Algebra

Michal Vaner

2. ledna 2013

1 Kontakt

- www.karlin.mff.cuni.cz/˜zemlicka

2 Cíl přednášky

Objekt algebry je množina opatřená operacemi. Všechny objekty jednoduché.

Není praktická informatická přednáška, přednáška je strukturní.

- Množiny
- Operace
- Relace

3 Obecné pojmy

Buď A množina a $n \in \mathbb{N}_0$. ***Operací*** (parity n) rozumíme každé zobrazení $A^n \to A$.

Poznámka:
n může být i 0

Buď $\alpha_i; i \in I$ operace na množině A. Pak ***algebrou*** nazveme každou takovou uspořádonou dvojici $A\,(\alpha_i | i \in I)$.

Příklad:
$\mathbb{Z}\,(+, -, 0)$ - celá čísla se sčítáním, odčítáním (binární) a nulou (0-ární operace).

Těleso je algebra s $+, *, -, 0, 1$ a inverzní prvek pro vše kromě 0. $T\,(+, *)$ s nějakými dalšími vlastnostmi. Nebo také $T\,(+, *, -, 0, 1)$ a ještě inverzní prvek—Možnost více zápisů.

Buď A množina, $B \subset A$. Je-li α n-ární operace na A, řekneme že B je ***uzavřená*** na α platí, že $\forall b_1, b_2, \ldots, b_n \in B; \alpha\,(b_1, \ldots, b_n) \in B$.

Je-li $A(\alpha_i|i \in I)$ algebra, potom $B(\alpha_i|i \in I)$ nazveme ***podalgebrou*** algebry A, pokud $\forall \alpha_i|i \in I$ jsou uzavřené na B.

Buď $A(\alpha_i|i \in I)$ algebra a B je podalgebra. $\beta_i : B^{n_i} \to B$ je n-ární operace, $\beta_i(b_1, b_2, \ldots, b_n) = \alpha_i(b_1, b_2, \ldots, b_n)$. Podalgebra tvoří algebru.

Poznámka:
Buď $A(\alpha_i|i \in I)$ algebra a $B_j, j \in J$ nechť jsou podalgebry algebry A. Pak $\cap_{j \in J} B_j$ je opět podalgebry. Důkaz z definice - vzit n-tici, co leži všude, výsledek musí ležet všude. α je n-ární operace na množinách A a B a $f : A \to B$ zobrazení. f je ***slučitelné*** s operací α, jestliže $\forall a_1, \ldots, a_n \in A; f(\alpha(a_1, \ldots, a_n)) = \alpha(f(a_1), \ldots, f(a_n))$.

Nechť $A(\alpha_i, i \in I), B(\alpha_i, i \in I)$ jsou ***stejného typu***, pokud je α_i n_i-ární operace na A i na B. Zobrazení $f : A \to B$ nazýváme ***homomorfizmus*** (na algebrách A a B), je-li slučitelné se všemi operacemi α_i.

Mějme algebry A, B, C a homomorfizmy $f : A \to B$, $g : B \to C$. Pak $g \cdot f : A \to C$ je také homomorfizmus. Důkaz vypadal bez nápadu.

Buď A, B algebry stejného typu a $f : A \to B$ homomorfizmus a C podalgebra algebry A, D podalgebra algebry B. $f(C)$ je podalgebra algebry B a $f^{-1}(D)$ je podalgebra algebry A.

Buď ρ ekvivalence na množině A, pak ***faktorovou množinou*** A podle ρ rozumíme $A/\rho = \left\{ [a]_\rho | a \in A \right\}, [a]_\rho = \{b | b \in A, (a, b) \in \rho\}$.

Nechť ρ je ekvivalence na množině A. Pak A/ρ tvoří rozklad A. (Je-li $\{B_i | I \in J\}$ rozklad A, pak relace ρ daná vztahem $(a, b) \in \rho \Leftrightarrow \exists i \in I; a, b \in B$ je ekvivalence. Buď $f : A \to B$ zobrazení a ρ ekvivalence. Pak ***jádro*** je $\ker f = \{(a, b) \in A; f(a) = f(b)\}$. $\pi_\rho : A \to A/\rho$ je ***přirozená projekce***, které prvku a přiřadí rozkladovou třídu obsuhující a.

