Jan Žemlička

Algebra I

Přepsal Petr Baudiš

v ak. roce 2005/2006

“”

© 2005/2006 Jan Žemlička, Petr Baudiš
Verze 0.20051006/L:1.616. Tato verze není garantována, nemusí být kompletní a může obsahovat chyby.
Aktuální verzi vždy najdete na `http://math.or.cz/`.
Sazba v programu TEX.

Algebry, homomorfismy a kongruence

Základní definice

Definice:

Nechť A je množina a $n \in \mathbb{N}_0$, pak o zobrazení

$$\alpha\colon A^n \to A$$

řekneme, že je n-ární operací *.

- 0-ární: nulární (operace $A_0 \to A$ je množina všech "nulatic" — dejme tomu $A_0 = \{*\}$)
- 1-ární: unární
- 2-ární: binární
- 3-ární: ternární

Nechť A je množina α_i, $i \in I$, a mějme (n_i-ární) operace. Pak posloupnost $A(\alpha_i | i \in I)$ nazveme **algebrou**.

Příklady:

(i) $\mathbb{N}(+, \cdot)$
(ii) $\mathbb{Z}(+, -, \cdot)$
(iii) $\mathbb{Q} \setminus \{0\}(\cdot, /)$
(iv) $\mathbb{R}(+, -, \cdot)$
(v) $\mathbb{R}^+(+, \cdot, \sqrt{})$

(Kromě dělení a odmocňování jde o binární operace — v případě dělení jde vpodstatě o hledání obrácené hodnoty.)

Definice:

Nechť A je množina s n-ární operací α a $B \subseteq A$. Řekneme, že B je **uzavřená na** operaci α, pokud

$$\forall b_1, \dots, b_n \in B : \alpha(b_1, \dots, b_n) \in B$$

Je-li $A(\alpha_i | i \in I)$ algebra a $B \subseteq A$, pak řekneme, že B je **podalgebra** A, pokud B je uzavřená na všechny α_i ($i \in I$).

Příklady:

(i) $\mathbb{N}(+, \cdot)$:

$$k \in \mathbb{N} : k\mathbb{N} = \{k \cdot n | n \in \mathbb{N}\} \text{ } \textit{(všechny násobky)}$$

Je taková podalgebra uzavřená?

(1) $b_1 + b_2 \in k\mathbb{N}$
(2) $b_1 \cdot b_2 \in k\mathbb{N}$

Jde tedy o podalgebru algebry $\mathbb{N}(+, \cdot)$.

* $A^n = \{(a_1, \dots, a_n) | a_i \in A\}$ (kartézský součin)

(ii) $\mathbb{Z}(+,-,0)$ má podalgebry

$$k \in \mathbb{Z} : k\mathbb{Z} = \{k \cdot z | z \in \mathbb{Z}\}$$

a jde dokonce o všechny podalgebry, neexistuje žádná jiná.
B buď podalgebra $\mathbb{Z}(+,-,0)$. Je uzavřená na nulární operaci? 0-tice $\mapsto 0 \subseteq B$.

(iii) Na vektorovém prostoru U nad tělesem T algebra $U(+, \cdot t | t \in T)$ s unární operací $\cdot t \colon U \to U$ definovanou jako $u \to u \cdot t$.
W je podprostor U, právě když W je podalgebra $U(+, \cdot t)$.

Pozorování:

$A(\alpha_i | i \in I)$ buď algebra, pak A je podalgebrou.
Pokud žádná α_i není nulární, $\emptyset$ je podalgebrou A.
Je-li $A(\alpha_i | i \in I)$ algebra (kde α_i je n_i-ární operace) a B její podalgebra,

$$\beta_i = \alpha_i \restriction_{B^{n_i}} \colon B^n \to B$$

má "přirozeně danou" strukturu algebry na B (s restringovanými ($\restriction$) operacemi).

Příklady:

(i) $\mathbb{Q}(+,\cdot)$, $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Z}$ je podalgebra.

$$\mathbb{Q}(+,\cdot) \overset{\text{restr.}}{\rightsquigarrow} \mathbb{Z}(+,\cdot)$$

(ii) Mějme $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \middle| r_i \in \mathbb{R} \right\}$ a algebru $M_2(\mathbb{R})(\cdot)$.

$$D_2(\mathbb{R}) = \left\{ \begin{pmatrix} r_1 & 0 \\ 0 & r_3 \end{pmatrix} \middle| r_1, r_3 \in \mathbb{R} \right\}$$

je podalgebra $M_2(\mathbb{R})(\cdot)$. Pak můžeme zavést např. $D_2(\mathbb{R})(\cdot)$ s operací

$$\cdot \colon \begin{pmatrix} r_1 & 0 \\ 0 & r_3 \end{pmatrix} \begin{pmatrix} s_1 & 0 \\ 0 & s_3 \end{pmatrix} = \begin{pmatrix} r_1 s_1 & 0 \\ 0 & r_3 s_3 \end{pmatrix}$$

Poznámka:

(i) Nechť A je množina s operací α a nechť A_j, $j \in J$, je systém podmnožin A uzavřených na α. Pak $\bigcap A_j$ je opět uzavřená na α.

(ii) Nechť $A(\alpha_i | i \in I)$ je algebra a A_j, $j \in J$ jsou její podalgebry. Pak $\bigcap_{j \in J} A_j$ je podalgebra.

DŮKAZ:

(i) α buď n-ární operace.

$$\bigcap_{j' \in J} A_{j'} \subseteq A_j \qquad \forall j \in J$$

T-O-D-O: tady je něco nějaké divné…?!

$$\implies \alpha(a_1, \dots, a_n) \in A_j \overset{\substack{\text{def.} \\ \text{průniku}}}{\implies} \alpha(a_1, \dots, a_n) \subseteq \bigcap_{j \in J} A_j$$

(ii) A_j jsou uzavřené na α_i pro $\forall i \in I$, $\forall j \in J$.

$$\stackrel{(1)}{\Longrightarrow} \bigcap_{j\in J} A_j \text{ je uzavřený na } \alpha_i \text{ pro } \forall i \in I$$

$$\Longrightarrow \bigcap_{j\in J} A_j \text{ je uzavřená na všechny operace na } A(\alpha_i | i \in I)$$

$$\stackrel{\text{def.}}{\Longrightarrow} \bigcap_{j\in J} A_j \text{ je podalgebra } A(\alpha_i | i \in I)$$

Q.E.D.

Definice:

Buď A a B množiny s n-ární operací α a $f\colon A \to B$. Řekneme, že f je **slučitelná s** α, pokud

$$\forall \alpha, a_n \in A : \alpha(f(a_1), f(a_2), \ldots, f(a_n)) = f(\alpha(a_1, \ldots, a_n)$$

Řekneme, že algebra $A(\alpha_i | i \in I)$ a $B(\alpha_i | i \in I)$ jsou **stejného typu**, pokud α_i na A a α_i operace na B jsou obě stejné arity (obě n_i-ární) $\forall i \in I$.

Buď $A(\alpha_i | i \in I)$ a $B(\alpha_i | i \in I)$ dvě algebry stejného typu. Pak zobrazení $f\colon A \to B$ je homomorfismus, pokud je f slučitelná s α_i pro $\forall i \in I$.

Poznámka:

(i) Buď A, B, C množiny s n-ární operací α, $f\colon A \to B$, $g\colon B \to C$ zobrazení slučitelná s a. Pak $gf (A \to C)$ je slučitelné s α. Pokud je f bijekce, tak f^{-1} je zase slučitelné s α.

(ii) Nechť $A(\alpha_i | i \in I)$, $B(\alpha_i | i \in I)$, $C(\alpha_i | i \in I)$ jsou algebry stejného typu a $f\colon A \to B$, $g\colon B \to C$ jsou homomorfismy. Pak gf je opět homomorfismus. Je-li f bijekce, pak f^{-1} je také homomorfismus.

