $a' \notin S$. Také $A = \{0, a\}$ je podsvaz svazu L, ovšem není podalgebrou této Booleovy algebry, neboť $1 \notin A$.

Dále zobrazení $h : L \to L$ dané předpisem $h(1) = a$, $h(a') = 0$, $h(a) = a$, $h(0) = 0$ je svazový homomorfismus, ale není homomorfismem Booleových algeber, jelikož $h(1) \neq 1$, $h(a') = 0 \neq a' = h(a)'$.

Příklad: Nechť $\mathcal{A} = (A; \vee, \wedge, ', 0, 1)$ je Booleova algebra. Zaveďme na A binární operaci, označenou $|$, takto:

$$a|b = a' \wedge b'$$

Tato operace se nazývá Shefferova. Snadno ověříme, že Shefferova operace splňuje tyto axiomy:

$$(b|a)|(b'|a) = a \ , \ a|(b|c) = [(c'|a)|(b'|a)]', \qquad \text{(S)}$$

kde x' označuje pro stručnost $x|x$.

Obráceně, je-li $|$ binární operace na množině A splňující (S), pak $\mathcal{A}$ je Booleovou algebrou $(A; \vee, \wedge, ', 0, 1)$ vzhledem k operacím zavedeným takto:

$$a' = a|a \ , \ a \vee b = (a|b)|(a|b) \ , \ a \wedge b = (a|a)|(b|b) \ , \ 0 = a \wedge a' \ , \ 1 = a \vee a'$$

(pro již zavedené $\vee, \wedge, '$). Tento poznatek umožňuje použití jediného prvku pro konstrukci logických obvodů.

Věta 6.1. *Každá konečná Booleova algebra* $(L; \vee, \wedge, ', 0, 1)$ *je izomorfní s Booleovou algebrou* $(Exp\, M; \cup, \cap, \setminus, \emptyset, M)$, *kde* M *je množina všech atomů svazu* $(L; \vee, \wedge)$.

Důkaz: Nechť $\mathcal{A} = (L; \vee, \wedge, ', 0, 1)$ je konečná Booleova algebra a nechť M je množina atomů svazu $(L; \vee, \wedge)$. Pro každý prvek $a \in L$ označme $A(a) = \{p \in M;\ p \leq a\}$. Zřejmě platí $A(a \vee b) \supseteq A(a)$, $A(a \vee b) \supseteq A(b)$, tedy $A(a \vee b) \supseteq A(a) \cup A(b)$. Obráceně, nechť $c \in A(a \vee b)$. Pak $c = c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b)$. Jelikož c je atom, plyne odtud $c = c \wedge a$ nebo $c = c \wedge b$, t.j. $c \leq a$ nebo $c \leq b$, odtud $c \in A(a)$ nebo $c \in A(b)$, a tedy $c \in A(a) \cup A(b)$. Dokázali jsme $A(a \vee b) \subseteq A(a) \cup A(b)$. Dohromady $A(a \vee b) = A(a) \cup A(b)$. Rovnost $A(a \wedge b) = A(a) \cap A(b)$ vyplývá ihned z faktu, že $c \leq a \wedge b$ právě když $c \leq a$ a současně $c \leq b$. Dokázali jsme tedy, že zobrazení $L \to Exp\, M$ dané předpisem $a \to A(a)$ je homomorfismus.

Jestliže $a, b \in L$ a platí $A(a) = A(b)$, pak vzhledem ke konečnosti množin $A(a)$, $A(b)$ platí $a = \vee A(a)$, $b = \vee A(b)$, tedy $a = \vee A(a) = \vee A(b) = b$, t.j. zobrazení $a \to A(a)$ je injektivní homomorfismus. Zbývá dokázat, že toto zobrazení je surjekce. Nechť $B \subseteq M$. Jelikož B je konečná, existuje $b = \vee B$, tedy B jsou všechny atomy $\leq b$, tedy $B = A(b)$, neboli $b \to B$. Dokázali jsme, že toto zobrazení je hledaný izomorfismus. $\square$

Důsledek:

(1) *Nechť* $\mathcal{A}$ *je konečná Booleova algebra. Pak existuje přirozené číslo* n *tak, že* $\mathcal{A}$ *má* 2^n *prvků.*

(2) *Jsou-li* $\mathcal{A}, \mathcal{B}$ *dvě konečné Booleovy algebry se stejným počtem prvků, pak jsou izomorfní.*

Důkaz:

(1) Je-li $\mathcal{A}$ konečná, pak je dle Věty 6.1. izomorfní s $(Exp\ M; \cup, \cap, \setminus, ', \emptyset, M)$, kde M je množina atomů Booleovy algebry $\mathcal{A}$. Jelikož $\mathcal{A}$ je konečná, je i M konečná; nechť $|M| = n$. Pak $|Exp\, M| = 2^n$, tudíž i $\mathcal{A}$ má 2^n prvků.

(2) Mají-li konečné Booleovy algebry $\mathcal{A}, \mathcal{B}$ stejný počet prvků, např. 2^n, pak $\mathcal{A} \cong (Exp\, M; \cup, \cap, ', \emptyset, M)$, $\mathcal{B} \cong (Exp\, M; \cup, \cap, ', \emptyset, M)$, kde M je n-prvková množina, a tedy i $\mathcal{A} \cong \mathcal{B}$. $\square$

Poznámka: Booleova algebra $\mathcal{A} = (A; \vee, \wedge, ', 0, 1)$ se nazývá *úplná* (*atomická*), je-li svaz $(A; \vee, \wedge)$ úplný (atomický). Analogicky jako ve Větě 6.1. lze dokázat:

Věta 6.2. *Každá úplná a atomická Booleova algebra $\mathcal{A}$ je izomorfní s Booleovou algebrou $(Exp\, M; \cup, \cap, ', \emptyset, M)$, kde M je množina atomů v A.*

Věta 6.3. *Nechť $\mathcal{A}$ je konečná Booleova algebra, která má 2^n prvků. Pak $\mathcal{A}$ je izomorfní s Booleovou algebrou $\mathcal{B}$ všech n-tic $(a_1, \ldots, a_n)$, kde $a_i \in \{0, 1\}$, přičemž nulou je v $\mathcal{B}$ prvek $o = (0, \ldots, 0)$, jednotkou je prvek $j = (1, \ldots, 1)$, komplementem $a = (a_1, \ldots, a_n)$ je prvek $a' = (a'_1, \ldots, a'_n)$, kde $0' = 1$, $1' = 0$ a operace $\vee, \wedge$ jsou v B definovány takto:*

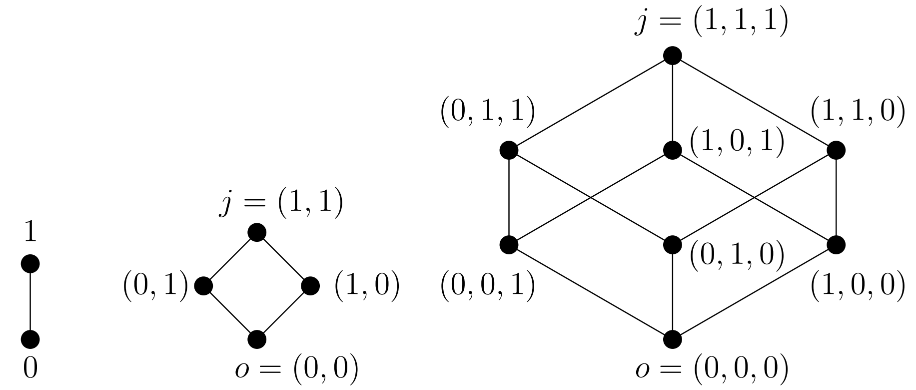
$$(a_1, \ldots, a_n) \vee (b_1, \ldots, b_n) = (a_1 \vee b_1, \ldots, a_n \vee b_n)$$

$$(a_1, \ldots, a_n) \wedge (b_1, \ldots, b_n) = (a_1 \wedge b_1, \ldots, a_n \wedge b_n).$$

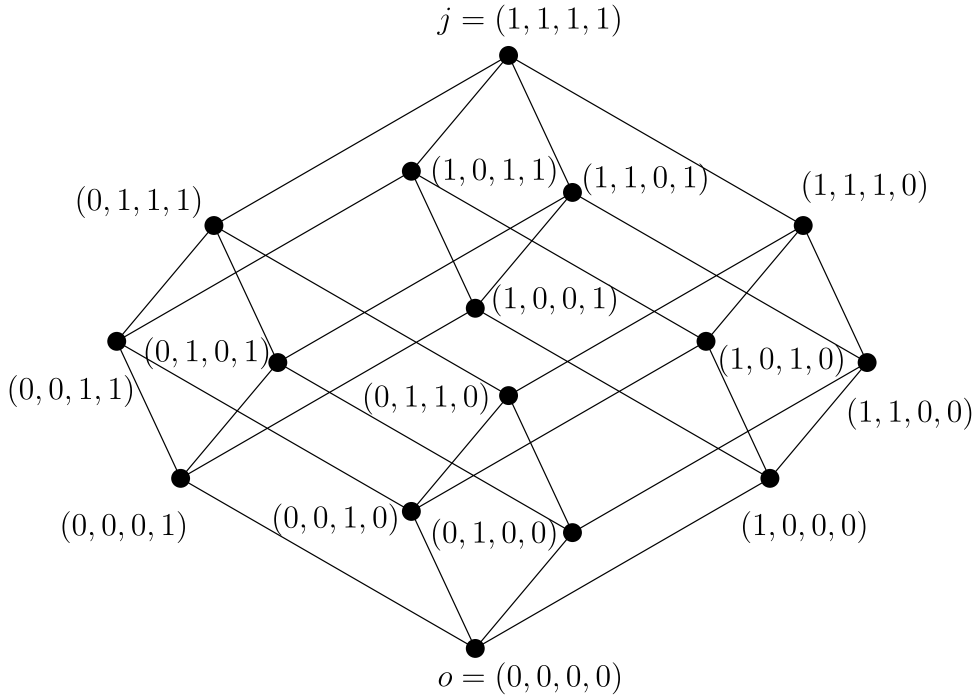
Důkaz: Nechť L je množina všech n-tic $(a_1, \ldots, a_n)$, jejichž prvky jsou 0 a 1. Zřejmě $|L| = 2^n$. Snadno ověříme, že $\mathcal{B} = (L; \vee, \wedge, ', o, j)$ je Booleova algebra. Jelikož $\mathcal{A}, \mathcal{B}$ mají stejný počet prvků, jsou dle předchozího Důsledku izomorfní. $\square$

Poznámka: Z předchozího výkladu je tedy zřejmé, že nejmenší Booleova algebra má právě dva prvky, a to 0 a 1. Pak platí $0' = 1$, $1' = 0$, $0 \vee 0 = 0$, $1 \vee 0 = 0 \vee 1 = 1 \vee 1 = 1$, $0 \wedge 1 = 1 \wedge 0 = 0$. Tato Booleova algebra je zřejmě izomorfní s Booleovou algebrou pravdivostních hodnot výrokové logiky, kde 1 je pravdivostní hodnota pravdivého výroku, 0 je pravdivostní hodnota nepravdivého výroku a operace $\vee$ resp. $\wedge$ lze interpretovat jako disjunkci resp. konjunkci, operaci $'$ jako negaci. Jsou-li $A_1, \ldots, A_n$ výroky, pro které chceme zjistit pravdivostní hodnotu některé logické funkce těchto výroků, pak, jak známe z výrokové logiky, interpretujeme jejich pravdivostní hodnoty pomocí m n-tic 0 a 1 (kde $m = 2^n$). Jelikož dle Věty 6.3. je množina všech těchto n-tic Booleovou algebrou (která má 2^n prvků), lze dle Věty 6.3. operace $\vee, \wedge$ interpretovat jako disjunkci a konjunkci (neboť jsou dle Věty 6.3. prováděny po souřadnicích a dle výše uvedeného lze tyto interpretovat v každé souřadnici jako disjunkci a konjunkci), komplement $'$ lze interpretovat jako negaci, tedy na logické operace s konečnou množinou výroků lze nahlížet jako na konečnou Booleovu algebru. To byla původní myšlenka, se kterou přišel v r.1847 George Boole při výzkumu formalizace matematické logiky.

Na obr.14 a 15 jsou znázorněny příslušné booleovské svazy, odpovídající Booleovým algebrám s 2, 4, 8 a 16 prvky (označení prvků dle Věty 6.3.):



Obr.14



Obr.15

Věta 6.4. *Nechť* $\mathcal{A} = (L; \vee, \wedge, ', 0, 1)$ *je Booleova algebra. Zaveďme operaci* $\oplus$ *na* L *takto:*

$$x \oplus y = (x \wedge y') \vee (x' \wedge y).$$

Pak $(L; \oplus)$ *je abelovská grupa.*

Důkaz: Z definice je zřejmé, že operace $\oplus$ je komutativní. Snadno se dokáže asociativita operace $\oplus$. Pro každé $x \in L$ je $x \oplus 0 = (x \wedge 0') \vee (x' \wedge 0) = x \wedge 1 = x$, tedy 0 je jednotkou v $(L; \oplus)$. Dále pro každé $x \in L$ je $x \oplus x = (x \wedge x') \vee (x' \wedge x) = 0 \vee 0 = 0$, tedy x je inversní prvek k sobě samému. Dokázali jsme, že $(L; \oplus)$ je abelovská grupa. □

Poznámka: Je-li $\mathcal{A} = (L; \vee, \wedge, ', 0, 1)$ Booleova algebra, pak je tedy
(i) $(L; \vee, \wedge)$ distributivní svaz,
(ii) $(L; \oplus)$ abelovská grupa.
Booleovy algebry jsou tedy takové algebraické struktury, které sjednocují vlastnosti (distributivních) svazů a (abelovských) grup.

Další zajímavý vztah Booleových algeber k okruhům objasníme v dalším výkladu.

Definice: Okruh R s alespoň dvěma prvky, jehož každý prvek je idempotentní (t.j. pro každé $a \in R$ platí $a \cdot a = a$), se nazývá *booleovský*.

Věta 6.5. *Každý booleovský okruh je komutativní a má charakteristiku rovnu* 2.

Důkaz: Nechť $(R; +, \cdot)$ je booleovský okruh. Pak pro každé $x, y \in R$ platí $x + y = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + xy + yx + y$, tedy $xy + yx = 0$. Položme $x = y$ a dostaneme $0 = x^2 + x^2 = x + x$, tedy R je charakteristiky 2. Dále, jestliže jsme dokázali $xy + yx = 0$ pro každé $x, y \in R$, pak

$$xy = xy + 0 = xy + xy + yx = 0 + yx = yx,$$

neboť R je charakteristiky 2, tedy R je komutativní. □

Příklad: Dvouprvkový booleovský okruh je okruh zbytkových tříd *mod* 2.

Věta 6.6. *Nechť* $\mathcal{A} = (L; \vee, \wedge, ', 0, 1)$ *je Booleova algebra. Definujme*

$$x \oplus y = (x \wedge y') \vee (x' \wedge y) \ , \ x \cdot y = x \wedge y.$$

Pak $\mathcal{R} = (L; \oplus, \cdot)$ *je booleovský okruh s jednotkou* 1.

Důkaz: Dle Věty 6.4. je $(L; \oplus)$ abelovská grupa. Operace $\cdot$ je zřejmě asociativní, neboť $\wedge$ je asociativní. Z distributivních zákonů pro operace $\vee, \wedge$ snadno odvodíme distributivní zákon $x \cdot (y \oplus z) = (x \cdot y) \oplus (x \cdot z)$. Tedy $\mathcal{R} = (L; \oplus, \cdot)$ je okruh. Jelikož pro každé $x \in L$ je $x \cdot x = x \wedge x = x$, je $\mathcal{R}$ booleovský okruh. Dále, $1 \cdot x = x \cdot 1 = x \wedge 1 = x$, tedy 1 je jednotkou v $\mathcal{R}$. □

Věta 6.7. *Nechť* $\mathcal{R} = (A; +, \cdot)$ *je booleovský okruh s* 1. *Definujme*

$$x \vee y = x + y + x \cdot y \quad , \quad x \wedge y = x \cdot y \quad , \quad x' = 1 + x\,.$$

Pak $\mathcal{A} = (A; \vee, \wedge, ', 0, 1)$, *kde* 0 *je nulou okruhu* $\mathcal{R}$, *je Booleova algebra.*

D ů k a z : Z komutativity a asociativity operací $+, \cdot$ lze odvodit asociativitu a komutativitu operací $\vee, \wedge$. Dále,

$$x \vee (x \wedge y) = x + xy + x^2y = x + xy + xy = x,$$

$$x \wedge (x \vee y) = x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x,$$

tedy $(A; \vee, \wedge)$ je svaz. Dále,

$$0 \vee x = 0 + x + 0 \cdot x = x \quad , \quad 0 \wedge x = 0 \cdot x = 0,$$

$$1 \vee x = 1 + x + 1 \cdot x = 1 + x + x = 1 \quad , \quad 1 \wedge x = 1 \cdot x = x.$$

Konečně

$$x \wedge x' = x(1 + x) = x + x^2 = x + x = 0,$$

$$x \vee x' = x + (1 + x) + x(1 + x) = x + 1 + x + 0 = 1,$$

tedy x' je komplement prvku x. Ověříme distributivitu svazu $(A; \vee, \wedge)$:

$$(x \wedge y) \vee (x \wedge z) = xy + xz + xyxz = xy + xz + xyz = x(y + z + yz) = x \wedge (y \vee z).$$

Tedy $(A; \vee, \wedge, ', 0, 1)$ je Booleova algebra. □

Poznámka: Je-li $\mathcal{R}$ booleovský okruh bez 1, pak konstrukcí operací $\vee, \wedge, '$ z Věty 6.7. obdržíme relativně komplementární distrubutivní svaz, tzv. *zobecněnou Booleovu algebru*. Obráceně, je-li L relativně komplementární svaz, pak konstrukcí podobnou jako ve Větě 6.6. obdržíme Booleovský okruh (bez 1).

Věta 6.8. *Nechť* $(L; \vee, \wedge)$ *je relativně komplementární distributivní svaz, nechť* $a, b \in L$, $a < b$. *Pak*

$$I(a, b) = ([a, b]; \vee, \wedge, ^*, a, b)$$

je Booleova algebra, kde symbol * *označuje relativní komplement v intervalu* $[a, b]$.

D ů k a z : Nechť $(L; \vee, \wedge)$ je relativně komplementární distributivní svaz, $a < b$, $a, b \in L$. Uvažujme interval $[a,b]$. Pak $[a,b]$ je podsvaz svazu $(L; \vee, \wedge)$, přičemž a je nejmenší a b je největší prvek v $[a,b]$. Pro $x \in [a, b]$ označme x^* relativní komplement prvku x v intervalu $[a,b]$. Jelikož L je distributivní, je i $[a,b]$ distributivní svaz, tedy komplementace je dle Věty 4.13. jednoznačná. Tedy $([a, b]; \vee, \wedge)$ je booleovský svaz, t.j. $I([a, b]) = ([a, b]; \vee, \wedge, ^*, a, b)$ je Booleova algebra. □

Definice: Nechť $\{x_1, \ldots, x_n\}$ je množina symbolů. *Booleovským termem v proměnných* $x_1, \ldots, x_n$ nazveme:
(i) každý prvek x_i ($i \in \{1, 2, \ldots, n\}$);
(ii) prvky 0 a 1;
(iii) jsou-li p, q booleovské termy, pak $p \vee q$, $p \wedge q$, p' jsou opět booleovské termy;
(iv) každý booleovský term vznikl konečným počtem kroků (i), (ii), (iii).

Příklad: Booleovské termy jsou tedy např. $(x_1 \vee x_2')' \wedge x_3$ nebo $(x_1 \wedge x_2' \wedge x_3) \vee (x_2 \wedge x_3')$ atd.

Elementární konjunkcí nazveme každý booleovský term tvaru

$$x_1^* \wedge x_2^* \wedge \ldots \wedge x_n^* \quad ,$$

kde pro každé $i \in \{1, 2, \ldots, n\}$ je buď $x_i^* = x_i$, nebo $x_i^* = x_i'$.

Snadno ověříme, že množina všech booleovských termů v proměnných $x_1, \ldots, x_n$ tvoří Booleovu algebru. Proto budeme s booleovskými termy pracovat analogicky jako s prvky Booleovy algebry, t.j. pro operace $\vee, \wedge$ budou platit všechny svazové identity, budeme používat distributivního zákona, De Morganových zákonů a pravidel $p \wedge p' = 0$, $p \vee p' = 1$ pro každý booleovský term p.

Disjunktní normální formou (ve zkratce *DNF*) nazveme booleovský term tvaru $p_1 \vee \ldots \vee p_k$ kde p_i, jsou elementární konjunkce.

Příklad: Nechť $\{x_1, x_2, x_3\}$ je množina symbolů. Elementární konjunkce v proměnných x_1, x_2, x_3 jsou např. $x_1' \wedge x_2' \wedge x_3'$ nebo $x_1 \wedge x_2' \wedge x_3$ nebo $x_1 \wedge x_2 \wedge x_3$ nebo $x_1' \wedge x_2' \wedge x_3$ atd.

Disjunktní normální formou v proměnných x_1, x_2, x_3 je např. term:

$$(x_1 \wedge x_2' \wedge x_3') \vee \ (x_1 \wedge x_2 \wedge x_3') \vee \ (x_1 \wedge x_2 \wedge x_3)$$

nebo

$$(x_1 \wedge x_2 \wedge x_3) \vee \ (x_1' \wedge x_2 \wedge x_3) \vee \ (x_1 \wedge x_2' \wedge x_3') \vee \ (x_1' \wedge x_2' \wedge x_3').$$

Věta 6.9. *Každý booleovský term lze vyjádřit* (*jednoznačně*) *ve tvaru disjunktní normální formy.*

Důkaz: Je-li booleovský term $p = 0$, pak je disjunktní normální forma spojením nulového počtu elementárních konjunkcí. Je-li $p = 1$, pak je *DNF* spojením všech (t.j. 2^n) elementárních konjunkcí. Nechť $p \neq 0$, $p \neq 1$. Pak postupně provádíme tyto úpravy termu p:

(1) Je-li operace komplementu vně závorky, používáme De Morganovy zákony: $(q \vee r)' = q' \wedge p'$, $(q \wedge r)' = q' \vee r'$. Tato úprava umožní, že operace komplementu je nakonec jen u proměnných $x_1, \ldots, x_n$.

(2) Opakovaně používáme distributivního zákona, až term p je ve tvaru $q_1 \vee q_2 \vee \ldots \vee q_k$, kde $q_1, \ldots, q_k$ již neobsahuje operaci $\vee$.

(3) Upravíme q_i na elementární konjunkce takto:

– jestliže q_i obsahuje x_j i x'_j, pak q_i vynecháme, neboť

$$x_j \wedge x'_j = 0 \Rightarrow \; q_i = 0;$$

– jestliže q_i neobsahuje ani x_j , ani x'_j , pak místo q_i píšeme $q_i^{(1)} \vee q_i^{(2)}$, kde $q_i^{(1)} = q_i \wedge x_j$, $q_i^{(2)} = q_i \wedge x'_j$. Z distributivního zákona totiž plyne $q_i^{(1)} \vee q_i^{(2)} = (q_i \wedge x_j) \vee (q_i \wedge x'_j) = q_i \wedge (x_j \vee x'_j) = q_i \wedge 1 = q_i$, tedy hodnota p se ani touto úpravou nezmění. Takto postupně nahradíme všechny q_i elementárními konjunkcemi, a tedy p bude ve tvaru *DNF.* $\square$

Příklad: Proceduru úpravy booleovského termu na *DNF*, jak byla popsána v důkazu Věty 6.8. si můžeme ilustrovat na následujícím příkladu: nechť $p = (x_1 \vee x_2) \wedge (x'_3 \wedge x_2)'$ je booleovský term v proměnných x_1, x_2, x_3. Dle (1) upravíme p na tvar:

$$p = (x_1 \vee x_2) \wedge (x_3 \vee x'_2)$$

Nyní opakovaně použijeme distributivní zákon, t.j. (2):

$$p = [x_1 \wedge (x_3 \vee x'_2)] \vee [x_2 \wedge (x_3 \vee x'_2)] = (x_1 \wedge x_3) \vee (x_1 \wedge x'_2) \vee (x_2 \wedge x_3) \vee (x_2 \wedge x'_2)$$

Dle (3) můžeme vynechat $x_2 \wedge x'_2$ (neboť $= 0$), tedy

$$p = (x_1 \wedge x_3) \vee (x_1 \wedge x'_2) \vee (x_2 \wedge x_3)$$

Jelikož žádná z konjunkcí neobsahuje všechny proměnné, musíme dle (3) rozšířit výrazy takto:

$$\begin{array}{lll} \text{místo } (x_1 \wedge x_3) & \text{doplníme} & (x_1 \wedge x_3 \wedge x_2) \vee (x_1 \wedge x_3 \wedge x'_2) \\ \text{místo } (x_1 \wedge x'_2) & \text{doplníme} & (x_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x'_2 \wedge x'_3) \\ \text{místo } (x_2 \wedge x_3) & \text{doplníme} & (x_2 \wedge x_3 \wedge x_1) \vee (x_2 \wedge x_3 \wedge x'_1); \end{array}$$

Pak $p = (x_1 \wedge x_3 \wedge x_2) \vee (x_1 \wedge x_3 \wedge x'_2) \vee (x_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x'_2 \wedge x'_3) \vee (x_2 \wedge x_3 \wedge x_1) \vee (x_2 \wedge x_3 \wedge x'_1)$.

Nyní je již p ve tvaru disjunkce elementárních konjunkcí, ovšem druhá a třetí elementární konjunkce se sobě rovnají, dle idempotence lze jednu vynechat. Také první a pátá se rovnají, jednu z nich vynecháme. Výsledná *DNF* termu p je tedy (po seřazení proměnných dle indexů):

$$p = (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2' \wedge x_3) \vee (x_1 \wedge x_2' \wedge x') \vee (x_1' \wedge x_2 \wedge x_3).$$

□

Dodatek

V tomto dodatku budeme blíže zkoumat ideály zejména na distributivních svazech. Jak bylo dokázáno v Lemmatu 3.4., je-li L svaz, $a \in L$, pak množina $I(a) = \{x \in L; x \leq a\}$ je ideál. Tyto ideály $I(a)$ pro $a \in L$ budeme nazývat *hlavní*. Zřejmě platí, že je-li L konečný svaz, je každý jeho ideál hlavní (viz Poznámka za Větou 3.5.). Zavedeme další významné druhy svazových ideálů.

Definice: Ideál I svazu L nazveme *prvoideál*, jestliže pro každé $a, b \in L$ platí implikace:

$$a \wedge b \in I \Rightarrow a \in I \text{ nebo } b \in I.$$

Jak bylo dokázáno ve Větě 3.3., je pro každý svaz L množina všech jeho ideálů spolu s $\emptyset$ úplným svazem (vzhledem k uspořádání množinovou inkluzí). Lze proto definovat:

Definice: Ideál I svazu L se nazývá maximální, jestliže $I \neq L$, a je-li J ideál svazu L, $J \neq I$ a platí-li $I \subseteq J \subseteq L$, pak $J = L$.

Ideál I svazu L nazveme *vlastní*, je-li $I \neq L$.

Snadno dokážeme

Lemma D.1. *Nechť L je svaz s 0 a 1, I je vlastní ideál svazu L, $a \in L$. Nechť b je komplement prvku a. Jestliže $a \in I$, pak $b \notin I$.*

D ů k a z: Jestliže $a \in I$ a také $b \in I$, pak také platí $a \vee b \in I$. Ale b je komplement prvku a, tedy $a \vee b = 1$, t.j. $1 \in I$. Zřejmě odtud plyne $I(1) \subseteq I$. Avšak $I(1) = L$, tedy $I = L$, spor. □

Zavedeme další pojem, duální k pojmu ideál:

Definice: Nechť L je svaz, $\emptyset \neq F \subseteq L$. Množinu F nazveme *filtr svazu* L, jestliže pro každé $a, b \in F$ a libovolné $x \in L$ platí: $a \wedge b \in F$, $a \vee x \in F$.

Analogicky jako pro ideály lze dokázat, že množina všech filtrů svazu L spolu s $\emptyset$ tvoří úplný svaz.

Lemma D.2. *Nechť L je svaz, I jeho ideál. Pak I je prvoideál právě když $L \setminus I$ je filtr.*

D ů k a z : Nechť $L \setminus I$ je filtr. Nechť $a \wedge b \in I$ a předpokládejme $a \notin I$, $b \notin I$. Pak $a \in L \setminus I$, spor. Odtud $a \in I$, nebo $b \in I$, t.j. I je prvoideál.

Obráceně, nechť I je prvoideál, nechť $c, d \in L \setminus I$, $x \in L$. Jestliže $c \wedge d \in I$, pak $c \in I$ nebo $d \in I$, což je spor. Tedy $c \wedge d \in L \setminus I$. Jestliže $c \vee x \in I$, pak (dle Poznámky za V.5.1.) také $c \leq c \vee x \Rightarrow c \in I$, opět spor. Tedy $c \vee x \in L \setminus I$, t.j. $L \setminus I$ je filtr. □

Filtr F svazu L nazveme *vlastní*, je-li $F \neq L$. Filtr U svazu L nazveme *ultrafiltr*, je-li maximální, t.j. jestliže U je vlastní, a pro každý filtr $F \neq U$ takový, že $U \subseteq F$ platí $F = L$.

Následující tvrzení udávají vztah mezi prvoideály a maximálními ideály.

Věta D.1. *Nechť L je distributivní svaz. Pak každý jeho maximální ideál je prvoideál.*

D ů k a z : Nechť M je maximální ideál svazu L. Nechť $x, y \in L$ a platí $x \wedge y \in M$. Nechť $x \notin M$. Pak ve svazu $\mathcal{J}$ všech ideálů na L je ideál $I(x) \vee M$ větší než M, ale M je maximální, tedy $I(x) \vee M = L$. Tedy $y \in I(x) \vee M$, t.j. $y \leq x \vee m$ pro některé $m \in M$. Z distributivity plyne $y = y \wedge (x \vee m) = (y \wedge x) \vee (y \wedge m)$. Ale $y \wedge x \in M$, $y \wedge m \in M$, tedy $y \in M$, t.j. M je prvoideál. □

Pro booleovské svazy lze dokázat i obrácené tvrzení:

Věta D.2. *Nechť L je booleovský svaz, I jeho ideál. Pak I je maximální právě když je prvoideál.*

D ů k a z : Nechť I je prvoideál svazu L. Nechť $a \notin I$. Dle Lemma D.1. platí $a' \in I$. Nechť J je ideál svazu L a platí $I \subseteq J$, $I \neq J$. Pak existuje $a \in J$, $a \notin I$. Ale $a' \in I \subseteq J$, tedy $1 = a \vee a' \in J$, t.j. $J = I(1) = L$. Neboli, I je maximální ideál.
Obrácené tvrzení plyne z Věty D.1. □

Věta D.3. *Nechť L je distributivní svaz. Nechť I je ideál a F filtr svazu L, a platí $I \cap F = \emptyset$. Pak existuje prvoideál P tak, že $I \subseteq P$ a $P \cap F = \emptyset$.*

D ů k a z : Nechť $\mathcal{S}$ je množina všech ideálů svazu L obsahujících I a disjunktních s F. Jelikož $I \in \mathcal{S}$, je $\mathcal{S} \neq \emptyset$. Nechť $\mathcal{C}$ je libovolný řetězec ideálů v $\mathcal{S}$ a nechť $M = \bigcup\{J; J \in \mathcal{C}\}$. Jestliže $a, b \in M$, pak $a \in J_1$, $b \in J_2$ pro některé $J_1, J_2 \in \mathcal{C}$. Jelikož $\mathcal{C}$ je řetězec, je buď $J_1 \subseteq J_2$ nebo $J_2 \subseteq J_1$. Předpokládejme tedy $J_1 \subseteq J_2$. Pak $a, b \in J_2$, a tedy $a \vee b \in J_2 \subseteq M$. Je-li $x \leq a$, pak $x \in J_2 \subseteq M$, tedy M je ideál svazu L. Zřejmě $M \cap F = \emptyset$, $I \subseteq M$. Odtud $M \in \mathcal{S}$. Podle Zornova Lemmatu (ekvivalentní s Axiomem výběru) existuje maximální prvek P v $\mathcal{S}$. Ukážeme, že P je prvoideál. Sporem: nechť $a \wedge b \in P$, ale $a \notin P$, $b \notin P$. Z maximality P plyne $(P \vee I(a)) \cap F \neq \emptyset$ a $(P \vee I(b)) \cap F \neq \emptyset$. Tedy existují $p, q \in P$ tak, že $p \vee a \in F$, $q \vee b \in F$. Odtud $x = (p \vee a) \wedge (q \vee b) \in F$ (jelikož F je filtr). Dále $x = (p \wedge q) \vee (p \wedge b) \vee (a \wedge q) \vee (a \wedge b) \in P$, odtud $P \cap F \neq \emptyset$, spor. □

Důsledek. *Nechť L je distributivní svaz, $a, b \in L$, $a \neq b$. Pak existuje prvoideál P obsahující a a neobsahující b.*

D ů k a z : Stačí uvažovat $I = I(a)$ a $F = F(b)$, t.j. hlavní filtr generovaný prvkem b. Aplikací Věty D.3. dostaneme tvrzení. □

Poznámka. Platí také věta obrácená k předchozímu důsledku. Jestliže totiž L není distributivní, obsahuje podsvaz N_5 nebo M_3, a lze snadno ukázat, že pak existují $a, b \in L$, $a \neq b$, které nelze "oddělit prvoideálem".

Definice. Nechť $A \neq \emptyset$. Podmnožina $\mathcal{S} \subseteq Exp\, A$ se nazývá *množinový okruh*, jestliže pro každé $X, Y \in \mathcal{S}$ také $X \cup Y \in \mathcal{S}$, $X \cap Y \in \mathcal{S}$. Množinový okruh $\mathcal{S}$ se nazývá *množinové těleso*, jestliže také pro každou $X \in \mathcal{S}$ platí $A \setminus X \in \mathcal{S}$.

Zřejmě každý množinový okruh je distributivní svaz a každé množinové těleso je booleovský svaz. Platí však také obrácené tvrzení, tedy:

Věta D.4. *Svaz L je distributivní tehdy a jen tehdy, když je izomorfní některému množinovému okruhu.*

Nástin důkazu. Nechť L je distributivní svaz, nechť $\mathcal{T}$ je množina jeho prvoideálů. Pro $a \in L$ položme $r(a) = \{P \in \mathcal{T}; a \notin P\}$. Pak systém množin $\mathcal{S} = \{r(a); a \in L\}$ tvoří množinový okruh, pričemž zobrazení: $a \mapsto r(a)$ je požadovaný izomorfismus.

Věta D.5. *Svaz L je booleovský tehdy a jen tehdy, je-li izomorfní některému množinovému tělesu.*

D ů k a z : plyne ihned z Věty D.4, neboť se snadno dokáže $r(a') = \mathcal{T} \setminus r(a)$. □

Jelikož filtry a zejména ultrafiltry na Booleovských algebrách hrají důležitou roli v konstrukcích variet univerzálních algeber, uvedeme zde několik důležitých výsledků.

