

Algebra 1

**poznámky ke studiu předmětu
verze 2016-2017**

Břetislav Fajmon

Obsah

1	Definice grupy	4
2	Grupa permutací	8
3	Grupa Z_n zbytkových tříd, dělitelnost v množině Z	12
4	Okruh, obor integrity a těleso	16
5	Základní vlastnosti grup	19
6	Podgrupy, cyklické grupy	20
7	Izomorfismy, homomorfismy a součiny grup	21
8	Relace, rozklady, uspořádané množiny	23
9	Význačné prvky v uspořádaných množinách	31
10	Polosvazy a svazy	43
11	Další vlastnosti svazů	52
12	Výsledky některých příkladů	62
12.1	Výsledky ke kapitole 8 – relace, uspořádané množiny	62
12.2	Výsledky ke kapitole 9 – význačné prvky v uspořádaných množinách	63
12.3	Výsledky ke kapitole 10 – polosvazy, svazy	63
12.4	Výsledky ke kapitole 11 – další vlastnosti svazů	64

Úvod

Vážení studenti,

tento text je podkladem pro zkoušku Algebra 1 a obsahuje materiál k 11 teoretickým otázkám, jež budou předmětem ústní zkoušky. Přednášky 5,6,7 nejsou zpracovány, ale podle odkazů do textu Rosický, jež najdete v IS, lze potřebný obsah dohledat ve skriptech nebo v zápiscích z přednášky.

Pokud odečteme pojmy, které jsou pokryty v jiném předmětu (kartézský součin, relace, zobrazení, bijekce, surjekce, injekce) nebo které nejsou v této fázi až zas tak důležité (jádro homomorfismu, horní a dolní jádro izotonního zobrazení), zůstává asi třicet devět pojmů, které musíte v tomto předmětu zvládnout. Pro jistotu uvádím jejich stručný přehled:

- Vlastnosti operací (1), (2), (3), (4), (5), (6), (7), (18), (19), (20).
- Struktury související s operacemi: grupoid, pologrupa, monoid, grupa, okruh, obor integrity, těleso, homomorfismus grup, izomorfismus grup, součin grup.
- Vlastnosti relací (11), (12), (13), úplná relace (nemá své číslo), operace průseku, operace spojení.
- Pojmy související s relací ekvivalence: ekvivalence, rozklad, faktormnožina, faktorgrupa.
- Pojmy související s uspořádanými množinami: poset (= částeně uspořádaná množina), coset (= řetězec = úplně uspořádaná množina), woset (= dobře uspořádaná množina), izotonní zobrazení posetů, izomorfismus posetů, \sqcap -polosvaz, \sqcup -polosvaz, svaz, úplný svaz.

Přeji Vám, abyste při studiu Algebry 1 našli něco, co Vás bude bavit, nebo aspoň viděli důležitost daných pojmů. Pomocí je také přemýšlet o konkrétních příkladech těchto pojmů v situacích známých číselných množin, operací průniku a sjednocení množin či vlastností dělitelnosti na množině celých nebo přirozených čísel.

Břeťa Fajmon,
prosinec 2016

Zdroje, ze kterých bylo čerpáno:

- Horák: Algebra a teoretická aritmetika, 1987 (jen mírně renovovaného v roce 2013, ovšem vydaného pod jiným názvem Základy matematiky);
- Rosický: Algebra – grupy a okruhy 2000, reprint textu z roku 1985, který obsahuje učivo v potřebné hloubce a rozsahu (a dobře podává přehled pojmů i pro předmět Algebra 3 ve druhém ročníku);
- Pinter: A book of Abstract Algebra, 2010. Není o moc novější než dvě předchozí knihy, je pouze reprintem druhého vydání z roku 1990 – dlužno říci, že tam, kde mi v předchozích dvou knihách chyběla motivace ke studiu či vysvětlení, mi je Pinter poskytl (vřele doporučuji);
- Ve druhé části (přednášky 8 až 11) jsem se držel především textu Kopka: Svazy a Booleovy algebry (Ústí nad Labem 1991, zejména str. 19-82).

1 Definice grupy

Struktura grupy, a vlastně vlastnosti očíslované (1) až (6), představuje axiomy běžně používané při práci s operacemi v aritmetice. Studovat tedy grupy a spol. znamená studovat axiomy, na kterých je založena celá aritmetika, věda počítání s čísly.

Tato kapitolka předkládá pouze definici vlastností (1) až (5), společně se základními příklady. Tyto vlastnosti budou podrobněji studovány v dalších kapitolách.



Definice 1.1. Axiom = fakt, jehož platnost se v dané matematické teorii předpokládá a nedokazuje (chceme jeho platnost předpokládat, protože se nám to jeví jako rozumné, ve shodě s realitou).



Definice 1.2. Operace $*$ na množině M ... zobrazení $M \times M \rightarrow M$, které přiřadí uspořádané dvojici $[a, b]$ (ve které záleží na pořadí) prvek $a * b \in M$.

Pojem operace je základní definicí prvních sedmi přednášek tohoto textu. Budeme si všimnout vlastností několika základních, ale též několika z různých důvodů zajímavých operací na konečných i nekonečných množinách.

Dříve, než začneme studovat konkrétní operace a struktury, několik označení pro stručný matematický zápis, která jsou bezpodmínečně nutná:

- označení: $\forall \dots$ pro každé, pro každou;
- označení: $\exists \dots$ existuje;
- označení: $\exists! \dots$ existuje právě jedno
- označení: $:$ (dvojtečka) ... tak, že; platí
- označení: $\Rightarrow \dots$ z toho plyne, odtud plyne; potom platí;
- označení: $\in \dots$ patří do, je prvkem;
- označení: $N = \{1, 2, 3, \dots\}$... množina přirozených čísel;
- označení: $N_0 = \{0, 1, 2, 3, \dots\}$... množina přirozených čísel včetně nuly;
- označení: $Z = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$... množina celých čísel;
- označení: množinu racionálních čísel označujeme a definujeme:

$$Q := \left\{ \frac{m}{n} : m \in Z, n \in N \right\}.$$

- označení: $\nexists \dots$ neexistuje, neexistují;
- označení: $\cap \dots$ průnik množin;
- označení: $\cup \dots$ sjednocení množin;
- označení: R ... množina reálných čísel;
- označení: I ... množina iracionálních čísel, tj. $R = Q \cup I$;

Axiomy pro počítání s čísly (které student zná ze střední školy) možná daly základ pro definice následujících vlastností, jež budou hrát klíčovou roli:



Definice 1.3. Vlastnost (1) ... uzavřenost množiny M vzhledem k operaci $*$:

$$\forall x, y \in M : x * y \in M. \quad (1)$$

Vlastnost (1) je přirozená – chceme, aby operace na množině byly definované takovým způsobem, aby výsledek operace zase byl prvkem dané množiny.



Definice 1.4. Vlastnost (2) ... asociativita operace $*$:

$$\forall x, y, z \in M : (x * y) * z = x * (y * z). \quad (2)$$

Vlastnost (2) platí pro většinu operací, o kterých bude za chvíli řeč – jednoduše řečeno, několikanásobné použití jedné operace nezávisí na uzávorkování. Snad jen operace $-$ a $:$ nejsou asociativní.



Definice 1.5. Vlastnost (3) ... existence jednotkového prvku vzhledem k operaci $*$:

$$\exists e \in M : x * e = e * x = x \quad \forall x \in M. \quad (3)$$

Příklad pro vlastnost (3): jednotkový prvek vzhledem k operaci sčítání je 0 (někdy nazýván též nulový prvek, aby nedošlo k záměně s prvkem 1), jednotkový prvek vzhledem k operaci násobení je 1.



Definice 1.6. Vlastnost (4) ... existence inverzních prvků vzhledem k operaci $*$:

$$\forall x \in M \exists x^{-1} \in M : x * x^{-1} = x^{-1} * x = e. \quad (4)$$

Příklad pro vlastnost (4): Pro číslo 2 je inverzním prvkem vzhledem k operaci sčítání číslo -2 , vzhledem k operaci násobení číslo $\frac{1}{2}$.

Uvedme nyní základní definice některých struktur, které splňují dané vlastnosti:



Definice 1.7.

- Grupoid $(M, *)$... množina M , na které operace $*$ splňuje vlastnost (1);
- Pologrupa $(M, *)$... množina M , na které operace $*$ splňuje vlastnosti (1),(2);
- Monoid $(M, *)$... množina M , na které operace $*$ splňuje vlastnosti (1),(2),(3) (někdy též: pologrupa s jednotkou, pologrupa s jednotkovým prvkem);
- Grupa $(M, *)$... množina M s operací $*$, která splňuje na množině M vlastnosti (1), (2), (3), (4).

Kromě těchto čtyř základních struktur, které byly právě definovány, ještě řada operací splňuje vlastnost (5) – viz následující definice. Tato vlastnost (5) už do samotné definice stěžejního pojmu grupy není zahrnuta, protože jak uvidíme v následujících dvou kapitolách, existují význačné příklady grup, které ji nespĺňují. Proto slovo „komutativní“ musíme k právě definovaným strukturám zvlášť dodat jako novou vlastnost.



Definice 1.8.

- Operace $*$ se nazývá komutativní na množině M , pokud platí vlastnost (5):

$$\forall x, y \in M : x * y = y * x. \quad (5)$$

- $(M, *)$ se nazývá komutativní grupoid, pokud je grupoid a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M .
- $(M, *)$ se nazývá komutativní pologrupa, pokud je pologrupa a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M .
- $(M, *)$ se nazývá komutativní monoid, pokud je monoid (tj. pokud je pologrupa s jednotkou) a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M .
- definice: $(M, *)$ se nazývá komutativní grupa, pokud je grupa a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M .

Podle předchozích pojmů platí tyto základní věty pro nám známé množiny:



Věta 1.9. $(N, +)$ je komutativní pologrupa.

Důkaz: Opravdu, operace sčítání je komutativní – platí (5). Sečtením dvou přirozených čísel je zase přirozené číslo – platí (1). Sečtení tří čísel z N nezáleží na uzávkování – platí (2). Vlastnosti (1),(2) platí na struktuře, která se nazývá pologrupa. Vlastnost (3) neplatí, protože $0 =$ jednotkový prvek vzhledem ke sčítání, není přirozené číslo (eventuálně bychom mohli tvrdit, že $(N_0, +)$ je monoid). Vlastnost (4) na $(N, +)$ neplatí, protože např. inverzní prvek k 2 je -2 , ale $-2 \notin N$. \square

Doplněním množiny N o nulový prvek a inverzní prvky vzhledem ke sčítání dostaneme:



Věta 1.10. $(Z, +)$ je komutativní grupa.

Dále se podívejme na některé základní množiny vzhledem k násobení:



Věta 1.11. (Z, \cdot) je komutativní monoid.

Důkaz: Opravdu, násobení je komutativní – platí (5). Vynásobením dvou celých čísel je zase celé číslo – platí (1). Násobení tří čísel nezávisí na uzávkování – platí (2). Jednotkovým prvkem vzhledem k násobení je číslo 1, což je celé číslo – platí tedy (3), tedy (Z, \cdot) je monoid. Ovšem inverzní prvky vzhledem k násobení nejsou celá čísla: např. inverzí k číslu 2 vzhledem k násobení je $\frac{1}{2}$, ale to není celé číslo, inverzí k 3 je $\frac{1}{3}$, ale $\frac{1}{3} \notin Z$, atd. \square

Doplněním množiny Z o inverzní prvky vzhledem k násobení by se zdálo, že se situace vylepší, ale pozor:



Věta 1.12. (Q, \cdot) , (R, \cdot) jsou komutativní monoidy.

Důkaz: Opravdu, přece jen chybí ještě jeden inverzní prvek, a sice pro nulu: rovnice $0 \cdot x = 1$ nemá řešení na množině Q nebo R , tj. neplatí vlastnost (4), dané množiny nejsou grupami vzhledem k násobení. \square

Čili vyloučením nuly z množin v předchozí větě dostaneme:



Věta 1.13. $(Q - \{0\}, \cdot)$, $(R - \{0\}, \cdot)$ jsou komutativní grupy.

Někdy též značíme

$$Q^* := Q - \{0\}, \quad R^* := R - \{0\},$$

tj. (Q^*, \cdot) , (R^*, \cdot) jsou komutativní grupy.

Tím, jak se axiomaticky zkonstruuje či popíše množina R pomocí množiny Q , se zde nebudeme zabývat, jen si nyní připomeňme, že existují jistá čísla, která nelze vyjádřit pomocí zlomku $\frac{p}{q} \in Q$; důkaz takového tvrzení je dobrou ilustrací dokazování sporem, takže by jej studenti mohli umět:



Věta 1.14. $\sqrt{2}$ není racionální číslo.

Důkaz: je např. ve skriptech Rosický, str. 15, za důkazem věty 3.6. \square

2 Grupa permutací

Kromě nekonečných množin, na kterých se definuje operace, se budeme občas zabývat i konečnými množinami. Například:

- označení: 2^A ... množina všech podmnožin množiny A ; to je totéž jako množina všech zobrazení množiny A do dvouprvkové množiny $\{0, 1\}$. Opravdu, např. pro $A = \{a, b, c, d, e\}$, když si vezmeme jakoukoli podmnožinu množiny A , například množinu $\{a, c, d\}$, tak ta je ekvivalentní tomu zobrazení f množiny A do $\{0, 1\}$, které zobrazí a, c, d na jedničku a b, e na nulu. Naopak, pokud si vezmeme jakékoli zobrazení $g : A \rightarrow \{0, 1\}$, například to, pro které $g(a) = 0, g(b) = 0, g(c) = 0, g(d) = 1, g(e) = 1$, to je ekvivalentní podmnožině $\{d, e\}$ množiny A . Pro všechny volby zobrazení dostáváme právě všechny různé podmnožiny množiny A .



Věta 2.1.

- Množina $(2^A, \cup)$ je komutativní monoid.*
- Množina $(2^A, \cap)$ je komutativní monoid.*

Důkaz: Opravdu, sjednocením či průnikem dvou podmnožin dané množiny A je zase nějaká podmnožina množiny A – platí (1). Operace \cup a \cap nezáleží na uzávkování – platí (2). Jednotkovým prvkem vzhledem ke sjednocení je \emptyset , jednotkovým prvkem vzhledem k průniku je celá množina A ... platí (3) vzhledem k oběma operacím. Inverze ke mnoha prvkům této struktury neexistují – například pro operaci sjednocení a podmnožinu $\{a\}$ množiny $A = \{a, b, c, d, e\}$ by musela existovat podmnožina X množiny A , aby $\{a\} \cup X = \emptyset$, a to neexistuje.

Důležitým příkladem (většinou konečné, ale i nekonečné, to závisí na počtu prvků dané množiny) je grupa permutací n -prvkové množiny, kde operací je skládání zobrazení.

Na permutaci např. 5-prvkové množiny se na SŠ pohlíželo jako na pořadí pěti jejich prvků, např. 51324. Na VŠ budeme na permutace pohlížet jako na:



Definice 2.2. Permutace n -prvkové množiny je bijektivní¹ zobrazení množiny $\{1, 2, \dots, n\}$ do sebe. S_n je množina všech permutací tohoto typu. Například permutace $f : M \rightarrow M$ pro $M = \{1, 2, 3, 4, 5\}$ definovaná

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

je bijektivní, takže existuje permutace f^{-1} k ní inverzní

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

¹Definice bijekce viz kapitola 6, nyní se spokojíme s intuitivní představou o bijekci, a sice že v bijekci $M \rightarrow M$ z každého prvku množiny M vychází právě jedna šipka, a do každého prvku množiny M směřuje právě jedna šipka daného zobrazení.

Protože permutace je zvláštní případ zobrazení a zobrazení $M \rightarrow M$ lze skládat za sebou, můžeme mluvit o operaci „skládání zobrazení“, respektive „skládání permutací“

- označení: $\circ \dots$ (čti „po“) operace skládání zobrazení;

Uvažme nyní například množinu permutací tříprvkové množiny $\{1, 2, 3\}$ do sebe – označme ji S_3 (písmeno S pravděpodobně pochází z toho faktu, že tyto permutace představují jakési jistým způsobem symetrické útvary, nebo modelují struktury, kterým se říká symetrie).



Věta 2.3. (S_3, \circ) je grupa, která není komutativní.

Množina S_3 má šest prvků:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix},$$

$$u = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}.$$

Prvek e je jednotkový, neprovede žádnou změnu v pořadí, například

$$s \circ e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = s.$$

Všimněme si, že nejprve je prováděno přiřazení e , a až poté ($\circ =$ „po“) je provedeno přiřazení s . Dále například

$$u \circ v = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = s,$$

$$v \circ u = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix} = t.$$

Čili je vidět, že $v \circ u \neq u \circ v$, tj. operace \circ je nekomutativní! Propočítáním všech možných 36 kombinací dostaneme přehlednou tabulku výsledků operace \circ .

Nejprve je potřeba říci, že u každé tabulky operace $*$ na konečné množině prvků je levý prvek x vybrán z levého sloupce záhlaví a pravý prvek y z horního řádku záhlaví; výsledek operace pak je znázorněn na průsečíku „řádku x “ a „sloupce y “:

$*$	\dots	y	\dots
\dots	\dots		
x	\dots	$x * y$	\dots
\dots	\dots		

Tedy konkrétně u operace \circ na množině S_3 dostaneme tabulku operace:

\circ	e	s	t	u	v	w
e	e	s	t	u	v	w
s	s	t	e	w	u	v
t	t	e	s	v	w	u
u	u	v	w	e	s	t
v	v	w	u	t	e	s
w	w	u	v	s	t	e

Uveďme nyní některé další vlastnosti této grupy, které vyplývají z kapitol 5 a 6, ale po jejich nastudování pak tyto vlastnosti přirozeně náleží do této kapitoly: Existuje šest podgrup² grupy (S_3, \circ) : tzv. triviální podgrupa, která obsahuje pouze jednotkový prvek e , s tabulkou operace

$$\begin{array}{c|c} \circ & e \\ \hline e & e \end{array},$$

další podgrupou je celá šestiprvková grupa (S_3, \circ) samotná. Kromě těchto dvou extrémně malých nebo velkých podgrup existují též tři dvouprvkové podgrupy

$$\begin{array}{c|cc} \circ & e & u \\ \hline e & e & u \\ u & u & e \end{array}, \quad \begin{array}{c|cc} \circ & e & v \\ \hline e & e & v \\ v & v & e \end{array}, \quad \begin{array}{c|cc} \circ & e & w \\ \hline e & e & w \\ w & w & e \end{array}$$

a jedna tříprvková podgrupa s tabulkou operace

$$\begin{array}{c|ccc} \circ & e & s & t \\ \hline e & e & s & t \\ s & s & t & e \\ t & t & e & s \end{array}.$$

Co se týká řádu³ jednotlivých prvků grupy (S_3, \circ) , platí:

- $e^1 = e$, tj. e je prvek řádu 1;
- $u^2 = v^2 = w^2 = e$, tj. prvky u, v, w jsou řádu 2;
- $s^3 = t^3 = e$, tj. prvky s, t jsou řádu 3.

Z řádů jednotlivých prvků také vidíme, že existuje $k = 6$ (nejmenší společný násobek řádů jednotlivých prvků) tak, že libovolný z prvků umocněný na šestou se rovná jednotce e :

$$e^6 = e, u^6 = (u^2)^3 = e^3 = e, v^6 = e, w^6 = e, s^6 = (s^3)^2 = e^2 = e, t^6 = e.$$

Dále, ohledně generátorů grupy S_3 lze říci, že (S_3, \circ) je generována dvěma svými prvky, a sice v a w , protože všechny další čtyři prvky grupy lze vyjádřit pomocí operace \circ a prvků v, w :

$$\begin{aligned} e &= v \circ v; \\ s &= v \circ w; \\ t &= s \circ s = (v \circ w)^2 = (v \circ w) \circ (v \circ w); \\ u &= w \circ s = w \circ (v \circ w). \end{aligned}$$

²Kapitola 6.

³Kapitola 5.

Podle označení množiny generátorů lze psát

$$(S_3, \circ) = \langle v, w \rangle .$$



Příklad 2.4. (reparát příkladu, který díky nesprávné definici skládání zobrazení na přednášce zaslouží také opravu) Jsou dány permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 3 & 1 & 4 & 6 & 2 & 7 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 1 & 6 & 3 & 4 & 2 & 5 \end{pmatrix} .$$

Vypočtěte $P \circ R^2$.

Řešení: Podle definice skládání zobrazení platí

$$P \circ R^2 = P \circ R \circ R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 1 & 6 & 3 & 4 & 2 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 7 & 2 & 6 & 3 & 1 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 7 & 3 & 2 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 7 & 3 & 2 & 1 & 5 & 4 \end{pmatrix} .$$

3 Grupa Z_n zbytkových tříd, dělitelnost v množině Z

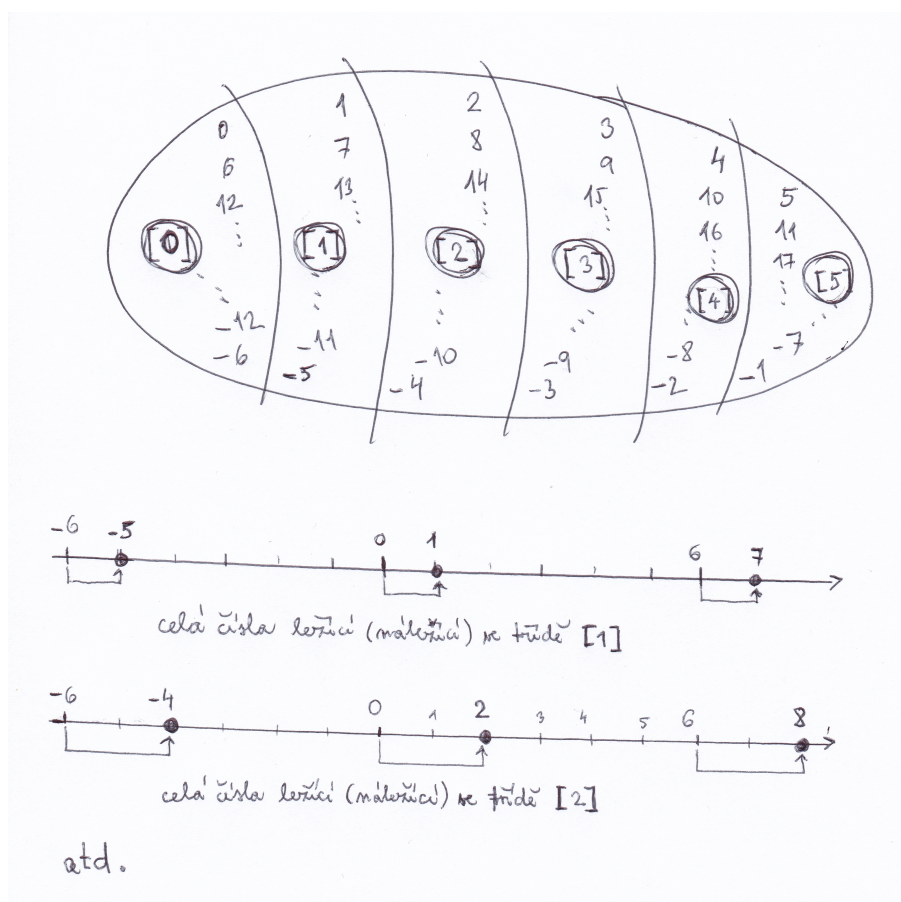
- definice: nesoudělná čísla a, b jsou taková celá čísla, která nemají žádného společného dělitele mezi přirozenými čísly, kromě jedničky;
- definice: dělitel čísla b (pro $b \in Z$);
- definice: největší společný dělitel dvou celých čísel b, c ;
- označení: $a|b$ (a dělí b , nebo též: a je dělitelem čísla b);
- důkaz věty 3.2 (Euklidova algoritmu) ze skript Rosický, str. 14.
- označení: $\wedge \dots$ a současně;
- označení: $\vee \dots$ nebo;
- definice: prvočíslo \dots takové přirozené číslo větší než 1, které je mezi přirozenými čísly dělitelné jen jedničkou a sebou samým;
- definice: celá čísla a, b jsou kongruentní podle modulu n , pokud $n|(b - a)$;
- označení: $a \equiv b \pmod{n}$;
- označení: $:= \dots$ definiční rovnítko – neznamená rovnici, ale definiční přiřazení, kdy levé straně přiřazujeme např. funkční předpis, označujeme nějakou množinu, a podobně.

