Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Algebra I

Peter Černo, 2010
petercerno@gmail.com

Garant: Mgr. Jan Žemlička, Ph.D.
E-mail: Jan.Zemlicka@mff.cuni.cz
Domácí stránka: http://www.karlin.mff.cuni.cz/~zemlicka/

Anotace: Přednáška je věnována základním algebraickým pojmům a strukturám. Míní se tím zejména pojmy algebra, homomorfismus, kongruence, uspořádání, dělitelnost, a struktury jako svazy, monoidy, grupy, okruhy a tělesa. V kursu se též věnuje pozornost modulární aritmetice a konstrukci konečných těles.

Sylabus:

1. Monoidy, grupy a podgrupy. Faktorizace grup a normální podgrupy.
2. Cyklické grupy a RSA.
3. Základní pojmy univerzální algebry: algebra, homomorfismus, kongruence.
4. Svazy a Booleovy algebry.
5. Okruhy a ideály. Podílová tělesa. Konstrukce konečných těles.

Literatura:

1. G. Birkhoff a T. C. Bartee: Aplikovaná algebra, Alfa Bratislava, 1981
2. G. Birkhoff a S. MacLane: Algebra, Alfa Bratislava, 1973
3. A. Drápal: text přednášky na http://www.karlin.mff.cuni.cz/~drapal/skripta/
4. S. Lang, Algebra, 3rd ed. New York 2002, Springer.
5. S. MacLane, G. Birkhoff, Algebra 3rd ed, Providence 1999, AMS Chelsea publishing company.
6. J. Žemlička: skripta na http://www.karlin.mff.cuni.cz/~zemlicka/

01.10.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

www.karlin.mff.cuni.cz/~zemlicka
SKRIPTA DRÁPALA

DEF.: BUĎ A MNOŽINA A n NEZÁPORNÉ CELÉ ČÍSLO. OPERÁCIOU (ARITY n, n-ÁRNU) ROZUMIEME KAŽDÉ ZOBRAZENIE $A^n \to A$. ($n=0$ $A^0 = \{()\}$, $A^0 \to A$ URČ. KONŠTANTY)
BUĎ α_i, $i \in I$, OPERÁCIA NA MNOŽINE A. POTOM ALGEBROU $A(\alpha_i, i \in I)$ NAZÝVAME USP. DVOJICU

PRÍKLAD: $\mathbb{Z}(+)$, $\mathbb{Z}(+,-,0)$, $\mathbb{Z}(+,\cdot,-,0,1)$

T TELESO S OPERÁCIAMI $+,\cdot$, $T(+,\cdot)$, $T(+,\cdot,-,0,1)$.
T TELESO S OP. $+,\cdot$, BUĎ V VEKT. PRIESTOR S $+$, $\cdot t$ $\forall t \in T$, $V(+, \cdot t, t \in T)$

DEF.: BUĎ A MNOŽINA, $B \subseteq A$. KEĎ JE α n-ÁRNA OP. NA A. HOVORÍME, ŽE B JE UZAVRETÁ NA α, KEĎ PRE $\forall b_1, \dots, b_n \in B$: $\alpha(b_1, \dots, b_n) \in B$.
KEĎ JE $A(\alpha_i, i \in I)$ ALGEBROU, POTOM $B \subseteq A$ NAZÝVAME PODALGEBROU ALG. $A(\alpha_i, i \in I)$, KEĎ JE B UZAVRETÁ NA $\forall$ OPERÁCIE α_i.

PRÍKLADY: 1) $k \in \mathbb{Z}$, $k\mathbb{Z} = \{kz, z \in \mathbb{Z}\}$
$k\mathbb{Z}$ JE PODALGEBROU ALGEBRY $\mathbb{Z}(+)$, $\mathbb{Z}(+,-,0)$.
$\mathbb{Z}$ JE PODALGEBROU $\mathbb{Q}(+,\cdot)$, $\mathbb{Q}(+,\cdot,-,0,1)$.
$\{1\}$ JE PODALGEBROU $\mathbb{Z}(\cdot)$ ALE NIE $\mathbb{Z}(+)$.
PODPRIESTOR VEKTOROVÉHO PRIESTORU V JE PODALGEBROU ALGEBRY $V(+, \cdot t \ t \in T)$.
POZOR! $\emptyset$ JE PODALGEBROU $V(+, \cdot t \ t \in T)$ ALE $\emptyset$ NIE JE PODPRIESTOR V.

