# Algebra

## 1. Algebry, homomorfismy, kongruence

**Def.:** *$A$ množina, zobrazení $\alpha : A^n \to A$, kde $n \in \{0, 1, ...\}$ je* **n-ární operace** *($n$ je* **arita***).*

**Def.:** *$\alpha_i, i \in I$ operace arity $\Omega_i$ na $A$, pak $A(\alpha_i | i \in I)$ je* **algebra**.

**Def.:** *mn. $B$ je* **uzavřená** *na operaci $\alpha$, když $\forall b_1, ...b_n \in B$ platí $\alpha(b_1, ...b_n) \in B$.*

**Def.:** *$A(\alpha_i | i \in I)$ algebra, $B \subseteq A$. $B$ je* **podalgebra** *$A$, je-li uzavřená na $\alpha_i \forall i \in I$.*

**Poznámka 1.1 : Průnik podalgeber je podalgebra.** *Důkaz: Vezmu $b_1, ...b_n \in \cap_{j \in J} A_j$. Vím že $\alpha(b_1, ..b_n) \in A_j \ \forall j \in J$.*

**Def.:** *Zobr. $f : A \to B$ je* **slučitelné** *s operací $\alpha$, pokud $a_1, ..a_n \in A \Rightarrow f(\alpha_{(A)}(a_1, ...a_n)) = \alpha_{(B)}(f(a_1), ...f(a_n))$.*

**Def.:** *Algebry $A$ a $B$, které mají stejný počet operací stejné arity, jsou* **algebry stejného typu**.

**Def.:** *Pro algebry stejného typu je $f : A \to B$* **homomorfismus**, *pokud je slučitelné se všemi jejich operacemi.*

**Poznámka 1.2 : Složení homomorfismů je homomorfismus. Je-li $f$ bijekce a homomorfismus, je $f^{-1}$ taky homomorfismus.** *Důkaz: pro 1 operaci, ze slučitelnosti, z def. bijekce.*

**Def.:** *Bijektivní homomorfismus je* **izomorfismus**, *algebry stejného typu jsou* **izomorfní**, *$\exists$-li mezi nimi aspoň 1 izomorfismus.*

**Poznámka 1.3 : Nechť $f : A \to B$ je homomorfismus, nechť $C$ je podalgebra $A$ a $D$ podalgebra $B$. Pak $f(C)$ je podalgebra $B$ a $f^{-1}(D) = \{a \in A | f(A) \in D\}$ je podalgebra $A$.** *Důkaz: pro 1 operaci ověřit uzavřenost, z def. homomorfismu, def. podalgebry.*

**Def.:Relace** *na množině $A$ je lib. podmnožina $\rho \subseteq A \times A$. $(a, b) \in \rho \equiv^{def} a \rho b$. $\rho^{-1} = \{(a, b) | (b, a) \in \rho\}$* - **opačná relace**, *$\rho^+ = \{(a, c) \in A \times A | \exists b_0, ..b_k \in A : b_0 = a, b_k = c, (b_i, b_{i+1}) \in \rho\}$* - **tranzitivní obal**.

**Def.:** *$id = \{(a, a) | a \in A\}$* - **identita**, *$\rho^{-1} \subseteq \rho$* - **symetrická**, *$id \subseteq \rho$* - **reflexivní**, *$\rho^+ \subseteq \rho$* - **tranzitivní**. *Reflexivní, symetrická a tranzitivní relace je* **ekvivalence**.

**Def.:** *$A/\rho = \{[a]_\rho | a \in A\}$ je* **faktorová množina**, *kde $[a]_\rho = \{b \in A | (a, b) \in \rho\}$ jsou* **třídy ekvivalence**.

**Def.: přirozená projekce** *mn. $A$ podle $\rho$ je $\pi_\rho : A \to A/\rho$, t.ž. $\pi_\rho(a) = [a]_\rho$.*

**Poznámka 1.4 : (1) Nechť $\rho$ je ekvivalence na $A$. Pak $\{[a]_\rho | A \in A\}$ tvoří (disjunktní) rozklad množiny A. (2) $A = \dot{\cup}_{j \in J} A_j$, tj. mám disj. rozklad $A$ na $A_j$, pak relace $\rho$ daná předpisem $(a, b) \in \rho \equiv^{def} \exists j \in J : a, b \in A_j$ tvoří ekvivalenci na A.** *Důkaz: (DCV)*

**Def.:***$\rho$ je* **slučitelná** *s $\alpha$, pokud $a_1, ...a_n, b_1, ...b_n : (a_i, b_i) \in \rho \ \forall i \Rightarrow \alpha(a_1, ...a_n) \rho \ \alpha(b_1, ...b_n)$.*

**Def.:kongruence** *je každá ekvivalence slučitelná se všemi operacemi algebry.*

**Def.:***$f : A \to B$,* $\ker f : (a_1, a_2) \in \ker f \equiv^{def} f(a_1) = f(a_2)$ *je* **jádro** *zobr. $f$.*

**Poznámka 1.5 : $f : A \to B$ zobr., $\rho$ ekviv. na $A$. (1) $\ker f$ je ekvivalence na $A$. (2) $f$ je prosté $\Leftrightarrow$ $\ker f = id$. (3) $\ker \pi_\rho = \rho$. (4) zobr. $g : A/\rho \to B$, splňující podmínku $g \circ \pi_\rho = f$ existuje $\Leftrightarrow \rho \subseteq \ker f$** *Důkaz: (1) ekvivalence $\ker f$ se dostane z ekvivalence " = ", (2),(3) triviální, (4) " $\Rightarrow$ " vezmu $(a_1, a_2) \in \rho$, potom $f(a_1) = f(a_2)$, tedy $(a_1, a_2) \in \ker f$. " $\Leftarrow$ " $a_1 \rho a_2 \Rightarrow (\rho \subseteq \ker f) f(a_1) = f(a_2) \Rightarrow g([a_1]_\rho) = g([a_2]_\rho)$, tedy g je dobře definované.*

**Poznámka 1.6 : $f : A \to B$ je homomorfismus algeber stejného typu $\Rightarrow \ker f$ je kongruence na $A$.** *Důkaz: $\ker f$ je ekvivalence z 1.5(1), slučitelnost přímo, z homomorfismu f*

**Věta 1.7 : $\rho$ kongruence na $A \Rightarrow$ přirozená projekce $\pi_\rho : A \to A/\rho$ je homomorfismus.** *Důkaz: $\forall$ operaci $\alpha$ na $A$ def. $\alpha$ na $A/\rho$ - faktor operaci, sluč. s $\pi_\rho$.*

**Def.:** *Algebra s 1 binární operací je* **grupoid**. *$e \in G : e \cdot g = g \cdot e = g \ \forall g \in G$ je* **neutrální prvek**. *Algebra $G(\cdot, e)$ s $\cdot$ asociativní je* **monoid**.