Klíčovou strukturu představuje následující definice:

- definice: množina zbytkových tříd modulo $n \dots$ je zde pomocí popsát celou konstrukci této množiny například pro $n = 6$: Rozdělíme všechna celá čísla do šesti podmnožin podle toho, jak daleko je dané číslo na číselné ose vpravo od nejbližšího násobku čísla 6 (viz obrázek 1). Pak v každé třídě jsou právě ta celá čísla, která jsou mezi sebou kongruentní modulo 6, tj.

$$a \equiv b, \text{ když } 6|(a - b).$$

- Třída [1] obsahuje čísla 1, 7, 13, atd. ale také záporná čísla $-5, -11, -17$, atd., protože nejbližší násobek čísla 6 je od nich vzdálený o jednu jednotku vlevo.
- Třída [2] obsahuje čísla 2, 8, 14, atd. ale také záporná čísla $-4, -10, -16$, atd. a jsou to právě ta čísla, od nichž je vzdálen násobek šesti o dvě jednotky vlevo.
- Třída [3] obsahuje čísla 3, 9, 15, atd. ale také záporná čísla $-3, -9, -15$, atd.
- Třída [4] obsahuje čísla 4, 10, 16, atd. ale také záporná čísla $-2, -8, -14$, atd.
- Třída [5] obsahuje čísla 5, 11, 17, atd. ale také záporná čísla $-1, -7, -13$, atd.
- A konečně třída [0] obsahuje všechna celá čísla dělitelná šesti, tj. 0, 6, 12, atd. ale také záporná čísla $-6, -12, -18$, atd.



Obrázek 1: Rozdělení celých čísel do šesti podmnožin.

V každé třídě takto vytvořené jsou právě ta celá čísla, která jsou mezi sebou kongruentní modulo 6. Každá z těchto šesti podmnožin je nekonečná, odtud tedy honosný název „třída“.

Nyní se budeme dále dívat na tyto třídy jako na prvky množiny Z_6 (tj. množina Z_6 je konečná a má jen šest prvků!!!) a definujeme na této množině operace \oplus , \odot následovně:

$$[a] \oplus [b] := [a + b];$$

tj. součet tříd je třída, která obsahuje celé číslo $a + b$,

$$[a] \odot [b] := [a \cdot b];$$

tj. součin tříd je třída obsahující celé číslo $a \cdot b$. Lze ukázat, že tyto dvě operace nezávisí na výběru celých čísel a, b z daných nekonečných množin. Pro takto definovanou šestiprvkovou množinu a operace na ní nyní platí, že (Z_6, \oplus) je grupa, (Z_6, \odot) je monoid (= pologrupa s jednotkou $[1]$). Tato grupa (resp. monoid) se nazývá grupa zbytkových tříd modulo 6 (resp. monoid zbytkových tříd modulo 6).



Příklad 3.1. a) Pomocí tabulky operace \oplus dokažte, že (Z_6, \oplus) je grupa:

b) Pomocí tabulky operace \odot dokažte, že (Z_6, \odot) je monoid:

Tabulka 1: Tabulka operace \oplus na množině Z_6 .

\oplus	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Tabulka 2: Tabulka operace \odot na množině Z_6 .

\odot	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

- označení: $Z_n \dots$ množina zbytkových tříd modulo n ;
- označení: $Z_n^* \dots$ množina zbytkových tříd modulo n mimo prvek $[0]$, tj.

$$Z_n^* := Z_n - \{[0]\}.$$

Toto označení používáme i pro klasické množiny Q^* (racionální čísla mimo nuly), R^* (reálná čísla mimo nuly), protože se nám hodí, že (Q^*, \cdot) , (R^*, \cdot) jsou grupy (nulu z těchto množin musíme vyloučit, protože pro ni neexistuje inverzní prvek vzhledem k operaci násobení).

Zbytkové třídy lze sestavit nejen pro $n = 6$, ale pro jakékoli přirozené $n > 1$. Následující dvě věty studenti nemusí umět dokázat (ale je dobré si zapamatovat, co říkají):



Věta 3.2. *Ve struktuře (Z_n^*, \odot) existuje k prvku $[k]$ inverzní prvek vzhledem k násobení \odot právě tehdy, když k, n jsou nesoudělná.*

Například v (Z_6, \odot) neexistují k prvkům $[2]$, $[3]$, $[4]$ inverzní prvky, protože čísla 2, 3, 4 jsou soudělná s číslem 6.



Věta 3.3. *Důsledek předchozí věty: Pokud n je prvočíslo, tak k, n jsou nesoudělná čísla pro $k = 1, 2, \dots, (n - 1)$, tj. ke všem prvkům (kromě $[0]$, kterou jsme vyloučili) existují inverzní prvky vzhledem k násobení \odot , a tedy (Z_n^*, \odot) je grupa.*

Například (Z_7^*, \odot) je grupa. Čtenář by se o tom mohl snadno přesvědčit z tabulky operace \odot na množině Z_7^* .

4 Okruh, obor integrity a těleso

Okruh je po grupě druhou základní definicí struktury v kursech moderní algebry. A je to definice naprosto přirozená. Když totiž zkoumáme množinu Z , nikdy o ní ne přemýšlíme jako o množině s jedinou operací, ale máme současně na mysli sčítání (odčítání je skryto v inverzních prvcích) a násobení (dělení je skryto v inverzních prvcích). Matematik se tedy snaží formulovat, jaké zákonitosti platí pro interakci operací $+$ a \cdot . Tato interakce je popsána v definici algebraické struktury zvané okruh:



Definice 4.1. okruh (anglicky: ring) je množina $(M, +, \cdot)$ s operacemi $+$ a \cdot , které splňují vlastnosti:

- Operace $+$ splňuje vlastnosti (1), (2), (3), (4), (5), tj. $(M, +)$ je komutativní grupa;
- operace \cdot splňuje vlastnosti (1), (2), (3), tj. množina (M, \cdot) je monoid (= pologrupa s jednotkou);
- interakce operací $+$ a \cdot splňuje tzv. distributivní zákon = vlastnost (6):

$$\forall x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + z \cdot x \quad (6)$$

(rovnice jsou dvě díky tomu, že operace \cdot není obecně komutativní).

Název „distributivní“ odpovídá tomu, že po odstranění závorek se prvek x rozdělí = distribuuje k oběma členům součtu. Na vlastnost (6), pokud se na ni díváme zprava doleva, lze také pohlížet jako na pravidlo vytýkání – je možné vytknout před (nebo za) závorku prvek x , pokud jím násobíme ze stejné strany dva členy součtu. Nejrozumnější pohled na vlastnost (6) je ten, že se jedná o pravidlo, které určuje větší prioritu operace násobení před sčítáním – násobení je tak agresivní, že po odstranění závorek se vrhne na oba členy součtu, které byly uvnitř. Podobně též platí např.

$$8 + 2 \cdot 3 = 14,$$

tj. operace \cdot váže jednotlivá celá čísla s větší prioritou než je tomu u sčítání a odčítání.



Příklad 4.2.

- Příkladem konečného okruhu je struktura zbytkových tříd z předchozího oddílu 3, tj. množina (Z_n, \oplus, \odot) .
- Příkladem nekonečného okruhu je $(Z, +, \cdot)$, tedy množina celých čísel s tradičními operacemi sčítání a násobení.

Ovšem struktura (Z_n, \cdot) z minulé kapitoly vykazuje určité defekty, tj. obsahuje tzv. netriviální dělitele nuly:



Definice 4.3. netriviální dělitelé nuly jsou takové prvky a, b množiny M , které se nerovnájí nule ($0 =$ jednotkový prvek⁴ v grupě $(M, +)$), ale jejich součin (= výsledek operace násobení v pologrupě (M, \cdot)) je roven nule: $a \cdot b = 0$;

⁴Někdy se mu též říká nulový prvek, protože označení „jednotka“ či „jednotkový prvek“ je vyhrazeno jednotce 1 v pologrupě (M, \cdot) vzhledem k násobení.



Příklad 4.4. Příkladem struktury s netriviálními děliteli nuly je množina Z_6 zbytkových tříd modulo 6: její prvky $[2]$, $[3]$ nebo $[3]$, $[4]$ jsou netriviální dělitelé nuly, protože platí

$$[2] \odot [3] = [0], \quad [3] \odot [4] = [0].$$

Tito netriviální dělitelé nuly jsou dosti překvapivým jevem, který například u celých čísel nenastane – a také nežádoucím jevem. Okamžitá otázka pro matematický popis vystává, kdy se taková situace vyskytne a jak zaručit, že k ní nedojde. Z tohoto důvodu definujeme obor integrity:



Definice 4.5. obor integrity⁵ (anglicky: integral domain) je množina⁶ $(M, +, \cdot)$ s operacemi $+$ a \cdot , která je okruhem a navíc jsou splněny vlastnosti:

ad a) Operace $+$ nesplňuje nic navíc;

ad b) operace \cdot splňuje navíc:

- M neobsahuje netriviální dělitele nuly (vzhledem k operaci \cdot);
- vlastnost (5), tj. operace \cdot je komutativní na M ;

ad c) díky komutativitě operace \cdot lze distributivní zákon psát v jediné rovnici:

$$\forall x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z = y \cdot x + z \cdot x = (y + z) \cdot x.$$



Příklad 4.6.

- (Z_7, \oplus, \odot) je konečný obor integrity, protože 7 je prvočíslo, tj. (Z_7^*, \odot) neobsahuje netriviální dělitele nuly.
- $(Z, +, \cdot)$ je nejen nekonečný okruh, ale i nekonečný obor integrity, protože neobsahuje netriviální dělitele nuly a násobení je komutativní, a tedy distributivní zákon lze psát v jedné rovnici.

V klasické teorii operací se definuje ještě jeden pojem, který je dokonce ještě silnější než obor integrity, a sice těleso:



Definice 4.7. Těleso (anglicky: field ... proto některé české učebnice používají též název „pole“) je množina $(M, +, \cdot)$, která je oborem integrity a navíc operace \cdot splňuje vlastnost (4), tj.

⁵Význam slova **integrita**: celistvost. Ve stejné rodině významů je i slovo integer = celek, celé číslo. Podobně i slovo „integrál“ vlastně znamená součet, spojení, sečtení. A fráze „is an integral part of ...“ = je nedílnou součástí, je zakomponovanou součástí. V Bibli je hebrejský výraz „iš támím“ překládán do angličtiny jako „the man of integrity“, do češtiny jako „muž bezúhonný“, ale lepší by byl překlad „celistvý člověk“ ... to neznamená člověk naprosto dokonalý, ale člověk, který je ochoten pracovat na všech třech hlavních oblastech života: na svém vztahu k Bohu, na vztahu k lidem i na svém vztahu k práci. Tedy integrita je něco pozitivního, velmi žádoucího a charakterního. Podobně tomu bude i v matematice: obor integrity neobsahuje patologický jev výskytu netriviálních dělitelů nuly.

⁶Aby byla definice naprosto čistá, měli bychom dodat, že množina je minimálně dvouprvková, obsahuje totiž nulu jako jednotkový prvek vzhledem ke sčítání a jedničku jako jednotkový prvek vzhledem k násobení a $0 \neq 1$.

ad a) Operace $+$ nesplňuje nic nového,

ad b) operace \cdot splňuje navíc vlastnost (4), tedy $(M - \{0\}, \cdot)$ je grupa⁷;

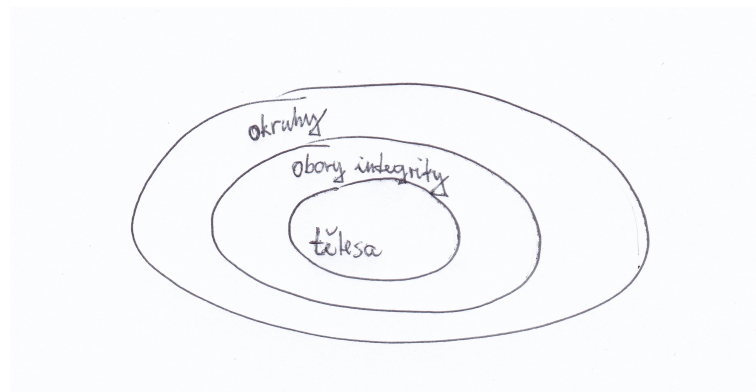
ad c) zde nic nového.



Příklad 4.8.

- $(\mathbb{Z}_7, \oplus, \odot)$ je konečný obor integrity, ale též i konečné těleso, protože v případě konečné množiny M pojmy obor integrity a těleso splývají.
- $(\mathbb{Q}, +, \cdot)$ je nekonečné těleso, protože $(\mathbb{Q} - \{0\}, \cdot)$ je grupa ... je splněna i vlastnost (4), že množina M obsahuje i inverzní prvky vzhledem k operaci násobení.
 $(\mathbb{Z}, +, \cdot)$ je nekonečný obor integrity, který není tělesem, protože množina \mathbb{Z} neobsahuje většinu inverzních prvků vzhledem k operaci násobení.

Tedy pojmy okruh, obor integrity a těleso představují struktury stále silnějších vlastností: Každé těleso je oborem integrity, každý obor integrity je i okruh (a z tranzitivity



Obrázek 2: Vztah mezi pojmy okruh, obor integrity, těleso.

pojmu plyne, že i každé těleso je okruh). Ale naopak to neplatí: existují okruhy, které nejsou oborem integrity, např. $(\mathbb{Z}_6, \oplus, \odot)$; a existují obory integrity, které nejsou tělesem, např. $(\mathbb{Z}, +, \cdot)$.

⁷Vlastnost (4) je silnější než vlastnost „neobsahuje netriviální dělitele nuly“, tj. u bodu b) je dostatečné uvést, že operace \cdot u tělesa splňuje (1),(2),(3),(4),(5). Lze dokázat tvrzení, že každé těleso je i oborem integrity, tj. těleso „neobsahuje netriviální dělitele nuly“.

5 Základní vlastnosti grup

- důkaz věty 1.6 ... Rosický, str.6;
- důkaz věty 1.8 ... Rosický, str.6;
- důkaz věty 4.1 indukcí ... Rosický, str. 22;
- definice: invertibilní prvek ... takový prvek, ke kterému v dané množině existuje prvek inverzní vzhledem ke studované operaci.
- definice: záporná mocnina prvku grupy se definuje jako příslušná kladná mocnina jeho inverzního prvku;
- definice: řád prvku grupy;
- znalost věty 4.17 = zákony o krácení ... vlastnost číslo (7): pokud (G, \cdot) je grupa a $a, b, c \in G$, pak platí implikace

$$a \cdot b = a \cdot c \Rightarrow b = c, \quad b \cdot a = c \cdot a \Rightarrow b = c. \quad (7)$$

Zde je dobré podotknout, že předpoklad, že G je grupa, je důležitý, protože například v problémové pologrupě (Z_6, \odot) zákony o krácení neplatí: například

$$[2] \odot [2] = [2] \odot [5],$$

ale po zkrácení prvku $[2]$ zleva bychom dostali $[2] = [5]$, což není pravda.

- důkaz věty 4.17 ... Rosický, str.26;

Pojmy záporná mocnina prvku a řád prvku doplňte prosím příklady.

6 Podgrupy, cyklické grupy

- definice: podgrupa H grupy G ;
- definice: vlastní podgrupy grupy G ... takové podgrupy, které „mají méně prvků“ než původní grupa G , tj. všechny možné podgrupy mimo samotnou grupu G .
- důkaz věty 5.5 ... Rosický, str.28.
- definice: podgrupa generovaná množinou M ... nejmenší možná podgrupa grupy G , která obsahuje množinu M .
- definice: cyklická grupa = grupa generovaná některým svým jediným prvkem
- označení: $\langle M \rangle$... podgrupa grupy G generovaná množinou M ;

Definice pojmů doplňte prosím příklady.

7 Izomorfismy, homomorfismy a součiny grup

- věta 4.18 a vlastnost (8): Pro grupu G a prvek $a \in G$ je následující zobrazení r_a bijekce:

$$r_a : G \rightarrow G \quad \text{je definované předpisem } r_a(x) := a \cdot x \quad \forall x \in G. \quad (8)$$

Tato věta ilustruje jeden důležitý fakt, že když vynásobíme jedním pevným prvkem a (to je pevné) po řadě všechny prvky x (to se mění), dostaneme jako výsledek těchto součinů zase všechny prvky grupy G , tj. daný řádek tabulky grupové operace obsahuje všechny prvky právě jednou (**tj. když se v řádku operace opakují některé prvky a nejsou všechny navzájem různé, tak víme, že množina G vzhledem k této operaci není grupa**).

Tohoto zobrazení se dále využívá v důkazu Caleyho věty (Rosický, str. 42, věta 8.14): Každá grupa je izomorfní nějaké podgrupě grupy permutací ... to plyne z toho, když si uvědomíme, že zobrazení r_a je permutace všech prvků grupy G , tj. přiřazení $a \rightarrow r_a$ je hledaný izomorfismus. Proto je r_a důležité a má své číslo⁸.

- vlastnost (9) ... Kdy zobrazení $f : (G_1, \cdot) \rightarrow (G_2, *)$ mezi grupami zachovává výsledky operace? Tehdy, když platí

$$f(a \cdot b) = f(a) * f(b) \quad \forall a, b \in G_1. \quad (9)$$

- definice: izomorfismus (součástí je vlastnost (9));
- definice: homomorfismus injektivní nebo surjektivní (součástí je vlastnost (9));
- definice: injekce⁹ = prosté zobrazení;
- definice: surjekce = zobrazení NA;
- definice: bijekce = vzájemně jednoznačné zobrazení;
- označení: $\cong \dots$ je izomorfní s;
- důkaz věty 4.18 ... Rosický, str.26;
- definice: jádro homomorfismu;
- označení: $\Leftrightarrow \dots$ právě tehdy, když;
- důkaz věty 6.4 ... Rosický, str.32;

⁸V roce 2016/17 studenti nemusí důkaz Caleyho věty umět ke zkoušce, ale v roce 2017/18 už ano.

⁹Lepší příklad injektivního homomorfismu než na přednášce: $f : R \rightarrow R$ je reálná funkce definovaná vztahem $f(x) = \exp x$... definiční obor je celé R , obor hodnot je pouze R^+ , tedy vlastní podmnožina množiny R .

- definice: součin grup ... Pokud G_1, G_2 jsou grupy, lze provést jejich kartézský součin $G_1 \times G_2$ a na tomto kartézském součinu definovat operaci \cdot vztahem (vlastnost (10))

$$[a, b] \cdot [c, d] := [a \cdot c, b \cdot d]. \quad (10)$$

Tato definice operace by se dala označit za přirozenou definici po složkách, $a \cdot c$ je totiž operace definovaná v grupě G_1 , a podobně $b \cdot d$ je operace definovaná v grupě G_2 – tedy nově definovaná operace těží z vlastností operací definovaných v jednotlivých grupách.

Důležitým příkladem součinu grup je množina $R \times R$, kde $(R, +)$ představuje množinu reálných čísel – pak grupa $R \times R$ s operací sčítání po složkách je množinou vektorů v rovině, grupa $R \times R \times R$ s operací sčítání po složkách je množinou vektorů v prostoru. Studium těchto důležitých grup se studenti budou věnovat v následujícím semestru v předmětu Algebra 2.

Definice pojmů doplňte prosím příklady.

8 Relace, rozklady, uspořádané množiny

V prvních sedmi přednáškách tohoto textu jsme se zabývali studiem pojmu „operace na množině M “, tj. zobrazení $M \times M \rightarrow M$. Sledovali jsme operace

- $+$, $-$ (odčítání bylo schováno v inverzích prvků u operace $+$),
- \cdot , $:$ (dělení bylo schováno u inverzí v grupě vzhledem k násobení),
- \cup , \cap ,
- \circ (= skládání zobrazení),
- \oplus , \odot (operace sčítání a násobení na množině zbytkových tříd).



Definice 8.1. V následujících zhruba čtyřech týdnech se budeme zabývat pojmem relace na množině M , což je obecně nějaká podmnožina kartézského součinu $M \times M$. Prvky relace jsou tedy uspořádané dvojice $[x, y]$, ve kterých záleží na pořadí.

Budeme studovat vlastnosti relací například

- \leq , \geq ;
- $|$ (dělí = je dělitelem);
- \subseteq , \supseteq ;
- \equiv (relace kongruence).

Hlavní rozdíl mezi relacemi a operacemi: výsledkem operace $*$ mezi dvěma prvky a , b byl obecně nějaký třetí prvek $a * b$, kdežto relace např. \leq jen uvádí do vztahu dané dva prvky a , b , když $a \leq b$ (odtud i název, který vychází z anglického relation = vztah).