DŮKAZ:

(i) $a_1, \ldots, a_n \in A$

$$g(f(\underbrace{\alpha}_{A}(a_1, \ldots, a_n))) = g(\underbrace{\alpha}_{B}(f(a_n), \ldots, f(a_n))) \stackrel{\text{def.}}{=} \underbrace{\alpha}_{C}(g(f(a_1)), g(f(a_2)), \ldots, g(f(a_n)))$$

Je-li f bijekce, f^{-1} je zobrazení $B \to A$.
$b_1, \ldots, b_n \in B$

$$f_{-1}(\underbrace{\alpha}_{B}(b_1, \ldots, b_n)) \stackrel{?}{=} \underbrace{\alpha}_{A}(f^{-1}(b_1), \ldots, f^{-1}(b_n))$$

$$f(\underbrace{\alpha}_{A}(f^{-1}(b_1), \ldots, f^{-1}(b_n))) \stackrel{\text{def}}{=} \underbrace{\alpha}_{B}(\underbrace{f(f^{-1}(b_1))}_{b_1}, \ldots))$$

$$\alpha(f^{-1}(b_1), \ldots, f^{-1}(b_n)) = f^{-1}(f(\alpha(f^{-1}(b_1)), \ldots)) =$$
$$= f^{-1}(\alpha(b_1, \ldots, b_n))$$

(ii) Dle (1) je ???? slučitelná s α_i pro $\forall i \in I$, tedy z definice gf je homomorfismus.
f^{-1} je slučitelna se všemi α_i, tedy opět z definice je i f^{-1} homomorfismus.

Q.E.D.

Definice:

Jsou-li $A(\alpha_i|i \in I)$, $B(\alpha_i|i \in I)$ algebry stejného typu a zobrazení $f\colon A \to B$ je bijektivní homomorfismus, mluvíme o **isomorfismu**.

A a B jsou **isomorfní** algebry, pokud mezi nimi existuje isomorfismus.

Isomorfismus zachovává všechny algebraické vlastnosti, tedy veškeré formule zapsané v jedné algebře platí i v té druhé. Tedy dvě isomorfní algebry mají "stejné algebraické vlastnosti". Přesná formulace a důkaz na rozmyšlenou, jste-li vzdělaní v logice.

Poznámka:

(i) Nechť A a B jsou množiny s operací α a $C \subseteq A$, $D \subseteq B$ jsou uzavřené na α. Je-li $f\colon A \to B$ slučitelná s α, pak $f(C)$ je uzavřené na α v B a $f^{-1}(D) = \{a \in A | f(a) \in D\}$ je množina uzavřená na α v A.

(ii) Nechť $A(\alpha_i|i \in I)$ a $B(\alpha_i|i \in I)$ jsou algebry stejného typu a $C \subseteq A$, $D \subseteq B$ jsou podalgebry. Je-li $f\colon A \to B$ homomorfismus, pak $f(C) \subseteq B$ a $f^{-1}(D) \subseteq A$ jsou podalgebry.

DŮKAZ:

(i) Je $f(C)$ uzavřené na α? (α buď n-ární.)

$$b_1 \dots b_n \in f(C) \Rightarrow \exists\, a_1, \dots, a_n \in C : f(a_i) = b_i$$
$$\alpha(b_1, \dots, b_n) = \alpha(f(a_1), \dots, f(a_n)) =$$

Protože f je slučitelné s α,

$$= f(\underbrace{\alpha(a_1, \dots, a_n)}_{\in C}) \in f(C)$$

tedy ať proženu skrz α cokoliv z C, vždy to skončí v $f(C)$. Jinak řečeno je $f(C)$ uzavřené na operaci α.

$$a_1, \dots, a_n \in f^{-1}(D) \Rightarrow f(a_i) \in D$$
$$f(\alpha(a_1, \dots, a_n)) \underset{\text{sluč.}}{\overset{\text{def}}{=}} \alpha(f(a_1, \dots, f(a_n)) \in D$$

protože všechny argumenty α leží v D a D je uzavřená na α.

$$\Rightarrow \alpha(a_1, \dots, a_n) \in f^{-1}(D)$$

(ii) Pro $\forall i \in I$ aplikuji (1) na α_i.

Q.E.D.

Příklady:

(i) Lineární zobrazení $f\colon U \to V$, kde U, V jsou vektorové prostory nad tělesem T, jsou homomorfismy algeber $U(+, \cdot t|t \in T)$ a $V(+, \cdot t|t \in T)$.

(ii) Determinant: $M_n(T) \to T$ je isomorfismus algebry $M_n(T)(\cdot)$ (maticové násobení) do $T(\cdot)$ (kde $M_n(T)$ je čtvercová matice $n \times n$ na tělese T).

(iii) $\Pi_n\colon \mathbb{Z} \to \mathbb{Z}_n$, $\Pi_n(k) = k \bmod n$. Pak Π_n je homomorfismus algebry $\mathbb{Z}(+, \cdot)$ do $\mathbb{Z}_n(\underbrace{+, \cdot}_{\bmod n})$.

Definice:

Řekneme, že ϱ je relace na množině A, pokud $\varrho \subseteq A \times A$. Buď ϱ relace na A, pak

$$\varrho^- = \{(b,a) \in A \times A | (a,b) \in \varrho\}$$
$$\varrho^+ = \{(a,b) \in A \times A | \exists\, a_1, \dots, a_n \in A : a_1 = a, a_n = b,\ (a_i, a_{i-1}) \in \varrho\}$$
$$(a,b),(b,c) \in \varrho \Rightarrow (a,c) \in \varrho^+$$
$$\mathrm{id} = \{(a,a) \subseteq A \times A | a \in A\}$$

Řekneme, že ϱ je:

- **reflexivní**, pokud $\mathrm{id} \subseteq \varrho$.
- **symetrická**, pokud $\varrho^- \subseteq \varrho$.
- **tranzitivní**, pokud $\varrho^+ \subseteq \varrho$.

ϱ je **ekvivalence**, jde-li o reflexivní, symetrickou a tranzitivní relaci. Lze ji zapsat jako:

$$(a,b) \in \varrho \Leftrightarrow a \varrho b$$

Definujme si ještě **faktor** A **podle** ϱ jako množinu

$$A/\varrho = \{[a]_\varrho : a \in A\} \qquad [a]_\varrho = \{b \in A : (a,b) \in \varrho\}$$

Poznámka:

A/ϱ tvoří rozklad.

DŮKAZ:

$$A = \bigcup \{[a]_\varrho : a \in A\} \Leftrightarrow a \in [a]_\varrho \ \textit{(reflexivita)}$$
$$x \in [a]_\varrho \cap [b]_\varrho \Rightarrow \left\{ \begin{array}{l} (a,x) \in \varrho \\ (x,b) \in \varrho \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} (x,a) \in \varrho \\ (x,b) \in \varrho \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} (a,b) \in \varrho \\ (b,a) \in \varrho \end{array} \right\} \Rightarrow (a,b) \in \varrho$$
$$[b]_\varrho = \{y \in A : (b,y) \in \varrho\}$$

Přitom však $(a,b) \in \varrho$, tedy zároveň tranzitivně $(a,y) \in \varrho$ a platí

$$\forall y \in [b]_\varrho : (a,y) \in \varrho \Rightarrow y \in [a]_\varrho$$

To znamená, že $[b]_\varrho \subseteq [a]_\varrho$. Ale symetricky i $[a]_\varrho \subseteq [b]_\varrho$. Tedy $[a]_\varrho = [b]_\varrho$.

Poznámka:

Mějme $\{B_i : i \in I\}$ rozklad množiny A. Pak relace na A definovaná předpisem

$$(a,b) \in \varrho \Leftrightarrow \exists\, i \in I : a,b \in B_i$$

je ekvivalence a $A/\varrho = \{B_i : i \in I\}$.

DŮKAZ:

(a) Reflexivita: $a \in B_i$ pro nějaké $i \in I$, neboť $(a,a) \in \varrho$

(b) Symetrie: $(a,b) \in \varrho \Rightarrow \exists\, i : a,b \in B_i \Rightarrow (b,a) \in \varrho$

(c) Tranzitivita: $(a,b),(b,c) \in \varrho \Rightarrow \exists\, i,j : a,b \in B_i,\ b,c \in B_j$
Ale v tom případě $B_i \cap B_j \neq \emptyset$, tedy nutně $B_i = B_j$ a $c \in B_i$.