**Poznámka 1.8 : Každý grupoid odsahuje nevýš 1 neutrální prvek.** *Důkaz: sporem pro 2 neutrální prvky*

**Poznámka 1.9 :** $M(\cdot, e)$ **monoid,** $a, b, c \in M$**. Pokud** $(a \cdot b = e)$ & $(b \cdot c = e)$**, pak** $a = c$ *Důkaz:* $a = ae = a(bc) = (ab)c = ec = c$.

**Def.:** $M(\cdot, e)$ *monoid,* $m \in M$*, Pak* $m^{-1} \in M$ *je* **inverzní prvek***, pokud* $m \cdot m^{-1} = m^{-1} \cdot m = e$*. Prvek je* **invertibilní***, pokud má nějaký inverzní prvek.*

**Poznámka 1.10 : Buď** $M(\cdot, e)$ **monoid, pak** $G = \{m \in M | \exists m^{-1}\}$ **je jeho podmonoid. Každý inverzní prvek je invertibilní.** *Důkaz: uzavřenost na* $e$*,* $\cdot$ *- pro součin 2 prvků z* $G$ *ex. inv. prvek; inverz k inverzu je pův. prvek.*

**Def.:** *Algebra* $G(\cdot, ^{-1}, e)$ *je* **grupa***, pokud je* $G(\cdot, e)$ *monoid a* $^{-1}$ *je operace inv. prvku.*

**Poznámka 1.11 :** $M(\cdot, e)$ **monoid,** $M^*$ **množ. všech jeho invertibilních prvků. Omezíme-li operaci** $\cdot$ **na** $\cdot_{M^*}$ **na prvky z** $M^*$ **a jako** $^{-1}$ **vezmeme operaci inv. prvku na** $M^*$**, pak** $M^*(\cdot_{M^*}, ^{-1}, e)$ **je grupa.** *Důkaz: Z 1.10 je možné* $\cdot$ *omezit na* $M^*$*,* $M^*$ *je podmonoid* $M(\cdot, e)$ *z def. je grupa.*

**Def.:** $H \subseteq G(\cdot, ^{-1}, e)$ *je* **normální podgrupa***, pokud je podgrupa a zároveň* $\forall g \in G\ \forall h \in H : g^{-1} \cdot h \cdot g \in H$*.* $G$ *je* **komutativní (abelovská)***, pokud je* $\cdot$ *komutativní.*

**Poznámka 1.12 : Každá podgrupa komutativní grupy je normální.** *Důkaz: z komutativity.*

**Věta 1.13 : Nechť** $G(\cdot, ^{-1}, e)$ **je grupa a** $\rho$ **relace na** $G$**. Pak** $\rho$ **je kongruence** $\Leftrightarrow [e]_\rho$ **je normální podgrupa** $G$ **a** $(g, h) \in \rho$ **právě když** $g^{-1} \cdot h \in [e]_\rho$**.** *Důkaz:* " $\Rightarrow$ " : $\rho$ *kongruence - ověřit uz. na* $e$ *(z refl.), uz. na* $^{-1}$*:* $(e, h) \in \rho \Rightarrow (e^{-1}(= e), h^{-1}) \in \rho$*; uz. na* $\cdot$*:* $(e, g), (e, h) \in \rho \Rightarrow (e \cdot e, g \cdot h) \in \rho$*; z toho* $[e_\rho]$ *je podgrupa.* $(e, h) \in \rho$*,* $g \in G \Rightarrow (g^{-1}(hg), g^{-1}(eg)) = (g^{-1}gh, e) \in \rho$ *(refl., sluč.)- normální podgrupa. Ověření* $(g, h) \in \rho \Leftrightarrow g^{-1}h \in [e]_\rho$*:* " $\Rightarrow$ " *ze sluč., vynásobit zleva* $g^{-1}$*,* " $\Leftarrow$ " *vynásobit zleva* $g$*.* " $\Leftarrow$ " : *def.* $\rho : (g, h) \in \rho \equiv^{def} g^{-1} \cdot h \in H$*, dokázat že* $\rho$ *je ekvivalence (přímo),* $[e]_\rho = H$ *(přímo), slučitelnost s operacemi - e platí* $\forall$ *refl. relaci,* $^{-1} : g^{-1}h \in H \Rightarrow h^{-1}g \in H \Rightarrow h(h^{-1}g)h \in H$*,* $\cdot : \bar{h}\bar{g}^{-1} \in H(= \bar{g}(\bar{g}^{-1}\bar{h})\bar{g}^{-1})$*;* $\bar{g}^{-1} \cdot (g^{-1} \cdot h \cdot \bar{h} \cdot \bar{g}^{-1}) \cdot \bar{g} = (g\bar{g})^{-1}(h\bar{h}) \in H$*.*

**Def.:** $\mathbf{G/H} = G/\rho_h$*, kde* $\rho_h$ *je kongruence odp. dle 1.13 normální podgrupě* $H$*.*

## 2. Uzávěrové systémy na algebrách

**Def.:** $A$ *množina,* $\mathcal{C} \subseteq \mathcal{P}(\mathcal{A})$*.* $\mathcal{C}$ *je* **uzávěrový systém***, pokud (1)* $A \in \mathcal{C}$*, (2)* $B_i \in \mathcal{C}$*,* $i \in I \Rightarrow \cap_{i \in I} B_i \in \mathcal{C}$*.*

**Def.:** *zobrazení* $cl_\mathcal{C} : \mathcal{P}(A) \to \mathcal{C} : cl_\mathcal{C}(B) = \cap_{C \in \mathcal{C}, B \subseteq C} C$ *se nazývá* **uzávěr**.

