O grupách a svazech

2.4 Axiomy distributivity a doplňku. Pojem Booleovy algebry

In: Ladislav Rieger (author): O grupách a svazech. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 143–150.

Persistent URL: http://dml.cz/dmlcz/403374

2,4. AXIOMY DISTRIBUTIVITY A DOPLŇKU. POJEM BOOLEOVY ALGEBRY. MNOŽINOVÉ SPOJOVÁNÍ A PROTÍNÁNÍ.

Vraťme se k příkladu svazu všech vybraných skupin (čili částí ze souboru (čili jak se matematice říká, *množiny*) tří různých předmětů a, b, c — (včetně skupiny prázdné $\emptyset = n$ a skupiny plné $(a, b, c) = j$). (Svazové úkony jsou nám již známé a jsou graficky vyznačeny na obr. 14.)

Tento svaz má $2^3 = 8$ prvků. Kdybychom se obecněji zabývali svazem všech skupin, které lze vytvořit z n daných předmětů $a_1, a_2, \ldots, a_n$, pak bychom určili snadno, že počet prvků tohoto svazu (t. j. počet řečených skupin) je 2^n. (Z n předmětů můžeme totiž vybrat, jak se čtenář pamatuje ze školy, $\binom{n}{k}$ skupin o k předmětech, kde

$$\binom{n}{k} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{1\,.\,2\ldots k}$$

je známý binomický koeficient. Pak dle binomické poučky je

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}.\ )$$

V takovémto svazu, čili, jak říkáme a budeme říkat a psát: *v Booleově algebře B_n všech částí konečného souboru (množiny) o n (= 3) předmětech je spojení dvou prvků* (t. j. částí), *dáno částí, která obsahuje právě a jen předměty, jež patří aspoň do jedné ze spojových částí. Průsek* dvou prvků (t. j. částí) *je pak část, obsahující právě a jen ty předměty, jež patří současně do obou protínaných částí.*

Půjde nám nejprve o to nalézt, jakými specifickými vlastnostmi je toto t. zv. *množinové spoje* čili *sjednocení a množinový průnik* čili *průnik* obdařeno, jaké jsou pro ně splněny další axiomy.

Čtenář si jistě dobře vzpomene na „samozřejmý“ zákon, jímž se řídíme při kombinovaném sečítání a násobení čísel (ať již jde o konkretně numericky daná čísla nebo o čísla, označená písmenky), totiž na t. zv. zásadu distributivity sečítání vůči násobení, prostěji řečeno, na zásadu vytýkání před závorku ze součtu. Tato zásada je dána identitou

$$x \, . \, (y + z) = x \, . \, y + x \, . \, z$$

(platnou pro každé x, y, z). (Násobek součtu je roven součtu násobků jednotlivých sčítanců.)

Mysleme si na okamžik, že písmenka x, y, z znamenají nějaké prvky Booleovy algebry B_n (uvažme pro určitost $n = 3$, $x = (a, b)$, $y = (b, c)$, $z = (a, c)$) — to jest nějaké části (skupiny) vybrané z daných n předmětů. Dále si nahraďme znak „.“ pro násobení znakem „$\cap$“ pro průnik a znak „$+$“ pro sečítání znakem „$\cup$“ pro spojování.

Pak platí v B_n identická rovnost, která se formálně nijak neliší od zákona distributivity. (V našem př. máme

$$\begin{aligned} &(a, b) \cap [(b, c) \cup (a)] = \\ &= [(a, b) \cap (b, c)] \cup [(a, b) \cap (a)] \end{aligned}$$

to jest

$$(a, b) \cap (a, b, c) = (a, b) = (b) \cup (a).)$$

Obecněji nalézáme splnění následujících dvou vzájemně duálních **axiomů distributivity** v takovýchto Booleových algebrách B_n:

Jsou-li x, y, z libovolné prvky, pak platí

6′	6″
$x \cap (y \cup z) =$ $= (x \cap y) \cup (x \cap z).$	$x \cup (y \cap z) =$ $= (x \cup y) \cap (x \cup z).$

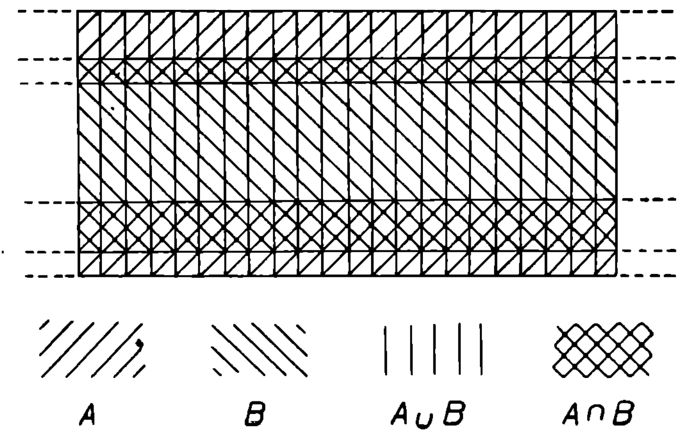
Svaz, v němž platí oba axiomy 6′ a 6″ se nazývá **distributivním svazem**.

