Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 2000/2001
Michal Marvan

8. Uspořádání a svazy

Uspořádání je další užitečná abstraktní struktura na množině. Modeluje takové vztahy mezi prvky jako větší (menší), obsažený (obsahující) apod. Přidáváním podmínek postupně dojdeme ke speciálním uspořádaným množinám – svazům a Booleovým algebrám –, které jsou zároveň algebrami se dvěma binárními operacemi a mají důležité aplikace, zejména v informatice.

1. Uspořádané množiny

Připomeňme, že *relace* na množině M je libovolná podmnožina kartézského součinu $M^2 = M \times M$. Je-li $\rho \subseteq M^2$ relace, pak vztah $(x, y) \in \rho$ zapisujeme $x\ \rho\ y$.

Definice. Buď dána množina M. Relace ρ na M se nazývá
1° *reflexivní*, platí-li $a\rho a$ pro všechna $a \in M$,
2° *antisymetrická*, platí-li implikace $a\rho b$, $b\rho a \Rightarrow a = b$,
3° *tranzitivní*, platí-li implikace $a\rho b$, $b\rho c \Rightarrow a\rho c$.
Relace, která je reflexivní, antisymetrická a tranzitivní zároveň, se nazývá *uspořádání*. Dvojice (M, ρ) se pak nazývá *uspořádaná množina*.

Příklady. 0) Na každé množině M je identická relace id_M uspořádáním (připomeňme, že $a\ \mathrm{id}_M\ b \Leftrightarrow a = b$).

1) $(\mathbf{R}, \le)$, $(\mathbf{Z}, \le)$, $(\mathbf{N}, \le)$ atd. jsou uspořádané množiny, je-li $\le$ obvyklé uspořádání čísel podle velikosti.

2) Buď M množina, buď $\mathbf{P}(M)$ množina všech podmnožin množiny M. Inkluze $\subseteq$ je uspořádání na $\mathbf{P}(M)$ a $(\mathbf{P}(M), \subseteq)$ je uspořádaná množina.

3) $(\mathbf{N}, |)$, kde $a|b$ (čteme *a dělí b*) právě tehdy, když existuje $m \in \mathbf{N}$ takové, že $am = b$. Relace „$|$“ se nazývá *relace dělitelnosti* a je uspořádáním.

Podejme důkaz antisymetrie. Jestliže $a|b$ a $b|a$, pak existují $m, n \in \mathbf{N}$ taková, že $am = b$ a $bn = a$. Odtud $a = amn$, ale $a \neq 0$, načež $1 = mn$. Rovnice $1 = mn$ však má v přirozených číslech jediné řešení: $m = 1$ a $n = 1$. Potom $b = a \cdot 1 = a$.

Upozorněme, že analogicky definovaná relace dělitelnosti na množině $\mathbf{Z}$ celých čísel není antisymetrická, protože $1|-1$ a $-1|1$, a přesto $1 \neq -1$ (to souvisí s tím, že rovnice $1 = mn$ má v celých číslech ještě další řešení $m = -1$ a $n = -1$).

Buď ρ uspořádání na množině M. Opačná relace ρ^{-1} (tj. relace definovaná předpisem „$a\rho^{-1}b$ právě když $b\rho a$“) je zase uspořádání. Nazývá se *duální uspořádání*. Často se obecné uspořádání označuje symbolem „$\le$“. Duální uspořádání $\le^{-1}$ se pak označuje symbolem „$\ge$“: $a \ge b$ právě tehdy, když $b \le a$. Podobně nakládáme se symboly „$\subseteq$“ atp.

Každá podmnožina $N \subseteq M$ uspořádané množiny $(M, \le)$ je opět uspořádaná množina. Relace $\le_N$, zadaná pro libovolná $x, y \in N$ předpisem $x \le_N y \Leftrightarrow x \le y$, je totiž uspořádání na N. Nazývá se *indukované uspořádání* a značí se rovněž $\le$.

Příklady. 1) Přirozené uspořádání $\leq$ na množině **N** je totožné s uspořádáním indukovaným z přirozeného uspořádání množiny **Z**. Totéž platí pro další dvojice z množin **N**, **Z**, **Q**, **R**.