**Def.:** *zobr.* $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ *je* **uzávěrový operátor***, pokud* $B \subseteq \alpha(B)\ \forall B \in \mathcal{P}(A)$*,* $\alpha(\alpha(B)) = \alpha(B)$*,* $B \subseteq C \Rightarrow \alpha(B) \subseteq \alpha(C)\ \forall B, C \in \mathcal{P}(A)$*.*

**Poznámka 2.1 : Systém všech podalgeber algebry A tvoří uzávěrový systém.** *Důkaz: z 1.1 - průnik podalgeber je podalgebra - vyhovuje*

**Věta 2.2 : (1) Je-li** $\mathcal{C}$ **uzávěrový systém, pak** $cl_\mathcal{C}$ **je uzávěrový operátor. (2) Je-li** $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ **uzávěrový operátor, pak množina** $\mathcal{C} = \{C \in \mathcal{P}(A), \alpha(C) = C\}$ **tvoří uzávěrový systém a** $\alpha = cl_\mathcal{C}$**.** *Důkaz: (1) dokázat axiomy uz. operátoru pro* $cl_\mathcal{C}$ *- 1. plyne z vl.* $cl_\mathcal{C}$*, 2. obě inkluze (*$\subseteq$ *z 1.,* $\supseteq$ *z 2. ax. uz. systému), 3. z teorie množin. (2) dokázat axiomy* $\mathcal{C}$ *- 1.* $A$ *a je pevný bod* $\alpha$*, 2.* $\alpha(\cap_{i \in I} B_i) = \cap_{i \in I} B_i$ *-* $\supseteq$ *z 1.ax.uz.op,* $\subseteq$ *z 3.ax.uz.op., dokázat že* $\alpha(B) = \cap_{C \in \mathcal{C}, B \subseteq C} C\ \forall B$ *-* $\alpha(B) \in \mathcal{C}$ *podle 2.ax.uz.op.,* $B \subseteq \alpha(B)$ *z 1.ax.* $\Rightarrow \alpha(B) \supseteq cl(B)$*.* $\alpha(B) \subseteq \cap\{C \in \mathcal{C}, B \subseteq C\}, \alpha(B) \subseteq \alpha(C) = C$ *- z 3.ax.*

**Poznámka 2.3 : Systém všech uzávěrových systémů na množině** $A$ **tvoří uzávěrový systém na** $\mathcal{P}(A)$**.** *Důkaz: 1.ax.:* $A \subseteq \mathcal{P}(A), \cap_{B_i \in \mathcal{P}(A)} B_i \in \mathcal{P}(A)$*, 2.ax.:* $\cap_{i \in I} \mathcal{C}_i$ *uz. systém?: 1.ax.:* $\mathcal{P}(A)$ *je uz. systém;* $A \in \cap_{i \in I} \mathcal{C}_i$*, 2.:* $B_j \in \cap_{i \in I} \mathcal{C}_i$ $j \in J \Rightarrow\ \cap_{j \in J} B_i \in \cap_{i \in I} \mathcal{C}_i$*.*

**Poznámka 2.4 : Nechť** $\mathcal{A}$ **a** $\mathcal{B}$ **jsou 2 uz. systémy na** $A$**;** $C, D \subseteq A$**, t.ž.** $\mathcal{A} \subseteq \mathcal{B}$ **a** $C \subseteq D$**, potom** $cl_\mathcal{B}(C) \subseteq cl_\mathcal{A}(D)$**.** *Důkaz:* $cl_\mathcal{B}(C) \subseteq cl_\mathcal{B}(D)$ *platí dle 2.2(1),* $cl_\mathcal{B}(D) \subseteq cl_\mathcal{A}(D)$ *rozepsat jako průniky množin, z teorie množin jako 2.2(1)-3.*

**Poznámka 2.5 : Množina věch reflexivních(symetrických, tranzitivních) relací a množina všech ekvivalencí na množině** $A$ **tvoří uzávěrový systém na** $A \times A$**.** *Důkaz: pro reflexivní* $id \subset A \times A$*,* $id \subset \cap_i \rho_i$*, kde* $\rho_i$ *je refl. - OK, symetrická a tranzitivní podobně, ekvivalence z 2.3 a průniku předch.*

**Poznámka 2.6 : Všechny kongruence na algebře tvoří uzávěrový systém na $A \times A$.** *Důkaz: pro každou operaci zvl. množina sluč. relací $\mathcal{R}_i$ je uz. systém, kongruence z průniku (je průnik uz. systém?). 1.ax $A \times A$ je sluč. s čímkoliv, 2.ax přímo*

**Poznámka 2.7 : Nechť $\rho$ je relace na $A$ Je-li reflexivní(symetrická), pak $\rho^+$ a $\rho \cup \rho^{-1}$ je taky reflexivní(symetrická).** *Důkaz: přímo.*

**Poznámka 2.8 : Nechť $\rho$ je relace, pak $((\rho \cup id) \cup (\rho \cup id)^{-1})^+ = (\rho \cup \rho^{-1} \cup id)^+$ je nejmenší ekvivalence obs. $\rho$ (uzávěr $\rho$ v uz. systému ekvivalencí).** *Důkaz: ekvivalence z 2.7, minimalita zřejmá (musím mít zaručenu refl., sym. i trans.)*

**Def.:** *Nechť $A$ je algebra, $X \subseteq A$, $\mathcal{A}$ je uz. systém všech podalgeber. Pak $cl_{\mathcal{A}}(X)$ je* **podalgebra generovaná množinou** *$X$.*

**Poznámka 2.9 : Nechť $f, g : A \to B$ jsou 2 homomorfismy algeber stejného typu a $cl_{\mathcal{A}}(X) = A$. Pokud $f(x) = g(x)\ \forall x \in X$ (mn. generátorů), pak $f = g$.** *Důkaz: Vezmu $Y = \{a \in A | f(a) = g(a)\}$, $Y \supseteq X$, dokážu sluč. s lib. operací $\Rightarrow$ $Y$ je podalgebra, $cl_{\mathcal{A}}(Y) \supseteq cl_{\mathcal{A}}(X)$.*

# 3. Izomorfismy

**Def.:** *$\rho \subseteq \sigma$ 2 ekvivalence na $A$. Pak $\sigma/\rho$* **- faktor-ekvivalence** *je relace definovaná: $([a]_\rho, [b]_\rho) \in \sigma/\rho \ \equiv^{def} \ (a, b) \in \sigma$.*