(Horák, str. 24) Relaci lze podle definice zadat jako množinu uspořádaných dvojic (ve kterých záleží na pořadí prvků), například

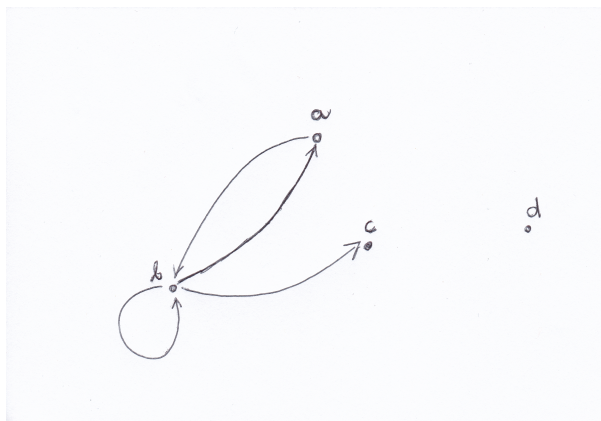
$$R = \{[a, b], [b, a], [b, c], [b, b]\};$$

ve shodě s učebním textem¹⁰ Kopka, Svazy a Booleovy algebry, str.17, budeme též relaci vypisovat takovým stylem, že označení relace bude umístěno v zápise mezi danými prvky (podobně jako \leq je napsáno mezi prvky a a b , tj. v našem příkladu tatáž relace bude zapsaná i vztahy

$$aRb, bRa, bRc, bRb.$$

Každou relaci na konečné množině můžeme též reprezentovat grafem, kde prvek $[a, b]$ znázorníme šipkou vycházející z a a směřující do b , prvek $[b, b]$ znázorníme smyčkou z b do b , atd. (viz obrázek Horák, str. 24):

¹⁰Zde náleží upozornění na kolizi značení: R v prvních sedmi kapitolách označovalo množinu reálných čísel, v kapitolách 8 až 11 to bude označovat relaci – obojí značení je tak tradiční a v literatuře zaužívané, že jej použiji i já navzdory tomu, že občas může dojít k nedorozumění.

Obrázek 3: Grafová reprezentace relace R – příklad.

Další způsob, jak lze reprezentovat relaci R , je matice relace (pro tentýž příklad):

$$\begin{array}{c} a \quad b \quad c \quad d \\ a \quad \left(\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \\ b \\ c \\ d \end{array}$$

(na průsečíku prvního řádku (= řádku prvku a) a druhého sloupce (= sloupce prvku b) matice je hodnota 1, protože uspořádaná dvojice $[a, b]$ je prvkem relace R ; dále na průsečíku druhého řádku a druhého sloupce matice je 1, protože smyčka $[b, b]$ je prvkem relace R ; na třetím a čtvrtém řádku matice jsou samé nuly, protože c ani d není první souřadnicí žádné uspořádané dvojice z R , atd. Čtyřem šipkám v grafové reprezentaci odpovídají čtyři hodnoty 1 v matici relace.



Příklad 8.2. (vyučující – studenti) V následující definici řekněte,

- (i) jak lze danou vlastnost poznat z grafové reprezentace relace (a z reprezentace maticí);
- (ii) jak musíme změnit výše obrázkem zadanou relaci, aby splňovala danou vlastnost (11), anti-(11), (12), anti-(12). *



Definice 8.3. Podobně jako u operací jsme studovali různé vlastnosti, i u relací budeme studovat určité vlastnosti a rysy. Nyní si uvedeme první z nich. Relace R na množině M se nazývá

$$\text{reflexivní, když } \forall x \in M : xRx; \quad (11)$$

$$\text{antireflexivní, když } \forall x \in M : \neg(xRx); \quad (\text{anti-11}),$$

$$\text{symetrická, když } \forall x, y \in M : xRy \Rightarrow yRx; \quad (12)$$

antisymetrická, když $\forall x, y \in M : (xRy \wedge yRx \Rightarrow x = y)$; (anti-12)

tranzitivní, když $\forall x, y, z \in M : xRy \wedge yRz \Rightarrow xRz$; (13)

V dalším budeme většinou uvažovat jen definici a grafovou reprezentaci relace, matricovou reprezentaci nemusíte příliš znát.



Příklad 8.4. (v trojicích, jen studenti) Vezměte si stránku A4 a rozdělte na osm částí. V každé části nakreslete pět bodů znázorňujících pětiprvkovou množinu, označte je a, b, c, d, e . Do množiny šipkami znázorněte relaci, která

1. je reflexivní,
2. je antireflexivní,
3. není ani reflexivní, ani antireflexivní,
4. je symetrická,
5. je antisymetrická,
6. není ani symetrická, ani antisymetrická,
7. je tranzitivní,
8. není tranzitivní. ★



Příklad 8.5. (v trojicích, jen studenti) Jaké vlastnosti splňuje relace $|$ (dělí, je dělitelem) na množině (Z, \cdot) ? Relaci $|$ definujeme normálně, jak bychom u dělitelnosti čekali:

$$\forall x, y \in Z : x|y \Leftrightarrow (\exists p \in Z : y = x \cdot p)$$



Definice 8.6. Relace R reflexivní a tranzitivní na M se nazývá kvaziuspořádání¹¹ (a splňuje tedy vlastnosti (11),(13)). Pokud R je navíc

- a) symetrická, nazývá se ekvivalence na M (tj. ekvivalence splňuje vlastnosti (11),(12),(13));
- b) antisymetrická, nazývá se uspořádání na M (tj. uspořádání splňuje vlastnosti (11),anti-(12),(13)).



Příklad 8.7. (vyučující – studenti) Jen dvě otázky, než pokročíme k vážnějším příkladům:

- Může být některá relace symetrická a antisymetrická současně?
- Může být některá relace ekvivalence a uspořádání současně? ★

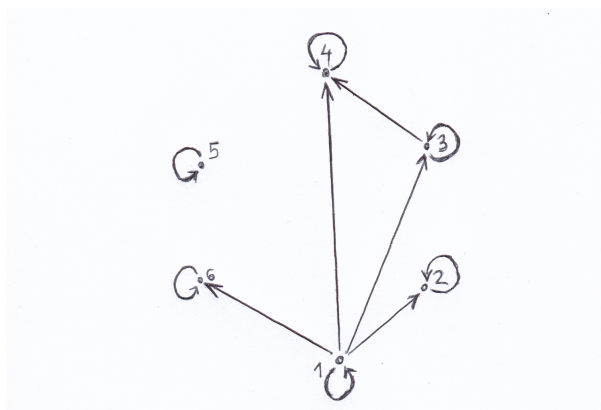
¹¹Další, název v novější literatuře: Předuspořádání ... tj. pokud přidáme dobrou třetí vlastnost této relace, stane se z ní uspořádání.

A nyní už zajímavější příklady:



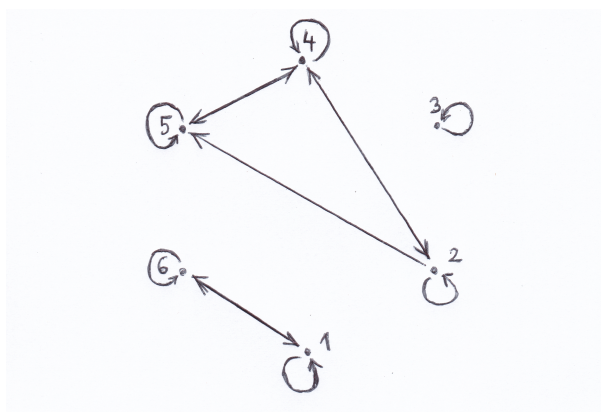
Příklad 8.8. (v trojicích, jen studenti) U následujících příkladů rozhodněte, jaké vlastnosti splňují zadané relace:

- Relace \leq na množině $N = \{1, 2, 3, \dots\}$;
- relace \parallel (být rovnoběžný) na množině přímek v rovině;
- Relace je zadána grafovou reprezentací¹² na obrázku 4:



Obrázek 4:

- Zadání opět grafem¹³, obrázek 5:



Obrázek 5:

V další definici a následném příkladu se podíváme na vztah mezi relací ekvivalence a rozkladem množiny. Tuto strukturu jsme zde už měli, ale nyní se na ni zaměříme ještě jednou spíše z pohledu relací než operací:

¹²Kopka, str.20, obr. 2a

¹³Kopka, str.20, obr. 2b.



Definice 8.9. Řekneme, že systém pomnožin M_i množiny M tvoří rozklad množiny M , když

$$\begin{aligned} a) \quad & \bigcup_{i=1, \dots, n} M_i = M; \\ b) \quad & M_i \cap M_j = \emptyset \text{ pro } i \neq j. \end{aligned}$$

Tj. ad a) sjednocením množin M_i je celá množina M , a ad b) množiny M_i jsou po dvou disjunktní, tj. každé dvě z nich mají prázdný průnik.

Definujeme-li nyní relaci R vztahem

$$xRy \Leftrightarrow x, y \in M_i \text{ pro nějaké } i, \quad (14)$$

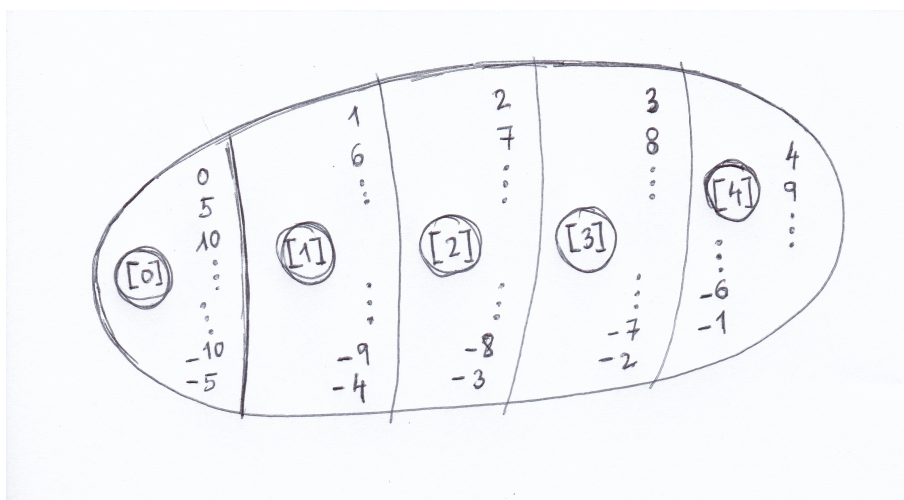
(prvky x, y jsou v relaci, když leží ve stejné třídě rozkladu), pak tato relace je ekvivalence a nazývá se relace určená (= indukovaná) rozkladem množiny M . Značíme

$$M/R := \{M_1, M_2, \dots, M_n\}$$

a množina M/R se nazývá faktorová množina množiny M podle ekvivalence R , nebo krátce faktormnožina¹⁴.



Příklad 8.10. Množina Z_5 : z kapitoly 3 už víme o relaci kongruence: $a \equiv b \pmod{5}$, když $5|(b-a)$. Podle této relace lze množinu celých čísel rozdělit do pěti podmnožin:



Obrázek 6: Množina zbytkových tříd Z_5 .

V této situaci lze nyní říci:

- Označíme-li $M_0 := [0]$, $M_1 := [1]$, $M_2 := [2]$, $M_3 := [3]$, $M_4 := [4]$, tak systém podmnožin $\{M_0, M_1, M_2, M_3, M_4\}$ tvoří rozklad množiny Z .
- Označíme-li znakem R danou relaci kongruence, můžeme psát xRy , když x, y náleží do stejné podmnožiny rozkladu ... tato relace je relací ekvivalence na Z (je to relace reflexivní (např. $5 \equiv 5$), symetrická (např. $5 \equiv 10$ implikuje¹⁵, že $10 \equiv 5$), tranzitivní ($5 \equiv 10$, $10 \equiv 30 \Rightarrow 5 \equiv 30$)).

¹⁴Česky: rozkladová množina (ale vžil se anglický název, FACTOR (jako sloveso) znamená ROZLOŽIT).

¹⁵Česky: z toho plyne, že ...

- c) Když se na M_i přestaneme dívat jako na množiny a začneme se na ně dívat jako na prvky, dostaneme pětiprvkovou množinu

$$Z/R := \{M_1, M_2, M_3, M_4, M_5\},$$

kde všechna čísla v každé množině M_i jsme ztotožnili v jedno a označili za jediný prvek. Je to faktorová množina množiny Z podle ekvivalence R , nebo krátce faktor-množina.

- d) $(Z/R, \oplus)$ je tzv. faktorgrupa, pokud definujeme sčítání \oplus pro nové prvky M_i , jak jsme to udělali v kapitole 3. Čili studenti se nemusí slova faktorgrupa bát – definujeme-li na faktormnožině operaci, která na ní splňuje vlastnosti (1),(2),(3),(4), mluvíme o faktorgrupě¹⁶. ★



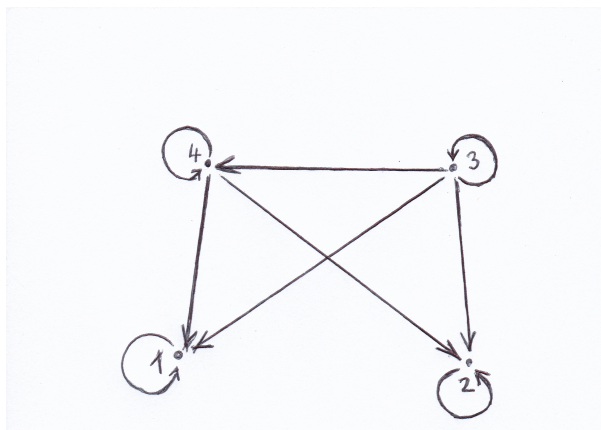
Příklad 8.11. (ve trojicích, jen studenti)

- i) Relace \equiv na $M := \{\frac{p}{q} : p \in Z, q \in N\}$ definovaná vztahem

$$\frac{a}{b} \equiv \frac{c}{d} \Leftrightarrow ad = bc$$

je ekvivalence. a) Jaké zlomky leží v jedné třídě rozkladu indukované touto relací?
b) co je to množina M/\equiv ?

- ii) Jaké vlastnosti splňuje relace na obrázku¹⁷ číslo 5?



Obrázek 7:



Definice 8.12. Množina M , na které je definovaná relace uspořádání, se nazývá (částečně) uspořádaná množina – v textu Kopka¹⁸ je označována poněkud nezvyklým termínem poset (z anglického PARTIALLY ORDERED SET)¹⁹.

¹⁶Vlastně probráno v kapitole 3, jen slovo faktorgrupa jsme tam nepoužili.

¹⁷Kopka 4b, str.24.

¹⁸Str.23, definice 1.6.

¹⁹Je to skutečně neobvyklý termín pro češtinu, až extrémní – ale navrhuji jej panu Kopkovi odpustit, určitě jej použil s dobrým záměrem, aby studenti a vyučující nemuseli stále vypisovat dlouhý termín **částečně uspořádaná množina**.

Ikdyž relace uspořádání je blízká relaci \leq (respektive \leq je čtenáři známým příkladem uspořádání), budeme ji označovat (v souladu s textem Kopka) obecnějším symbolem \trianglelefteq , který zaručuje, že se ne vždy bude jednat o relaci zcela totožnou s klasickou relací \leq na množině celých či reálných čísel.



Příklad 8.13. Je $(\mathbb{Z}, |)$ (s relací dělitelnosti) částečně uspořádaná množina (= poset)?
★

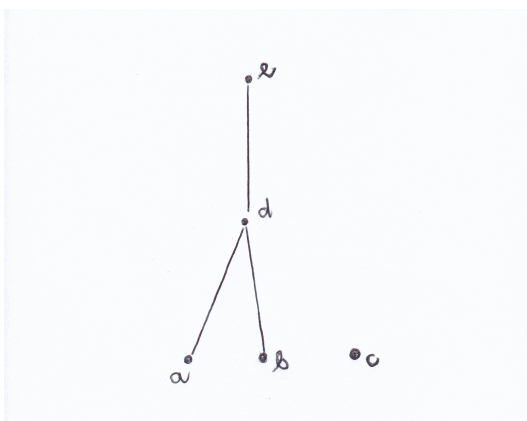


Definice 8.14. Pro relaci uspořádání zavádíme kromě grafové reprezentace přehlednější strukturu, a sice tzv. Hasseovy diagramy, ve kterých

1. reflexivitu (= smyčky) nevyznačujeme, protože ji automaticky předpokládáme u všech prvků uspořádané množiny;
2. šipky odstraníme tak, že Hasseův diagram jednoznačně orientujeme zdola nahoru – jestliže prvek je spojen s jiným prvkem výš v diagramu, tak je s ním v relaci;
3. hranami vyznačíme jen bezprostředně následující prvky – ostatní šipky vyplývající z tranzitivity nevykresluje; pak pokud $x \trianglelefteq y$, tak je mezi prvky x a y „řetězec“ spojů mezi bezprostředními předchůdci a následovníky;
4. antisymetrie bude z nákrešů patrna též – ta ovšem spočívá spíše v neexistenci oboustranných šipek mezi různými prvky.

Jako příklad zkusíme nakreslit Hasseův diagram pro pětiprvkovou množinu $M = \{a, b, c, d, e\}$ a relaci R na M definovanou výčtem uspořádaných dvojic (výsledek viz obrázek 8):

$$R = \{[a, a], [b, b], [c, c], [d, d], [e, e], [a, d], [d, e], [a, e], [b, d], [b, e], [d, e]\}.$$

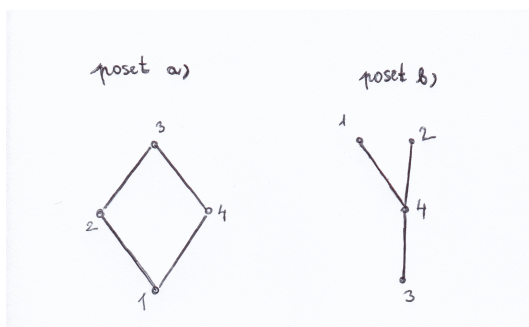


Obrázek 8: Hasseův diagram relace uspořádání.



Příklad 8.15. (ve trojicích, jen studenti) Vypište podle Hasseova diagramu relaci R výčtem uspořádaných dvojic na obrázku 9: a) poset a; b) poset b²⁰:

²⁰Kopka, str.28, obrázky 5a,5b.



Obrázek 9: Dvě uspořádané množiny.

Pojmy, označení a důkazy, které studenti musí znát z této kapitoly: studenti musí vysvětlit definice následujících patnácti pojmů a uvést vždy nějaký příklad: 1) relace, 2) reflexivní relace, 3) antireflexivní relace, 4) symetrická relace, 5) antisymetrická relace, 6) tranzitivní relace, 7) kvaziuspořádání, 8) ekvivalence, 9) uspořádání, 10) rozklad množiny, 11) třídy rozkladu, 12) ekvivalence indukovaná rozkladem, 13) faktorová množina množiny M podle ekvivalence R , 14) uspořádaná množina (= poset), 15) Hasseův diagram.

9 Význačné prvky v uspořádaných množinách

V této kapitole začneme studovat vlastnosti částečně uspořádaných množin (tzv. posetů, nečesky řečeno), tj. množin, na kterých je definována relace uspořádání, kterou lze reprezentovat Hasseovým diagramem.



Definice 9.1. Pokud (P, \leq) je poset, označme či definujme

- relace \triangleleft se nazývá ostré uspořádání v množině P , když $\forall x, y \in P$:

$$x \triangleleft y \Leftrightarrow (x \leq y \wedge x \neq y);$$

- relace \prec se nazývá pokrytí v množině P , když $\forall x, y \in P$:

$$x \prec y \Leftrightarrow x \triangleleft y \wedge (\forall a \in P : x \triangleleft a \leq y \Rightarrow a = y)$$

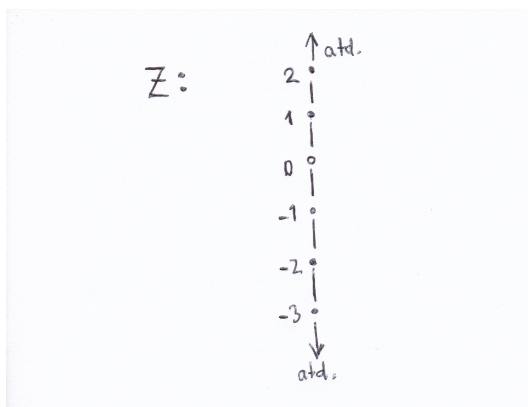
(jinými slovy, pokrytí je relace nejbližšího následovníka, tj. pokud x je pokryto prvkem y (tj. $x \prec y$), tak mezi x , y už nelze vložit další prvek a různý od y). Říkáme, že y „bezprostředně následuje za x “, nebo že „ y pokrývá x “.

- dodejme zde ještě definici úplně uspořádané množiny neboli řetězce: (P, \leq) je úplně uspořádaná množina = řetězec, pokud \leq je uspořádání a současně úplná relace, tj. pokud platí $x \leq y$ nebo $y \leq x$ pro každé dva $x, y \in P$. (anglicky: coset = completely ordered set)

Poznámka: pomocí ostrého uspořádání a pokrytí lze lépe popsat konstrukci Hasseových diagramů: vyznačujeme v nich hranami pouze relaci bezprostředního následovníka²¹.



Příklad 9.2. (ilustrační příklad) Na obrázku 10 vidíte příklad jednoho cosetu = řetězce – je jím nekonečná množina \mathbb{Z} .



Obrázek 10: Množina \mathbb{Z} je coset = řetězec.

²¹Kopka, str.30, lemma 4. Platí tedy pro konečný poset (P, \leq) a $a, b \in P$ toto: $a \triangleleft b$ (ostře menší než) znamená, že v množině P existuje řetězec bezprostředních následovníků $a = x_0 \prec x_1 \prec x_2 \prec \dots \prec x_n = b$.