2) Buď A množina, uvažujme o množině $A^2 = A \times A$. Množina všech podmnožin množiny A^2, čili $\mathbf{P}(A^2)$, je vlastně množina všech binárních relací na množině A. Inkluze $\subseteq$ pak představuje uspořádání na $\mathbf{P}(A^2)$. Přitom

$$\rho \subseteq \sigma$$

právě tehdy, když platí implikace $(x, y) \in \rho \Rightarrow (x, y) \in \sigma$, to jest, implikace

$$x\rho y \Rightarrow x\sigma y.$$

Definice. Řekneme, že prvky a, b uspořádané množiny M jsou *srovnatelné*, platí-li $a \leq b$ nebo $a \geq b$. Uspořádaná množina M se nazývá *řetězec*, jsou-li každé dva prvky $a, b \in M$ srovnatelné.

Příklad. $(\mathbf{R}, \leq)$, $(\mathbf{Z}, \leq)$, $(\mathbf{N}, \leq)$ atd. jsou řetězce.

Cvičení. Dokažte, že každá podmnožina řetězce je opět řetězec, vzhledem k indukovanému uspořádání.

Buď $\leq$ uspořádání na M. Zaveďme označení $a < b$, jestliže $a \leq b$ a zároveň $a \neq b$. Dále zaveďme označení $a \lessdot b$, jestliže $a < b$ a neexistuje $c \in M$ takové, že $a < c$, $c < b$. Je-li $a \lessdot b$, pak říkáme, že prvek b *pokrývá* prvek a.

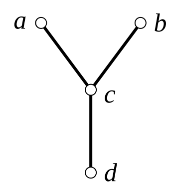
Příklady. 1) V množině **N** s přirozeným upořádáním podle velikosti platí $1 < 2$ a $1 \lessdot 2$. Dále platí $1 < 3$ ale nikoliv $1 \lessdot 3$.

2) V množině **Q** všech racionálních čísel s přirozeným uspořádáním neplatí $a \lessdot b$ pro žádnou dvojici $a < b$. Skutečně, prvek $c = \frac{1}{2}(a + b)$ pak splňuje $a < c$, $c < b$.

Konečnou uspořádanou množinu $(M, \leq)$ můžeme znázornit diagramem. Prvky množiny M znázorníme jako body v rovině, v níž je zadán horizontální směr. Prvky a, b, splňující $a \lessdot b$ vyznačíme tak, že a leží níže než b a spojíme je úsečkou.

Z diagramu pak můžeme určit uspořádání množiny M: $a \leq b$ právě tehdy, když a leží níže než b a existuje zdola nahoru směřující posloupnost na sebe navazujících úseček z bodu a do bodu b.

Příklad. V uspořádné množině Y s diagramem vpravo platí:
- $c \lessdot a$, $c \lessdot b$, $d \lessdot c$;
- $d < a$, ale nikoliv $d \lessdot a$;
- prvky a, b jsou nesrovnatelné.



Cvičení. Nakreslete diagram
1) čtyřprvkového řetězce;
2) uspořádané množiny duální k uspořádané množině Y z předchozího příkladu;
3) Uspořádáné množiny $(\mathbf{P}(M), \subseteq)$, je-li M jedno-, dvou-, tří- a čtyřprvková množina.

Definice. Buď $(M, \leq)$ uspořádaná množina. Prvek $x \in M$ se nazývá
- *nejmenší*, je-li $x \leq a$ pro všechna $a \in M$;
- *největší*, je-li $x \geq a$ pro všechna $a \in M$;
- *maximální*, neexistuje-li $a \in M$ takový, že $a > x$;
- *minimální*, neexistuje-li $a \in M$ takový, že $a < x$.

Příklad. V uspořádné množině Y z předchozího příkladu platí:
– d je nejmenší prvek a zároveň jediný prvek minimální;
– největší prvek neexistuje, zatímco a, b jsou dva prvky maximální;

Cvičení. Dokažte:
(1) V každé uspořádané množině existuje nejvýše jeden největší a nejvýše jeden nejmenší prvek.
(2) Existuje-li nejmenší prvek, pak je jediným minimálním prvkem. Existuje-li největší prvek, pak je jediným maximálním prvkem.