**Poznámka 3.1 : (1) Nechť $\rho \subseteq \sigma$ jsou ekvivalence na $A$. Pak $\sigma/\rho$ je ekvivalence na $A$. (2) Nechť $\eta$ je ekvivalence na $A/\rho$, pak ex. právě 1 ekvivalence $\sigma$ na $A$, t.ž. $\rho \subseteq \sigma$ a $\sigma/\rho = \eta$.** *Důkaz: (1) dokázat korektnost definice $\sigma/\rho$ - $([a_1]_\rho = [a_2]_\rho, [b_1]_\rho = [b_2]_\rho, (a_1, b_1) \in \sigma) \Rightarrow$ (z tranzitivity $\sigma$) $(a_2, b_2) \in \sigma$. důkaz ekvivalence - přímo. (2) $\sigma$ najdu podle předpisu $([a]_\rho, [b]_\rho) \in \eta \Leftrightarrow (a, b) \in \sigma$, $\sigma \subset \rho$, $\sigma$ je ekvivalence (z ekvivalence $\eta$) $\Rightarrow$ ex. faktor-ekvivalence.*

**Poznámka 3.2 : Nechť $\rho$ je kongruence na $A$ a $\sigma$ ekvivalence na $A$, $\rho \subseteq \sigma$. Pak $\sigma$ je kongruence na $A \Leftrightarrow \sigma/\rho$ je kongruence na $A/\rho$.** *Důkaz: " $\Rightarrow$ " - z 3.1 plyne ekvivalence $\sigma/\rho$, dokázat slučitelnost s lib. operací $\alpha([a_1]_\rho, ...[a_n]_\rho) = [\alpha(a_1, ...a_n)]$ - ze sluč. $\sigma$. " $\Leftarrow$ " dokázat slučitelnost - to samé naopak.*

**Poznámka 3.3 (Věta o homomorfismu) : Nechť $f : A \to B$ je homomorfismus algeber stejného typu a $\rho$ kongruence na $A$. Pak (1) ex. homomorfismus $g : A/\rho \to B$, t.ž. $f = g\pi_\rho$, právě když $\rho \subseteq \ker f$. (2) $g$ je navíc izomorfismus, právě když $f$ je na a $\rho = \ker f$.** *Důkaz: (1) " $\Rightarrow$ " přímý důsledek 1.5(4), " $\Leftarrow$ " zobr. $g : g([a_i]_\rho) = f(a_i)$ je dobře definované podle 1.5(4), slučitelnost přímo z předpokladů. (2) " $\Rightarrow$ " $(a_1, a_2) \in \rho \Rightarrow g([a_1]) = f(a_1) = f(a_2) = g([a_2])$ (g prosté) $\Rightarrow [a_1] = [a_2]$. " $\Leftarrow$ " dokázat prostost g: $f(a_1) = g([a_1]) = g([a_2]) = f(a_2) \ \Rightarrow \ (a_1, a_2) \in \ker f = \rho \ \Rightarrow$ $[a_1]_\rho = [a_2]_\rho$.*

**Věta 3.4 (1. věta o izomorfismu) : Nechť $f : A \to B$ je homomorfismus algeber stejného typu, pak $f(A)$ je algebra stejného typu a ${}^{A}/_{\ker f}$ je izomorfní algebře $f(A)$.** *Důkaz: definuji $\rho = \ker f$, z pozn. 3.3 ex. homomorfismus $g : {}^{A}/_{\ker f} \to f(A)$, $g$ je na $f(A)$, protože $f$ je na $f(A)$, $\rho = \ker f \Rightarrow g$ je izomorfismus.*

**Věta 3.5 (2. věta o izomorfismu) : Nechť $\rho \subseteq \eta$ jsou kongruence na algebře $A$. Pak ${}^{(A/\rho)}/_{(\eta/\rho)}$ je izomorfní ${}^{A}/_{\eta}$.** *Důkaz: z 3.3 (pro $f = \pi_\eta$) $\exists$ homomorfismus $g : A/\rho \to A/\eta : g([a]_\rho) = [a]_\eta$. $g$ je (z def.) na, z 3.4 (pro g): $A/\eta \ \simeq \ {}^{(A/\rho)}/_{\ker g}$. z def. $g$ $\ker g = \eta/\rho$.*

# 4. Svazy

**Def.:** *Relace $\leq$ na mn. $A$ je (částečné)* **uspořádání**, *pokud je reflexivní, tranzitivní a slabě antisymetrická (tj. $a \leq b, b \leq a \Rightarrow a = b$).*

**Def.:** *Pro usp. $\leq$ na $A$, $B \subseteq A$ je $a \in B$* **nejmenší(největší) prvek**, *jestliže $\forall b \in B a \leq b (\forall b \in B b \leq a)$. $m \in A$ je* **infimum(supremum)** *mn. $B$, jde li o největší prvek množiny $\{a \in A, a \leq b \ \forall b \in B\}$ (nejmenší prvek množiny $\{a \in A, b \leq a \ \forall b \in B\}$. Značení: $\inf_\leq B, \sup_\leq B$.*

**Def.:** *Dvojici $(A, \leq)$ nazvu* **svazem**, *je-li $\leq$ uspořádání a $\forall$ dvojici $\{a, b\} \subseteq A$ ex. $\sup_\leq(\{a, b\})$ a $\inf_\leq(\{a, b\})$.*

**Def.:** *O svazu $(A, \leq)$ řekneme, že je* **úplný**, *jestliže ex. $\inf_\leq(B)$, resp. $\sup_\leq(B)$ pro $\forall B \subseteq A$ (implikuje existenci nejv. a nejm. prvku)*

**Poznámka 4.1 : Buď $A$ svaz, definujme bin. operace na $A$: $\wedge$(průsek) a $\vee$(spojení): $a \wedge b = \inf_{\leq}(\{a,b\})$ a $a \vee b = \sup_{\leq}(\{a,b\})$. Pak platí: (1) $a \wedge b = b \wedge a$, $a \vee b = b \vee a$, (2) $a \vee a = a = a \wedge a$, (3) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (pro $\vee$ stejně), (4) $a \wedge (b \vee a) = a = a \vee (b \wedge a)$. (pro $a, b$ lib. z $A$).** *Důkaz: (1),(2) triviální, (3) z def. suprema a tranzitivity $a \leq (a \vee b) \vee c$, stejně pro b,c; proto pro nejmenší horní odhad $\{b,c\}$, tj. $b \vee c$ platí taky; dále nejm. odhad $\{a,(b \vee c)\} \Rightarrow a \vee (b \vee c) \leq (a \vee b) \vee c$, zpět symetricky. (4) $a \leq a \vee (b \wedge a)$ z def. suprema, opačně platí - horní odhady $(b \wedge a) \leq a$.*