Nechť $f : A \to B$ je zobrazení a ρ je ekvivalence na A. Potom platí:

- Jádro zobrazení je ekvivalence.
- f je prosté $\Leftrightarrow \ker f =$ identita.
- $\ker \pi_\rho = \rho$
- Zobrazení $g : A/\rho \to B$ takové, že $\exists g \pi_\rho = f \Leftrightarrow \rho \subset \ker f$

Buď ρ ekvivalence na A, α je n-ární operace na A. Řekněme, že ρ je ***slučitelná*** s α, platí-li:

$$\forall a_1, \ldots, a_n, b_1, \ldots, b_n \in A; (a_i, b_i) \in \rho \Rightarrow (\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \rho$$

Řekneme, že ekvivalence ρ na algebře $A(\alpha_i)$ je ***kongurence***, jestliže ρ je slučitelná se všemi α_i.

Buď $f : A \to B$ homomorfizmus dvou algeber stejného typu (jiné homomorfizmy ani neuvažujeme). Potom $\ker f$ je kongurence na A.

Nechť $A\,(\alpha_i)$ je algebra a ρ je kongurence na A. Potom na A/ρ definujeme strukturu algebry tak, že vyberu z každé rozkladové třídy reprezentanta a vezmu to skrz ty α_i.

Definice struktury na A/ρ je korektní a je stejného typu jako na A.

Algebra $G(\cdot)$ nazveme ***grupoid*** je-li $\cdot$ binární operace. Prvek $e \in G$ nazveme ***neutrální prvek***, pokud $\forall g \in G; g \cdot e = e \cdot g = g$. Řekneme, že $G(\cdot, e)$ je ***monoid***, jestliže $\cdot$ je asociativní a e je neutrální prvek.

Podgrupoid (***podmonoid***) je podalgebra grupoidu (monoidu).

Každý grupoid obsahuje nejvýše jeden neutrální prvek. Je-li $S(\cdot, 1)$ monoid, potom platí $a^{-1} \in S$ pro nějaké $a \in S$ nazveme ***inverzním***, pokud $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

Prvek, pro který existuje inverzní prvek nazveme ***invertibilní***.

Poznámka:
Nechť $S(\cdot, 1)$ je monoid a označíme S^* množinu všech invertibilních prvků tohoto monoidu. Pak S^* je podmonoid monoidu $S(\cdot, 1)$. Navíc každý jeho prvek je invertibilní.

Algebru $G(\cdot, ^{-1}, 1)$ nazveme ***grupou***, je-li $(\cdot, 1)$ monoid a $^{-1}$ je unární operace $^{-1} : G \to G$, která každému prvku přiřadí inverzní prvek (tedy všechny prvky jsou invertibilní).

Komutativní (Abelova) grupa je taková grupa, jejíž $\cdot$ je komutativní.

Podgrupa je grupa, jejíž nosná množina je podmnožina jiné grupy.

Poznámka:
Nechť $S(\cdot, 1)$ je monoid a S^* je množina všech invertibilních prvků. Nechť $\odot$ je restrikce $\cdot$ na S^* a $^{-1}$ budiž operace inverzního prvku. $S^*(\odot, ^{-1}, 1)$ je grupa.

Všechny tyto operace jsou dobře definovány.

Normální podgrupa bude podgrupa splňující $\exists g \in G \forall h \in H; g \cdot h \cdot g^{-1} \in G$.

Poznámka:
Nechť $G(\cdot, ^{-1}, 1)$ je grupa a ρ je relace na G. Pak je ρ kongurence na G právě tehdy, když $[1]_\rho$ je te normální podgrupa G a $(g, h) \in \rho \Leftrightarrow g^{-1}h \in [1]_\rho$.