(d) Faktor: $a \in B_i \Rightarrow [a]_\varrho = B_i$.

Definice:

Nechť $f\colon A \to B$ je zobrazení. Pak **jádrem** f nazveme relaci Ker danou předpisem:

$$(a_1, a_2) \in \operatorname{Ker} f \Leftrightarrow f(a_1) = f(a_2)$$

Je-li ϱ ekvivalence na množině A, pak zobrazení $\Pi_\varrho\colon A \to A/\varrho$ daném $\Pi_\varrho(a) = [a]_\varrho$ řekneme **přirozená projekce podle** ϱ.

Poznámka:

Buď $f\colon A \to B$ zobrazení a ϱ ekvivalence na A. Pak platí:

(i) $\operatorname{Ker}_\varrho$ je ekvivalence
(ii) f je prosté $\Leftrightarrow \operatorname{Ker} = \mathrm{id}$
(iii) $\operatorname{Ker} \Pi_\varrho = \varrho$
(iv) Zobrazení $\varrho\colon A/\varrho \to B$ s vlastností $(g \cdot \Pi_\varrho) = f$ existuje $\Leftrightarrow \varrho \subseteq \operatorname{Ker}_f$

DŮKAZ:

(i) Ověříme všechny tři vlastnosti:
  (1) $f(a) = f(a) \Rightarrow (a, a) \in \operatorname{Ker} f$
  (2) $f(a_1) = f(a_2) \Rightarrow (a_1, a_2) \in \operatorname{Ker} f \Rightarrow (a_2, a_1) \in \operatorname{Ker} f$
  (3) $(a_1, a_2), (a_2, a_3) \in \operatorname{Ker} f \Rightarrow f(a_1) = f(a_2) = f(a_3) \Rightarrow (a_1, a_3) \in \operatorname{Ker} f$
(ii) $a_1 \neq a_2 \Rightarrow (f(a_1) \neq f(a_2) \Leftrightarrow (a_1, a_2) \notin \operatorname{Ker} f)$
(iii) $(a_1, a_2) \in \operatorname{Ker} \Pi_\varrho \Leftrightarrow \Pi_\varrho(a_1) = \Pi_\varrho(a_2) \Leftrightarrow (a_1, a_2) \in \varrho$
(iv) Ověříme obě implikace:

"$\Rightarrow$"

Předpokládejme existenci g:

$$g\Pi_\varrho = f$$

$$\forall a \in A : g([a]_\varrho) = g \circ \Pi_\varrho(a) = f(a)$$

Nyní stačí vzít $a, b \in \varrho : [a]_\varrho = [b]_\varrho$:

$$f(a) = g([a]_\varrho) = g([b]_\varrho) = f(b) \Rightarrow (a, b) \in \operatorname{Ker} f$$

"$\Leftarrow$"

Předpokládejme $\varrho \in \operatorname{Ker} f$:

$$g([a]_\varrho) = f(a)$$

Máme ale problém s korektností definice g. Musíme ji ověřit:

$$[a]_\varrho = [b]_\varrho \Rightarrow (a, b) \in \varrho \subseteq \operatorname{Ker} f$$

$$g([a]_\varrho) = f(a) = f(b) = g([b]_\varrho)$$

Tedy je g skutečně definována korektně. $g\Pi_\varrho = f$ je zřejmé.

Q.E.D.

Definice:

Nechť α je n-ární operace na A a ϱ je ekvivalence na A. Řekneme, že ϱ **je slučitelné s** α, pokud pro $i = 1 \dots n$ platí:

$$(a_i, b_i) \in \varrho \Rightarrow \alpha(a_1, \dots, a_n) \varrho \alpha(b_1, \dots, b_n)$$

Je-li $A(\alpha_i : i \in I)$ algebra a ϱ je ekvivalence na A, pak ϱ **je kongruence na** A, pokud ϱ je slučitelné s α_i pro $\forall i \in I$.

Poznámka:

(i) Nechť A, B jsou množiny, α je operace na A, B a f je zobrazení $A \to B$ slučitelné s α. Pak $\operatorname{Ker} f$ je slučitelné s α.

(ii) Buď A, B algebry stejného typu a f homomorfismus $A \to B$. Potom $\operatorname{Ker} f$ je kongruence.

DŮKAZ:

(i) $(a_i, b_i) \in \operatorname{Ker} f \Rightarrow f(a_i) = f(b_i) \qquad \forall i = 1, \dots, n$

$$f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) = \alpha(f(b_1), \dots, f(b_n)) = f(\alpha(b_1, \dots, b_n))$$

$$\Rightarrow (\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \operatorname{Ker} f$$

$\operatorname{Ker} f$ je ekvivalence (dle V1.6-(i)).

(ii) plyne z (i).

Q.E.D.

VĚTA 1.8 ():

(i) Nechť ϱ je ekvivalence na A, α je operace na A. Pak ϱ je slučitelná s α, právě když Π_ϱ je slučitelná s α.

(ii) Nechť ϱ je ekvivalence na algebře A. Pak ϱ je kongruence, právě když Π_ϱ je homeomorfismus.

DŮKAZ:

A buď množina s ekvivalencí ϱ a relací α. Definujme operaci α na A/ϱ:

$$\alpha([a_1]_\varrho, \dots, [a_n]_\varrho) = [\alpha(a_1, \dots, a_n)]_\varrho$$

Na algebře A/ϱ definuji stejným způsobem algebru stejného typu jako A za předpokladu, že A je algebra. Definice je korektní, právě když

$$\begin{array}{ccc} [a_1]_\varrho = [b_1]_\varrho & & (a_1, b_1) \in \varrho \\ \vdots & \Rightarrow & \vdots \\ [a_n]_\varrho = [b_n]_\varrho & & (a_n, b_n) \in \varrho \end{array}$$

Všimněme si, že

$$[\alpha(a_1, \dots, a_n)]_\varrho = [\alpha(b_1, \dots, b_n)]_\varrho$$

platí, právě když ϱ je slučitelné s α. Pro algebry je definice korektní, právě když ϱ je kongruence.

(i) Dokážeme obě implikace:

"$\Rightarrow$"

ϱ je slučitelná s $\alpha \Rightarrow \alpha$ je dobře definovaná na A/ϱ.
Je $\Pi_\varrho\colon A \to A/\varrho$ slučitelné s α?

$$\Pi_\varrho(\alpha(a_1,\dots,a_n)) = [\alpha(a_1,\dots,a_n)] = \alpha([a_1]_\varrho,\dots,[a_n]_\varrho = \alpha(\Pi_\varrho(a_1),\dots,\Pi_\varrho(a_n))$$

Tedy Π_ϱ je s α slučitelné s α.

"$\Leftarrow$"

Π_ϱ je slučitelné s α, $\operatorname{Ker}\Pi_\varrho = \varrho$ (V1.6-(iii)). Tedy α je korektně definována (V1.7-(i)).

Q.E.D.

Grupoidy, monoidy, grupy

Definice:

Grupoidem nazveme algebru $G(\cdot)$ s binární operací "$\cdot$". Prvek $e \in G$ nazveme neutrálním prvekm grupoidu $G(\cdot)$, pokud

$$e \cdot g = g \cdot e = g \qquad \forall g \in G$$

Řekneme, že algebra $M(\cdot, e)$ je **monoid**, pokud "$\cdot$" je asociativní binární operace a e je neutrální prvek $M(\cdot)$.

Příklady:

(i) $\mathbb{X}$ buď množina "písmen", množina slov pak bude

$$M(\mathbb{X}) = \{x_1, \dots, x_n : x_i \in \mathbb{X}\}$$

$$x_1 \dots x_n \cdot y_1 \dots y_n = x_1 \dots x_n y_1 \dots y_n$$

Pak e buď prázdné slovo, a $M(\mathbb{X}, e)$ monoid (tzv. **slovní monoid**).

(ii) $X \neq \emptyset$, $T(X) = \{f\colon X \to X : f$ je zobrazení $\}$. Pak $T(X)(\circ, \mathrm{id}_X)$ je tzv. **transformační monoid**.

