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 na A, pak $A(\alpha_i | i \in I)$ je* **algebra**.
Def.: *mn. B je* **uzavřená** *na operaci α, 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 α, 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. ($\forall \alpha, a_1, ..a_n \in A : f(\alpha_A(a_1, ..a_n)) = \alpha_B(f(a_1), ..f(a_n))$)*

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

Poznámka ★ 1.3 : Nechť $f : A \to B$ je homomorfismus, nechť C je podalgebra 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 lib.operaci ověřit uzavřenost, z def. homomorfismu, def. podalgebry.*

Def.: *Bijektivní homomorfismus je* **izomorfismus***(mezi množinami můžeme bez ztráty jakékoliv informace přecházet), algebry stejného typu jsou* **izomorfní**, *$\exists$-li mezi nimi aspoň 1 izomorfismus.*
Def.: Relace *na množině A je lib. podmnožina $\rho \subseteq A \times A$. $(a, b) \in \rho \overset{\text{def}}{\equiv} a \rho b$,*
$\rho^{-1} = \{(a, b) | (b, a) \in \rho\}$ - **opačná relace**, *$\rho^+ = \{(a, c) | \exists a = b_0, ..b_n = c \in A; (b_i, b_{i+1}) \in \rho\}$ -* **tranzitivní obal**, *$id = \{(a, a) | a \in A\}$ -* **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.: *$f : A \to B$,* $\ker f : (a_1, a_2) \in \ker f \overset{\text{def}}{\equiv} f(a_1) = f(a_2)$ *je* **jádro** *zobr. f.*
Def.: **přirozená projekce** *mn. A podle ρ je $\pi_\rho : A \to A/\rho$, t.ž. $\pi_\rho(a) = [a]_\rho$.*

Poznámka ★ 1.4 : *$f : A \to B$* **zobr.,** *ρ* **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) z def.* $\ker f$ *se dostane z ekvivalence " = ", (2),(3) z def., (4) ($\Rightarrow$) vezmu $(a_1, a_2) \in \rho$, potom $f(a_1) = f(a_2)$, tedy $(a_1, a_2) \in \ \ker f$. ($\Leftarrow$) $a_1 \rho a_2 \overset{\rho \subseteq \ker f}{\Rightarrow} f(a_1) = f(a_2) \Rightarrow g([a_1]_\rho) = g([a_2]_\rho)$, tedy g je korektně definované.*

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

Poznámka ★ 1.5 : (1) Nechť $\rho \subseteq \sigma$ jsou ekvivalence na A. Pak σ/ρ je ekvivalence na A. (2) Nechť η je ekvivalence na A/ρ, pak ex. právě 1 ekvivalence σ na A, t.ž. $\rho \subseteq \sigma$ a $\sigma/\rho = \eta$. *Důkaz: (1) dokázat korektnost definice σ/ρ - ($[a_1]_\rho = [a_2]_\rho, [b_1]_\rho = [b_2]_\rho$, $(a_1, b_1) \in \sigma) \Rightarrow$ (z tranzitivity σ) $(a_2, b_2) \in \sigma$. důkaz ekvivalence - přímo. (2) σ najdu podle předpisu $([a]_\rho, [b]_\rho) \in \eta \Leftrightarrow (a, b) \in \sigma$, $\sigma \subset \rho$, σ je ekvivalence (z ekvivalence η) $\Rightarrow$ ex. faktor-ekvivalence.*

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 1.4(1), slučitelnost přímo z homomorfismu f*

Def.: *Relace* ρ **slučitelná s** α*, pak* α *na* A/ρ *def.:* $\alpha([a_1]_\rho, ...[a_n]_\rho) = [\alpha(a_1, ...a_n)]_\rho$*. Kongruence* ρ *na* A*, pak stejným způsobem def. na* A/ρ *strukturu algebry.*

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

Poznámka ★ 1.8 : Nechť ρ **je kongruence na** A **a** σ **ekvivalence na** A**,** $\rho \subseteq \sigma$**. Pak** σ **je kongruence na** $A \Leftrightarrow \sigma/\rho$ **je kongruence na** A/ρ**.** *Důkaz:* $(\Rightarrow)$ *- z 1.5 plyne ekvivalence* σ/ρ*, dokázat slučitelnost s lib. operací* $\alpha([a_1]_\rho, ...[a_n]_\rho) = [\alpha(a_1, ...a_n)]_\rho$ *- ze sluč.* σ*.* $(\Leftarrow)$ *dokázat slučitelnost - to samé naopak.*

Poznámka ★ 1.9 (Věta o homomorfismu) : Nechť $f : A \to B$ **je homomorfismus algeber stejného typu a** ρ **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 1.4(4),* $(\Leftarrow)$ *zobr.* $g : g([a_i]_\rho) = f(a_i)$ *je dobře definované podle 1.4(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 ★ 1.10 (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. 1.9 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 ★ 1.11 (2. věta o izomorfismu) : Nechť $\rho \subseteq \eta$ **jsou kongruence na algebře** A**. Pak** ${}^{(A/\rho)}/_{(\eta/\rho)}$ **je izomorfní** ${}^{A}/_{\eta}$**.** *Důkaz: z 1.9 (pro* $f = \pi_\eta$*)* $\exists$ *homomorfismus* $g : A/\rho \to A/\eta : g([a]_\rho) = [a]_\eta$*. g je (z def.) na, z 1.10 (pro g):* $A/\eta \simeq {}^{(A/\rho)}/_{\ker g}$*. z def. g* $\ker g = \eta/\rho$*.*