4 Uzávěrové systémy

Buď A množina. Řekneme, že $C \subset \mathcal{P}(A)$ (podmnožina systému podmnožin) je ***uzávěrový systém na*** A, platí li:

- $$A \in \mathcal{C}$$
- $$\mathcal{B} \subseteq \mathcal{C} \Rightarrow \bigcap_{B \in \mathcal{B}} \in \mathcal{C}$$

Uzávěrem v uzávěrovém systému budeme rozumět $d_{\mathcal{C}}\mathcal{P}(A) \to \mathcal{P}(A)$: $cl(x) = \{x \in \mathcal{C}; x \subset \mathcal{C}\}$.

Uzávěrovým operátorem na A budeme rozumět $\alpha : \mathcal{P}(A) \to \mathcal{P}$ splňující:

- $\forall B \subseteq A : B \subseteq \alpha(B)$ (Smí ale nemusí to zvětšit).
- $\forall B \subseteq A : \alpha(\alpha(B)) = \alpha(b)$
- $\forall B \subseteq C \subseteq A \Rightarrow \alpha(B) \subseteq \alpha(C)$

Věta:
Je-li $\mathcal{C}$ uzávěrový systém, pak $cl_{\mathcal{C}}$ je uzávěrovým operátorem. Je-li α uzávěrový operátor na množině A, pak množina $\mathcal{C}$, která obsahuje právě všechny pevné body ($\mathcal{C} := \{C \in \mathcal{P}(A); \alpha(C) = C\}$) je uzávěr. Navíc, když z uzávěrového systému udělám uzávěrový operátor a z něj zase uzávěrový systém, dostanu ten samý.

Důkaz:
Mějme uzávěrový systém. První podmínka je triviální. Druhou dokážu dvěma inkluzemi:

- $cl_{\mathcal{C}}(x) \subseteq cl_{\mathcal{C}}(cl_{\mathcal{C}}(x))$ dle první podmínky.
- Opačně: obsahuje $cl_{\mathcal{C}}$, dělá se přes všechno průnik, nemůže to být větší než toto.

Třetí podmínku: uvážím ty dvě množiny A a B. Zase přes průniky.

Nyní mějme uzávěrový operátor α. Chci dokázat, že $\mathcal{C} := \{C \in \mathcal{P}(A); \alpha(C) = C\}$ je uzávěrový systém. A tam zřejmě leží ($A \subseteq \alpha(A) \subseteq A$). Dále, nechť $\mathcal{B} \subseteq \mathcal{C}$. $\bigcap \mathcal{B} \subseteq B \forall B \in \mathcal{B}$, $\alpha(B) = B$, $\alpha(\bigcap \mathcal{B}) \subseteq \alpha(B) = B \Rightarrow \alpha(B) \subseteq \bigcap \mathcal{B}$. *TODO: Ještě opačným směrem.*

Nakonec, to že $\forall x \subset A; cl(x) = \alpha(x)$.

$$\bigcap \{c \in \mathcal{C}; x \subset C\} \subseteq \alpha(x) \Rightarrow \alpha(\alpha(x)) = \alpha(x)$$

$$x \subseteq C, C \in \mathcal{C}, \alpha(x) \subseteq \alpha(c) = C \Rightarrow \bigcap \{C \in \mathcal{C}; x \subseteq C\} = \left(\bigcap \{C \in \mathcal{C}; \alpha(x) \subseteq C\} \supseteq \alpha(x)\right)$$

Poznámka:
Systém všech uzávěrových systému na množině A tvoří uzávěrový systém na množině $\mathcal{P}(A)$.