(iii) T buď těleso, $M_n(T)$ čtvercové matice nad T. Monoid je $M_n(T)(\cdot, I_n)$.
Mějme $\det\colon M_n(T) \to T$, to je homomorfismus monoidů $M_n(T)(\cdot, I_n)$ a $T(\cdot, 1)$.

Poznámka:

Nechť $G(\cdot)$ je grupoid. Pak na G existuje nejvýše jeden neutrální prvek.

DŮKAZ:

Nechť $e, f \in G$ jsou neutrální:

$$e \overset{f}{=} e \cdot f \overset{e}{=} f$$

Q.E.D.

Poznámka:

Buď $M(\cdot, e)$ monoid. Mějme $a, b, c \in M$ takové, že $e = a \cdot b = c \cdot a$. Pak $b = c$.

DŮKAZ:

$$c = c \cdot (a \cdot b) \overset{\text{asoc.}}{=} (c \cdot a) \cdot b = e \cdot b = b$$

Q.E.D.

Definice:

Mějme monoid $M(\cdot, 1)$. Pak prvek m^{-1} nazveme **inverzním prvkem** k $m \in M$, pokud

$$m \cdot m^{-1} = m^{-1} \cdot m = 1$$

Prvek m je **invertibilní**, existuje-li k němu prvek inverzní.

Příklady:

(i) Slovní monoid $M(\mathbb{X})$ obsahuje pouze jeden invertibilní prvek, a to prázdné slovo.

(ii) V transformačním monoidu $T(X)$ jsou invertibilní právě bijekce.
Nechť X je nekonečná. Pak $\exists\, f \in T(X)$, pro něj najdeme $g \in T(x)$: $g \circ f = \mathrm{id}$, ale f není invertibilní.
Vezměme např. $f\colon \mathbb{N} \to \mathbb{N}$, $n \to 2n$ (*prosté*, ale ne *na*). K němu pak vybereme $g\colon \mathbb{N} \to \mathbb{N}$, $n \to [n/2]$. Pak $gf = \mathrm{id}$, ale fg není na.

Poznámka:

(1.11) Nechť $M(\cdot, 1)$ je monoid a M^* množina všech invertibilních prvků. Pak M^* tvoří podmonoid a navíc inverzní prvek (k nějakému invertibilní) je stále invertibilní.

DŮKAZ:

$$M^* = \{n \in M : \exists\, n \in M : n \cdot m = m \cdot n = 1\}$$

Platí, že $1 \cdot 1 = 1$, tj. 1 je inverzní sám k sobě. Tudíž $1 \in M^*$ (uzavřenost na operaci "1").

$$a, b \in M^* \Rightarrow \exists\, c, d \in M \qquad \begin{array}{l} a \cdot c = c \cdot a = 1 \\ b \cdot d = d \cdot b = 1 \end{array}$$

$$(a \cdot b)(d \cdot c) = a \cdot (b \cdot d) \cdot c = (a \cdot 1) \cdot c = a \cdot c = 1$$

$$(d \cdot c)(a \cdot b) = d \cdot (c \cdot a) \cdot b = (d \cdot 1) \cdot b = d \cdot b = 1$$

Tedy $(a \cdot b) \in M^*$.

$$\forall m \in M\ \exists\, n : n \cdot m = m \cdot n = 1$$

(Pro n vezmu vhodné m; $(m^{-1})^{-1} = m$.)
Q.E.D.

Definice:

Řekneme, že $G(\cdot, {}^{-1}, 1)$ je **grupa**, pokud $G(\cdot, 1)$ je monoid a ${}^{-1}$ je unární operace inverzního prvku (tj. $()^{-1} : G \to G$, $\forall g : g \cdot g^{-1} = g^{-1} \cdot g = 1$).

Poznámka:

(1.12) Nechť $M(\cdot, 1)$ je monoid, M^* množina všech invertibilních prvků a $\cdot \restriction_{M^*}\colon M^* \times M^* \to M^*$ operace taková, že $m \cdot \restriction_{M^*} n = m \cdot n$ pro $\forall m, n \in M^*$ a $()^{-1}$ přiřadí každému prvku z M^* prvek k němu inverzní. Pak $M^*(\cdot \restriction_{M^*}, {}^{-1}, 1)$ je grupa.
Důkaz: Definice a poznámka 1.11. *Q.E.D.*

Příklady:

(i) $T(X)(\circ, \mathrm{id})$ buď monoid a $S(X)$ všechny bijekce. Pak $(T(X))^* = S(X)$ a podle pozn. 1.12 bude platit, že $S(X)(\circ, {}^{-1}, \mathrm{id})$ je grupa.
Speciálně $S(\{1, \dots, n\})$ jsou permutace na $\{1, \dots, n\}$.

(ii) $M_n(T)(\cdot, I_n)$ je monoid, $GL_n(T)(\cdot, {}^{-1}, \mathrm{id})$ je grupa.

Definice:

Nechť $G(\cdot, ^{-1}, 1)$ je grupa. Řekneme, že $H \subseteq G$ je **podgrupa**, pokud H je podalgebra algebry $G(\cdot, ^{-1}, 1)$. Řekneme, že podgrupa H je **normální**, pokud

$$\forall g \in G, \forall h \in H : g \cdot h \cdot g^{-1} \in H$$

Řekneme, že grupa $G(\cdot, ^{-1}, 1)$ je komutativní, je-li operace $\cdot$ komutativní.

Poznámka:

Všechny podgrupy komutativní grupy jsou normální.

DŮKAZ:

Nechť $G(\cdot, ^{-1}, 1)$ je komutativní grupa a nechť H je podgrupa G.

$$g \in G,\ h \in H; g \cdot h \cdot g^{-1} = (g \cdot g^{-1}) \cdot h = h \in H$$

Q.E.D.

Příklad:

$$S(\{1,2,3\})(\cdot, ^{-1}, \mathrm{id})$$
$$H = \{\mathrm{id}, (12)\} \ \textit{(podgrupa)}$$
$$(13) \circ (12) \circ (13)^{-1} = (23) \neq H$$

(Tedy H není normální.)

VĚTA 1.14 ():

Nechť $G(\cdot, ^{-1}, 1)$ je grupa. Pak ϱ je kongruence na grupě $G(\cdot, ^{-1}, 1)$, právě když $[1]_\varrho$ je normální podgrupa, a také platí $(g,h) \in \varrho \Leftrightarrow g^{-1}h \in [1]_p$.

DŮKAZ:

“$\Rightarrow$”

$$[1]_\varrho = \{h \in G : (1,h) \in \sigma\}$$

$[1]_\varrho$ je podgrupa. $(1,1) \in \varrho$, z definice kongruence $1 \in [1]_\varrho$.

Nechť $h \in [1]_\varrho$, tj. $(1,h) \in \varrho$, ale ze slučitelnosti ϱ s $^{-1}$ platí $(1^{-1}, h^{-1}) \in \varrho$, tedy $h^{-1} \in [1]_\varrho$.

$h_1, h_2 \in [1]_\varrho$, tedy ze slučitelnosti ϱ s $\cdot$:

$$\left.\begin{array}{r}(1,h_1) \in \varrho \\ (1,h_2) \in \varrho\end{array}\right\} \Rightarrow (1 \cdot 1, h_1 \cdot h_2) \in \varrho$$

Tedy $h_1 \cdot h_2 \in [1]_\varrho$.

Zbývá dokázat, že $[1]_\varrho$ je normální. Vezměme $g \in G$. $h \in [1]_\varrho$, tedy $(1,h) \in \varrho$. ϱ je ekvivalence, tedy $(g,g) \in \varrho$ a $(g^{-1}, g^{-1}) \in \varrho$. Ze slučitelnosti ϱ s $\cdot$ ale

$$(g \cdot 1, g \cdot h) \in \varrho$$
$$(g \cdot 1 \cdot g^{-1}, g \cdot h \cdot g^{-1}) \in \varrho$$
$$\Rightarrow ghg^{-1} \in [1]_\varrho$$

?

?