Definice. Buď $A \subseteq M$ podmnožina uspořádané množiny $(M, \leq)$. Prvek $x \in M$ se nazývá
– *dolní závora* množiny A, je-li $x \leq a$ pro všechna $a \in A$;
– *horní závora* množiny A, je-li $x \geq a$ pro všechna $a \in A$;
– *supremum* množiny A, je-li x nejmenší prvek množiny všech horních závor množiny A; píšeme $x = \sup A$;
– *infimum* množiny A, je-li x největší prvek množiny všech dolních závor množiny A; píšeme $x = \inf A$.

Příklad. V naší uspořádné množině Y platí:
– podmnožina $\{a, b\}$ má dolní závory c, d, z nich největší je c, a proto $\inf\{a, b\} = c$.
– podmnožina $\{a, b\}$ nemá žádnou horní závoru, a proto $\sup\{a, b\}$ neexistuje (množina horních závor je prázdná, a proto nemá největší prvek).

Cvičení. Dokažte:
(1) Každá podmnožina má nejvýše jedno supremum a nejvýše jedno infimum.
(2) Jestliže $x \leq y$, pak $\inf\{x, y\} = x$ a $\sup\{x, y\} = y$.
(3) Jestliže $\inf\{x, y\} = x$, pak $x \leq y$.
(4) Jestliže $\sup\{x, y\} = y$, pak $x \leq y$.

Uvažujme o matematickém pojmu, v jehož definici vystupuje nějaké uspořádání $\leq$. Nahradíme-li toto uspořádání duálním uspořádáním $\geq$, obdržíme definici *duálního pojmu*. Tak například, duálním pojmem k pojmu nejmenšího prvku je pojem největšího prvku.

Buď A libovolné tvrzení o uspořádáných množinách. Náhradou pojmů duálními pojmy vznikne *duální tvrzení* B. Jestliže obecně platí tvrzení A, pak obecně platí i duální tvrzení B. Důkaz tvrzení B obdržíme, nahradíme-li ve všech krocích důkazu tvrzení A všechny pojmy pojmy duálními.

2. Izotonní zobrazení

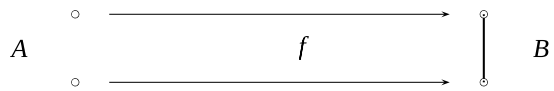
Definice. Buďte $(M, \leq)$, $(N, \leq)$ dvě uspořádané množiny. Zobrazení $f : M \to N$ se nazývá *izotonní*, jestliže platí implikace $a \leq b \Rightarrow f(a) \leq f(b)$.

Je-li zobrazení f bijektivní a f i f^{-1} jsou izotonní, pak říkáme, že f je *izomorfismus* uspořádaných množin, a že uspořádané množiny $(M, \leq)$, $(N, \leq)$ jsou *izomorfní*.

Příklad. Identické zobrazení $\mathrm{id} : (\mathbf{N}, |) \to (\mathbf{N}, \leq)$ je izotonní zobrazení. Skutečně, jestliže $a|b$, pak $b = na$ pro nějaké $n \in \mathbf{N}$, ale $n \geq 1$, a proto $b = na \geq a$.

Inverzní zobrazení $\mathrm{id} : (\mathbf{N}, \leq) \to (\mathbf{N}, |)$ není izotonní zobrazení, protože neplatí implikace $a \leq b \Rightarrow a|b$ (například $2 \leq 3$, ale neplatí $2|3$).

Příklad. Buďte $A = B = \{0, 1\}$ dvouprvkové množiny, opatřené uspořádáním podle následujících diagramů:



Buď $f : A \to B$ identické zobrazení. Pak f je izotonní bijekce, jejíž inverze f^{-1} není izotonní.

Cvičení. Dokažte, že kompozice izotonních zobrazení je izotonní zobrazení.

Svazy

Definice. Buď $(M, \le)$ uspořádaná množina. Nechť pro každé dva prvky $x, y \in M$ existuje infimum $\inf\{x, y\}$ a supremum $\sup\{x, y\}$. Pak říkáme, že M je *svazově uspořádaná množina*.