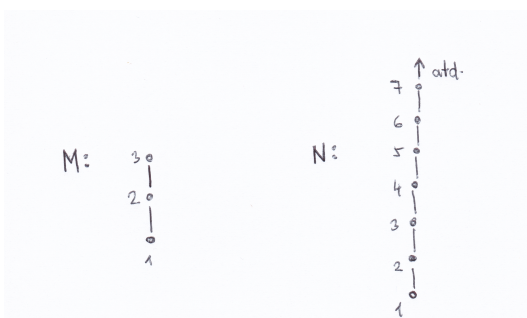


Definice 9.3. (Význačné prvky posetu) Pokud (P, \leq) je poset, $M \neq \emptyset$ je podmnožina množiny P , tak prvek $a \in M$ nazveme²²

- a) nejmenší prvek množiny M , když $\forall x \in M : a \leq x$;
- b) minimální prvek množiny M , když $\nexists x \in M : x < a$;
- c) největší prvek množiny M , když $\forall x \in M : a \geq x$;
- d) maximální prvek množiny M , když $\nexists x \in M : x > a$;

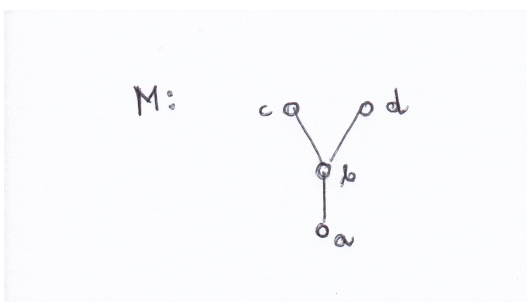


Příklad 9.4. (ilustrační příklad) Ad obrázek 11: V tříprvkové množině M s uspořádáním zadaným na Hasseovském diagramu je 1 prvek minimální a nejmenší současně, a dále 3 je prvek maximální a největší současně. V množině N s klasickým uspořádáním \leq je nejmenší prvek 1 a je to též minimální prvek. Největší prvek množiny N neexistuje.



Obrázek 11: Dvě dobře uspořádané množiny = wosety.

Dále na obrázku 12 je množina M , ve které a je minimální i nejmenší prvek současně. Na druhé straně, největší prvek tato množina nemá – má pouze dva maximální prvky c , d .



Obrázek 12: Rozdíl mezi maximálním a největším prvkem.

Tj. maximální prvek množiny M je takový, „nad kterým“ už není v této množině žádný prvek. Na druhé straně největší prvek musí být srovnatelný se všemi prvky množiny M a musí být větší nebo roven než libovolný z nich. *

²²Tyto definice nebudu zkoušet v Algebře 1, protože patří do předmětu Základy matematiky.

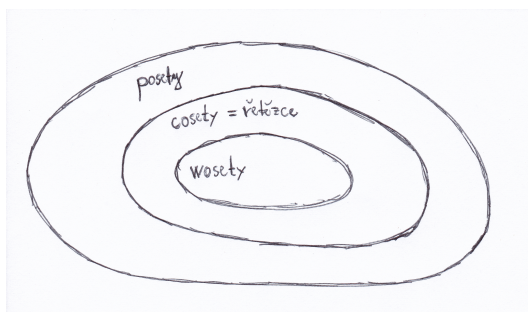
V úvodních definicích ještě budeme potřebovat zmínit definici dobře uspořádané množiny:



Definice 9.5. Poset (P, \leq) se nazývá dobře uspořádaná množina (woset ... z anglického well ordered set), když $\forall M \neq \emptyset, M \subseteq P: M$ má nejmenší prvek.

V dobře uspořádané množině musí tedy i každá dvouprvková podmnožina mít nejmenší prvek, tedy každé dva prvky jsou srovnatelné. Tedy **každá dobře uspořádaná množina je řetězec** (= každý woset je coset).

Jaký je tedy rozdíl mezi wosetem a cosetem? V cosetu nemusí mít některé podmnožiny (ani celá daná množina samotná) nejmenší prvek, kdežto ve wosetu ano. Tedy M a N z obrázku 11 jsou dobře uspořádané množiny, kdežto Z z obrázku 10 ne, protože samotná množina Z nemá nejmenší prvek.



Obrázek 13: Vztah mezi danými pojmy.

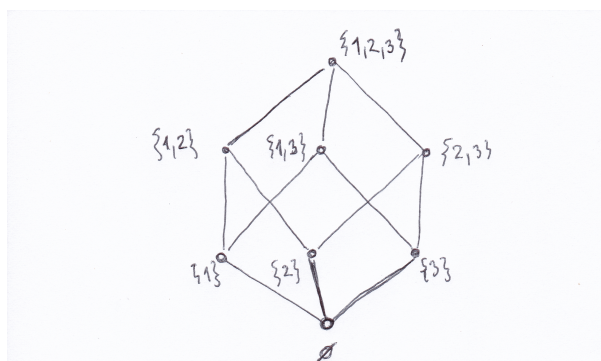
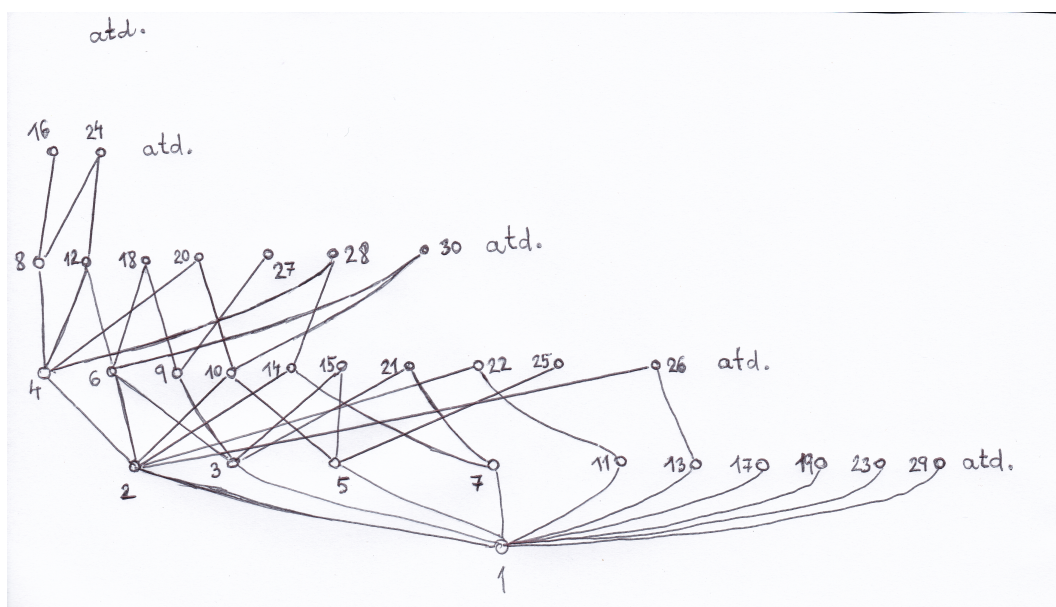
Na obr. 13 vidíme vztah mezi danými třemi pojmy: jen některé velmi hezké řetězce jsou wosety, všechny řetězce jsou cosety (to je ekvivalentní označení), a nejvíce je posetů, protože to jsou mnohem obecnější struktury, které mohou obsahovat i dvojice navzájem nesrovnatelných prvků.

Poté, co jsme si odbyli nezajímavé definice (ony tedy jsou důležité, ale dostane se na ně až v předmětu „teorie množin“), vraťme se k posetům a uvedeme si některé klíčové příklady posetů, které nejsou řetězce (tj. posety, které nejsou cosety).



Příklad 9.6. (ilustrační)

- Vraťme se k označení 2^P (viz kapitola 2) a nakreslíme strukturu posetu $(2^P, \subseteq)$ pro $P = \{1, 2, 3\}$ (tj. nezajímá nás v této chvíli operace průniku nebo sjednocení, ale relace \subseteq):
- Na množině N definujme uspořádání pomocí dělitelnosti, tj. $a \leq b \Leftrightarrow a|b$. Pak (N, \leq) je poset, který má nekonečně mnoho prvků. Na obrázku 6 je nakreslena jen jeho dolní část:

Obrázek 14: 2^P pro $P = \{1, 2, 3\}$.

Ze struktury dělitelů vidíme, že např. číslo 24 má vlastní dělitele 1, 2, 4, 8, 3, 6, 12 (a sebe sama jako nevlastního dělitele).



Příklad 9.7. (studenti ve trojicích) Nakreslete Hasseovský diagram posetu 2^P pro $P = \{1, 2, 3, 4\}$ – pro zjednodušení k uzlům diagramu nevpisujte závorky a čárky, tj. množiny budou označeny jen znaky prvků: např. \emptyset , 12, 124 jsou označení různých množin.

Podívejme se nyní na další význačné prvky v posetech:



Definice 9.8. Když (P, \leq) je poset a M je nějaká neprázdná podmnožina množiny P , nazýváme prvek $a \in P$ (pokud takový prvek existuje):

- dolní závora množiny M , pokud $a \leq x \quad \forall x \in M$;
- infimum množiny M (označujeme $\inf M$), pokud je největším prvkem na množině všech dolních závor množiny M ; tj. a je infimum, pokud pro všechny další dolní závory d platí

$$d \leq x \quad \forall x \in M \Rightarrow d \leq a;$$

- horní závora množiny M , pokud $a \succeq x \ \forall x \in M$;
- supremum množiny M (označujeme $\sup M$), pokud je nejmenším prvkem na množině všech horních závor množiny M . Tj. a je supremum, pokud pro všechny další horní závory h platí

$$h \succeq x \ \forall x \in M \Rightarrow h \preceq a;$$

Nejdůležitějším postřehem k předchozím definicím je asi to, že závory nebo infima-suprema množiny M nemusí samy být prvky množiny M !! Obecně závora, infimum či supremum je prvek množiny P , který může a nemusí ležet v dané množině M .



Příklad 9.9. (ilustrační)

- a) Například v posetu přirozených čísel s uspořádáním zadaným dělitelností těchto čísel (obr. 6) uvažujme množinu $M = \{12, 8, 20\}$. Dolní závorou množiny M jsou čísla 1, 2, 4 (společní dělitelé prvků v množině M), a tedy infimem je číslo 4 jako největší z těchto prvků (tj. infimem v $(N, |)$ je největší společný dělitel prvků v množině M).

Analogicky horní závorou množiny M jsou společné násobky čísel 12, 8, 20, tj. čísla 120, 240, 360, atd., a tedy supremem je nejmenší horní závora, tedy číslo 120.

- b) V posetu podmnožin tříprvkové množiny (obr. 14) například platí

$$\inf\{\{1, 2\}, \{1, 3\}\} = \{1, 2\} \cap \{1, 3\} = \{1\},$$

$$\inf\{\{1, 2\}, \{2\}, \{2, 3\}\} = \{2\},$$

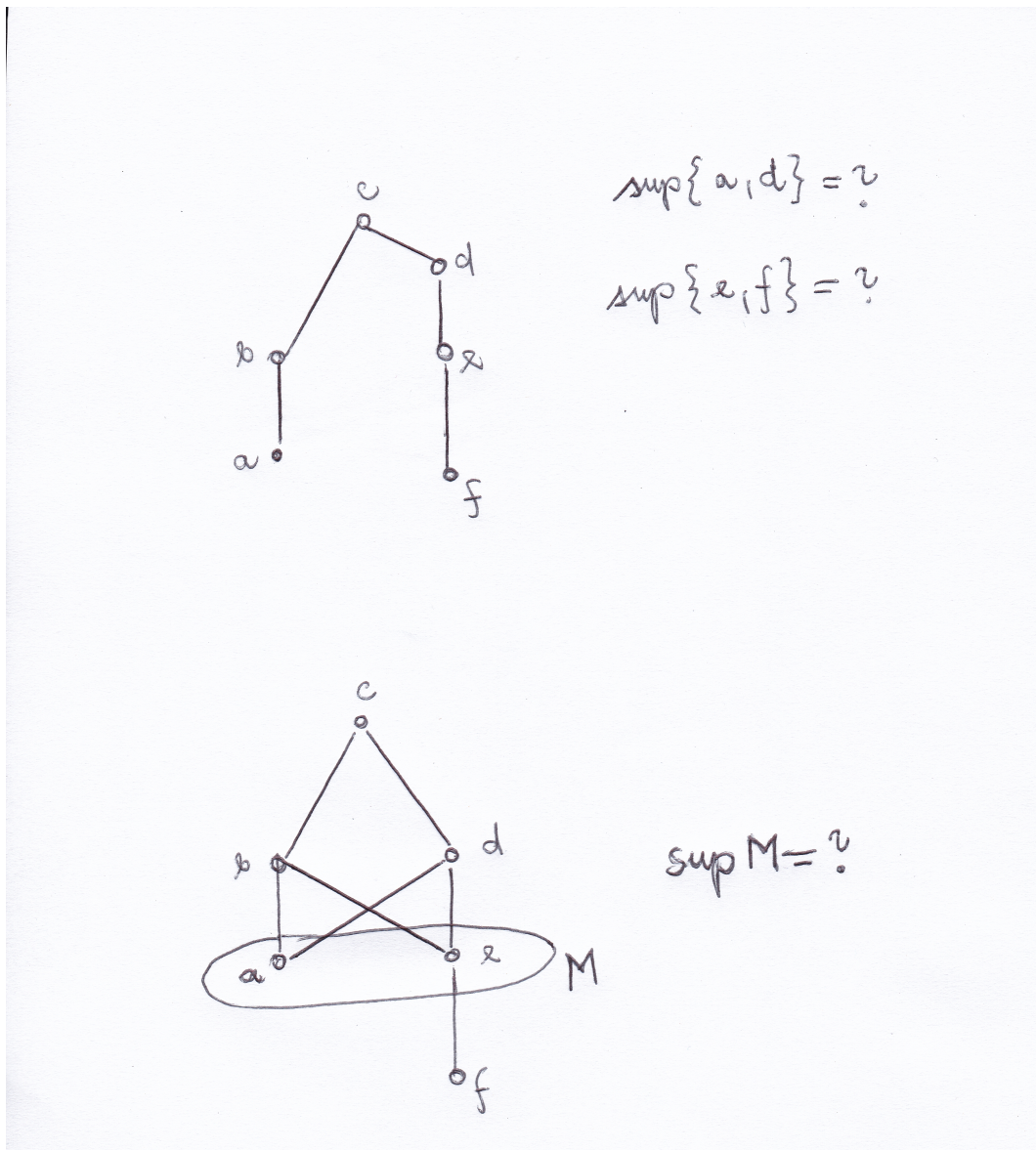
tedy infimem několika množin je jejich vzájemný průnik,

$$\sup\{\{1, 2\}, \{1\}\} = \{1, 2\} \cup \{1\} = \{1, 2\}$$

(supremem několika množin v dané struktuře je jejich sjednocení).



Příklad 9.10. Najděte suprema množin na obrázku, pokud existují:



Pojďme se nyní věnovat zobrazování mezi posety – to je už poslední částí této kapitoly a do velké míry to bude obsahovat podobné otázky jako homomorfismus grup. V případě posetů zde ovšem vystupuje pojem analogický, který budeme označovat jako izotonní zobrazení²³.



Definice 9.11. (Kopka, str.41) (P, \leq) , (A, \leq_1) jsou posety (index 1 u uspořádání posetu A naznačuje, že se jedná obecně o jinou relaci uspořádání, než je relace \leq v posetu P). Zobrazení $F : P \rightarrow A$ se nazývá izotonní zobrazení, když

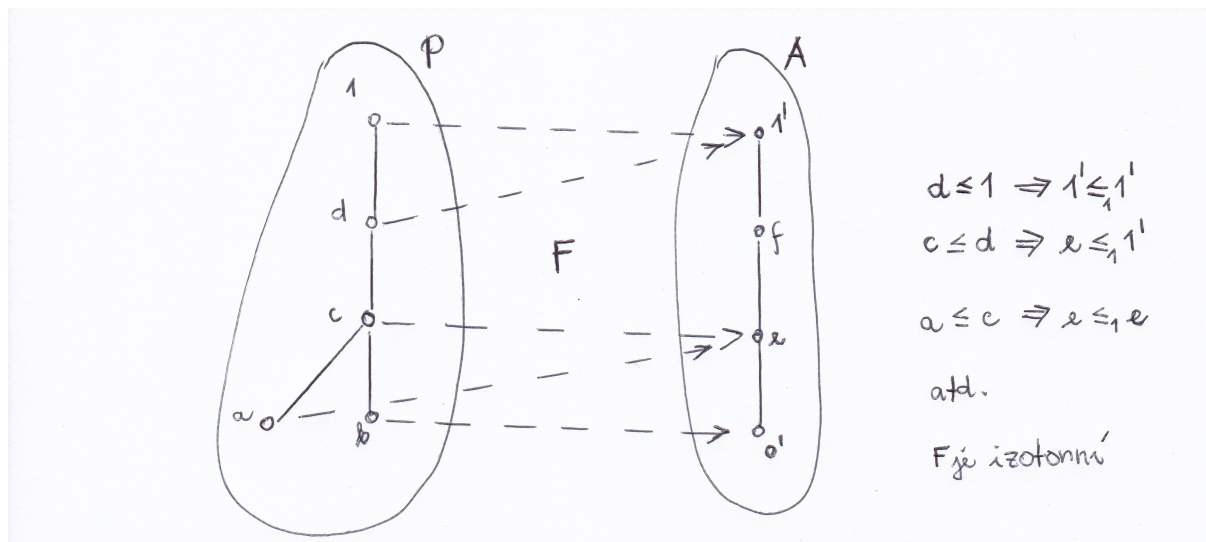
$$\forall x, y \in P : x \leq y \Rightarrow F(x) \leq_1 F(y). \quad (15)$$

²³Medicína: tonus = napětí (svalů), tj. špatný tonus znamená nachlazená, tvrdá a bolestivá záda nebo nohy (křeč ve svalech při zranění, podchlazení nebo s rostoucím věkem a nedostatkem pohybu). Izotonní roztok je takový roztok, který má stejné pH (= stejnou kyselost) jako tkáň, do které se má tento roztok při lékařském zákroku injekcí dostat (no a v matematice bude izotonní zobrazení asi zobrazení, které bude zachovávat určitou vlastnost).

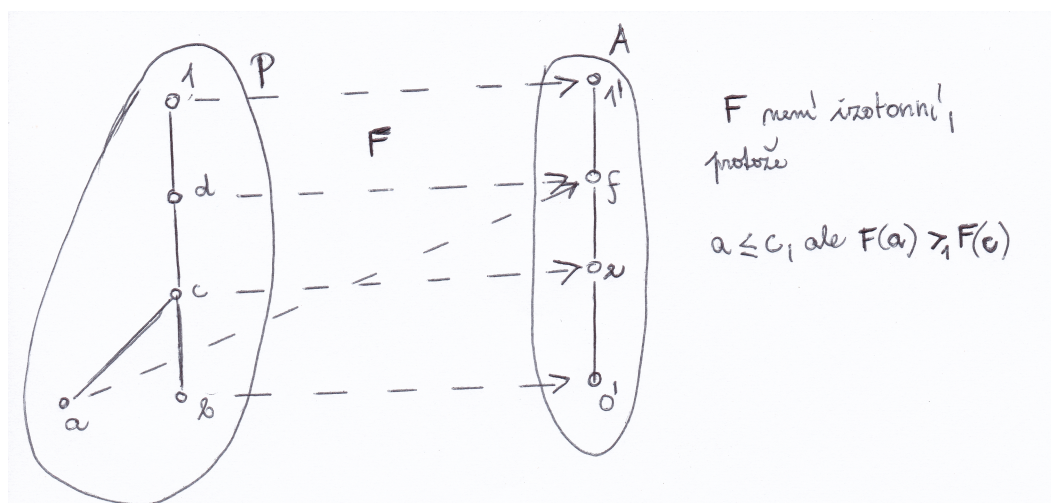
Poznámka: izotonní zobrazení tedy zachovává uspořádání – každé dva prvky uspořádané v množině P se zobrazí na dva prvky, které jsou uspořádané v množině A .



Příklad 9.12. (ilustrační)



Obrázek 15: Příklad izotonního posetového zobrazení F .



Obrázek 16: Zobrazení F není izotonní.

Z obrázku 15 je vidět, že izotonní zobrazení nemusí být injekce ani surjekce, a dokonce může zobrazit dva srovnatelné, ale různé prvky v množině P na jeden a tentýž prvek množiny A .

Celkem přirozeně tedy vyvstává definice izomorfismu posetů, který, podobně jako u izomorfismu grup, bude naprosto zachovávat celou strukturu a vlastnosti:



Definice 9.13. (P, \trianglelefteq) , (A, \trianglelefteq_1) jsou posety. Zobrazení $F : P \rightarrow A$ se nazývá posetový izomorfismus, když je izotonní bijekce a F^{-1} je také izotonní. Dané posety označujeme v takovém případě jako navzájem izomorfní.

Jinými slovy, jsou-li dva posety izomorfní, jsou v podstatě totožné, se všemi svými vlastnostmi, až na přeznačení prvků. To je vidět z následující věty, která vypisuje základní vlastnosti izomorfismu posetů:



Věta 9.14. $F : P \rightarrow A$ je posetový izomorfismus, (P, \trianglelefteq) , (A, \trianglelefteq_1) jsou posety. Pak platí:

(i) Ostře srovnatelné prvky se zobrazí na ostře srovnatelné prvky:

$$\forall x, y \in P : x \triangleleft y \Rightarrow F(x) \triangleleft_1 F(y);$$

(ii) F zachovává nesrovnatelné²⁴ prvky:

$$\forall x, y \in P : x \ntriangleleft y \Rightarrow F(x) \ntriangleleft_1 F(y);$$

(iii) F zachovává nejmenší prvek: obrazem nejmenšího prvku 0 (pokud existuje) posetu P je nejmenší prvek 0' posetu A ;

(iv) F zachovává minimální prvek: obrazem minimálního prvku (pokud existuje) posetu P je minimální prvek posetu A ;

(v) F zachovává infima konečných množin: Pro neprázdnou konečnou množinu $M \subseteq P$ je obrazem $\inf M$ (pokud toto existuje) v množině P prvek $\inf(F(M))$ množiny A , kde $F(M) \subseteq A$ je množina obrazů prvků z M , tj. $F(M) := \{F(x) : x \in M\}$:

$$F(\inf M) = \inf(F(M));$$

(vi) F zachovává největší prvek: obrazem největšího prvku 1 (pokud ten existuje) posetu P je největší prvek 1' posetu A ;

(vii) F zachovává maximální prvek: obrazem maximálního prvku (pokud ten existuje) posetu P je maximální prvek posetu A ;

(viii) F zachovává suprema konečných množin, pokud tato existují pro $M \subseteq P$:

$$F(\sup M) = \sup(F(M));$$

Důkaz: Podívejme se jen na platnost vlastností (i), (ii), ostatní vlastosti je možné dokázat analogicky.

Ad (i): Chceme dokázat, že posetový izomorfismus zachovává ostré uspořádání \triangleleft , které odpovídá danému neostrému uspořádání \trianglelefteq .

Tak tedy: uvažujme, že platí $x \triangleleft y$, tedy platí také $x \trianglelefteq y$ (to si připravujeme půdu pro použití vlastnosti (15), která platí pro neostré uspořádání). Protože izomorfismus F splňuje vlastnost (15), platí $F(x) \trianglelefteq_1 F(y)$.