2 Algebry s jednou binární operací

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

Poznámka ★ 2.1 : Každý grupoid odsahuje nevýš 1 neutrální prvek. *Důkaz: mějme* e, f *dva neutr.prvky pak:* $e = e.f = f$

Poznámka 2.2 : $M(., e)$ **monoid,** $a, b, c \in M$**. Pokud** $(a.b = e)$ & $(b.c = e)$**, pak** $a = c$ *Důkaz:* $a = ae = a(bc) = (ab)c = ec = c$*.*

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

Poznámka ★ 2.3 : Buď $M(., e)$ **monoid, pak** $M^* = \{m \in M | \exists m^{-1}\}$ **je jeho podmonoid. Každý inverzní prvek je invertibilní.** *Důkaz: uzavřenost na* $e \in M^*$ *;* $\cdot$ *pro součin 2 prvků z* M^* *ex. inv. prvek; inverz k inverzu je pův. prvek z def.*

Def.: *Algebra* $G(\cdot, ^{-1}, e)$ *je* **grupa***, pokud je* $G(\cdot, e)$ *monoid a* $^{-1}$ *je operace inv. prvku.*
Def.: Normální podgrupa *je každá podgrupa* H *grupy* G *kde* $\forall g \in G \ \forall h \in H : g.h.g^{-1} \in H$*.*
G *je* **komutativní (abelovská)***, pokud je* $\cdot$ *komutativní.*

Poznámka ★ 2.4 : $M(\cdot, e)$ **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 2.3 je možné* $\cdot$ *omezit na* M^**,* M^* *je podmonoid* $M(\cdot, e)$ *z def. je grupa.*

Poznámka 2.5 : Každá podgrupa komutativní grupy je normální. *Důkaz:* H *podgrupa* G *komutativní,* $g \in G\ h \in H : g.h.g^{-1} = g.g^{-1}.h = 1.h = h \in H$*.*

Věta 2.6 : Nechť $G(\cdot, ^{-1}, e)$ **je grupa a** ρ **relace na** G**. Pak** ρ **je kongruence** $\Leftrightarrow [e]_\rho$ **je normální podgrupa** G **a** $(g, h) \in \rho$ **právě když** $g^{-1}.h \in [e]_\rho$**.** *Důkaz:* " $\Rightarrow$ " : ρ *kongruence - ověřit uz. na e (z refl.), uz. na* $^{-1}$*:* $(e, h) \in \rho \Rightarrow (e^{-1}(= e), h^{-1}) \in \rho$*; uz. na* $\cdot$*:* $(e, g), (e, h) \in \rho \Rightarrow (e.e, g.h) \in \rho$*; 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.* $\rho : (g, h) \in \rho \overset{\text{def}}{\equiv} g^{-1}.h \in H$*, dokázat že* ρ *je ekvivalence (přímo),* $[e]_\rho = H$ *(přímo), slučitelnost s operacemi - e platí* $\forall$ *refl. relaci,* $^{-1} : g^{-1}h \in H \Rightarrow h^{-1}g \in H \Rightarrow h(h^{-1}g)h \in H$*,* $\cdot : \bar{h}\bar{g}^{-1} \in H(= \bar{g}(\bar{g}^{-1}\bar{h})\bar{g}^{-1})$*;* $\bar{g}^{-1} \cdot (g^{-1} \cdot h.\bar{h}.\bar{g}^{-1}).\bar{g} = (g\bar{g})^{-1}(h\bar{h}) \in H$*.*

Def.: G/H $= G/\rho_h$*, kde* ρ_h *je kongruence odp. dle 2.6 normální podgrupě* H*.*

3 Uzávěrové systémy na algebře

Def.: *A množina,* $\mathcal{C} \subseteq \mathcal{P}(\mathcal{A})$*.* $\mathcal{C}$ *je* **uzávěrový systém***, pokud* **(1)** $A \in \mathcal{C}$ **(2)** $\{B_i | i \in I\} \subseteq \mathcal{C} \Rightarrow \cap_{i\in I} B_i \in \mathcal{C}$**.**
Def.: Uzávěr *je zobrazení* $cl_\mathcal{C} : \mathcal{P}(A) \to \mathcal{C}$ *definované* $cl_\mathcal{C}(B) = \cap_{C\in\mathcal{C}, B\subseteq C} C$
Def.: *Zobrazení* $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ *je* **uzávěrový operátor***, pokud* **(1)** $B \subseteq \alpha(B)\ \forall B \in \mathcal{P}(A)$ **(2)** $\alpha(\alpha(B)) = \alpha(B)\ \forall B \in \mathcal{P}(A)$ **(3)** $\alpha(B) \subseteq \alpha(C)\ \forall B \subseteq C \subseteq A$**.**

Poznámka 3.1 : Systém všech podalgeber algebry A tvoří uzávěrový systém. *Důkaz: z 1.1 - průnik podalgeber je podalgebra - vyhovuje*

Věta ★ 3.2 : (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* α*, 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 ★ 3.3 : Množina 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 3.4 : 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 3.2(1),* $cl_\mathcal{B}(D) \subseteq cl_\mathcal{A}(D)$ *rozepsat jako průniky množin, z teorie množin jako 3.2(1)-3.*