Příklady. 1) Buď M množina, pak je $(\mathbf{P}(M), \subseteq)$ svazově uspořádaná množina, přičemž platí $\inf\{X, Y\} = X \cap Y$ a $\sup\{X, Y\} = X \cup Y$ pro libovolné prvky $X, Y \in \mathbf{P}(M)$.

2) $(\mathbf{N}, |)$ je svazově uspořádaná množina, přičemž $\inf\{a, b\} =$ největší společný dělitel, $\sup\{a, b\} =$ nejmenší společný násobek čísel $a, b \in \mathbf{N}$.

3) Každý řetězec $(M, \le)$ je svazově uspořádaná množina, přičemž $\inf\{a, b\} = \min\{a, b\}$ je menší, resp. $\sup\{a, b\} = \max\{a, b\}$ je větší z prvků $a, b \in M$.

Tvrzení. *Buď $(M, \le)$ svazově uspořádaná množina. Označme*

$$x \vee y := \sup\{x, y\}, \qquad x \wedge y := \inf\{x, y\}.$$

Pak

$$\begin{aligned} x \vee x &= x, & x \wedge x &= x, \\ x \vee y &= y \vee x, & x \wedge y &= y \wedge x, \\ x \vee (y \vee z) &= (x \vee y) \vee z, & x \wedge (y \wedge z) &= (x \wedge y) \wedge z, \\ x \vee (y \wedge x) &= x, & x \wedge (y \vee x) &= x \end{aligned} \tag{$*$}$$

pro libovolná $x, y, z \in M$.

Důkaz. Asociativita: Cvičení. Návod: Ukažte, že $x \vee (y \vee z) = \sup\{x, y, z\} = (x \vee y) \vee z$.
Zbytek: Cvičení.

Cvičení. Dokažte, že $x_1 \vee x_2 \vee \cdots \vee x_n = \sup\{x_1, x_2, \ldots, x_n\}$. (Vlevo nezáleží na uzávorkování, protože operace je asociativní.)

Definice. Algebraická struktura $(M, \wedge, \vee)$ se dvěma binárními operacemi $\wedge$ a $\vee$ se nazývá *svaz*, jestliže jsou splněny podmínky $(*)$. Binární operace $\wedge$ se nazývá *průsek*, binární operace $\vee$ se nazývá *spojení*.

Ukázali jsme, že každá svazově uspořádaná množina je svaz. Platí však i obráceně, že každý svaz je svazově uspořádaná množina.

Cvičení. A) Buď $(M, \wedge, \vee)$ svaz. Pak platí:
(1) Položme $x \leq_\wedge y$ právě když $x \wedge y = x$. Pak je $\leq_\wedge$ uspořádání na množině M.
(2) Položme $x \leq_\vee y$ právě když $x \vee y = y$. Pak je $\leq_\vee$ uspořádání na množině M.
(3) Uspořádání $\leq_\wedge$ je shodné s uspořádáním $\leq_\vee$ a je svazové, přičemž

$$\sup\{x, y\} = x \vee y, \qquad \inf\{x, y\} = x \wedge y.$$

B) Buď $(M, \wedge, \vee)$ svaz. Ukažte, že $(M, \vee, \wedge)$ je také svaz; nazývá se *duální svaz*. Ověřte, že duální svaz má duální uspořádání.

Nadále budeme používat termín svaz i pro svazově uspořádané množiny. Svazy budeme chápat i jako algebraické struktury i jako uspořádané množiny současně. Víme totiž, že uspořádání jednoznačně určuje algebraickou strukturu a algebraická struktura zase jednoznačně určuje uspořádání.

Cvičení. S každým svazem jsou spojeny dvě pologrupy $(M, \wedge)$ a $(M, \vee)$.
A) Dokažte, že následující výroky o svazu $(M, \wedge, \vee)$ jsou ekvivalentní:
(1) M má největší prvek e;
(2) $(M, \wedge, e)$ je monoid.
B) Zformulujte a dokažte „duální“ výsledek o monoidu $(M, \vee, e)$.