Nechť B je booleova algebra, $X \subseteq B$. Označme $X' = \{x'; x \in X\}$.

Věta D.6. *Nechť B je Booleova algebra, $I \subseteq B$, $F \subseteq B$. Pak platí:*
(a) *I je ideál právě když I' je filtr;*
(b) *F je filtr právě když F' je ideál.*

D ů k a z : Nechť $a, b \in I$. Pak $a', b' \in I'$. Dle DeMorganových zákonů platí $a \vee b \in I$ právě když $(a \vee b)' = a' \wedge b' \in I'$. Dále pro $a \in I$ je $c \leq a$ právě když $a' \leq c'$, tedy $c \in I$ právě když $c' \in I'$. Odtud plyne tvrzení (a). Tvrzení (b) se dokáže duálně. □

Jak víme z kapitoly 5., existuje jednoznačná korespondence mezi ideály a kongruencemi v Booleových algebrách. Jelikož filtr je pojem duální k pojmu ideál, plyne bezprostředně z výše uvedeného poznatku a z Věty D.6., že existuje také jednoznačná korespondence mezi filtry a kongruencemi v Booleově algebře. Přesněji, je-li B Booleova algebra a Θ kongruence na B, pak třída $[1]_\Theta$ je filtr. Je-li F filtr na B, pak relace definovaná vztahem

$$\langle x, y\rangle \in \Theta_F \text{ právě když } x \wedge w = y \wedge w \text{ pro některé } w \in F$$

je kongruence na B, přičemž $[1]_{\Theta_F} = F$.

Věta D.7. *Nechť F je filtr a I je ideál na Booleově algebře B. Pak F je ultrafiltr* (*resp. I je maximální ideál*) *právě když pro každé $a \in B$ právě jeden z prvků a, a' patří do F* (*resp. patří do I*)*.*

D ů k a z : Vzhledem k dualitě pojmů provedeme důkaz pouze pro ideály. Nechť I je maximální ideál na B, nechť Θ_I je kongruence indukovaná ideálem I. Uvažujme faktorovou Booleovu algebru B/Θ_I. Jestliže B/Θ_I má více než dva prvky, pak na ní existuje vlastní kongruence Φ. Tedy na B existuje kongruence $\Phi^* \neq B \times B$ větší než Θ_I. Je-li J ideál indukovaný Φ^*, t.j. $J = [0]_{\Phi^*}$, pak J je vlastní ideál, $J \neq I$, $I \subseteq J$, spor s maximalitou I. Tedy B/Θ_I je dvouprvková Booleova algebra. Je-li $h : B \to B/\Theta_I$ přirozený homomorfismus, pak buď $h(a) = [0]_{\Theta_I} = I$ (a $h(a') = [1]_{\Theta_I}$) nebo $h(a') = [0]_{\Theta_I} = I$ (pak $h(a) = [1]_{\Theta_I}$), jak plyne z vlastnosti homomorfismu Booleových algeber. Tedy buď $a \in I$ nebo $a' \in I$. Obráceně, nechť pro každé $a \in B$ platí buď $a \in I$ a nebo $a' \in I$. Nechť existuje ideál J tak, že $I \subseteq J$, $I \neq J$. Zvolme $a \in J \setminus I$. Jelikož $a \notin I$, platí $a' \in I$, ale $I \subseteq J$, tedy $a' \in J$. Odtud $1 = a \vee a' \in J$, t.j $J = I(1) = B$. Tedy ideál I je maximální. □

Dualizací Lemmatu D.2 a Věty D.2. ihned obdržíme:

Lemma D.3. *Nechť L je booleovský svaz, F jeho filtr. Pak F je ultrafiltr právě když $L \setminus F$ je ideál.*

Nechť L je svaz, $a \in L$. Zřejmě množina $F(a) = \{x \in L; x \geq a\}$ je filtr (tzv. *hlavní filtr* generovaný prvkem a). Je-li $At(L)$ množina všech atomů svazu L a platí-li $a \in At(L)$, pak zřejmě $F(a)$ je maximální vlastní filtr, t.j. hlavní ultrafiltr. Je-li B konečná Booleova algebra a F je ultrafiltr na B, pak každý filtr, a tedy i F, je nutně hlavní, t.j. $F = F(a)$ pro některé $a \in B$. Je-li $b \in At(B)$, $b < a$, pak ale $F(a) \subseteq F(b)$, $F(a) \neq F(b)$. Tedy:

Věta D.8. *Je-li B konečná Booleova algebra, pak její ultrafiltry jsou právě všechny hlavní filtry $F(a)$ pro $a \in At(B)$.*

UNIVERSÁLNÍ ALGEBRA

7 POJEM ALGEBRY, PODALGEBRY, A HOMOMORFISMU

Definice: Nechť A je neprázdná množina, $n \geq 0$ celé číslo. Zobrazení $f : A^n \to A$ nazveme n-ární operace na A.

Poznámka: Nechť $n = 0$. Pak $A^0 = \{\emptyset\}$, a tedy f přiřazuje této jednoprvkové množině jediný prvek $a_f \in A$. Tento vybraný prvek pak nazýváme *nulární operace*. Je-li $n = 1$, pak se operace nazývá *unární*. Je-li $n = 2$, pak se operace nazývá *binární*, pro $n = 3$ *ternární*, pro $n = 4$ *kvarternární* atd. Číslo n nazýváme *arita* operace f.

Definice: *Typem* nazveme množinu F spolu se zobrazením $\sigma : F \to \boldsymbol{N} \cup \{0\}$. Prvky z F budeme nazývat symboly operací. Zobrazení σ tedy každému symbolu operace $f \in F$ přiřazuje jeho aritu $\sigma(f)$, t.j. f je $\sigma(f)$-ární.

Definice: *Algebrou typu* (F, σ) nazýváme dvojici $\mathcal{A} = (A, F)$, kde neprázdná množina A je tzv. *nosič algebry* $\mathcal{A}$ a pro každý symbol operace $f \in F$ je přiřazena $\sigma(f)$-ární operace f_A na A. F nazýváme *množina* (*fundamentálních*) *operací* algebry $\mathcal{A}$.

Poznámka: Místo f_A často píšeme jen f. Je-li množina F konečná, t.j. $F = \{f_1, \ldots, f_k\}$, pak místo $(A, \{f_1, \ldots, f_k\})$ píšeme jen stručně $(A; f_1, \ldots, f_k)$, a typ algebry $(A; f_1, \ldots, f_k)$ zapisujeme ve tvaru $(\sigma(f_1), \ldots, \sigma(f_k))$.

Příklady:
(1) *Grupoid* $(G, \circ)$ je algebra typu (2).
(2) *Grupu* $(G; \cdot, ^{-1}, e)$ lze takto chápat jako algebru typu (2,1,0).
(3) *Svaz* $(L; \vee, \wedge)$ je algebra typu (2,2). Také *okruh* je algebra typu (2,2).
(4) *Booleova algebra* $(B; \vee, \wedge, ', 0, 1)$ je typu (2,2,1,0,0).
(5) *Unární algebrou* nazýváme algebru (A,F), kde každá $f \in F$ je unární. Algebra $(A\,,\, f)$ se nazývá *momounární*, je-li typu (1).
(6) *Monoid* je algebra typu (2,0).

Definice: Nechť $\mathcal{A} = (A, F)$ je algebra typu (F, σ) a $\emptyset \neq B \subseteq A$. Řekneme, že B je *podalgebra* algebry $\mathcal{A}$, jestliže pro každou $f \in F$ $(\sigma(f) = n)$ a pro libovolné $b_1, \dots, b_n \in B$ platí $f(b_1, \dots, b_n) \in B$.

Jinými slovy, podalgebra algebry $\mathcal{A}$ je taková podmnožina B jejího nosiče, která je uzavřená na výsledky všech operací s prvky z B.

Tedy podalgebra B algebry $\mathcal{A} = (A, F)$ typu (F, σ) je sama rovněž algebrou typu (F, σ), kde pro $f \in F, \sigma(f) = n$, a pro $b_1, \dots, b_n \in B$ platí

$$f_B(b_1, \dots, b_n) = f_A(b_1, \dots, b_n).$$

Proto tuto algebru zapisujeme dle naší konvence $\mathcal{B} = (B, F)$. Je-li zřejmé, o jakou podalgebru se jedná, budeme místo f_B psát opět jen f.

Speciálně algebra $\mathcal{A} = (A, F)$ je podalgebrou $\mathcal{A} = (A, F)$.

Věta 7.1. *Nechť $\mathcal{A} = (A, F)$ je algebra a pro každé $i \in I$ je B_i podalgebra algebry $\mathcal{A}$. Je-li $B = \cap\{B_i; i \in I\} \neq \emptyset$, pak je B podalgebra algebry $\mathcal{A}$.*

Důkaz: Nechť $B \neq \emptyset$ a $f \in F$, $\sigma(f) = n$, $b_1, \dots, b_n \in B$. Pak pro každé $i \in I$ platí $b_1, \dots, b_n \in B_i$, ale B_i je podalgebra, tedy také $f(b_1, \dots, b_n) \in B_i$ pro každé $i \in I$. Odtud $f(b_1, \dots, b_n) \in \cap\{B_i; i \in I\} = B$. $\square$

Definice: Nechť $M \neq \emptyset$. Neprázdný systém podmnožin $\mathcal{M} \subseteq Exp\, M$ nazveme *uzávěrový systém*, je-li uzavřený vzhledem k libovolným průnikům, t.j. pro každý systém podmnožin $\mathcal{N} \subseteq Exp\, M$ takový, že $\mathcal{N} \subseteq \mathcal{M}$ platí $\cap\mathcal{N} \subseteq \mathcal{M}$.

Poznámka: Je-li $\mathcal{M} \subseteq Exp\, A$ uzávěrový systém, pak $A \in \mathcal{M}$, neboť A je průnik prázdného systému $\emptyset = \mathcal{N} \subseteq \mathcal{M}$.

Nechť $\mathcal{M} \subseteq Exp\, A$ je uzávěrový systém a $X \subseteq A$. Nechť $\mathcal{N} = \{B \in \mathcal{M}; X \subseteq B\}$. Zřejmě $\mathcal{N} \neq \emptyset$, neboť $A \in \mathcal{N}$ (neboť $X \subseteq A$). Množinu $[X] = \cap\{B \in \mathcal{M}; X \subseteq B\}$ nazveme *člen uzávěrového systému $\mathcal{M}$ generovaný množinou X*, nebo *uzávěr X*.

Věta 7.2. *Nechť $\mathcal{M} \subseteq Exp\, A$ je uzávěrový systém a $X, Y \subseteq A$. Pak platí:*
(a) $X \subseteq [X]$;
(b) $[X]$ *je nejmenší prvek z $\mathcal{M}$ obsahující X;*
(c) $[[X]] = [X]$;
(d) $X \subseteq Y \Rightarrow [X] \subseteq [Y]$.

D ů k a z:

(a) Jelikož $[X] = \cap\{B \in \mathcal{M}; X \subseteq B\}$, tedy $X \subseteq B$ pro $B \in \mathcal{M}$ implikuje také $X \subseteq \cap\{B \in \mathcal{M}; X \subseteq B\} = [X]$.

(b) Zřejmě průnik je menší než každá z množin tohoto průniku.

(c) Jelikož $[X] \in \mathcal{M}$, kde $[X] = \cap\{B \in \mathcal{M}; X \subseteq B\}$, je $[[X]] = [X] \cap (\cap\{B \in \mathcal{M}; X \subseteq B\}) = [X] \cap [X] = [X]$.

(d) Nechť $X \subseteq Y$. Položme $\mathcal{N}_X = \{B \in \mathcal{M}; X \subseteq B\}$ a $\mathcal{N}_Y = \{B \in \mathcal{M}; Y \subseteq B\}$. Z $X \subseteq Y$ plyne $\mathcal{N}_X \supseteq \mathcal{N}_Y$. Ale průnik menšího systému je větší, tedy

$$[X] = \cap\mathcal{N}_X \subseteq \cap\mathcal{N}_Y = [Y].$$

□

Věta 7.3. *Nechť $\mathcal{M} \subseteq Exp\, M$ je uzávěrový systém. Pak $(\mathcal{M}, \subseteq)$ je úplný svaz, jehož největším prvkem je M a nejmenším prvkem je $\cap\mathcal{M}$.*

D ů k a z: Věta 7.3. je přímým důsledkem Věty 3.1. □

Definice: Uzávěrový systém $\mathcal{M} \subseteq Exp\, M$ se nazývá *algebraický*, jestliže pro každou $X \subseteq M$ platí

$$(*) \qquad [X] = \cup\{[Y]; Y \subseteq X, Y \text{ je konečná}\}.$$

Člen uzávěrového systému $[X] \in \mathcal{M}$ se nazývá *konečně generovaný*, jestliže $[X] = [Y]$ pro některou konečnou množinu $Y \subseteq M$.

Tedy v algebraickém uzávěrovém systému je každý člen $[X]$ sjednocením konečně generovaných členů.

Věta 7.4. *Nechť $\mathcal{M} \subseteq Exp\, M$ je algebraický uzávěrový systém. Pak $(\mathcal{M}, \subseteq)$ je algebraický svaz, jehož kompaktní prvky jsou právě všechny konečně generované členy.*

D ů k a z: Dle Věty 7.3. je $(\mathcal{M}, \subseteq)$ úplný svaz. Dokážeme, že $[X]$ je kompaktní, právě když je konečně generovaný. Nechť $X = \{a_1, \ldots, a_k\}$ a

$$[X] \subseteq \vee\{[A_i]; i \in I\} = [\cup\{A_i; i \in I\}].$$

Pro každé $a_j \in X$ dle $(*)$ existuje konečná $X_j \subseteq \cup\{A_i; i \in I\}$ tak, že $a_j \in [X_j]$. Tedy existuje konečná množina indexů $\{j_1, \ldots, j_s\}$ tak, že $X_j \subseteq A_{j_1} \cup \ldots \cup A_{j_s}$, t.j.

$$a_j \in [A_{j_1} \cup \ldots \cup A_{j_s}].$$

Odtud $X \subseteq \cup\{[A_{j_1} \cup \ldots \cup A_{j_s}]; j = 1, \ldots, k\}$, tedy

$$X \subseteq [\cup\{A_{j_i}; j = 1, \ldots, k; i = 1, \ldots, s\}], \text{ a tedy}$$

$$[X] \subseteq [\cup\{A_{j_i}; j = 1, \ldots, k; i = 1, \ldots, s\}] = \\ = \vee\{[A_{j_i}]; j = 1, \ldots, k; i = 1, \ldots, s\}.$$

Tedy $[X]$ je kompaktní.

Obráceně, nechť $[X]$ je kompaktní prvek v $(\mathcal{M}, \subseteq)$ a předpokládejme, že neexistuje konečná $Y \subseteq M$ tak, že $[X] = [Y]$. Jelikož

$$[X] \subseteq \cup\{[Y]; Y \subseteq X, Y \text{ je konečná}\},$$

pak $[X]$ nemůže být obsaženo v žádném konečném sjednocení takových $[Y]$, Y je konečná. Tedy $[X]$ není kompaktní – spor.

Z definice algebraického uzávěrového systému vidíme, že každý prvek úplného svazu $(\mathcal{M}, \subseteq)$ je spojením kompaktních prvků, tedy $(\mathcal{M}, \subseteq)$ je algebraický svaz. □

Věta 7.5. *Nechť $\mathcal{A} = (A, F)$ je algebra. Označme $Sub\,\mathcal{A}$ množinu všech podalgeber algebry $\mathcal{A}$ spolu s $\emptyset$. Pak $Sub\,\mathcal{A} \subseteq Exp\,A$ je algebraický uzávěrový systém.*

Důkaz: Z Věty 7.1. ihned plyne, že $Sub\,\mathcal{A}$ je uzávěrový systém. Dokážeme, že je algebraický. Nechť $\mathcal{A} = (A, F)$ je algebra a $X \subseteq A$. Definujme

$$E(X) = X \cup \{f(a_1, \ldots, a_n); f \in F\,,\ \sigma(f) = n\,,\ a_1, \ldots, a_n \in X\},$$

a položme

$$E^0(X) = X \qquad , \qquad E^{n+1}(X) = E(E^n(X)).$$

Zřejmě

$$X \subseteq E(X) \subseteq E^2(X) \subseteq \ldots \subseteq E^n(X) \subseteq \ldots .$$

Položme $\overline{X} = X \cup E(X) \cup E^2(X) \cup \ldots$. Zřejmě každá podalgebra, obsahující X, obsahuje také každou $E^n(X)$, tedy $\overline{X} \subseteq [X]$. Nechť $f \in F$, $\sigma(f) = n$ a $a_1, \ldots, a_n \in \overline{X}$. Pak existuje $m \in \boldsymbol{N} \cup \{0\}$ takové, že $a_1, \ldots, a_n \in E^m(X)$, a tedy $f(a_1, \ldots, a_n) \in E^{m+1}(X) \subseteq \overline{X}$, tudíž $\overline{X}$ je podalgebra, obsahující X, tedy $[X] \subseteq \overline{X}$, neboť dle Věty 7.2. je $[X]$ nejmenší prvek této vlastnosti. Odtud $[X] = \overline{X}$. Nechť tedy $a \in [X]$. Pak $a \in \overline{X}$, t.j. existuje konečná množina $Y_a \subseteq A$ tak, že $a \in [Y_a]$ (neboť $a \in E^n(X)$, t.j. vznikla konečným počtem operací z konečně mnoha prvků). Jelikož

$$[X] = \cup\{a; a \in [X]\}, \text{ je tedy } [X] = \cup\{[Y_a]; a \in X\},$$

neboť zřejmě $[Y_a] \subseteq [X]$ pro každé $a \in [X]$, ale každá Y_a je konečná, tedy každý člen $[X]$ je spojením kompaktních prvků, t.j. $Sub\,\mathcal{A}$ je algebraický uzávěrový systém. $\square$

Nechť $\mathcal{A} = (A, F)$ je algebra a $X \subseteq A$. Dle Věty 7.5. existuje nejmenší podalgebra, obsahující množinu X, totiž $[X]$ v $Sub\,\mathcal{A}$. Tuto algebru $[X]$ nazýváme *podalgebra algebry $\mathcal{A}$ generovaná množinou X*. Je-li X konečná, $[X]$ se nazývá *konečně generovaná podalgebra*.

Poznámka: Nejmenší podalgebrou algebry $\mathcal{A}$, pokud taková existuje, je tedy podalgebra generovaná prázdnou množinou, t.j. $[\emptyset]$. Pro grupu $(G, \cdot, ^{-1}, e)$ je zřejmě $[\emptyset] = \{e\}$, pro Booleovu algebru $(B; \vee, \wedge, ', 0, 1)$ je $[\emptyset] = \{0, 1\}$, pro okruh charakteristiky 0 s jednotkou 1 je $[\emptyset] = (\boldsymbol{Z}; +, \cdot)$, pro okruh charakteristiky n s 1 je $[\emptyset] = (\boldsymbol{Z}_n; +, \cdot)$. Naproti tomu svaz nemusí obsahovat nejmenší podsvaz, generovaný prázdnou množinou. Je-li např. $C_n = \{0, a, 1\}$ tříprvkový řetězec (t.j. svaz), pak $\{0, 1\}$, $\{0, a\}$, $\{a, 1\}$ jsou jeho podsvazy, ale jejich průnik je $\emptyset$, tedy $[\emptyset] = \emptyset$.

Definice: Nechť $\mathcal{A} = (A, F)$, $\mathcal{B} = (B, F)$ jsou algebry téhož typu. Zobrazení $h : A \to B$ se nazývá *homomorfismus*, jestliže pro každou $f \in F$, $\sigma(f) = n$ a pro každé $a_1, \dots, a_n \in A$ platí

$$h(f_A(a_1, \dots, a_n)) = f_B(h(a_1), \dots, h(a_n)).$$

Je-li homomorfismus h bijekce, nazývá se *izomorfismus*.

Věta 7.6. *Nechť $\mathcal{A}, \mathcal{B}, \mathcal{C}$ jsou algebry téhož typu a h je homomorfismus $\mathcal{A}$ do $\mathcal{B}$, g je homomorfismus $\mathcal{B}$ do $\mathcal{C}$. Pak $h \cdot g$ je homomorfismus $\mathcal{A}$ do $\mathcal{C}$.*

Důkaz: Nechť $f \in F$, $\sigma(f) = n$, $a_1, \dots, a_n \in A$. Pak

$$h \cdot g(f(a_1, \dots, a_n)) = g(f(h(a_1), \dots, h(a_n))) =$$

$$= f(g(h(a_1)), \dots, g(h(a_n))) = f(h \cdot g(a_1), \dots, h \cdot g(a_n)).$$

$\square$

Věta 7.7. *Nechť h je homomorfismus algebry $\mathcal{A}$ do $\mathcal{B}$. Je-li $\mathcal{C}$ podalgebra $\mathcal{A}$, je $h(\mathcal{C})$ podalgebra algebry $\mathcal{B}$. Je-li $\mathcal{D}$ podalgebra algebry $h(\mathcal{A})$, pak je $h^{-1}(\mathcal{D})$ podalgebra algebry $\mathcal{A}$.*

Důkaz: Nechť h je homomorfismus $\mathcal{A}$ do $\mathcal{B}$, $\mathcal{C}$ podalgebra $\mathcal{A}$. Nechť $f \in F$, $\sigma(f) = n$ a $d_1, \dots, d_n \in h(\mathcal{C})$. Pak existují $c_1, \dots, c_n \in C$ tak, že $h(c_i) = d_i$ $(i = 1, \dots, n)$. Ale $\mathcal{C}$ je podalgebra, tedy $f(c_1, \dots, c_n) = c \in \mathcal{C}$, tedy

$$f(d_1, \dots, d_n) = f(h(c_1), \dots, h(c_n)) = h(f(c_1, \dots, c_n)) = h(c) \in h(\mathcal{C}),$$

tedy i $h(\mathcal{C})$ je podalgebra.

Nechť $\mathcal{D}$ je podalgebra $h(\mathcal{A})$, nechť $f \in F$ je n-ární a $c_1, \dots, c_n \in h^{-1}(\mathcal{D})$. Pak $h(c_i) \in \mathcal{D}$ pro $i = 1, \dots, n$, ale $\mathcal{D}$ je podalgebra, a tedy i

$$f(h(c_1), \dots, h(c_n)) \in \mathcal{D}, \text{ tedy}$$

$$f(c_1, \dots, c_n) \in h^{-1}(\mathcal{D}), \text{ neboť}$$

$$h(f(c_1, \dots, c_n)) = f(h(c_1), \dots, h(c_n)) \in \mathcal{D}.$$

□

Věta 7.8. *Nechť $\mathcal{A}, \mathcal{B}, \mathcal{C}$, jsou algebry téhož typu a h je izomorfismus $\mathcal{A}$ na $\mathcal{B}$, g je izomorfismus $\mathcal{B}$ na $\mathcal{C}$. Pak*

(a) *$h \cdot g$ je izomorfismus $\mathcal{A}$ na $\mathcal{C}$;*

(b) *h^{-1} je izomorfismus $\mathcal{B}$ na $\mathcal{A}$;*

(c) *identické zobrazení id_A je izomorfismus $\mathcal{A}$ na $\mathcal{A}$.*

Důkaz:

(a) je přímý důsledek Věty 7.6. a známého tvrzení, že složení dvou bijekcí je bijekce.

(b) Inversní zobrazení h^{-1} je zřejmě opět bijekce. Nechť $f \in F$ je n-ární a $b_1, \dots, b_n \in B$. Pak existují $a_1, \dots, a_n \in A$ tak, že $a_i = h^{-1}(b_i)$, a odtud

$$h^{-1}(f(b_1, \dots, b_n)) = h^{-1}(f(h(a_1), \dots, h(a_n))) =$$

$$= h^{-1}(h(f(a_1, \dots, a_n))) = f(a_1, \dots, a_n) = f(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Tvrzení (c) je evidentní. □

Je-li tedy h izomorfismus $\mathcal{A}$ na $\mathcal{B}$, je h^{-1} dle Věty 7.8. izomorfismus $\mathcal{B}$ na $\mathcal{A}$; budeme v tomto případě říkat, že $\mathcal{A}$, $\mathcal{B}$ jsou *izomorfní*, což budeme značit symbolem $A \cong B$. Dle Věty 7.8. tedy platí:

$$A \cong B \quad , \quad B \cong C \Rightarrow \ A \cong C$$

$$A \cong B \Rightarrow \ B \cong A$$

$$A \cong A,$$

tedy relace "býti izomorfní" je ekvivalencí na třídě všech algeber téhož typu.

8 KONGRUENCE A FAKTOROVÉ ALGEBRY

Definice: Nechť $\mathcal{A} = (A, F)$ je algebra a θ je ekvivalence na množině A. θ se nazývá *kongruence* na $\mathcal{A}$, jestliže je kompatibilní s operacemi algebry $\mathcal{A}$, neboli splňuje *substituční podmínku*:

(SP) jestliže $f \in F$ je n-ární a $a_1, \dots, a_n, b_1, \dots, b_n \in A$, pak

$\langle a_i, b_i\rangle \in \theta$ $(i = 1, \dots, n)$ implikuje $\langle f(a_1, \dots, a_n), f(b_1, \dots, b_n)\rangle \in \theta$.

Nechť $\mathcal{A} = (A, F)$ je algebra. Označme $Ekv\, A$ resp. $Con\, A$ množinu všech ekvivalencí na A resp. množinu všech kongruencí na A. Zřejmě identická ekvivalence ω a úplný čtverec $\iota = A \times A$ jsou kongruence na každé algebře $\mathcal{A} = (A, F)$.

Věta 8.1. *Nechť $A \neq \emptyset$. Pak $(Ekv\, A; \subseteq)$ je úplný svaz.*

Důkaz: Nechť $\theta_i \in Ekv\, A$ pro $i \in I$. Položme $\theta = \cap\{\theta_i; i \in I\}$. Je snadné dokázat, že θ je opět reflexivní, symetrická a tranzitivní relace, tedy ekvivalence, t.j. $\theta \in Ekv\, A$. Neboli $Ekv\, A$ je uzavřená na libovolné průniky, tedy dle Věty 3.1. je $(Ekv\, A; \subseteq)$ úplný svaz. $\square$

Věta 8.2. *Nechť $A \neq \emptyset$. Ve svazu $(Ekv\, A; \subseteq)$ je*
$\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$
$\theta_1 \vee \theta_2 = \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup (\theta_1 \circ \theta_2 \circ \theta_1 \circ \theta_2) \cup \dots .$

Důkaz: Zřejmě $\theta_1 \cap \theta_2$ je největší ekvivalence obsažená v θ_1 i θ_2, tedy $\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$.

$\theta_1 \vee \theta_2$ je nejmenší ekvivalence, obsahující současně θ_1 i θ_2. Tedy $\theta_1 \subseteq \theta_1 \vee \theta_2$, $\theta_2 \subseteq \theta_1 \vee \theta_2$. Jestliže $\langle a, c\rangle \in \theta_1 \circ \theta_2$, pak existuje $b \in A$ tak, že $\langle a, b\rangle \in \theta_1$, $\langle b, c\rangle \in \theta_2$, tedy $\langle a, b\rangle \in \theta_1 \vee \theta_2$, $\langle b, c\rangle \in \theta_1 \vee \theta_2$, z tranzitivity tedy také $\langle a, c\rangle \in \theta_1 \vee \theta_2$. Odtud $\theta_1 \circ \theta_2 \subseteq \theta_1 \vee \theta_2$. Takto postupně dokážeme $\theta_1 \circ \theta_2 \circ \theta_1 \subseteq \theta_1 \vee \theta_2$, atd., t.j.

$$\theta_1 \vee \theta_2 \supseteq \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \dots .$$

Obráceně, $\theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \dots$ je zřejmě reflexivní a symetrická (neboť θ_1, θ_2 jsou reflexivní a symetrické), z konstrukce plyne, že je i tranzitivní, je to tedy ekvivalence. Zřejmě obsahuje θ_1, ale $\theta_2 \subseteq \theta_1 \circ \theta_2$, tedy obsahuje i θ_2, tudíž musí obsahovat i nejmenší ekvivalenci, obsahující θ_1, θ_2, t.j. $\theta_1 \vee \theta_2$; odtud $\theta_1 \vee \theta_2 \subseteq \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \dots .$ $\square$

Věta 8.3. *Nechť* $\mathcal{A} = (A, F)$ *je algebra. Pak* $(Con\, A; \subseteq)$ *je úplný svaz, který je podsvazem svazu* $(Ekv\, A; \subseteq)$.

Důkaz: Nechť $\theta_i \in Con\, A$ pro $i \in I$. Pak $\theta_i \in Ekv\, A$, tedy dle Věty 8.1. je i $\theta = \cap\{\theta_i; i \in I\}$ ekvivalence. Nechť $\langle a_j, b_j\rangle \in \theta$ pro $j = 1, \ldots, n$ a $f \in F$ je n-ární. Pak $\langle a_j, b_j\rangle \in \theta_i$ pro každé $i \in I$, ale θ_i splňuje (SP), tedy také $\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\rangle \in \theta_i$ pro každé $i \in I$, tj. $\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\rangle \in \theta$. Tedy θ je kongruence. Dokázali jsme, že $Con\, A$ je uzavřena vzhledem k průnikům, t.j. dle Věty 3.1. je $(Con\, A; \subseteq)$ úplný svaz, kde $\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$.

Zřejmě $Con\, A \subseteq Ekv\, A$. Nechť $\theta_1, \theta_2 \in Con\, A$. Pak $\theta_1 \vee \theta_2$ ve svazu $Con\, A$ je nejmenší kongruence, obsahující θ_1 i θ_2, tedy obsahuje i nejmenší ekvivalenci, obsahující θ_1 i θ_2, t.j. dle Věty 8.2. je

$$\theta_1 \vee \theta_2 \supseteq \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \ldots .$$

Nechť $f \in F$ je n-ární, a_i, $b_i \in A$ pro $i = 1, .., n$ a nechť $\langle a_i, b_i\rangle \in \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \ldots$. Jelikož

$$(**) \qquad \theta_1 \subseteq \theta_1 \circ \theta_2 \subseteq \theta_1 \circ \theta_2 \circ \theta_1 \subseteq \ldots ,$$

platí $\langle a_i, b_i\rangle \in \theta_1 \circ \theta_2 \circ \ldots \circ \theta_1 \circ \theta_2$ pro některý člen posloupnosti $(**)$. Relační součin relací splňujících (SP) však zřejmě také splňuje (SP), tedy i

$$\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\rangle \in \theta_1 \circ \theta_2 \circ \ldots \circ \theta_1 \circ \theta_2 \subseteq \theta_1 \cup (\theta_1 \circ \theta_2) \cup \ldots .$$

Dokázali jsme, že ekvivalence $\theta_1 \cup (\theta_1 \circ \theta_2) \cup \ldots$ je kongruencí (obsahující dle Věty 8.2. kongruence θ_1, θ_2), tedy

$$\theta_1 \vee \theta_2 \subseteq \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup \ldots .$$

Dohromady z obou dokázaných inkluzí plane již tvrzení věty. □

Svaz $(Con\, A; \subseteq)$ nazýváme *svaz kongruencí algebry* $\mathcal{A}$. Zřejmě ω je nejmenší a ι je největší prvek svazu $Con\, A$. Jelikož $Con\, A$ je úplný svaz pro každou algebru $\mathcal{A} = (A, F)$, je tedy uzávěrovým systémem na $Exp\, A \times A$. Tedy pro každou $X \subseteq A \times A$ existuje nejmenší kongruence obsahující X, tzv. *kongruence generovaná množinou* X. Budeme ji označovat symbolem $\theta(X)$. Speciálně, je-li $X = \{\langle a, b\rangle\}$, označíme ji $\theta(a, b)$ a nazveme ji *hlavní kongruence generovaná dvojicí* $\langle a, b\rangle$. Je-li $M = \{a_1, \ldots, a_n\} \subseteq A$, pak kongruence generovaná množinou $M \times M$ se nazývá *konečně generovaná* a označujeme ji symbolem $\theta(a_1, \ldots, a_n)$. Podle Věty 7.4. jsou konečně generované kongruence právě všechny kompaktní prvky svazu $Con\, A$.

Věta 8.4. *Nechť* $\mathcal{A} = (A, F)$ *je algebra,* $a_1, b_1, \ldots, a_n, b_n \in A$. *Pak*
(a) $\theta(\{\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\}) = \theta(a_1, b_1) \vee \ldots \vee \theta(a_n, b_n)$;

(b) $\theta(a_1, \ldots, a_n) = \theta(a_1, a_2) \vee \theta(a_2, a_3) \vee \ldots \vee \theta(a_{n-1}, a_n)$;
(c) *pro každou* $\theta \in Con\, A$ *je* $\theta = \vee\{\theta(a, b); \langle a, b\rangle \in \theta\}$.

Důkaz:

(a) Zřejmě $\langle a_i, b_i\rangle \in \theta(\{\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\})$, tedy také $\theta(a_i, b_i) \in \theta(\{\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\})$ pro $i = 1, \ldots, n$. Odtud

$$\theta(a_1, b_1) \vee \ldots \vee \theta(a_n, b_n) \subseteq \theta(\{\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\}).$$

Obráceně, $\langle a_i, b_i\rangle \in \theta(a_i, b_i) \subseteq \theta(a_1, b_1) \vee \ldots \vee \theta(a_n, b_n)$, tedy

$$\{\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\} \subseteq \theta(a_1, b_1) \vee \ldots \vee \theta(a_n, b_n), \text{ odtud}$$

$$\theta(\{\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\}) \subseteq \theta(a_1, b_1) \vee \ldots \vee \theta(a_n, b_n).$$

(b) Dle definice $\theta(a_1, \ldots, a_n) = \theta(\{\langle a_i, a_j\rangle; i, j \in \{1, \ldots, n\}\})$. Jelikož $\theta(a_i, a_j) = \theta(a_j, a_i)$, plyne tvrzení (b) ihned z (a).

(c) Nechť $\langle a, b\rangle \in \theta$. Pak zřejmě

$$\langle a, b\rangle \in \theta(a, b) \subseteq \theta \quad , \quad \text{tedy} \quad \vee\{\theta(a, b); \langle a, b\rangle \in \theta\} \subseteq \theta.$$

Obráceně $\theta = \cup\{\langle a, b\rangle; \langle a, b\rangle \in \theta\} \subseteq \vee\{\theta(a, b); \langle a, b\rangle \in \theta\}$. □

Dle Věty 8.3. je $Con\, \mathcal{A}$ úplný svaz, tedy uzávěrový systém. Dle Věty 8.4. je každý prvek $\theta \in Con\, \mathcal{A}$ sjednocením konečně generovaných prvků, neboť $\theta = \vee\{\theta(a, b); \langle a, b\rangle \in \theta\}$ a $\theta(a, b)$ jsou konečně generované. Tedy tento uzávěrový systém je algebraický. Dle Věty 7.4. ihned dostáváme:

Věta 8.5. *Nechť* $\mathcal{A} = (A, F)$ *je algebra. Pak* $(Con\, A; \subseteq)$ *je algebraický svaz.*

Poznámka: Vzniká přirozená otázka, zda platí také věta obrácená k Větě 8.5., t.j. zda každý algebraický svaz je svazem kongruencí některé algebry. Tento problém rozřešili v roce 1963 matematici *G.Grätzer* a *E.T.Schmidt*:

Věta 8.6. *Nechť* L *je algebraický svaz s alespoň dvěma prvky. Pak existuje algebra* $\mathcal{A}$ *taková, že* $L \cong Con\, \mathcal{A}$.