Poznámka 3.5 : 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* ρ_i *je refl. - OK, symetrická a tranzitivní podobně, ekvivalence z 3.3 a průniku předch.*

Poznámka 3.5 : 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 : Nechť ρ je relace na A Je-li reflexivní(symetrická), pak ρ^+ a $\rho \cup \rho^{-1}$ je taky reflexivní(symetrická). *Důkaz: přímo.*

Poznámka 3.6 : Nechť ρ je relace, pak $((\rho \cup id) \cup (\rho \cup id)^{-1})^+ = (\rho \cup \rho^{-1} \cup id)^+$ je nejmenší ekvivalence obs. ρ (uzávěr ρ v uz. systému ekvivalencí). *Důkaz: ekvivalence z předchozí pozn., 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.*

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)** *množiny 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)*
Def.: *$\forall a, b \in A$ označme bin.operace* **spojení** $m \vee n = \sup_{\leq}(\{m, n\})$ *a* **průsek** $m \wedge n = \inf_{\leq}(\{m, n\})$

Poznámka ★ 4.1 : Buď $A(\wedge, \vee)$ svaz 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) {a,b}={b,a}, (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: $a \leq b \overset{\text{def}}{\equiv} (a \vee b = b)$. 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: $\subseteq$ je zjevně uspořádání. $\bigcap \mathcal{B} \in \mathcal{C}$, $\bigcap \mathcal{B} \subseteq B\ \forall B \in \mathcal{B}$, $X \subseteq B\ \forall B \in \mathcal{B} \Rightarrow X \subseteq \bigcap \mathcal{B}$. $\forall B \in \mathcal{B}\quad B \subseteq \bigcup \mathcal{B} \subseteq_{\mathcal{C}} (\bigcup \mathcal{B}) \in \mathcal{C}$.*

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

Def.: *Nechť $S(\wedge, \vee)$ je svaz, potom a* **pokrývá** *b ($b < \cdot a$), pokud $a, b, c \in S:\ b \leq a,\ b \neq a$, $b \leq c \leq a \Rightarrow b = c$ nebo $a = c$.*
Def.: **Hasseův diagram** *svazu je graf s vrcholy z S, mezi a, b bude hrana že a bude* **pod** *b,*

pokud $a < \cdot b$.

Poznámka ★ 4.5 (slabá modularita) : 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.: $S(\wedge,\vee)$ *je* **distributivní***, pokud* $\forall a,b,c \in S : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Poznámka ★ 4.6 : $S(\wedge,\vee)$ **distributivní ⇔ pokud je opačný** $S(\vee,\wedge)$ **distributivní** *Důkaz:* $(\Rightarrow)$ $(a\wedge b)\vee(a\wedge c) = ((a\wedge b))\wedge((a\wedge b)) = a\wedge((a\wedge b)) = a\wedge((a\vee c)\wedge(b\vee c)) = (a\wedge(a\vee c))\wedge(b\vee c) = a \wedge (b \vee c)$. $(\Leftarrow)$ *to samé opačně*

Poznámka ★ 4.7 : Každý distributivní svaz je modulární *Důkaz:* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \overset{a\leq c}{=} (a \vee b) \wedge c$

Věta 4.8 : $S(\wedge,\vee)$ **modulární ⇔ obsahuje podsvaz pentagon** *Důkaz: dokážeme že pentagon není modulární, S pokud je modulární nemůže obsahovat podsvaz izomorfní s pentagonem, pokud S není modulární...*

Def.: *Nechť* $0 \in S$ $(1 \in S)$ *je nejmenší(největší) prvek S, potom a nazveme* **atom(koatom)** *svazu S, jestliže* $0 < \cdot a$ $(a < \cdot 1)$. **Komplement** $a' \in S$ *k* $a \in S$ *je def.* $a \vee a' = 1$ *a* $a \wedge a' = 0$

Poznámka 4.9 : Každý prvek distr. svazu má nejvýše 1 komplement *Důkaz: b,c komplementy a. Pak* $b = b \wedge 1 = b \wedge (a \vee b \wedge a) \vee (b \wedge c) = b \wedge c$. *Tudíž* $b \geq c$. *Obdobně dostaneme* $b \leq c$, *a tedy* $b = c$.

Def.: Booleovou algebrou *nazveme* $S(\vee,\wedge,0,1,')$, *že* $S(\wedge,\vee)$ *je distributivní svaz s nejv. prvkem* 1 *a nejm.* 0 *a unární operace* $'$ *která přiřadí každému prvku komplement*

Poznámka 4.10 : $S(\vee,\wedge,0,1,')$ **je Booleova algebra,** $\forall a,b \in S$ **platí: (1)** $(a')' = a$**, (2)** $(a \vee b)' = a' \wedge b'$**, (3)** $(a \wedge b)' = a' \vee b'$**, (4)** $(1)' = 0$ $(0)' = 1$ *Důkaz: (1) podle 4.9 (2)(3)* $(a\wedge b)\vee(a'\vee b') = (a\vee a'\vee b')\wedge(b\vee a'\vee b') = 1\wedge 1 = 1.(a\wedge b)\wedge(a'\vee b') = (a\wedge b\wedge a')\vee(a\wedge b\wedge b') = 0\vee 0 = 0$

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).*

Věta ★ 4.11 : $S(\vee,\wedge,0,1,')$ **je konečná Booleova algebra a A je množina všech atomů svazu S. Potom** $\varphi : P(A) \to S$ **dané** $\varphi(A) = \vee_B$ **je izomorfismus bool. algeber** $S(\vee,\wedge,0,1,')$ **a** $P(A)(\cup,\cap,\emptyset,X,')$ *Důkaz: TODO (15.2)*

Poznámka ★ 4.12 : Homomorfismus svazů je monotónní. *Důkaz:* $a \leq b$ *⇒(4.2)* $b = a \vee b \Rightarrow f(b) = f(a \vee b) = f(a) \vee f(b)\ \Rightarrow\ f(a) \leq f(b)$.