NECH $A(\lambda_i, i \in I)$ JE ALGEBRA A B JEJ PODALGEBRA.
NECH $\beta_i : B^{n_i} \to B$ JE DEF. $\beta_i(b_1, \dots, b_n) := \lambda_i(b_1, \dots, b_n)$.
ZREJME $B(\beta_i, i \in I)$ JE ALGEBRA.

POZNÁMKA: BUĎ $A(\lambda_i, i \in I)$ ALGEBRA, B_j, $j \in J$
NECH SÚ PODALGEBRY A.
POTOM $\bigcap B_j$ JE OPÄŤ PODALGEBRA. (DÔKAZ ZREJMÝ)

03.10.2007 Ut
PETER ČERNO

MAI062 EX: ALGEBRA I

NIE JE HODNOTENÁ DOCHÁDZKA
3 PÍSOMKY (MESIACOVÉ INTERVALY)
www.karlin.mff.cuni.cz/~zemlicka

EUKLIDOV ALGORITMUS NA HĽADANIE NAJVÄČŠIEHO SPOLOČNÉHO DELITEĽA

$a_0, a_1 \in \mathbb{N} \quad a_0 \geq a_1$

$a_n = a_{n-2} \bmod a_{n-1}$

PRÍKLAD: $\gcd(1554, 1050) = 42$
(a_0, a_1)

$a_2 = 1554 \bmod 1050 = 504$ 420
$a_3 = 1050 \bmod 504 = 42$ 462
$a_4 = 504 \bmod 42 = 0$ 504

SPÄTNÝ BEH EUKLIDOVHO ALGORITMU

VETA: $a_0, a_1 \in \mathbb{N}$ $a_0 \geq a_1$ $\exists x, y \in \mathbb{Z}$:
$\gcd(a_0, a_1) = x \cdot a_0 + y \cdot a_1$

$$a_k = a_{k-2} \bmod a_{k-1} = a_{k-2} - \underbrace{\left\lfloor \frac{a_{k-2}}{a_{k-1}} \right\rfloor}_{p_k} a_{k-1}$$

$$a_n = a_{n-2} - p_n a_{n-1}$$

$a_{n-4} - p_{n-2} a_{n-3}$ $\quad$ $a_{n-3} - p_{n-1} a_{n-2}$

1554
1050
504 = 1554 - 1050
42 = 1050 - 2.504
0

$42 = 1050 - 2.(1554 - 1050) = \underline{\underline{-2.1554 + 3.1050}}$

HW: VYMYSLIET REKURENTNÝ VZOREC NA HĽADANIE x, y

PRÍKLAD: NÁJDITE $x, y \in \mathbb{Z}$ TAK, ABY $3 = x.42 + y.81$

81
42
39 = 81 - 42
3 = 42 - 39 = 42 - (81 - 42) = $\underline{\underline{2.42 - 81}}$

$$\gcd(a_0, a_1) = \left(x_0 \pm k \frac{\mathrm{lcm}(a_0, a_1)}{a_0}\right) a_0 + \left(x_1 \mp k \frac{\mathrm{lcm}(a_0, a_1)}{a_1}\right) a_1$$

PRÍKLAD: NÁJDITE x A y TAK, ABY $5 = x.71 + y.93$

93
71
22 = 93 - 71
5 = 71 - 3.22
2 = 22 - 4.5
1 = 5 - 2.2 = 71 - 3.22 - 2.(22 - 4.5) =
0 = 71 - 5.22 + 8.5 =

= 71 - 5.(93 - 71) + 8.(71 - 3.22) =
= 6.71 - 5.93 + 8.71 - 24.22 =
= 14.71 - 5.93 - 24.(93 - 71) =
= 38.71 - 29.93 $\Rightarrow$ $5 = -145.93 + 190.71$

$\Rightarrow$ [redacted] $5 = +4.71 - 3.93$

03.10.2007
PETER ČERNO

MAI062 EX: ALGEBRA I

PRÍKLAD:

NECH $\gcd(a_0, a_1) = x_0 \cdot a_0 + y_0 a_1 =$
$= x_1 \cdot a_0 + y_1 \cdot a_1$

$a_0 (x_0 - x_1) + a_1 (y_0 - y_1) = 0$

HĽADÁME VŠETKY RIEŠENIA SÚSTAVY

$\xi a_0 + \eta \cdot a_1 = 0$

ZREJME $\left(-\frac{k a_1}{\gcd(a_0, a_1)}\right) \cdot a_0 + \left(\frac{k a_0}{\gcd(a_0, a_1)}\right) \cdot a_1 = 0$

PRÍKLAD: NÁJDITE VŠETKY x, y:

$10 = 215 x + 320 \cdot y$

320
215 :
$105 = 320 - 215$
$5 = 215 - 2 \cdot 105 = 215 - 2 \cdot (320 - 215) =$
$0 = 3 \cdot 215 - 2 \cdot 320$

$10 = 6 \cdot 215 - 4 \cdot 320 = \left(6 + k \cdot \frac{320}{5}\right) \cdot 215 - \left(4 + k \cdot \frac{215}{5}\right) \cdot 320$

$x = 6 + k \cdot 64$
$y = -4 - k \cdot 43$

PRÍKLAD: NÁJDITE 22^{-1} v $\mathbb{Z}_{101}$

$22 \cdot x + 101 \cdot y = 1$

$$\begin{array}{r} 22 \\ 23 \\ \hline 66 \\ 44 \\ \hline 506 \end{array}$$

$$\begin{array}{rl} 101 & \\ 22 & \\ 13 & = 101 - 4 \cdot 22 \\ 9 & = 22 - 13 \\ 4 & = 13 - 9 \\ 1 & = 9 - 2 \cdot 4 \\ 0 & \end{array}$$

$= 22 - 13 - 5 \cdot (13 - 11) =$

$= 22 - 6 \cdot 13 + 5 \cdot 11 =$

$= 22 - 6 \cdot (101 - 4 \cdot 22) + 5 \cdot (22 - 13) =$

$= 2222 - 6 \cdot 101 - 5 \cdot (101 - 4 \cdot 22) =$

$= 4 \cdot 22 - 11 \cdot 101$

$1 = 9 - 2 \cdot 4 = 22 - 13 - 2 \cdot (13 - 9) =$

$= 22 - 3 \cdot 13 + 2 \cdot (22 - 13) =$

$= 3 \cdot 22 - 5 \cdot (101 - 4 \cdot 22) =$

$= -5 \cdot 101 + 23 \cdot 22$

08.10.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

DEF.: NECH α (JEDNÝM SYMBOLOM OZNAČUJEME DVE OPERÁCIE) JE OPERÁCIA ARITY n NA MNOŽINÁCH A a B. A $f: A \to B$. HOVORÍME, ŽE f JE ZLUČITEĽNÉ (KOMPATIBILNÉ) S OPERÁCIOU α, KEĎ $\forall a_1, \dots, a_n \in A$

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

NECH $A(\alpha_i \mid i \in I)$, $B(\alpha_i, i \in I)$ SÚ ALGEBRY. HOVORÍME, ŽE SÚ ROVNAKÉHO TYPU, KEĎ α_i JE n_i-ARNÁ OPERÁCIA NA A I B.

O ZOBRAZENÍ $f: A \to B$ POVIEME, ŽE JE HOMOMORFIZMUS ALGEBIER $A(\alpha_i, i \in I)$, $B(\alpha_i, i \in I)$, KEĎ JE ZLUČITEĽNÉ SO VŠETKÝMI α_i.

PRÍKLADY: (1) $V_1(+, \cdot t)$, $V_2(+, \cdot t)$ SÚ VP NAD T. HOMOMORFIZMY ALGEBIER $V_1(+, \cdot t)$, $V_2(+, \cdot t)$ SÚ PRÁVE LINEÁRNE ZOBRAZENIA.

(2) det JE HOMOMORFIZMUS ALGEBIER $[M_n(T)](\cdot)$ A $T(\cdot)$
MNOŽINA ŠTVORCOVÝCH MATÍC Z $T^{n \times n}$.

det JE HOMOMORFIZMUS ALGEBIER $[M_n(T)](\cdot, \underbrace{I_n}_{1}, \underbrace{O_n}_{0})$ A $T(\cdot, 1, 0)$.

ZLUČITEĽNOSŤ S NULÁRNOU OPERÁCIOU $\det(I_n) = 1$

(3) $\Pi_n : \mathbb{Z} \to \mathbb{Z}_n$ $\Pi_n(z) \overset{\text{def}}{=} (z) \bmod n$ $n \geq 2$

Π_n JE HOMOMORFIZMUS $\mathbb{Z}(+, -, \cdot, 0, 1)$ A $\mathbb{Z}_n(+, -, \cdot, 0, 1)$.

POZNÁMKA: NECH $A(\alpha_i, i \in I)$, $B(\alpha_i, i \in I)$, $C(\alpha_i, i \in I)$ SÚ ALGEBRY ROVNAKÉHO TYPU A $f: A \to B$, $g: B \to C$ SÚ HOMOMORFIZMY, POTOM $g \circ f: A \to C$ JE HOMOMORFIZMUS. NAVYŠE KEĎ JE f BIJEKCIA, POTOM I f^{-1} JE HOMOMORFIZMUS.