Typické příklady distributivních svazů jsou právě ty svazy, jejichž prvky jsou jisté (nikoli obecně všechny) *části* (podmnožiny) *daného souboru* (množiny) a kde je spojování a protínání dáno *množinovým způsobem* tak jako ve svazu B_n). (Prvky uvažovaných svazů mohou být obecně ovšem částí konečné nebo nekonečné.)

Takovým svazům, jejichž prvky jsou (nějaké) části dané množiny (souboru předmětů) a v nichž všechna spojení i všechny průseky jsou sjednocení a průniky, množin se říká **množinové okruhy**. Uveďme alespoň dva příklady na množinové okruhy.

4. **příklad**: Prvky svazu nechť jsou všechny **konečné** části (soubory předmětů) vybrané z daného nekonečného souboru, na př. všechny konečné soubořy (části množiny) přirozených čísel. Dostáváme tak *množinový okruh* všech *konečných* částí *nekonečné množiny*. sjednocení dvou konečných částí je ovšem konečná část — a tím spíše to platí pro průnik; tento svaz (množinový okruh) nemá jednotku svazu.)

5. **příklad**: Za prvky našeho svazu, t. j. množinového okruhu, vezměme ty části roviny (t. j. části množiny všech bodů roviny), které jsou uvnitř jednoho nebo několika) vodorovných pásů (viz obr. 20) (rovnoběžných s osou x). (Každá taková konečná sku pina pásů představuje jistou část roviny ležící uvnitř uvažovaných pásů. Tedy body ležící na přímkách pásy omezu jících do našich částí roviny nepatří.) Pak sjednocení dvou takovýchto pásových částí roviny je opět takovou pásovou částí roviny, kde pásy — rozumí se, že v konečném počtu — vzniknou tak, že dva do sebe zapadající pásy splynou v jeden širší pás a pásy od ostatních oddělené se prostě přidají. Průnik dvou takovýchto částí roviny je opět takovouto částí roviny, který se bude patrně skládat ze všech užších pásů, tvořících spo-



Obr. 20.

lečnou část vždy některých dvou pásů z jedné a druhé z našich částí roviny (t. j. jedné a z druhé skupiny pásů).

Dokažme si obecně, že *množinové okruhy jsou distributivními svazy*. Buďtež tedy obecně dány libovolně tři prvky množinového okruhu X, Y, Z (t. j. části jakési výchozí množiny). Pak tvrdíme, že části $X \cap (Y \cup Z)$ a $(X \cap Y) \cup (X \cap Z)$ z nich utvořené jsou si rovny (t. j. vše, co patří do jedné, patří i do druhé množiny — a obráceně). Rovněž tak jsou si rovny části $X \cup (Y \cap Z)$ a $(X \cup Y) \cap (X \cup Z)$.

Dokažme jen první z obou rovností (druhá se dokáže duálně). Nejprve tedy nechť předmět x je obsažen v části $X \cap (Y \cup Z)$. T. j., x je v X a zároveň aspoň v jedné z obou množin Y, Z. Pak zřejmě x je obsaženo buď současně v X i v Y, nebo je současně obsaženo v X i v Z (nebo v obojím). Tedy je zřejmě

$$X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z) \text{ *)} \qquad \text{(a)}$$

Naopak však platí (v každém svazu vždy) nerovniny $X \cap Y \subseteq X$ a $X \cap Z \subseteq X$, takže jejich spojením (viz pozn. na str. 134) a na základě zásady idempotentnosti (str. 131) máme

$$(X \cap Y) \cup (X \cap Z) \subseteq X \cup X = X. \qquad (+)$$

Dále je ovšem i $X \cap Y \subseteq Y$ a $X \cap Z \subseteq Z$, takže spojením těchto nerovnin máme

$$(X \cap Y) \cup (X \cap Z) \subseteq Y \cup Z. \qquad (++)$$

Protětím nerovnin $(+)$ a $(++)$ máme pak nerovninu

$$(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cup Z). \qquad \text{(b)}$$

Obě (neostré) nerovniny (a) a (b) konečně za pomoci zásady ztotožňování zaručují distributivní zákon (axiom) 6′:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

pro množinové okruhy, c. b. d. (Ověření duálního zákona (axiom 6″) přenechávám čtenáři.) Poznamenejme, že v před-