Věta ★ 4.13 : Bijekce svazů f **je izomorfismus ⇔** f **i** f^{-1} **jsou monotónní.** *Důkaz:* $(\Rightarrow)$ *zřejmé (4.12);* $(\Leftarrow)$ *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 ★ 4.14 : 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;* φ *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 φ^{-1} monotónní, $\rho \subseteq \eta : \varphi(\rho) = [e]_\rho \subseteq [e]_\eta = \varphi(\eta)$ - φ 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 (4.13).

Věta ★ 4.15 : Množina všech normálních podgrup grupy tvoří svaz, izomorfní svazu všech kongruencí. *Důkaz: podle (4.14) - z (2.6) $[e]_\rho, \rho \in \mathcal{C}$ je norm. podgrupa $\Rightarrow$ (4.14(1)) OK, $\forall N \in \mathcal{N} : \rho_N : (a,b) \in \rho_N \overset{\text{def}}{\equiv} a^{-1}b \in N$ je z (2.6) kongruence a $N = [e]_{\rho_N} \Rightarrow$ (4.14(2)) OK, $[e]_\rho \subseteq [e]_\eta$ z (2.6) $\Rightarrow \rho \subseteq \eta \Rightarrow$ (4.14(3)) OK. $\varphi(\rho) = [e]_\rho$ je izomorfismus.*

Def.: *Nechť A a B jsou množiny. Dvojici zobrazeni $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ se říka* **Galoisova korespondence**, *jsou-li $\forall A_1, A_2 \in \mathcal{P}(A)$ a $\forall B_1, B_2 \in \mathcal{P}(B)$ splněny následující podmínky: **(1)** $A_1 \subseteq A_2 \Rightarrow \alpha(A_2) \subseteq \alpha(A_1)$ a $B_1 \subseteq B_2 \Rightarrow \beta(B2) \subseteq \beta(B1)$, **(2)** $A_1 \subseteq \beta\alpha(A_1)$ a $B_1 \subseteq \alpha\beta(B1)$.*

Věta ★ 4.16 : Buď $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ Galoisova korespondence. Potom jsou zobrazení $\beta\alpha$ a $\alpha\beta$ uzávěrové operátory. Označme A a B uzávěrové systémy příslušné uzávěrovým operátorům $\beta\alpha$ a $\alpha\beta$. Pak $\alpha(A) \subseteq B$ a $\beta(B) \subseteq A$. Označíme-li $\alpha' : A \to B$ a $\beta' : B \to A$ příslušné restrikce zobrazení α a β, pak α' a β' jsou bijekce a $\alpha' = (\beta')^{-1}$. Navíc $\forall A_1, A_2 \in A$ a $\forall B_1, B_2 \in B$ platí, že $A_1 \subseteq A_2 \Leftrightarrow \alpha(A_2) \subseteq \alpha(A_1)$ a $B_1 \subseteq B_2 \Leftrightarrow \beta(B_2) \subseteq \beta(B_1)$. *Důkaz: Z $A_1 \subseteq A_2 \subseteq A$ podle **(1)** dostáváme $\alpha(A_1) \supseteq \alpha(A_2)$, a opět podle **(1)** $\beta\alpha(A_1) \subseteq \beta\alpha(A_2)$. Podle 4.14 je $\beta\alpha\beta\alpha(A_1) = \beta\alpha(A_1)$. Dokázali jsme, že $\beta\alpha$ je uzávěrový operátor. Podobně je i $\alpha\beta$ uzávěrový operátor. Je-li $A_1 \subseteq A$, je $\alpha\beta\alpha(A_1) = \alpha(A_1)$, a tudíž $\alpha(A_1) \in \mathcal{B}$. Podobně $\beta(B_1) \in \mathcal{A}$ pro $B_1 \subseteq B$. Pro $A_1 \in \mathcal{A}$ je $\beta\alpha(A_1) = A_1$ a pro $B_1 \in \mathcal{B}$ je $\alpha\beta(B_1) = B_1$, takže α' a β' jsou vzájemně inverzní. Jsou-li $A_1, A_2 \in \mathcal{A}$, tak z $A_1 \subseteq A_2$ plyne $\alpha(A_1) \supseteq \alpha(A_2)$ podle **(1)**. Platí-li $\alpha(A_1) \supseteq \alpha(A_2)$, tak $A_1 = \beta\alpha(A_1) \subseteq \beta\alpha(A_2) = A_2$.*

5 Grupy

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

Def.: $H, K \subseteq G(\cdot, ^{-1}, 1)$, $g \in G$: $\mathbf{HK} = \{h.k |\ h \in H\, k \in K\}$, $\mathbf{gH} = \{g\}H$, $\mathbf{Hg} = H\{g\}$
H podgrupa G, pak def. relace: $(a,b) \in \mathbf{rmod_H} \overset{\text{def}}{\equiv} ab^{-1} \in H$, $(a,b) \in \mathbf{lmod_H} \overset{\text{def}}{\equiv} a^{-1}b \in H$.