DŮKAZ: α_i JE OPERÁCIA ARITY n_i

$$g \circ f\left(\alpha_i(a_1, \dots, a_{n_i})\right) = g\left[f\left(\alpha_i(a_1, \dots, a_{n_i})\right)\right] =$$

$$= g\left[\alpha_i\left(f(a_1), \dots f(a_{n_i})\right)\right] = \alpha_i\left(g \circ f(a_1), \dots, g \circ f(a_{n_i})\right) . \square$$

f JE BIJEKCIA $\Rightarrow$ EXISTUJE f^{-1} $\quad \forall b_1, \dots, b_n \in B$

$$f^{-1}\left(\alpha_i(b_1, \dots, b_{n_i})\right) =$$

$\exists a_i : f(a_i) = b_i$

$$= f^{-1}\left(\alpha_i\left(f(a_1), \dots, f(a_{n_i})\right)\right) =$$

$$= f^{-1}\left(f\left(\alpha_i(a_1, \dots, a_{n_i})\right)\right) = \alpha_i(a_1, \dots, a_{n_i}) =$$

$$= \alpha_i\left(f^{-1}(b_1), \dots, f^{-1}(b_{n_i})\right) . \square$$

POZNÁMKA: BUĎ $A(\alpha_i, i \in I)$, $B(\alpha_i, i \in I)$ ALGEBRY ROVNAKÉHO TYPU, $f: A \to B$ HOMOMORFIZMUS
A C BUĎ PODALGEBROU A, D PODALGEBROU B.
POTOM $f(C)$ JE PODALGEBROU B A ÚPLNÝ VZOR $f^{-1}(D) = \{a \in A, f(a) \in D\}$ JE PODALGEBROU A.
α_i JE ĽUBOVOĽNÁ OPERÁCIA ARITY n_i,

a) $b_1, \dots, b_{n_i} \in f(C)$, TJ. $\exists a_1, \dots, a_{n_i} \in C$
$f(a_i) = b_i$

$$\alpha_i(b_1, \dots, b_{n_i}) = \alpha_i\left(f(a_1), \dots, f(a_{n_i})\right) =$$

$$= f\underbrace{\left(\alpha_i(a_1, \dots, a_{n_i})\right)}_{\in C,\ C \text{ JE ALGEBRA}} \in f(C) . \square$$

b) $a_1, \dots, a_{n_i} \in f^{-1}(D)$ TJ. $f(a_i) \in D$

$$f\left(\alpha_i(a_1, \dots, a_{n_i})\right) = \alpha_i\left(f(a_1), \dots, f(a_{n_i})\right) \in D, \ D \text{ JE ALGEBRA}$$

$$\Rightarrow \alpha_i(a_1, \dots, a_{n_i}) \in f^{-1}(D) . \square$$

08.10.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

ÚZUS: KEĎ JE DANÁ ŠTRUKTÚRA $A(a_i, i \in I)$, BUDEME ČASTO HOVORIŤ ALGEBRA A NAMIESTO ALGEBRA $A(a_i, i \in I)$.

$\rho \subseteq A \times A$ NAZVEME RELÁCIOU NA A.
$(a,b) \in \rho$ BUDEME TIEŽ ZAPISOVAŤ $a \rho b$.
KEĎ ρ JE RELÁCIA NA A, $\rho^{-1} = \{(a,b) \in A \times A \mid (b,a) \in \rho\}$

$\rho^+ = \{(a,b) \in A \times A, \exists a_0, \dots, a_n \in A :$
$a = a_0, b = a_n, (a_i, a_{i+1}) \in \rho\}$

$id = \{(a,a), a \in A\}$

RELÁCIA ρ JE SYMETRICKÁ, REFLEXÍVNA, TRANZITÍVNA, KEĎ $\rho^{-1} \subseteq \rho$, $id \subseteq \rho$, $\rho^+ \subseteq \rho$

FAKTOR A PODĽA ρ JE $A/\rho = \{[a]_\rho, a \in A\}$, KDE
$[a]_\rho = \{b \in A, (a,b) \in \rho\}$

POZNÁMKA: 1) NECH η JE EKVIVALENCIA NA MNOŽINE A.
POTOM A/η TVORÍ ROZKLAD A.
2) KEĎ JE $\{B_i, i \in I\}$ ROZKLAD A, T.J. $B_i \cap B_j = \emptyset$, $\bigcup B_i = A$.
POTOM $(a,b) \in \eta \Leftrightarrow \exists i \in I, a,b \in B_i$ DEF. EKVIVALENCIE