**Poznámka 4.2 : Buď $S(\wedge,\vee)$ algebra s 2 bin. operacemi pro něž platí 4.1. Definujme relaci $\leq$ na $S$: $a \leq b \equiv^{def} (a \vee b = b)$. Potom $(S,\leq)$ tvoří svaz, kde $\sup_{\leq}(\{a,b\}) = a \vee b$, $\inf_{\leq}(\{a,b\}) = a \wedge b$. Tj. můžeme "svaz" říkat algebře $S(\wedge,\vee)$.** *Důkaz: a): ověřit že $\leq$ je uspořádání (přímo), pak $a \leq b \equiv a = a \wedge b$ (z def., 4.1(1)), potom $\inf_{\leq}\{a,b\} = a \wedge b$: $a \wedge b \leq a, a \wedge b \leq b$ (z 4.1) $\Rightarrow a \wedge b \leq \inf\{a,b\}$, pak $c \leq a, b \Rightarrow c \leq (a \wedge b)$. (pro $\sup$ symetricky).*

**Věta 4.3 : Každý uzávěrový systém $\mathcal{C}$ je úplným svazem $(\mathcal{C},\subseteq)$, kde $\sup_{\subseteq}(\mathcal{B}) = cl_{\mathcal{C}}(\cup\mathcal{B})$ a $\inf_{\subseteq}(\mathcal{B}) = cl_{\mathcal{C}}(\cap\mathcal{B})$.** *Důkaz: viz vlastnosti uz. systémů*

**Def.:** *$(S,\leq)$ nechť je svaz $S(\wedge,\vee)$, potom $a$* **pokrývá** *$b$ ($b < \cdot a$), pokud $a,b \in S$ :, $b \leq a, b \neq a, b \leq c \leq a \Rightarrow b = c$ nebo $a = c$.*

**Def.:** *Nechť $e(f) \in S$ je nejmenší(největší) prvek $S$, potom $a$ nazveme* **atom(koatom)** *svazu $S$, jestliže $e < \cdot a$ ($a < \cdot f$).*

**Def.: Hasseův diagram** *svazu je orientovaný graf s vrcholy z $S$, mezi $a,b$ bude hrana z $a$ do $b$ ($a$ bude* **pod** *$b$), pokud $a < \cdot b$.*

**Poznámka 4.4 : Je-li $S(\wedge,\vee)$ svaz, potom je $S(\wedge,\vee)$ taky svaz (opačný svaz)** *Důkaz: plyne z (4.1), (4.2)*

**Poznámka 4.5 : Nechť $S(\wedge,\vee)$ je svaz, $a,b,c \in S$. Pokud $a \leq c$, potom $a \vee (b \wedge c) \leq (a \vee b) \wedge c$)** *Důkaz: z dolních odhadů : $a \leq ((a \vee b) \wedge c)$, $b \wedge c \leq ((a \vee b) \wedge c)$*

**Def.:** *$S(\wedge,\vee)$ je* **modulární**, *pokud $\forall a,b,c \in S : a \leq c \Rightarrow\ a \vee (b \wedge c) = (a \vee b) \wedge c$.*

**Def.:** *$f : A \to B$, kde $(A,\leq),(B,\leq)$ jsou svazy. Pak $f$ je* **monotónní**, *pokud $\forall a_1, a_2 \in A : a_1 \leq a_2 \Rightarrow f(a_1) \leq f(a_2)$ (opačné se nepoužívá).*

**Poznámka 4.6 : Homomorfismus svazů je monotónní.** *Důkaz: $a \leq b \Rightarrow$(4.2) $b = a \vee b \Rightarrow f(b) = f(a \vee b) = f(a) \vee f(b)\ \Rightarrow\ f(a) \leq f(b)$.*

**Poznámka 4.7 : $f : A \leftrightarrow B$ je izomorfismus svazů $\Leftrightarrow$ $f$ i $f^{-1}$ jsou monotónní.** *Důkaz: " $\Rightarrow$ " zřejmé (4.6), " $\Leftarrow$ " sluč. s $\vee$ (podle (4.4) platí i pro $\wedge$). Z monotonie a odhadů $f(a) \vee f(b) \leq f(a \vee b)$, z monotonie $f^{-1}$ $a \vee b \leq f^{-1}(f(a) \vee f(b))$, aplikovat $f$, vyjde op. nerovnost. $f$ je bijekce, proto i $f^{-1}$ je homomorfismus.*

**Poznámka 4.8 : Nechť $A$ je množina, $e \in A$, $\mathcal{C}$ je uz. systém na $A \times A$, obsažený v množině všech ekvivalencí (tj. podmnožina množiny ekvivalencí), systém podmnožin $\mathcal{N} \subseteq \mathcal{P}(A)$. Nechť platí: (1) $[e]_\rho \in \mathcal{N}\ \forall \rho \in \mathcal{C}$, (2) $\forall N \in \mathcal{N}\ \exists \rho \in \mathcal{C} :\ N = [e]_\rho$, (3) $\forall \rho,\eta \in \mathcal{C} : [e]_\rho \subseteq [e]_\eta\ \Rightarrow\ \rho \subseteq \eta$. Pak $\mathcal{N}$ tvoří uzávěrový systém, zobrazení $\varphi : \mathcal{C} \to \mathcal{N} : \varphi(\rho) = [e]_\rho$ je svazový izomorfismus.** *Důkaz: $\mathcal{N}$ je usp. množina; $\varphi$ je dobře definované, na z (1),(2); z (3) je prosté - $\varphi(\rho) = \varphi(\eta) \Rightarrow \rho = \eta$ $\Rightarrow$ je bijekce, $\varphi^{-1}([e]_\rho) = \rho$. Z (3) je $\varphi^{-1}$ monotónní, $\rho \subseteq \eta : \varphi(\rho) = [e]_\rho \subseteq [e]_\eta = \varphi(\eta)$ - $\varphi$ je monotónní. Mám bijekci oběma směry mezi svazem a usp. množinou $\Rightarrow$ mám na $\mathcal{N}$ i $\mathcal{C}$ stejnou strukturu vzhledem k $\subseteq$. Proto $\mathcal{N}$ je uz. systém, zbytek z (4.7).*