Poznámka ★ 5.2 : Pro $G(\cdot, ^{-1}, 1)$, H podgrupa G a $a, b \in G$ platí: (1) rmod_H **i** 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 (2.6) pro norm. podgrupy. (2) přímo z def., symetrie* lmod. *(3) ex. bijekce z lmod_H do 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) $[a_{\mathrm{rmod}_H}] = \{x \in G | \exists h \in H : h^{-1}a = x\} = Ha$, lmod_H symetricky. (5) def. zobr. $b : H \to Ha : b(h) = ha$. zjevně na, prosté: $h_1 a = b(h_1) = b(h_2) = h_2 a$, vynásobit a^{-1} zprava.*

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

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 - |H|/|G|. *Důkaz: plyne z (5.3)*

Def.: *Grupa* $G(\cdot,^{-1},1)$ *a* $a \in G$. *Definujme* **indukci***:* $a^0 = 1$, $a^n = a^{n-1}.a\ \forall n > 0$, $a^n = (a^{-1})^{-n}.a\ \forall n < 0$,

Poznámka 5.5 : Je-li $\varphi : \mathbf{Z} \to G : \varphi_g(n) = g^n$**, kde** $g \in G(\cdot,^{-1},1)$**, pak** φ **je grupový homomorfismus** $\mathbf{Z}(+,-,0)$ **do** $G(\cdot,^{-1},1)$ **a** $\varphi(\mathbb{Z}) = \{g^z | z \in \mathbb{Z}\} = \langle g \rangle$**.** *Důkaz: Podle (5.1) slučitelnost* $s \cdot$ *stačí. Přímo, zvl. případy pro* $\varphi(m+n)$*, kde* $m, n \geq, < 0$*. Podle 1.3* $\varphi(\mathbb{Z})$ *je podgrupa* G*,* $g = g^{-1}$*,* $\forall$ *podgrupa s* g *obsahuje* $g \cdot ..g$ *a* $g^{-1} \cdot ..g^{-1}$ *(obojí k-krát)* $\forall k \in \mathbb{N}$*, tedy* $\varphi(\mathbb{Z}) = \langle g \rangle$*.*

Def.: *Pro* $G(\cdot,^{-1},1), g \in G$ *je* $\langle g \rangle = \langle \{g\} \rangle$ *nejmenší podgrupa obs. prvek* g*.*
G *je* **cyklická***, pokud* $\exists g \in G : \langle g \rangle = G$**. Řád prvku** *cyklické grupy je nejmenší mocnina daného prvku, že výsledkem je neutrální prvek.*

Poznámka 5.6 : (1) $\forall H$ **podrupa** $\mathbf{Z}(+,-,0)$ $\exists k \geq 0, k \in \mathbf{Z}$ **t.ž.** $k\mathbf{Z} = \langle k \rangle = H$ **(**$\forall$ **podgrupa je cyklická). (2)** $\forall H$ **podrupa** $\mathbf{Z_n}(+,-,0)(n \in \mathbf{N})$ $\exists k : k = 0$ **nebo** $k|n$**, t.ž.** $k\mathbf{Z_n} = \langle k \rangle = H$**.** *Důkaz:* $H = \{0\}$ *triv. příp., vezmu* $H \neq \{0\}$*.* $\exists k \in H, k > 0$*, vezmu nejmenší takové.* $\langle k \rangle \subseteq H$*,* $a \in H$ *lib., vydělím* $a \div k$ *se zbytkem* $y = a + k \cdot (. - x)$*.* $a \in H, k(-x) \in H \Rightarrow y \in H$*,* $y < k \Rightarrow y = 0, \langle k \rangle = H$*. 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.* $l = \alpha k + \beta n (\alpha, \beta \in \mathbf{Z})$*.* $l \bmod n = (\alpha k) \mathrm{mod}\ n$ $\Rightarrow l \in \langle k \rangle \Rightarrow l \in H$*, ale* k *je minimální,* $l < k, NSD \geq 1$ *- spor.*

Věta ★ 5.7 : 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* $\langle g \rangle = G$*, podle (5.5) je* $\varphi : \mathbf{Z} \to G : \varphi(z) = g^z$ *homomorfismus.* $\ker \varphi$ *je z (2.6) kongruence v* $\mathbf{Z} \Rightarrow$ *jednozn. korespondence s nějakou normální podgrupou* $H \leq \mathbf{Z}$*. Z (1.10)* $\mathbf{Z}/\ker \varphi \simeq G$*. 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 ★ 5.8 (důsledek): Každá (1) podgrupa a (2) faktorová grupa cyklické grupy je cyklická. *Důkaz: (1) G z (5.7) a (5.6); (2) pro* $g, \langle g \rangle = G$*:* $\langle [g]_\rho \rangle = G/\rho$*.*

Poznámka ★ 5.9 : Nechť $G(\cdot,^{-1},1)$ **je konečná grupa, Pak** $\forall g \in G : g^{|G|} = 1$**.** *Důkaz:* $g^k = 1$*, kde* $k = |\langle g \rangle|$ *(z izomorf. s* $\mathbf{Z}_k$*), podle (5.4)* $k \mid |G|$*,* $g^{|G|} =$*(důsledek 5.5),(5.4)* $(g^k)^{\frac{|G|}{k}} = 1^{\frac{|G|}{k}} = 1$*.*