Důkaz:
$\mathcal{C}$ jsou všechny uzávěrové systémy na A. $\mathcal{P}(A)$ je uzávěrový systém (zřejmé) – $\mathcal{P}(A) \in \mathcal{C}$.

$$\begin{aligned} \mathcal{B} \subseteq \mathcal{C} \quad &? \quad \bigcap \mathcal{B} \text{ je uzávěrový systém} \\ \forall \Gamma \in \mathcal{B} \quad &; \quad \Gamma \text{ je uzávěrový systém na } A \Rightarrow A \in \Gamma \\ &\Rightarrow \quad A \in \bigcap \mathcal{B} = \bigcap_{\Gamma \in \mathcal{B}} \Gamma \end{aligned}$$

$$\begin{aligned}
\Gamma_i \in \mathcal{B}, \mathcal{B} &= \{\Gamma_i; \forall i\} \\
B_j \in \bigcap \mathcal{B} &\rightarrow B_j \in \Gamma_i; \forall i, j \\
\bigcap B_j \in \Gamma_i & \quad \text{protože } \Gamma_i \text{ je uzávěrový systém} \\
\bigcap B_j \in \bigcap \Gamma_i &= \bigcap \mathcal{B}
\end{aligned}$$

Pozorování:
Jsou-li $\mathcal{A} \subseteq \mathcal{B}$ dva uzávěrové systémy na množině A a $C \subseteq D$, pak $cl_{\mathcal{B}}(C) \subseteq cl_{\mathcal{A}}(D)$.

Důkaz:

$$\begin{aligned}
cl_{\mathcal{B}}(C) &\subseteq cl_{\mathcal{B}}(D) \\
cl_{\mathcal{B}}(D) &\subseteq cl_{\mathcal{A}}(D)
\end{aligned}$$

Poznámka:
Množina všech reflexivních (symetrických, tranzitivních) relací na množině A, stejně jako ekvivalence na A tvoří uzávěrový systém na $A \times A$.

Důkaz:
$\mathcal{R}$ je množina všech reflexivních relací, $\mathcal{S}$ symetrických a $\mathcal{T}$ tranzitivních.

- $A \times A \in \mathcal{R}, \mathcal{S}, \mathcal{T}$
- Průnik nějakých reflexivných (obsahují identitu) také obsahuje identitu, tedy je také reflexivní.
- Pokud byly všechny symetrické, i jejich průnik je symetrický (pokud tam leželo nějaké (a, b), pak tam leží i (b, a)).
- Obdobně s tranzitivními.

Sloučením tohoto to získáme pro ekvivalence. Poznámka:
Množina všech kongurencí na algebře tvoří uzávěrový systém.

Důkaz:
α je nějaká operace na A. φ_α jsou všechny ekvivalence slučitelné s α. Z toho to skoro přímočaře plyne.

Poznámka:
$\mathcal{C}$ uzávěrový systém na A. $\rfloor\updownarrow_{\mathcal{C}}(X)$ je nejmenší (vzhledem k inkluzi) v $\mathcal{C}$

Nechť $A(\alpha_i)$ je algebra a $X \subseteq A/\rho \subseteq A \times A$, potom množina X ***generuje*** podalgebru $\rfloor\updownarrow_{\mathcal{A}}(x)$ (budu-li uvažovat relaci, pak generuje kongurenci $\rfloor\updownarrow_{\mathcal{C}}(\rho)$), kde $\mathcal{A}$ jsou všechny podalgebry a $\mathcal{C}$ všechny kongurence na algebře A.

Nechť f, g jsou dva homomorfizmy algeber $A \rightarrow B$ stejného typu a nechť X generuje A. $\forall x \in X; f(x) = g(x) \Rightarrow f = g$.

Každý bijektivní homomorfizmus se nazývá ***izomorfizmus***.

Buď ρ a σ nějaké operace. Operaci $\frac{\sigma}{\rho}$ na $\frac{A}{\rho}$ následující $([a]_\rho, [b]_\rho) \in \frac{\sigma}{\sigma} \equiv (a, b) \in \sigma$. Této ekvivalenci říkáme ***faktorová ekvivalence***.

Poznámka:
Buď ρ z kongurence na algebře A a σ je nějaká ekvivalence na A. Pak σ je kongurence na A, pokud $\frac{\sigma}{\rho}$ je kongurence na algebře A/ρ.

Věta o izomorfizmu:
Nechť $f : A \to B$ je homomorfizmus. Pak $f(A)$ je algebrou stejného typu jako algebry A, B, tedy $f(A) \subseteq B$ a $\frac{A}{\ker f} \cong f(A)$.