²⁴Označení: $x \ntriangleleft y$ znamená, že prvky x, y jsou navzájem nesrovnatelné v relaci \trianglelefteq .

Mohou nastat dvě situace, a sice $F(x) \triangleleft_1 F(y)$ (a to máme dokázat, takže to je příznivá situace), nebo $F(x) = F(y)$ (to je nepříznivá situace). Prozkoumejme nepříznivou situaci: $F(x) = F(y)$ nemůže nastat, protože pak by platilo (protože inverzní zobrazení F^{-1} je též izotonní)

$$x = F^{-1}(F(x)) = F^{-1}(F(y)) = y,$$

ale to je spor s předpokladem, že $x \triangleleft_1 y$. Tedy musí nastat příznivá situace, a sice $F(x) \triangleleft_1 F(y)$.

Ad (ii): Dokazujeme sporem, a sice předpokládáme platnost negace, a z toho dospějeme ke sporu: Předpokládejme platnost negace $A \Rightarrow B$, a tedy platnost $A \wedge \neg B$:

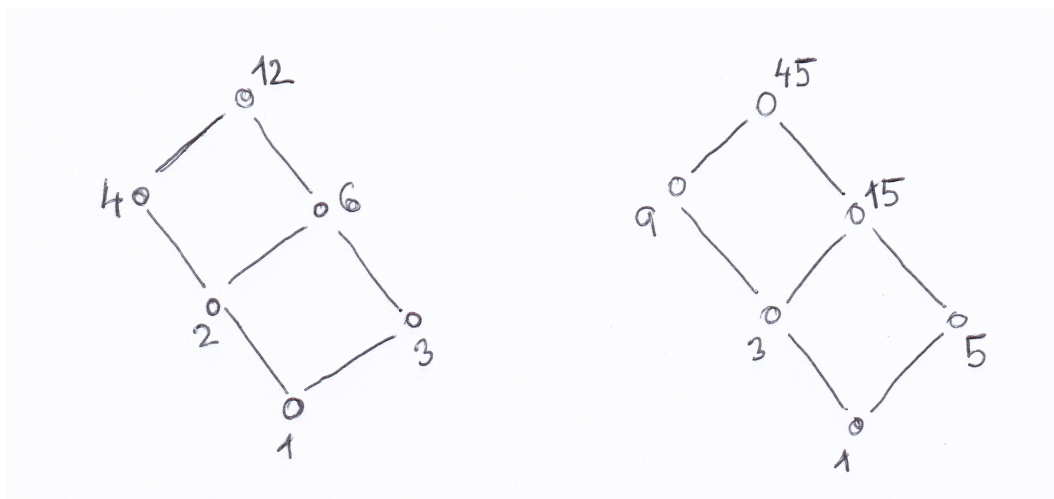
$$x \ntriangleleft y \wedge F(x), F(y) \text{ jsou srovnatelné.}$$

Pak protože F^{-1} je izotonní, musí být srovnatelné i prvky $F^{-1}(F(x)), F^{-1}(F(y))$, a protože $F^{-1}(F(x)) = x$ a $F^{-1}(F(y)) = y$, je to spor s předpokladem, že x, y jsou nesrovnatelné. \square



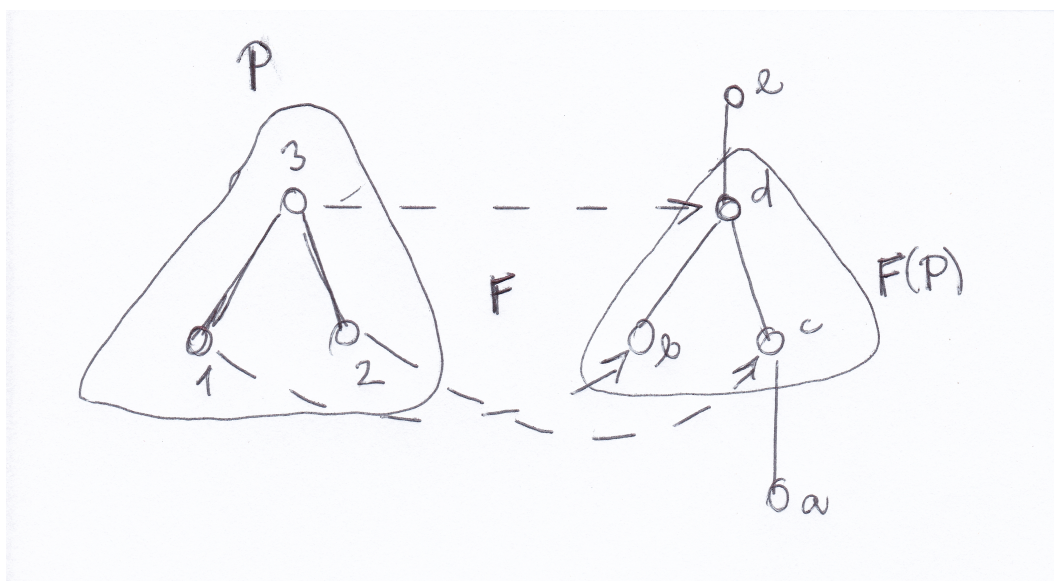
Příklad 9.15. Uspořádejme si tedy informace o izotonních zobrazeních mezi posety z hlediska analogického pojmu homomorfismus z teorie grup:

- Stejně jako u izomorfismu grup, i izomorfismus uspořádaných množin (= posetů) zachovává celou strukturu mezi danými dvěma množinami, všechny jejich vlastnosti. Například pro relaci dělitelnosti na množině přirozených čísel, uvažujme dva podposety posetu $(\mathbb{N}, |)$, které vidíme na obrázku 17 – poset dělitelů čísla 12 a poset dělitelů čísla 45. Z obrázku vidíme, že tyto posety jsou izomorfní.



Obrázek 17: Izomorfní posety.

- Podobně jako u injektivního homomorfismu grup se jednalo vlastně o izomorfismus první grupy s nějakou vlastní podmnožinou druhé grupy, i u injektivního izotonního zobrazení se jedná o izomorfismus prvního posetu s nějakou vlastní podmnožinou druhého posetu. Tj. všechny vlastnosti prvního posetu jsou zachovány jako součást vlastností druhého posetu.



Obrázek 18: Injektivní izotonní zobrazení = izomorfní vnoření jednoho posetu do druhého.

Na obrázku 18 vidíme injektivní izotonní zobrazení F – říkáme též, že poset P je **izomorfně vnořen** do druhého posetu A .

- Do třetice, podobně jako u surjektivního homomorfismu grup (projekce, která zachovává jistou vlastnost, ale jiné ztrácí), i surjektivní izotonní zobrazení sice zachovává vlastnost (15), ale některé charakteristiky prvního posetu ztrácí: Například prvky 1, 2 na obrázku 19 v posetu P nesrovnatelné jsou surjektivním homomorfismem zobrazeny na tentýž prvek $a \in A$.
- A konečně je teoreticky možná i čtvrtá situace, že totiž F je izotonní, ale není bijekce, ani injekce, ani surjekce – touto situací jsme se u grup ani nezabývali, i když určitě může nastat²⁵. Takové izotonní zobrazení vidíme na obr. 15 – vypuštěním prvku f z posetu A bychom ovšem dostali surjektivní izotonní zobrazení, tj. předchozí případ (tj. podobně jako případ 2 je ukryt v případě 1 – izotonní injekce je izomorfismem s nějakou vlastní podmnožinou posetu A – i případ 4 je ukryt v případě 3, a sice izotonní neinjektivní zobrazení je izotonní surjekcí na nějakou vlastní podmnožinu posetu A). Lze tedy mluvit o tom, že případ 4 znamená **surjektivní projekci posetu P na nějaký vlastní podposet posetu A** .



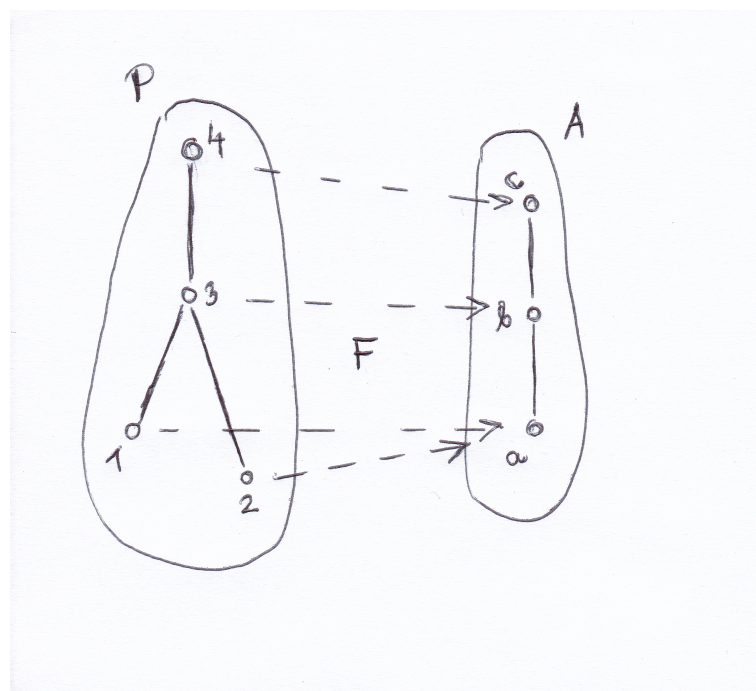
Příklad 9.16. Nakreslete Hasseovské diagramy všech neizomorfních posetů pro tříprvkovou²⁶ množinu.



Příklad 9.17. Nakreslete Hasseovské diagramy všech neizomorfních posetů pro čtyřprvkovou množinu.

²⁵Například projekce grupy $(\mathbb{Z}, +)$ do grupy permutací (S_3, \circ) definovaná $f(l) = e$ pro l liché, $f(s) = u$ pro s sudé ... f je jistě homomorfismus grup, protože $\{e, u\}$ je podgrupa grupy S_3 , ale není to injekce (jedná se o projekci všech sudých čísel na jeden prvek a všech lichých čísel na druhý prvek), ani surjekce, protože grupa S_3 má ještě další čtyři prvky – ovšem tuto situaci lze vypuštěním těchto čtyř prvků převést na situaci surjektivního homomorfismu. V ROCE 2017/18 DOPLNIT DO KAPITOLY 7.

²⁶Jednoprvkový poset existuje jediný, dvouprvkové posety existují dva neizomorfní.



Obrázek 19: Surjektivní izotonní zobrazení.

Stejně jako u homomorfismu grup byl význačným pojmem jádro homomorfismu, bude existovat i zde pojem „jádro izotonního zobrazení“. Ovšem na rozdíl od grupy (kde sledujeme, jaké prvky se zobrazí v homomorfismu na jednotku), v posetu máme teoreticky i dva význačné prvky – nejmenší prvek a největší prvek celého posetu (pokud tyto prvky existují). Definice jádra tedy budou dvě: horní jádro a dolní jádro.



Definice 9.18. $F : P \rightarrow A$ je izotonní zobrazení²⁷ mezi posety. Dolní jádro tohoto izotonního zobrazení se nazývá množina všech prvků posetu P , které se zobrazí na nejmenší prvek $0' \in A$,

$$\text{Ker}_d F := \{x \in P : F(x) = 0'\}$$

Horní jádro izotonního zobrazení se nazývá množina všech prvků posetu P , které se zobrazí na největší prvek $1' \in A$,

$$\text{Ker}^h F := \{x \in P : F(x) = 1'\}$$

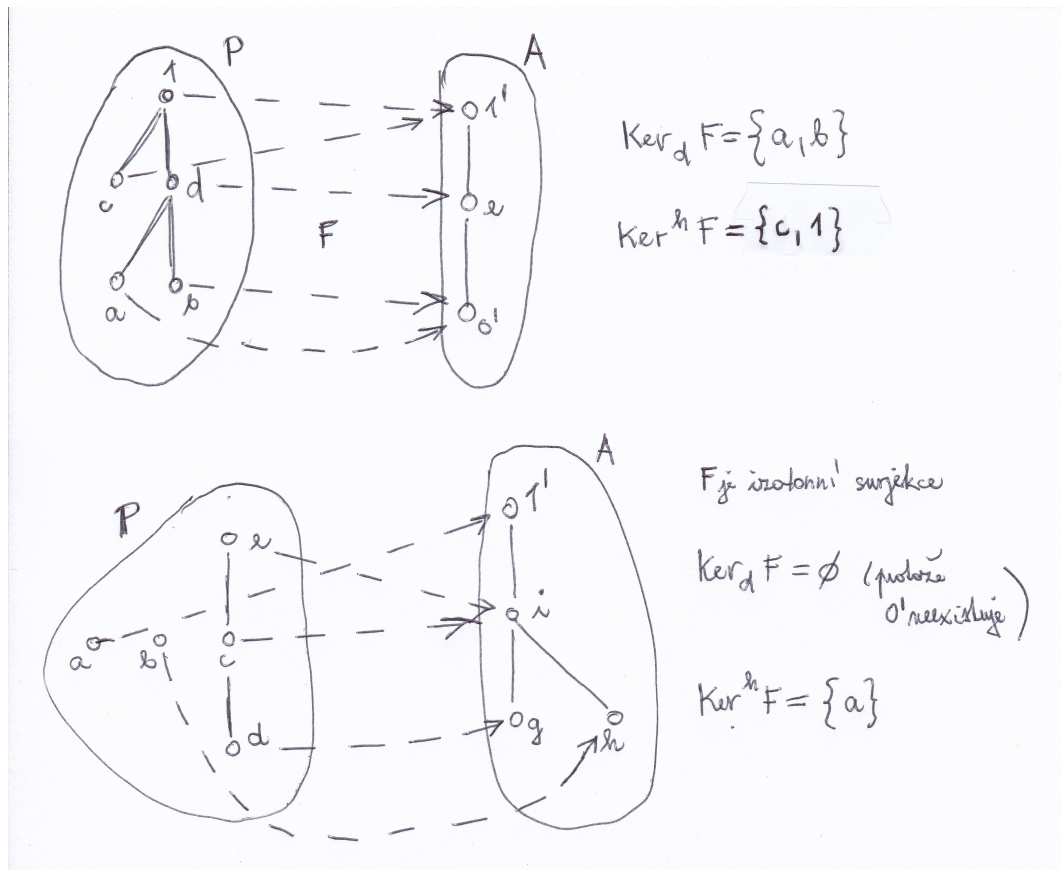
Pokud nejmenší (největší) prvek cílové množiny A neexistuje, říkáme, že $\text{Ker}_d F = \emptyset$ ($\text{Ker}^h F = \emptyset$).

A příkladem předchozího pojmu zakončíme tuto kapitolu:



Příklad 9.19. (ilustrační) Obrázek ilustruje různá horní a dolní jádra izotonní surjekce ve dvou situacích:

²⁷Kopka definuje horní jádro jen pro izotonní surjekci – to je jen malý rozdíl; obecně jádro má cenu sledovat jen u surjekce, protože u injekce je jádro buď jednoprvková, nebo prázdná množina, což není moc zajímavé.



Pojmy, označení a důkazy, které studenti musí znát z této kapitoly: studenti musí vysvětlit definice následujících pojmů a uvést jejich příklady a dokázat dvě drobné vlastnosti izomorfismu posetů: 1) ostré uspořádání, 2) relace pokrytí příslušná ostrému uspořádání, 3) coset = řetězec, 4) woset = dobře uspořádaná množina, 5) dolní závora, 6) infimum, 7) horní závora, 8) supremum, 9) izomorfismus posetů, 10) izotonní injekce, 11) izotonní surjekce, 12) důkaz věty 9.14.i), 13) dk. věty 9.14.ii), 14) dolní jádro izotonní surjekce, 15) horní jádro izotonní surjekce.

10 Polosvazy a svazy

V předešlé kapitole jsme zavedli pojmy infimum (= největší dolní závora) a supremum (= nejmenší horní závora). Pomocí těchto pojmů nyní definujeme na posetu P dvě operace²⁸: průsek \sqcap a spojení \sqcup .



Definice 10.1. Pokud v posetu (P, \leq) má každá dvouprvková podmnožina své infimum, lze definovat operaci průsek

$$x \sqcap y := \inf\{x, y\} \quad (16)$$

a poset (P, \leq) se nazývá průsekový polosvaz; to tedy znamená, že

$$\bullet x \sqcap y \text{ je dolní závora, tj. } x \sqcap y \leq x, \quad x \sqcap y \leq y; \quad (16a)$$

$$\bullet x \sqcap y \text{ je největší dolní závora, tj. } \forall d \in P : (d \leq x \wedge d \leq y \Rightarrow d \leq x \sqcap y). \quad (16b)$$

Pokud v posetu (P, \leq) má každá dvouprvková podmnožina své supremum, lze definovat operaci spojení

$$x \sqcup y := \sup\{x, y\} \quad (17)$$

a poset (P, \leq) se nazývá spojový polosvaz; to tedy znamená, že

$$\bullet x \sqcup y \text{ je horní závora, tj. } x \leq x \sqcup y, \quad y \leq x \sqcup y; \quad (17a)$$

$$\bullet x \sqcup y \text{ je nejmenší horní závora, tj. } \forall h \in P : (x \leq h, \quad y \leq h \Rightarrow x \sqcup y \leq h). \quad (17b)$$

Poznámka: Lidové vysvětlení pojmů průsek a spojení (a tedy potažmo i vysvětlení pojmů infimum, supremum):

a) Pokud poset (P, \leq) je průsekový polosvaz, v jeho Hasseově diagramu $\forall x, y \in P \exists! z \in P$,

- do něhož se po hranách dostanete z x i y cestou stále dolů (z je dolní závora množiny $\{x, y\}$),
- přičemž z je ze všech takových uzlů nejvýše (je největší dolní závora množiny $\{x, y\}$).

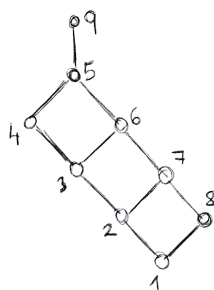
b) Pokud poset (P, \leq) je spojový polosvaz, v jeho Hasseově diagramu $\forall x, y \in P \exists! z \in P$,

- do něhož se po hranách dostanete z x i y cestou stále vzhůru (z je horní závora množiny $\{x, y\}$),
- přičemž z je ze všech takových uzlů nejnižší (je nejmenší horní závora množiny $\{x, y\}$).



Příklad 10.2. Rozhodněte, zda je daný poset také průsekový polosvaz nebo spojový polosvaz, vypočtete dané operace průseku nebo spojení:

²⁸Pozor: prvních sedm přednášek bylo věnováno operacím, přednáška 8 a 9 relacím – nyní v kapitolách 10 a 11 na struktuře zvané poset dochází k souhře těchto pojmů: pomocí relace uspořádání budeme definovat dvě operace. Studium této souhry relací a operací je svým způsobem zlatým hřebem tohoto předmětu.

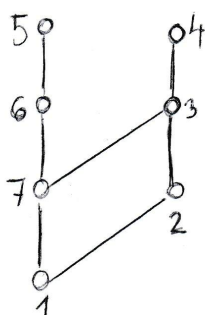


$$4 \sqcap 7 = \dots \quad 3 \sqcup 7 = \dots$$

$$6 \sqcap 2 = \dots \quad 6 \sqcup 8 = \dots$$

$$7 \sqcap 7 = \dots$$

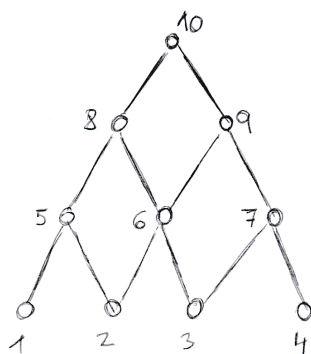
(i)



$$6 \sqcap 3 = \dots$$

$$6 \sqcup 3 = \dots$$

(ii)

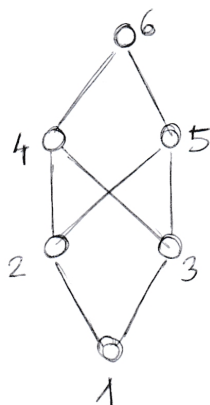


$$5 \sqcup 7 = \dots$$

$$2 \sqcap 3 = \dots$$

$$2 \sqcap 7 = \dots$$

(iii)



$$4 \sqcap 5 = \dots$$

$$2 \sqcup 3 = \dots$$

(iv)

Poznámka: Jak si studenti dobře zapamatují operace \sqcap , \sqcup ?

- operace \sqcap na množině²⁹ $(2^A, \subseteq)$ je totéž jako operace \cap ;
- operace \sqcup na množině $(2^A, \subseteq)$ je totéž jako operace \cup .

Tj. $(2^A, \subseteq)$ je důležitým příkladem posetu, který je současně průsekovým i spojovým polosvazem.

\sqcap , \sqcup jsou operace – lze tedy studovat bližší vlastnosti těchto operací!!!!!!!!!!!!!! Jsou pro ně splněny vlastnosti (1) až (7) definované v první polovině tohoto textu? Podívejme se pro začátek alespoň na vlastnosti (1) až (5), a pak zmíníme jednu novou, kterou označíme číslem (18):

- (1) Uzavřenost operace na dané množině platí z podstaty věci: z definice \sqcap –polosvazu nebo \sqcup –polosvazu už je zaručeno, že na daném nosiči (= v množině P) existuje příslušné infimum či supremum ... tj. tato vlastnost platí: operace \sqcap je uzavřená na daném \sqcap –polosvazu, operace \sqcup je uzavřená na každém \sqcup –polosvazu.
- (2) Asociativita operací \sqcap , \sqcup je splněna a je velmi zajímavé a instruktivní důkaz provést, využívá se při něm totiž základních vlastností operací průsek a spojení, které jsou obsaženy přímo v definici (tedy vlastnosti (16a),(16b), respektive (17a),(17b)). Dokažme³⁰ například asociativitu operace průsek:

$$\forall x, y, z \in P : (x \sqcap y) \sqcap z = x \sqcap (y \sqcap z).$$

The image shows a handwritten mathematical proof of the associativity of the intersection operation (\sqcap). The proof is divided into two parts. The first part shows $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$ using properties (16a) and (16b). The second part shows $x \sqcap (y \sqcap z) = x \sqcap y \sqcap z$ using properties (16a) and (16b).

²⁹Označení 2^A vysvětleno v kapitole 2.