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

Poznámka 5.11 : (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)* $k = (ax) + ny = (ax) \mathrm{mod}\ n$*,* $k|a \Rightarrow \exists \mu : (k\mu) \mathrm{mod}\ n = a \Rightarrow a \in \langle k \rangle$*. (2)* $(\Leftarrow)$ *plyne z (1) pro* $k = 1$*.* $(\Rightarrow)$*:* $\exists x, y : ax + ny = 1$*,* $c|a, c|n \Rightarrow c|1$*, 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** *(určuje počet všech nesoudělných čísel menších než dané číslo).*

Poznámka ★ 5.12 : $\varphi(n) = |\{k \in \mathbf{Z}_n \mid \exists x : x.k = 1\}|$**, z (5.11(2))** $= |\{k \in \mathbf{Z}_n \mid \langle k \rangle = \mathbf{Z}_n\}|$ $= |\{$**invertibilní prvky monoidu** $\mathbf{Z}_n\}|$**.** *Důkaz: (5.11(2)), z def.*

Věta ★ 5.13 (Malá Fermatova) : $\forall a < n, NSD(a,n) = 1$ **platí:** $(a^{\varphi(n)})\text{mod } n = 1$**.** *Důkaz:* $a \in Z_n^*(\cdot, 1)$, Z_n^* *je podle (2.4) grupa, podle (5.12)* $|Z_n^*| = \varphi(n)$, *z (5.9) platí.*

Def.: *Nechť* $A_j(\alpha_i | i \in I)$ *jsou algebry stejného typu pro* $j = 1, \ldots, k$. *Na* $\Pi_{j=1}^k A_j$ *definujme* **strukturu algebry stejného typu na součinu**.
Je-li α_i *n-ární operace, definuji* $\alpha_i : (\Pi A_j)^n \to \Pi A_j$ $\alpha_i((a_{11}, \ldots, a_{1k}), \ldots, (a_{n1}, \ldots, a_{nk})) = (\alpha_i(a_{11}, a_{21}, \ldots, a_{n1}), \ldots, \alpha_i(a_{1k}, \ldots, a_{nk}))$.

Poznámka 5.14 : Mějme $M_j(\cdot, 1)$ **pro** $j \leq k$ **monoidy. Pak** $\Pi M_i(\cdot, (1, ..., 1))$ **je opět monoid a platí: (1)** $(m_1, m_2, ..., m_k) \in \Pi M_i$ **je invertibilni** $\Leftrightarrow$ **jsou všechny prvky** $m_j, j = 1, ..., k$ **invertibilni. (2)** $(m_1, m_2, ..., m_k)^n = (m_1, m_2, ..., m_k) \Leftrightarrow m_j^n = m_j \ \forall j = 1, ..., k$**,** $\forall m_j \in M_j$ **a** $n \in N$**.** *Důkaz: Stačí uvážit, že* $(m_1, m_2, ..., m_k) \cdot (r_1, r_2, ..., r_k) = (m_1.r_1, m_2.r_2, ..., m_k.r_k) = (1, 1, ..., 1)$, *respektive* $(m_1, m_2, ..., m_k)^n = (m_1^n, m_2^n, ..., m_k^n)$.

Věta ★ 5.15 (Čínská věta o zbytcích) : Nechť $n_1, n_2, ..., n_k$ **jsou po dvou nesoudělná kladná celá čísla a** $n = n1, n2, ..., n_k$**, potom zobrazeni** $f : Z_n \to \Pi Z_{ni}$ **dané předpisem** $f(x) = (x\text{mod } n_1, x\text{mod } n_2, ..., x\text{mod } n_k)$ **je izomorfismus algeber** $Z_n(+, -, 0, \cdot, 1)$ **a** $\Pi Z_{ni}(+, -, 0, \cdot, 1)$ *Důkaz: Přímo z definice snadno vidíme, že je f zobrazeni slučitelne se všemi operacemi. Zbyva nahlednout, že jde o bijekci. Protože jsou* Z_n *a* ΠZ_{ni} *stejně velké konečné množiny, stačí nahlédnout, že je f proste. Nechť pro* $a \leq b \in Z_n$ *platí, že* $f(a) = f(b)$. *Potom* $f(b-a) = 0$, *tedy* $n_i / b - a \ \forall i = 1, ..., k$. *Protože jsou* n_i *po dvou nesoudělná a* $0 \leq b - a \leq n - 1$, *mame i* $n / b - a$, *tudíž* $b = a$.

Poznámka ★ 5.16 : (1) $\varphi(p^n) = (p-1)p^{n-1}$ **pro** p **prvočíslo a** $n \in \mathbf{N}$**. (2)** $\varphi(n.m) = \varphi(m).\varphi(n)$ **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.* $f : \mathbf{Z}_{mn} \to \mathbf{Z}_n \times \mathbf{Z}_m : f(k) = (k\text{mod } n, k\text{mod } m)$ *je homomorfismus (přímo ověřit slučitelnost s* $" \cdot ", 1$*), je prosté (*$f(k) = f(l), k \leq l$ *- k* mod $n = l$ mod n, k mod $m = l$ mod 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 5.12)*$|\mathbf{Z}_{nm}^*| = |(\mathbf{Z}_n \times \mathbf{Z}_m)^*| = |\mathbf{Z}_n^* \times \mathbf{Z}_m^*| = |\mathbf{Z}_n^*| \cdot |\mathbf{Z}_m^*| =$*(5.12)*$\varphi(n).\varphi(m)$.