**Věta 4.9 : Množina všech normálních podgrup grupy tvoří svaz, izomorfní svazu všech kongruencí.** *Důkaz: podle (4.8) - z (1.13) $[e]_\rho, \rho \in \mathcal{C}$ je norm. podgrupa $\Rightarrow$ (4.8(1)) OK, $\forall N \in \mathcal{N}$ : $\rho_N : (a,b) \in \rho_N \equiv^{def} a^{-1}b \in N$ je z (1.13) kongruence a $N = [e]_{\rho_N}$ $\Rightarrow$ (4.8(2)) OK, $[e]_\rho \subseteq [e]_\eta$ z (1.13) $\Rightarrow \rho \subseteq \eta \Rightarrow$ (4.8(3)) OK. $\varphi(\rho) = [e]_\rho$ je izomorfismus.*

# 5. Grupy

**Poznámka 5.1 : Je-li zobr. $f : G \to H$, kde $G,H$ jsou grupy, slučitelné s bin. operací, pak je homomorfismus.** *Důkaz: pro e: $f(e) = f(e \cdot e) = f(e) \cdot f(e)$. $f(e)^{-1}$ ex. (z def. grupy), zleva jím vynásobit. pro $^{-1}$: $e = f(e) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$, opačné symetricky, chová se jako inverz k $f(g)$.*

**Def.:** $H \leq G$, $a \in G$: **aH**$= \{a \cdot h, h \in H\}$, **Ha**$= \{h \cdot a, h \in H\}$, $\mathrm{rmod}_H$, $\mathrm{lmod}_H$ *jsou relace dané:* $(a,b) \in \mathrm{rmod}_H \equiv^{def} ab^{-1} \in H$, $(a,b) \in \mathrm{lmod}_H \equiv^{def} a^{-1}b \in H$.

**Poznámka 5.2 : Pro** $G(\cdot,^{-1},1)$**,** $H \leq G$ **a** $a,b \in G$ **platí: (1)** $\mathrm{rmod}_H$ **i** $\mathrm{lmod}_H$ **jsou ekvivalence. (2)** $(a,b) \in \mathrm{rmod}_H \Leftrightarrow (a^{-1},b^{-1}) \in \mathrm{lmod}_H$ **(pro norm. podgrupy** lmod **a** rmod **splývají a jsou navíc kongruence). (3)** $|G/\mathrm{rmod}_H| = |G/\mathrm{lmod}_H|$**, (4)** $[a]_{\mathrm{rmod}_H} = Ha$**,** $[a]_{\mathrm{lmod}_H} = aH$**, (5)** $|[a]_{\mathrm{rmod}_H}| = |[a]_{\mathrm{lmod}_H}| = |H|$**.** *Důkaz: (1) reflexivní z uzavřenosti H na e, symetrické z uz. H na* $^{-1}$*, tranzitivní z uz. H na* $\cdot$*, detail viz (1.13) pro norm. podgrupy. (2) přímo z def., symetrie* lmod*. (3) ex. bijekce z* $\mathrm{lmod}_H$ *do* $\mathrm{rmod}_H$*:* $f : G \to G : f(g) = f(g^{-1})$ *(involuce), proto mám bijekci* $g : G/\mathrm{rmod}_H \to G/\mathrm{lmod}_H$ : $g([a]_{\mathrm{rmod}_H}) = [a^{-1}]_{\mathrm{lmod}_H}$*. (4)* $[a_{\mathrm{rmod}_H}] = \{x \in G | \exists h \in H : h^{-1}a = x\} = Ha$*,* $\mathrm{lmod}_H$ *symetricky. (5) def. zobr.* $b : H \to Ha : b(h) = ha$*. zjevně na, prosté:* $h_1a = b(h_1) = b(h_2) = h_2a$*, vynásobit* $a^{-1}$ *zprava.*

**Def.:** $H \leq G(\cdot,^{-1},1)$. **index** $H$ *v* $G$ *je číslo* $[G:H] = |G/\mathrm{rmod}_H| = |G/\mathrm{lmod}_H|$.

**Věta 5.3 (Lagrange) : Je-li** $H \leq G(\cdot,^{-1},1)$**, pak** $|G| = [G:H] \cdot |H|$**.** *Důkaz:* $|G| = |\dot{\cup}\{A \mid A \in G/\mathrm{rmod}_H\}| = \sum_{A \in G/\mathrm{rmod}_H} |A|$*(5.2(5))*$= \sum_{A \in G/\mathrm{rmod}_H} |H| = |H| \cdot [G:H]$.

**Poznámka 5.4 (důsledek) : Velikost podgrupy dělí velikost konečné grupy.** *Důkaz: plyne z (5.3)*

**Poznámka 5.5 : Je-li** $\varphi : \mathbf{Z} \to G : \varphi_g(n) = g^n$**, kde** $g \in G(\cdot,^{-1},1)$**, pak** $\varphi$ **je grupový homomorfismus** $\mathbf{Z}(+,-,0)$ **a** $G(\cdot,^{-1},1)$**.** *Důkaz: Podle (5.1) slučitelnost* $s \cdot$ *stačí. Přímo, zvl. případy pro* $\varphi(m+n)$*, kde* $m,n \geq, < 0$

**Poznámka 5.6 (důsledek) : Nechť** $G(\cdot,^{-1},1)$ **je grupa,** $n,m \in \mathbf{Z}$**. Pak** $\forall g \in G$**: (1)** $(g^n)^{-1} = (g^{-1})^n = g^{-n}$**, (2)** $(g^n)^m = g^{nm}$**.** *Důkaz: (1) slučitelnost* $\varphi$ *s* $^{-1}$*, (2) pro kladná čísla z definice, záporná z ind. rozšíření.*

**Def.:** *Pro* $G(\cdot,^{-1},1), g \in G$ *je* $< g >=< \{g\} >$ *nejmenší podgrupa obs.* $g$*.* $G$ *je* **cyklická***, pokud* $\exists g \in G :< g >= G$.