Důkaz této věty nalezne čtenář v knize [7] (původní důkaz byl dlouhý asi 25 stran, podstatně kratší důkaz, asi na 6 stran, vytvořil v roce 1976 český matematik *Pavel Pudlák*). Nevýhodou těchto důkazů však je, že zkonstruovaná algebra $\mathcal{A}$ je vždy nekonečná, a to i v případě, že L je konečný svaz, který je např. svazem kongruencí konečného grupoidu; nadto množina operací takto zkonstruované algebry je rovněž nekonečná.

Nechť $\mathcal{A}$ je algebra. Dle Věty 7.5. a 7.4. je množina $Sub\, \mathcal{A}$ všech podalgeber algebry $\mathcal{A}$ spolu s prázdnou množinou také algebraický svaz. Naskýtá se tedy otázka obdobná jako u kongruencí: Je-li dán algebraický svaz S, existuje algebra $\mathcal{A}$ taková, že $S \cong Sub\,\mathcal{A}$? V úvaze lze pokračovat. Množina $Aut\,\mathcal{A}$ všech izomorfismů $\mathcal{A}$ na $\mathcal{A}$ (tzv. *automorfismů*) je dle Věty 7.8. zřejmě grupou vzhledem k operaci skládání zobrazení. Vzniká tedy opět otázka: Je-li G grupa, existuje algebra $\mathcal{A}$ tak, že $G \cong Aut\,\mathcal{A}$?

Tyto otázky spadají do tzv. problémů *representace*. Svazům $Sub\,\mathcal{A}$, $Con\,\mathcal{A}$ a grupě $Aut\,\mathcal{A}$ říkáme souhrně tzv. *doprovodné struktury* (existují i další doprovodné struktury). Na výše uvedené otázky byla nalezena souhrnná odpověď, na níž se podíleli zejména *G.Birkhoff*, *O.Frink*, *G.Grätzer*, *W.A.Lampe* a *E.T.Schmidt*, a to koncem šedesátých let:

Věta 8.6a. *Nechť G je grupa, L algebraický svaz aspoň se dvěma prvky, S algebraický svaz. Pak existuje algebra $\mathcal{A}$ taková, že $G \cong Aut\,\mathcal{A}$, $L \cong Con\,\mathcal{A}$, $S \cong Sub\,A$.*

Nechť $\mathcal{A} = (A, F)$ je algebra a $\theta \in Con\,\mathcal{A}$. Označme $[a]_\theta = \{x \in A; \langle a, x\rangle \in \theta\}$ pro $a \in A$. Tedy $[a]_\theta$ je třída ekvivalence θ obsahující prvek a. Proto $[a]_\theta$ nazveme *třída kongruence θ obsahující a*. Jak víme, třídy $[a]_\theta$ pro $a \in A$ tvoří rozklad A. Množinu všech tříd kongruence označíme A/θ. Na množině A/θ lze zavést operace takto:

Nechť $f \in F$ je n-ární, $a_1, \ldots, a_n \in A$. Definujme

$$(Q) \qquad f([a_1]_\theta, \ldots, [a_n]_\theta) = [f(a_1, \ldots, a_n)]_\theta.$$

Ukážeme, že tato definice je skutečně definicí operace, t.j. že f je skutečně zobrazení množiny $(A/\theta)^n$ do A/θ. Pro důkaz toho, že f je zobrazení, je nutné dokázat, že výsledek $f([a_1]_\theta, \ldots, [a_n]_\theta)$ je jednoznačně určen třídami $[a_1]_\theta, \ldots, [a_n]_\theta$, a nikoliv výběrem prvků z těchto tříd.

Nechť tedy $b_i \in [a_i]_\theta$, $i = 1, \ldots, n$. Pak $\langle a_i, b_i\rangle \in \theta$, ale θ splňuje substituční podmínku, tudíž $\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\rangle \in \theta$, odtud $f(b_1, \ldots, b_n) \in [f(a_1, \ldots, a_n)]_\theta$. Dokázali jsme, že pro libovolné prvky z $[a_1]_\theta, \ldots, [a_n]_\theta$ je vždy výsledek ve třídě $[f(a_1, \ldots, a_n)]_\theta$, tedy v (Q) zavedená relace f je vskutku operace. Dohromady dostáváme:

$$(A/\theta, F) \text{ je algebra téhož typu jako } (A, F).$$

Algebru $\mathcal{A}/\theta = (A/\theta, F)$ budeme nazývat *faktorová algebra* algebry $\mathcal{A}$ dle kongruence θ.

Nyní ukážeme souvislost mezi kongruencemi a homomorfismy.

Věta 8.7. *Nechť h je homomorfismus algebry $\mathcal{A}$ do algebry $\mathcal{B}$. Pak relace θ_h, definovaná předpisem*

$$\langle a, b\rangle \in \theta_h \quad \textit{právě když} \quad h(a) = h(b)$$

je kongruence na $\mathcal{A}$ (tzv. kongruence indukovaná homomorfismem h).

D ů k a z : Jelikož $h : A \to B$ je zobrazení, je θ_h ekvivalence. Stačí tedy dokázat substituční podmínku. Nechť $f \in F$ je n-ární, $a_i, b_i \in A$ pro $i = 1, \ldots, n$ a nechť $\langle a_i, b_i \rangle \in \theta_h$ $(i = 1, \ldots, n)$. Pak $h(a_i) = h(b_i)$ pro každé i, tedy

$$h(f(a_1, \ldots, a_n)) = f(h(a_1), \ldots, h(a_n)) = f(h(b_1), \ldots, h(b_n)) = h(f(b_1, \ldots, b_n)),$$

tedy $\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n) \rangle \in \theta_h$. □

Věta 8.8. *Nechť θ je kongruence na algebře $\mathcal{A} = (A, F)$ a nechť h_θ je zobrazení $\mathcal{A}$ do faktorové algebry $\mathcal{A}/\theta = (A/\theta, F)$, dané předpisem*

$$h_\theta(x) = [x]_\theta.$$

Pak h_θ je surjektivní homomorfismus (tzv. přirozený homomorfismus indukovaný kongruencí θ) .

D ů k a z : Nechť $\theta \in Con\,\mathcal{A}$ a $h_\theta(x) = [x]_\theta$. Pak pro každou n-ární operaci $f \in F$ a libovolné $a_1, \ldots, a_n \in A$ platí

$$h_\theta(f(a_1, \ldots, a_n)) = [f(a_1, \ldots, a_n)]_\theta = f([a_1]_\theta, \ldots, [a_n]_\theta) = f(h(a_1), \ldots, h(a_n)),$$

neboť takto je definována operace f na faktorové algebře $\mathcal{A}/\theta$. Zřejmě h_θ je surjektivní. □

Poznámka: Z Věty 8.8. a 8.7. je zřejmé, že je-li $\theta \in Con\,\mathcal{A}$, pak $\theta_{h_\theta} = \theta$. Tedy každá kongruence algebry $\mathcal{A}$ je indukovaná homomorfismem (totiž h_θ).

Věta 8.9. Věta o homomorfismu. *Nechť $\mathcal{A}, \mathcal{B}$ jsou algebry téhož typu a h je homomorfismus $\mathcal{A}$ do $\mathcal{B}$. Pak existuje injektivní homomorfismus g faktorové algebry $\mathcal{A}/\theta_h$ do $\mathcal{B}$ tak, že $h = p \cdot g$, kde p je přirozený homomorfismus $\mathcal{A}$ na $\mathcal{A}/\theta_h$ (t.j. $p = h_{\theta_h}$).*

D ů k a z : Dle Věty 8.7. je θ_h kongruence, tedy existuje faktorová algebra $\mathcal{A}/\theta_h$; dle Věty 8.8. je $p : \mathcal{A} \to \mathcal{A}/\theta_h$ homomorfismus. Definujme $g : \mathcal{A}/\theta_h \to \mathcal{B}$ takto:

$$g([x]_{\theta_h}) = h(x).$$

Pak zřejmě $p \cdot g(x) = g([x]_{\theta_h}) = h(x)$, tedy skutečně $h = p \cdot g$. Dokážeme, že g je injektivní homomorfismus. Nechť $g([x]_{\theta_h}) = g([y]_{\theta_h})$, pak $h(x) = h(y)$, a tedy $\langle x, y \rangle \in \theta_h$, tedy $[x]_{\theta_h} = [y]_{\theta_h}$, t.j. g je injekce. Nechť $f \in F$ je n-ární. Pak

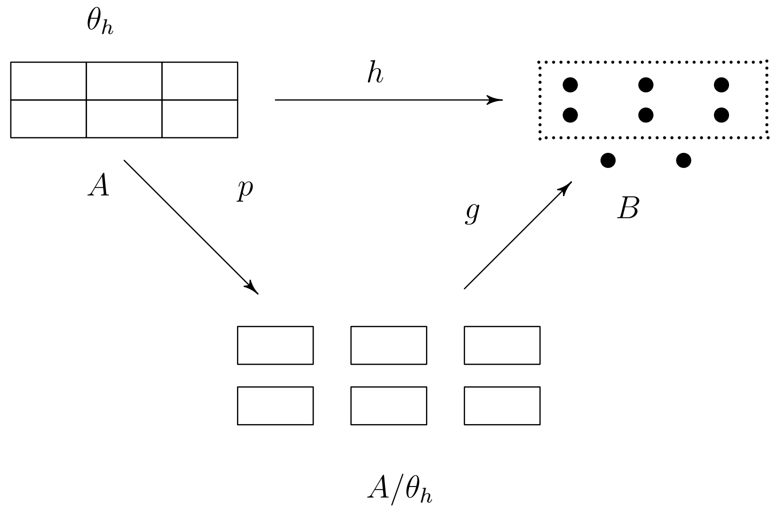
$$g(f([a_1]_{\theta_h}, \ldots, [a_n]_{\theta_h})) = g([f(a_1, \ldots, a_n)]_{\theta_h}) = h(f(a_1, \ldots, a_n)) =$$

$$= f(h(a_1), \ldots, h(a_n)) = f(g([a_1]_{\theta_h}), \ldots, g([a_1]_{\theta_h})),$$

tedy g je homomorfismus. $\square$

Důsledek: *Je-li h surjektivní homomorfismus algebry $\mathcal{A}$ na algebru $\mathcal{B}$, pak $h = p \cdot g$, kde p je přirozený (surjektivní) homomorfismus $\mathcal{A}$ na $\mathcal{A}/\theta_h$ a g je izomorfismus.*

Grafické schema Věty o homomorfismu je toto:



Definice: Nechť $\mathcal{A} = (A, F)$ je algebra a $\theta, \Phi \in Con\,\mathcal{A}$ tak, že $\theta \subseteq \Phi$. Na faktorové množině A/θ definujme relaci Φ/θ:

$$\langle [a]_\theta, [b]_\theta \rangle \in \ \Phi/\theta \quad \text{právě když} \quad \langle a, b \rangle \in \Phi.$$

Lemma 8.10. *Jestliže $\theta, \Phi \ \in Con\,\mathcal{A}$ a $\theta \subseteq \Phi$, pak Φ/θ je kongruence na faktorové algebře $\mathcal{A}/\theta$.*

Důkaz: Z definice je zřejmé, že Φ/θ je ekvivalence. Nechť $f \in F$ je n-ární a nechť $\langle [a_i]_\theta, [b_i]_\theta \rangle \in \Phi/\theta$, $i = 1, \ldots, n$. Pak

$$\langle a_i, b_i \rangle \in \Phi \ \Rightarrow \ \langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n) \rangle \in \Phi, \text{ a tedy}$$

$\langle [f(a_1, \ldots, a_n)]_\theta, [f(b_1, \ldots, b_n)]_\theta \rangle \in \Phi/\theta$, tedy, jelikož $\mathcal{A}/\theta$ je faktorová algebra, také

$$\langle f([a_1]_\theta, \ldots, [a_n]_\theta), f([b_1]_\theta, \ldots, [b_n]_\theta) \rangle \in \Phi/\theta,$$

tedy Φ/θ je kongruence na $\mathcal{A}/\theta$. $\square$

Věta 8.11. První věta o izomorfismu. *Nechť $\mathcal{A}$ je algebra a $\theta, \Phi \ \in Con\,\mathcal{A}, \ \theta \subseteq \Phi$. Pak*

$$(\mathcal{A}/\theta)/(\Phi/\theta) \cong \ \mathcal{A}/\Phi,$$

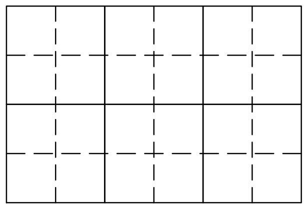
přičemž tento izomorfismus $h : (\mathcal{A}/\theta)/(\Phi/\theta) \rightarrow \mathcal{A}/\Phi$ *je dán předpisem* $h([[a]_\theta]_{\phi/\theta}) = [a]_\phi$.

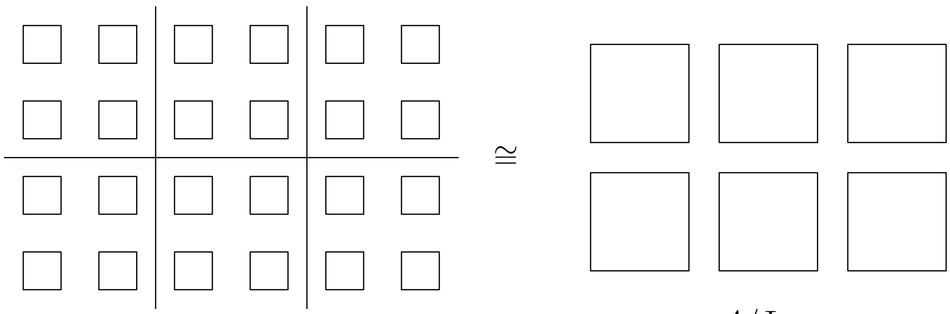
Důkaz: Je zřejmé, že h je bijekce. Nechť $f \in F$ je n-ární, $a_1, \ldots, a_n \in A$. Pak

$$h(f([[a_1]_\theta]_{\phi/\theta}, \ldots, [[a_n]_\theta]_{\phi/\theta})) = h([f([a_1]_\theta, \ldots, [a_n]_\theta)]_{\phi/\theta}) =$$
$$= h([[f(a_1, \ldots, a_n)]_\theta]_{\phi/\theta}) = [f(a_1, \ldots, a_n)]_\phi \ = f([a_1]_\phi, \ldots, [a_n]_\phi) =$$
$$= f(h([[a_1]_\theta]_{\phi/\theta}), \ldots, h([[a_1]_\theta]_{\phi/\theta})).$$

□

Grafické schema 1.věty o izomorfismu je následující:


A


$(A/\theta)/(\Phi/\theta)$ $\cong$ A/Φ

plnou čarou jsou vyznačeny třídy kongruence Φ kombinace plné čáry a přerušované (t.j. malé čtverečky) jsou třídy θ

Definice: Nechť $\mathcal{A} = (A, F)$ je algebra, $\theta \in Con\,\mathcal{A}$. Pro $B \subseteq A$ označme $B^\theta = \{a \in A; B \cap [a]_\theta \neq \emptyset\}$; tedy B^θ je sjednocení všech tříd kongruence θ, s kterými je B incidentní. Symbolem $\theta|B$ označme *restrikci* (t.j. zúžení) kongruence θ na podmnožinu B, t.j.

$$\theta|B = \theta \ \cap (B \times B).$$

Věta 8.12. Druhá věta o izomorfismu. *Nechť* $\mathcal{A} = (A, F)$ *je algebra,* $\theta \in Con\,\mathcal{A}$ *a* $\mathcal{B} = (B, F)$ *je podalgebra algebry* $\mathcal{A}$. *Pak* B^θ *je rovněž podalgebra algebry* $\mathcal{A}$ *a platí*

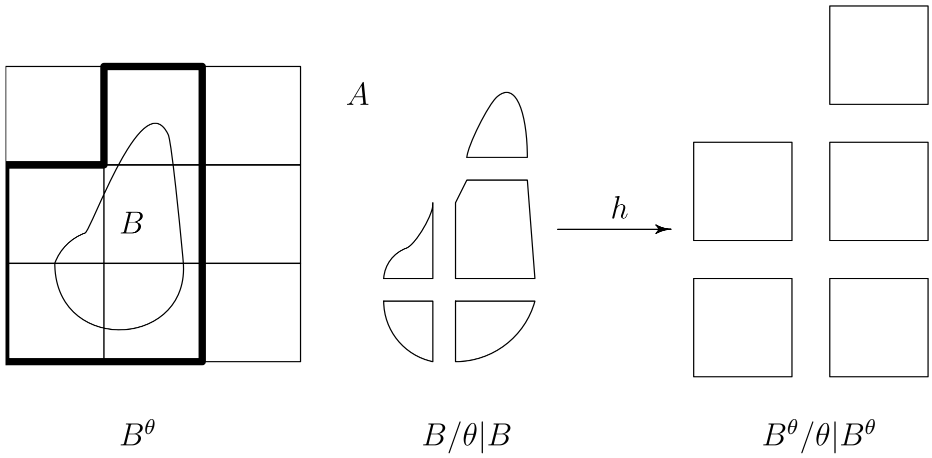
$$B/\theta|B \cong \ B^\theta/\theta|B^\theta.$$

D ů k a z: Nechť $\mathcal{B} = (B, F)$ je podalgebrou $\mathcal{A}$, $\theta \in Con\,\mathcal{A}$. Nechť $f \in F$ je n-ární, $a_1, \dots, a_n \in B^\theta$. Pak existují $b_1, \dots, b_n \in B$ tak, že $a_i \in [b_i]_\theta$, t.j. $\langle a_i, b_i\rangle \in \theta$, odtud

$$\langle f(a_1, \dots, a_n), f(b_1, \dots, b_n)\rangle \in \theta,$$

tedy $f(a_1, \dots, a_n) \in [f(b_1, \dots, b_n)]_\theta$. Jelikož $\mathcal{B}$ je podalgebra, platí $f(b_1, \dots, b_n) \in B$, tedy $f(a_1, \dots, a_n) \in B^\theta$, t.j. B^θ je podalgebra. Zřejmě zobrazení $h : [b]_{\theta|B} \to [b]_{\theta|B}\theta$ je hledaný izomorfismus. □

Grafické schema 2.věty o izomorfismu:



Věta 8.13. *Nechť $\mathcal{A}$ je algebra a $\theta \in Con\,\mathcal{A}$. Pak*

$$Con\,\mathcal{A}/\theta \;\cong\; [\theta, \iota] \subseteq Con\,\mathcal{A}$$

přičemž $h(\Phi) = \Phi/\theta$ je izomorfismus intervalu $[\theta, \iota]$ na svaz $Con\,\mathcal{A}/\theta$.

D ů k a z:

(i) h je injekce: Nechť $\Psi, \Phi \in [\theta, \iota]$, $\Psi \neq \Phi$. Nechť $\langle a, b\rangle \in \Phi \setminus \Psi$. Pak $\langle [a]_\theta, [b]_\theta\rangle \in (\Phi/\theta) \setminus (\Psi/\theta)$, t.j. také $h(\Phi) \neq h(\Psi)$.

(ii) h je surjekce: Nechť $\Phi \in Con\,\mathcal{A}/\theta$. Pak zřejmě $\Phi \supseteq \theta$. Definujme relaci Ψ, jakožto kongruenci indukovanou homomorfismem $p_1 \cdot p_2$, kde p_1 je přirozený homomorfismus $\mathcal{A}$ na $\mathcal{A}/\Phi$ a p_2 je přirozený homomorfismus $\mathcal{A}/\Phi$ na $\mathcal{A}/(\Phi/\theta)$. Pak $\langle [a]_\theta, [b]_\theta\rangle \in \Psi/\theta$, právě když $\langle a, b\rangle \in \Psi$, právě když $\langle [a]_\theta, [b]_\theta\rangle \in \Phi$, t.j. $\Phi = \Psi/\theta$. Tedy Φ je obrazem Ψ, t.j. h je surjekce.

(iii) Abychom dokázali, že h je svazový izomorfismus, stačí dle Věty 2.12. ukázat, že je izotonní. To je ale zřejmé, neboť $\Psi \subseteq \Phi \Rightarrow \Psi/\theta \subseteq \Phi/\theta$. □

9 DIREKTNÍ A SUBDIREKTNÍ SOUČINY

Definice: Nechť $\mathcal{B} = (B, F)$, $\mathcal{C} = (C, F)$ jsou algebry téhož typu. *Direktním součinem* $\mathcal{B}\times\mathcal{C}$ nazýváme algebru $(B\text{x}C, F)$, kde operace jsou definovány takto: $f \in F$ n-ární, $\langle b_i, c_i\rangle \in B \times C$, $i = 1, \dots, n$, pak

$$f(\langle b_1, c_1\rangle, \dots, \langle b_n, c_n\rangle) = \langle f(b_1, \dots, b_n), f(c_1, \dots, c_n)\rangle.$$

Indukcí zřejmě můžeme rozšířit definici direktního součinu na konečný počet algeber téhož typu:
pro $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n$ pak položíme

$$\mathcal{A}_1 \times \mathcal{A}_2 \times \dots \times \mathcal{A}_n = (\dots((\mathcal{A}_1 \times \mathcal{A}_2) \times \mathcal{A}_3) \times \dots) \times \mathcal{A}_n.$$

Definici direktního součinu můžeme rozšířit i pro libovolný (t.j. i nekonečný) systém algeber téhož typu. Nechť $A_i \neq \emptyset$ pro $i \in I$. Prvky kartézského součinu $\Pi\{A_i; i \in I\}$ jsou zřejmě všechna zobrazení $I \to \cup\{A_i; i \in I\}$ taková, že $f(i) \in A_i$ pro každé $i \in I$.

Nechť $\mathcal{A}_i = (A_i, F)$ jsou algebry téhož typu pro $i \in I \neq \emptyset$. *Direktním součinem* $\Pi\{\mathcal{A}_i; i \in I\}$ algeber $\mathcal{A}_i$ $(i \in I)$ nazveme algebru
$\mathcal{A} = (\Pi\{\mathcal{A}_i; i \in I\}, F)$, kde operace jsou definovány takto: pro každou n-ární $f \in F$ a libovolné $a_1, \dots, a_n \in \Pi\{\mathcal{A}_i; i \in I\}$ je pro každé $i \in I$

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

neboli operace f je prováděna "po souřadnicích".

Nechť $\Pi\{\mathcal{A}_i; i \in I\}$ je direktní součin. Zobrazení

$$pr_i : \Pi\{\mathcal{A}_i; i \in I\} \to \mathcal{A}_i$$

dané předpisem $pr_i\, a = a(i)$ se nazývá *i-tá projekce.*

Lemma 9.1. *Každá i-tá projekce je surjektivní homomorfismus.*

Důkaz: Je evidentní. □

Označme θ_i kongruenci indukovanou i-tou projekcí. Tuto kongruenci nazveme *faktorová kongruence.* Je-li tedy $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2 \times ... \times \mathcal{A}_n$, pak n projekcí $pr_1, pr_2, ..., pr_n$ indukuje n faktorových kongruencí $\theta_1, \dots, \theta_n$.

Lemma 9.2. *Nechť algebry $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ jsou téhož typu. Pak*
(a) $\mathcal{A}_1 \times \mathcal{A}_2 \cong \mathcal{A}_2 \times \mathcal{A}_1$
(b) $\mathcal{A}_1 \times (\mathcal{A}_2 \times \mathcal{A}_3) \cong (\mathcal{A}_1 \times \mathcal{A}_2) \times \mathcal{A}_3$.

D ů k a z : V případě (a) je izomorfismus dán předpisem

$$h(\langle x_1, x_2\rangle) = \langle x_2, x_1\rangle,$$

v případě (b)

$$h(\langle a_1, \langle a_2, a_3\rangle\rangle) = \langle\langle a_1, a_2\rangle, a_3\rangle.$$

□

Poznámka: Teprve Lemma 9.2. nám vlastně dává oprávnění k předchozímu rozšíření definice direktního součinu pro více než dvě algebry.

Je-li θ_i faktorová kongruence, pak pro $a, b \in \Pi\{\mathcal{A}_j; j \in I\}$ platí

$$\langle a, b\rangle \in \theta_i \quad \text{právě když} \quad a(i) = b(i).$$

Věta 9.3. *Nechť $\mathcal{A}_1, \mathcal{A}_2$ jsou algebry téhož typu a $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$. Pak pro faktorové kongruence θ_1, θ_2 platí:*
(i) $\theta_1 \wedge \theta_2 = \omega$
(ii) $\theta_1 \vee \theta_2 = \iota$
(iii)$\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$.

D ů k a z : Nechť $a = \langle a_1, a_2\rangle$, $b = \langle b_1, b_2\rangle$ jsou prvky algebry $\mathcal{A}$ a platí $\langle a, b\rangle \in \theta_1 \wedge \theta_2$. Tedy $\langle\langle a_1, a_2\rangle, \langle b_1, b_2\rangle\rangle \in \theta_1 \wedge \theta_2$, t.j. $a_1 = b_1$, $a_2 = b_2$, tedy $a = b$. Tedy platí (i). Dokážeme (ii) a (iii):

Nechť a,b jsou libovolné prvky z $\mathcal{A}$. Pak $a = \langle a_1, a_2\rangle$, $b = \langle b_1, b_2\rangle$ splňují

$$\langle\langle a_1, a_2\rangle, \langle a_1, b_2\rangle\rangle \in \theta_1 \quad , \quad \langle\langle a_1, b_2\rangle, \langle b_1, b_2\rangle\rangle \in \theta_2,$$

tedy $\langle a, b\rangle \in \theta_1 \circ \theta_2$. Odtud $\theta_1 \circ \theta_2 = \iota$. Dle Věty 8.2. je tedy $\theta_1 \circ \theta_2 = \theta_1 \vee \theta_2 = \iota$, odtud platí (ii) a kongruence θ_1, θ_2 jsou permutabilní: $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$. □

Věta 9.4. *Nechť $\mathcal{A}$ je algebra a $\theta_1, \theta_2 \in Con\,\mathcal{A}$ splňují* (i),(ii),(iii) z Věty 9.3. *Pak $\mathcal{A} \cong \mathcal{B} \times \mathcal{C}$, kde $\mathcal{B} = \mathcal{A}/\theta_1$, $\mathcal{C} = \mathcal{A}/\theta_2$.*

D ů k a z : Nechť h je zobrazení $\mathcal{A}$ do $\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$ dané předpisem $h(a) = \langle [a]_{\theta_1}, [a]_{\theta_2}\rangle$. Pak platí:

(a) h je injekce: Je-li $h(a) = h(b)$, pak $[a]_{\theta_1} = [b]_{\theta_1}, [a]_{\theta_2} = [b]_{\theta_2}$, tedy $\langle a, b\rangle \in \theta_1, \langle a, b\rangle \in \theta_2$, odtud $\langle a, b\rangle \in \theta_1 \wedge \theta_2 = \omega$, t.j. $a = b$.

(b) h je surjekce: Nechť $\langle b, c\rangle$ je libovolný prvek z $\mathcal{B} \times \mathcal{C}$. Jelikož $\mathcal{B} = \mathcal{A}/\theta_1$, $\mathcal{C} = \mathcal{A}/\theta_2$, je $b = [a]_{\theta_1}, c = [d]_{\theta_2}$ pro některé $a, d \in \mathcal{A}$. Dle (ii) a (iii) je $\theta_1 \circ \theta_2 = \iota$, t.j. $\langle a, d\rangle \in \theta_1 \circ \theta_2$. Tedy existuje prvek $x \in A$ tak, že $\langle a, x\rangle \in \theta_1, \langle x, d\rangle \in \theta_2$. Pak ale $[x]_{\theta_1} = [a]_{\theta_1} = b$, $[x]_{\theta_2} = [d]_{\theta_2} = c$, tedy $h(x) = \langle b, c\rangle$, t.j. h je surjekce.

(c) h je homomorfismus: Nechť $f \in F$ je n-ární, $a_1, \ldots, a_n \in A$. Pak

$$h(f(a_1, \ldots, a_n)) = \langle [f(a_1, \ldots, a_n)]_{\theta_1}, [f(a_1, \ldots, a_n)]_{\theta_2} \rangle =$$

$$= \langle f([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}), f([a_1]_{\theta_2}, \ldots, [a_n]_{\theta_2}) \rangle =$$

$$= f(\langle [a_1]_{\theta_1}, [a_1]_{\theta_2} \rangle, \ldots, \langle [a_n]_{\theta_1}, [a_n]_{\theta_2} \rangle) =$$

$$= f(h(a_1), \ldots, h(a_n)).$$

□

Definice: Algebra $\mathcal{A}$ se nazývá *netriviální*, má-li aspoň dva prvky. Algebra $\mathcal{A}$ se nazývá *direktně nerozložitelná*, jestliže není izomorfní direktnímu součinu netriviálních algeber.

Poznámka: Každá algebra $\mathcal{A}$ je izomorfní s direktním součinem, stačí totiž vzít $\theta_1 = \omega$, $\theta_2 = \iota$. Pak θ_1, θ_2 splňují (i), (ii), (iii) Věty 9.3., a tedy dle Věty 9.4. je $\mathcal{A} \cong \mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$. Jelikož $\theta_2 = \iota$, je $\mathcal{A}/\theta_2$ jednoprvková, t.j. triviální. Zajímáme se proto jen o případ, kdy je algebra rozložitelná na direktní součin netriviálních algeber.

Věta 9.5. *Každá konečná algebra je izomorfní direktnímu součinu konečného počtu direktně nerozložitelných algeber.*

Důkaz: Nechť $\mathcal{A}$ je konečná algebra. Je-li $\mathcal{A}$ triviální, je zřejmě direktně nerozložitelná. Je-li $\mathcal{A}$ direktně nerozložitelná, jsme hotovi. Je-li $\mathcal{A}$ rozložitelná, t.j. $\mathcal{A} \cong \mathcal{B} \times \mathcal{C}$, pak má-li $\mathcal{A}$ n prvků, $\mathcal{B}$ m prvků, $\mathcal{C}$ k prvků, platí zřejmě $n = mk$, tedy $m < n$, $k < n$, jsou-li $\mathcal{B}, \mathcal{C}$ netriviální. Postup opakujeme pro $\mathcal{B}$ resp. pro $\mathcal{C}$ (buď jsou již nerozložitelné, a jsme hotovi, nebo $\mathcal{B} = \mathcal{B}_1 \times \mathcal{B}_2$, $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2$, kde $\mathcal{B}_i$ má méně prvků než $\mathcal{B}$, $\mathcal{C}_i$ má méně prvků než $\mathcal{C}$. Po konečném počtu kroků jsme s rozkladem hotovi. □

Poznámka: Zřejmě jediná direktně nerozložitelná Booleova algebra je dvouprvková. Je-li $\mathcal{B}$ konečná Booleova algebra, pak má dle Věty 6.2. právě 2^n prvků pro některé $n \in \boldsymbol{N}$. Pak je tedy $\mathcal{B}$ direktním součinem právě n dvouprvkových Booleových algeber, jak je vidět z obr.15 a obr.16. Analogie pro nekonečné Booleovy algebry neplatí, tedy zobecnění Věty 9.5. pro nekonečné algebry neplatí. Cílem další části této kapitoly je ukázat jinou algebraickou konstrukci podobnou direktnímu součinu, pro kterou analogie Věty 9.5. platí pro libovolnou algebru.

Definice: Algebra $\mathcal{A}$ se nazývá *subdirektním součinem* algeber $\mathcal{A}_i$ $(i \in I)$, jestliže

(i) $\mathcal{A}$ je podalgebra direktního součinu $\Pi\{\mathcal{A}_i; i \in I\}$;

(ii) pro každé $i \in I$ platí $pr_i\mathcal{A} = \mathcal{A}_i$.

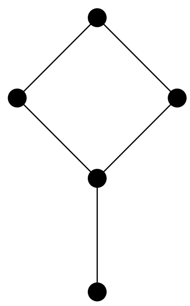
Příklady:

(1) Každý direktní součin je zřejmě subdirektním součinem.

(2) Každá algebra $\mathcal{A}$ je izomorfní subdirektnímu součinu, a to $\omega \subseteq \mathcal{A}\times\mathcal{A}$; izomorfismus je dán předpisem

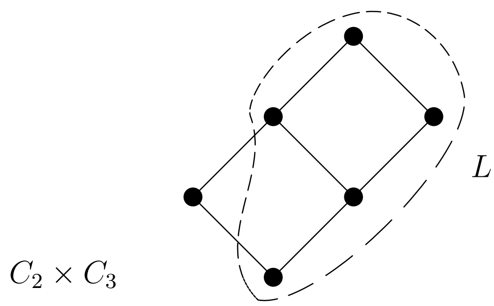
$$a \to \langle a, a\rangle.$$

(3) Nechť L je svaz, jehož diagram je



Obr.16

Pak L je subdirektním součinem dvouprvkového a tříprvkového řetězce, jak je vidět z obr.17, přičemž L není direktním součinem těchto řetězců.



Obr.17

Věta 9.6. *Algebra $\mathcal{A}$ je izomorfní subdirektnímu součinu algeber $\mathcal{A}_i$ $(i \in I)$, právě když existují $\theta_i \in Con\,\mathcal{A}$ tak, že platí*

$$\cap\{\theta_i; i \in I\} = \omega.$$

V tomto případě lze položit $\mathcal{A}_i = \mathcal{A}/\theta_i$.

Důkaz:

(1) Nechť $\mathcal{A}$ je izomorfní subdirektnímu součinu algeber $\mathcal{A}_i$, t.j. $\mathcal{A}$ je podalgebrou $\Pi\{\mathcal{A}_i; i \in I\}$ a pro každé $i \in I$ je $pr_i\mathcal{A} \cong \mathcal{A}_i$. Nechť $a, b \in A$ a nechť $\langle a, b\rangle \in \cap\{\theta_i; i \in I\}$, kde θ_i jsou faktorové kongruence. Pak $\forall i \in I$ je $a_i = b_i$, tedy $a = b$, t.j. $\cap\{\theta_i; i \in I\} = \omega$.

