14.1 Lemma. *Buď $L = L(\wedge, \vee)$ svaz a ať jsou $a, b, c \in L$. Je-li $a \leq c$, je $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.*

Důkaz. $a \leq a \vee b$ a $a \leq c$, proto $a \leq (a \vee b) \wedge c$. Současně $b \wedge c \leq a \vee b$, $b \wedge c \leq c$, takže $b \wedge c \leq (a \vee b) \wedge c$. $\square$

Poznámka. Zkusme získat duální nerovnost k nerovnosti $a \vee (b \wedge c) \leq (a \vee b) \wedge c$ ($\vee$ a $\wedge$ prohodíme a $\leq$ zaměníme za $\geq$). Ta bude znít, že z $a \geq c$ plyne $a \wedge (b \vee c) \geq (a \wedge b) \vee c$. Vyměníme-li a a c, dostaneme, že z $a \leq c$ plyne $c \wedge (b \vee a) \geq (c \wedge b) \vee a$. To ovšem je naše původní nerovnost, čili jsme neobdrželi žádný nový vztah. Uvedená nerovnost je samoduální.

14.2 Tvrzení. *Bud $L = L(\wedge, \vee)$ svaz. Potom jsou následující podmínky ekvivalentní.*

(i) $a \vee (b \wedge c) = (a \vee b) \wedge c$, *kdykoliv $a, b, c \in L$ a $a \leq c$.*
(ii) $(a \wedge c) \vee (b \wedge c) = ((a \wedge c) \vee b) \wedge c$ *pro všechna $a, b, c \in L$.*
(iii) $(a \vee c) \wedge (b \vee c) = ((a \vee c) \wedge b) \vee c$ *pro všechna $a, b, c \in L$.*

Důkaz. (i) $\Longleftrightarrow$ (ii) : Položíme-li $a' = a \wedge c \leq c$, bude mít identita (ii) tvar $a' \vee (b \wedge c) = (a' \vee b) \wedge c$.

(i) $\Longleftrightarrow$ (iii) : Položíme-li $c' = a \vee c \geq c = a'$, získá identita (iii) tvar $c' \wedge (b \vee a') = (c' \wedge b) \vee a'$. $\square$

Svaz, který vyhovuje ekvivalentním podmínkám tvrzení 14.2, se nazývá *modulární.*

14.3 Lemma. *Buď a, b, c prvky svazu L, $a \leq c$. Je-li $a \leq b$ nebo $b \leq c$, platí $a \vee (b \wedge c) = (a \vee b) \wedge c$.*

Důkaz. Stačí ukázat $a \vee (b \wedge c) \geq (a \vee b) \wedge c$. Ať nejprve $b \geq a$. Pak $a \vee (b \wedge c) \geq b \wedge c = (a \vee b) \wedge c$. Pokud $b \leq c$, tak dostáváme $a \vee (b \wedge c) = a \vee b \geq (a \vee b) \wedge c$. $\square$

Na množině $\{0, 1, u, v, w\}$ definujeme uspořádání tak, že u a v pokrývají 0, w pokrývá v a 1 pokrývá w a u. Takto definované uspořádání dává svaz, a ten se obvykle značí N_5. (Nakreslete si Hasseův diagram!).

14.4 Tvrzení. *Svaz L je modulární právě když neobsahuje podsvaz izomorfní svazu N_5.*

Důkaz. Svaz N_5 modulární není, neboť $v \vee (u \wedge w) = v$, zatímco $(v \vee u) \wedge w = w$. Proto L, je-li modulární, nemůže obsahovat podsvaz izomorfní s N_5.