Cvičení. Ukažte, že pologrupa $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ s operací „$\sqcup$“ zadanou tabulkou

$\sqcup$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\spadesuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\spadesuit$
$\diamondsuit$	$\heartsuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$

je pologrupou $(A, \sqcup)$ některého svazu $(A, \sqcap, \sqcup)$. Nakreslete diagram tohoto svazu a vysvětlete, jak jej lze použít k důkazu asociativity operace „$\sqcup$“.

Při počítání ve svazech můžeme použít následující užitečné implikace:

Tvrzení. *Pro každé tři prvky x, a, b svazu L platí*
(i) *jestliže $a \leq b$, pak $a \wedge x \leq b \wedge x$;*
(ii) *jestliže $a \leq b$, pak $a \vee x \leq b \vee x$;*
(iii) *jestliže $x \leq a$, $x \leq b$, pak $x \leq a \wedge b$;*
(iv) *jestliže $x \geq a$, $x \geq b$, pak $x \geq a \vee b$.*

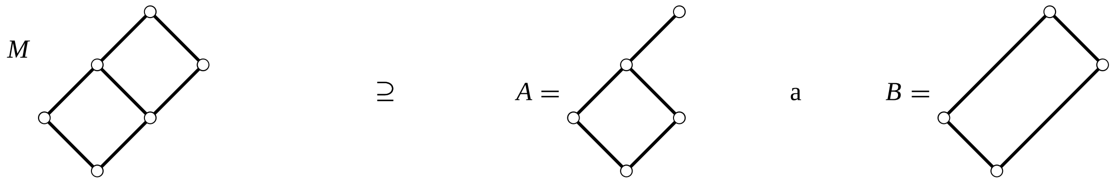
Důkaz. (i) Nechť $a \leq b$, pak $a \wedge b = a$, načež $(a \wedge x) \wedge (b \wedge x) = a \wedge b \wedge x = a \wedge x$; odtud tvrzení. (ii) cvičení; (iii) a (iv) plynou ihned z definice infima a suprema (cvičení).

Je-li $(L, \wedge, \vee)$ svaz, pak je $(L, \vee, \wedge)$ také svaz. Identity $(*)$ definující svaz jsou totiž symetrické vzhledem k vzájemné záměně $\wedge$ a $\vee$. Nazývá se *duální svaz* ke svazu L a budeme jej značit L^*.

Stává se, že podmnožina A svazu M obsahuje i všechna suprema a infima všech dvojic svých prvků, a je potom sama svaz.

Definice. *Podsvaz* svazu $(M, \wedge, \vee)$ je podmnožina $A \subset M$ taková, že pro každé $x, y \in A$ platí $x \wedge y \in A$ a $x \vee y \in A$.

Příklad. Svaz M a dva jeho podsvazy A a B:



Cvičení. (1) Každá podmnožina řetězce je podsvaz.
(2) Každá podmnožina svazu, která je řetězcem, je podsvaz.

Nicméně, podmnožina A může být svazem vzhledem k indukovanému uspořádání, aniž by byla podsvazem:

Příklad. Svaz M a jeho podmnožina A, která je svazem, ale není podsvazem.

Supremum $x \vee_A y$ v A je různé od suprema $x \vee_M y$ v M!

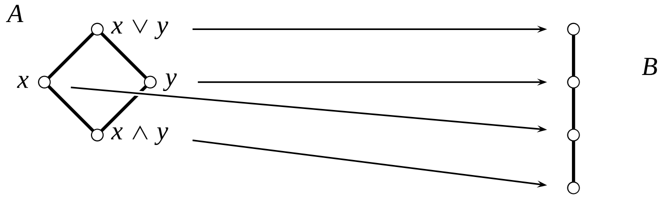
Definice. Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy. Zobrazení $f : L \to R$ se nazývá *homomorfismus* svazů, jestliže $f(a \wedge b) = f(a) \wedge f(b)$ a $f(a \vee b) = f(a) \vee f(b)$ pro každé $a, b \in X$.

Tvrzení. *Každý homomorfismus svazů je izotonní zobrazení.*

Důkaz. Buďte $(X, \wedge, \vee)$, $(Y, \wedge, \vee)$ svazy, buď $f : X \to Y$ homomorfismus. Nechť $a, b \in X$ a nechť $a \le b$, takže $a \wedge b = a$, načež $f(a) \wedge f(b) = f(a \wedge b) = f(a)$, a proto $f(a) \le f(b)$, což se mělo dokázat.