(2) Obráceně, nechť na $\mathcal{A}$ existují kongruence $\theta_i (i \in I)$ tak, že $\cap\{\theta_i; i \in I\} = \omega$. Nechť $h : \mathcal{A} \to \Pi\{\mathcal{A}/\theta_i; i \in I\}$ je dané předpisem

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

Pak zřejmě h je homomorfismus a h je injekce, neboť $h(a) = h(b)$ implikuje $[a]_{\theta_i} = [b]_{\theta_i}$, přičemž poslední rovnost nastane, právě když $\langle a, b\rangle \in \theta_i$ pro každé $i \in I$, tedy $\langle a, b\rangle \in \cap\{\theta_i; i \in I\} = \omega$, tedy $a = b$. Z předpisu pro zobrazení h je patrné, že

$$pr_i(h(\mathcal{A})) = h(\mathcal{A})(i) = \mathcal{A}/\theta_i,$$

tedy skutečně h je izomorfismus $\mathcal{A}$ na subdirektní součin algeber $\mathcal{A}_i = \mathcal{A}/\theta_i$ $(i = 1, \ldots, n)$. □

Definice: Algebra $\mathcal{A}$ se nazývá *subdirektně irreducibilní* (*nerozložitelná*), jestliže v případě, že $\mathcal{A}$ je izomorfní subdirektnímu součinu algeber $\mathcal{A}_i$ $(i \in I)$, pak existuje $i_0 \in I$ tak, že $\mathcal{A}$ je izomorfní s $\mathcal{A}_{i_0}$.

Z Věty 9.6. tedy plyne, že $\mathcal{A}$ je subdirektně nerozložitelná, právě když pro libovolné $\theta_i \in Con\,\mathcal{A}$ $(i \in I)$ platí:

$$\text{jestliže } \cap\{\theta_i; i \in I\} = \omega \quad \text{, pak} \quad \exists i_0 \in I \text{ tak, že } \theta_{i_0} = \omega.$$

Odtud již přímo plyne:

Věta 9.7. *Algebra $\mathcal{A}$ je subdirektně irreducibilní, právě když je triviální, nebo $\cap\{\theta \in Con\,\mathcal{A}; \theta \neq \omega\} \neq \omega$, t.j. právě když $Con\,\mathcal{A}$ obsahuje právě jeden atom.*

Důsledek *Je-li $\mathcal{A}$ subdirektně irreducibilní, pak je i direktně nerozložitelná.*

Příklady:

(1) Konečná abelovská grupa je subdirektně irreducibilní, právě když je cyklickou grupou, jejíž řád je mocninou prvočísla.

(2) Každá jednoduchá grupa je subdirektně irreducibilní.

(3) Každá dvouprvková algebra je subdirektně irreducibilní.

(4) Polosvaz S je subdirektně irreducibilní, právě když má nejvýše dva prvky.

Věta 9.8. Birkhoffova. *Každá algebra je izomorfní subdirektnímu součinu subdirektně irreducibilních algeber.*

Důkaz: Jelikož triviální algebra je subdirektně irreducibilní, budeme zkoumat pouze netriviální algebry $\mathcal{A}$. Tedy existují $a, b \in \mathcal{A}, a \neq b$. Nechť θ_{ab} je maximální kongruence, neobsahující dvojici $\langle a, b\rangle$ (její existence plyne z Zornova lemmatu, neboť uspořádaná podmnožina $\mathcal{M}_{ab} = \{\theta \in Con\,\mathcal{A}; \langle a, b\rangle \notin \theta\}$ je podmnožina svazu $Con\,\mathcal{A}$, je neprázdná, neboť $\omega \in \mathcal{M}_{ab}$, *shora* omezená, a má tedy maximální prvek). Uvažujme faktorovou algebru $\mathcal{A}/\theta_{ab}$. Zřejmě $[a]_{\theta_{ab}} \neq [b]_{\theta_{ab}}$, a tedy $\theta(a, b) \vee \theta_{ab}$ je nejmenší prvek v intervalu $[\theta_{ab}, \iota]$ svazu $Con\,\mathcal{A}$, různý od θ_{ab}. Dle Věty 8.13. je $Con\,\mathcal{A}/\theta_{ab} \cong [\theta_{ab}, \iota]$, tedy $Con\,\mathcal{A}/\theta_{ab}$ má právě jeden atom. Dle Věty 9.7. je pak $\mathcal{A}/\theta_{ab}$ subdirektně irreducibilní. Avšak zřejmě

$$\cap\{\theta_{ab}; a \neq b\} = \omega,$$

tedy $\mathcal{A}$ je dle Věty 9.6. izomorfní subdirektnímu součinu subdirektně irreducibilních algeber $\mathcal{A}/\theta_{ab}$ (kde $a, b \in \mathcal{A}, a \neq b$). □

Poznámka: Uvedená Birkhoffova věta má v algebře zcela zásadní význam. Jestliže lze každou algebru rozložit na subdirektní součin subdirektně irreducibilních algeber, pak stačí zkoumat jen tyto subdirektně irreducibilní algebry, a každou algebru z nich zkonstruovat (konstrukcí subdirektního součinu). Subdirektně irreducibilní algebry tedy tvoří jakési základní "cihličky" naší stavby. Z tohoto hlediska je zajímavá zejména následující věta:

Věta 9.9. *Každý alespoň dvouprvkový distributivní svaz je subdirektním součinem dvouprvkových řetězců.*

Důkaz: Je-li L dvouprvkový distributivní svaz, pak je zřejmě subdirektně irreducibilní. Nechť tedy existuje $a \in L$ takový, že $b < a < c$ pro některé $b, c \in L$. Položme $h(x) = x \wedge a$, $g(x) = x \vee a$. Tato zobrazení jsou vzhledem k distributivitě L zřejmě homomorfismy $L \to L$. Nechť $k(x) = \langle h(x), g(x)\rangle$. Pak zřejmě k je homomorfismus svazu L do direktního součinu svazů

$$\{b \in L; b \leq a\} \times \{b \in L; a \leq b\} = D.$$

Jestliže $k(x) = k(y)$, pak $x \wedge a = y \wedge a$, $x \vee a = y \vee a$, a podle Důsledku Věty 4.6. odtud plyne $x = y$, tedy k je injekce. Tedy k je izomorfismus L na podsvaz S svazu D. Je-li $y \in \{b \in L; b \leq a\}$, pak $h(y) = y$, tedy každý prvek z $\{b \in L; b \leq a\}$ je obsažen jako první komponenta v S. Analogické tvrzení platí pro $\{b \in L; a \leq b\}$, je tedy S subdirektní součin svazů $\{b \in L; b \leq a\}$, $\{b \in L; a \leq b\}$. Jestliže $L_1 = \{b \in L; b \leq a\}$ není dvouprvkový, pak existuje $a_1 \in L_1$ tak, že $b_1 < a_1 < c_1$ pro některé $b_1, c_1 \in L_1$, a můžeme pro svaz L_1

opakovat výše uvedenou proceduru (rozklad L_1 na direktní součin $L_{11} \times L_{12}$ tak, že L_1 je izomorfní subdirektnímu součinu těchto svazů). Analogisky pro svaz $L_2 = \{b \in L; a \leq b\}$. Tak postupujeme tak dlouho, až L je izomorfní subdirektnímu součinu dvouprvkových svazů. $\square$

Důsledek *Distributivní svaz je subdirektně irreducibilní, právě když má nejvýše dva prvky.*

Důsledek *Booleova algebra je subdirektně irreducibilní, právě když je dvouprvková.*

10 OPERÁTORY NA TŘÍDÁCH ALGEBER

Dosud jsme zkoumali jednotlivé algebry. Nyní se budeme zabývat celými třídami algeber. Nechť K je některá třída algeber téhož typu. Pak vytvoříme třídy $I(K)$, $S(K)$, $H(K)$, $P(K)$ takto: Algebra

$\mathcal{A} \in I(K)$ právě když je $\mathcal{A}$ izomorfní s některou $\mathcal{B} \in K$,

$\mathcal{A} \in S(K)$ právě když je $\mathcal{A}$ podalgebrou některé $\mathcal{B} \in K$,

$\mathcal{A} \in H(K)$ právě když je $\mathcal{A}$ homomorfním obrazem některé $\mathcal{B} \in K$,

$\mathcal{A} \in P(K)$ právě když je $\mathcal{A}$ direktním součinem neprázdného systému algeber z K.

Zřejmě $K \subseteq I(K)$, $K \subseteq S(K)$, $K \subseteq H(K)$, $K \subseteq P(K)$.

Definice: Třída algeber K je *uzavřená na*

podalgebry, jestliže $S(K) \subseteq K$,

homomorfní obrazy, jestliže $H(K) \subseteq K$,

direktní součiny, jestliže $P(K) \subseteq K$.

Třída algeber K se nazývá *varieta*, je-li uzavřena na H, S, P.

Varietu nazveme *triviální*, jestliže obsahuje pouze jednoprvkové algebry. Jinak se nazývá *netriviální*.

Poznámka: Jsou-li X, Y některé z operátorů H, S, P, a je-li K třída algeber téhož typu, budeme místo $X(Y(K))$ zapisovat jen stručně $XY(K)$. Pro operátory H, S, P a libovolnou třídu K lze dokázat tyto inkluze: $SH(K) \subseteq HS(K)$, $PH(K) \subseteq HP(K)$, $PS(K) \subseteq SP(K)$, avšak obrácené inkluze obecně neplatí. Jak dokázal v r.1935 Garret Birkhoff, platí však $HSP(HSP(K)) = HSP(K)$. Odtud plyne základní věta teorie variet algeber:

Věta 10.1. *Třída K algeber téhož typu je varieta právě když platí $K = HSP(K)$. Každá varieta je určena svými subdirektně irreducibilními algebrami.*

Druhé tvrzení Věty 10.1. plyne ihned z Věty 9.8.

Je-li tedy K třída algeber téhož typu, pak nejmenší varieta, která K obsahuje, je právě $HSP(K)$. Tuto varietu budeme označovat $\mathcal{V}(K)$ a nazývat *varieta generovaná třídou* K. Specielně, je-li K jednoprvková, t.j. $K = \{\mathcal{A}\}$ pro některou algebru $\mathcal{A}$, pak $\mathcal{V}(K)$ označíme $\mathcal{V}(\mathcal{A})$ a nazveme *varieta generovaná algebrou* $\mathcal{A}$.

Tedy varieta distributivních svazů (zřejmě je třída všech distributivních svazů varietou - je uzavřena na H, S, P) je určena dvouprvkovým svazem.

Nyní budeme charakterizovat třídy algeber, uzavřené na jednotlivé operátory H, S, P. Pro tento a pro další účely zavedeme následující pojmy:

Definice: Nechť (F, σ) je typ a $X \neq \emptyset$ je množina symbolů zvaných *proměnné* taková, že $X \cap F = \emptyset$. *Termem* (typu (F, σ)) *nad množinou proměnných* X nazveme:
(i) každou proměnnou $x \in X$,
(ii) je-li $f \in F$ n-ární a $p_1, \ldots, p_n$ jsou termy, pak je i $f(p_1, \ldots, p_n)$ termem
(iii) všechny termy typu (F, σ) vznikly konečným počtem kroků (i), (ii).
Symbolem $T(X)$ označme množinu všech termů typu (F, σ) nad množinou proměnných X.

Příklady:
(1) Termy typu (2) jsou např. x, y, $x \cdot y$, $x \cdot (y \cdot z)$, $(x \cdot x) \cdot x$ atd.
(2) Nechť $(\vee, \wedge)$ je typu $(2, 2)$. Pak termy typu $(\vee, \wedge)$ jsou např. x, $x \vee y$, $x \wedge (y \vee z)$, $(x \vee y) \wedge (x \vee z)$, $x \wedge x$, $x \vee (x \vee x)$ atd.

Věta 10.2. *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou algebry typu (F, σ). Pak platí:*
(a) *Je-li $\theta \in Con\,\mathcal{A}$ a p je n-ární term typu (F, σ), pak pro $a_i, b_i \in \mathcal{A}$ $(i = 1, \ldots, n)$ platí:*
jestliže $\langle a_i, b_i \rangle \in \theta$ $(i = 1, \ldots, n)$, pak

$$\langle p(a_1, \ldots, a_n), p(b_1, \ldots, b_n) \rangle \in \theta.$$

(b) *Je-li $h : \mathcal{A} \to \mathcal{B}$ homomorfismus a p je n-ární term typu (F, σ), pak pro každé $a_1, \ldots, a_n \in \mathcal{A}$ platí*

$$h(p(a_1, \ldots, a_n)) = p(h(a_1), \ldots, h(a_n)).$$

(c) *S je podalgebra algebry $\mathcal{A}$, jestliže pro každý n-ární term p a pro libovolné $a_1, \ldots, a_n \in S$ platí*

$$p(a_1, \ldots, a_n) \in S.$$

D ů k a z : Plyne bezprostředně z definice termu. □

Poznámka: Z definice termů je ihned zřejmé, že $T(X)$ je opět algebrou typu (F, σ) (viz (ii)). Tuto algebru $(T(X), F)$ nazveme *algebra termů*, nebo též *absolutně volná algebra typu* (F, σ) *generovaná množinou volných generátorů* X.

Lemma 10.3. *Nechť* $T(X)$ *je algebra termů typu* (F, σ), *nechť* $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_m) \in T(X)$. *Pak*

$$p(x_1, \ldots, x_n) = q(x_1, \ldots, x_m)$$

tehdy a jen tehdy, když $n = m$ *a* $p = q$.

D ů k a z : Opět plyne ihned z definice termů. □

Dle Lemma 10.3. tedy v algebře termů neplatí žádné netriviální rovnosti mezi termy.

Věta 10.4. *Nechť* K *je třída algeber typu* (F, σ) *a nechť* $T(X)$ *je algebra termů typu* (F, σ). *Pak pro každou algebru* $\mathcal{A} \in K$ *a pro každé zobrazení* $g : X \to \mathcal{A}$ *existuje homomorfismus* $h : T(X) \to \mathcal{A}$ *takový, že* $h(x) = g(x)$ *pro každé* $x \in X$.

Poznámka: Vlastnost, splněnou algebrou $T(X)$ v tvrzení Věty 10.4. nazveme *vlastnost universálního zobrazení pro třídu* K.

D ů k a z : Nechť $g : X \to \mathcal{A}$. Definujme h takto:
(i) pro každé $x \in X$ položme $h(x) = g(x)$;
(ii) je-li pro termy $p_1, \ldots, p_n \in T(X)$ již definováno $h(p_1), \ldots, h(p_n)$, a je-li $f \in F$ n-ární, položme

$$h(f(p_1, \ldots, p_n)) = f(h(p_1), \ldots, h(p_n)).$$

Z definice termů je zřejmé, že takto je h definováno pro každý term $p \in T(X)$ a z procedury je zřejmé, že h je homomorfismus. □

Dle Věty o homomorfismu indukuje každý homomorfismus kongruenci. Má-li tedy $T(X)$ vlastnost universálního zobrazení pro třídu K, je tedy dle Věty o homomorfismu pro některou kongruenci θ algebra $T(X)/\theta$ izomorfní podalgebře některé $\mathcal{A} \in K$. Tedy definujme:

Definice: Nechť K je třída algeber typu (F, σ). Pro množinu proměnných X definujme kongruenci $\theta_K(X)$ na $T(X)$ takto: $\theta_K(X) = \cap\ \Phi_K(X)$, kde

$\Phi_K(X) = \{\theta \ \in Con\, T(X); T(X)/\theta \in IS(K)\}$. Algebru

$$F_K(X) = T(X)/\theta_K(X)$$

nazveme *volná algebra třídy* K.

Důsledek *Nechť* K *je třída algeber typu* (F, σ) , $X \neq \emptyset$. *Pak* $F_K(X)$ *má vlastnost universálního zobrazení pro třídu* K.

Důkaz: Dle Věty 10.4. má tuto vlastnost $T(X)$, tedy pro libovolnou $\mathcal{A} \in K$ a libovolné zobrazení $g : X \to \mathcal{A}$ existuje homomorfismus $h : T(X) \to \mathcal{A}$, t.j. $B = h(T(X)) \cong \ T(X)/\theta_h$. Zřejmě B je podalgebra $\mathcal{A}$. Jelikož $\mathcal{A} \in K$, je $\theta_h \supseteq \ \theta_K(X)$. Dle 1.Věty o izomorfismu pak

$$B \cong \ T(X)/\theta_h \cong \ (T(X)/\theta_K(X))/(\theta_h/\theta_K(X)) = F_K(X)/\theta$$

kde $\theta = \theta_h/\theta_K(X)$.

Označme j tento izomorfismus $F_K(X)/\theta$ na B, daný předpisem $j([z]_\theta) = h(z)$, a označme p přirozený homomorfismus $F_K(X)$ na $F_K(X)/\theta$ indukovaný kongruencí θ. Zřejmě $h_0 = p \cdot j$ je homomorfismus $F_K(X)$ na B, který je rozšířením zobrazení g, neboť pro $x \in X$ platí

$$h_0(x) = j(p(x)) = j([x]_\theta) = h(x) = g(x).$$

$\square$

Poznámka: Z definice volné algebry neplyne, že $F_K(X) \in K$. Existují tedy třídy, které mají volné algebry pro různé množiny X a existují třídy, které volné algebry nemají.

Věta 10.5. *Nechť* K *je třída algeber typu* (F, σ). *Pak*

$$F_K(X) \in ISP(K).$$

Důkaz: Jelikož je $\theta_K(X) = \cap\Phi_K(X)$ a $F_K(X) = T(X)/\theta_K(X)$, tedy dle 1.Věty o izomorfismu jsou $\Phi_K(X)/\theta_K(X)$ kongruence na faktorové algebře $T(X)/\theta_K(X) = F_K(X)$ a platí

$$\cap\Phi_K(X)/\theta_K(X) = \theta_K(X)/\theta_K(X) = \omega.$$

Tedy dle Věty 9.6. je $F_K(X)$ izomorfní subdirektnímu součinu algeber $F_K(X)/\theta$ pro $\theta \in \Phi_K(X)$, t.j. algeber z K, tedy $F_K(X)$ je izomorfní podalgebře direktního součinu algeber z K, tedy $F_K(X) \in ISP(K)$. $\square$

Důsledek *Ve třídě* K *existuje volná algebra* $F_K(X)$, *je-li* $K = ISP(K)$. *Speciálně, v každé netriviální varietě existuje* $F_K(X)$ *pro každou množinu proměnných* X.

11 IDENTITY

Definice: *Identitou* typu (F, σ) nad množinou proměnných X nazveme dvojici $\langle p, q\rangle$, kde $p, q \in T(X)$. Algebra $\mathcal{A} = (A, F)$ typu (F, σ) *splňuje identitu* $\langle p, q\rangle$, právě když (jsou-li p,q n-ární) pro každé $a_1, \ldots, a_n \in A$ platí rovnost

$$p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n).$$

Z důvodů ustálené konvence budeme identity místo $\langle p, q\rangle$ zapisovat ve tvaru

$$\text{(I)} \qquad p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n).$$

Nechť K je třída algeber typu (F, σ). Řekneme, že K *splňuje identitu* (I), právě když $\mathcal{A}$ splňuje (I) pro každou $\mathcal{A} \in K$.

Nechť K je třída algeber téhož typu. Označme $Id_K(X)$ množinu všech identit, které K splňuje. Duálně, nechť Σ je množina identit typu (F, σ). Označme Σ^* třídu všech algeber typu (F, σ), které splňují všechny identity ze Σ.

Příklady identit: asociativita: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
komutativita: $x \cdot y = y \cdot x$
absorpce: $x \vee (x \wedge y) = x$
distributivita: $x \cdot (y + z) = x \cdot y + x \cdot z$
idempotence: $x \cdot x = x$
modularita: $x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$
(viz Věta 4.5.)

Věta 11.1. Birkhoffova. *Třída algeber K typu (F, σ) je varieta tehdy a jen tehdy, jestliže existuje množina identit Σ typu (F, σ) tak, že $K = \Sigma^*$.*

Důkaz: Nechť Σ je množina identit typu (F, σ). Zřejmě identity jsou zachovávány vzhledem k podalgebrám, homomorfním obrazům i direktním součinům, tedy $HSP(\Sigma^*) = \Sigma^*$, t.j. Σ^* je varieta.

Obráceně, nechť $K = HSP(K)$. Položme $\Sigma = Id_K(X)$. Zřejmě $K \subseteq \Sigma^*$. Dokážeme obrácenou inkluzi. Jelikož K je varieta, existuje v K volná algebra $F_K(X)$ pro každou množinu proměnných X. Identity, splněné v $F_K(X)$, jsou stejné jako v K, tedy Σ. Nechť $\mathcal{A} = (A, F) \in \Sigma^*$. Zvolme X tak, aby $|X| = |A|$. Pak zřejmě existuje bijekce X na A, a dle Důsledku Věty 10.4. existuje surjektivní homomorfismus $F_K(X)$ na $\mathcal{A}$. Jelikož K je uzavřená na homomorfní obrazy, plyne odtud $\mathcal{A} \in K$. Dokázali jsme $\Sigma^* \subseteq K$. □

Dle Birkhoffovy věty jsou tedy varietami právě ty třídy algeber téhož typu, které lze charakterizovat identitami. T.j. varietami jsou například:

(1) Varieta všech pologrup;
(2) Varieta všech komutativních pologrup;
(3) Varieta všech grup (typu $(\cdot, ^{-1}, 1)$)
(4) Varieta všech abelovských grup;
(5) Varieta všech okruhů;
(6) Varieta všech svazů;
(7) Varieta všech modulárních svazů;
(8) Varieta všech distributivních svazů;
(9) Varieta všech Booleových algeber;
(10) Varieta všech polosvazů.

Naproti tomu třída všech těles nebo všech oborů integrity nejsou variety. Třída všech grup jakožto algeber typu $(\cdot)$ také není varieta. Třída všech komplementárních svazů není varieta.

Pomocí aparátu identit lze nyní zavést volnou algebru ve varietě K jednodušším způsobem: Nechť K je varieta, nechť $R = \{\langle p, q\rangle; p = q \in \ Id(K)\}$. Nechť $\theta = \theta(R)$, t.j. θ je nejmenší kongruence na $T(X)$ generovaná množinou R (viz Kap.8). Pak $F_K(X) = T(X)/\theta$.

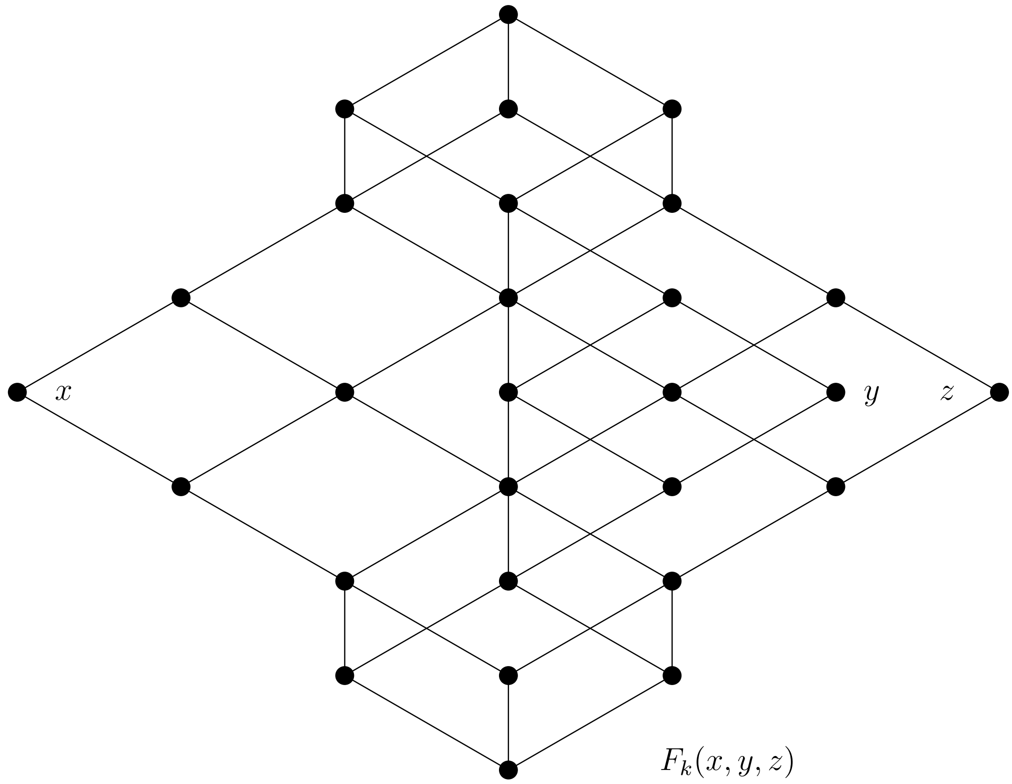
Čtenář se snadno přesvědčí o ekvivalenci takto zavedené volné algebry v K s definicí $F_K(X)$ v Kap.10.

Příklady volných algeber:

(1) Varieta všech svazů
   (a) Je-li $X = \{x\}$, pak zřejmě $F_K(X) = \{x\}$, jednoprvkový svaz.
   (b) Je-li $X = \{x, y\}$, pak $F_K(X) = \{x, y, x \vee y, x \wedge y\}$, t.j. čtyřprvkový svaz.
   (c) Je-li $|X| \geq 3$, pak $F_K(X)$ je již nekonečný svaz.

(2) Varieta modulárních svazů

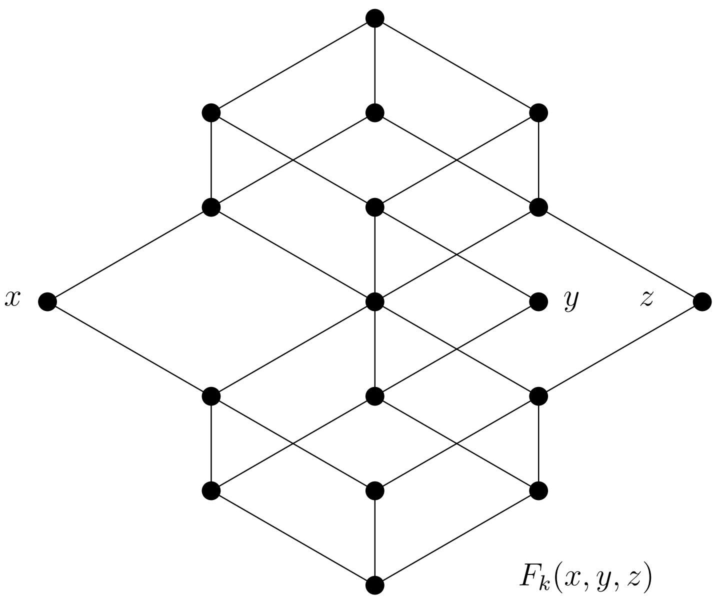
Je-li $X = \{x\}$ nebo $X = \{x, y\}$, jsou $F_K(X)$ stejné jako ve třídě všech svazů. Pro $X = \{x, y, z\}$ je $F_K(X)$ na obr.18 (má 28 prvků). Pro $|X| \geq 4$ je již $F_K(X)$ nekonečný a velmi komplikovaný.



Obr.18

(3) Varieta distributivních svazů

Zřejmě pro $X = \{x\}$ nebo $X = \{x, y\}$ jsou $F_K(X)$ stejné jako ve varietě všech svazů, neboť tyto svazy jsou distributivní. Pro $X = \{x, y, z\}$ je $F_K(X)$ 18-ti prvkový, viz obr.19. Pro $|X| = n$ je počet prvků v $F_K(X)$ roven počtu neprázdných antiřetězců v uspořádané množině neprázdných podmnožin n-prvkové množiny.



Obr.19

(4) Varieta Booleových algeber

Jelikož každý booleovský term lze psát ve tvaru DNF, snadno se přesvědčíme, že pro $|X| = n$ má $F_K(X)$ právě 2^{2^n} prvků.

(5) Varieta abelovských grup

Zřejmě pro $X = \{x_1, \ldots, x_n\}$ je $F_K(X)$ množina všech termů $x_1^{e_1} \cdot x_2^{e_2} \cdot \ldots \cdot x_n^{e_n}, e_i \in \boldsymbol{Z}$. Je-li $X = \{x\}$, pak $F_K(x)$ je izomorfní nekonečné cyklické grupě $(Z, +)$.

(6) Varieta všech komutativních pologrup

Pro $X = \{x_1, \ldots, x_n\}$ je $F_K(X)$ množina všech termů $x_1^{n_1} \cdot x_2^{n_2} \cdot \ldots \cdot x_k^{n_k}$, kde $n_i \in \boldsymbol{N} \cup \{0\}$.

Pro některé jiné typy variet ale $F_K(X)$ tak jednoduchý tvar nemají.

Prvky algebry $T(X)$ jsou termy. Je-li K varieta algeber, pak $F_K(X) = T(X)/\theta$, kde $\theta = \theta(R)$ pro $R = \{\langle p, q\rangle; p = q \in Id_K(X)\}$, jak bylo výše uvedeno. Tedy prvky algebry $F_K(X)$ jsou třídy termů. Je-li např. K varieta všech pologrup, pak $R = \{x \cdot (y \cdot z) = (x \cdot y) \cdot z\}$, a tedy třída

$$[x \cdot (y \cdot z)]_\theta$$

má právě dva prvky. Kdybychom dále pracovali s třídami termů, bylo by označení příliš těžkopádné. Proto místo třídy bereme jednoho reprezentanta této třídy, t.j. term, ale pokládáme ho rovný kterémukoliv jinému termu z této třídy. Neboli, z předchozího příkladu, prvkem $F_K(X)$ ve varietě všech pologrup (pro $X = \{x, y, z, \ldots\}$) bude opět term $x \cdot (y \cdot z)$, ale bude roven termu $(x \cdot y) \cdot z$. Odtud plyne

Konvence: *Prvky* $F_K(X)$ *pro* $X = \{x_1, ..., x_n\}, K$ *varieta, budou právě všechny n-ární termy, mezi nimiž však platí všechny identity z* $Id_K(X)$.

Je-li tedy $\mathcal{S}$ varieta všech svazů, $X = \{x, y\}$, pak $F_{\mathcal{S}}(X)$ má prvky $x = x \vee x = x \wedge x$, $x \vee y = y \vee x = x \vee (x \vee y) = \dots$, $x \wedge y = y \wedge x = x \wedge (x \wedge y) = \dots$, $y = y \vee y = y \wedge y = y \wedge y \wedge y = \dots$.

Příklady:

(1) Je-li $\mathcal{S}$ varieta všech polosvazů a $X = \{x, y, z\}$, pak $F_{\mathcal{S}}(X)$ má právě 7 prvků, a to x, y, x, $x \cdot y$, $x \cdot z$, $y \cdot z$, $x \cdot y \cdot z$. Je-li $X = \{x_1, \dots, x_n\}$, má $F_{\mathcal{S}}(X)$ právě $2^n - 1$ prvků.

(2) Je-li $\mathcal{R}$ varieta okruhů a $X = \{x\}$, pak prvky $F_{\mathcal{R}}(X)$ jsou termy tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x \ ,$$

kde $a_1, \dots, a_n$ jsou celá čísla.

(3) Je-li $\mathcal{U}$ varieta unitárních okruhů (t.j. okruhů s jednotkou), $X = \{x\}$, pak prvky $F_{\mathcal{U}}(X)$ jsou termy tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \ ,$$

kde $a_0, \dots, a_n$ jsou celá čísla.

Definice: Varieta $\mathcal{V}$ se nazývá *lokálně konečná*, jestliže pro každou konečnou množinu proměnných X je v $F_{\mathcal{V}}(X)$ konečná.

Příklady:(1) Varieta všech Booleových algeber je lokálně konečná.
(2) Varieta všech distributivních svazů je lokálně konečná.
(3) Varieta všech polosvazů je lokálně konečná.

Naopak, jak jsme výše ukázali,
(4) Varieta všech svazů ani varieta všech modulárních svazů nejsou lokálně konečné.
(5) Varieta grup ani varieta okruhů není lokálně konečná.

Existují dokonce variety, kde každá algebra, která je *netriviální* (t.j. má více než jeden prvek) je již nekonečná:

Příklad: Nechť $\mathcal{V}$ je varieta typu $(2, 1)$ s operacemi označenými $\circ$ a $'$ zadaná jedinou identitou

$$(x' \circ y) \circ z = y \qquad \text{(J)}$$

Pak každá netriviální algebra z $\mathcal{V}$ je nekonečná.

D ů k a z: Zřejmě varieta $\mathcal{V}$ je netriviální. Stačí vzít množinu všech přirozených čísel N a definovat operace $\circ$ a $'$ takto $x \circ y = x - 1$ pro $x > 1$, $x \circ y = y + 1$ pro $x = 1$, a dále $x' = 1$ pro každé $x \in N$. Pak zřejmě

$$(x' \circ y) \circ z = (1 \circ y) \circ z = (y + 1) \circ z = (y + 1) - 1 = y \ ,$$

tedy $(N; \circ, ') \in \mathcal{V}$, t.j. $\mathcal{V}$ je netriviální.

Nechť nyní $(A, \circ, ') \in \mathcal{V}$, nechť $|A| > 1$. Pak pro každé $a \in A$ je $T_a(x) = a' \circ x$ zobrazení $A \to A$. Je-li $x \neq y$ a $T_a(x) = T_a(y)$, pak $a' \circ x = a' \circ y$, a dle (J) platí $x = (a' \circ x) \circ a = (a' \circ y) \circ a = y$, t.j. $x = y$, spor. Tedy $T_a(x)$ je injekce. Je-li ovšem $T_a(x)$ surjekce, pak existuje $b \in A$ tak, že $T_a(b) = a'$, tedy $a' \circ b = a'$. Dle (J) odtud plyne $b = (a' \circ b) \circ x = a' \circ x = T_a(x)$ pro každé $x \in A$, což je spor s tím, že $T_a(x)$ je injekce.

Neboli $T_a : A \to A$ je injekce, která není surjekce, tedy množina A je nekonečná. $\square$

Nyní se vrátíme k operátorům na třídách algeber. Nejprve definujme:

Definice: Nechť (F, σ) je typ. *Atomickou formulí* typu (F, σ) nazveme každou identitu typu (F, σ). *Formulí* typu (F, σ) nazveme:
(i) každou atomickou formuli;
(ii) je-li Φ formule, je i $\neg\Phi$ formule;
(iii) jsou-li Φ, Ψ formule, je i $\Phi \vee \Psi$ formule;
(iv) je-li Φ formule, je i $\exists x \Phi$ formule.

Použitím pravidel predikátové logiky ihned ověříme, že jsou-li Φ, Ψ formule, je i $\Phi \wedge \Psi$ formule a $\forall x \ \Phi$ je formule.

Definice: Formuli Ψ nazveme *existenciální*, je-li tvaru $\Psi = \exists x_1 \exists x_2 \dots \exists x_n \Phi$, kde Φ je formule, neobsahující kvantifikátory. Formule Ψ se nazývá *universální*, je-li tvaru $\Psi = \forall x_1 \forall x_2 \dots \forall x_n \Phi$, kde Φ je formule, neobsahující kvantifikátory. Formule Φ se nazývá *positivní*, jestliže neobsahuje spojku $\neg$ (ale může obsahovat spojky $\vee, \wedge$).

Následující věty uvádíme bez důkazu; důkazy čtenář najde v knize [7]:

Věta 11.2. *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou algebry téhož typu. Je-li $\mathcal{B}$ izomorfní podalgebře algebry $\mathcal{A}$, pak každá universální formule, platná v $\mathcal{A}$, platí také v $\mathcal{B}$ a každá existenciální formule, platná v $\mathcal{B}$, platí také v $\mathcal{A}$.*

Příklad:
(1) Je-li $(S, \cdot)$ pologrupa, pak v S platí asociativní zákon: $\forall x \forall y \forall z \ (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$. Je-li tedy H podgrupoid $(S, \cdot)$, je také

H pologrupa, neboť v ní platí opět asociativní zákon, který je universální formulí.