T-O-D-O: tady toho spoustu chybí, musím ještě dopsat
T-O-D-O: tenhle fragment je extrémně neuhlazený :/

VĚTA 3.6 (první věta o isomorfismu):

Nechť $f\colon A \to B$ je homomorfismus algeber stejného typu. Pak $f(A)$ je podalgebra B (čili algebra stejného typu) a $A/\operatorname{Ker} f \cong f(A)$.

DŮKAZ:

$f\colon A \to f(A) \subseteq B$
3.5: $\varrho = \operatorname{Ker} f$

$$\exists \operatorname{Ker} f = \varrho \to g \text{ je isomorfismus}$$

Příklady:

(i) $\varphi_n\colon \mathbb{Z} \to \mathbb{Z}_n$, $\varphi_n(k) = (k) \bmod n$
φ_n je homomorfismus $\mathbb{Z}(+,-,0)$ a $\mathbb{Z}_n(+,-,0)$ $(\bmod n)$.

$$\mathbb{Z}/\operatorname{Ker}\varphi_n \cong \varphi(\mathbb{Z}) = \mathbb{Z}_n$$

$$(k,l) = \operatorname{Ker}\varphi_n = (k) \bmod n = (l) \bmod n = n/k \cdot l$$

(ii) $\psi_\alpha : \mathbb{R}[x] \to \mathbb{R}$, $\psi_\alpha(p) = p(\alpha)$, $\alpha \in \mathbb{R}$
ψ_α je homomorfismus algeber $\mathbb{R}[x](+,-,0,1,\cdot)$ a $\mathbb{R}(+,-,0,1,\cdot)$. 3.6 -¿ $\mathbb{R}[x]/\operatorname{Ker}\psi_\alpha \cong \mathbb{R}$

VĚTA 3.7 ():

Nechť $\varrho \subseteq \sigma$ jsou dvě kongruence na algebře A. Pak $A/\varrho \,/\, \sigma/\varrho \cong A/\sigma$.

DŮKAZ:

$$A \xrightarrow{\Pi_\varrho} A/\sigma$$

$$\varrho \subseteq \sigma$$

$$\operatorname{Ker}\Pi_\sigma = \sigma$$

$$\exists g : A/\varrho \to A/\sigma$$

$$g([a]_\varrho) = [a]_\sigma$$

homomorfismus
g je dle 3.6 *na*, tedy $A/\varrho \,/\, \operatorname{Ker} g \cong A/\sigma$.

$$\operatorname{Ker} g = \{([a]_\varrho, [b]_\varrho) : \underbrace{[a]_\sigma = [b]_\sigma}_{\Rightarrow (a,b)=\sigma}\}$$

$$\overset{\text{def}}{=} \sigma/\varrho$$

$$\Rightarrow A/\varrho \,/\, \sigma/\varrho = A/\varrho \,/\, \operatorname{Ker} g \cong A/\sigma$$

Q.E.D.

Příklad:

$\varphi_n\colon \mathbb{Z} \to \mathbb{Z}_n$, $\varphi_m\colon \mathbb{Z} \to \mathbb{Z}_m$

$$\operatorname{Ker}\varphi_n \subseteq \operatorname{Ker}\varphi_m \Leftrightarrow n/m(n = my)$$

$$(a,b) \in \operatorname{Ker}\varphi_n \Leftrightarrow n/(a-b)((a-b) = nx = nxy)$$

Svazy

Definice:

Řekneme, že relace $\leq$ na M je uspořádání, pokud je $\leq$ reflexivní, tranzitivní a platí

$$a \leq b, b \leq a \Rightarrow a = b$$

(tzv. **slabá antisymetrie**).

Příklady:

(i) $\mathcal{P}(x)$ — potence na X, pak $\subseteq$ je uspořádání.
(ii) $\leq$ na $\mathbb{Z}$ je uspořádání.
(iii) / na $\mathbb{N}$ ("dělí": $a/b \Leftrightarrow \exists\, x \in \mathbb{N} : b = xa$).
(iv) id na M

Definice:

Nechť $\leq$ je uspořádání na $M \neq \emptyset$ a $A \subseteq M$. Řekneme, že $m \in A$ je **největší** (resp. **nejmenší**) **prvek** A, platí-li

$$\forall a \in A : a \leq m$$

Řekneme, že $\sup_{\leq}(A)$ (resp. $\inf_{\leq}(A)$) $\in M$ je **supremum** (resp. **infimum**) množiny A, pokud $\sup_{\leq}(A)$ je nejmenší prvek množiny

$$\{m \in M : a \leq m \quad \forall a \in A\}$$

a $\inf_{\leq}(A)$ je největší prvek množiny

$$\{m \in M : m \leq e \quad \forall a \in A\}$$

Řekneme, že dvojice $(M, \leq)$ je **svaz**, existuje-li $\sup_{\leq}(\{a, b\})$ i $\inf_{\leq}(\{a, b\})$ pro $\forall a, b \in M$.
O svazu $(M, \leq)$ řekneme, že je **úplný**, existuje-li $\sup_{\leq}(A)$ a $\inf_{\leq}(A)$ pro $\forall A \subset M$.

Příklady:

(i) Mějme $\mathcal{P}(x)$. Vezmeme $\mathcal{B} \subseteq \mathcal{P}(x)$, $\bigcap \mathcal{B} = \inf_{\subseteq}(\mathcal{B})$. Naopak $\bigcup \mathcal{B} = \sup_{\subseteq}(\mathcal{B})$. Tedy $(\mathcal{P}(x), \subseteq)$ je úplný svaz.
(ii) Mějme $\leq$ na $\mathbb{Z}$. Pak $\inf_{\leq}(\{a, b\}) = \min_{\leq}(a, b)$ a naopak $\sup_{\leq}(\{a, b\}) = \max_{\leq}(a, b)$. Tedy je $(\mathbb{Z}, \leq)$ svaz (ale ne úplný, museli bychom mít $\pm\infty$).
(iii) Pro / na $\mathbb{N}$ je $\inf_{/}(a, b) = \mathrm{NSD}(a, b)$, $\sup_{/}(a, b) = \mathrm{nsn}(a, b)$.

Poznámka:

Nechť $(M, \leq)$ je svaz a definujme lineární $\vee$, $\wedge$ na M předpisem

$$a, b \in M : a \wedge b = \inf_{\leq}(\{a, b\}) \quad a \vee b = \sup_{\leq}(\{a, b\})$$

Pak pro $\forall a, b, c \in M$ platí

(i) $a \wedge b = b \vee a$, $a \vee b = b \wedge a$
(ii) $a \wedge a = a = a \vee a$

(iii) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
$a \vee (b \vee c) = (a \vee b) \vee c$

(iv) $a \wedge (b \vee a) = a$
$a \vee (b \wedge a) = a$

DŮKAZ:

(i) Triviální.

(ii) Triviální.

(iii) Dokažme pro $\wedge$ (pro $\vee$ bude symetrický). Stačí dokázat, že

$$a \wedge (b \wedge c) \stackrel{?}{=} \inf(\{a, b, c\}) \quad (= c \wedge (a \wedge b))$$

Jak bude vypadat největší dolní odhad? $i \leq a$, $i \leq b$, $i \leq c$. Tedy $i \leq a$, $i \leq b \wedge c$ (neboť $b \wedge c$ je definován jako *největší* dolní odhad). Tudíž $i \leq a \wedge (b \wedge c) = J$.

Z definice pak $J \leq a$, ale zároveň $J \leq (b \wedge c)$, tedy $J \leq b$ a $J \leq c$. To ale znamená, že $a \wedge (b \wedge c) \leq i$. Ovšem máme slabou antisymetrii, tedy $a \wedge (b \wedge c) = i$.

(iv) Víme, že $a \wedge (b \vee a) \leq a$. Z reflexivity $a \leq a$, zároveň zřejmě $a \leq b \vee a$ (tady je a nějaký dolní odhad $\{a, b \vee a\}$). Tudíž $a \leq a \wedge (b \vee a)$. A díky slabé antisymetrii proto $a = a \wedge (b \vee a)$.

Q.E.D.