Důkaz:
f je homomorfizmus na $f(A)$. Použijeme $\rho := \ker f$. Tedy existuje homomorfizmus $g : \frac{A}{\ker f} \to f(A)$, který je izomorfizmus.

Druhá věta o izomorfizmu:
Nechť ρ a σ jsou kongurence na algebře A. Potom $\frac{\frac{A}{\rho}}{\frac{\sigma}{\rho}} \cong \frac{A}{\sigma}$. Tedy, faktory lze krátit.

5 Svazy

Relaci $\leq$ na množině S nazveme ***uspořádáním***, je-li:

- Reflexivní.
- Tranzitivní.
- Slabě antisymetrická:

$$\forall a, b \in S; a \leq b \wedge b \leq a \Rightarrow a = b$$

Poznámka:
Dovoluje i částečné uspořádání, tedy např. inkluze.

$s \in S$ je ***nejmenší prvek***, pokud

$$\forall a \in S; s \leq a$$

$s \in S$ je ***největší prvek***, pokud

$$\forall a \in S; a \leq s$$

Infimem množiny $A \subseteq S$ je největší prvek množiny $\{s \in S | \forall a \in A; s \leq A\}$.
Supremum je přesně naopak.

Množinu S nazveme ***svazem***, existuje-li infimum a supremum $\forall \{a, b\}, a, b \in S$.

Úplným svazem budeme rozumět svaz, kde existuje infimum a supremum $\forall A \subseteq S$.

Poznámka:
Konečné svazy lze reprezentovat nejen pomocí algeber, ale také pomocí grafů.

Poznámka:
Je-li M množina s uspořádáním $\leq$, pak infimum a supremum jednoprvkové množiny je ten jeden prvek sám.

Vlastnosti:
Nechť $(M, \leq, \wedge, \vee)$ je svaz. ($a \wedge b = \inf\{a, b\}, a \vee b = \sup\{a, b\}$.) Potom každé $\forall a, b, c \in M$ platí:

1. $$a \wedge b = b \wedge a, a \vee b = b \vee a$$
2. $$a = a \wedge a = a \vee a$$
3. $$a \wedge (b \wedge c) = (a \wedge b) \wedge c, a \vee (b \vee c) = (a \vee b) \vee c$$
4. $$a \vee (b \wedge a) = a, a \wedge (b \vee a) = a$$

Důkaz:

1. $$\{a, b\} = \{b, a\}$$
2. Triviální.
3. Z vlastností infima – dokážu, že $a \wedge (b \wedge c)$ je infimum trojice $\{a, b, c\}$ (a že existuje).
4. Z vlastností infima a suprema. Dokázat, že ta závorka je větší než infimum/menší než supremum.

Postačující podmínka:
Nechť $M(\wedge, \vee)$ je algebra s binárními operacemi $\wedge$ a $\vee$ splňující výše zmíněné podmínky ($\forall a, b, c \in M$).

Definujeme-li na M relaci $\leq$ předpisem $a \leq b \Leftrightarrow b = a \vee b$, pak $(M, \leq)$ je svazem, pro který platí, že $a \wedge b = \inf\{a, b\}$ a $a \vee b = \inf\{a, b\}$.

Důkaz:
Nejprve dokažme, že $b = a \vee b \Leftrightarrow a = a \wedge b$. Předpokládejme, že $b = a \vee b$ a chci zjistit, kolik je $a \wedge b$. Dosadím za b, tedy $a \wedge (a \vee b)$, na což vezmu vlastnosti a dostanu a. Opačně to lze dokázat stejně.

Dále dokážeme, že je to uspořádání.

- $$a \vee a = a \longrightarrow a \leq a$$
- $$a \leq b, b \leq c; a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c \longrightarrow a \leq c$$
- $$a \leq b, b \leq a; b = a \vee b = b \vee a = a \longrightarrow a = b$$

Nakonec dokážeme, že $a \vee b = \sup\{a, b\}$.