(2) Je-li $(G, \circ)$ grupoid, H jeho podgrupoid a v H existuje idempotentní prvek a, pak platí v H: $\exists a(a \circ a = a)$. Pak tedy existuje idempotentní prvek i v $(G, \circ)$, neboť uvedená formule je existenciální.

(3) Existence dělitele nuly v okruhu.

Věta 11.3. *Nechť $\mathcal{A}$, $\mathcal{B}$ jsou algebry téhož typu. Je-li $\mathcal{B}$ homomorfním obrazem algebry $\mathcal{A}$, každá positivní formule, která platí v $\mathcal{A}$, platí také v $\mathcal{B}$.*

Příklad: Nechť $\mathcal{A}$, $\mathcal{B}$ jsou svazy, $\mathcal{A}$ je n-prvkový řetězec $x_1 < x_2 < \ldots < x_n$. Nechť $h : \mathcal{A} \to \mathcal{B}$ je homomorfismus. Pak v $\mathcal{A}$ platí positivní formule

$$(x_1 \wedge x_2 = x_1) \quad \text{a} \quad (x_2 \wedge x_3 = x_2) \quad \text{a} \quad \ldots \text{ a } (x_{n-1} \wedge x_n = x_{n-1}).$$

Tedy tato formule platí i v $\mathcal{B}$, tedy $\mathcal{B}$ je řetězec.

Naopak, nechť $\mathcal{A} = \{0, x, y, 1\}$ je čtyřprvkový svaz, kde prvky x,y jsou nesrovnatelné. Pak $\mathcal{A}$ není řetězec, tedy v $\mathcal{A}$ platí

$$\neg(x \wedge y = x) \qquad \text{a} \qquad \neg(x \wedge y = y).$$

To není positivní formule, tedy se nemusí zachovávat homomorfismem. Vskutku homomorfním obrazem $\mathcal{A}$ může být dvouprvkový svaz, t.j. řetězec, kde tedy $h(x) \wedge h(y) = h(x)$.

Definice: *Elementární Hornovskou formulí*, nazveme formuli tvaru $\delta_1 \vee \ldots \vee \delta_n$, kde δ_i je buď atomická formule nebo negace atomické formule, ale aspoň pro jedno $i \in \{1, \ldots, n\}$ je δ_i atomická. *Hornovskou formulí* nazveme formuli ve tvaru $Q_1(x_1) \ldots Q_n(x_n)\Phi$, kde $Q_1(x_1), \ldots, Q_n(x_n)$ jsou kvantifikátory (t.j. $\forall$ nebo $\exists$) a Φ je konjunkce elementárních Hornovských formulí.

Věta 11.4. *Nechť Φ je universální Hornovská formule. Jestliže Φ platí v A_i $(i \in I)$, pak Φ platí také v direktním součinu Π $\{A_i; i \in I\}$.*

Příklad: Nechť $p = q$, $s = t$ jsou identity typu (F, δ), nechť $\mathcal{A}_i$ $(i \in I)$ jsou algebry typu (F, δ), a nechť Φ je implikace $p = q \Rightarrow s = t$. Pak zřejmě Φ lze vyjádřit ve tvaru $\neg(p = q) \vee (s = t)$, což je (elementární) Hornovská formule. Jestliže tedy každá $\mathcal{A}_i$ $(i \in I)$ splňuje formuli Φ, pak dle Věty 11.4. také $\mathcal{A} = \prod\{\mathcal{A}_i; i \in I\}$ splňuje formuli Φ. Neboli implikace identit se zachovávají operátorem P.

V následující větě dokážeme, že volná algebra dané variety nese veškerou informaci o této varietě, která se dá vyjádřit identitami:

Věta 11.5. *Nechť K je varieta, nechť $p, q \in T(X)$. Varieta K splňuje identitu $p = q$, právě když tuto identitu splňuje $F_K(X)$.*

D ů k a z: Jestliže $p, q \in T(X)$ a K splňuje identitu $p = q$, pak tuto identitu splňuje každá algebra z K, dle Věty 10.5. tedy i $F_K(X)$.

Obráceně, nechť $p = q$ platí v $F_K(X_0)$. Dle Důsledku Věty 10.4. je každá algebra $\mathcal{A}$ v K homomorfním obrazem volné algebry $F_K(X)$ pro $|X| \geq |A|$. Lze dokázat (viz např. Věta 6.3.15. v [8]), že tato $F_K(X)$ je podalgebrou direktního součinu algeber $F_K(X_0)$ pro $X_0 \subseteq X$. Jelikož $p = q$ je universální positivní Hornovská formule, platí dle Vět 11.2.,11.3.,11.4. tato identita v každé $\mathcal{A} \in K$. □

12 KONGRUENČNÍ PODMÍNKY A STRUKTURA VARIET

V kapitole 8 jsme dokázali, že pro každou algebru $\mathcal{A}$ je množina všech kongruencí $Con\,\mathcal{A}$ úplným svazem, ukázali jsme, jak jsou konstruovány svazové operace v $Con\,\mathcal{A}$ (Věta 8.2.), a že každá kongruence je supremum tzv. hlavních kongruencí $\theta(a, b)$ (Věta 8.4.). V této kapitole proto nejprve popíšeme konstrukci $\theta(a, b)$ a pak ukážeme, jak vlastnosti svazu $Con\mathcal{A}$ pro každou algebru $\mathcal{A}$ z variety $\mathcal{V}$ ovlivní vlastnosti této variety $\mathcal{V}$.

Věta 12.1. Mal'cevovo lemma. *Nechť $\mathcal{A} = (A, F)$ je algebra typu (F, σ) a nechť $a, b, c, d \in A$. Pak $\langle a, b\rangle \in \theta(c, d)$, právě když existují termy $p_i(x, y_1, \ldots, y_k)$ typu (F, σ) $(i = 1, .., m)$ a prvky $e_1, \ldots, e_k \in A$ tak, že*

$$a = p_1(s_1, e_1, \ldots, e_k)$$
$$p_i(t_i, e_1, \ldots, e_k) = p_{i+1}(s_{i+1}, e_1, \ldots, e_k) \qquad , \qquad i = 1, \ldots, m-1$$
$$p_m(t_m, e_1, \ldots, e_k) = b,$$

kde $\{s_i, t_i\} = \{c, d\}$ pro $i = 1, \ldots, m$.

D ů k a z: Nechť $p_i(x, y_1, \ldots, y_k)$ jsou termy, splňující podmínky věty a $e_1, \ldots, e_k \in A$. Pak $\langle c, d\rangle \in \theta(c, d)$, z reflexivity $\langle e_j, e_j\rangle \in \theta(c, d)$ pro $j = 1, \ldots, k$, tedy dle substituční podmínky (indukcí rozšířené pro termy) platí

$$\langle p_i(c, e_1, \ldots, e_k), p_i(d, e_1, \ldots, e_k)\rangle \in \theta(c, d), \;\; i = 1, \ldots, m.$$

Je-li tedy $\{s_i, t_i\} = \{c, d\}$, pak z uvedených podmínek pro termy dostaneme:

$$\begin{array}{l} a = p_1(s_1, e_1, \ldots, e_k) \\ \langle p_1(s_1, e_1, \ldots, e_k), p_1(t_1, e_1, \ldots, e_k)\rangle \in \theta(c, d) \\ \qquad\qquad\qquad\qquad\qquad \| \\ \qquad\qquad\qquad\qquad\qquad \langle p_2(s_2, e_1, \ldots, e_k), p_2(t_2, e_1, \ldots, e_k)\rangle \in \theta(c, d) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \end{array}$$

$$\begin{aligned} \langle p_3(s_3, e_1, \ldots, e_k), p_3(t_3, e_1, \ldots, e_k)\rangle \in\ & \theta(c,d) \\ & . \\ & . \\ & . \\ p_m(t_m, e_1, \ldots, e_k) =\ & b, \end{aligned}$$

tedy z tranzitivity dostaneme $\langle a, b\rangle \in \theta(c,d)$.

Obráceně, nechť $c, d \in A$, a nechť θ je relace, obsahující všechny dvojice $\langle a, b\rangle$ takové, že a,b splňují podmínky věty. Zvolíme-li $m = 1$ a $p_1(x, y_1, \ldots, y_k) = y_1$, pak tedy pro každé $y_1 \in A$ je $\langle y_1, y_1\rangle \in \theta$, t.j. θ je reflexivní. Nechť $\langle a, b\rangle \in \theta$ pro některé $a, b \in A$. Pak $a = p_1 \ldots p_m(\ldots) = b$, tedy očíslujeme termy $p_1, \ldots, p_m$ v obráceném pořadí (neboli položme $p'_{i+1} = p_{m-i}$ pro $i = 0, \ldots, m-1$) a obdržíme $b = p'_1, \ldots, p'_m(\ldots) = a$, t.j. $\langle b, a\rangle \in \theta$, neboli θ je symetrická. Nechť $\langle a, b\rangle \in \theta, \langle b, g\rangle \in \theta$ pro některé $a, b, g \in A$. Pak dle předpisu existují $p_1, \ldots, p_m, p'_1, \ldots, p'_{m'}$ tak, že

$$a = p_1 \ldots p_m(\ldots) = b = p'_1 \ldots p'_{m'}(\ldots) = g,$$

tedy opět existuje konečná posloupnost termů, a to $p_1, \ldots, p_m, p_{m+1}, \ldots, p_n$, kde $n = m + m'$ a $p_{m+1} = p'_1, \ldots, p_n = p'_{m'}$, splňující podmínky věty, tedy $\langle a, g\rangle \in \theta$, t.j. θ je tranzitivní.

Položíme-li $m = 1, p_1(x, y_1, \ldots, y_k) = x$, pak ihned dostaneme $\langle c, d\rangle \in \theta$, tedy θ je ekvivalence obsahující $\langle c, d\rangle$.

Nechť $f \in F$ je n-ární a $\langle a_i, b_i\rangle \in \theta$ pro $i = 1, \ldots, n$. Pak

$$\begin{aligned} & a_1 = p^1_1 \ldots p^1_{m_1}(\ldots) = b_1 \\ & a_2 = p^2_1 \ldots p^2_{m_2}(\ldots) = b_2 \\ & . \\ & . \\ & . \\ & a_n = p^n_1 \ldots p^n_{m_n}(\ldots) = b_n \end{aligned}$$

Jelikož čísla $m_1, m_2, \ldots, m_n$ mohou být různá, položme $m = max(m_1, ..., m_n)$, a ty posloupnosti $p^i_1, \ldots, p^i_{m_i}$, které mají méně než m členů, doplňme do délky m termy $p^i_{m_i+1} = x, \ldots, p^i_m = x$. Pak výše uvedené posloupnosti jsou stejně dlouhé a splňují podmínky věty, tedy

$$f(a_1, \ldots, a_n) = f(p^1_1(\ldots), \ldots, p^n_1(\ldots)), \ldots, f(p^1_m(\ldots), \ldots, p^n_m(\ldots)) =$$

$$= f(b_1, \ldots, b_n),$$

kde zřejmě $f(p^1_i(\ldots), \ldots, p^n_i(\ldots))$ jsou opět termy $p'_i(\ldots)$ splňující podmínku věty, tedy

$$\langle f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)\rangle \in\ \theta,$$

t.j. θ je kongruence, obsahující $\langle c, d\rangle$, t.j. $\theta(c,d) \subseteq \theta$.

Jestliže však některá kongruence Φ obsahuje $\langle c,d\rangle$, pak z reflexivity, symetrie, tranzitivity a substituční podmínky plyne, že musí též obsahovat všechny $\langle a,b\rangle$, vzniklé procedurou z podmínky věty. Tedy musí obsahovat θ, t.j. $\theta \subseteq \Phi$. Volíme-li za $\Phi = \theta(c,d)$, pak $\theta \subseteq \theta(c,d)$, odtud $\theta = \theta(c,d)$. $\square$

Budeme zkoumat, kdy je množina $Con\,\mathcal{A}$ pologrupou vzhledem k relačnímu součinu:

Věta 12.2. *Nechť $\mathcal{A}$ je algebra, $\theta, \Phi \in Con\,\mathcal{A}$. Pak $\theta \circ \Phi$ je kongruence na $\mathcal{A}$, právě když $\theta \circ \Phi = \Phi \circ \theta$.*

Důkaz:

(a) Nechť $\theta, \Phi \in Con\,\mathcal{A}$ a $\theta\circ\Phi \in Con\,\mathcal{A}$. Pak, jelikož θ, Φ jsou symetrické, platí $\theta = \theta^{-1}$, $\Phi = \Phi^{-1}$, ale $\theta \circ \Phi$ je kongruence, t.j. opět symetrická, tedy $(\theta \circ \Phi)^{-1} = \theta \circ \Phi$. Pak ze základní vlastnosti inverze relačního součinu plyne

$$\theta \circ \Phi = (\theta \circ \Phi)^{-1} = \Phi^{-1} \circ \theta^{-1} = \Phi \circ \theta.$$

(b) Obráceně, nechť platí $\theta \circ \Phi = \Phi \circ \theta$ pro $\theta, \Phi \in Con\,\mathcal{A}$ a dokážeme, že $\theta\circ\Phi \in Con\,\mathcal{A}$. Zřejmě $\theta\circ\Phi$ je vždy reflexivní a splňuje substituční podmínku. Jelikož θ, Φ jsou symetrické, platí $\theta^{-1} = \theta$, $\Phi^{-1} = \Phi$, a tedy

$$\theta \circ \Phi = \theta^{-1} \circ \Phi^{-1} = (\Phi \circ \theta)^{-1} = (\theta \circ \Phi)^{-1},$$

t.j. $\theta \circ \Phi$ je také symetrická. Zbývá dokázat tranzitivitu. Nechť $\langle a,b\rangle \in \theta \circ \Phi$, $\langle b,c\rangle \in \theta \circ \Phi$. Pak

$$\langle a,c\rangle \in \theta \circ \Phi \circ \theta \circ \Phi = \theta \circ (\Phi \circ \theta) \circ \Phi = \theta \circ (\theta \circ \Phi) \circ \Phi = \theta \circ \theta \circ \Phi \circ \Phi.$$

Jelikož θ, Φ jsou reflexivní a tranzitivní, je

$$\theta = \theta \circ \theta \quad , \quad \Phi = \Phi \circ \Phi \quad , \quad \text{tedy } \langle a,c\rangle \in \theta \circ \Phi.$$

$\square$

Poznámka: Z Věty 12.2. vidíme, že kongruence, splňující $\theta \circ \Phi = \Phi \circ \theta$, jsou velmi důležité. Budeme tedy zkoumat algebry, ve kterých tato rovnost platí. Algebru $\mathcal{A}$ nazveme *permutabilní*, jestliže pro každé $\theta, \Phi \in Con\,\mathcal{A}$ platí $\theta \circ \Phi = \Phi \circ \theta$. Třída algeber K se nazývá *permutabilní*, má-li tuto vlastnost každá $\mathcal{A} \in K$.

Z Věty 8.2. ihned obdržíme:

Věta 12.3. *Je-li algebra $\mathcal{A}$ permutabilní, pak pro každé dvě $\theta, \Phi \in Con\,\mathcal{A}$ platí $\theta \vee \Phi = \theta \circ \Phi$.*

To je další velice důležitá vlastnost permutabilní algebry, neboť dle Věty 8.2. vidíme, že pro nepermutabilní algebry je konstrukce $\theta \vee \Phi$ komplikovaná (a dokonce obecně nekonečná).

Lemma 12.4. *Nechť $\mathcal{A}$ je algebra, $\theta, \Phi \in Con\,\mathcal{A}$. Pak je ekvivalentní:*
(a) $\theta \circ \Phi \ = \Phi \circ \theta$
(b) $\theta \circ \Phi \ \subseteq \ \Phi \circ \theta$.

Důkaz: Implikace (a) $\Rightarrow$ (b) je triviální, dokážeme (b) $\Rightarrow$ (a): Nechť $\theta \circ \Phi \ \subseteq \ \Phi \circ \theta$. Pak

$$\Phi \circ \theta \ = \Phi^{-1} \circ \ \theta^{-1} = (\theta \circ \Phi)^{-1} \subseteq \ (\Phi \circ \theta)^{-1} = \theta^{-1} \circ \ \Phi^{-1} = \theta \circ \Phi,$$

tedy platí i inkluze $\Phi \circ \theta \ \subseteq \ \theta \circ \Phi$, t.j. platí (a). □

Věta 12.5. *Je-li algebra $\mathcal{A}$ permutabilní, je svaz $Con\,\mathcal{A}$ modulární.*

Důkaz: Nechť $\theta, \Phi, \Psi \in Con\,\mathcal{A}$, $\Phi \subseteq \Psi$. Stačí zřejmě dokázat pouze nerovnost $(\theta \vee \Phi) \wedge \Psi \ \subseteq \ (\theta \wedge \Psi) \vee \Phi$. Vzhledem k permutabilitě tedy dle Věty 12.3. máme dokázat jen

$$(\theta \circ \Phi) \wedge \Psi \ \subseteq \ (\theta \wedge \Psi) \circ \Phi.$$

Nechť $\langle a, c\rangle \in (\theta \circ \Phi) \wedge \Psi$. Pak $\langle a, c\rangle \in \Psi$ a existuje $b \in A$ tak, že $\langle a, b\rangle \in \theta$, $\langle b, c\rangle \in \Phi$. Tedy $\langle a, c\rangle \in \Psi, \langle c, b\rangle \in \Phi \subseteq \Psi, \Psi$ je tranzitivní, tedy $\langle a, b\rangle \in \Psi$; ale $\langle a, b\rangle \in \theta$, t.j. $\langle a, b\rangle \in \Psi \wedge \theta$. Jelikož $\langle b, c\rangle \in \Phi$, máme $\langle a, c\rangle \in (\theta \wedge \Psi) \circ \Phi$. □

Zajímavou charakteristiku permutabilních variet odvodil *A.I.Mal'cev* v roce 1954:

Věta 12.6. *Nechť $\mathcal{V}$ je varieta. Pak je ekvivalentní:*
(1) *$\mathcal{V}$ je permutabilní;*
(2) *existuje ternární term $p(x,y,z)$ tak, že platí*

$$p(x, x, z) = z \qquad a \qquad p(x, z, z) = x.$$

Před důkazem této věty nejprve dokážeme:

Lemma 12.7. *Nechť K je varieta algeber. Pak*

$$F_K(x, y, z)/\theta(y, z) \cong \ F_K(x, y).$$

Důkaz: Jelikož $F_K(x, y, z)$ je volná algebra v K, má tedy dle Důsledku Věty 10.4. vlastnost universálního zobrazení. Dle Důsledku Věty 10.5. je $F_K(x, y) \in K$, tedy pro každé zobrazení $g : \{x, y, z\} \to F_K(x, y)$ existuje homomorfismus $h : F_K(x, y, z) \to F_K(x, y)$ tak, že na $\{x, y, z\}$ je $g = h$. Zvolme g takto: $x \to x, y \to y, z \to y$. Pak $h(x) = x, h(y) = y, h(z) = y$, tedy zřejmě pro indukovanou kongruenci θ_h platí $\theta_h = \theta(y, z)$. Dle Věty o homomorfismu je $F_K(x,y,z)/\theta(y,z) \cong F_K(x,y)$. $\square$

D ů k a z Věty 12.6.: (1) $\Rightarrow$ (2): Nechť $\mathcal{V}$ je permutabilní, $\mathcal{A} = F_V(x,y,z)$. Z permutability kongruencí plyne, že pro $\theta(x,y), \theta(y,z) \in Con\,\mathcal{A}$ platí

$$\langle x,z\rangle \in \theta(x,y) \circ \theta(y,z) = \theta(y,z) \circ \theta(x,y),$$

t.j. existuje $d \in \mathcal{A}$ tak, že $\langle x,d\rangle \in \theta(y,z)$, $\langle d,z\rangle \in \theta(x,y)$. Jelikož $\mathcal{A} = F_V(x,y,z)$, existuje 3-ární term $p(x,y,z)$ tak, že $d = p(x,y,z)$, t.j. $\langle x, p(x,y,z)\rangle \in \theta(y,z)$, $\langle p(x,y,z), z\rangle \in \theta(x,y)$.

Pak tedy na faktorové algebře $F_V(x,y,z)/\theta(y,z)$ platí $p(x,z,z) = x$. Dle Lemma 12.7. je ale tato algebra opět volná algebra variety $\mathcal{V}$. Tedy $p(x,z,z) = x$ platí ve volné algebře variety $\mathcal{V}$, dle Věty 11.5. pak platí $p(x,z,z) = x$ v celé varietě $\mathcal{V}$.

Analogicky v $F_V(x,y,z)/\theta(x,y)$ platí $p(x,x,z) = z$, tedy tato identita platí ve $\mathcal{V}$.

(2) $\Rightarrow$ (1): Nechť existuje $p(x,y,z)$ splňující (2) a nechť $\mathcal{A} \in \mathcal{V}$, $\theta, \Phi \in Con\,\mathcal{A}$. Jestliže $\langle a,b\rangle \in \theta \circ \Phi$, pak existuje $c \in \mathcal{A}$ tak, že $\langle a,c\rangle \in \theta$, $\langle c,b\rangle \in \Phi$. Z reflexivity a substituční podmínky odtud plyne

$$\langle a, p(a,c,b)\rangle = \langle p(a,b,b), p(a,c,b)\rangle \in \Phi,$$

$$\langle p(a,c,b), b\rangle = \langle p(a,c,b), p(a,a,b)\rangle \in \theta,$$

tedy $\langle a,b\rangle \in \Phi \circ \theta$. Dokázali jsme $\theta \circ \Phi \subseteq \Phi \circ \theta$, dle Lemma 12.4. dostaneme (1). $\square$

Příklady:

(1) Každá grupa má permutabilní kongruence. Ve varietě všech grup položme $p(x,y,z) = x \cdot y^{-1} \cdot z$. Pak

$$p(x,x,z) = x \cdot x^{-1} \cdot z = z,$$

$$p(x,z,z) = x \cdot z^{-1} \cdot z = x.$$

(2) Každá varieta okruhů má permutabilní kongruence:

$$p(x,y,z) = x - y + z.$$

(3) Varieta Booleových algeber má permutabilní kongruence:

$$p(x,y,z) = x \oplus y \oplus z,$$

kde $\oplus$ je operace symetrické diference, viz Věta 6.4.

(4) Kvazigrupou nazýváme algebru typu (2,2,2), jejíž operace jsou označeny $\cdot$, $/$, $\backslash$, splňující identity

$$(x/y) \cdot y = x \qquad (x \cdot y)/y = x$$

$$x \cdot (x \backslash y) = y \qquad x \backslash (x \cdot y) = y.$$

Tedy $/$ je dělení zprava a $\backslash$ je dělení zleva vzhledem k operaci $\cdot$. Zřejmě každá grupa je kvazigrupou, ale existují kvazigrupy, které nejsou grupami (nemusí mít jednotku vzhledem k operaci $\cdot$, operace $\cdot$ nemusí být asociativní). Nejmenší kvazigrupa, která není grupou je pětiprvková — její tabulka operace $\cdot$ je :

	a	b	c	d	e
a	e	d	b	c	a
b	c	e	d	a	b
c	d	a	e	b	c
d	b	c	a	e	d
e	a	b	c	d	e

Jelikož jsou kvazigrupy definované identitami, tvoří dle Věty 11.1 třída všech kvazigrup varietu. Tato varieta je permutabilní, lze uvažovat např. term $p(x, y, z) = (x/(y \backslash y)) \cdot (y \backslash z)$.

Ternární term $p(x, y, z)$ splňující podmínku (2) z Věty 12.6. se nazývá *Mal'cevův term.*

Věta 12.6. má zajímavý důsledek:

Důsledek (H. Werner): *Nechť $\mathcal{V}$ je permutabilní varieta, nechť $\mathcal{A} = (A, F) \in \mathcal{V}$. Pak každá reflexivní relace na A splňující substituční podmínku vzhledem k F je kongruence na $\mathcal{A}$.*

Důkaz: Nechť $\mathcal{A} = (A, F) \in \mathcal{V}$ a R je reflexivní relace na A splňující substituční podmínku vzhledem k F. Dle Věty 10.2 splňuje R substituční podmínku také vzhledem ke každému termu. Nechť tedy $p(x, y, z)$ je Mal'cevův term variety $\mathcal{V}$, nechť $a, b, c \in A$. Pak
$\langle a, b \rangle \in R \Rightarrow \langle b, a \rangle = \langle p(a, a, b), p(a, b, b) \rangle \in R$, tj. R je symetrická
$\langle a, b \rangle \in R$, $\langle b, c \rangle \in R \Rightarrow \langle a, c \rangle = \langle p(a, b, b), p(b, b, c) \rangle \in R$, tj. R je tranzitivní, tedy $R \in Con\, \mathcal{A}$. □

Poznámka:

(1) Jak dokázal H. Werner, je výše uvedená vlastnost dokonce ekvivalentní s tím, že varieta $\mathcal{V}$ je permutabilní.

(2) Zkoumáme-li tedy v grupě, okruhu nebo Booleově algebře, zda je

daná relace kongruencí, stačí ověřit pouze reflexivitu (což je triviální) a substituční podmínku. Obvykle pracné ověřování tranzitivity je zbytečné.

(3) Svazy netvoří permutabilní varietu. Lze však dokázat, že každý relativně komplementární svaz je permutabilní.

Podobně lze definovat podmínku slabší, tzv. *n-permutabilitu*: nechť $\mathcal{A}$ je algebra, nechť $n \in \mathbf{N}, n \geq 2$. Řekneme, že $\mathcal{A}$ je n-permutabilní, jestliže pro libovolné dvě kongruence $\Theta, \Phi \in Con\,\mathcal{A}$ platí

$$\Theta \circ \Phi \circ \Theta \circ \ldots = \Phi \circ \Theta \circ \Phi \circ \ldots \ ,$$

(kde na obou stranách rovnosti je právě n činitelů).

Je ihned patrné, že i pro n-permutabilní algebry je velmi jednoduchý popis operace $\vee$ ve svazu $Con\,\mathcal{A}$:

Lemma 12.8. *Nechť $\mathcal{A}$ je n-permutabilní algebra a Θ, $\Phi \in Con\,\mathcal{A}$. Pak $\Theta \vee \Phi = \Theta \circ \Phi \circ \Theta \circ \ldots$ (n činitelů).*

Podobně jako pro permutabilní algebry, varieta $\mathcal{V}$ se nazývá *n-permutabilní*, má-li tuto vlastnost každá $\mathcal{A} \in \mathcal{V}$. Uvedeme bez důkazu (je obdobný důkazu Věty 12.6.) následující tvrzení:

Věta 12.9. (J. Hagemann, A. Mitschke) *Varieta $\mathcal{V}$ je n-permutabilní, právě když existují ternární termy $p_0(x,y,z)$, …, $p_n(x,y,z)$ tak, že platí*

$$p_0(x,y,z) = x \ , \ p_n(x,y,z) = z$$

$$p_i(x,x,z) = p_{i+1}(x,z,z) \ \textit{pro} \ i = 0,\ldots,n-1 \ .$$

Příklad: Důležitou algebrou, používanou v logice pro popis vlastností výrokové spojky implikace jsou tzv. *implikativní algebry*. Implikativní algebra je grupoid $(A, \Rightarrow)$ splňující identity (tj. identity spojky implikace v libovolné logice):

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

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

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

Pro stručnost budeme operaci $\Rightarrow$ označovat jen symbolem $\cdot$, a uvedené axiomy tedy zapisujeme ve tvaru

$$(a \cdot b) \cdot a = a, \quad (a \cdot b) \cdot b = (b \cdot a) \cdot a, \quad a \cdot (b \cdot c) = b \cdot (a \cdot c) \ .$$

Snadno lze ověřit, že také platí důsledek: $(a \cdot a) \cdot b = b$, a také $a \cdot a = b \cdot b$, tj $a \cdot a$ je konstanta, tj. nulární term. Obvykle se označuje symbolem 1. Platí tedy $1 \cdot a = a$, $a \cdot a = 1 = a \cdot 1$. Jelikož jsou implikativní algebry zadané identitami, tvoří dle Věty 11.1 třída všech implikativních algeber varietu. Tato varieta je 3-permutabilní, příslušné ternární termy jsou: $p_0(x, y, z) = x$, $p_1(x, y, z) = (z \cdot y) \cdot x$, $p_2(x, y, z) = (x \cdot y) \cdot z$, $p_3(x, y, z) = z$. Snadno ověříme identity z Věty 12.9.:

$$p_0(x, x, z) = x = (z \cdot z) \cdot x = p_1(x, z, z)$$
$$p_1(x, x, z) = (z \cdot x) \cdot x = (x \cdot z) \cdot z = p_2(x, z, z)$$
$$p_2(x, x, z) = (x \cdot x) \cdot z = z = p_3(x, z, z) \ .$$

Na příkladu lze ukázat, že existuje implikativní algebra, která není permutabilní.

Poznámka:

(1) Je-li algebra n-permutabilní pro některé $n \geq 2$, pak je také m-permutabilní pro každé $m \geq n$.

(2) Lze dokázat, že varieta všech svazů není n-permutabilní pro žádné $n \geq 2$.

Lze dokázat následující větu, která je analogií Wernerova důsledku pro permutabilní variety:

Věta 12.10. (Chajda, Rachůnek) *Varieta $\mathcal{V}$ je n-permutabilní pro některé $n \geq 2$, právě když pro každou $\mathcal{A} = (A, F) \in \mathcal{V}$ je každá reflexivní a tranzitivní relace na A splňující substituční podmínku vzhledem k F kongruencí na $\mathcal{A}$.*

Zajímavý je rovněž vztah mezi 3-permutabilitou kongruencí a modularitou $Con\,\mathcal{A}$:

Věta 12.11. *Je-li algebra $\mathcal{A}$ 3-permutabilní, pak je $Con\,\mathcal{A}$ modulární svaz.*

Důkaz: Nechť Θ, Φ, $\Psi \in Con\,\mathcal{A}$ a platí $\Psi \subseteq \Theta$. Stačí zřejmě dokázat inkluzi $\Theta \cap (\Phi \vee \Psi) \subseteq (\Theta \cap \Phi) \vee \Psi$. Nechť tedy $\langle x, y\rangle \in \Theta \cap (\Phi \vee \Psi)$. Jelikož $\mathcal{A}$ je 3-permutabilní, plyne odtud $\langle x, y\rangle \in \Theta$ a $\langle x, y\rangle \in \Psi \circ \Phi \circ \Psi$, tj. existují z_1, $z_2 \in A$ tak, že $\langle x, z_1\rangle \in \Psi$, $\langle z_1, z_2\rangle \in \Phi$, $\langle z_2, y\rangle \in \Psi$. Avšak $\Psi \subseteq \Theta$, tedy $\langle x, z_1\rangle \in \Theta$, $\langle z_2, y\rangle \in \Theta$, což spolu s $\langle x, y\rangle \in \Theta$ (symetrie a tranzitivita Θ) dává $\langle z_1, z_2\rangle \in \Theta$. Neboli $\langle z_1, z_2\rangle \in \Theta \cap \Phi$. Jelikož $\langle x, z_1\rangle \in \Psi$, $\langle z_2, y\rangle \in \Psi$, plyne odtud (dle Věty 8.2) ihned $\langle x, y\rangle \in \Psi \circ (\Theta \cap \Phi) \circ \Psi \subseteq (\Theta \cap \Phi) \vee \Psi$. $\square$

Poznámka: Z věty 12.11. a předchozí poznámky tedy plyne, že také každá permutabilní algebra $\mathcal{A}$ má modulární svaz $Con\,\mathcal{A}$. Dá se na příkladu ukázat, že pro $n \geq 4$ již n-permutabilita neimplikuje modularitu $Con\,\mathcal{A}$.

Další důležitou kongruenční podmínkou je distributivita: algebra $\mathcal{A}$ se nazývá *distributivní*, je-li svaz $Con\,\mathcal{A}$ distributivní. Varieta $\mathcal{V}$ se nazývá *distributivní*, má-li tuto vlastnost každá $\mathcal{A} \in \mathcal{V}$.

Následující větu dokázal Bjarni Jónsson v roce 1967:

Věta 12.12. *Varieta $\mathcal{V}$ je distributivní, právě když pro některé $n \geq 1$ existují ternární termy $p_0(x,y,z), \ldots p_n(x,y,z)$ splňující:*
$p_0(x,y,z) = x$, $p_n(x,y,z) = z$
$p_i(x,y,x) = x$ *pro* $i = 0,1,\ldots,n$
$p_i(x,x,y) = p_{i+1}(x,x,y)$ *pro i sudé*
$p_i(x,y,y) = p_{i+1}(x,y,y)$ *pro i liché.*

D ů k a z: Nechť $\mathcal{V}$ je distributivní a $F_{\mathcal{V}}(x,y,z)$ je její volná algebra s generátory x, y, z. Pak je zřejmé, že platí

$$\langle x,z\rangle \in \Theta(x,z) \cap (\Theta(x,y) \vee \Theta(y,z)) ,$$

a tedy také $\langle x,z\rangle \in [\Theta(x,z) \cap \Theta(x,y)] \vee [\Theta(x,z) \cap \Theta(y,z)]$. Tedy existují $p_1,\ldots,p_n \in F_{\mathcal{V}}(x,y,z)$ (tj. $p_i = p_i(x,y,z)$ je 3-ární term) tak, že

$$x[\Theta(x,z) \cap \Theta(x,y)]p_1[\Theta(x,z) \cap \Theta(y,z)]p_2 \ldots p_{n-1}[\Theta(x,z) \cap \Theta(y,z)]z.$$

Postupem analogickým jako v důkaze Věty 12.6., tj faktorizací volné algebry, odtud obdržíme identity (2).