**Poznámka 5.7 : (1) Pro každou** $H \leq \mathbf{Z}(+,-,0)$ **ex. číslo** $k$**, t.ž.** $k\mathbf{Z} = < k > = H$ **(**$\forall$ **podgrupa je cyklická). (2)** $\forall H \leq \mathbf{Z}_n(+,-,0)(n \in \mathbf{N})\ \exists k : \ k = 0$ **nebo** $k|n$**, t.ž.** $< k > = H$**.** *Důkaz:* $H = \{0\}$ *triv. příp., vezmu* $H \neq \{0\}$*.* $\exists k \in H, k > 0$*, vezmu nejmenší takové.* $< k > \subseteq H$*,* $a \in H$ *lib., vydělím* $a \div k$ *se zbytkem* $y = a + k \cdot (\cdot - x)$*.* $a \in H, k(-x) \in H \Rightarrow y \in H$*,* $y < k \Rightarrow \ y = 0, < k > = H$*. Pro (2) odlišnosti:* $a = (kx)\mathrm{mod}\ n + y\mathrm{mod}\ n$ *Nechť* $k \not| n$*:* $l := NSD(k,n)$*, ze zpětného chodu Euklidova alg.* $l = \alpha k + \beta n (\alpha, \beta \in \mathbf{Z})$*.* $l \bmod n = (\alpha k)\mathrm{mod}\ n \Rightarrow l \in < k > \Rightarrow l \in H$*, ale* $k$ *je minimální,* $l < k, NSD \geq 1$ *- spor.*

**Věta 5.8 : Nechť** $G(\cdot,^{-1},1)$ **je cyklická. (1) Je-li** $G$ **nekonečná, pak** $G \simeq \mathbf{Z}(+,-,0)$**. (2) Je-li** $n = |G|$ **konečné, pak** $G(\cdot,^{-1},1) \simeq \mathbf{Z}_n(+,-,0)$**.** *Důkaz: Nechť* $< g >= G$*, podle (5.5) je* $\varphi : \mathbf{Z} \to G : \varphi(z) = g^z$ *homomorfismus.* $\ker \varphi$ *je z (1.13) kongruence v* $\mathbf{Z} \Rightarrow$ *jednozn. korespondence s nějakou normální podgrupou* $H \leq \mathbf{Z}$*. Z (3.4)* $\mathbf{Z}/\ker \varphi \simeq G$*. z (5.7)* $\exists n \in Z, H = n\mathbf{Z}$ *(*$(a,b) \in \ker \varphi \Leftrightarrow (a-b) \in n\mathbf{Z}$*), pro* $n = 0$ $\ker \varphi = id$*, dostanu (1),* $n > 0$ *: z (5.5) dostanu izomorfismus* $\psi : \mathbf{Z} \to \mathbf{Z}_n$*, z (3.4)* $\mathbf{Z}_n \simeq \mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/\ker \varphi \simeq G$ *- dostanu (2).*

**Poznámka 5.9 (důsledek): Každá (1) podgrupa a (2) faktorová grupa cyklické grupy je cyklická.** *Důkaz: (1)* $G$ *z (5.8) a (5.7); (2) pro* $g, < g >= G$*:* $< [g]_\rho >= G/\rho$.

**Poznámka 5.10 (důsledek): Nechť** $G(\cdot,^{-1},1)$ **je konečná cyklická grupa a** $k||G|$**, pak** $\exists! H \leq G$**, t.ž.** $|H| = k$**.** *Důkaz:* $k = 1 \Rightarrow H = \{0\}$*,* $k > 1 : H =< \frac{n}{k} >= \{0, \frac{n}{k}, \frac{2n}{k}, ... \frac{(k-1)n}{k}\}$*. Jednoznačnost:* $|K| = k, \exists a : K =< a > K \simeq \mathbf{Z}_k (1 \leftrightarrow a, x \leftrightarrow (ax)\mathrm{mod}\ n)$*.* $\exists b \in Z : ka = bn$*,* $a = b(\frac{n}{k}) \ \Rightarrow$ *a leží v* $< k >$*.* $K$ $a < k >$ *jsou 2 stejně velké konečné mn. - ex. izomorfismus.*

**Poznámka 5.11 : Nechť** $G(\cdot,^{-1},1)$ **je konečná grupa, Pak** $\forall g \in G : g^{|G|} = 1$**.** *Důkaz:* $g^k = 1$*, kde* $k = | < g > |$ *(z izomorf. s* $\mathbf{Z}_k$*), podle (5.4)* $k \mid |G|$*,* $g^{|G|} =$*(5.6),(5.4)* $(g^k)^{\frac{|G|}{k}} = 1^{\frac{|G|}{k}} = 1$.

**Poznámka 5.12 : (1) Nechť** $n \in \mathbf{N}, a \in \mathbf{Z}_n$**,** $k = NSD(a,n)$**, Pak** $a\mathbf{Z}_n = k\mathbf{Z}_n$**. (2)** $a\mathbf{Z}_n = \mathbf{Z}_n \ \Leftrightarrow NSD(a,n) = 1$**.** *Důkaz: (1)* $k = (ax) + ny = (ax)\mathrm{mod}\ n$*,* $k|a \Rightarrow \exists \mu : (k\mu)\mathrm{mod}\ n = a \Rightarrow a \in < k >$*. (2) " ⇐ " plyne z (1) pro* $k = 1$*. " ⇒ ":* $\exists x, y : ax + ny = 1$*,* $c|a, c|n \Rightarrow c|1$*, tj.* $NSD(a,n) = 1$.

**Def.:** *Zobrazení* $\varphi : \mathbf{N} \to \mathbf{N}$*:* $\varphi(n) = |\{k, 0 < k < n : NSD(k,n) = 1\}|$ *je* **Eulerova funkce**.