Věta:
Je-li C uzávěrový systém, pak $(\mathcal{C}, \subseteq)$ tvoří úplný svaz, kde $\inf_{\subseteq} \mathcal{B} = \bigcap \mathcal{B}$ a $\sup_{\subseteq} \mathcal{B} = d_{\mathcal{C}}(\bigcup \mathcal{B})$

Důkaz:
$\subseteq$ je zjevně uspořádání.
$\bigcap \mathcal{B} \subseteq B \forall B \in \mathcal{B} \longrightarrow \bigcap \mathcal{B} \in \mathcal{C}$. Nic většího už tam nacpat nejde $\Rightarrow$ je to infimum. Obdobně lze dokázat pro supremum.

Poznámka:
Je-li algebra $M(\wedge, \vee)$ svaz, pak i $M(\vee, \wedge)$ je svaz (a uspořádání je naopak).

Buď $(M, \leq)$ svaz. Řekneme, že a ***pokrývá*** b $(a \lessdot b)$, jestliže $a \leq b, a \neq b, a \leq c \leq b \Rightarrow (a = c) \vee (b = c)$. Tedy, jsou sousedé. *TODO: Zkontrolovat, jestli to pokrývání není naopak - b pokrývá a*

Nechť e je nejmenší prvek svazu a f nevětší prvek svazu, poté ***atomem (koatomem)*** nazvu každý prvek $a \in M$ $(c \in M)$, který splňuje, že $e \lessdot a$ $(c \lessdot f)$.

Hasseovým diagramem konečného svazu rozumím orientovaný graf, kde vrcholy odpovídají prvkům a hrana $a \to b$ je přítomná $\Leftrightarrow a \lessdot b$.

Poznámka:
Buď S svaz a $a, b, c \in S$.

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

Lze jednoduše odvodit z odhadů.

O svazu S řekneme, že je ***modulární***, jestliže $\forall a, b, c$ platí stejná podmínka jako výše, ale s rovností, tedy:

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

Buď $(A, \leq), (B, \leq)$ svazy a $f : A \to B$. f je ***monotónní***, platí-li implikace

$$a_1, a_2 \in A, a_1 \leq a_2 \Rightarrow f(a_1) \leq f(a_2)$$

(Mohli bychom nadefinovat i opačnou monotonii, která by byla nerostoucí místo neklesající.)

Poznámka:
Homomorfizmus svazů je monotónní. Je zřejmé z definice homomorfizmu.

O bijekci svazů:
Bijekce svazů f je izomorfizmus $\Leftrightarrow f, f^{-1}$ jsou monotónní zobrazení.

Důkaz:
Je-li f homomorfizmus, pak i f^{-1} je homomorfizmus, pak jsou oba monotónní.

Opačným směrem předpokládáme, že f i f^{-1} jsou monotónní. Stačí dokázat, že se chová hezky k jedné z operací. $a, b \leq a \vee b$. Když to proženu skrz f a f^{-1} a vyjde, že musí být stejné.

6 Grupy

Poznámka:
Buď $f : G \to H$, kde $G(\cdot,^{-1},1), H(\cdot,-1,1)$ jsou grupy slučitelné s $\cdot$. Pak je f homomorfizmus.

Důkaz:
$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ To jde vynásobit 1^{-1} z obou stran a musí to fungovat. Proto je to slučitelné na 1.

Také $f(1) = f(g \cdot g^{-1})$ a z toho ještě odvodíme slučitelnost pro $^{-1}$.

G je grupa, $H, K \subseteq G$ a $g \in G$. $HK = \{hk | h \in H, k \in K\}$, $gH = \{g\}\, H$, $Hg = H\, \{g\}$.