Izotonní zobrazení svazů však nemusí být homomorfismus:

Příklad. Zobrazení f je izotonní zobrazení svazů, je-li



Toto zobrazení *není* homomorfismus svazů, protože $f(x) \vee f(y) = f(y) \neq f(x \vee y)$

Cvičení. Buď $f : A \to B$ zobrazení svazu $(A, \wedge, \vee)$ do svazu $(B, \wedge, \vee)$. Dokažte, že následující výroky jsou ekvivalentní:
1° f je izomorfismus uspořádaných množin;
2° f je izomorfismus svazů.

Úplné svazy

Definice. Buď L svaz, řekneme, že L je *úplný*, má-li každá podmnožina v L supremum i infimum.

Příklad. (1) Každý konečný svaz je úplný a platí $\sup\{x_1, \ldots, x_n\} = x_1 \vee \ldots \vee x_n$, $\inf\{x_1, \ldots, x_n\} = x_1 \wedge \ldots \wedge x_n$.
(2) Svaz $(\mathbf{P}(M), \subseteq)$ je úplný. Infima jsou průniky, suprema jsou sjednocení.
(3) Svaz $(\mathbf{N}, \leq)$ není úplný. Schází například supremum celé množiny $\mathbf{N}$.

Každý úplný svaz L má největší prvek $\sup L$ i nejmenší prvek $\inf L$.

Věta. *Buď L uspořádaná množina, jejíž každá podmnožina má infimum. Pak L je úplný svaz.*

Důkaz. Buď $X \subseteq L$. Označme Y množinu všech horních závor množiny X. Položme $s = \inf Y$ a dokažme, že $s = \sup X$.

Nejprve dokažme, že s je horní závora množiny X. Buď tedy $x \in X$ libovolné. Pro každý prvek $y \in Y$ pak máme $y \geq x$, protože y je horní závora množiny X. To ale znamená, že x je dolní závora množiny Y. Odtud $x \leq s$, protože s je největší dolní závora množiny Y.

Předchozí výsledek znamená, že $s \in Y$. Protože navíc $s = \inf Y$, je s nejmenší prvek množiny Y, a tedy nejmenší horní závora množiny X, což se mělo dokázat.

Cvičení. Dokažte, že $\inf \emptyset$ je největší prvek v X. Mezi předpoklady věty proto je i předpoklad, že X má největší prvek. Například $(\mathbf{N}, \leq)$ není úplný svaz, přestože každá *neprázdná* podmnožina má infimum.

Posledně uvedená věta poskytuje cenný způsob důkazu, že některá uspořádaná množina je svaz.

Příklad. Buď A grupa, označme $\mathbf{P}(A)$ množinu všech podgrup grupy A. Pak je $(\mathbf{P}(A), \subseteq)$ úplný svaz.

Snadno se totiž ukáže, že pro libovolné podgrupy A_i, $i \in I$, je $\bigcap_{i \in I} A_i$ zase podgrupa (cvičení), která je současně infimem $\inf\{A_i\}_{i \in I}$ (cvičení). Podle předchozí věty je potom $(\mathbf{P}(A), \subseteq)$ úplný svaz. Proto existuje i supremum $\sup\{A_i\}_{i \in I}$ a je průnikem všech podgrup, které obsahují všechny podgrupy A_i. Příklad je zformulován pro grupy, ale jeho analogie platí i pro pologrupy, monoidy a v podstatě jakékoliv algebraické struktury.

Problém k řešení. Označme $E(A)$ množinu všech relací ekvivalence na A. Protože $E(A) \subseteq \mathbf{P}(A^2)$, vzniká na $E(A)$ indukované uspořádání. Dokažte, že $E(A)$ je úplný svaz.

3. Distributivní svazy

Definice. Řekneme, že svaz $(M, \wedge, \vee)$ je *distributivní*, platí-li pro každé tři prvky $x, y, z \in M$ distributivní zákony
(i) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$;
(ii) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.