**Poznámka 5.13 :** $\varphi(n) = |\{k \in \mathbf{Z}_n \mid \exists x : x \cdot k = 1\}|$**, z (5.12(2))** $= |\{k \in \mathbf{Z}_n \mid < k >= \mathbf{Z}_n\}|$ $= |\{$**invertibilní prvky monoidu** $\mathbf{Z}_n\}|$**.** *Důkaz: (5.12(2)), z def.*

**Věta 5.14 (Malá Fermatova) :** $\forall a < n, NSD(a,n) = 1$ **platí:** $(a^{\varphi(n)}) \bmod n = 1$**.** *Důkaz:* $a \in Z_n^*(\cdot, 1)$*,* $Z_n^*$ *je podle (1.11) grupa, podle (5.13)* $|Z_n^*| = \varphi(n)$*, z (5.11) platí.*

**Poznámka 5.15 : (1)** $\varphi(p^n) = (p-1)p^{n-1}$ **pro** $p$ **prvočíslo a** $n \in \mathbf{N}$**. (2)** $\varphi(n \cdot m) = \varphi(m) \cdot \varphi(n)$ **pro** $n, m \in \mathbf{N}, NSD(n,m) = 1$**.** *Důkaz: (1)* $\varphi(p^n) = (p^n - 1) - |\{0 < k < p^n \mid NSD(k, p^n) > 1\}|$*. (2) na* $\mathbf{Z}_n \times \mathbf{Z}_m$ *definovat násobení, dostanu "součinový" monoid.* $f : \mathbf{Z}_{mn} \to \mathbf{Z}_n \times \mathbf{Z}_m : f(k) = (k \bmod n, k \bmod m)$ *je homomorfismus (přímo ověřit slučitelnost s* " $\cdot$ ", $1$*), je prosté (*$f(k) = f(l), k \leq l$ *-* $k \bmod n = l \bmod n, k \bmod m = l \bmod m$*, z nesoudělnosti* $n, m$ $l = k$*). je i na (2 stejně velké konečné mn.)* $\Rightarrow$ *je izomorfismus.* $(a,b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ *je invertibilní* $\Leftrightarrow$ $a, b$ *jsou invertibilní v* $\mathbf{Z}_{nm}$*.* $\varphi(nm) =$*(z 5.13)*$|\mathbf{Z}_{nm}^*| = |(\mathbf{Z}_n \times \mathbf{Z}_m)^*| = |\mathbf{Z}_n^* \times \mathbf{Z}_m^*| = |\mathbf{Z}_n^*| \cdot |\mathbf{Z}_m^*| =$*(5.13)*$\varphi(n) \cdot \varphi(m)$*.*

**Věta 5.16 : Je-li** $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_l^{k_l}$ **prvočíselný rozklad čísla** $n$**, t.j** $p_i$ **jsou prvočísla,** $p_i \neq p_j$ $i \neq j, k_i \geq 1$**, pak** $\varphi(n) = \Pi_{i=1}^{l}(p_i - 1)p_i^{k_i - 1}$**.** *Důkaz: indukcí z (5.15(2)), úprava výrazu podle (5.15(1))*

**Věta 5.17 : Nechť** $T$ **je těleso s operacemi** $+, \cdot$**.** $(T - \{0\})(\cdot, ^{-1}, 1)$ **je komutativní grupa (z lin. algebry). Nechť** $G$ **je konečná podgrupa** $(T - \{0\})(\cdot, ^{-1}, 1)$**. Pak je** $G$ **cyklická.** *Důkaz: bez důkazu.*

# 6. Okruhy

**Def.:** *Nechť* $R(+, \cdot, -, 0, 1)$ *je algebra, t.ž.* $R(+, -, 0)$ *tvoří komutativní grupu,* $R(\cdot, 1)$ *je monoid a platí* $a(b + c) = ab + ac$ $a$ $(a + b)c = ac + bc$ $\forall a, b \in R$*. Pak je* $R$ **okruh**.

**Poznámka 6.1 : Pro každé 2 prvky** $a, b \in R(+, \cdot, -, 0, 1)$ **platí: (1)** $0a = a0 = 0$**, (2)** $(-a)b = a(-b) = -(ab)$**, (3)** $(-a)(-b) = ab$**, (4)** $|R| > 1 \Leftrightarrow 0 \neq 1$ *Důkaz: (1), (2), (3) z lin. algebry, jednoduchými triky; (4)* " $\Leftarrow$ " *triviální, mám 2 prvky;* " $\Rightarrow$ " *obměnou* $0 = 1 \Rightarrow \forall a \in R : a = 1a = 0a = 0$*.*

**Def.:** *Nechť* $R(+, \cdot, -, 0, 1)$ *je okruh a* $I \subseteq R$*. Pak* $I$ *je* **pravý(levý) ideál**, *pokud* $I \leq R(+, -, 0)$ *(je i normální, protože* $R$ *je komutativní) a* $\forall i \in I, r \in R : i \cdot r \in I$ *(levý* $r \cdot i \in I$*) (důsledek: uzavřenost* $I$ *na násobení).* $I$ *je* **ideál**, *pokud je pravý a zároveň levý ideál.*

**Def.:** *Ideál je* **netriviální**, *pokud* $I \neq \{0\}$ *a* $I \neq R$ *.*

**Věta 6.2 : Buď** $R(+, \cdot, -, 0, 1)$ **okruh. Pak zobrazení, které kongruenci** $\rho$ **na okruhu** $R$ **přiřadí** $[0]_\rho$ **je izomorfismus svazu všech kongruencí a svazu všech ideálů (tj.** $[0]_\rho$ **je ideál). Navíc** $(a,b) \in \rho \Leftrightarrow a + (-b) \in [0]_\rho$**.** *Důkaz: z (4.8), předp. (4.8(1)) -* $\rho$ *je kongruence i na* $R(+, -, 0)$*,* $[0]_\rho$ *je norm. podgrupa (z (1.13),(4.9)), ověřit* $\forall i \in [0]_\rho$*,* $\forall r \in R : ir \in [0]_\rho, ri \in [0]_\rho$ *- z* $(i, 0) \in \rho, (r, r) \in \rho$*,* $\rho$ *sluč. s* " $\cdot$ "*. (4.8(2)) z 1.13* $\rho$ *kongruence na* $R(+, -, 0)$*, dokázat slučitelnost s* " $\cdot$ "$, 1$ *-* "$1$" *z reflexivity;* " $\cdot$ " $: (a_1, a_2) \in \rho$*,* $(b_1, b_2) \in \rho$*,* $(a_1 - a_2)b_1 \in I$*,* $a_2(b_1 - b_2) \in I \Rightarrow (a_1b_1) - (a_2b_2) = (a_1 - a_2)b_1 + a_2(b_1 - b_2) \in I$*. (4.8(3))* $\rho, \eta : [0]_\rho \subseteq [0]_\eta \Rightarrow \rho \subseteq \eta$ *- platí i pro systém kongruencí na* $R(+, -, 0)$ *z (4.9), ten je větší* $\Rightarrow$ *platí.*