Věta ★ 5.17 : Je-li $n = p_1^{k_1}.p_2^{k_2} \cdot ....p_l^{k_l}$ **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 (5.16(2)), úprava výrazu podle (5.16(1))*

Věta 5.18 : 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 a ideály

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 $(a + b)c = ac + bc \ \forall a, b \in R$ *(distributivita). Pak je* R **okruh**. *Pokud je* $\cdot$ *komutativní pak* R *je* **komutativní 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)** $(-1).b = b.(-1) = -b$**, (4)** $(-a)(-b) = ab$**, (5)** $|R| > 1 \Leftrightarrow 0 \neq 1$ *Důkaz: (1)* $0.a = (0 + 0).a = 0.a + 0.a \Rightarrow 0 = 0.a$*; (2)* $0 = 0.b = (a + (-a)).b = a.b + (-a).b \Rightarrow -(a.b) = (-a).b$*; (3)* $0 = 0.b = (1 + (-1)).b = 1.b + (-1).b \Rightarrow (-1).b = -b$*; (4)*$(-a).(-b) = -(a.(-b)) = -(-(a.b)) = a.b$*; (5) předp. že* $0 = 1$, $\forall r \in R$, $r = 1.r = 0.r = 0$, *tedy* $R = \{0\}$.

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

Def.: *Ideál je* **netriviální** *nebo* **vlastní**, *pokud $I \neq \{0\}$ a $I \neq R$. $a \in R \quad aR = \{a.r | r \in R\}$ je* **hlavní pravý ideál**, *$Ra = \{r.a | r \in R\}$ je* **hlavní levý ideál**.

Věta ★ 6.2 : Buď $R(+,\cdot,-,0,1)$ okruh. Pak zobrazení, které kongruenci ρ 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 (4.14), předp. (4.14(1)) - ρ je kongruence i na $R(+,-,0)$, $[0]_\rho$ je norm. podgrupa (z (2.6),(4.15)), ověřit $\forall i \in [0]_\rho$, $\forall r \in R : ir \in [0]_\rho, ri \in [0]_\rho$ - z $(i,0) \in \rho, (r,r) \in \rho$, ρ sluč. s " $\cdot$ ". (4.14(2)) z 2.6 ρ kongruence na $R(+,-,0)$, dokázat slučitelnost s " $\cdot$ ", 1 - "1" z reflexivity; " $\cdot$ " : $(a_1,a_2) \in \rho$, $(b_1,b_2) \in \rho$, $(a_1-a_2)b_1 \in I$, $a_2(b_1-b_2) \in I \Rightarrow (a_1b_1)-(a_2b_2) = (a_1-a_2)b_1 + a_2(b_1-b_2) \in I$. (4.14(3)) $\rho,\eta : [0]_\rho \subseteq [0]_\eta \Rightarrow \rho \subseteq \eta$ - platí i pro systém kongruencí na $R(+,-,0)$ z (4.15), ten je větší $\Rightarrow$ platí.*

Def.: Invertibilním prvkem *okruhu $R(+,\cdot,-,0,1)$ rozumíme invertibilní prvek monoidu $R(\cdot,1)$. Okruh nazvu* **tělesem**, *je-li každý jeho nenulový prvek invertibilní ($R^* = R \setminus \{0\}$). Ideál I je* **maximální**, *jestliže I je koatom ve svazu všech ideálů.*

Poznámka 6.3: *$R(+,\cdot,-,0,1)$* **je okruh a** *$a \in R$,* **a je invertibilní** $\Leftrightarrow aR = Ra = R$ *Důkaz: Je-li $Ra = R$, $\exists c \in R$, že $ca = 1$. Je-li c inverzní prvek a, je $r = rca \in Ra \; \forall r \in R$*

Věta ★ 6.4: V netriviálním $R(+,\cdot,-,0,1)$ je ekvivalentní: (1) $R(+,\cdot,-,0,1)$ je těleso, (2) $\{0\}, R$ jsou jediné pravé ideály okruhu, (3) $\{0\}, R$ jsou jediné levé ideály okruhu
Důkaz: ($\Rightarrow$) Buď I pravý ideál $\neq \{0\}$, tj. $\exists i \in I \quad i \neq 0$. R je těleso, tedy ke každému prvku existuje inverzní prvek, $1 = i.i^{-1} \in I$. Tedy $\forall r \in R \quad r = 1.r \in I$ a proto $I = R$.
($\Leftarrow$) Ověříme existenci inverzního prvku pro $a \in R \setminus \{0\}$. Vezměme pravý ideál aR a pro ten platí $0 \neq a = a.1 \in aR \neq \{0\}$. $aR = R$ tj. $\exists b \quad a.b = 1$ (mohu předpokládat že $0 \neq 1$), $b \neq 0$ dle 6.1 Stejný argument značí, že $bR = R$ tj. $\exists c \quad b.c = 1$. Tedy $a = c$, tj. $b = a^{-1}$.