³⁰Při odvozování důkazu je nad implikacemi nebo nerovnostmi vždy číslo vlastnosti, na základě které příslušná implikace nebo nerovnost platí. Vysvětlivky těchto vlastností:

(16a) ... průsek dvou prvků je menší nebo roven než každý z nich;

(16b) ... pokud nějaký prvek je menší nebo roven než jiné dva, pak z definice je též menší nebo roven než jejich průsek;

(17a) ... spojení dvou prvků je větší nebo rovno než každý z nich;

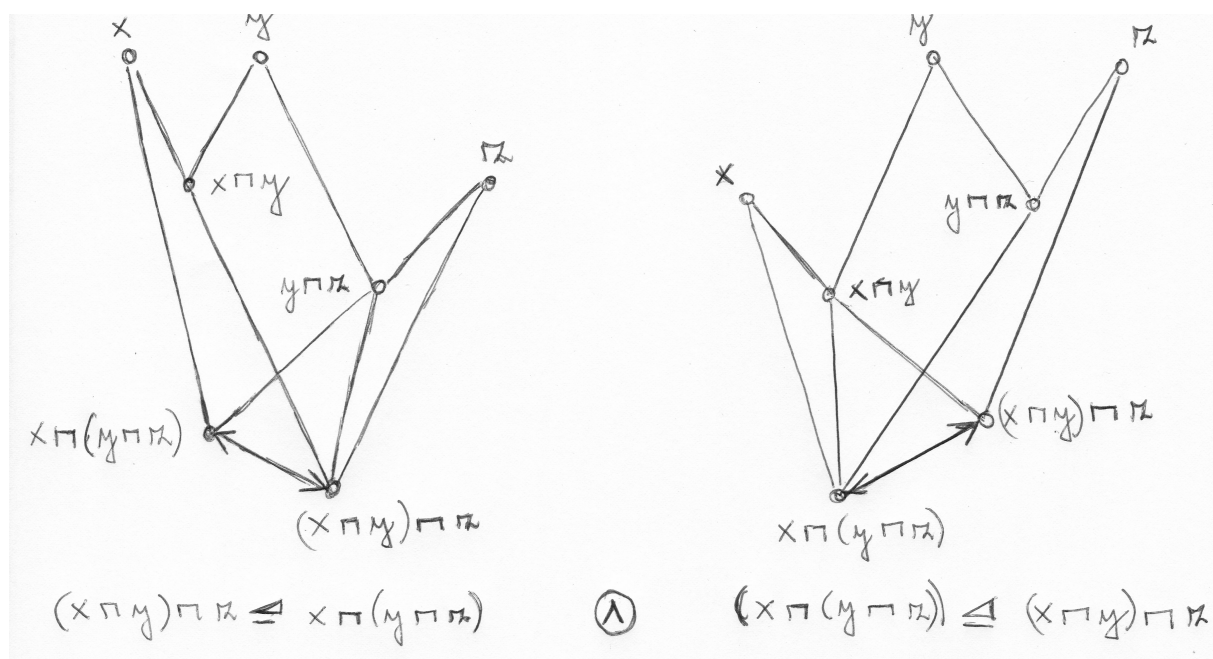
(17b) ... pokud nějaký prvek je větší nebo roven než jiné dva, pak z definice je též větší nebo roven než jejich spojení.

No a v této fázi důkazu zbývá už jen malý kousek, stačí si uvědomit, že relace \leq je antisymetrická, tj. platí

$$a \leq b \wedge b \leq a \Rightarrow a = b.$$

Tedy z obou nerovností, ke kterým jsem při odvozování dospěli, plyne nakonec rovnost, což je vlastnost (anti-12). **Asociativita pro druhou operaci, \sqcup , je dokazatelná analogicky.**

Pokud by stále ještě daný důkaz byl příliš náročný, lze si jednotlivé jeho části i nakreslit. První tři řádky předchozího odvozování lze znázornit v levé části následujícího obrázku, další tři řádky v pravé části:



Z obrázku je vidět, že antisymetrie (anti-12) zaručuje, že oba prvky, mezi kterými by existovaly oboustranné šipky, se musí rovnat.

- (3) Existuje v polosvazech jednotkový prvek vzhledem k operaci průsek či spojení? Jen někdy: Jednotkou vzhledem k operaci \cap je největší prvek \top -polosvazu, pokud ten existuje (on existovat nemusí pro tento typ polosvazu – například obrázek (ii) za definicí polosvazu). Podobně jednotkou vzhledem k operaci \sqcup je nejmenší prvek \perp -polosvazu, pokud tento existuje (existovat totiž nemusí pro \sqcup -polosvaz – například obrázek (iii) za definicí polosvazu).
- (4) Vzhledem k analogii \cap s operací průniku ve struktuře $(2^A, \subseteq)$ – viz úvodní označení a věta 1 v kapitole 2 – a faktu, že $(2^A, \subseteq)$ je průsekový polosvaz, neexistuje v této struktuře většina inverzních prvků, i když existuje jednotka vzhledem k dané operaci. Podobné platí o operaci \sqcup , když uvážíme, že $(2^A, \subseteq)$ je i spojový polosvaz. To jsou tedy protipříklady, které ukazují, že obecně neplatí vlastnost (4).
- (5) Komutativita platí!!! To plyne z faktu, že existence infima či suprema dvouprvkové množiny nezávisí na pořadí prvků v této množině.

- (18) A konečně slibovaná nová vlastnost, kterou nazveme idempotence (z latinského idem = totéž, stejné): Operace \sqcap , \sqcup jsou idempotentní na příslušných polosvazech, na kterých je lze definovat, a sice

$$\forall x \in P : x \sqcap x = x, x \sqcup x = x. \quad (18)$$

Idempotence je zajímavá vlastnost, protože vylučuje existenci mocnin – x^2 vzhledem k operaci \sqcap je totiž $x \sqcap x$, a to je rovno x , podobně

$$x^3 = x \sqcap x \sqcap x = x,$$

atd., zkrátka práce s mocninami je touto vlastností eliminována. Alespoň někdy nemusíme počítat žádné mocniny!! Analogicky platí pro operaci spojení

$$x^3 := x \sqcup x \sqcup x = x, x^4 = x, \text{ atd.}$$

Poznámka: Idempotentní prvek v grupě je jediný, a to jednotka této grupy – jen jednotka grupy splňuje vlastnost $e \cdot e = e$ (a více jednotek v grupě být nemůže, jak jsme dokázali o vlastnostech grupy). Ovšem pozor, idempotentní prvky (což jsou v polosvazech všechny prvky) nejsou vzhledem k polosvazové operaci průseku či spojení jednotky, protože vlastnost (18) platí vždy jen pro prvek samotný, nikoli pro různé prvky x, y . Polosvazy jsou (pokud splňují vlastnost (3)) většinou pologrupy, ale jejich operace \sqcap, \sqcup jsou jiného charakteru než operace v grupách. Lze tedy uzavřít, že pologrupy nám jsou zdrojem řady zvláštních vlastností – existence dělitelů nuly v Z_n , vlastnost idempotence ve struktuře všech podmnožin, apod. Co nás tady ještě čeká?

Analogií operace \sqcap s průnikem a operace \sqcup se sjednocením na struktuře $(2^A, \subseteq)$ jsme si připravili půdu k následující definici, která je tedy celkem přirozená. V dalším se teď budeme zabývat otázkou: Jaké vlastnosti má poset, který je současně polosvazem obou typů?



Definice 10.3. Poset (P, \leq) , který je současně průsekový i spojový polosvaz, se nazývá svaz³¹. Analogicky lze říci, že protože svaz je spojením vlastností průsekového polosvazu a spojového polosvazu, tak pro svaz je charakteristické, že s každou svou dvouprvkovou podmnožinou obsahuje i její infimum a supremum³².

Pod svazem tedy chápeme strukturu $(P, \leq, \sqcap, \sqcup)$, kde

- relace \leq splňuje vlastnosti (11), (anti-12), (13);
- operace \sqcap splňuje vlastnost (16) (tedy prakticky obě z vlastností (16a),(16b));
- operace \sqcup splňuje vlastnost (17), tedy prakticky v řeči nerovností to jsou vlastnosti (17a),(17b).



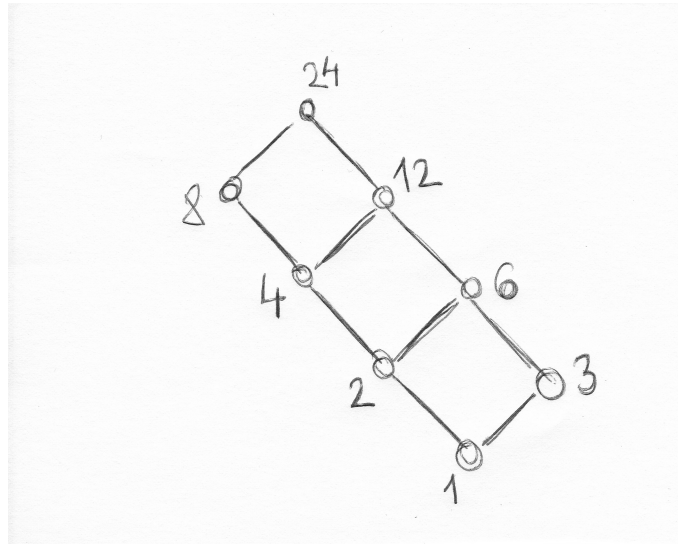
Příklad 10.4. Několik příkladů svazů:

³¹Anglicky: lattice. Pozor, neplést s hlávkovým salátem: lettuce. Anglicky polosvaz: semilattice.

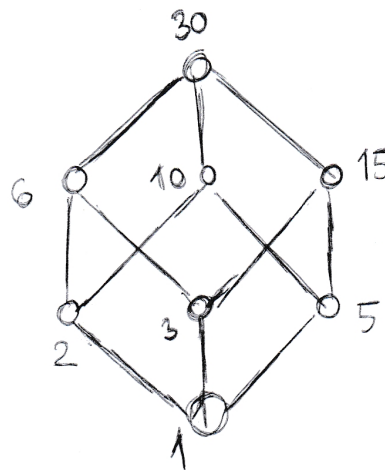
³²Které ovšem nemusí ležet přímo v dané dvouprvkové podmnožině, jak jsme už na několika příkladech viděli.

Př. 1 Po struktuře $(2^4, \subseteq)$ je i druhý hlavní příklad předchozí kapitoly (6 b)), množina N s relací definovanou na základě dělitelnosti, svaz. Průsekem dvou přirozených čísel je jejich největší společný dělitel, spojením dvou čísel je jejich nejmenší společný násobek – tyto dvě charakteristiky vždy existují pro každá dvě přirozená čísla.

Př. 2 I některé podposety svazu $(N, |)$ jsou svazy, například podsvaz³³ všech dělitelů čísla 24

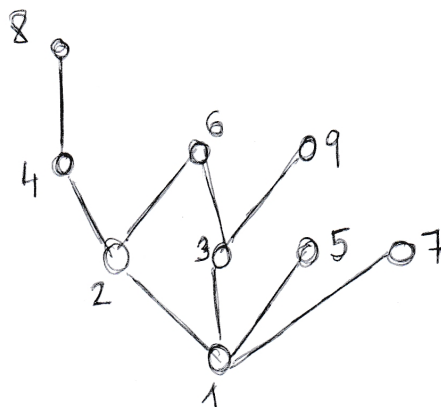


nebo podsvaz všech dělitelů čísla 30



Naopak řada podposetů posetu $(N, |)$ svazem není, protože nejsou uzavřené na operaci průseku a spojení. Například podposet prvních devíti přirozených čísel není svazem, protože v něm neexistuje například supremum dvouprvkové množiny $\{4, 6\}$:

³³Z příkladů je vidět, že aby podmnožina svazu byla též svazem, musí být uzavřená vzhledem k operacím průsek a spojení.



Př. 3 Každý řetězec (= coset) je svaz ... například N s klasickým uspořádáním \leq je svaz, (\mathbb{Z}, \leq) je svaz.

Př. 4 Vybrané podmnožiny trojrozměrného prostoru R^3 s přirozeným uspořádáním \subseteq tvoří svaz: prázdná množina, všechny jednoprvkové množiny (= všechny body trojrozměrného prostoru), všechny přímky, všechny roviny, a nakonec celý prostor R^3 samotný.

Pak na této struktuře lze definovat průsek zcela normálně množinově (pro přímky p, q je $p \sqcap q$ jejich průsečík, nebo prázdná množina v případě rovnoběžných různých nebo mimoběžných přímek; pro přímku a rovinu je jejich průsekem též průsečík, nebo prázdná množina, pokud průsečík neexistuje, nebo celá daná přímka, pokud v dané rovině leží; průsekem dvou rovin je jejich průnik, atd.).

Operaci spojení nelze definovat přímo množinově jako sjednocení, protože mnohá sjednocení nejsou mezi vybranými prvky struktury – ovšem definujeme-li např. spojení dvou různoběžných či rovnoběžných přímek jako rovinu, která obě přímky obsahuje, spojení bodu a přímky jako buď tuto přímku, pokud na ní bod leží, nebo celou rovinu, ve které leží od i přímka, spojení dvou mimoběžek jako celý prostor R^3 , protože to je jediný mezi prvky struktury, který obě mimoběžky obsahuje, atd., tak je opět zaručeno, že pro každé dva prvky struktury existuje v ní i jejich supremum³⁴.

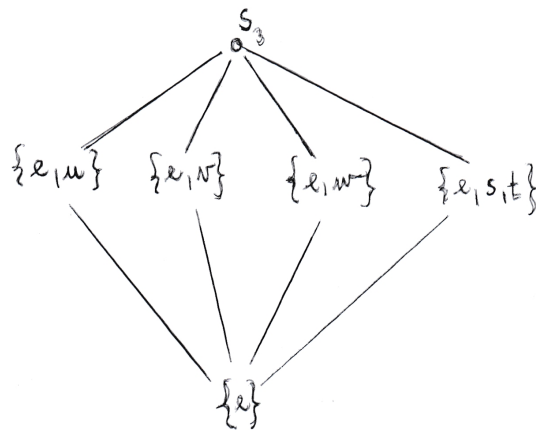
Př. 5 A abychom zavzpomínali na témata 1 až 7, tak i množina všech podgrup dané grupy, s uspořádáním množinovým \subseteq tvoří svaz. Průsek na této struktuře lze definovat jako množinový průnik, spojení opět nefunguje jako sjednocení, ale musíme je definovat

$$G_1 \sqcup G_2 := \langle G_1 \cup G_2 \rangle, \text{ což je}$$

podgrupa generovaná sjednocením množin G_1, G_2 , tj. „nejbližší větší“ podgrupa, která obě množiny obsahuje.

Například vezmeme-li naši starou známou grupu permutací (S_3, \circ) , svaz jejích podgrup lze znázornit v Hasseově diagramu:

³⁴Tedy operaci spojení dvou prvků musíme definovat jako průnik těch množin, které oba prvky obsahují. Intuitivně řečeno je to „nejbližší větší prvek“ v dané struktuře.



Každé dvě z podrup na prostřední vrstvě vygenerují vzájemným skládáním prvků už všech šest prvků, tedy celou grupu S_3 , tj. např.

$$\{e, v\} \sqcup \{e, w\} = \langle \{e, v\} \cup \{e, w\} \rangle = S_3,$$

jak jsme viděli v kapitole 2. *

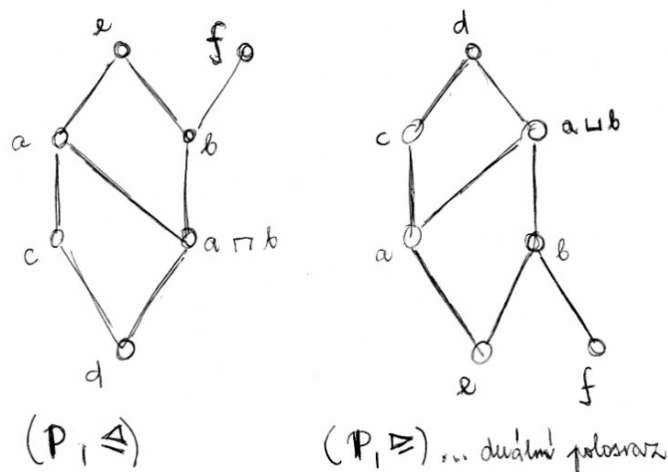
Dříve než přistoupíme ke studiu dalších vlastností svazu, všimneme si ještě jedné věci, která platí i v každém polosvazu – každý polosvaz definuje tzv. duální polosvaz, jehož Hasseovský diagram je obrácen vzhůru nohama o 180 stupňů:



Definice 10.5. Pokud například (P, \sqsubseteq) je průsekový polosvaz, tak duální uspořádání \sqsupseteq definujeme jako relaci, ve které obrátíme směr všech šipek. Struktura (P, \sqsupseteq) se pak nazývá duální polosvaz a jedná se o spojový polosvaz.



Příklad 10.6.



Na obrázku vidíme \sqcap -polosvaz (P, \sqsubseteq) a vedle něj nakreslený \sqcup -polosvaz (P, \sqsupseteq) zadaný toutéž množinou, pouze všechny šípky mají opačný směr, tj. Hasseovský diagram je oproti původnímu polosvazu „hlavou dolů“.

Z příkladu je vidět i duální vztah mezi příslušnými pojmy v daném duálním polosvazu:

- K dolní závoře v \sqcap -polosvazu je jednoznačně přiřazena horní závora v duálním \sqcup -polosvazu.
- K infimu $a \sqcap b$ v \sqcap -polosvazu je jednoznačně přiřazena supremum $a \sqcup b$ v duálním \sqcup -polosvazu;

Tedy ve vztahu duality nejsou jen relace \leq a \geq , ale i operace \sqcap a \sqcup . Například vztahy (16a), (16b) jsou duálními ke vztahům (17a),(17b). Pokud jsme podrobně dokázali asociativitu (2) pro operaci \sqcap , tak analogický vztah asociativity pro operaci \sqcup bychom dokázali přesně stejným postupem, pouze

- znak \sqcap bychom zaměnili za znak \sqcup ;
- znak \leq bychom zaměnili za znak \geq ;
- vlastnost (16a), pojem dolní závory, bychom zaměnili za vlastnost (17a), pojem horní závory;
- vlastnost (16b), pojem infima, bychom zaměnili za vlastnost (17b), pojem suprema.

Ve svazech, kde jsou definovány obě operace současně, tj. existují současně infima i suprema dvouprvkových podmnožin, lze někdy využívat těchto duálních vztahů mezi pojmy a z platnosti určité vlastnosti jednoduše dokázat příslušnou duální vlastnost pouze záměnou \sqcup za \sqcap , \geq za \leq , horních závor za dolní závory, suprem za infima. To je pro matematiky velmi pomocný poznatek, protože jim usnadňuje práci s dokazováním vlastností ve svazech na polovinu.

Pojmy, označení a důkazy, které studenti musí znát z této kapitoly: 1) průsek a spojení, 2) průsekový polosvaz, spojový polosvaz, 3) dk. asociativity (2) pro průsek, 4) příklad polosvazu, kde platí vlastnost (3) pro spojení (průsek), 5) příklad polosvazu, kde neplatí vlastnost (4) pro spojení (průsek), 6) definice a význam idempotence, 7) definice a příklady svazu, 8) duální uspořádání a duální polosvaz, 9) vytvoření duálního vztahu (17a) ze vztahu (16a), 10) vytvoření duálního vztahu (16b) ze vztahu (17b).

11 Další vlastnosti svazů

Z předchozí kapitoly víme, že ve svazu platí pro operace \sqcap, \sqcup vlastnosti (1), (2), (5), (16a), (16b), (17a), (17b), (18), protože to jsou vlastnosti, které si tyto operace přinesly z příslušných polosvazů (tj. platí i v každém polosvazu).

V této kapitole se podíváme ještě na několik vlastností, které platí v každém polosvazu, nebo které platí speciálně pouze ve svazech. Pak můžeme spokojeně uzavřít tento semestr s pocitem, že o vlastnostech svazů víme řadu věcí.

Následující vlastnost snad ještě patří do předešlé kapitoly, protože formálně dokazuje základní fakt, který jsme už vyzorovali při hledání výsledků operace průseku a spojení pro srovnatelné prvky.



Věta 11.1. (Kopka, str. 66) V každém svazu $(S, \leq, \sqcap, \sqcup)$ platí:

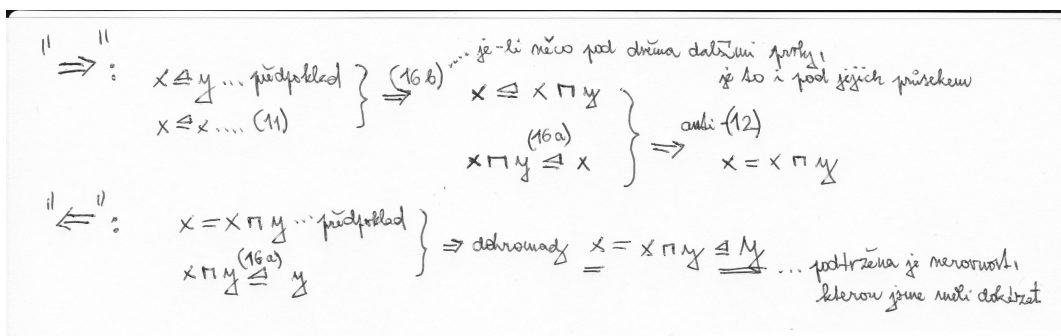
a)

$$x \leq y \Leftrightarrow x \sqcap y = x \quad (\text{platí i v } \sqcap\text{-polosvazu});$$

b)

$$x \leq y \Leftrightarrow x \sqcup y = y \quad (\text{platí i v } \sqcup\text{-polosvazu}).$$

Důkaz: ad a) Viz sken:



Příklad 11.2. Dokažte část (b) předchozího tvrzení, když víte, že je duálním ke tvrzení (a).

Protože $(2^A, \subseteq, \cap, \cup)$ je svaz, budeme studovat vlastnosti této celkem přijatelné struktury v následujícím příkladu.



Příklad 11.3. Už víte, že struktura 2^A je pogruba vzhledem k operacím sjednocení a průniku (viz začátek kapitoly 2, první věta v té kapitole) – zkuste ještě operace průniku a sjednocení více prozkoumat a najděte nějakou jejich další vlastnost: buď vlastnost odděleně jedné z těchto operací, nebo vlastnost vzájemné interakce obou z nich.