Není-li L modulární, lze najít $a, b, c \in L$, že $a \leq c$ a $a \vee (b \wedge c) < (a \vee b) \wedge c$. Ukážeme, že $\{b \wedge c, a \vee (b \wedge c), (a \vee b) \wedge c, a \vee b, b\}$ tvoří podsvaz izomorfní s N_5. Z $b \wedge c = a \vee (b \wedge c)$ plyne $a \leq b \wedge c$, odkud $a \leq b$. Z $a \vee b = (a \vee b) \wedge c$ dostáváme $a \vee b \leq c$, takže $b \leq c$. Ovšem podle 14.3 neplatí ani $a \leq b$ ani $b \leq c$. Proto $b \wedge c < a \vee (b \wedge c) \leq (a \vee b) \wedge c < a \vee b$ a $b \wedge c < b < a \vee b$. Tím jsou dány operace $\wedge$ a $\vee$ na uvedených řetězcích. Zbývá určit $b \wedge x$ a $b \vee x$, kde $x \in \{a \vee (b \wedge c), (a \vee b) \wedge c\}$. Platí $b \wedge c \leq b \wedge (a \vee (b \wedge c)) \leq b \wedge ((a \vee b) \wedge c) = (b \wedge c) \wedge (a \vee b) \leq b \wedge c$, takže

$b \wedge c = b \wedge (a \vee (b \wedge c)) = b \wedge ((a \vee b) \wedge c)$. Obdobně $b \vee a \geq b \vee ((a \vee b) \wedge c) \geq b \vee a \vee (b \wedge c) = b \vee a$. $\square$

Modulární svazy jsou v matematice velmi důležité. Bez důkazu uvedeme jednu jejich typickou vlastnost: Jestliže $a = a_0 < \cdots < a_k = b$ a $c = c_0 < \cdots < c_r = d$ jsou dvě posloupnosti prvků modulárního svazu, kde každý člen posloupnosti pokrývá člen předchozí, tak z $a = c$ a $b = d$ plyne $r = k$. (V konečném modulárním svazu tedy platí, že každé dvě cesty v Hasseově diagramu mezi dvěma prvky jsou stejně dlouhé – pokud se ovšem pohybujeme pouze zdola nahoru nebo pouze zeshora dolů.)

14.5 Tvrzení. *Buď G grupa a A a B její podgrupy. Je-li A normální v G, tak podgrupa generovaná $A \cup B$ je rovna $AB = BA$. Svaz normálních podgrup G je modulární.*

Důkaz. Podgrupu generovanou $A \cup B$ označíme $A \vee B$. Uvažme množinu AB. Jsou-li $a_i \in A$, $b_i \in B$, $i = 1, 2$, tak $a_1 b_1 a_2 b_2 = a_1 b_1 a_2 b_1^{-1} b_1 b_2$, přičemž $b_1 a_2 b_1^{-1} \in A$. Proto je množina AB uzavřená na binární operaci $\cdot$. Dále $(a_1 b_1)^{-1} = b_1^{-1} a_1^{-1} = b_1^{-1} a_1^{-1} b_1 b_1^{-1} \in AB$.

Buď nyní A, B, C normální podgrupy G, $A \subseteq C$. Je třeba ukázat $A \vee (B \cap C) \supseteq (A \vee B) \cap C$, čili $A(B \cap C) \supseteq (AB) \cap C$. Je-li $a \in A$, $b \in B$ a $ab \in C$, je $b = a^{-1}(ab) \in C$, takže $b \in B \cap C$. $\square$

14.6 Tvrzení. *Buď L svaz. Potom jsou následující podmínky ekvivalentní.*

(i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ *pro všechna* $a, b, c \in L$.
(ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *pro všechna* $a, b, c \in L$.
(iii) $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$ *pro všechna* $a, b, c \in L$.

Přitom svaz splňující tyto podmínky je modulární.

Důkaz. (i) $\Longrightarrow$ (ii) : $(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge ((a \wedge b) \vee c) = a \wedge ((a \vee c) \wedge (b \vee c)) = (a \wedge (a \vee c)) \wedge (b \vee c) = a \wedge (b \vee c)$.

(ii) $\Longrightarrow$ (i) : Identity (i) a (ii) jsou duální. V předchozím důkazu tedy stačí zaměnit $\wedge$ a $\vee$.

(i+ii) $\Longrightarrow$ (iii) : $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \wedge (b \vee c)) \vee (b \wedge c) = ((a \wedge (b \vee c)) \vee b) \wedge ((a \wedge (b \vee c)) \vee c) = ((a \vee b) \wedge (b \vee c)) \wedge ((a \vee c) \wedge (b \vee c)) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$.

