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* $\alpha_i \forall i \in I$*.*

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 <u>stejného typu</u> je* $f : A \to B$ **homomorfismus***, pokud je slučitelné se všemi jejich operacemi.* $(\forall \alpha, a_1, ..a_n \in A : f(\alpha_A(a_1, ..a_n)) = \alpha_B(f(a_1), ..f(a_n)))$

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.* $\pi_\rho(a) = [a]_\rho$*.*

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

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.*

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***.*

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.*

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.*

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)** $\alpha(B) \subseteq \alpha(C)\ \forall B \subseteq C \subseteq A$.

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** $m \wedge n = \inf_{\leq}(\{m, n\})$

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 $a < \cdot b$.*

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 $\forall a, b, c \in S : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.*

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 $a \wedge a' = 0$*

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*

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).*

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 $B_1 \subseteq \alpha\beta(B1)$.*

5 Grupy

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: $(a, b) \in \mathbf{rmod_H} \overset{\text{def}}{\equiv} ab^{-1} \in H$, $(a, b) \in \mathbf{lmod_H} \overset{\text{def}}{\equiv} a^{-1}b \in H$.

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 $|G|$.*

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

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.*

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).*

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* $\alpha_i : (\Pi A_j)^n \to \Pi A_j$ $\alpha_i((a_{11}, \ldots, a_{1k}), \ldots, (a_{n1}, \ldots, a_{nk})) = (\alpha_i(a_{11}, a_{21}, \ldots, a_{n1}), \ldots, \alpha_i(a_{1k}, \ldots, a_{nk}))$.

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**

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***.*

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.*

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)** $n \times a = |n| \times (-a) \quad \forall n < 0$

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

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

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