Relace na G pro každou podgrupu H:

- $rmodH : (a, b) \in rmodH \equiv a \cdot b^{-1} \in H$
- $lmodH : (a, b) \in lmodH \equiv a^{-1} \cdot b \in H$

Poznámka:
Buď G grupa a H její podgrupa. Pak platí:

- $rmodH$ a $lmodH$ jsou ekvivalence. (nemusí být kongurence)
- $$\forall a, b \in H; (a, b) \in rmodH \Leftrightarrow (a^{-1}, b^{-1}) \in lmodH$$
- $$\left|\frac{G}{rmodH}\right| = \left|\frac{G}{lmodH}\right|$$
- $$[a]_{rmodH} = Ha, [a]_{lmodH} = aH$$
- $$|H| = |[a]_{rmodH}| = |[a]_{lmodH}|$$

Řádem grupy nazveme počet jejích prvků.

La-Grangeova:
Je-li G grupa a H její podgrupa, pak řád grupy $|G| = [G : H] \cdot |H|$.

Důkaz:

$$|G| = \left| \overset{\circ}{\bigcup_{A \in rmodH}} A \right| = \sum_{A \in \frac{G}{rmodH}} |A| = \sum_{A \in \frac{G}{rmodH}} |H|$$

Důsledek:
Je-li G konečná grupa a H její podgrupa, pak $|H|/|G|$.

O grupě G řeknu, že je ***cyklická***, existuje-li $g \in G$, takové $\langle \{g\} \rangle = G$.

Poznámka:
Buď G grupa, $\varphi : \mathbb{Z} \to G$ takové, že $\varphi(z) = g^z$. Potom φ je homomorfizmus grup, $\varphi(\mathbb{Z}) = \langle g \rangle$.

Důsledek:
Je-li G grupa, $g \in G$ a $m, n \in \mathbb{Z}$, pak $\left(g^{-1}\right)^n = (g^n)^{-1}$ a $(g^n)^m = g^{n \cdot m}$.

Poznámka:
Nechť $A \subseteq \mathbb{Z}$. Pak A je podgrupa $\mathbb{Z}(+, -, 0) \Leftrightarrow \exists k \geq 0, k \in \mathbb{Z} : A = k \cdot \mathbb{Z}$.

Poznámka:
Nechť $A \subseteq \mathbb{Z}_n$. Pak je podgrupa grupy $\mathbb{Z}_n(+, -, 0) \Leftrightarrow \exists x \in \mathbb{Z}_n; k = 0 \vee (k|n \wedge A = k \cdot \mathbb{Z}_n)$.

Důkaz:
Vezmeme nejmenší kladný prvek, to už lze dokázat.

Věta:
Nechť $G(\cdot, ^{-1}, 1)$ je cyklická grupa. Je-li nekonečná, pak je izomorfní $G(\cdot, ^{-1}, 1) \cong \mathbb{Z}(+, -, 0)$. Pokud $n = |G|$ konečné, pak $G(\cdot, ^{-1}, 1) \cong \mathbb{Z}_n(+, -, 0)$.

Nechť $A_j(\alpha_i | i \in I)$ jsou algebry stejného typu, $j \in 1, \ldots, k$. Na kartézkém součinu $\prod_{j=1}^{k} A_j$ definujeme strukturu algebry stejného typu následovně: Je-li α_i n-ární operace, pak $\alpha_i(\prod A_j)^n \to \prod A_j$. Výsledek z k-tice hodnot součinu vezmu po složkách.

7 Okruhy a ideály

Algebru $R(+, \cdot, -, 0, 1)$ nazvu ***okruhem***, jestliže $R(+, -, 0)$ je komutativní grupa, $R(\cdot, 1)$ je monoid a platí:

- $\forall a, b, c \in R; a \cdot (b + c) = (a \cdot c) + (b \cdot c)$
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Komutativní okruh je okruh, jehož $\cdot$ je komutativní.

Poznámka:
Nechť $a, b \in R$. Pak platí:

- $0 \cdot a = a \cdot 0 = 0$
- $(-a) \cdot b = a(-b) = -(a \cdot b)$
- $(-1) \cdot b = b \cdot (-1) = -b$
- $(-a) \cdot (-b) = a \cdot b$
- $0 \neq 1 \Leftrightarrow |R| > 1$

Buď $I \subseteq R$. Řekneme, že I je ***pravý (levý) ideál*** okruhu, jestliže I je podgrupa $R(+, -, 0)$ a $\forall i \in I \forall r \in R : i \cdot r \in I, (r \cdot i \in I)$.