Obráceně, nechť Θ, Φ, $\Psi \in Con\mathcal{A}$, $\mathcal{A} \in \mathcal{V}$, $\mathcal{V}$ splňuje předepsané identity pro ternární termy $p_1,\ldots,p_n$. Zřejmě stačí dokázat $\Phi \cap (\Psi \vee \Theta) \subseteq (\Phi \cap \Psi) \vee (\Phi \cap \Theta)$. Nechť tedy $\langle a,b\rangle \in \Phi \cap (\Psi \vee \Theta)$. Pak $\langle a,b\rangle \in \Phi$, a dle Věty 8.2. existují $c_1,\ldots,c_k \in A$ tak, že

$$\langle a,c_1\rangle \in \Psi,\ \langle c_1,c_2\rangle \in \Theta,\ \langle c_2,c_3\rangle \in \Psi,\ldots,\langle c_k,b\rangle \in \Theta.$$

Pro $i = 0,1,\ldots,n$ tedy dostaneme

$$p_i(a,a,b)\Psi p_i(a,c_1,b)\Theta p_i(a,c_2,b)\Psi \ldots p_i(a,b,b) .$$

Položme $c_0 = a$, $c_{k+1} = b$. Pak ze vztahu $\langle a,b\rangle \in \Phi$ a z identit věty plyne

$$p_i(a,c_j,b)\Phi p_i(a,c_j,a) = a = p_i(a,c_{j+1},a)\Phi p_i(a,c_{j+1},b) ,$$

t.j.

$$\langle p_i(a,c_j,b), p_i(a,c_{j+1},b)\rangle \in \Phi$$

pro každé i a pro $j = 0, \ldots, k$. Dohromady tedy:

$$p_i(a,a,b)(\Phi \cap \Psi)p_i(a,c_1,b)(\Phi \cap \Theta)p_i(a,c_2,b) \ldots p_i(a,b,b),$$

tedy

$$\langle p_i(a,a,b), p_i(a,b,b)\rangle \in (\Phi \cap \Psi) \vee (\Phi \cap \Theta).$$

V důsledku identit odtud dostaneme

$$a = p_0(a,a,b) = p_1(a,a,b)[(\Phi \cap \Psi) \vee (\Phi \cap \Theta)]p_1(a,b,b) =$$

$$= p_2(a,b,b)[(\Phi\cap\Psi)\vee(\Phi\cap\Theta)]p_2(a,a,b) = p_3(a,a,b)[(\Phi\cap\Psi)\vee(\Phi\cap\Theta)] \ldots = b\,,$$

tedy

$$\langle a, b\rangle \in (\Phi \cap \Psi) \vee (\Phi \cap \Theta).$$

□

Důsledek: *Nechť $\mathcal{V}$ je varieta, ve které existuje tzv. majoritní term, tj. ternární term $m(x,y,z)$ splňující $m(x,x,y) = m(x,y,x) = m(y,x,x) = x$. Pak $\mathcal{V}$ je distributivní.*

Důkaz: Položme $n = 2$ a $p_0(x,y,z) = x$, $p_2(x,y,z) = z$, $p_1(x,y,z) = m(x,y,z)$. Pak zřejmě $p_i(x,y,x) = x$ pro $i = 0,1,2$ a pro i sudé (tj $i = 0$) platí

$$p_0(x,x,y) = x = m(x,x,y) = p_1(x,x,y),$$

pro i liché (tj. $i = 1$) platí

$$p_1(x,y,y) = m(x,y,y) = y = p_2(x,y,y).$$

Z Věty 12.12. plyne již tvrzení. □

Příklady:

(1) Každá varieta svazů je distributivní. Stačí zvolit

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

a použít předchozí Důsledek.

(2) Odtud ihned plyne, že také varieta Booleových algeber je distributivní.

(3) Varieta implikativních algeber je distributivní.

Položme $n = 3$, $p_0(x,y,z) = x$, $p_1(x,y,z) = (y \cdot (z \cdot x)) \cdot x$, $p_2(x,y,z) = (x \cdot y) \cdot z$, $p_3(x,y,z) = z$. Pak platí

$$p_0(x,y,x) = x$$

$$p_1(x,y,x) = (y \cdot (x \cdot x)) \cdot x = (y \cdot 1) \cdot x = x$$
$$p_2(x,y,x) = (x \cdot y) \cdot x = x$$
$$p_3(x,y,x) = x,$$

a dále, pro i sudé:

$$p_0(x,x,y) = x = 1 \cdot x = (y \cdot 1) \cdot x = (y(xx))x = (x \cdot (y \cdot x)) \cdot x = p_1(x,x,y)$$

$$p_2(x,x,y) = (x \cdot x) \cdot y = y = p_3(x,x,y) \ ,$$

pro i liché:

$$p_1(x,y,y) = (y \cdot (y \cdot x)) \cdot x = (y \cdot x) \cdot x = (x \cdot y) \cdot y = p_2(x,y,y).$$

Nazvěme algebru $\mathcal{A}$ *modulární*, je-li modulární její svaz kongruencí $Con\,\mathcal{A}$. Varieta $\mathcal{V}$ je *modulární*, má-li tuto vlastnost každá $\mathcal{A} \in \mathcal{V}$. Uvedeme bez důkazu následující charakterizaci (kde podmínku (2) dokázal v roce 1969 A. Day, podmínku (3) pak v roce 1981 H.-P. Gumm):

Věta 12.13. *Nechť $\mathcal{V}$ je varieta, pak je ekvivalentní:*
(1) *$\mathcal{V}$ je modulární;*
(2) *existuje $n \geq 1$ a 4-ární termy $m_0, \ldots, m_n$ tak, že platí:*
$m_0(x,y,z,v) = x, \quad m_n(x,y,z,v) = v$
$m_i(x,y,y,x) = x$, *pro* $i = 0,1,\ldots,n$
$m_i(x,y,y,z) = m_{i+1}(x,y,y,z)$ *pro i sudé*
$m_i(x,x,y,y) = m_{i+1}(x,x,y,y)$ *pro i liché;*
(3) *existuje $n \geq 1$ a ternární termy t, $p_0, \ldots, p_n$ tak, že platí:*
$p_0(x,y,z) = x$
$p_i(x,y,x) = x$ *pro* $i = 0,1,\ldots,n$
$p_i(x,x,y) = p_{i+1}(x,x,y)$ *pro i sudé,* $i \leq n-1$
$p_i(x,y,y) = p_{i+1}(x,y,y)$ *pro i liché,* $i \leq n-1$
$p_n(x,y,y) = t(x,y,y)$,
$t(x,x,y) = y$.

Z podmínky (3) je patrné, že termy pro modularitu tvoří "slepenec" Jónssonových termů $p_0, \ldots p_n$ pro distributivitu a Mal'cevova termu t pro permutabilitu. Pro důkaz (2) se použije obvyklá procedura jako ve větě 12.6. nebo 12.12., důkaz (3) ale není takto konstruován a je založen na poměrně obtížné teorii tzv. *komutátorů* kongruencí (tento pojem zavedl J. D. H. Smith v roce 1976, teorii rozvinuli J. Hagemann, Ch. Herrmann, R. Freese a R. McKenzie).

Algebru $\mathcal{A}$ nazveme *aritmetická*, je-li $\mathcal{A}$ současně distributivní a permutabilní. Varieta $\mathcal{V}$ je *aritmetická*, má-li tuto vlastnost každá $\mathcal{A} \in \mathcal{V}$. Jak jsme již viděli v předchozích příkladech, je každá Booleova algebra aritmetická. Variety aritmetické charakterizoval v roce 1963 A. F. Pixley:

Věta 12.14. *Varieta $\mathcal{V}$ je aritmetická, právě když ve $\mathcal{V}$ existuje ternární term $t(x,y,z)$ splňující identity: $t(x,x,z)=z$, $t(x,y,x)=x$, $t(x,z,z)=x$.*

Důkaz: Jestliže ve $\mathcal{V}$ existuje term t splňující uvedené identity, pak $\mathcal{V}$ je zřejmě permutabilní, netoť t je Mal'cevův term, a $\mathcal{V}$ je distributivní, stačí položit $n=2$, $p_0(x,y,z)=x$, $p_1(x,y,z)=t(x,t(x,y,z),z)$, $p_2(x,y,z)=z$, tj. $\mathcal{V}$ je aritmetická.

Obráceně, nechť $\mathcal{V}$ je aritmetická, $F_{\mathcal{V}}(x,y,z)$ její volná algebra s generátory x, y, z. Podle Věty 12.3. je $\Theta \vee \Phi = \Theta \circ \Phi$ pro každé dvě kongruence Θ, Φ na $F_{\mathcal{V}}(x,y,z)$, zřejmě

$$\langle x,z\rangle \in \Theta(x,z) \cap (\Theta(x,y) \circ \Theta(y,z)),$$

a tedy z distributivity plyne

$$\langle x,z\rangle \in [\Theta(x,z) \cap \Theta(x,y)] \circ [\Theta(x,z) \cap \Theta(y,z)].$$

Tedy existuje $q=q(x,y,z) \in F_{\mathcal{V}}(x,y,z)$ tak, že

$$\langle x,q(x,y,z)\rangle \in \Theta(x,z) \cap \Theta(x,y)$$

$$\langle q(x,y,z),z\rangle \in \Theta(x,z) \cap \Theta(y,z).$$

Neboli ve faktorové algebře $F_{\mathcal{V}}(x,y,z)/\Theta(x,y)$ platí

$$x=q(x,x,z)$$

a ve faktorové algebře $F_{\mathcal{V}}(x,y,z)/\Theta(x,z)$ platí

$$x=q(x,y,x).$$

Jelikož $\mathcal{V}$ je permutabilní, existuje ve $\mathcal{V}$ Mal'cevův term $p(x,y,z)$. Položme nyní $t(x,y,z)=p(x,q(x,y,z),z)$. Snadno nahlédneme, že $t(x,y,z)$ splňuje požadované identity. $\square$

Příklad: Pro Booleovy algebry lze položit

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

Poznámka: Ve větách 12.6., 12.9., 12.12., 12.13., a 12.14. jsme charakterizovali variety, jejichž kongruence splňují některou kongruenční identitu, pomocí existence termů, splňujících jisté identity; takové podmínce se, na počest prvního algebraika, který uvedený postup objevil, říká *mal'evovská* *podmínka*. V 70-tých letech se někteří algebraici zabývali problémem, zda lze takto charakterizovat i jiné identity než výše uvedené. Nezávisle na sobě dokázali v letech 1973–74 W. D. Neumann a W. Taylor, že pro každou kongruenční identitu existuje maL'cevovská podmínka, charakterizující variety s touto kongruenční podmínkou. Ukázalo se však, že pomocí mal'cevovských podmínek lze charakterizovat i jiné kongruenční vlastnosti než identity.

Jsou-li $\mathcal{A}$, $\mathcal{B}$ algebry téhož typu a $\Theta_A \in Con\,\mathcal{A}$, $\Theta_B \in Con\,\mathcal{B}$, pak zřejmě $\Theta_A \times \Theta_B \in Con\,\mathcal{A} \times \mathcal{B}$, kde $\Theta_A \times \Theta_B$ je na $A \times B$ definována takto:

$$\langle [x_1, x_2], [y_1, y_2] \rangle \in \Theta_A \times \Theta_B \Leftrightarrow \langle x_1, y_1 \rangle \in Con\,\mathcal{A} \text{ a } \langle x_2, y_2 \rangle \in \Theta_{\mathcal{B}}.$$

Zavedeme následující pojem: Nechť K je třída algeber téhož typu. Řekneme, že K má *direktně rozložitelné kongruence*, jestliže pro každé $\mathcal{A}$, $\mathcal{B} \in K$ a libovolnou $\Theta \in Con\,\mathcal{A} \times \mathcal{B}$ existují $\Theta_A \in Con\,\mathcal{A}$, $\Theta_B \in Con\,\mathcal{B}$ tak, že platí $\Theta = \Theta_A \times \Theta_B$.

Označme symbolem Π_1, Π_2 tzv. *projekční kongruence* na direktním součinu $\mathcal{A} \times \mathcal{B}$, tj. Π_1, Π_2 jsou indukované projekcemi $pr_1 : \mathcal{A} \times \mathcal{B} \to \mathcal{A}$, $pr_2 : \mathcal{A} \times \mathcal{B} \to \mathcal{B}$, neboli $\Pi_1 = \omega_A \times \iota_B$, $\Pi_2 = \iota_A \times \omega_B$.

V roce 1970 dokázali G. A. Fraser a A. Horn:

Věta 12.15. *Nechť K je třída algeber téhož typu uzavřená na direktní součiny. Pak je ekvivalentní:*

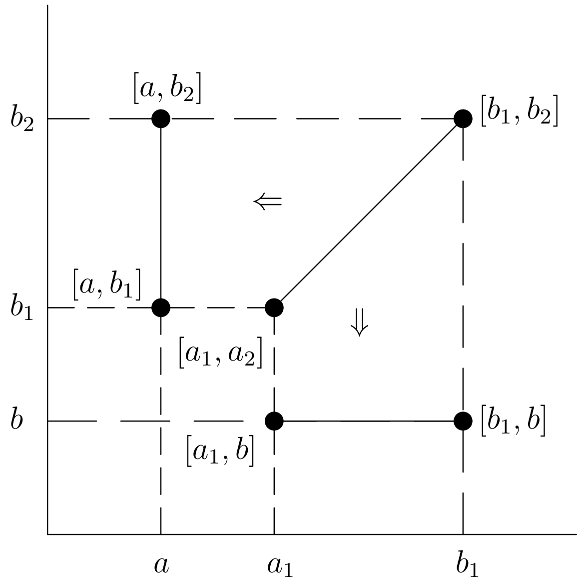
(1) *K má direktně rozložitelné kongruence;*

(2) $\Pi_2 \cap (\Pi_1 \vee \Theta) \subseteq \Theta$, $\Pi_1 \cap (\Pi_2 \vee \Theta) \subseteq \Theta$ *pro každé $\mathcal{A}$, $\mathcal{B} \in K$ a libovolnou $\Theta \in Con\,\mathcal{A} \times \mathcal{B}$;*

(3) *pro každé a, a_1, $b_1 \in \mathcal{A} \in K$, b, a_2, $b_2 \in \mathcal{B} \in K$*

$$\langle [a_1, a_2], [b_1, b_2] \rangle \in \Theta \Rightarrow \langle [a_1, b], [b_1, b] \rangle \in \Theta \; a \; \langle [a, a_2], [a, b_2] \rangle \in \Theta.$$

Podmínku (3) lze graficky znázornit takto:



Obr.20

D ů k a z : Nejdříve dokážeme pomocné tvrzení (T):
Jestliže $\mathcal{A}$, $\mathcal{B}$ *jsou téhož typu a* Θ_1, $\Phi_1 \in Con\,\mathcal{A}$, Θ_2, $\Phi_2 \in Con\,\mathcal{B}$, *pak*

$$(\Phi_1 \times \Phi_2) \vee (\Theta_1 \times \Theta_2) = (\Phi_1 \vee \Theta_1) \times (\Phi_2 \vee \Theta_2).$$

Důkaz tvrzení (T): Zřejmě

$$\Phi_1 \times \Phi_2 \subseteq (\Phi_1 \vee \Theta_1) \times (\Phi_2 \vee \Theta_2)$$

$$\Theta_1 \times \Theta_2 \subseteq (\Phi_1 \vee \Theta_1) \times (\Phi_2 \vee \Theta_2),$$

a tedy teké

$$(\Phi_1 \times \Phi_2) \vee (\Theta_1 \times \Theta_2) \subseteq (\Phi_1 \vee \Theta_1) \times (\Phi_2 \vee \Theta_2).$$

Obráceně, nechť $\langle a, b \rangle \in (\Phi_1 \vee \Theta_1) \times (\Phi_2 \vee \Theta_2)$. Pak

$$a = [a_1, a_2] \in \Phi_1 \circ \Theta_1 \circ \Phi_1 \circ \ldots \text{ (2m činitelů)}$$

$$b = [b_1, b_2] \in \Phi_2 \circ \Theta_2 \circ \Phi_2 \circ \ldots \text{ (2m činitelů).}$$

Odtud

$$\langle a, b \rangle \in (\Phi_1 \circ \Theta_1 \circ \Phi_1 \circ \ldots) \times (\Phi_2 \circ \Theta_2 \circ \Phi_2 \circ \ldots) =$$
$$= (\Phi_1 \times \Phi_2) \circ (\Theta_1 \times \Theta_2) \circ (\Phi_1 \times \Phi_2) \circ \ldots \subseteq (\Phi_1 \times \Phi_2) \vee (\Theta_1 \times \Theta_2).$$

Nyní již dokážeme Větu 12.15.

(1) $\Rightarrow$ (2): Je-li $\Theta = \Theta_{\mathcal{A}} \times \Theta_{\mathcal{B}}$, pak dle (T) platí $\Pi_2 \cap (\Pi_1 \vee \Theta) = \Pi_2 \cap ((\omega_A \times \iota_B) \vee (\Theta_A \times \Theta_B)) = (\iota_A \times \omega_B) \cap (\Theta_A \times \iota_B) = \Theta_A \times \omega_B \subseteq \Theta$, analogicky $\Pi_1 \cap (\Pi_2 \vee \Theta) \subseteq \Theta$.

(2) $\Rightarrow$ (3): Nechť $\langle [a_1, a_2], [b_1, b_2] \rangle \in \Theta$. Jelikož $\langle [a_1, b], [a_1, a_2] \rangle \in \Pi_1$, $\langle [b_1, b_2], [b_1, b] \rangle \in \Pi_1$, platí $\langle [a_1, b], [b_1, b] \rangle \in \Pi_1 \circ \Theta \circ \Pi_1 \subseteq \Pi_1 \vee \Theta$, a tedy $\langle [a_1, b], [b_1, b] \rangle \in \Pi_2 \cap (\Pi_1 \vee \Theta)$. Dle (2) odtud plyne $\langle [a_1, b], [b_1, b] \rangle \in \Theta$. Analogicky se dokáže druhý vztah.

(3) $\Rightarrow$ (1): Položme

$$\Theta_A = \{\langle a_1, b_1 \rangle; \text{ existuje } b \in B \text{ tak, že } \langle [a_1, b], [b_1, b] \rangle \in \Theta\}$$

$$\Theta_B = \{\langle a_2, b_2 \rangle; \text{ existuje } a \in A \text{ tak, že } \langle [a, a_2], [a, b_2] \rangle \in \Theta\} .$$

Dle (3) platí

$$\langle [a_1, a_2], [b_1, a_2] \rangle \in \Theta$$

$$\langle [b_1, a_2], [b_2, a_2] \rangle \in \Theta,$$

z tranzitivity Θ odtud plyne

$$\langle [a_1, a_2], [b_1, b_2] \rangle \in \Theta,$$

tj. $\Theta_A \times \Theta_B \subseteq \Theta$. Obrácená inkluze je triviální, tedy platí (1). □

Důsledek: *Je-li $\mathcal{V}$ distributivní varieta, pak má $\mathcal{V}$ direktně rozložitelné kongruence.*

D ů k a z: Jelikož $\Pi_1 \cap \Pi_2 = \omega_{A \times B}$, pak (2) z Věty 12.15. plyne ihned z distributivity svazu $Con\mathcal{A} \times \mathcal{B}$. □

Příklad: Každá varieta svazů má direktně rozložitelné kongruence.

Poznámka: V roce 1970 charakterizovali variety s direktně rozložitelnými kongruencemi Fraser a Horn pomocí mal'cevovské podmínky. Tato podmínka je však velice komplikovaná a prakticky nepoužitelná pro aplikace. V případě permutabilních variet lze určit příslušnou Mal'cevovskou podmínku v mnohem jednodušším tvaru:

Věta 12.16. (I. Chajda, J. Duda) *Nechť $\mathcal{V}$ je varieta. Pak $\mathcal{V}$ je permutabilní a má direktně rozložitelné kongruence, právě když existuje $(n+1)$-ární term p a binární termy $s_1, t_1, \ldots, s_n, t_n$ tak, že platí identity:*

$$x = p(x, s_1(x, y), \ldots, s_n(x, y))$$

$$x = p(y, s_1(x, y), \ldots, s_n(x, y))$$

$$x = p(y, t_1(x, y), \ldots, t_n(x, y))$$
$$y = p(x, t_1(x, y), \ldots, t_n(x, y)) \ .$$

Příklad: Varieta všech okruhů s jednotkou má permutabilní a direkntě rozložitelné kongruence. Stačí zvolit $n = 2$, $p(x, y, z) = x \cdot y + z$, $s_1(x, y) = 0$, $s_2(x, y) = x$, $t_1(x, y) = -1$, $t_2(x, y) = x + y$.

Poznámka: J. Duda tento výsledek zobecnil i pro n-permutabilní variety (příklad 3-permutabilní variety s direktně rozložitelnými kongruencemi je varieta implikativních algeber) a v roce 1989 odvodil novou mal'cevovskou podmínku pro direktní rozložitelnost kongruencí, která je podstatně jednodušší než původní pomínka Frasera a Horna.

Další důležitou kongruenční podmínkou je tzv. *regularita*: algebra $\mathcal{A} = (A, F)$ je *regulární*, jestliže pro každé Θ, $\Phi \in Con\,\mathcal{A}$ a libovolné $a \in A$ platí

$$[a]_\Theta = [a]_\Phi \ \text{ implikuje } \ \Theta = \Phi \ .$$

Neboli, algebra $\mathcal{A}$ je regulární, je-li každá její kongruence jednoznačně určená svojí libovolnou třídou. Varietu $\mathcal{V}$ nazveme *regulární*, má-li tuto vlastnost každá $\mathcal{A} \in \mathcal{V}$.

Mal'cevovskou podmínku pro regularitu variety $\mathcal{V}$ odvodili v roce 1970 nezávisle na sobě B. Csákány, G. Grätzer a R. Wille. Tato podmínka je ale dosti komplikovaná. Pro praktické použití je výhodnější jiná podmínka, podobná podmínce mal'cevovské, kterou odvodil B. Csákány:

Věta 12.17. *Varieta $\mathcal{V}$ je regulární, právě když ve $\mathcal{V}$ existují ternární termy $p_1(x, y, z), \ldots, p_n(x, y, z)$ tak, že platí:*

$$[p_1(x, y, z) = z, \ \ldots \ , p_n(x, y, z) = z] \ \Rightarrow \ x = y.$$

Příklady:

(1) Pro variety grup lze volit $n = 1$, $p_1(x, y, z) = x \cdot y^{-1} \cdot z$

(2) Pro okruhy lze volit $n = 1$, $p_1(x, y, z) = x - y + z$

(3) Pro Booleovy algebry lze volit $n = 1$,

$$p_1(x, y, z) = (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y \wedge z).$$

Pro permutabilní a regulární variety lze získat jednoduchou mal'cevovskou podmínku (I. Chajda, J. Duda, 1980):

Věta 12.18. *Pro varietu $\mathcal{V}$ je ekvivalentní:*

(1) *$\mathcal{V}$ je regulární a permutabilní;*

(2) *existuje* $n \geq 1$, $(3+n)$*-ární term* p *a ternární termy* $t_1, \dots, t_n$ *tak, že platí*
$t_i(x,x,z) = z$ *pro* $i = 1, \dots, n$
$x = p(x,y,z,t_1(x,y,z), \dots, t_n(x,y,z))$
$y = p(x,y,z,z,\dots,z)$.

Příklad: Pro varietu grup lze volit $n = 1$, $t_1(x,y,z) = z \cdot y^{-1} \cdot x$, $p(x,y,z,v) = y \cdot z^{-1} \cdot v$. Pak vskutku
$p(x,y,z,t_1(x,y,z)) = y \cdot z^{-1} \cdot (z \cdot y^{-1} \cdot x) = x$
$p(x,y,z,z) = y \cdot z^{-1} \cdot z = y$.

Ve zbývající části této kapitoly ukážeme, jak některé z uvedených kongruenčních vlastností ovlivňují strukturu dané variety.

Nejprve se soustředíme na strukturu distributivních variet.

Nechť $\mathcal{V}$ je varieta, nechť $\mathcal{A}_i \in \mathcal{V}$ pro $i \in I \neq \emptyset$. Jelikož $(Exp\ I; \cup, \cap, ', \emptyset, I)$ je Booleova algebra, můžeme na ní uvažovat některý ultafiltr U (viz Dodatek v kapitole svazů). Na algebře $\mathcal{A} = \prod\{\mathcal{A}_i; i \in I\}$ zaveďme relaci Θ_U takto:

$$\langle a, b\rangle \in \Theta_U, \text{ právě když } \{i \in I; pr_i\, a = pr_i\, b\} \in U\ .$$

Snadno nahlédneme, že $\Theta_U \in Con\, \mathcal{A}$. Označme symbolem $\prod \mathcal{A}_i/U$ faktorovou algebru $\mathcal{A}/\Theta_U$ a nazvěme ji *ultrasoučinem* algeber $\mathcal{A}_i (i \in I)$ *dle ultrafiltru* U.

Pro a, $b \in \prod\{\mathcal{A}_i; i \in I\}$ zřejmě platí

$$[a]_{\Theta_U} = [b]_{\Theta_U} \quad , \text{ právě když } \ \{i \in I; pr_i\, a = pr_i\, b\} \in U\ .$$

Pro stručnost budeme místo $\{i \in I; pr_i\, a = pr_i\, b\}$ zapisovat jen $[|a = b|]$.

Lemma 12.19. *Nechť* $I \neq \emptyset$ *a* $W \subseteq Exp\, I$, $W \neq \emptyset$ *tak, že*
(i) $I \in W$
(ii) *jestliže* $J \in W$ *a* $J \subseteq K \subseteq I$, *pak* $K \in W$
(iii) *jestliže* $J_1 \cup J_2 \in W$, *pak* $J_1 \in W$ *nebo* $J_2 \in W$.
Pak existuje ultrafiltr U *na* I *tak, že* $U \subseteq W$.

Důkaz: Jestliže $\emptyset \in W$, pak $W = Exp\, I$, a tedy pro každý ultrafiltr U platí $U \subseteq W$. Jestliže $\emptyset \notin W$, pak snadno ověříme, že $Exp\, I \setminus W$ je vlastní ideál. Dle Lemma D.3 dostaneme tvrzení. □

Definice: Označme sybolem $P_U(K)$ třídu všech ultrasoučinů třídy K. Označme $P_S(K)$ třídu všech subdirektních součinů algeber z K.

Věta 12.20.(Jónssonovo lemma) *Nechť* K *je třída algeber téhož typu a varieta* $\mathcal{V}(K)$ *je distributivní. Pak* $\mathcal{A} \in \mathcal{V}(K)$ *je subdirektně irreducibilní, právě když* $\mathcal{A} \in HSP_U(K)$.

D ů k a z : Nechť $\mathcal{A}$ je subdirektně irreducibilní algebra ve varietě $\mathcal{V}(K)$. Jestliže $\mathcal{A}_i \in K$ pro $i \in I$ a $\mathcal{B}$ je podalgebra direktního součinu $\prod\{\mathcal{A}_i; i \in I\}$, pak existuje surjektivní homomorfismus $h : \mathcal{B} \to \mathcal{A}$ (neboť $\mathcal{V}(K) = HSP(K)$). Nechť $\Theta = \Theta_h$. Pro $J \subseteq I$ položme

$$\Theta_J = \{\langle a, b\rangle \in \Pi\{\mathcal{A}_i; i \in I\} \times \Pi\{\mathcal{A}_i; i \in I\}, J \subseteq [|a = b|]\}.$$

Snadno nahlédneme, že Θ_J je kongruence na $\Pi\{\mathcal{A}_i; i \in I\}$. Nechť $\Theta_{J|B} = \Theta_J \cap (B \times B)$ je restrikce Θ_J na B. Definujme $W = \{J \subseteq I; \Theta_{J|B} \subseteq \Theta\}$. Zřejmě $I \in W$ a $\emptyset \notin W$, jestliže $J \in W$ a $J \subseteq K \subseteq I$, pak $\Theta_{K|B} \subseteq \Theta$, neboť $\Theta_{K|B} \subseteq \Theta_{J|B}$. Předpokládejme $J_1 \cup J_2 \in W$. Pak $\Theta_{(J_1 \cup J_2)|B} \subseteq \Theta$, avšak $\Theta_{J_1 \cup J_2} = \Theta_{J_1} \cap \Theta_{J_2}$, neboli $\Theta_{(J_1 \cup J_2)|B} = \Theta_{J_1|B} \cap \Theta_{J_2|B}$. Jelikož $\Theta = \Theta \vee (\Theta_{J_1|B} \cup \Theta_{J_2|B})$, z distributivity plyne

$$\Theta = (\Theta \vee \Theta_{J_1|B}) \cup (\Theta \vee \Theta_{J_2|B}) \qquad \text{(v)}$$

Podle Věty 8.13. platí $Con\,\mathcal{B}/\Theta \cong [\Theta, B \times B] \subseteq Con\,\mathcal{B}$. Jelikož $\mathcal{B}/\Theta \cong \mathcal{A}$, musí být $\mathcal{B}/\Theta$ subdirektivně irreducibilní. Tedy $Con\,\mathcal{B}/\Theta$, a tedy i $[\Theta, B \times B]$ má jediný atom. Ze vztahu (v) odtud plyne $\Theta = \Theta \vee \Theta_{J_i|B}$, kde buď $i = 1$ nebo $i = 2$, tj $\Theta_{J_i|B} \subseteq \Theta$, takže buď J_1 nebo J_2 patří do W. Dle Lemma 12.19. tedy existuje ultrafiltr $U \subseteq W$. Z definice W pak dostaneme $\Theta_{U|B} \subseteq \Theta$, jelikož $\Theta_U = \cup\{\Theta_J; J \in U\}$.
Nechť nyní p je přirozený homomorfismus $\Pi\{\mathcal{A}_i; i \in I\}$ na $\Pi\mathcal{A}_i/U$, nechť $q : \mathcal{B} \to p(\mathcal{B})$ je restrikce p na $\mathcal{B}$. Pak $\Theta_q = \Theta_{U|B} \subseteq \Theta$. Tedy $\mathcal{A} \cong \mathcal{B}/\Theta \cong (\mathcal{B}/\Theta_q)/(\Theta/\Theta_q)$ dle 1.věty o izomorfismu. Avšak $\mathcal{B}/\Theta_q \cong p(\mathcal{B})$, což je podalgebra $\prod \mathcal{A}_i/U$, tedy $\mathcal{B}/\Theta_q \in ISP_U(K)$, odtud $\mathcal{A} \in HSP_U(K)$. □

Důsledek: *Je-li $\mathcal{V}(K)$ distributivní varieta, pak $\mathcal{V}(K) = IP_SHSP_U(K)$. Je-li nadto K konečná množina konečných algeber, pak $\mathcal{V}(K) = IP_SHS(K)$, a je-li $\mathcal{A} \in \mathcal{V}(K)$ subdirektivně irreducibilní, pak $\mathcal{A} \in HS(K)$.*

D ů k a z : Jelikož každá algebra ve $\mathcal{V}(K)$ je subdirektním součinem (tj. podalgebrou direktního součinu) subdirektně irreducibilních algeber, je z třídy $IP_S(C)$, kde C je třída subdirektně irreducibilních algeber z $\mathcal{V}(K)$. Z Věty 12.20. ihned plyne $\mathcal{V}(K) = IP_SHSP_U(K)$.

Dále, je-li K konečná množina konečných algeber, pak také I je konečná množina. Dle Věty D.8. je každý ultrafiltr hlavní, tj. $U = F(i)$ pro některé $i \in I$. Je-li tedy U ultrafiltr konečné množiny $I = \{1, \ldots, n\}$, pak existuje $i_0 \in I$ tak, že $\prod \mathcal{A}_i/U \cong \mathcal{A}_{i_0}$. Dle Věty 12.20. je tedy každá algebra z $P_U(K)$ izomorfní některé algebře z K, tj. $HSP_U(K) = HS(K)$. Odtud již plyne druhé tvrzení. □

Poznámka: Zdánlivě nám Věta 12.20. komplikuje strukturu variety, neboť dle Birkhoffovy věty je $\mathcal{V}(K) = HSP(K)$, ale dle Jónssonova lemmatu je pro distributivní variety $\mathcal{V}(K) = IP_S HSP_U(K)$. Často však pracujeme s varietami, generovanými konečnou množinou konečných algeber K. Pak ale v případě distributivní variety hledáme subdirektně irreducibilní algebry jen mezi faktorovými algebrami podalgeber z K, které jsou tedy rovněž konečné, a je jich rovněž konečný počet. To je značná výhoda, neboť celý postup je potom konstruktivní.

Speciální případ nastane, je-li varieta $\mathcal{V}(K)$ generovaná jedinou algebrou $\mathcal{A}$, která je navíc jednoduchá (tj. $Con\,\mathcal{A} = \{\omega, \iota\}$). Pak subdirektně irreducibilní algebry patří jen mezi podalgebry algebry $\mathcal{A}$, tj. do třídy $S(\mathcal{A})$, což je (v případě konečné $\mathcal{A}$) velice jednoduché.

Typický příklad:

(1) Varieta $\mathcal{D}$ všech distributivních svazů je distributivní a je generována dvouprvkovým řetězcem C_2, který je jediný subdirektně irreducibilní svaz v $\mathcal{D}$, nadto je jednoduchý. Tedy $\mathcal{D} = IP_S(C_2)$, tj. dostaneme ihned Větu 9.9.

(2) Analogicky, je-li B_2 dvouprvková Booleova algebra, pak pro varietu $\mathcal{V}$ Booleových algeber platí $\mathcal{B} = IP_S(B_2)$.

Čtenář snadno nahlédne, oč je toto vyjádření jednodušší, než pomocí operátorů H, S, P.

Poznámka: Poněkud slabší výsledek lze získat i pro modulární variety, což dokázal R. Freese, ovšem za použití tzv. teore komutátorů.

Řekneme, že varieta $\mathcal{V}$ je *konečně generovaná*, je-li $\mathcal{V} = \mathcal{V}(K)$, kde K je konečná třída konečných algeber. Dalším důsledkem Jónssonova lemmatu je:

Důsledek: *Každá distributivní konečně generovaná varieta má pouze konečně mnoho podvariet.*

Toto tvrzení plyne bezprostředně z faktu, že tato varieta má pouze konečně mnoho subdirektně irreducibilních algeber.

Poněkud překvapujícím faktem v universální algebře je skutečnost, že existují konečné algebry s konečnou množinou operací, které však nemají tzv. *konečnou basi identit*, tj. je-li $\mathcal{A}$ taková algebra, pak neexistuje *konečná* množina identit Σ tak, že $Id(\mathcal{V}(\mathcal{A})) = \Sigma^*$. První příklad takové algebry udal v roce 1954 R. Lyndon, v roce 1965 pak V. I. Murskij udal takový příklad tříprvkového grupoidu a ukázal, že nejmenší algebra této vlastnosti je tříprvková. V roce 1977 dokázal K. A. Baker, že tento "patologický případ" nemůže nastat, je-li varieta distributivní. Pro značnou zdlouhavost důkazu uvedeme tuto slavnou větu bez důkazu:

Věta 12.21. (Věta o konečné basi identit): *Je-li $\mathcal{V}$ distributivní konečně generovaná varieta konečného typu, pak má $\mathcal{V}$ konečnou basi identit.*

Důsledek: *Každý konečný svaz má konečnou basi identit.*

Poznámka: V roce 1987 dokázal R. McKenzie, že je-li $\mathcal{A}$ konečná algebra s konečnou množinou operací, a je-li $\mathcal{V}(\mathcal{A})$ modulární, a má-li $\mathcal{V}(\mathcal{A})$ pouze konečný počet subdirektně irreducibilních algeber, které jsou všechny konečné, pak $\mathcal{A}$ má konečnou basi identit. Dále dokázali R. McKenzie, R. Padmanabhan a R. Quackenbush následující tvrzení pro aritmetické variety:

Věta 12.22. *Má-li aritmetická varieta konečnou basi identit, pak má basi, sestávající se z jediné identity.*

Tedy např. varietu Booleových algeber lze zadat jedinou identitou.

Jako poslední téma této kapitoly bude studium struktury variet, které jsou permutabilní.