Projděme tedy ještě jednou jednotlivé vlastnosti průniku a sjednocení, a přidáme si i vlastnosti, které jsme ještě neměli:

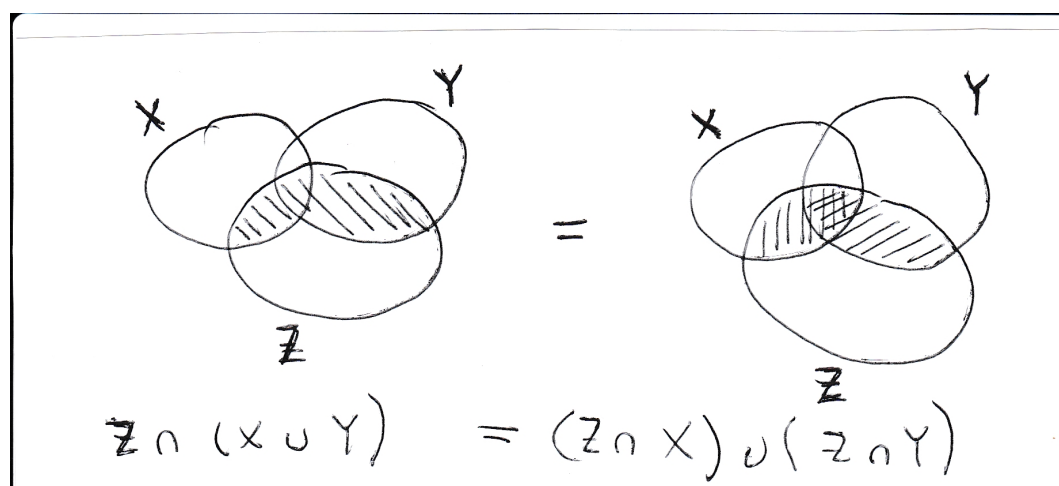
Množiny (1),(2),(3) Tyto vlastnosti platí.

Množiny (4) Neplatí, inverzní prvky vzhledem k operacím \cup, \cap většinou neexistují.

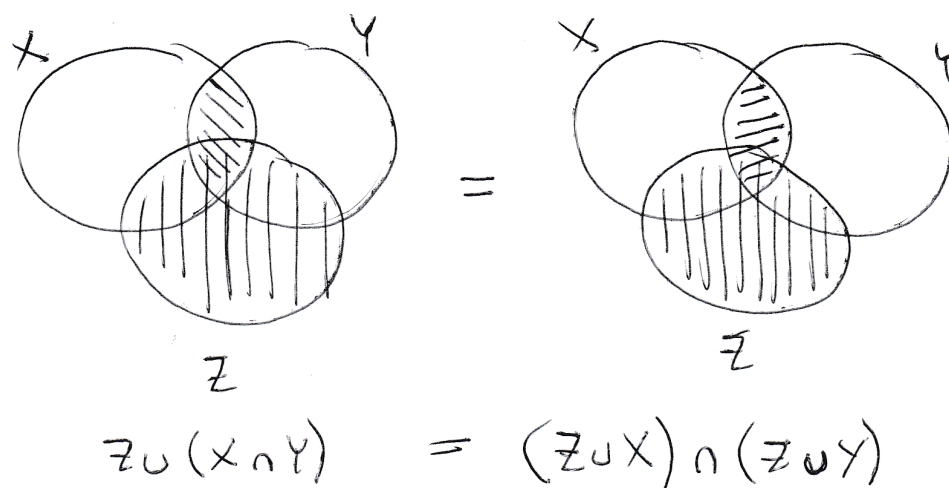
Množiny (5) Platí ... sjednocení a průnik nezáleží na pořadí vstupujících množin.

Množiny (6) Platí oboustranně tj. operace \cap , \cup lze v distributivním zákonu zaměnit: pro podmnožiny X, Y, Z množiny A :

$$Z \cap (X \cup Y) = (Z \cap X) \cup (Z \cap Y) \quad (6a),$$



$$Z \cup (X \cap Y) = (Z \cup X) \cap (Z \cup Y) \quad (6b).$$



Důkaz těchto rovností jsme provedli jen schematicky pomocí tzv. Vennových diagramů, ve kterých šrafuje danou množinu na levé straně rovnosti, pak na pravé straně rovnosti a výsledek porovnáme – viz obrázky pod jednotlivými tvrzeními.

No to je teda bomba, to je ultravlastnost!! Operace průniku a sjednocení jsou navzájem distributivní v obou směrech!! Ta množina všech podmnožin je skutečně zvláštní struktura!!

Množiny (anti-7) (rozšíření rovnosti) Pro každé dvě podmnožiny platí

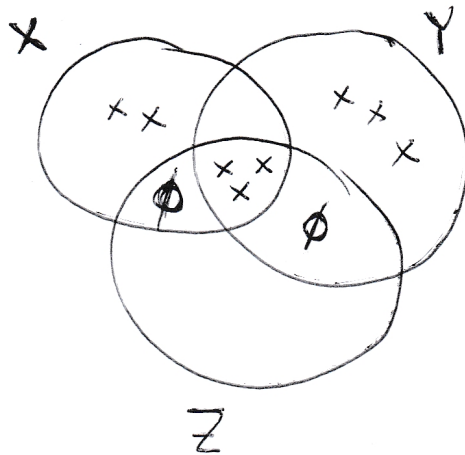
$$X = Y \Rightarrow X \cap Z = Y \cap Z, \quad X \cup Z = Y \cup Z.$$

Toto platí vždy pro podmnožiny dané množiny, podobně jako (anti-7) platí v každém grupoidu ... stačí, aby struktura byla uzavřená na danou operaci a výsledek operace existoval (vlastnost (1)).

Množiny (7) (krácení v rovnosti průniku) Platí následující vztah?

$$X \cap Z = Y \cap Z \Rightarrow X = Y.$$

(7a) Jak ukazuje následující sken, i kdyby některé části diagramu byly bez prvků (vyznačeno ve skenu) a platilo $X \cap Z = Y \cap Z$, tak obecně, pokud množiny X, Y obsahují další prvky mimo svůj společný průnik, neplatí žádaná rovnost $X = Y$, ani neplatí dílčí nerovnosti $X \subseteq Y, X \supseteq Y$:



$$X \cap Z = Y \cap Z,$$

ale

$$X \neq Y$$

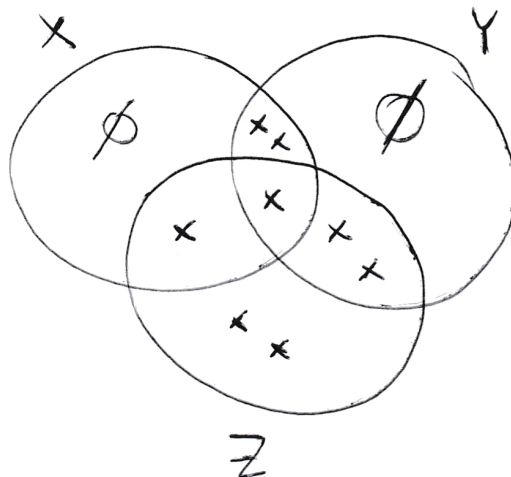
$$X \not\subseteq Y$$

$$X \not\supseteq Y$$

(7b) Analogicky existují takové množiny, že

$$X \cup Z = Y \cup Z \not\Rightarrow X = Y;$$

Viz sken:



$$X \cup Z = Y \cup Z,$$

ale

$$X \neq Y$$

$$X \not\subseteq Y$$

$$X \not\supseteq Y$$

Množiny (18) Idempotence³⁵ $X \cap X = X$, $X \cup X = X$ platí téměř zřejmě, tím jsme se už zabývali v předchozí kapitole, str. 45.

Množiny (19) (absorbce) Jednoduše pomocí množinových Vennových diagramů pro obě strany rovnosti lze ověřit, že platí pro každé dvě podmnožiny dané množiny

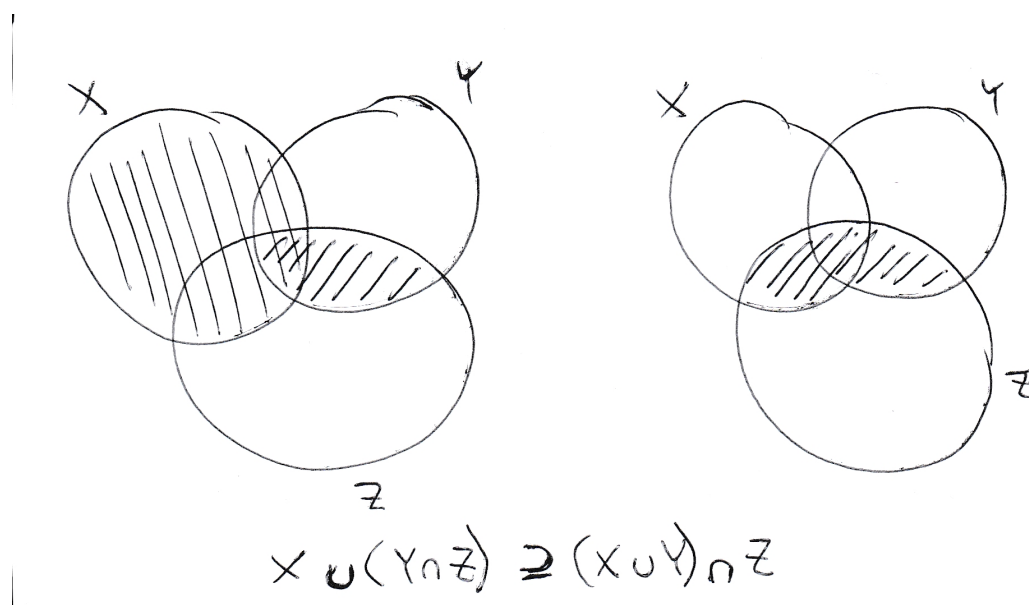
$$(X \cap Y) \cup Y = Y, \quad (X \cup Y) \cap Y = Y. \quad (19)$$

První rovnost vyjadřuje, že průnik dvou množin je pohlcen (= absorbován) sjednocením s libovolnou z nich (tedy platí též $(X \cap Y) \cup X = X$), druhá rovnost praví, že sjednocení dvou množin je pohlceno (absorbováno) průnikem s libovolnou z nich (tj. přeznačením X za Y lze psát také $(X \cup Y) \cap X = X$).

Množiny (20) (modularita) Zabývejme se chvíli otázkou, zda platí pro každé dvě podmnožiny dané množiny vztah

$$X \cup (Y \cap Z) = (X \cup Y) \cap Z. \quad (20)$$

Tato rovnost připomíná asociativitu (2), ale nyní jsou v ní zahrnuty dvě operace. A kdyby platila, byla by to tedy supervlastnost, protože interakce dvou operací by nezáležela na uzávorkování, to by byl teda gól. Z Vennových diagramů vidíme, že vlastnost neplatí:



Ovšem je vidět, že platí inkluze

$$\forall X, Y, Z: \quad X \cup (Y \cap Z) \supseteq (X \cup Y) \cap Z.$$

Tuto inkluzi (česky: vlastnost „být podmnožinou“) bychom mohli nazvat jako polomodularitu³⁶ nebo cizím slovem semimodularitu, přičemž rovnost nastane jen tehdy, když $X - Z = \emptyset$.

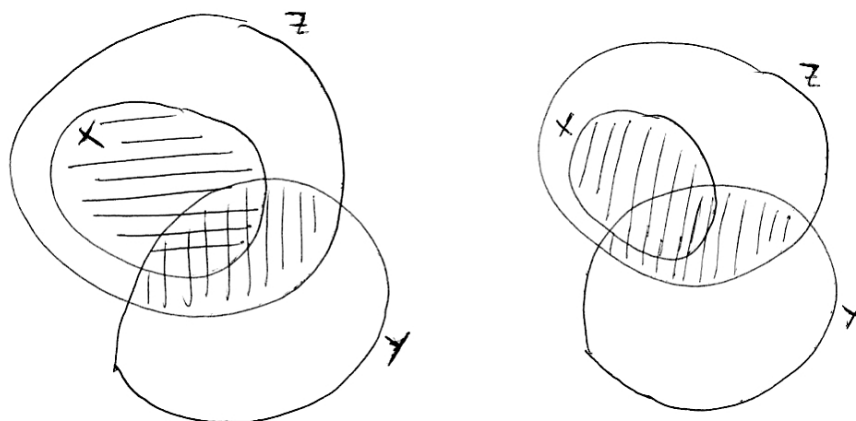
³⁵Příští rok, pokud budu přednášet, tato vlastnost bude mít číslo 8, vlastnost (19) číslo 9 a vlastnost (20) číslo 10 – v letnošním školním roce už to asi není rozumné přečíslovat. Tak budou vlastnosti (1) až (10) představovat různé možné vlastnosti operací. Při letošním označení (1) až (7), (18), (19), (20), I am sorry.

³⁶Pomůcka k zapamatování této přirozené polomodularity: vnější sjednocení (= sjednocení před závorkou) je nadmnožinou, podobně jako spojení dvou prvků je větší nebo rovno jednotlivým prvkům.

Množiny modif-(20) (modifikovaná modularita) Z jistých důvodů se při studiu množin a svazů používá vlastnost tzv. modifikované modularity – do předpokladů modularity přidáváme podmínku $X \subseteq Z$. Je to pravděpodobně proto, že situace srovnatelných prvků X, Z je většinou ta, která nás zajímá. U mnoha vlastností je jedno, zda množiny X, Y, Z mají nějaké další prvky mimo své vzájemné průniky, ale zde u vlastnosti (20) je snad zajímavější sledovat situaci za podmínky $X \subseteq Z$. Tak tedy:

$$\bullet \forall X, Y, Z: X \subseteq Z \Rightarrow X \cup (Y \cap Z) = (X \cup Y) \cap Z. \quad (\text{modif-10})$$

A u množin platí modifikovaná modularita jako rovnost! Lze snadno odtušit kreslením Vennových diagramů:



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

Přechod: Svaz $(2^A, \subseteq, \cap, \cup)$ je tedy velmi zajímavá struktura, protože splňuje vlastnosti (1),(2),(3), (5),(6), (18),(19),(20) (není splněno pouze (4) a (7) ze všech deseti vlastností operací, kterými jsme se v tomto semestru zabývali). Nesplňuje ovšem tato superstruktura něco navíc než každý svaz s operací průseku a spojení? Které z těchto vlastností platí v každém svazu $(S, \leq, \sqcap, \sqcup)$ ³⁷?

Svazy (6) Platí v každém svazu distributivita? To by pro interakci průseku a spojení muselo platit

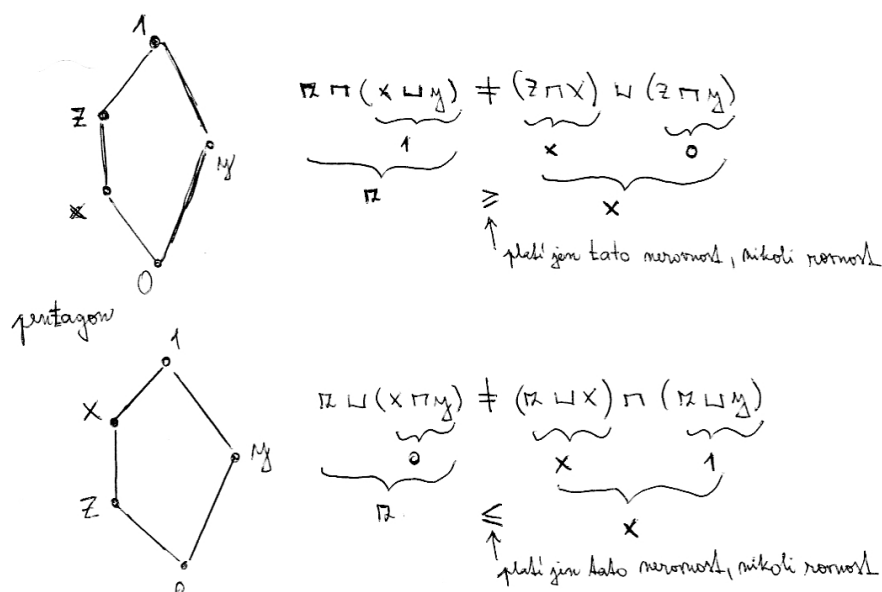
$$z \sqcap (x \sqcup y) = (z \sqcap x) \sqcup (z \sqcap y), \quad z \sqcup (x \sqcap y) = (z \sqcup x) \sqcap (z \sqcup y).$$

Obecně zde neplatí rovnost, jak ukazuje následující příklad svazu, který se nazývá **pentagon**:

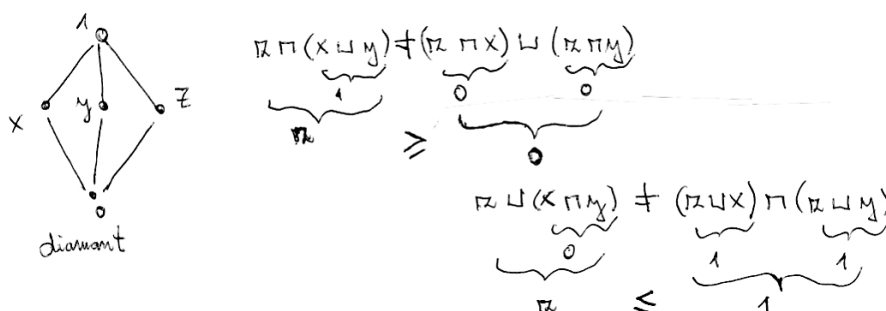


Příklad 11.4. V pentagonu (viz následující sken) obecně neplatí žádná z distributivních rovností, platí jen jednostranné nerovnosti:

³⁷Vlastnosti (1) až (5) byly u svazů vlastně prověřeny v předchozí kapitole v rámci studia polosvazů – totéž lze říci i ve svazech, tj. svazy (respektive operace průseku a spojení v nich) nesplňují (3),(4).



Příklad 11.5. V diamantu (viz následující sken) obecně neplatí žádná z distributivních rovností, platí jen jednostranné nerovnosti:



Zdá se ovšem, že jednostranné nerovnosti platí, tedy vzhledem k (6) jsou svazy polodistributivní = semidistributivní!



Věta 11.6. V každém svazu $(S, \leq, \sqcap, \sqcup)$ platí $\forall x, y, z \in S$:

- $z \sqcap (x \sqcup y) \supseteq (z \sqcap x) \sqcup (z \sqcap y)$, (6a)
- $z \sqcup (x \sqcap y) \supseteq (z \sqcup x) \sqcap (z \sqcup y)$. (6b)

Pomůcka k zapamatování (6a),(6b): překvapivě platí ty nepřírozené části, ty, které bychom neodvodili z operace průseku či spojení z definice. (6a) ... vnější průsek je nad spojením závorek, (6b) ... vnější spojení je pod průsekem závorek. Tj platí jen jednostranné nerovnosti, ale „zrovna ty silné, ty, které bychom nehádali či nečekali, že budou platit“.

Důkaz: Dokažme (6a), pak duální vztah (6b) je ke cvičení pro studenty:

$$\begin{array}{l}
 x \sqcap z \leq z \quad (16a) \\
 x \sqcap z \leq x \leq x \sqcup y \quad (16a, 17a)
 \end{array}
 \left. \vphantom{\begin{array}{l} x \sqcap z \leq z \\ x \sqcap z \leq x \leq x \sqcup y \end{array}} \right\} \Rightarrow (16b) \dots \text{kdyp\u017e\u016f je m\u011bvo pod druhou pr\u016fky, je to i pod jejich pr\u016fsekem} \\
 x \sqcap z \leq z \sqcap (x \sqcup y)$$

$$\begin{array}{l}
 y \sqcap z \leq z \quad (16a) \\
 y \sqcap z \leq y \leq x \sqcup y \quad (16a, 17a)
 \end{array}
 \left. \vphantom{\begin{array}{l} y \sqcap z \leq z \\ y \sqcap z \leq y \leq x \sqcup y \end{array}} \right\} \Rightarrow (16b) \quad y \sqcap z \leq z \sqcap (x \sqcup y)$$

$$z \sqcap (x \sqcup y) \geq (x \sqcap z) \sqcup (y \sqcap z) \quad (17b) \dots \text{kdyp\u017e\u016f je m\u011bvo nad druhou pr\u016fky, je to i nad jejich spojen\u00edm}$$



P\u0159\u00edklad 11.7. Doka\u017ete vztah (6b) pro svazy.

Svazy =-anti-(7) (roz\u0161\u00edren\u00ed rovnosti) Z rovnosti $x = y$ plyne v ka\u017ed\u00e9m svazu, \u017ee

$$x \sqcap z = y \sqcap z, \quad x \sqcup z = y \sqcup z.$$

Svazy \(\leq\)-anti-(7) (roz\u0161\u00edren\u00ed nerovnosti) Plat\u00ed t\u011b\u017e, tj. pro $x \leq y$ plat\u00ed v ka\u017ed\u00e9m svazu, \u017ee

- a) $x \sqcap z \leq y \sqcap z$;
- b) $x \sqcup z \leq y \sqcup z$.