*) Čtenář sám snadno nahlédne, že množinová inkluse (viz. pozn. 35) je svazovým polouspořádáním v každém množinovém okruhu.

chozím důkazu jsme úmyslně odvodili nerovninu (b) nezávisle na předpokladu, že jde o množinové spojování a protínání, jen ze základních axiomů. Platí tedy tato nerovnina nejen v množinových okruzích, nýbrž v každém svazu vůbec.) Kdybychom se omezili na možinové okruhy, dokázali bychom (v tomto případě téměř zřejmou) nerovninu (b) kratčeji, což doporučuji čtenáři jako snadné cvičení.

Zajímavá a důležitá je tu obrácená souvislost: *Když jsou v libovolném svazu splněny oba distributivní zákony* 6′ *a* 6″, *potom lze takový svaz, jak se říká, representovat množinově.* To znamená, že lze vždy udat *množinový okruh, který je s daným distributivním svazem isomorfní.* Tuto větu[39] o množinové representaci distributivních svazů zde nebudeme dokazovat. Její důkaz není sice obtížný, ale vyžaduje některých pojmů z theorie množin, jež se vymykají z rámce této knížky.

Jsou tedy (množinové okruhy pomocí axiomů 1′ až 4″, 6′ a 6″ *plně abstraktně charakterisovány.*

Distributivními zákony 6′, 6″ však nejsou ještě vyčerpány vlastnosti těch svazů, jako je na př. svaz B_n, které obsahují *veškery části* (podmnožiny) dané množiny. V takových svazech máme ještě další typický axiom, t. zv. axiom komplementu (doplňku).

7. *Ke každému prvku* x (na př. ve svazu B_n) *existuje* (*alespoň jeden*) *prvek* x', *t. zv. doplněk prvku* x, *tak, že platí*:

$$x \cup x' = j, \ x \cap x' = n$$

(kde j je jednotkový, n je nulový prvek daného svazu).

(Tímto x' k dané části (množině) x je zřejmě souhrn (množina) všech těch uvažovaných předmětů, které nejsou obsaženy v x. Tak na př. ve svazu B_3 všech částí množiny o 3 předmětech a, b, c

$$\text{pro } x = (a, b) \text{ je } x' = (c),$$

pro $x = (b)$ je $x' = (a, c)$ a pod. (Jednotka svazu B_3 je $j = (a, b, c)$, nula svazu B_3, $n = \emptyset$ (prázdná část)).

[39] Čtenář si připomene obdobnou větu z theorie grup (str. 50).

Svazu, který splňuje — kromě základních axiomů 1′ až 5″ — ještě axiom 7 (axiom doplňku) říkáme komplementární svaz.

K samotnému axiomu 7 je třeba poznamenat toto:

Předně, splnění tohoto axiomu žádá již implicitně přítomnost jak jednotkového, tak i nulového prvku ve svazu (axiom 5′, 5″). Tak na př. svaz všech konečných souborů (množin) přirozených čísel, t. j. množinový okruh z př. 4, je sice distributivní, ale nikoli komplementární, protože, ač má nulový, nemá jednotkový prvek. (Tímto jednotkovým prvkem by musela být množina všech přirozených čísel, ale ta je nekonečná). Naproti tomu důležité svazy geometrického spojování a protínání jsou komplementární, ale nikoli distributivní (splňujíce místo axiomů distributivity jistý slabší axiom, t. zv. *axiom modularity*, viz 1,9).

Za druhé, axiom 7 *nežádá jednoznačnost* doplňku: Nikde *není řečeno*, že by doplněk musel být k danému prvku komplementárního svazu *jen jeden*, a skutečně také na př. ve svazech geometrického spojování a protínání není dokonce nikdy jen jeden — až na dvě výjimky: Doplňkem nulového prvku může být vždy jen jednotkový prvek a doplňkem jednotkového prvku může být jen nulový prvek. (Toto pravidlo o jednoznačnosti doplňku jednotky a nuly platí obecně v každém komplementárním svazu. Čtenář si je dokáže jako snadné cvičení 2.) Dokážeme si však co nevidět, že v případě, že jde o distributivní svaz, pak je již (dle axiomů 6′ a 6″) jednoznačnost doplňku ke každému prvku zaručena.

Za třetí, axiomem 7 se zdá porušena duálně souměrná stavba axiomatiky theorie svazů, neboť kde je axiom duální k axiomu 7? Avšak princip duality platí nadále, neboť axiom 7 je duální sám k sobě, jak se pouhým pohledem čtenář přesvědčí. (K jednotce je duální nula, k nule jednotka svazu.)