Věta ★ 6.5: Je-li $R(+,\cdot,-,0,1)$ komutativní okruh, I je ideál, pak $R/I(+,\cdot,-,0,1)$ je těleso právě tehdy když I je maximální. *Důkaz: Je-li J ideál, pak dle věty 6.2 je ϱ_J kongruence odpovídající J. J je koatom právě tehdy když ϱ_J je koatom. Dle věty 6.2 stačí dokázat, že R/I je tělesem právě tehdy když ϱ_I je koatom ve svazu kongruencí na $R(+,\cdot,-,0,1)$ (dle tvrzení 1.8, je-li η ekvivalence na R/ϱ_I, potom $\exists \sigma \supseteq \varrho_I \quad \eta = \sigma/\varrho_I$). Tedy a $R/I \times R/I$ jsou jediné kongruence na $R/I(+,\cdot,-,0,1)$. Dle věty 6.4 je $R/I(+,\cdot,-,0,1)$ těleso právě tehdy když obsahuje právě $\{[0]_{\varrho_I}\}, R/I$, což jsou jediné ideály, a tedy dle věty 6.2 za R/I máme právě kongruence $\underbrace{\varrho_{\{[0]_{\varrho_I}\}}}_{id}$ a $\underbrace{\varrho_{R/I} = R/I \times R/I}_{R/I \times R/I}$.*

Def.: $a \in R, n \in \mathbb{Z}$ **(1)** $0 \times a = 0 \in R$, **(2)** $n \times a = ((n-1) \times a) + a \quad \forall n > 0$, **(3)** $n \times a = |n| \times (-a) \quad \forall n < 0$

Poznámka 6.6: Definujme zobrazení $\varphi : \mathbb{Z} \to R$ předpisem $\varphi(n) = n \times 1$. Pak φ je okruhový homomorfismus ($\mathbb{Z}(+,\cdot,-,0,1)$ a $R(+,\cdot,-,0,1)$), $\varphi(\mathbb{Z})$ je nejmenší podobraz R obsahující 1 a existuje jednoznačně určené $p \in \mathbb{N}_0$ takové, že $\{n \in \mathbb{Z} | \varphi(n) = 0\} = p\mathbb{Z}$. *Důkaz: Podle 5.5 je φ homomorfismus grupy $\mathbb{Z}(+,-,0)$, $R(+,-,0)$, navíc $\varphi(\mathbb{Z}) = 1$. $\varphi(1) = 1 \times 1 = 1$, $\varphi(a).\varphi(b) = (a \times 1).(b \times 1) = a \times (b \times 1) \overset{??}{=} (a \times b) \times 1 = \varphi(a.b)$. $\varphi(\mathbb{Z})$ je podokruh dle 1.1, tedy $\varphi(\mathbb{Z})$ je nejmenší podokruh. Buď $I = \{n | \varphi(n) = 0\}$, platí $n \in I \quad \varphi(-n) = -\varphi(n) = -0 = 0$, $n+m \in I \quad \varphi(n+m) = \varphi(n) + \varphi(m) = 0 + 0 = 0$, tedy I je podgrupa $\mathbb{Z}(+,-,0)$. Dle tvrzení 5.6 $\exists p \geq 0 \quad p\mathbb{Z} = I$.*

Def.: Charakteristikou okruhu $R(+,\cdot,-,0,1)$ *rozumíme* p *z poznámky 6.6.*

Poznámka 6.7: Buď $R(+,\cdot,-,0,1)$ **komutativní okruh,** $a,b \in R$ $n \in \mathbb{N}$ $(a+b)^n = (\underbrace{(a+b).\cdots.(a+b)}_{n}) = \sum_{k=0}^{n} \binom{n}{k} \times a^k.b^{n-k}$ *Důkaz: Stejně jako v* $\mathbb{R}$.

Poznámka 6.8 (důsledek) : Buď $R(+,\cdot,-,0,1)$ **komutativní okruh prvočíselné charakteristiky** p**. Pak zobrazení** $R \to R : a \to a^p$ **je okruhový homomorfismus (Frobeniův).**
Důkaz: Platí $(a+b)^p = a^p + \underbrace{\left(\sum_{k=1}^{p-1} \binom{p}{k} \times a^k.b^{p-k}\right)}_{p \text{ dělí tento člen}} + b^p = a^p + b^p$. *Dle 5.1 je* $a \to a^p$ *homomorfismus na* $R(+,-,0)$ *a* $R(+,-,0)$, $1^p = 1$ *a* $(a.b)^p = a^p.b^p$.

Def.: *Komutativní okruh* $R(+,\cdot,-,0,1)$ *je* **obor integrity** *pokud* $\forall a,b \in R$ *platí* $a.b = 0 \Rightarrow a = 0$ *nebo* $b = 0$ ($a \neq 0, b \neq 0 \Rightarrow a.b \neq 0$).

Poznámka ★ 6.9: Pro algebru $F(+,\cdot,-,0,1)$ **(1)** $F(+,0)$**,** $F(\cdot,1)$ **jsou komutativní monoidy, (2)** $\sim$ **je kongruence na algebře** $F(+,\cdot,-,0,1)$**, (3)** $(0,1) \sim (0,a)$ **a** $(1,1) \sim (a,a)$ $\forall a \in R \setminus \{0\}$**, (4)** $F/\sim (+,\cdot,-,[0]_\sim,[1]_\sim)$ **je komutativní těleso, (5)** $R \to F/\sim : r \to [(r,1)]_\sim$ **je prostý okruhový homomorfismus.**
Důkaz:

Def.: *Komutativní těleso* $F/\sim (+,\cdot,-,[0]_\sim,[1]_\sim)$ *nazýváme* **podílovým tělesem**, *píšeme* $\frac{a}{b} = [(a,b)]_\sim$