Věta 12.23. (I. Fleischer) *Nechť $\mathcal{V}$ je permutabilní varieta, nechť $\mathcal{A}$, $\mathcal{B} \in \mathcal{V}$ a nechť $\mathcal{C}$ je podalgebra direktního součinu $\mathcal{A} \times \mathcal{B}$. Označme $\mathcal{A}' = pr_1 \mathcal{C}$, $\mathcal{B}' = pr_2 \mathcal{C}$. Pak existují surjektivní homomorfismy $\alpha : \mathcal{A}' \to \mathcal{C}/\Theta$, $\beta : \mathcal{B}' \to \mathcal{C}/\Theta$, kde $\Theta = \prod_1 /\mathcal{C} \vee \prod_2 /\mathcal{C}$ tak, že*

$$\mathcal{C} = \{\langle a, b\rangle \in \mathcal{A}' \times \mathcal{B}'; \alpha(a) = \beta(b)\} \ .$$

D ů k a z: Definujme $\alpha : \mathcal{A}' \to \mathcal{C}/\Theta$ a $\alpha : \mathcal{B}' \to \mathcal{C}/\Theta$ jako homomorfismy, splňující

$$p = \alpha \cdot pr_1|_{\mathcal{C}} \quad , \quad p = \beta \cdot pr_2|_{\mathcal{C}} \quad ,$$

kde p je přirozený homomorfismus $\mathcal{C}$ na $\mathcal{C}/\Theta$. Pak

$$c = \langle pr_1 \, c, pr_2 \, c\rangle \in \mathcal{A}' \times \mathcal{B}'$$

a platí

$$\alpha(pr_1 \, c) = p(c) = \beta(pr_2 \, c) \ ,$$

a tedy

$$c \in \{\langle a, b\rangle \in \mathcal{A}' \times \mathcal{B}'; \alpha(a) = \beta(b)\} \ .$$

Obráceně, jestliže $\langle a, b\rangle \in \mathcal{A}' \times \mathcal{B}'$ a platí $\alpha(a) = \beta(b)$, pak nechť c_1, $c_2 \in \mathcal{C}$ a platí $pr_1 \, c_1 = a$, $pr_2 \, c_2 = b$. Pak

$$p(c_1) = \alpha(pr_1 \, c_1) = \alpha(a) = \beta(b) = \beta(pr_2 \, c_2) = p(c_2) \ ,$$

tj. $\langle c_1, c_2\rangle \in \Theta$, neboli $\langle c_1, c_2\rangle \in \prod_1 \cdot \prod_2$, jelikož $\mathcal{C}$ má permutabilní kongruence. Tedy existuje $d \in \mathcal{C}$ tak, že $\langle c_1, d\rangle \in \prod_1$, $\langle d, c_2\rangle \in \prod_2$, tj. $pr_1\, d = pr_1\, c_1 = a$, $pr_2\, d = pr_2\, c_2 = b$, odtud $d = \langle a, b\rangle$, neboli $\langle a, b\rangle \in \mathcal{C}$. To dokazuje

$$\mathcal{C} = \{\langle a, b\rangle \in \mathcal{A}' \times \mathcal{B}'; \alpha(a) = \beta(b)\}\ .$$

□

Důsledek (Foster–Pixley): *Nechť $\mathcal{V}$ je permutabilní varieta a $S_1, \ldots, S_n$ jsou jednoduché algebry z $\mathcal{V}$. Je-li $\mathcal{C}$ subdirektní součin $S_1, \ldots, S_n$, pak existuje $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ tak, že $\mathcal{C} \cong S_{i_1} \times \cdots \times S_{i_k}$.*

Definice: Algebra $\mathcal{A}$ je *poloprostá*, je-li izomorfní subdirektnímu součinu jednoduchých algeber. Varieta $\mathcal{V}$ je *poloprostá*, je-li poloprostá každá $\mathcal{A} \in \mathcal{V}$.

Lemma 12.24. *Varieta $\mathcal{V}$ je poloprostá, právě když je každá subdirektně irreducibilní algebra z $\mathcal{V}$ jednoduchá.*

Důkaz: Nechť $\mathcal{A} \in \mathcal{V}$ je subdirektně irreducibilní. pak jsou-li S_i $(i \in I)$ jednoduché algebry a $h : \mathcal{A} \to \prod\{S_i, i \in I\}$ je izomorfní vnoření, existuje zřejmě $i_0 \in I$ tak, že $pr_{i_0} \cdot h$ je izomorfismus $\mathcal{A}$ na S_{i_0}, tj. $\mathcal{A}$ je jednoduchá. Obrácené tvrzení je zřejmé, neboť každá algebra je izomorfní subdirektnímu součinu subdirektně irreducibilních algeber. □

Věta 12.25. (S. Burris) *Nechť $\mathcal{V}$ je distributivní varieta taková, že každá direktně nerozložitelná algebra ve $\mathcal{V}$ je subdirektně irreducibilní. Pak $\mathcal{V}$ je poloprostá.*

Důkaz: Nechť $\mathcal{A} \in \mathcal{V}$ je nejednoduchá subdirektně irreducibilní algebra, nechť Θ je nejmenší kongruence v $Con\,\mathcal{A}$ různá od ω (tj. atom). Tedy $\Theta \neq \mathcal{A} \times \mathcal{A}$. Pak Θ je podalgebra $\mathcal{A} \times \mathcal{A}$, tj. $\Theta \in \mathcal{V}$, a je direktně nerozložitelná algebra, která není subdirektně irreducibilní, jelikož $\varrho_1 \cap \varrho_2 = \omega$, kde $\varrho_i = \prod_i \cap \Theta^2$. □

Definice: Varieta $\mathcal{V}$ je *direktně representovatelná*, je-li konečně generovaná, a má-li konečný počet konečných direktně nerozložitelných algeber.

Definice: Algebra $\mathcal{A} = (A, F)$ je *uniformní*, jestliže pro každou $\Theta \in Con\,\mathcal{A}$ a libovolné a, $b \in A$ platí $card\,[a]_\Theta = card\,[b]_\Theta$. Varieta $\mathcal{V}$ je *uniformní*, má-li tuto vlastnost každá $\mathcal{A} \in \mathcal{V}$.

Příklad: Jak víme ze základního kursu, je každá grupa, každý okruh a každá Booleova algebra uniformní. Také každá kvazigrupa je uniformní. Avšak, viz Příklad za Větou 5.2., distributivní svazy už obecně uniformní nejsou.

Poznámka: V roce 1974 dokázal W. Taylor, že neexistuje mal'cevovská podmínka, charakterizující uniformní variety.

Bez důkazu uvedeme následující tvrzení, charakterizující strukturu důležitých tříd variet:

Věta 12.26. (Clark–Kraus) *Je-li* $\mathcal{V}$ *lokálně konečná varieta, jejíž konečné algebry jsou uniformní, pak* $\mathcal{V}$ *je permutabilní.*

Důsledek (McKenzie): *Je-li varieta* $\mathcal{V}$ *direktně representovatelná, pak je permutabilní.*

Věta 12.27. (Burris) *Nechť* $\mathcal{V}$ *je distributivní konečně generovaná varieta. Pak* $\mathcal{V}$ *je direktně representovatelná, právě když je poloprostá a aritmetická.*

VYBRANÉ KAPITOLY UNIVERSÁLNÍ ALGEBRY

13 EKVACIONÁLNÍ LOGIKA

V této kapitole budeme zkoumat vztahy mezi varietami a identitami na těchto varietách při použití jistých kongruencí na algebře termů.

Definice: Kongruence θ na algebře $\mathcal{A}$ se nazývá *FI-kongruence* (z anglického *fully invariant congruence*), jestliže pro každý homomorfismus $h : \mathcal{A} \to \mathcal{A}$ (tzv. endomorfismus) platí:

$$\langle a, b\rangle \in \theta \Rightarrow \langle h(a), h(b)\rangle \in \theta\,.$$

Označme $Con_{FI}\mathcal{A}$ množinu všech FI-kongruencí na $\mathcal{A}$. FI-kongruence jsou tedy ty kongruence na $\mathcal{A}$, které mají substituční podmínku vzhledem k endomorfismům. Snadno lze dokázat, že $Con_{FI}\mathcal{A}$ je algebraický uzávěrový systém na $A \times A$, tedy pro každou množinu $S \subseteq A \times A$ existuje nejmenší FI-kongruence, obsahující S; označme ji $\theta_{FI}(S)$.

Nechť $Id(X)$ je množina všech identit v proměnných z X typu (F, σ), nechť $T(X)$ je algebra termů typu (F, σ). Označme τ bijekci $Id(X) \to T(X) \times T(X)$ definovanou takto:

$$\tau(p = q) = \langle p, q\rangle.$$

Věta 13.1. *Nechť K je třída algeber typu (F, σ) a X je množina proměnných. Pak $\tau(Id_K(X))$ je FI-kongruence na $T(X)$.*

D ů k a z : Jelikož $(p = p) \in Id_K(X)$, dále $(p = q) \in Id_K(X) \Rightarrow (q = p) \in Id_K(X)$, a také $(p = q)\,, (q = r) \in Id_K(X) \Rightarrow (p = r) \in Id_K(X)$, tedy $\tau(Id_K(X))$ je ekvivalence na $T(X)$. Dále, jestliže $f \in F$ je n-ární a $(p_i = q_i) \in Id_K(X))$ $(i = 1, \ldots, n)$, pak zřejmě také

$$(f(p_1, \ldots, p_n) = f(q_1, \ldots, q_n)) \in Id_K(X),$$

tedy $\tau(Id_K(X))$ je kongruence na $T(X)$. Nechť h je homomorfismus $T(X)$ do $T(X)$ a platí

$$(p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)) \in Id_K(X).$$

Snadno ověříme, že také

$$(p(h(x_1), \ldots, h(x_n))\,, (q(h(x_1), \ldots, h(x_n))) \in Id_K(X),$$

tedy $\tau(Id_K(X))$ je FI-kongruence. □

Věta 13.2. *Nechť X je množina proměnných a θ je FI-kongruence na $T(X)$. Nechť $p, q \in T(X)$. Pak $p = q$ platí v $T(X)/\theta$, právě když $\langle p, q\rangle \in \theta$, tedy $T(X)/\theta$ je volná algebra ve varietě $HSP(T(X)/\theta)$.*

Poznámka : Je-li $\mathcal{A}$ algebra, pak $HSP(\mathcal{A})$ je nejmenší varieta, obsahující algebru $\mathcal{A}$, t.j. třída všech homomorfních obrazů všech podalgeber všech direktních součinů (t.j. mocnin) algebry $\mathcal{A}$. Je to tedy nejmenší varieta, splňující všechny identity z $Id_{\mathcal{A}}(X)$.

Důkaz: Nechť $p = p(x_1, \ldots, x_n)$, $q = q(x_1, \ldots, x_n)$. Jestliže v $T(X)/\theta$ platí $p = q$, pak

$$p([x_1]_\theta, \ldots, [x_n]_\theta) = q([x_1]_\theta, \ldots, [x_n]_\theta), \quad \text{tedy}$$

$$[p(x_1, \ldots, x_n)]_\theta = [q(x_1, \ldots, x_n)]_\theta, \text{ t.j. } \langle p, q\rangle \in \theta.$$

Obráceně, nechť $r_1, \ldots, r_n \in T(X)$. Je-li $h : T(X) \to T(X)$ homomorfismus takový, že $h(x_i) = r_i$ $(i = 1, \ldots, n)$ (takový existuje, neboť $T(X)$ má vlastnost universálního zobrazení), pak

$$\langle p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)\rangle \in \theta \quad \text{implikuje}$$

$$\langle h(p(x_1, \ldots, x_n)), h(q(x_1, \ldots, x_n))\rangle \in \theta,$$

ale θ je FI-kongruence, tedy $\langle p(r_1, \ldots, r_n), q(r_1, \ldots, r_n)\rangle \in \theta$
odtud $p([r_1]_\theta, \ldots, [r_n]_\theta) = q([r_1]_\theta, \ldots, [r_n]_\theta)$, neboli $p = q$ platí v $T(X)/\theta$.

Nechť nyní $\langle p, q\rangle \in \theta$; to je ekvivalentní s tím, že $p = q$ platí v $T(X)/\theta$, což je ekvivalentní s tím, že $p = q$ platí v $HSP(T(X)/\theta)$, neboli $T(X)/\theta$ je volná algebra v $HSP(T(X)/\theta)$. □

Věta 13.3. *Nechť $\Sigma \subseteq Id(X)$. Pak existuje třída algeber K taková, že $\Sigma = Id_K(X)$, právě když $\tau(\Sigma)$ je FI-kongruence na $T(X)$.*

Důkaz: Implikace $\Rightarrow$ plyne z Věty 13.1. Obráceně, nechť $\tau(\Sigma) = \theta$ je FI-kongruence. Položme $K = \{T(X)/\theta\}$. Dle Věty 13.2. platí $p = q$ v K právě když $\langle p, q\rangle \in \theta$, což je ekvivalentní s $(p = q) \in \Sigma$. Tedy $\Sigma = Id_K(X)$. □

Definice: Podmnožina, identit $\Sigma \subseteq Id(X)$ se nazývá *ekvacionální teorie*, jestliže existuje třída algeber K taková, že $\Sigma = Id_K(X)$.

Důsledek: *Ekvacionální teorie (typu F) nad X tvoří algebraický svaz, který je izomorfní svazu $Con_{FI}T(X)$.*

Definice: Nechť X je množina proměnných a Σ množina identit typu F s proměnnými z X. Řekneme, že identita $p = q$ *je důsledkem* Σ, jestliže $p = q$ platí v každé algebře, ve které platí Σ.

Věta 13.4. *Nechť Σ je množina identit nad X a $p = q$ je identita nad X. Pak $p = q$ je důsledkem Σ právě když $\langle p, q\rangle \in \theta_{FI}(\tau(\Sigma))$.*

Důkaz: Plyne z Věty 13.1, 13.2, 13.3. □

Definice: Nechť p je term. *Subtermem termu* p se nazývá

(i) term p

(ii) Je-li $f(p_1, \dots, p_n)$ subterm termu p a $f \in F$ je n-ární, pak každý p_i je subterm p.

Definice: Množina identit Σ nad X je *uzavřená na substituci*, jestliže pro každou identitu $(p = q) \in \Sigma$ a libovolné $r \in T(X)$, jestliže nahradíme každý výskyt proměnné x v termech p,q termem r, pak opět získáme identitu ze Σ.

Množina identit Σ je *uzavřená na záměny*, jestliže pro každou $(p = q) \in \Sigma$ a libovolné $r \in T(X)$, jestliže je p subterm r, pak zaměníme-li p za q , dostaneme term s a platí $(r = s) \in \Sigma$.

Definice: Nechť Σ je množina identit nad X. *Deduktivní uzávěr* $D(\Sigma)$ množiny Σ je nejmenší podmnožina $Id(X)$ obsahující Σ taková, že platí:

$(p = p) \in D(\Sigma)$ pro každý term $p \in T(X)$
$(p = q) \in D(\Sigma) \Rightarrow (q = p) \in D(\Sigma)$
$(p = q)\, ,\, (q = r) \in D(\Sigma) \Rightarrow (p = r) \in D(\Sigma)$
$D(\Sigma)$ je uzavřená na substituce a na záměny.

Věta 13.5. *Nechť $\Sigma \subseteq Id(X)$ a $(p = q) \in Id(X)$. Pak $p = q$ je důsledkem Σ právě když $(p = q) \in D(\Sigma)$.*

Důkaz: Z definice $D(\Sigma)$ je zřejmé, že $\tau(D(\Sigma))$ je FI-kongruence, tedy $\tau(D(\Sigma)) \supseteq \theta_{FI}(\tau(\Sigma))$. Avšak $\tau^{-1}(\theta_{FI}\tau(\Sigma))$ splňuje zřejmě všechny vlastnosti deduktivního uzávěru a obsahuje Σ, odtud $\tau(D(\Sigma)) = \theta_{FI}(\tau(\Sigma))$. Neboli $p = q$ je důsledkem Σ právě když $\langle p, q\rangle \in \theta_{FI}(\tau(\Sigma))$ (dle Věty 13.4.), což je ekvivalentní s $(p = q) \in D(\Sigma)$. □

Definice: Nechť Σ je množina identit nad X. Pro $(p = q) \in Id(X)$ řekneme, že $p = q$ *je dokazatelné* ze Σ, jestliže existuje posloupnost $(p_1 = q_1), \dots, (p_n = q_n) \in Id(X)$ taková, že buď $(p_i = q_i) \in \Sigma$ nebo je tvaru $p = p$ nebo vznikla některým pravidlem z definice deduktivního uzávěru pomocí identit $(p_1 = q_1), \dots, (p_{i-1} = q_{i-1})$, přičemž $(p_n = q_n) = (p = q)$.

Posloupnost $(p_1 = q_1), \ldots, (p_n = q_n)$ se nazývá *formální dedukce* identity $p = q$, n je délka této dedukce.

Věta 13.6. **(Birkhoffova věta o úplnosti ekvacionální logiky).** *Nechť $\Sigma \subseteq Id(X)$ a $(p = q) \in Id(X)$. Pak $p = q$ je důsledkem Σ tehdy a jen tehdy, když $p = q$ je dokazatelná ze Σ.*

Důkaz: Je zřejmé, že když $p = q$ je dokazatelná ze Σ, pak $(p = q) \in D(\Sigma)$, t.j. $p = q$ je důsledkem Σ. Dokážeme obrácenou implikaci. Zřejmě $p = q$ je dokazatelná ze Σ pro každou $(p = q) \in \Sigma$, a zřejmě každá identita $p = p$ je dokazatelná ze Σ. Jestliže $p = q$ je dokazatelná ze Σ, pak existuje její formální dedukce $(p_1 = q_1), \ldots, (p_n = q_n)$. Pak ale $(p_1 = q_1), \ldots, (p_n = q_n)\,, (q_n = p_n)$ je formální dedukce $(q = p)$, tedy i $(q = p)$ je dokazatelná ze Σ. Jsou-li $p = q$, $q = r$ dokazatelné ze Σ, $(p_1 = q_1), \ldots, (p_n = q_n)$ a $(s_1 = r_1), \ldots, (s_k = r_k)$ jsou jejich formální dedukce, pak $(p_1 = q_1), \ldots, (p_n = q_n)\,, (s_1 = r_1), \ldots, (s_k = r_k)\,, (p_n = r_k)$ je formální dedukce $p = r$.

Je-li $p = q$ dokazatelná ze Σ a $(p_1 = q_1), \ldots, (p_n = q_n)$ její formální dedukce, nechť $r(\ldots p \ldots)$ je term s jistým výskytem subtermu p. Pak $(p_1 = q_1), \ldots, (p_n = q_n)\,, (r(\ldots p_n \ldots) = r(\ldots q_n \ldots))$ je formální dedukce identity $r(\ldots p \ldots) = r(\ldots q \ldots)$.

Konečně, je-li $(p_1 = q_1), \ldots, (p_n = q_n)$ formální dedukce $p = q$ a $f \in F$ je n-ární, pak

$$(p_1 = q_1), \ldots, (p_n = q_n) \;\; , \;\; (f(p_1, \ldots, p_n), f(p_1, \ldots, p_{n-1}, q_n)), \ldots ,$$

$$(f(p_1, \ldots, p_n), f(q_1, \ldots, g_n))$$

je formální dedukce $(f(p_1, \ldots, p_n), f(q_1, \ldots, q_n))$.

Tedy $D(\Sigma) \subseteq \{p = q; (p = q) \text{ je dokazatelná ze } \Sigma\}$. Z obou inkluzí plyne tvrzení věty. $\square$

14 ALGEBRAICKÁ TEORIE AKCEPTORŮ

Již v roce 1943 vypracovali *McCulloch* a *Pitts* model nervové sítě, který byl později formalizován v teorii automatů. Základní myšlenka je jednoduchá. Nervová síť se uvažuje jako konečná množina neuronů a senzorů a čas je uvažován diskrétní, přičemž v každém časovém okamžiku je každý neuron či senzor buď aktivní nebo neaktivní. Aktivace či desaktivace prvků nastává po příchodu aktivačního či desaktivačního impulsu. Každý neuron akceptuje určitý počet (tzv. práh) aktivačních impulsů, a pak je aktivní v dalším časovém intervalu. Senzory lze aktivovat jen impulsem ze vstupu. V každém časovém okamžiku je nervová síť tedy zcela určena stavem svých neuronů a vstupy do senzorů.

Vstupy (t.j. vstupní impulsy) nazýváme *znaky* (písmena), množina všech znaků se nazývá *abeceda*. Posloupnost vstupů se nazývá *slovo*. Slovo je *akceptováno* (neboli rozpoznáno akceptorem) nervové sítě, jestliže senzory po zpracování každého znaku (impulsu) tohoto slova dají impuls neuronům, a ty přejdou do některého z tzv. *akceptovatelných stavů*.

V roce 1956 *S.C.Kleene* analyzoval, která slova mohou být akceptována nervovou sítí, a ukázal, že tato slova tvoří tzv. *regulární jazyk. J.Myhill* ukázal souvislost mezi regulárními jazyky a jistými kongruencemi na volných monoidech.

Zde budeme abstrahovat od nervové sítě a budeme algebraicky vyšetřovat tyto souvislosti mezi vstupními slovy a akceptory.

Definice: *Akceptor* typu (F, σ) je čtveřice $\mathcal{A} = (A, F, a_0, A_0)$, kde (A,F) je konečná unární algebra typu (F, σ), $a_0 \in A$ a $A_0 \subseteq A$. Množina A se nazývá *množina stavů* akceptoru $\mathcal{A}$, a_0 je tzv. *počáteční stav*, A_0 množina *koncových stavů*.

Definice: Nechť (F, σ) je konečný typ unární algebry, nechť $(F^*; ., 1)$ je monoid, kde F^* jsou konečné posloupnosti symbolů z F a operace jsou definovány takto: jestliže $f, g, \ldots, h \in F$, $p, q, \ldots, r \in F$, pak $fg \ldots h \in F^*$, $pq \ldots r \in F^*$ a

$$(fg \ldots h) \cdot (pq \ldots r) = fg \ldots hpq \ldots r$$

$$1 \cdot (fg \ldots h) = (fg \ldots h) \cdot 1 = fg \ldots h.$$

Nechť $w = fg \ldots h \in F^*$, nechť $\mathcal{A} = (A, F, a_0, A_0)$ je akceptor typu (F, σ) a nechť $a \in A$. Označme $w(a)$výsledek dosazení za a do termu

$$w(x) = fg \ldots h(x) = f(g(\ldots(h(x) \ldots)),$$

t.j.

$$w(a) = f(g(\ldots(h(a) \ldots)) \; .$$

Dále definujme $1(a) = a$.

Definice: *Jazykem* typu F nazýváme podmnožinu F^*. Slovo $w \in F^*$ je *akceptováno* akceptorem $\mathcal{A} = (A, F, a_0, A_0)$ typu (F, σ), jestliže $w(a_0) \in A_0$. Jazyk je *akceptovatelný* akceptorem $\mathcal{A}$, což zapisujeme symbolem $\mathcal{L}(\mathcal{A})$, jestliže každé slovo $w \in F$ je akceptováno.

Definice: Nechť L, L_1, L_2 jsou jazyky typu (F, σ) unární algebry. Definujeme $L_1 \cdot L_2 = \{w_1 \cdot w_2; w_1 \in L_1, w_2 \in L_2\}$. L^* je podmonoid $(F^*, \cdot, 1)$ generovaný množinou L. Množinou *regulárních jazyků* typu (F, σ) rozumíme nejmenší množinu takových podmnožin F^*, které obsahují všechny jednoprvkové jazyky $\{f\}$, kde $f \in F \cup \{1\}$, a jsou uzavřené vzhledem k množinovým operacím $\cup, \cap$, komplement a vzhledem k výše zavedené operaci " $\cdot$ ".

Definice: *Parciální unární algebrou* typu F (nezapisujeme již (F, σ), neboť u unární algebry je $\sigma(f) = 1$ pro každé $f \in F$) nazveme dvojici (A,F), kde každé $f \in F$ je parciální unární operace na A, t.j. f je zobrazení $B \subseteq A$ do A.

Definice: *Parciální akceptor* typu F je čtveřice $\mathcal{A} = (A, F, a_0, A_0)$, kde (A,F) je konečná parciální unární algebra typu F, $a_0 \in A$, $A_0 \subseteq A$.

Akceptovatelný jazyk pro parciální akceptor $\mathcal{A}$ bude opět označen $\mathcal{L}(\mathcal{A})$.

Lemma 14.1. *Každý jazyk akceptovatelný parciálním akceptorem je akceptovatelný akceptorem.*

Důkaz: Nechť $\mathcal{A} = (A, F, a_0, A_0)$ je parciální akceptor, nechť $b \notin A$, a položme $B = A \cup \{b\}$. Pro $f \in F, a \in A$ definujme: jestliže $f(a)$ neexistuje v $\mathcal{A}$ (není definována parciální operace f pro toto a), položme $f(a) = b$. Zřejmě $\mathcal{B} = (B, F, a_0, A_0)$ je akceptor, akceptující stejný jazyk jako $\mathcal{A}$. $\square$

Definice: Nechť $\mathcal{A} = (A, F, a_0, A_0)$ je parciální akceptor. Pro $a \in A$, $w \in F^*$ definujme *rank* $Rg(w,a)$ jako množinu

$$\{f_n(a), f_{n-1}f_n(a), \ldots, f_1 f_2 \ldots f_n(a)\},$$

je-li $w = f_1 \ldots f_n$, a rovnu $\{a\}$, je-li $w = 1$.

Lemma 14.2. *Jazyk akceptovatelný akceptorem je regulární.*

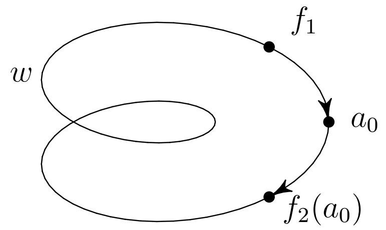
Důkaz: Nechť L je jazyk akceptovatelný parciálním akceptorem $\mathcal{A} = (A, F, a_0, A_0)$. Dokážeme tvrzení indukcí přes $|A|$. Zřejmě $\emptyset$ je regulární jazyk, neboť $\emptyset = \{f\} \cap \{f\}'$($'$ značí množinový komplement) pro každé $f \in F$. Nechť $|A| = 1$. Je-li $A_0 = \emptyset$, pak $\mathcal{L}(\mathcal{A}) = \emptyset$, což je regulární jazyk. Je-li $A_0 = \{a_0\}$, označme $G = \{f \in F; f(a_0)$ je definováno$\}$. Pak $\mathcal{L}(\mathcal{A}) = G^* = (\cup\{\{f\}; f \in G\})^*$, což je opět regulární jazyk.

Nyní předpokládejme, že $|A| > 1$, a že pro parciální akceptor $\mathcal{B} = (B, F, b_0, B_0)$, kde $|B| < |A|$, je $\mathcal{L}(\mathcal{B})$ již regulární. Je-li $A_0 = \emptyset$, pak $\mathcal{L}(\mathcal{A}) = \emptyset$, t.j. je regulární. Nechť tedy $A_0 \neq \emptyset$. Jádrem důkazu je rozložit každé akceptovatelné slovo do součinu slov, jež lze znázornit jako posloupnost cyklů, jež následují po necyklech, zobrazujících a_0 do A_0, je-li $a_0 \notin A_0$. Nechť

$$C = \{\langle f_1, f_2 \rangle \in F * F; f_1 w f_1(a_0) = a_0 \text{ pro některé } w \in F^*, f_2(a_0) \neq a_0 \text{ a}$$

$$Rg(w\,,\,f(a)) \subseteq A \setminus \{a\}\},$$

viz obr. 21



Obr.21

Nechť $\langle f_1, f_2\rangle \in C$, označme

$$C(f_1, f_2) = \{w \in F^*; f_1 w f_2(a_0) = a_0; Rg(w; f_2(a_0)) \subseteq A \setminus \{a_0\}\}.$$

Pak $C(f_1, f_2)$ je jazyk akceptovatelný akceptorem

$$(A \setminus \{a_0\}, F, f_2(a_0), f_1^{-1}(a_0) \setminus \{a_0\}),$$

t.j. $C(f_1, f_2)$ je dle indukčního předpokladu regulární (neboť $|A\setminus\{a_0\}| < |A|$).
Nechť
$\mathcal{H} = \{f \in F; f(a_0) = a_0\} \cup \{1\}$
$\mathcal{D} = \{f \in F; f(a_0) \neq a_0\}$.
Pro $f \in \mathcal{D}$ označme

$$E_f = \{w \in F^*; wf(a_0) \in A_0\,,\, Rg(w; f(a_0)) \subseteq A \setminus \{a_0\}\}.$$

Pak E_f je jazyk akceptovatelný akceptorem

$$(A \setminus \{a_0\}, F, f(a_0), A_0 \setminus \{a_0\}),$$

je tedy dle indukčního předpokladu regulární. Nechť

$$E = \left[\begin{array}{ll} \cup\{E \cdot \{f\}; f \in \mathcal{D}\} & \text{je-li } a_0 \notin A_0 \\ \cup\{E_f \cdot \{f\} \cup \{1\}; f \in \mathcal{D}\} & \text{je-li } a_0 \in A_0. \end{array}\right.$$

Pak $L = E \cdot (\mathcal{H} \cup \{\cup\{\{f_1\} \cdot C(f_1, f_2) \cdot \{f_2\}; \langle f_1, f_2\rangle \in C\})^*$, t.j. L je regulární jazyk. □

Definice: Nechť F je typ unární algebry a $t \notin F$. Homomorfismus $d_t : (F \cup \{t\})^* \to F^*$ nazveme *vypouštějící*, jestliže $d_t(f) = f$ pro každé $f \in F$ a $d_t(t) = 1$.

Lemma 14.3. *Nechť L je jazyk typu $F \cup \{t\}$, kde $t \notin F$, který je akceptovatelný některým akceptorem. Pak $d_t(L)$ je jazyk typu F, který je opět akceptovatelný některým akceptorem.*

Důkaz: Nechť $\mathcal{A} = (A, F \cup \{t\}, a_0, A_0)$ je akceptor, $L = \mathcal{L}(\mathcal{A})$ jazyk. Pro $w \in F^*$ definujme

$$S_w = \{\overline{w}(a_0); \overline{w} \in (F \cup \{t\})^* \, , \, d_t(\overline{w}) = w\}$$

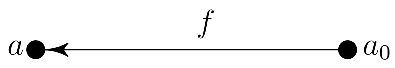
a nechť $B = \{S_w; w \in F^*\}$. Jelikož A je konečná množina, jsou S_w a B konečné. Pro $f \in F$ definujme $f(S_w) = S_{fw}$. (Zřejmě S_{fw} závisí jen na S_w, ale ne na w). Nechť $b_0 = S_1$

$$B_0 = \{S_w \, ; \, S_w \cap A_0 \neq \emptyset\}.$$

Pak (B, F, b_0, B_0) akceptuje w právě když $w(S_1) \in B_0$, což je ekvivalentní s $S_w \cap A_0 \neq \emptyset$, což je ekvivalentní s $\overline{w}(a_0) \in A_0$ pro některé $\overline{w} \in d_t^{-1}(w)$, což je ekvivalentní s $\overline{w} \in L$ pro některé $\overline{w} \in d_t^{-1}(w)$, což je ekvivalentní s $w \in d_t(L)$. $\square$

Věta 14.4. (**Kleene**) *Nechť L je jazyk. Pak L je akceptovatelný některým akceptorem právě když L je regulární.*

Důkaz: Z Lemma 14.2. plyne implikace $\Rightarrow$. Dokážeme obrácenou implikaci $\Leftarrow$. Je-li $L = \{f\}$, pak příslušný akceptor je na obr.22,



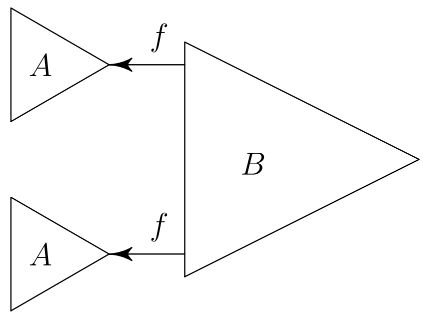
Obr.22

kde tam, kde chybí šipky, není f definována a platí $A_0 = \{a\}$. Je-li $L = \{1\}$, pak $A = A_0 = \{a_0\}$ a f není nikde definována.

Dále předpokládejme, že L_1 je jazyk akceptoru (A, F, a_0, A_0) a L_2 je jazyk akceptoru (B, F, b_0, B_0). Pak $L_1 \cap L_2$ je jazyk akceptoru $(A \times B, F, \langle a_0, b_0 \rangle, A_0 * B_0)$, kde $f(\langle a, b \rangle) = \langle f(a), f(b) \rangle$ (direktní součin). Dále L_1' je jazyk akceptoru $(A, F, a_0, A \setminus A_0)$.

Použitím De Morganových zákonů na Booleově algebře $Exp\, F^*$ vidíme, že rovněž jazyk $L_1 \cup L_2$ je jazyk některého akceptoru.

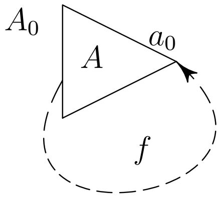
Abychom zkonstruovali akceptor k jazyku $L_1 \cdot L_2$, rozšiřme typ na $F \cup \{t\}$. Pak zobrazení každého členu z B_0 na vstup kopie akceptoru $\mathcal{A}$ dává akceptor jazyka $L_1 \cdot \{t\} \cdot L_2$, viz. obr.23



Obr.23

Dle Lemma 14.3. je pak v $L_1 \cdot L_2$ jazyk, akceptovatelný některým akceptorem.

Podobně pro jazyk L_1^* nechť t zobrazí každý prvek z A_0 na a_0, viz obr. 24.



Obr.24

Pak $(L_1 \cdot \{t\})^* \cdot L_1$ je jazyk tohoto parciálního akceptoru, tedy $L_1^* = d_t((L_1 \cdot \{t\})^* \cdot L_1 \cup \{1\})$ je jazyk, akceptovatelný některým akceptorem. $\square$

Definice: Označme τ zobrazení F^* do $T(X)$, t.j. množiny všech termů typu F s množinou proměnných $X = \{x\}$, definované takto: $\tau(w) = w(x)$.

Lemma 14.5. *Zobrazení τ je izomorfismus monoidu $(F^*; \cdot, 1)$ na monoid $(T(x); \circ, x)$, kde $\circ$ je skládání operací.*

Důkaz: Je zřejmý.

Definice: Nechť $\theta \in Con(F^*; \cdot, 1)$. Položme

$$\theta(x) = \{\langle w_1(x)\,,\, w_2(x)\rangle; \langle w_1, w_2\rangle \in \theta\}.$$

Lemma 14.6. *Zobrazení $\theta \to \theta(x)$ je svazový izomorfismus svazu $Con\,(F^*; \cdot, 1)$ do svazu FI-kongruencí na $T(X)$.*

Důkaz: je zřejmý, neboť pro $\theta \in Con\,(F^*; \cdot, 1)\,,\, \langle w_1, w_2\rangle \in \theta\,,\, u \in F^*$, a $\langle uw_1, uw_2\rangle \in \theta$ stačí dokázat, že $\theta(x) \in Con\,T(X)$ a $\langle w_1u, w_2u\rangle \in \theta$, což dokazuje, že $\theta(x)$ je FI-kongruence. $\square$

Připomeňme, že je-li $\mathcal{A} = (A, F)$ algebra, $\theta \in Con\,\mathcal{A}$, $B \subseteq A$, pak značíme $B^\theta = \{a \in A; B \cap [a]_\theta \neq \emptyset\}$; viz 2.věta o izomorfismu.