LEMMA4.2L1:

$$a \vee b = b \Leftrightarrow a \wedge b = a$$

DŮKAZ:

"$\Rightarrow$"

$$a \wedge b = a \wedge (a \vee b) = a \wedge (b \vee a) = a$$

"$\Leftarrow$"

$$a = a \wedge b$$

$$b \vee a = b \vee (a \wedge b) = b$$

Q.E.D.

Poznámka:

Nechť $M(\wedge, \vee)$ je algebra s dvojicí lineárních operací splňujících V4.1-(i)-(iv). Definujme na M relaci $\leq$ předpisem

$$a \leq b \stackrel{\text{def}}{=} a \wedge b = b$$

(nebo $a \wedge b = a$). Pak $(M, \leq)$ je svaz a platí

$$a \wedge b = \inf_{\leq}(\{a, b\})$$

$$a \vee b = \sup_{\leq}(\{a, b\})$$

DŮKAZ:

Platí $a \wedge a = a$, $a \vee a = a$, tedy $a \leq a$ (reflexivita $\leq$).

T-O-D-O: (a little of) stuff missing

VĚTA 4.3 ():

Nechť $\mathcal{C}$ je uzávěrový systém. Pak $(\mathcal{C}, \leq)$ je úplný svaz, kde $\inf_{\leq}(\mathcal{B}) = \bigcap \mathcal{B}$ a $\sup_{\leq}(\mathcal{B}) = \mathrm{cl}_{\mathcal{C}}(\bigcup \mathcal{B})$ (pro $\mathcal{B} \subseteq \mathcal{C}$).

DŮKAZ:

Přímo z definice uzávěrového systému a sup a inf.
Q.E.D.

Poznámka:

Buď $M(\wedge, \vee)$ svaz. Pak $M(\vee, \wedge)$ je také svaz (je "opačným" uspořádáním $\geq$).

DŮKAZ:

Definice $\leq$ ($a \leq b \stackrel{\mathrm{def}}{=} b \geq a$). (S1)–(S4) symetrické.
Q.E.D.

Definice:

Nechť $(M, \leq)$ je svaz a $a, b \in M$. Řekneme, že b **pokrývá** a a $(a < b)$, pokud $a \leq b$, $a \neq b$,

$$a \leq c \leq b \Rightarrow a = c$$

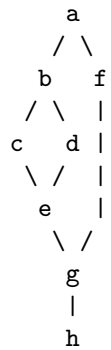
nebo $b = c$.

Nechť $e \in M$ je nejmenší (a $f \in M$ největší) prvek M. Řekneme, že $a \in M$ je **atom** (resp. **koatom**), pokud $e < a$ (resp. $a < f$). O (orientovaném) grafu řekneme, že je **Hasseovým diagramem** svazu M, pokud jeho vrcholy tvoří M.

Dva prvky a, b jsou spojené hranou tak, že a je pod b, pokud $a < b$.

Příklady:

(i)



$$M = \{a, b, c, d, e, f, g, h\}$$

$$c \wedge f = \inf_{\leq}(\{c, f\}) = g$$

$$c \vee f = \sup_{\leq}(\{c, f\}) = a$$

$$c \vee d = e$$

$$b \vee e = b$$

$$b \wedge e = e$$

(ii)

není Hasseův diagram svazu!

Poznámka 4.5:

Nechť $(M, \leq)$ je svaz. Pokud $a, b, c \in M$, $a \leq c$, potom $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

DŮKAZ:

$$a \leq a \vee ba \leq c\,\} \Rightarrow a \leq (a \vee b) \wedge c$$

(nějaké nejlepší a **T-O-D-O:** nečitelné)

$$b \wedge c \leq b \leq a \vee ba \wedge c \leq c\,\} \Rightarrow (b \wedge c) \leq (a \vee b) \wedge c$$

Teď to dáme dohromady:

$$\Rightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$$

nejmenší
Q.E.D.

Definice:

Řekneme, že svaz $M(\wedge, \vee)$ je **modulární**, pokud $a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$.

T-O-D-O: a zase kus chybí

Poznámka 4.8:

Nechť $\mathcal{C}$ je uzávěrový systém ležící v množině všech ekvivalencí na A. Nechť $\mathcal{N} \in \mathcal{P}(A)$ a $e \in A$ tak, že:

(i) $\varrho \subset \mathcal{C} \Rightarrow [e]_\varrho \in \mathcal{N}$

(ii) $N \in \mathcal{N} \Rightarrow \exists\, \varrho \in \mathcal{C} : N = [e]_\varrho$

(iii) $[e]_\varrho \subseteq [e]_\mu$, bla $\varrho, \mu \in \mathcal{C} \Rightarrow \varrho \subseteq \mu$

Pak $\mathcal{N}$ je uzávěrový systém (tudíž dle V4.3- svaz) a zobrazení $\varphi\colon \mathcal{C} \to \mathcal{N}$ dané vztahem $\varphi(\varrho) = [e]_\varrho$ je svazový isomorfismus.

T-O-D-O: a zase velký kus chybí...;-)

Definice:

Nechť A, B jsou množiny a $\alpha\colon \mathcal{P}(A) \to \mathcal{P}(B)$, $\beta\colon \mathcal{P}(B) \to \mathcal{P}(A)$. řekneme, že α, β tvoří **Galoisovu korespondenci**, platí-li pro $\forall A_1, A_2 \in \mathcal{P}(A),\ B_1, B_2 \in \mathcal{P}(B)$:

(i) $A_1 \subseteq A_2 \Rightarrow \alpha(A_1) \supseteq \alpha(A_2)$
$V_1 \subseteq B_2 \Rightarrow \beta(B_1) \supseteq \beta(B_2)$

(ii) $A_1 \subseteq (\beta\alpha)(A_1)$, $B_1 \subseteq (\alpha\beta)(B_1)$

Poznámka 4.10:

Nechť $\alpha\colon \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta\colon \mathcal{P}(B) \to \mathcal{P}(A)$ je Galoisova korespondence. Pak $\beta\alpha$ (resp. $\alpha\beta$) je uzávěrový operátor na $\mathcal{P}(A)$ (resp. na $\mathcal{P}(B)$.

Buď $\mathcal{A}$ resp. $\mathcal{B}$ uzávěrové systémy příslušné $\beta\alpha$ resp. $\alpha\beta$. Dále $\alpha(\mathcal{A}) \subseteq \mathcal{B}$, $\beta(\mathcal{B}) \subseteq \mathcal{A}$.

Restrinkce α (resp. β) na $\mathcal{A}$ (resp. $\mathcal{B}$) (označíme $\alpha'\colon \mathcal{A} \to \mathcal{B}$, $\beta'\colon \mathcal{B} \to \mathcal{A}$) jsou vzájemně inverzní bijekce (mezi $\mathcal{A}$ a $\mathcal{B}$).

(Restrinkce == omezení) $f\colon C \to D$ $E \subseteq C$ $g = f \restriction E$ $g\colon E \to \begin{cases} D \\ f(E) \end{cases}$ $g(e) = f(e)$

DŮKAZ:

$\beta\alpha$ je uzávěrový operátor ($\alpha\beta$ symetricky).

(ii) $\Rightarrow a_1 \subseteq \beta\alpha(A_1)$ $A_1 \subseteq A_2 \overset{(1)?}{\Rightarrow} \alpha(A_1) \supseteq \alpha(A_2) \Rightarrow \beta\alpha(A_1) \subseteq \beta\alpha(A_2)$
? $(\beta\alpha)(\beta\alpha)(A_1) = \beta\alpha(A_1)$

$\beta\alpha(A_1) \Rightarrow \beta\alpha(\beta\alpha(A_1)) \supseteq \beta\alpha(A_2)$ $\alpha(A_1)(= B_1) \overset{(2)}{\Rightarrow} \alpha\beta(\alpha(A_1)) \supseteq \alpha(A_1) \overset{(1)}{\Rightarrow} \beta\alpha\beta\alpha(A_1) \subseteq \beta\alpha(A_1)$

$$\mathcal{A} = \{A_1 \in \mathcal{P}(A) : \beta\alpha(A_1) = A_1\}$$

$$\mathcal{B} = \{B_1 \in \mathcal{P}(B) : \alpha\beta(B_1) = B_1\}$$

? $\alpha(\mathcal{A}) \subseteq \mathcal{B}$ ($\beta(\mathcal{B}) \subseteq \mathcal{A}$ symetricky)
$A_1 \in \mathcal{A} \Rightarrow \beta\alpha(A_1) = A_1$
$\alpha\beta(\alpha(A_1)) = \alpha(\beta\alpha(A_2)) = \alpha(A_1) \Rightarrow \alpha(A_1) \in \mathcal{B}$
$\alpha'\beta'\colon \mathcal{B} \to \mathcal{B} \overset{?}{=} \mathrm{id}_{\mathcal{B}}$ $\beta'\alpha'\colon \mathcal{A} \to \mathcal{A} \overset{?}{=} \mathrm{id}_{\mathcal{A}}$
$\alpha'\beta'(B_1) = \alpha\beta(B_1) = B_1 \Rightarrow \alpha'\beta' = \mathrm{id}_{\mathcal{B}}$ $\alpha\beta(B_1) = B_1 \qquad \forall B_1 \in \mathcal{B}$
Q.E.D.