Ideálem nazveme takové I, které je zároveň pravým i levým ideálem. Někdy se mu říká také oboustranný ideál.

O kongurenci:
Množina všech ideálů tvoří uzávěrový systém a zobrazení $\rho \to [0]_\rho$ je izomorfizmus svazu všech kongurencí okruhu a ideálu na okruhu. Navíc $(a, b) \in \rho \Leftrightarrow b - a \in [0]_\rho$. ρ je kongurence $\Leftrightarrow$ je dána takovouto podmínkou.

7.0.1 Značení

- $R\,(+, \cdot, -, 0, 1)$ okruh
- I ideál
- ρ_I kongurence ideálu I
- Místo R/ρ_I budeme psát R/I

Invertibilní prvek okruhu $R(+, \cdot, -, 0, 1)$ rozumíme invertibilní prvek monoidu $R(, \cdot, 1)$.

Okruh nazveme ***tělesem***, jestliže je každý jeho nenulový prvek invertibilní.

Ideál I je ***maximální***, jestliže I je koatom v množině všech ideálů.

Věta:
Následující je pro okruh ekvivalentní

- $R(+, \cdot, -, 0, 1)$ je těleso
- $0, R$ jsou jediné pravé ideály okruhu
- $0, R$ jsou jediné levé ideály okruhu

Důkaz:
Nechť R je těleso. Pro nulu lze dokázat snadno, že je pravý ideál. Nyní si vezmeme nějaké I ideál $\neq \{0\}$. Proto je roven $0 + i$, $i \in I$. Dokážu, že jedna v tom ideálu leží, proto tam musí ležet všechny prvky toho R.

Pro levý ideál podobně.

Vezmu pravý i levý ideál jako R. Nyní dokážu, že každý jeho prvek je invertibilní kromě 0.

Věta:
Je-li $R(+, \cdot, -, 0, 1)$ komutativní okruh, I nechť je ideál. Pak faktorový okruh R/I. $R/I(+, \cdot, -, 0, 1)$ je těleso $\Leftrightarrow$ I je maximální okruh.

Důkaz:
J-ideál je koatom $\Leftrightarrow$ ρ_j je koatom.

Stačí dokázat, že R/I je těleso $\Leftrightarrow$ ρ_i je koatom ve svazu kongurencí na $R(+, \cdot, -, 01,)$.

Poznámka:
Definujme zobrazení $\varphi : \mathbb{Z} \to R$ předpisem $\varphi(n) = n \times 1$. Pak φ je okruhový koeficient $\mathbb{Z}(+, \cdot, -, 0, 1)$ a $R(+, \cdot, -, 0, 1)$. $\varphi(\mathbb{Z})$ je nejmenší podokruh R okruhu 1 a definuje právě jedno $p \in \mathbb{N}_0$ takové, že $\{n \in \mathbb{R} | \varphi(n) = 0\} = p \cdot \mathbb{Z}$.

Charakteristikou okruhu $R(+, \cdot, -, 0, -)$ rozumíme p z minulé poznámky.

Poznámka:
Nechť R je komutativní okruh. $a, b \in R, n \in \mathbb{N}$.

Pak $(a + b)^n = \sum_{i=0}^{n} \binom{n}{k} \times a^n \cdot b^{n-k}$.

Důkaz:
Stejně jako obyčejná binomická věta na reálných číslech – indukcí.

Důsledek:
R je komutativní okruh prvočíselné charakteristiky p. Pak zobrazení $R \to R : a \to a^p$ je okruhový homomorfizmus.

Důkaz:
Přes binomickou větu.

Poznámka:
Nechť $R(+, \cdot, -, 0, 1)$ je komutativní těleso a G je konečná podgrupa grupy $R - \{0\}$. Pak G je cyklická.

TODO: Tady něco chybí