Výčtem axiomů 1′ až 7 jsme dosáhli uzavřeného a důležitého systému axiomů. (Tato uzavřenost má dokonce doslovný význam; dá se totiž dokázat, že připojení dalšího axiomu, který by měl tvar identity a nebyl důsledkem axiomů právě napsaných, by již vedlo k logickému rozporu.) Svaz, který splňuje všechny dosud vytčené axiomy 1′ až 7 (tedy celkem 13 axiomů) se nazývá distributivním a komplementárním svazem, čili krátce známým nám již názvem Booleova algebra. Příklady Booleových algeber již známe: Jsou to množinové okruhy *všech* částí nějaké dané množiny (konečné nebo i nekonečné); existují však četné jiné příklady.

Theorie Booleových algeber má aplikace v těchto matematických disciplinách: Theorie pravděpodobnosti a statistika, theorie míry a integrálu, obecná topologie, matematická logika, theorie množin. Praktické aplikace mají Booleovy algebry v matematické statistice, v elektrických sítích a v počítacích strojích.

Z theorie Booleových algeber můžeme zde podat ovšem jen malou část. Naším hlavním cílem je věta o množinové representaci Booleových algeber (ovšem jen v konečném případě) — a její užití. Ukážeme si totiž, že ať se dojde ke konečné Booleově algebře jakkoli, vždy lze k ní najít isomorfní algebru všech částí jisté konečné množiny; jsou tedy dosud nám známé příklady *konečných* Booleových algeber typickými příklady. Podstatně složitější jsou poměry v nekonečných Booleových algebrách — a zvláště složité jsou v Booleových algebrách, jakých je potřeba v theorii pravděpodobnosti, kde se totiž dá spojovat (a protínat) nejen konečně, ale i nekonečně mnoho prvků. Těmito aplikacemi theorie Booleových algeber se však nemůžeme zde zabývat. Omezíme naše úsilí na to, abychom si objasnili podstatu aplikace konečných Booleových algeber v *elektrotechnice* a v *matematické logice*.

Cvičení k 2,4.

1. Dokažte (postupem duálním k postupu v textu) platnost duálního distributivního axiomu v množinových okruzích.

2. Dokažte, že k jednotkovému prvku v libovolném svazu může

být doplňkem jen nulový prvek a k nulovému prvku jen jednotkový prvek — je-li splněn axiom 7 doplňku.

3. Dokažte, že rovnost $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ je v každém svazu vždy splněna, je-li některý z prvků (a, b, c) nulou svazu. Totéž pro jednotku svazu na místě nuly. Totéž pro rovnost duální $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

4.*Dokažte, že svaz geometrického spojování a protínání bodů, přímek a rovin (k nimž přidána prázdná část prostoru = nulový prvek svazu) a celý prostor = jednotkový prvek svazu) není distributivní. (Návod: Zvolte a, b, c vhodně jako bod, přímku, rovinu.)

5.*Najděte, které ze svazů na obr. 16, 17, 18, 19 jsou distributivní. Které z nich splňují axiom doplňku? Které obojí?

6.*Dokažte, že svaz je distributivní, když a jen když neobsahuje podsvaz tvaru IV ani podsvaz tvaru V z obr. 19.

(Ukažte, že existence takových podsvazů by porušovala distributivní zákon — a obráceně, že tři prvky a, b, c porušující distributivní zákon, by vytvořily podsvaz typu IV nebo V z obr. 19.)

7.* Dokažte, že svaz všech kladných celistvých dělitelů libovolného celého čísla $N \geq 1$ (ve smyslu dělitelnosti jakožto částečného uspořádání) je konečný distributivní. Kolik prvků má tento svaz? Co je nulou a co jednotkou svazu?

8. Dokažte, že svaz všech racionálních dělitelů celého čísla N, které jsou celistvými násobky čísla $\frac{1}{N}$ (ve smyslu cvičení 4 k 2,3) je distributivní konečný svaz o jednotce svazu rovné číslu N a nule svazu rovné číslu $\frac{1}{N}$.

2,5. THEORIE (KONEČNÝCH) BOOLEOVÝCH ALGEBER.

Odvoďme si nejprve několik jednoduchých a potřebných důsledků z axiomů pro distributivní a komplementární svazy (Booleovy algebry).

1. *V distributivním svazu může existovat* (ve smyslu axiomu 7) *nejvýše jeden doplněk k danému prvku.* — Neboť vskutku, nechť k prvku x daného distributivního svazu — rozumí se svazu s nulou n a s jednotkou j — máme dva doplňky, x' a x^+. Pak je tedy (dle axiomu 7)