Příklad:

T-O-D-O: dopsat později

Grupy

Podívejme se na grupy nyní ještě jednou a tentokrát pořádně.

Mějme $G(\cdot, ^{-1}, 1)$. Řekneme, že jde o **grupu**, a 1 nazveme **neutrálním prvkem**, pokud $\cdot$ označuje binární operaci, $^{-1}$ unární, a platí

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

.

Poznámka 5.1:

Nechť $G(\cdot, ^{-1}, 1)$ a $H(\cdot, ^{-1}, 1)$ jsou dvě grupy a $f: G \to H$ je slučitelné s $\cdot$. Pak f je homomorfismus $G(\cdot, ^{-1}, 1)$ do $H(\cdot, ^{-1}, 1)$.

DŮKAZ:

Díky slučitelnosti s $\cdot$ platí:

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$$

$$f(1) = f(1) \cdot f(1)$$

$$(f(1) \cdot f(1)^{-1}) = f(1) \qquad f(1)^{-1} \in H$$

Tedy f je slučitelná s 1.

$$1 = f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

$$\Rightarrow (f(a))^{-1} = f(a^{-1}) \text{ (zprava vynásobím } f(a^{-1}))$$

Tedy je f slučitelná i s $^{-1}$.

Q.E.D.

Definice:

Nechť $G(\cdot, ^{-1}, 1)$ je grupa a $H, K \subseteq G$. Definujme si:

$$H \cdot K = \{h \cdot k : h \in H,\ k \in K\} \qquad h \in G$$

$$h \cdot K = \{h\} \cdot K \quad K \cdot h = K \cdot \{h\}$$

Zavedeme relace $r \bmod H \subseteq G \times G$ (resp. $l \bmod H \subseteq G \times G$) tak, že $(a, b) \in r \bmod H$ (resp. $\in l \bmod H$) definujeme jako $ab^{-1} \in H$ (resp. $a^{-1}b \in H$).

Poznámka 5.2:

Nechť $G(\cdot, ^{-1}, 1)$ je grupa a H její podgrupa. Pak platí pro $a, b \in G$:

(a) $r \bmod H$, $l \bmod H$ jsou ekvivalence na G

(b) $(a, b) \in r \bmod H \Leftrightarrow (a^{-1}, b^{-1}) \in l \bmod H$

(c) $|G/_{r \bmod H}| = |G/_{l \bmod H}|$

(d) $[a]_{r \bmod H} = Ha$, $[a]_{l \bmod H} = aH$

(e) $|H| = |[a]_{r \bmod H}| = |[a]_{l \bmod H}|$

DŮKAZ:

(a) (viz také V1.14-) $a^{-1}a = aa^{-1} = 1 \in H \Rightarrow r \bmod H$ $(l \bmod H)$ je reflexivní.
$ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow r \bmod H$ $(l \bmod H)$ je symetrická.

$$\left.\begin{array}{l} ab^{-1} \in H \\ bc^{-1} \in H \end{array}\right\} \Rightarrow ac^{-1} = (ab^{-1})(bc^{-1}) \in H$$

tedy $r \bmod H$ $(l \bmod H)$ je symetrická.

(b) Vezměme $(a,b) \in r \bmod H$. Z uzavřenosti H na $^{-1}$:

$$ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} \Rightarrow (b^{-1}, a^{-1}) \in l \bmod H \overset{\text{(a)}}{\Rightarrow} (a^{-1}, b^{-1}) \in l \bmod H$$

Zpětná implikace se dokáže symetricky.

(c) $G/_{r \bmod H} \overset{\text{f}}{\to} G/_{l \bmod H} \overset{\text{g}}{\to} G/_{r \bmod H}$:

$$[a]_{r \bmod H} \to [a^{-1}]_{l \bmod H} \quad [b]_{l \bmod H} \to [b^{-1}]_{l??? \bmod H}$$

Tedy fg i gf jsou identity. Z (b) tedy plyne korektnost definice f i g, a to takto:

$$[a_1]_{r \bmod H} = [a_2]_{r \bmod H} \Rightarrow (a_1, a_2) \in r \bmod H$$

ale (b) nám říká, že i $(a_1^{-1}, a_2^{-1}) \in l \bmod H$, tedy $f(a_1) = f(a_2)$.

(d) Podívejme se, čemu se vlastně rovná $[a]_{r \bmod H}$:

$$[a]_{r \bmod H} = \{x \in G : \underbrace{(a,x) \in r \bmod H}_{\Leftrightarrow ax^{-1} \in H}\} = \{x \in G : \exists h \in H,\ \underbrace{ax^{-1} = h}_{\substack{\Leftrightarrow a = hx \\ \Leftrightarrow h^{-1}a = x}}\} =$$

$$= \{x \in G : \exists h' \in H,\ h'a = x\} = Ha$$

(e) $H \overset{\text{b}}{\to} Ha$, $h \to ha$. Tvrdím, že b je na:

$$h_1 a = b(h_1) = b(h_2) = h_2 a$$

Pronásobením a^{-1} dostanu $h_1 = h_2$.

Q.E.D.

Definice:

$|G|$ říkáme **řád grupy**.
Indexem podgrupy H v G nazveme

$$[G : H] = |G/_{r \bmod H}| = |G/_{l \bmod H}|$$

VĚTA 5.3 (Lagrange):

Nechť $G(\cdot, ^{-1}, 1)$ je grupa a H je její podgrupa. Pak platí

$$|G| = |H| \cdot |G/_{r \bmod H}| = |H| \cdot |G/_{l \bmod H}| = |H| \cdot [G : H]$$

DŮKAZ:

Položme $G' = G/_{r \bmod H}$:

$$G = \left|\bigcup \{[g]_{r \bmod H} : [g]_{r \bmod H} \in G'\}\right| = \sum_{x \in G'} |x| \overset{\text{V5.2-(e)}}{=} \sum_{x \in G'} |H| = |H| \cdot |G/'|$$

Q.E.D.

Příklad:

Nechť S_4 je podgrupa permutací na čtyřech prvcích:

$$|S_4| = 4! = 24$$

tedy neexistují žádné podgrupy S_4 o patnácti nebo sedmi prvcích.

Definice:

$G(\cdot, ^{-1}, 1)$ buď grupa, $g \in G$, $n \in \mathbb{Z}$. Definujme umocňování:

(i) $g^0 = 1$
(ii) $g^n = g \cdot g^{n-1} \quad \forall n > 0$
(iii) $g^n = (g^{-1})^{-n} \quad \forall n < 0$

Poznámka 5.4:

Definujme zobrazení $f: \mathbb{Z} \to G$ tak, že vezmeme nějaké $g \in G$ a položíme $f(n) = g^n$. Pak f je homomorfismus grup $\mathbb{Z}(+, -, 0)$ a $G(\cdot, ^{-1}, 1)$.