(iii) $\Longrightarrow$ (i) : Nejprve ukážeme modularitu. Je-li $a \leq c$, dostáváme $a \vee (b \wedge c) = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c) = (a \vee b) \wedge c$. Buď nyní $a, b, c \in L$ libovolná. Položme $u = (a \wedge b) \vee (b \wedge c) \vee (a \wedge c)$. Pak $a \wedge (b \vee c) = a \wedge u = (((a \wedge b) \vee (a \wedge c)) \vee (b \wedge c)) \wedge a = ((a \wedge b) \vee (a \wedge c)) \vee (b \wedge c \wedge a) = (a \wedge b) \vee (a \wedge c)$. $\square$

Svazy, které splňují ekvivalentní podmínky tvrzení 14.6 se nazývají *distributivní* a vztahy (i) a (ii) se nazývají distributivními zákony.

Na množině $\{0, u, v, w, 1\}$ definujme svaz tak, že 0 je nejmenší prvek, 1 největší prvek, $u \wedge v = u \wedge w = v \wedge w = 0$ a $1 = u \vee v = u \vee w = v \vee w$. Tento svaz se obvykle značí M_5. Často se mu říká 'diamant'.

M_5 zjevně není distributivní. Proto žádný distributivní svaz neobsahuje podsvaz izomorfní N_5 nebo M_5. Platí i obrácené tvrzení.

14.7 Tvrzení. *Svaz L je distributivní právě když neobsahuje podsvaz izomorfní N_5 nebo M_5.*

Nástin důkazu. Potřebujeme ukázat, že pokud modulární svaz není distributivní, lze v něm nalézt M_5. Není-li L distributivní, lze najít $x, y, z \in L$ takové, že $r = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z) \wedge (y \vee z) = s$. Pak $r < s$ a pro $a = (x \wedge s) \vee r$, $b = (y \wedge s) \vee r$, $c = (z \wedge s) \vee r$ lze s trochou počítání pomocí modulárního zákona ukázat, že $a \wedge b = r$ a $a \vee b = s$. Ze symetrie pak vyplyne, že $a \wedge c = r = b \wedge c$ a $a \vee c = s = b \vee c$. Zbytek je již snadný. □

Buď $L = L(\wedge, \vee, \mathbf{0}, \mathbf{1})$ 0,1–svaz, a ať $a \in L$. Potom $b \in L$ nazveme *komplementem* (doplňkem), jestliže $a \wedge b = 0$ a $a \vee b = 1$. Z definice plyne, že je-li b komplementem a, je a komplement b.

14.8 Tvrzení. *Buď L distributivní 0,1–svaz. Potom má každý prvek nejvýše jeden komplement.*

Důkaz. Buď b a c komplementy a. Pak $b = b \wedge \mathbf{1} = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = b \wedge c$. Tudíž $b \geq c$. Obdobně dostaneme $b \leq c$, a tedy $b = c$. □

V N_5 má každý prvek komplement, ale tento komplement nemusí být jednoznačný. Totéž platí o M_5. Představme si, že v distributivním 0,1–svazu L má každý prvek komplement. Pak je jednoznačně určena unární operace $'$ taková, že pro všechna $a \in L$ je $a \wedge a' = \mathbf{0}$ a $a \vee a' = \mathbf{1}$.

Algebra $L = L(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$, kde $L(\vee, \wedge, \mathbf{0}, \mathbf{1})$ je distributivní 0,1–svaz a $'$ je unární operace, která vyhovuje identitám $a \wedge a' = \mathbf{0}$ a $a \vee a' = \mathbf{1}$, se nazývá *Booleova algebra.*

14.9 Lemma. *Ať $L = L(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ je Booleova algebra. Potom*

(i) $(a')' = a$ *pro všechna* $a \in L$.
(ii) $\mathbf{0}' = \mathbf{1}$ a $\mathbf{1}' = \mathbf{0}$.
(iii) $(a \wedge b)' = a' \vee b'$ a $(a \vee b)' = a' \wedge b'$ *pro všechna* $a, b \in A$. *(De Morganovy zákony.)*

Důkaz. (i) a je komplement a'. Podle 14.8 je komplement jednoznačně určen. Proto $a = (a')'$.
(ii) Toto jistě každý zvládne.
(iii) $(a \wedge b) \vee (a' \vee b') = (a \vee a' \vee b') \wedge (b \vee a' \vee b') = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. $(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$. Druhý zákon je k prvému duální. □