Tyto vztahy je ov\u0161em pot\u0159eba dok\u00e1zat, protože nevíme p\u0159esn\u011b, co v\u0161e lze od obecn\u00e9ho uspo\u0159\u00e1d\u00e1n\u00ed \u010dekat:

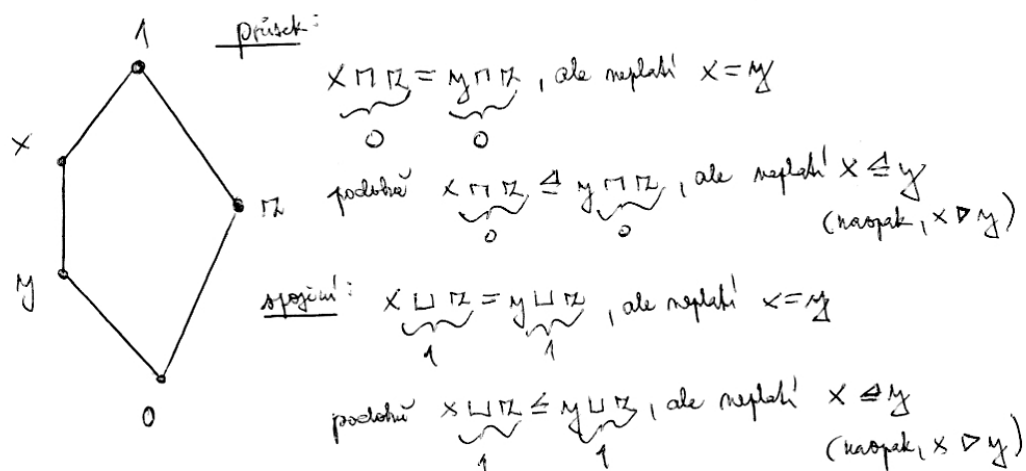
$$\begin{array}{l}
 a) \quad \begin{array}{l} x \sqcap z \leq x \leq y \quad (16a) \\ x \sqcap z \leq z \quad (16a) \end{array} \left. \vphantom{\begin{array}{l} x \sqcap z \leq x \leq y \\ x \sqcap z \leq z \end{array}} \right\} \Rightarrow (16b) \quad x \sqcap z \leq y \sqcap z
 \end{array}$$

je-li m\u011bvo pod druhou pr\u016fky, je to i pod jejich pr\u016fsekem

$$\begin{array}{l}
 b) \quad \begin{array}{l} x \leq y \leq y \sqcup z \quad (17a) \\ z \leq y \sqcup z \quad (17a) \end{array} \left. \vphantom{\begin{array}{l} x \leq y \leq y \sqcup z \\ z \leq y \sqcup z \end{array}} \right\} \Rightarrow (17b) \quad x \sqcup z \leq y \sqcup z
 \end{array}$$

je-li m\u011bvo nad druhou pr\u016fky, je to i nad jejich spojen\u00edm

Svazy (7) Kr\u00e1cen\u00ed platilo jen v grup\u011b\u011b, a neplat\u00ed v mno\u017ein\u00e1ch – d\u00e1 se tedy \u010dekat, \u017ee nebude platit ani ve svazech, kter\u00e9 jsou pologrupy vhladem ke operaci pr\u016fseku a spojen\u00ed. A opravdu, n\u00e1sleduj\u00edc\u00ed p\u0159\u00edklad ukazuje, \u017ee kr\u00e1cen\u00ed neplat\u00ed ani pro rovnost, ani pro nerovnost, ani pro pr\u016fsek, ani pro spojen\u00ed. Vyu\u017eijem p\u0159itom svaz zvan\u00fd pentagon je\u0161t\u011b jednou:



Svazy (18) (idempotence) Už bylo probráno v předchozí kapitole, idempotence operací průsek a spojení platí v každém příslušném polosvazu, tedy i ve svazech.

Svazy (19) (absorbční zákony pro svazy)

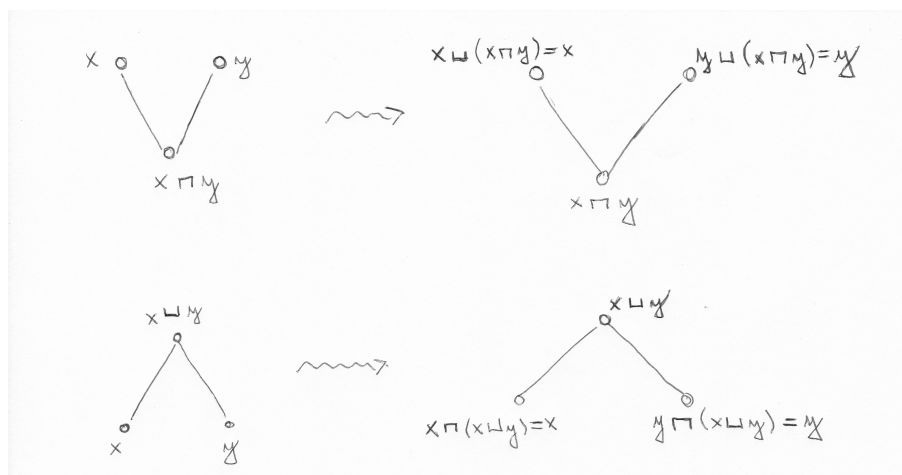


Věta 11.8. Pro svaz (S, \leq, \cap, \cup) platí tzv. absorbční zákony (19)

$$\forall x, y \in S: 19a) (x \cap y) \cup y = y, 19b) (x \cup y) \cap x = x.$$

Absorbce = pohlcení. Vlastnost a): průsek dvou prvků je pohlcen (= absorbován) spojením s kterýmkoli z nich;

Vlastnost b): spojení dvou prvků je pohlceno (= absorbováno) průsekem s kterýmkoli z nich.



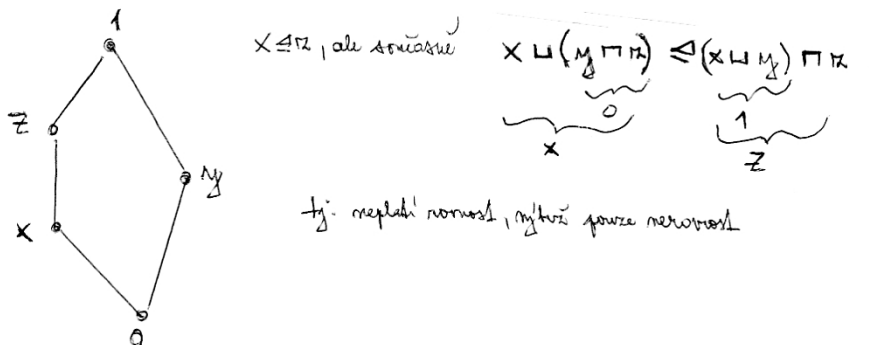
Důkaz: Dokážeme jen tvrzení a), a pak totiž tvrzení b) plyne z tvrzení a), protože je k němu duální:

$$\left. \begin{array}{l} y \stackrel{17a)}{\leq} (x \cap y) \cup y \\ y \stackrel{(11)}{\leq} y \\ x \cap y \stackrel{16a)}{\leq} y \end{array} \right\} \stackrel{17b)}{\Rightarrow} (x \cap y) \cup y \leq y \quad \left. \vphantom{\begin{array}{l} y \\ y \\ x \cap y \end{array}} \right\} \stackrel{(\text{anti-12})}{\Rightarrow} y = (x \cap y) \cup y$$



Příklad 11.9. (ve dvojici či trojici) Dokažte vztah (b) z předchozí věty podrobněji!!

Svazy modif-(20) U množin platila v modif-(20) rovnost, nyní platí u svazů pouze nerovnost, jak je vidět opět z příkladu pentagonu:



Pomůcka k zapamatování modifikované semimodularity: vnější průsek je nepřirozeně nad (= větší nebo roven), vnější spojení je nepřirozeně pod (= menší nebo rovno). Vztah je tzv. autoduální, tj. duální k sobě samému, neexistuje žádný jiný vztah modifikované semimodularity.



Věta 11.10. V každém svazu platí vlastnost modif-semi-(20), tj.

$$\forall x, y, z : x \leq z \Rightarrow x \sqcup (y \sqcap z) \leq (x \sqcup y) \sqcap z.$$

Důkaz: Vztah je nyní jediný, jeho důkaz je opět v kategorii standardních důkazů, které využívají definice průseku jako infima (16a),(16b) a spojení jako suprema (17a),(17b) dvouprvkových množin:

$$\left. \begin{array}{l} x \leq z \\ x \leq x \sqcup y \end{array} \right\} \xRightarrow{(16b)} x \leq (x \sqcup y) \sqcap z$$

$$\left. \begin{array}{l} y \sqcap z \leq y \\ y \sqcap z \leq z \end{array} \right\} \xRightarrow{(16a)} y \sqcap z \leq (x \sqcup y) \sqcap z$$

$$\left. \begin{array}{l} x \leq (x \sqcup y) \sqcap z \\ y \sqcap z \leq (x \sqcup y) \sqcap z \end{array} \right\} \xRightarrow{(17a)} x \sqcup (y \sqcap z) \leq (x \sqcup y) \sqcap z$$

Zdá se tedy, že struktura $(2^A, \subseteq, \cap, \cup)$ vykazuje ještě lepší vlastnosti než obecný svaz $(S, \leq, \sqcap, \sqcup)$. Proto, abychom ve svazech zajistili přesně to, co se odehrává v množinách, tj. například vlastnosti modif-(20) a (6) a nikoli jen polovlastnosti, musíme ještě k definici svazu přidat další podmínky. Které? Směřujeme ke struktuře, které se říká Booleova algebra, kde 2^A je příkladem Booleovy algebry. Ale na to už nebudeme mít nyní čas – možná až v algebře 3.

Poslední poznámka na závěr studia svazů: lze definovat pojem podsvazu jako podmnožinu svazu, která je uzavřená vzhledem k operacím průseku a spojení. To je ovšem pojem přirozený a lze jej očekávat.

V každém svazu existuje průsek (či spojení) dvou prvků, a tedy existuje též průsek (spojení) k prvků $x_1 \sqcap x_2 \sqcap \dots \sqcap x_k$. Dalším směrem matematického zkoumání je rozšíření operace spojení a průseku na nekonečně mnoho prvků³⁸:

³⁸Kopka, str.72-73.



Definice 11.11. Pokud v daném posetu S existují infima a suprema všech jeho nekonečných podmnožin M , označujeme operace zobecněný průsek

$$\sqcap_z M := \inf M \text{ i pro } M \text{ nekonečnou,} \quad (21)$$

zobecněné spojení

$$\sqcup_z M := \sup M \text{ i pro } M \text{ nekonečnou.} \quad (22)$$

Struktura $(S, \subseteq, \sqcap_z, \sqcup_z)$ se nazývá úplný svaz³⁹.



Příklad 11.12. Množina přirozených čísel s klasickým uspořádáním \leq je svaz, ale není to úplný svaz, protože neexistuje supremum celé nekonečné množiny N . Podobně množina Z je svaz, ale není úplný svaz, protože v ní neexistuje např. supremum podmnožiny všech kladných celých čísel, nebo infimum podmnožiny všech záporných celých čísel.

Na studium úplných svazů zde nyní už není prostor (více viz Kopka, str.72-82). Poznamenejme zde jen, že pojem má smysl u nekonečných množin, protože **každý konečný svaz je současně i úplný svaz**. Proto by více detailů mohlo následovat v předmětu Algebra 3 nebo v magisterském předmětu Teorie množin, který se zevrubněji zabývá množinami nekonečnými. Každopádně pojem úplného svazu směřuje k zajímavému hlavnímu výsledku, že **každý poset lze izomorfně vnořit do úplného svazu (Mac Neillova věta)**, jehož vedlejším produktem je popis konstrukce množiny reálných čísel jako úplného svazu, do kterého lze izomorfně vnořit svaz Q racionálních čísel⁴⁰.

Z této kapitoly by studenti měli znát: 1) Definicí úplného svazu a příklad svazu, který není úplný; 2) dk. věty 11.1; 3) vyslovit a dokázat (pomocí Venových diagramů) některé z vlastností průniku a sjednocení množin, zejména vlastnosti (6), (19) a modif-(20); 4) vyslovit a dokázat některé vlastnosti svazů, zejména semi-(6), (19) a semi-modif-(20).

³⁹Pozor, slovo „úplný“ nyní není vzato z terminologie úplné relace – v úplném svazu nadále mohou existovat nesrovnatelné prvky. Spíše se zde mívá úplnost vzhledem k supremům a infimům – úplný svaz obsahuje i infima a suprema svých nekonečných podmnožin, což v obyčejném svazu platit nemuselo.

⁴⁰Množina Q totiž neobsahuje suprema a infima některých svých nekonečných podmnožin – když množinu Q o tato infima a suprema doplníme, dostaneme množinu R .

12 Výsledky některých příkladů

12.1 Výsledky ke kapitole 8 – relace, uspořádané množiny

Viz příklad 2: reflexivní relace je reprezentována smyčkami u všech prvků (jedničkami na celé hlavní diagonále), antireflexivní relace nepřítomností smyček (nepřítomností jedniček na hlavní diagonále), symetrická relace má pro každou šipku též šipku v opačném směru, antisymetrická relace nemůže mít oboustranné šípky mezi dvěma různými prvky, tranzitivní relace musí pro např. šipku od a do b a od b do c obsahovat i šipku od a do c .

Viz příklad 4: Studentům by mělo být jasné, že např. antireflexivní relace není negací relace reflexivní, ale úplným protipólem reflexivní relace – tj. že existují relace s nějakou smyčkou, které nejsou ani reflexivní, ani antireflexivní. Podobně u tranzitivní relace nemusí být všechny možné tranzitivní spoje prvky relace, ale jen ty, které jsou vynuceny šípkami v posloupnosti tří prvků (tj. xRy a yRz vynucují šipku xRz).

Viz příklad 5: R je reflexivní a tranzitivní, tedy kvaziuspořádání. Je důležité si všimnout, že relace R není antisymetrická, protože například $3|(-3)$ a $(-3)|3$, ale odtud neplatí $3 = -3$. Není ani symetrická, protože pokud $3|6$, neplatí odtud, že $6|3$.

Viz příklad 7: ad a) může ale jen podmnožina reflexivní relace, bez šipek mezi různými prvky;

ad b) jediná relace je současně ekvivalence i uspořádání, a sice samotná reflexivní relace $xRx \quad \forall x \in M$. To není zajímavý příklad ani ekvivalence (každý prvek je v relaci jen se sebou samým), ani uspořádání (všechny prvky jsou navzájem mezi sebou nesrovnatelné – k jejich „vzájemnému uspořádání“ vlastně nedošlo).

Viz příklad 8: ad a) R je reflexivní, antisymetrická a tranzitivní, tedy uspořádání.

ad b) R je reflexivní, symetrická a tranzitivní, tedy ekvivalence.

ad c) R je reflexivní, antisymetrická a tranzitivní, tedy uspořádání.

ad d) R je pouze reflexivní, jinak nic rozumného nelze říci.

Viz příklad 11: ad i) a) v jedné třídě rozkladu leží zlomky, které lze zkrátit na stejný základní tvar;

b) množina M/\equiv je množina všech racionálních čísel (všechny zlomky upravitelné na tentýž základní tvar jsme ztotožnili v jedno racionální číslo).

ii) Relace je reflexivní, antisymetrická a tranzitivní, takže je to uspořádání!!

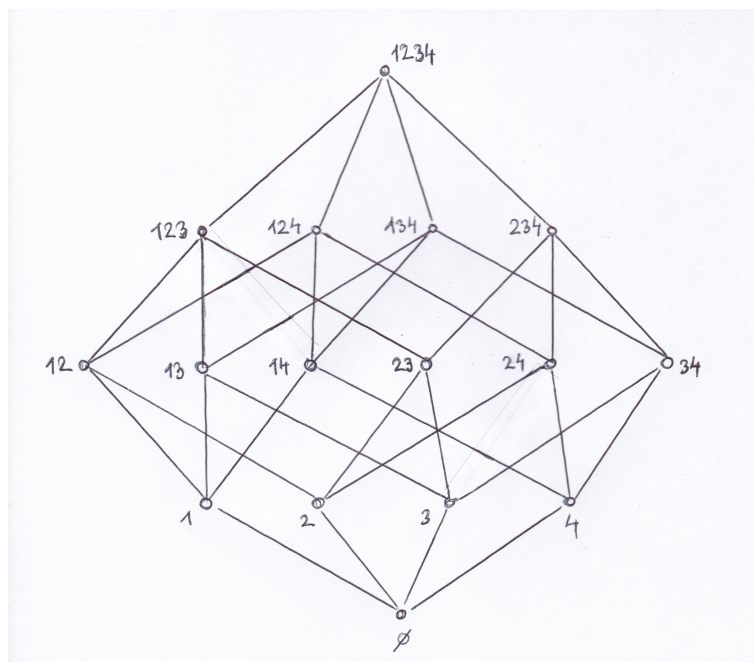
Viz příklad 13: Ne, protože není antisymetrická. Ale (Z/E) už je poset, pokud relace E ztotožňuje $3, -3$ do jednoho prvku $[3]$, dále $4, -4$ do jednoho prvku $[4]$, atd. a uprostřed nulu nechává nulou a označuje ji jako $[0]$. Tím pádem jsme dostali strukturu N_0 , kde relace dělitelnosti je už antisymetrická (pro žádné různé prvky $(x \neq y)$ neplatí $x|y \wedge y|x$).

Viz příklad 15: ad a) $[1, 1], [2, 2], [3, 3], [4, 4], [1, 2], [2, 3], [1, 3], [1, 4], [4, 3], [1, 3]$.

ad b) $[1, 1], [2, 2], [3, 3], [4, 4], [3, 4], [4, 1], [3, 1], [4, 2], [3, 2]$.

12.2 Výsledky ke kapitole 9 – význačné prvky v uspořádaných množinách

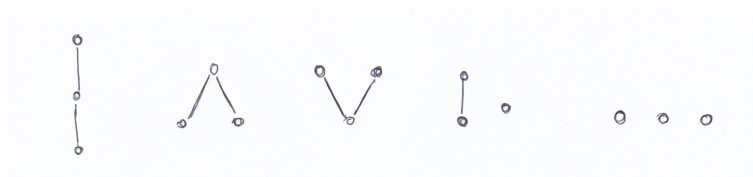
Viz příklad 7: Jedná se o poset zobrazený na titulní straně textu Kopka: obrázek 20.



Obrázek 20: 2^P pro $P = \{1, 2, 3, 4\}$.

Viz příklad 10: ad a) $\sup\{a, d\} = c$, $\sup\{e, f\} = e$.
ad b) $\sup M$ neexistuje, protože množina horních závor $\{b, c, d\}$ nemá nejmenší prvek.

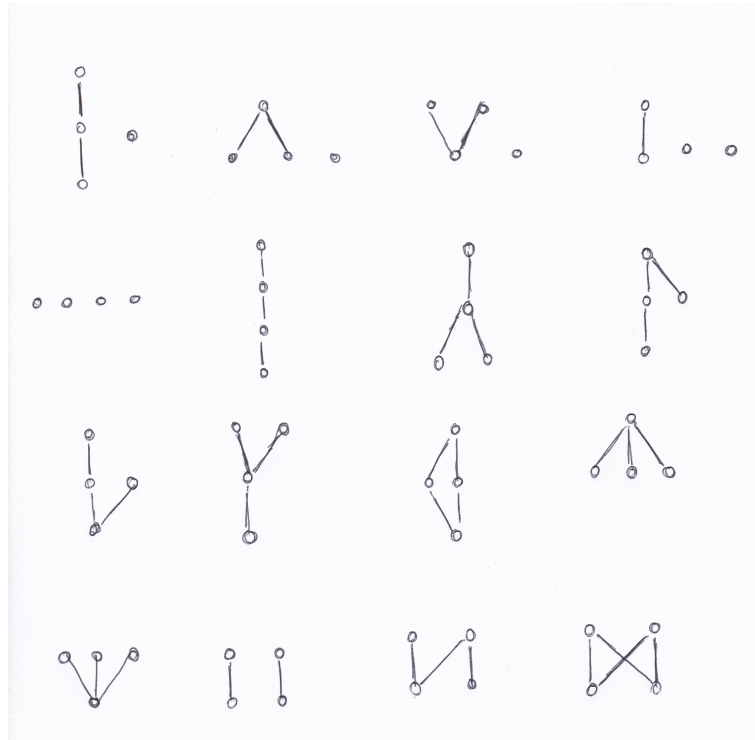
Viz příklad 16: Neizomorfních posetů na tříprvkové množině je pět – viz obrázek:



Viz příklad 17: Neizomorfních posetů na čtyřprvkové množině je šestnáct – viz obrázek 21.

12.3 Výsledky ke kapitole 10 – polosvazy, svazy

Viz příklad 2: ad i) $4 \sqcap 7 = 2$, $6 \sqcap 2 = 2$, $7 \sqcap 7 = 7$, $3 \sqcup 7 = 6$, $6 \sqcup 8 = 6$; jedná se o průsekový i spojový polosvaz;
ad ii) $6 \sqcap 3 = 7$, $6 \sqcup 3$ neexistuje. Jedná se o průsekový polosvaz, který není spojovým polosvazem.



Obrázek 21: Všechny navzájem neizomorfní čtyřprvkové posety.

ad iii) $5 \sqcup 7 = 10$, $2 \sqcap 3$ neexistuje, $2 \sqcap 7$ neexistuje. Jedná se o spojový polosvaz, který není průsekovým polosvazem.

ad iv) $4 \sqcap 5$ neexistuje, $2 \sqcap 3$ neexistuje. Tedy daný poset není ani průsekovým, ani spojovým polosvazem.

12.4 Výsledky ke kapitole 11 – další vlastnosti svazů

Viz příklad 2: Důkaz věty $x \leq y \Leftrightarrow x \sqcup y = y$:

$$\begin{array}{l}
 \Rightarrow \\
 \left. \begin{array}{l} x \leq y \dots \text{předpoklad} \\ y \leq y \dots (11) \end{array} \right\} \Rightarrow \begin{array}{l} (17b) \dots \text{je-li mezi dvěma prvky současně,} \\ \text{je to i mezi jejich spojinkou} \\ x \sqcup y \leq y \\ (17a) \quad y \leq x \sqcup y \end{array} \xrightarrow{\text{anti-(12)}} y = x \sqcup y
 \end{array}$$

$$\begin{array}{l}
 \Leftarrow \\
 x \sqcup y = y \dots \text{předpoklad } p \Rightarrow \underline{x \leq} \quad \underline{x \sqcup y} \stackrel{(p)}{=} \underline{y} \dots \text{potřebuje se ukázat,} \\
 \text{kteřou jinu má dokázat}
 \end{array}$$

Viz příklad 7: Důkaz distributivity (6b) s vnějším spojením:

$$\begin{array}{l}
 \left. \begin{array}{l}
 X \sqcup Z \supseteq Z \quad 17a \\
 X \sqcup Z \supseteq X \supseteq X \cap Y \quad 17a, 16a
 \end{array} \right\} \Rightarrow X \sqcup Z \supseteq Z \sqcup (X \cap Y) \quad 17b \\
 \\
 \left. \begin{array}{l}
 Y \sqcup Z \supseteq Z \quad 17a \\
 Y \sqcup Z \supseteq Y \supseteq X \cap Y \quad 17a, 16a
 \end{array} \right\} \Rightarrow Y \sqcup Z \supseteq Z \sqcup (X \cap Y) \quad 17b
 \end{array}$$

*jedná se navíc pod druhou podmínkou
 je to i pod jejími průseky*

$$\left. \begin{array}{l}
 \\
 \\
 \end{array} \right\} \Rightarrow Z \sqcup (X \cap Y) \subseteq (Z \sqcup X) \cap (Z \sqcup Y) \quad (16b)$$

Viz příklad 9: Důkaz absorpce spojení průsekem:

$$\left. \begin{array}{l}
 (X \sqcup Y) \cap Y \leq Y \quad 16a \\
 Y \leq Y \quad (M) \\
 Y \leq X \sqcup Y \quad 17a
 \end{array} \right\} \Rightarrow Y \leq (X \sqcup Y) \cap Y \quad 16b$$

$$\left. \begin{array}{l}
 \\
 \end{array} \right\} \Rightarrow Y = (X \sqcup Y) \cap Y \quad (\text{anti-12})$$