DŮKAZ:

Stačí dokázat slučitelnost $+ \leftrightarrow \cdot$.

$$n = 0, m = 0 : f(n+m) = f(n) \cdot f(m)$$

$$n, m > 0 : f(n+m) = \underbrace{g \cdots g}_{n+m}$$

$$f(n) \cdot f(m) = \underbrace{(g \cdots g)}_{n} \cdot \underbrace{(g \cdots g)}_{m}$$

$$n + m \geq 0,\ n > 0 > m : f(n+m) = \underbrace{g \cdots g}_{n+m} = f(n) \cdot f(m)$$

$$f(n) \cdot f(m) = \underbrace{g \cdots (g}_{n} \cdot \underbrace{g^{-1}) \cdots g^{-1}}_{-m} = \underbrace{g \cdots g}_{n-(-m)} = f(n+m)$$

Q.E.D.

T-O-D-O: jedna a kousek přednášky

Okruhy a ideály

Definice:

O algebře $R(+,\cdot,-,0,1)$ řekneme, že je **okruhem**, pokud $R(+,-,0)$ je komutativní grupa, $R(\cdot,1)$ je monoid, a platí

$$\forall a,b,c \in R : a(b+c) = a\cdot b + a\cdot c \quad (a+b)\cdot c = a\cdot c + b\cdot c$$

Komutativní okruh má rovněž operaci $\cdot$ komutativní.

Příklady:

(i) $\mathbb{Z}(+,\cdot,-,0,1)$, $\mathbb{Z}_n(+,\cdot,-,0,1)$ — komutativní okruhy

(ii) T buď těleso, pak $T(+,\cdot,-,0,1)$ je okruh

(iii) V buď vektorový prostor nad tělesem T, $End(V) = \{f\colon V \to V : f\ T\text{-lineární }\}$:

$$0(v) = 0$$

$$[f+g](v) = f(v) + g(v)$$

$$[-f](v) = -f(v)$$

V takovém případě $End(V)(+,\cdot,0,\mathrm{id}_V)$ je okruh.

Značení

$R(+,\cdot,-,0,1)$ bude vždy okruh, $a,b \in \mathbb{R}$, $a-b = a+(-b)$.

Poznámka 6.1:

(i) $0\cdot a = a\cdot 0 = 0$

(ii) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$

(iii) $(-1)\cdot b = b\cdot(-1) = -b$

(iv) $(-a)\cdot(-b) = a\cdot b$

(v) $0 \neq 1 \Leftrightarrow |R| > 1$

DŮKAZ:

(i) $0\cdot a = (0+0)\cdot a = 0a + 0a \Rightarrow 0 = 0a$, symetricky $a\cdot 0 = 0$.

(ii) $(-a)\cdot b + a\cdot b = (-a+a)\cdot b = 0\cdot b = 0$

(iii) (ii) pro $a = 1$

(iv) $(-a)\cdot(-b) = -(a\cdot(-b)) = -(-a(a\cdot b)) = a\cdot b$

(v) $0 = 1 \Rightarrow \forall r \in R : r = r\cdot 1 = r\cdot 0 = 0$, tedy $R = \{0\}$

Q.E.D.

Definice:

Množina $I \subseteq R$ je **pravý** (resp. levý) **ideál** okruhu R, pokud I je podgrupa grupy $R(+,-,0)$ a platí

$$\forall i \in I,\ \forall r \in R : i \cdot r \in I$$

(resp. $r \cdot i \in I$). I je **ideál**, jde-li o pravý i levý ideál.

Příklady:

(i) $\{0\}$ a R jsou ideály každého okruhu R.

(ii) Ideály $\mathbb{Z}(+,\cdot,-,0,1)$ a $\mathbb{Z}_n(+,\cdot,-,0,1)$ jsou právě tvaru

$$k \cdot \mathbb{Z} = \{k \cdot x : x \in \mathbb{Z}\}$$

$$k \cdot \mathbb{Z}_n = \{k \cdot x : x \in \mathbb{Z}_n\}$$

$$k \cdot x \in k \cdot \mathbb{Z}$$

$$(k \cdot x) \cdot r = k \cdot (x \cdot r) \in k \cdot \mathbb{Z} \qquad \forall r \in \mathbb{Z}$$

(iii) R buď okruh, $a \in R$. Pak

$$aR = \{a \cdot r : r \in R\}$$

nazveme **hlavním pravým ideálem**,

$$Ra = \{r \cdot a : r \in R\}$$

nazveme **hlavním levým ideálem** daného prvku a.

VĚTA 6.2 ():

Nechť ϱ je relace na okruhu R. Pak ϱ je kongruence, právě když $[0]_\varrho$ je ideál. Navíc $(a,b) \in \varrho$, právě když $b - a \in [0]_p$.

Množina všech ideálů tvoří uzávěrový systém a svazy všech kongruencí na R a všech ideálů jsou isomorfní.

DŮKAZ:

$\mathcal{C}$ nechť jsou všechny kongruence na R a $\mathcal{N}$ množina všech ideálů. Mějme $\varphi(\varrho) = [0]_\varrho$.
Ověřujeme předpoklady V4.8-:

(i) ϱ je kongruence, je $[0]_\varrho$ ideál?
ϱ je kongruence na $R(+,-,0)$, což je komutativní grupa (tedy dle V1.13- je každá podgrupa normální). Podle V1.14- je $[0]_\varrho$ podgrupa $R(+,-,0)$. Neboť jde o kongruenci,

$$i \in [0]_\varrho : (i,0) \in \varrho \quad r \in R : (r,r) \in \varrho$$

$$\Rightarrow \begin{matrix} (i \cdot 0, 0 \cdot r) = (i \cdot 0, 0) \in \varrho \\ (r \cdot i, r \cdot 0) = (r \cdot i, 0) \in \varrho \end{matrix}$$

$$\Rightarrow r \cdot i, i \cdot r \in [0]_\varrho$$

$$\Rightarrow [0]_p \in \mathcal{N}$$

(ii) I je ideál, tzn. $(a,b) \in \varrho \Leftrightarrow b-a \in I$. I je normální podgrupa $R(+,-0)$, tedy dle V1.14- je ϱ kongruencí na $R(+,-,0)$, $[0]_\varrho = I$.
Zbývá dokázat slučitelnost ϱ s $\cdot$ a 1. $(1,1) \in \varrho$, bez problémů.

$$(r_1,s_1) \in \varrho \quad (r_2,s_2) \in \varrho$$

$$\Rightarrow \begin{matrix} s_1 - r_1 \in I \\ s_2 - r_2 \in I \end{matrix} \Rightarrow \begin{matrix} (s_1-r_1)\cdot s_2 \in I \\ r_1 \cdot (s_2 - r_2) \in I \end{matrix}$$

$$s_1 \cdot r_2 - r_1 \cdot s_2 = (s_1 - r_1)\cdot s_2 + r_1 \cdot (s_2 - r_1) \in I$$

$$\Rightarrow (r_1,r_2),(s_1,s_2) \in \varrho$$

(iii) Přímo z V1.14- plyne, že φ je prosté.

Tedy dle tvrzení V4.8- je φ isomorfismus svazů a $\mathcal{N}$ je uzávěrový systém (tj. svaz).
Q.E.D.

Značení

I je ideál, odpovídá mu jednoznačně (díky V6.2-) kongruence ϱ_I.

$$R/\varrho_I = R/I$$

Definice:

Řekneme, že prvek $a \in R$ je **invertibilní** v okruhu $R(+,\cdot,-,0,1)$, je-li invertibilní v $R(\cdot,1)$.

Poznámka 6.3:

$a \in R$ je invertibilní, právě když $aR = Ra = R$.

DŮKAZ:

"$\Rightarrow$"

$$\exists\, a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1$$

$$1 = a \cdot a^{-1} \in aR$$

$$1 = a^{-1} \cdot a \in Ra$$

$$\Rightarrow \forall r \in R : r = \begin{cases} r \cdot 1 \in Ra \\ 1 \cdot r \in aR \end{cases}$$

$$\Rightarrow R = Ra = aR$$

"$\Leftarrow$"

$$1 \in R = aR = Ra$$

$$\exists\, x \in R \quad y \in R : 1 = a \cdot x = y \cdot a \overset{\text{V1.10-}}{\Longrightarrow} x = y$$

a tedy a je invertibilní.

Q.E.D.