Lemma 14.7. *Nechť L je jazyk typu F akceptovatelný některým akceptorem. Pak existuje $\theta \in Con\,(F^*; \cdot, 1)$ tak, že $(F^*; \cdot, 1)/\theta$ je konečný monoid a $L = L^\theta$.*

Důkaz: Nechť $\mathcal{A}$ je akceptor typu F tak, že $\mathcal{L}(\mathcal{A}) = L$. Nechť $F_A(x)$ je volná algebra s jedním volným generátorem ve varietě, generované algebrou $\mathcal{A}$, tj. ve varietě $HSP(\mathcal{A})$. Nechť $h : T(X) \to F_A(x)$ je příslušný přirozený homomorfismus a nechť $g : F_A(x) \to (A, F)$ je homomorfismus, který je rozšířením zobrazení $x \to a_0$. Pak pro $L(x) = \{w(x); w \in L\}$ je $L(x) = h^{-1}g^{-1}(A_0) = \cup\{[p]_{\theta_h}; p \in q^{-1}(A_0)\}$, odtud $L(x) = L(x)^{\theta_h}$. Dle Lemma 14.6. je $\theta_h(x)$ FI-kongruence na $T(X)$, tedy $\theta = \theta(x)$ pro některou $\theta \in Con\,(F^*; \cdot, 1)$. Tedy $L(x) = L(x)^{\theta(x)}$, odtud $L = L^\theta$. Jelikož $T(X)/\theta_h$ je konečná, je i $(F^*; \cdot, 1)/\theta$ konečná. □

Věta 14.8. (Myhill) *Nechť L je jazyk typu F. Pak L je akceptovatelný některým akceptorem právě když existuje $\theta \in Con\,(F^*; \cdot, 1)$ taková,že $(F^*; \cdot, 1)/\theta$ je konečný a platí $L^\theta = L$.*

Důkaz: Implikace ⇒ plyne z Lemmatu 14.7. Obráceně, nechť θ je kongruence, splňující podmínky věty, a nechť
$A = \{[w]_\theta; w \in F$, $f([w]_\theta) = [fw]_\theta$ pro $f \in F$, $a_0 = [1]_\theta$,
$A_0 = \{[w]_\theta\ ;\ w \in L\}$. Pak (A, F, a_0, A_0) akceptuje w právě když $w([1]_\theta) \in A_0$, což je ekvivalentní $[w]_\theta \in A_0$, což je ekvivalentní $[w]_\theta = [u]_\theta$ pro některé $u \in L$, což je ekvivalentní s $w \in L$. □

Definice: Nechť L je jazyk typu F. Definujme relaci Φ_L na F^* takto:

$$\langle w_1, w_2\rangle \in \Phi_L \Longleftrightarrow (uw_1v \in L \Longleftrightarrow uw_2v \in L \text{ pro } u, v \in F^*).$$

Lemma 14.9. *Nechť L je jazyk typu F. Pak Φ_L je největší kongruence θ na $(F^*; \cdot, 1)$ taková, že $L^\theta = L$.*

Důkaz: Nechť $L = L^\theta$. Pak pro $\langle w_1, w_2\rangle \in \theta$, $u, v \in F^*$ platí

$$\langle uw_1v, uw_2v\rangle \in \theta,\ \text{odtud } uw_1v \in L \Longleftrightarrow uw_2v \in L,$$

tedy $[uw_1v]_\theta = [uw_2v]_\theta$ a $L = \cup\{[w]_\theta; w \in L\}$. Tedy $\theta \subseteq \Phi_L$.

Obráceně, nechť $\langle w_1, w_2\rangle \in \Phi_L$, $\langle w_1', w_2'\rangle \in\ \Phi_L$. Φ_L je zřejmě ekvivalence, zbývá dokázat substituční podmínku. Pak pro každé $u, v \in F^*$

$$uw_1w_1'w \in L \Longleftrightarrow uw_1w_2'v \in L \Longleftrightarrow uw_2w_2'v \in L, \text{ tedy}$$

$\langle w_1w_1', w_2w_2'\} \in \Phi_L$, tj. Φ_L je kongruence na $(F^*; \cdot, 1)$.

Nechť $w \in L$ a $\langle w, w'\} \in \Phi_L$. Pak $1 \cdot w \cdot 1 \in L \Longleftrightarrow 1 \cdot w' \cdot 1 \in L$, což implikuje $w' \in L$. Tedy $[w]_{\phi_L} \subseteq L$, odtud $L^\theta = L$ pro $\theta = \Phi_L$. □

Definice: Nechť L je jazyk typu F. Pak monoid $M_L = (F^*; \cdot, 1)/\Phi_L$ nazýváme *syntaktický monoid.*

Věta 14.10. *Jazyk L je akceptovatelný některým akceptorem právě když syntaktický monoid M_L je konečný.*

Důkaz: Je kombinací Věty 14.8. a Lemma 14.9. □

15 PRIMÁLNÍ A FUNKČNĚ ÚPLNÉ ALGEBRY

Definice: Konečná algebra $\mathcal{A} = (A, F)$ se nazývá *primální*, jestliže pro každé přirozené číslo n a pro libovolné zobrazení $h : A^n \to A$ existuje term t algebry $\mathcal{A}$ takový, že

$$h(a_1, \dots a_n) = t(a_1, \dots, a_n) \text{ pro každé } a_1, \dots, a_n \in \ A.$$

Konečná algebra $\mathcal{A} = (A, F)$ je *funkčně úplná*, je-li algebra $\mathcal{A}_A = (A, F \cup A)$ primální (prvky z A se uvažují jako nulární operace).

Definice: Nechť $\mathcal{A} = (A, f)$ je algebra typu (F, σ), nechť $t(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m})$ je $n + m$-ární term typu (F, σ) pro $n \in \boldsymbol{N}$, $m \geq 0$ celé, a nechť $c_1, \dots, c_m \in A$. Funkci

$$p(x_1, \dots, x_n) = t(x_1, \dots, x_n, c_1, \dots, c_m)$$

nazveme *n-ární polynom algebry $\mathcal{A}$*.

Poznámka : Konečná algebra $\mathcal{A} = (A, F)$ je funkčně úplná, jestliže pro každé $n \in \boldsymbol{N}$ a libovolné zobrazení $h : A^n \to A$ existuje n-ární polynom p algebry $\mathcal{A}$ tak, že

$$h(a_1, \dots a_n) = p(a_1, \dots, a_n)$$

pro každé $a_1, \dots, a_n \in A$.

Algebra $\mathcal{A}$ se nazývá *jednoduchá,* je-li $Con\, \mathcal{A} = \{\omega, \iota\}$.

Poznámka :

(a) Každá primální algebra je funkčně úplná, neboť každý term je polynom.

(b) Každá funkčně úplná algebra je jednoduchá.

(c) Každá primální algebra $\mathcal{A}$ je jednoduchá,
nemá žádnou podalgebru různou od $\mathcal{A}$ a jediný izomorfismus $\mathcal{A}$ na $\mathcal{A}$ je identické zobrazení.

Příklad : Dvouprvková Booleova algebra je primální.

Nechť A je konečná množina, $0, 1 \in A$, $0 \neq 1$, a nechť $+, \cdot$ jsou binární operace na A splňující:

$$x + 0 = 0 + x = x \quad , \quad x \cdot 1 = x \quad , \quad x \cdot 0 = 0.$$

Pro každé $a \in A$ definujme unární operaci $v_a(x)$ takto:

$$v_a(x) = 1 \text{ pro } x = a \quad , \quad v_a(x) = 0 \text{ pro } x \neq a.$$

Pro $b_1, \ldots, b_n \in A$ označme

$$\sum_{i=1}^{n} b_i = (\ldots((b_1 + b_2) + b_3) + \ldots + b_n),$$

$$\prod_{i=1}^{n} b_i = (\ldots((b_1 \cdot b_2) \cdot b_3) \cdot \ldots \cdot b_n).$$

Věta 15.1. *Nechť A je konečná množina, $|A| \geq 2$, a nechť h je libovolné zobrazení $A^n \to A$. Pak platí*

$$h(x_1, \ldots, x_n) = \sum_{j=1}^{|A|^n} h(a_{1j}, \ldots, a_{nj}) \cdot \prod_{i=1}^{n} v_{a_{ij}}(x_i),$$

tedy algebra $(A; +, \cdot, \{v_a; a \in A\})$ je funkčně úplná.

Důkaz: Snadno se přesvědčíme, že

$$\prod_{i=1}^{n} v_{a_{ij}}(x_i) = 1 \text{ pro } (x_1, \ldots, x_n) = (a_{1j}, \ldots, a_{nj}) \text{ jinak rovno } 0.$$

Odtud již plyne tvrzení. □

Poznámka : Z věty 15.1. bezprostředně plyne, že každou n-ární operaci na konečné množině lze vytvořit pomocí binárních a unárních operací. (*W.Sierpinski* 1954). Existuje také jiná konstrukce, dokazující tento fakt i pro nekonečné množiny.

Důsledek : *Pro každé prvočíslo p je těleso Z_p zbytkových tříd $\mathrm{mod}\, p$ primální.*

Důkaz: V Z_p platí $x^{p-1} = 1$ pro každé $x \neq 0$. Pro každé $k \in Z_p$ je $v_k(x) = 1 - (x - k)^{p-1}$, ostatní operace $+, \cdot$ jsou operace okruhu Z_p, tedy dle Věty 15.1. je Z_p funkčně úplná. Avšak každý prvek $k \in Z_p$ je výsledkem termu, totiž $k = 1 + 1 + \ldots + 1$ (k sčítanců), t.j. Z_p je primální. □

Věta 15.2. *Nechť $Z_n = \{0, 1, \ldots, n-1\}$. Definujme binární operaci $\wedge$ takto : $x \wedge y = min\,(x, y)$, a unární operaci g takto : $g(x) = x + 1 \pmod n$. Pak $(Z_n; \wedge, g)$ je primální.*

D ů k a z : Pro $k \in N$ označme $g^k(x) = g(g(\ldots(g(x))\ldots))$ (k krát). Zřejmě $\wedge$ je asociativní. Definujme

$$x + y = g(g^{n-1}(x) \wedge g^{n-1}(y)) \quad , \quad x \cdot y = x \wedge y,$$

$$v_i(x) = g^{n-1}(1 \wedge g^{n-i}(x)).$$

Tyto operace splňují předpoklady Věty 15.1 (kde $n-1$ hraje roli jedničky.) Avšak pro každé $i \in Z_n$ platí

$$i = g^i(x \wedge g(x) \wedge \ldots \wedge g^2(x) \wedge \ldots \wedge g^{n-1}(x) \ ,$$

tedy každý polynom je termem, t.j. $(Z_n, \wedge, g)$ je primální. $\square$

Příklady :

(1) Definujme $x|y = min\,(x, y) + 1 \ \ (mod\, n)$. Pak $(Z_n, |)$ je primální. (Operace $|$ je tzv. *Shefferova*). Zřejmě $g(x) = x|x$ a $x \wedge y = g^{n-1}(x|y)$

(2) Z Věty 15.2. ihned plyne, že dvouprvková Booleova algebra je primální (stačí uvažovat $g(x) = x'$)

(3) n-hodnotová Postova algebra $P_n = (\{0, 1, \ldots, n-1\}, \vee, \wedge, ', 0, 1)$, je algebra typu (2,2,1,0,0), s uspořádáním $0 < n-1 < n-2 < \ldots < 2 < 1$, přičemž $1' = 2$, $2' = 3, \ldots$, $(n-2)' = n-1$, $(n-1)' = 0$, $0' = 1$. P_n je primální (Postova algebra P_n hraje v n-hodnotové logice tutéž roli, jako dvouprvková Booleova algebra ve dvouhodnotové logice). Pro $n = 2$ je P_2 dvouprvková Booleova algebra.

Definice: *Ternární diskriminátor* na množině A je funkce $t : A^3 \to A$ daná předpisem $t(a, b, c) = a$ pro $a \neq b$, $t(a, a, c) = c$.

Věta 15.3. *Konečná algebra $\mathcal{A}$ je funkčně úplná právě když je ternární diskriminátor jejím polynomem.*

D ů k a z : Je-li $\mathcal{A}$ funkčně úplná, pak každá funkce je polynomem, tedy i diskriminátor. Obráceně, nechť ternární diskriminátor $t(x, y, z)$ je polynomem v $\mathcal{A}$. Je-li $|A| = 1$, je tvrzení evidentní. Nechť $|A| \geq 2$.
Pak zvolme dva různé prvky z A, označme je 0,1 a definujme polynomy

$x + y = t(x, 0, y)$,
$x \cdot y = t(y, 1, x)$
$v_0(x) = t(0, x, 1)$
$v_a(x) = t(0, t(a, x, 0), 1)$ pro $a \neq 0$.

Výpočtem se lze přesvědčit, že platí předpoklady Věty 15.1., tedy $\mathcal{A}$ je funkčně úplná. $\square$

Důsledek *Nechť* $(R, +, \cdot, 1)$ *je unitární okruh. Definujme* $g(0) = 0$, $g(x) = 1$ *pro* $x \neq 0$. *Pak* $(R, +, \cdot, 1, g)$ *je funkčně úplná algebra.*

Důkaz: Snadno se přesvědčíme, že $t(x, y, z) = z + (x - z) \cdot g(x - y)$ je ternární diskriminátor. □

Poznámka : Z Věty 15.3. plyne, že každá funkčně úplná algebra $\mathcal{A}$ je jednoduchá. Nechť $\theta \in Con\,\mathcal{A}$ a nechť $\theta \neq \omega$. Pak existují $a \neq b$ tak, že $\langle a, b\rangle \in \theta$. Nechť $c, d \in \mathcal{A}$ jsou libovolné prvky. Pak

$$\langle c, a\rangle = \langle t(a, a, c), t(a, b, c)\rangle \in \theta$$

$$\langle d, a\rangle = \langle t(a, a, d), t(a, b, d)\rangle \in \theta,$$

z tranzitivity θ tedy $\langle c, d\rangle \in \theta$, t.j. $\theta = \iota$, neboli $Con\,\mathcal{A} = \{\omega, \iota\}$. □

Bez důkazu uvedeme větu, kterou dokázal *H. Werner* v r. 1974:

Věta 15.4. *Nechť* $\mathcal{A}$ *je netriviální konečná algebra z permutabilní variety.* $\mathcal{A}$ *je funkčně úplná právě když* $Con\,\mathcal{A} \times \mathcal{A}$ *obsahuje tyto čtyři kongruence :* ω, ι, *a obě faktorové kongruence.*

Důležitou charakterizaci primálních algeber dokázali v r.1970 A. Foster a A. F. Pixley:

Věta 15.5. *Je-li* $\mathcal{A}$ *konečná algebra, pak je ekvivalentní:*

(a) $\mathcal{A}$ *je primální;*

(b) $\mathcal{A}$ *je jednoduchá, nemá vlastní podalgebru, jediný izomorfismus* $\mathcal{A} \to \mathcal{A}$ *je identické zobrazení, a varieta* $HSP(\mathcal{A})$ *je aritmetická;*

(c) $\mathcal{A}$ *nemá vlastní podalgebru, jediný izomorfismus* $\mathcal{A} \to \mathcal{A}$ *je identické zobrazení a ternární diskriminátor je termem na* $\mathcal{A}$.

Příklad: Algebry, na nichž je ternární diskriminátor termem jsou:

(1) Dvouprvková Booleova algebra, kde $x \oplus y = (x \wedge y') \vee (x' \wedge y)$

$$t(x, y, z) = [(x \oplus y) \wedge x] \vee [(x \oplus y \oplus 1) \wedge z] .$$

(2) Těleso zbytkových tříd $mod\, p$ (p je prvočíslo), kde

$$t(x, y, z) = (x - y)^{p-1} \cdot x + [1 - (x - y)^{p-1}] \cdot z \qquad .$$

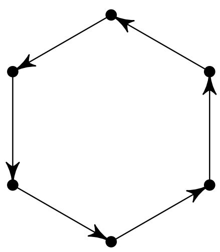
16 Unární algebry

V kapitole 14. jsme aplikovali unární operaci na řešení jistého problému teorie automatů. Odtud je patrné, že unární operace a unární algebry mají značnou důležitost. Proto tuto kapitolu věnujeme zkoumání základních vlastností unárních algeber.

Unární algebra s jedinou unární operací se nazývá *monounární.* Typickým případem monounárních algeber jsou *řetězec* (nekonečný):

$$0 \to 1 \to 2 \to 3 \to \ldots\ldots$$

(unární operace je vyznačena šipkou - zde je to operace následovníka) a *cyklus*:



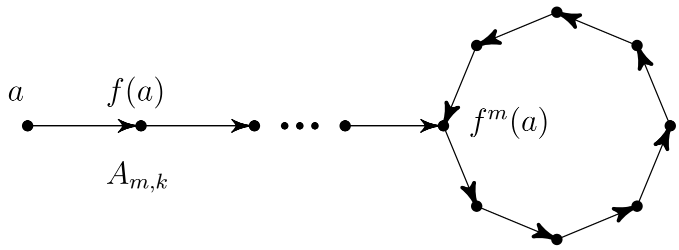
Je ihned patrné, že každá monounární algebra sestává ze souvislých komponent: řekneme, že $x, y \in A$ *patří do téže komponenty* algebry (A,f), jestliže existují celá čísla $m, n \geq 0$ tak, že $f^m(x) = f^n(y)$, Přičemž definujeme: $f^0(x) = x$, $f^1(x) = f(x)$, $f^{n+1}(x) = f(f^n(x))$. Zřejmě každá komponenta algebry (A, f) je její podalgebrou. Zřejmě platí: (A, f) je *souvislá* t.j. má jedinou komponentu, právě když každé dvě její podalgebry mají společný prvek.

Jelikož se každá monounární algebra skládá z disjunktních souvislých komponent (podalgeber), je tato algebra zcela popsána, jsou-li popsány její komponenty. Stačí tedy zkoumat jen souvislé monounární algebry.

Je ihned patrné, že monounární algebra s jedním generátorem je souvislá. Dáme její úplný popis. Je-li a generátor (A, f) , pak
$A = \{f^n(a); n = 0, 1, 2, \ldots\}$. Je-li $f^n(a) \neq f^m(a)$ pro každé $m \neq n$, pak (A, f) je zřejmě nekonečný řetězec:

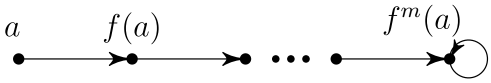
$$a \to f(a) \to f^2(a) \to f^3(a) \to \ldots.$$

Je-li pro některé $m \in \boldsymbol{N} \cup \{0\}$ a některé $k \in \boldsymbol{N}$
$f^m(a) = f^{m+k}(a)$, a je-li m nejmenší číslo této vlastnosti, pak tuto algebru označme $A_{m,k}$; zřejmě má tuto strukturu:



cyklus má k prvků

tedy specielně pro $m = 0$ je $A_{0,k}$ k-prvkový cyklus, pro $k = 1$ je $A_{m,1}$ tvaru :



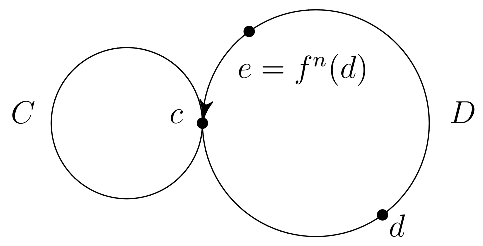
Závěr : Každá monounární algebra s jedním generátorem je buď nekonečný řetězec nebo $A_{m,k}$.

Definice: Nechť (A, f) je monounární algebra. *Jádrem* (A, f) nazýváme takovou podalgebru, na které je f injektivní.

Je-li tedy (A, f) monounární s jedním generátorem, je její jádro buď nekonečný řetězec nebo $A_{0,k}$ pro některé $k \in N$.

Lemma 16.1. *Je-li (A, f) souvislá, pak její jádro je buď nekonečný řetězec nebo $A_{0,k}$. Má-li (A, F) konečné jádro, pak je toto jádro v (A, f) jediné.*

Důkaz: Nechť C je jádro (A, f) . Nechť C je konečné, a nechť D je také jádro (A, f) . Pak $C \cap D$ je neprázdná podalgebra (A,f), je podalgebrou jádra (t.j. podalgebry) D, tedy i jádro D je konečné, t.j. C i D jsou cykly. Nechť C je k-prvkový cyklus. Nechť $c \in C \cap D$ a nechť $d \in D \setminus C$. Pak pro některé $n \in \boldsymbol{N}$ platí $f^n(d) = c$. Nechť n je nejmenší takové číslo. Pak $e = f^{n-1}(d) \notin C$. Avšak $f(e) = f^n(d) = c$, $f^k(c) = c, e \neq c$, tedy f není na D jednoznačná, t.j. D není jádro - spor. Tedy $D \setminus C = \emptyset$, t.j. $D \subseteq C$. Analogicky se dokáže $C \subseteq D$, t.j. $D = C$, tedy (A, f) má jediné konečné jádro. $\square$



Obr.25

Nyní můžeme popsat všechny souvislé monounární algebry. Dle Lemma 16.1. má (A, f) jádro C , a $A \setminus C$ neobsahuje žádný cyklus; lze tedy $A \setminus C$ uspořádat takto:

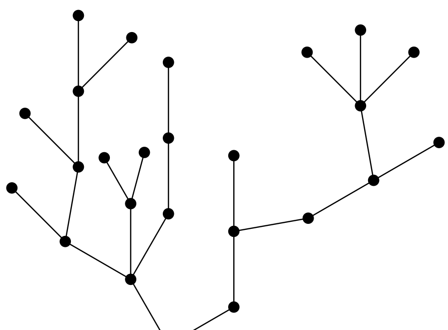
$$a \le b \Longleftrightarrow f^n(h) = a \text{ pro některé } n \ .$$

Množina M minimálních prvků tohoto uspořádání se skládá z těch $a \notin C$, pro které $f(a) \in C$. Jelikož každá podalgebra s jedním generátorem $\{b, f(b), f^2(b), \ldots\}$ má společný prvek s C, musí každý prvek z $A \setminus C$ být v uspořádání $\le$ nad některým $a \in M$. Pro $b \in A \setminus C$, prvky z $A \setminus C$ menší nebo rovny b tvoří tedy řetězec

$$b \ge f(b) \ge f^2(b) \ge f^m(b) = a \in M \ .$$

Definice: Uspořádaná množina T s nejmenším prvkem 0 se nazývá *kořenový strom* (0 je *kořen*), jestliže pro každé $t \in T$ je interval $[0,t]$ konečný řetězec.

Příklad : viz Obr. 26

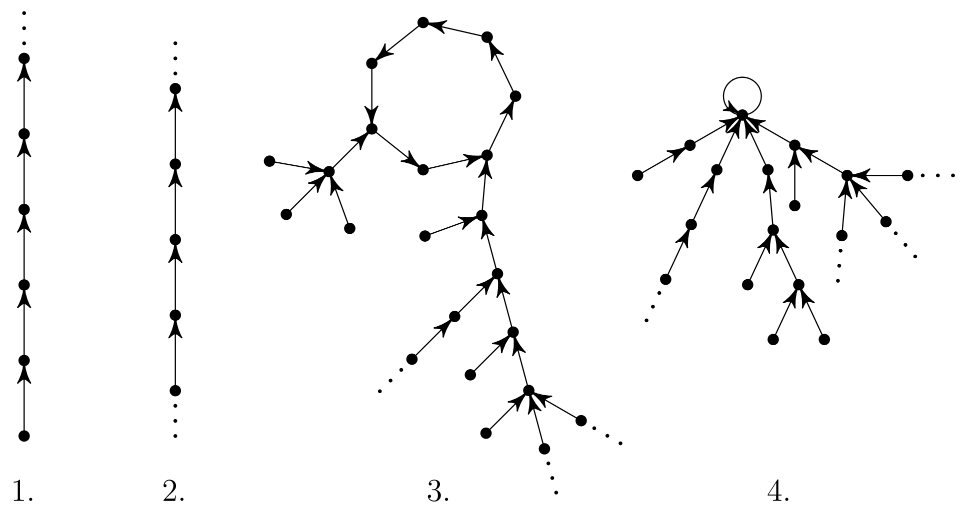


Obr. 26

Je tedy patrné, že uspořádaná množina $A \setminus C$ je sjednocením disjunktních kořenových stromů.

Věta 16.2. *Každá monounární algebra je sjednocením vzájemně disjunktních souvislých monounárních algeber. Každá souvislá monounární algebra (A, f) má podalgebru C, izomorfní buď konečnému cyklu nebo nekonečnému řetězci (s operací následovníka). Množina $A \setminus C$ je sjednocením disjunktních kořenových stromů, kde kořen padne do C a $x \leq y$ právě když $f^n(y) = x$ pro některé $n \in \boldsymbol{N} \cup \{0\}$.*

Typické příklady monounárních algeber (souvislých):



1. 2. 3. 4.

Obr.27

Důsledek *Je-li (A, f) monounární algebra taková, že f je bijekce na A, pak je sjednocením komponent, z nichž každá je buď řetězec izomorfní se Z nebo cyklus $A_{0,k}$.*

Nyní budeme zkoumat unární algebry s více unárními operacemi. Obecný popis takových algeber není znám, jen v případě, že každá operace je bijekce, lze vyslovit jistou charakterizaci.

Nechť (A,F) je unární algebra taková, že každé $f \in F$ je bijekce. Zřejmě množina všech bijekcí na A tvoří grupu. Algebra (A,F) se nazývá G-algebra, jestliže existuje konečná grupa G taková, že $(A,F) = (A, \{f_g; g \in G\})$, kde pro každé $g \in G$ je f_g bijekce. Zřejmě f_e je identita (e je jednotka grupy G) a $f_{g^{-1}} = f_g^{-1}$. Pro tyto algebry lze dokázat:

Věta 16.3. *Každá unární G-algebra je sjednocením disjunktních komponent, což jsou podalgebry, z nichž každá je izomorfní G/K-algebře pro některou podgrupu K grupy G.*

V teorii automatů mají význam i tzv. parciální unární algebry, t.j. takové (A,F), kde pro každé $f \in F$ je $f : B \to A$ pro $B \subseteq A$; je-li $B = A$, pak f je unární operace, je-li $B \neq A, f$ je *parciální unární operace.* Pak $def(f) = B$ je tzv. definiční obor f.

Definice: Nechť f je parciální unární operace na A. Dvojice (A, f) se nazývá parciální monounární algebra, neboli *Pawlakův stroj*.

Jsou-li (A, f) , (B, g) dva Pawlakovy stroje, zkoumáme, kdy lze "(A, f) realizovat pomocí (B, g)", přesněji:

Definice: Nechť (A, f) , (B,g) jsou Pawlakovy stroje a $\mu : A \to B$. Zobrazení μ se nazývá *simulace* (A, f) v (B, g), jestliže

(i) pro každé $x \in A, x \in def\,(f) \Longleftrightarrow \mu(x) \in def\,(g)$;

(ii) pro každé $x \in def\,(f)$ existuje $k \in \boldsymbol{N}$ tak, že $\mu(x) \in def\,(g^k)$ a $\mu(f(x)) = g^k(\mu(x))$.

Problém : Určit všechny simulace Pawlakova stroje (A, f) v (B,g).
Tento problém řešil v 80-tých letech *M.Novotný*:
Stejně jako pro monounární algebry, každý Pawlakův stroj je sjednocením souvislých komponent. Nechť (A, f) je souvislý Pawlakův stroj. Je-li (C,f) jeho podstroj, označme $C^* = C \cup f^{-1}(C)$; zřejmě (C^*, f) je opět podstroj (A, f) . Je-li $x \in A$, označme $[x]$ podstroj, generovaný prvkem x.

Označme $A_0 = \{x \in A; f^{-1}(x) = \emptyset\}$; dále, je-li $\alpha > 0$ ordinální číslo a A_λ je definováno pro každé $\lambda < \alpha$, definujme

$$A_\alpha = \{x \in A \setminus \cup\{A_\lambda; \lambda < \alpha; f^{-1}(x) \subseteq \cup\{A_\lambda; \lambda < \alpha\}\} .$$

Pro Pawlakův stroj (A, f) označme δ_A nejmenší ordinální číslo, pro které je $A_{\delta_A} = \emptyset$. Nechť ∞ je symbol, který neoznačuje žádné ordinální číslo.

Na třídě *Ord* všech ordinálních čísel rozšíříme uspořádání tak, že $\alpha < \infty$ pro každé $\alpha \in Ord$. Položme $A_\infty = \emptyset$. Označme $W(\alpha) = \{\lambda \in ord; \lambda < \alpha\}$ pro každé $\alpha \in Ord$. Pro každé $x \in A$ položme $S_A(x) = \alpha$, jestliže $x \in A_\alpha$, a $\alpha \in W(\sigma_A) \cup \{\infty\}$.

Pro $x \in A$ položme $\delta(x) = n$, jestliže $x \in def(f^i)$ pro každé $0 \leq i < n$ a $x \notin def\,(f^n)$; $\delta(x) = \Omega$ jesliže $x \in def(f^i)$ pro každé $i = 0, 1, 2, \ldots$. (Ω je ordinální číslo množiny $\boldsymbol{N}$).

Pawlakův stroj (B,g) je *přípustný* ke stroji (A, f) , jestliže pro každé $x \in A, x' \in B$ a posloupnost celých čísel $\{k_i; 0 \leq i < \delta(x)\}$ platí :

(i) $x' \in def\,(g^{k_i})$ pro každé $0 \leq i < \delta(x)$

(ii) Je-li $\delta(x) \neq \Omega$, pak $x' \notin def\,(g)$

(iii) $S_A(f^i(x)) \leq S_B(g(x'))$ pro každé $0 \leq i < \delta(x)$.

Lemma 16.4. *Platí-li* $\mu(f^i(x)) = g^{k_i}(x)$ *pro každé* $0 \leq i < \delta(x)$, *pak* μ *je simulace* $[x]$ *v* (B, g) *taková, že* $S_A(t) \leq S_B(\mu(t))$ *pro každé* $t \in [x]$.

Lemma 16.5. *Je-li* C *podstroj* (A, f) *a* μ *je simulace* (C, f) *v* (B, g) *taková, že* $S_A(x) \leq S_B(\mu(x))$ *pro každé* $x \in C$, *pak existuje simulace* ν *stroje* (C^*, f) *v* (B, g), *která je rozšířením* μ *a* $S_A(x) \leq S_B(\nu(x))$ *pro každé* $x \in C^*$.

Kombinací obou lemmat je dokázáno, že každou simulaci podstroje $[x]$ v (B,g) definovanou v 16.4. lze rozšířit na simulaci (A, f) v (B,g). Tomuto postupu říkáme *konstrukce* C.

Věta 16.6. *Nechť* (A, f) , (B, g) *jsou souvislé Pawlakovy stroje,* $\mu : A \rightarrow B$ *zobrazení. Pak* μ *je simulace* (A, f) *v* (B, g) *tehdy a jen tehdy když* μ *je vytvořeno konstrukcí* C.

Tento postup lze snadno rozšířit pro libovolné Pawlakovy stroje:
Nechť (A, f) , (B,g) jsou Pawlakovy stroje. Pro každou komponentu C stroje (A, f) nechť μ_c je zobrazení C do komponenty D stroje (B,g), zkonstruované konstrukcí C. Nechť μ je sjednocení všech μ_c pro všechny komponenty C stroje (A, f) . Pak řekneme, že μ je *zkonstruováno konstrukcí* K.

Věta 16.7. (M.Novotný). *Nechť* (A, f) , (B, g) *jsou Pawlakovy stroje,* $\mu : A \rightarrow B$ *zobrazení. Pak* μ *je simulace* (A, f) *v* (B, g) *právě když* μ *bylo zkonstruováno konstrukcí* K.

Reference

[1] Birkhoff G.: *Lattice Theory*, 1-st ed., Publ. Amer. Math. Soc., Providence, R.I.(USA), 1940.

[2] Birkhoff G.: *Lattice Theory*, 3-rd revised ed., Publ. Amer. Math. Soc., Providence, R.I.(USA), 1967, ruský překlad: Těorija rešetok, Moskva, Nauka 1984.

[3] Birkhoff G.,Bartee T.C.: *Modern applied algebra*, McGrow-Hill, ruský překlad: Sovremennaja prikladnaja algebra, Mir Moskva 1976.

[4] Burris S., Sankappanavar H. P. : *A Course in Universal Algebra*, Springer-Verlag 1981.

[5] Cohn P.M.: *Universal Algebra*, Harper and Row Publ., N.Y.,Evanston, London 1965; ruský překlad: Universalnaja algebra, Mir Moskva 1968.

[6] Grätzer G.: *General lattice theory*, Akademie-Verlag Berlin 1978, ruský překlad: Obščaja teoria rešetok, Mir Moskva 1982

[7] Grätzer G.: *Universal Algebra*, 2-nd ed. Springer-Verlag 1979.

[8] Ihringer Th.: *Allgemeine Algebra*, Teubner Studien-bücher, Stuttgart 1988.

[9] Ježek J.: *Universální algebra a teorie modelů*, SNTL Praha 1976.

[10] Jónsson B.: *Topics in Universal Algebra*, Springer-Verlag, Leclures Notes in Mathematics 250, 1972.

[11] Kuroš A.G.: *Kapitoly z obecné algebry*, Academia Praha 1968.

[12] Mal'cev A.I.: *Algebraičeskije sistěmy* (rusky), Sovremennaja algebra, Nauka Moskva 1970.

[13] McKenzie R., McNulty G.F., Taylor W.: *Algebres, lattices, varietes*, Vol 1, Wadswarth and Brooks, Monterey, Califormia 1987.

[14] Salij V. N.: *Rešetki s jediničnimi dopolněnijami* (rusky), Nauka Moskva 1984.

[15] Sikorski R.: *Boolean Algebras*, 2-nd ed., Academia Press, N. Y. 1964, ruský překlad:

[16] Szász G.: *Introduction to lattice theory*,Academiai Kiadó Budapest 1963. (existuje německý a francouzský překlad)

[17] Werner H.: *Einführung in die Allgemeine Algebra*, B.I.-Wissenschaftsverlag, Mannheim 1979.

[18] Wille R.: *Kongruenzklassengeometrien*, Springer-Verlag, Leclures Notes in Mathematics 113, 1970.

OBSAH

1. Část: Teorie svazů 1
1. Uspořádané množiny 2
2. Svazy 8
3. Úplné svazy 14
4. Modulární, distributivní a komplementární svazy 18
5. Kongruence a ideály na svazech 28
6. Booleovy algebry 33
Dodatek 42

2. Část: Universální algebra
7. Pojem algebry, podalgebry a homomorfismus 47
8. Kongruence a faktorové algebry 53
9. Direktní a subdirektní součiny 61
10. Operátory na třídách algeber 67
11. Identity 71
12. Kongruenční podmínky 78

3. Část: Vybrané kapitoly universální algebry
13. Ekvacionální logika 100
14. Algebraická teorie akceptorů 103
15. Primální a funkčně úplné algebry 111
16. Unární algebry 114

17. Reference 121