10.10.2007 We
PETER ČERNO

EX: MAI062 ALGEBRA I

PRÍKLAD: DOKÁŽTE SPRÁVNOSŤ EUKLIDOVHO ALGORITMU

$a \leq b \quad gcd(a,b) = gcd(a, b-a)$

$d \mid a, b \Leftrightarrow d \mid a, b-a$

PRE POLYNÓMY

$$a_{i+1} = a_{i-1} - p_i a_i$$

NECH $c = gcd(a_i, a_{i+1})$, TJ. $c \mid a_i, a_{i+1}$

KEĎŽE $a_{i-1} = a_{i+1} + p_i a_i \Rightarrow c \mid a_{i-1} \Rightarrow c \mid gcd(a_{i-1}, a_i)$

NAOPAK, NECH $d = gcd(a_{i-1}, a_i)$, TJ. $d \mid a_{i-1}, a_i$

KEĎŽE $a_{i+1} = a_{i-1} - p_i a_i \Rightarrow d \mid a_{i+1} \Rightarrow d \mid gcd(a_i, a_{i+1})$

$c \mid d \wedge d \mid c \Rightarrow c = d.$

PRÍKLAD:

$$a_i = x_i a_0 + y_i a_1$$

$$a_0 = 1 \cdot a_0 + 0 \cdot a_1$$

$$a_1 = 0 \cdot a_0 + 1 \cdot a_1$$

$$a_{i+1} = a_{i-1} - p_i a_i = \left(x_{i-1} a_0 + y_{i-1} a_1\right) - p_i \left(x_i a_0 + y_i a_1\right) =$$

$$= \underbrace{\left(x_{i-1} - p_i x_i\right)}_{x_{i+1}} a_0 + \underbrace{\left(y_{i-1} - p_i y_i\right)}_{y_{i+1}} a_1$$

PRÍKLAD: $\mathbb{R}[x]$ REÁLNE POLYNÓMY

$id \quad x \mapsto x$

...

$x \mapsto \sum_{i=0}^{n} a_i x^i$

PODOBNE PRE TELESO T $T[x]$

= VŠETKY KONEČNÉ POSTUPNOSTI S PRVKAMI Z TELESA

$+, \cdot$ BINÁRNE OPERÁCIE, KOMUTATÍVNE, ASOCIATÍVNE OPERÁCIE NA $T[x]$.

ASOCIATIVITA $\left[\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right)\right]\left(\sum_k c_k x^k\right) =$

$= \left[\sum_i \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i\right]\left(\sum_k c_k x^k\right) =$

$= \sum_i \left[\sum_{j=0}^{i} \left(\left(\sum_{k=0}^{j} a_k b_{j-k}\right) c_{i-j}\right)\right] x^i$

$= \sum_i \left(\sum_{j=0}^{i} \sum_{k=0}^{j} a_k b_{j-k} c_{i-j}\right) x^i$

$k = r$, $j - k = s$, $i - j = t$ $\leftrightarrow$ $k = r$, $j = s + r$, $i = t + s + r$

$\left(\sum_i a_i x^i\right)\left[\left(\sum_j b_j x^j\right)\left(\sum_k c_k x^k\right)\right] =$

$= \left(\sum_i a_i x^i\right)\left[\sum_j \left(\sum_{k=0}^{j} b_k c_{j-k}\right) x^j\right] =$

$= \sum_i \left[\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right] x^i =$

$= \sum_i \left(\sum_{j=0}^{i} \sum_{k=0}^{i-j} a_j b_k c_{i-j-k}\right) x^i$

$\rightarrow \sum_{r,s,t \in \mathbb{N}_0,\ r+s+t=i} a_r b_s c_t$

$j = r$, $k = s$, $i - j - k = t$ $\leftrightarrow$ $j = r$, $k = s$, $i = r + s + t$

PODOBNE DISTRIBUTIVITA

15.10.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

DEF.: BUĎ $f: A \to B$ ZOBRAZENIE A ρ EKVIVALENCIA NA A

$\ker f = \{ (a_1, a_2) \in A \times A \mid f(a) = f(b) \}$ JADRO ZOBRAZENIA f.

$\Pi_\rho : A \to A|_\rho$ NECH JE PRIRODZENÁ PROJEKCIA:

$\Pi_\rho(a) = [a]_\rho$

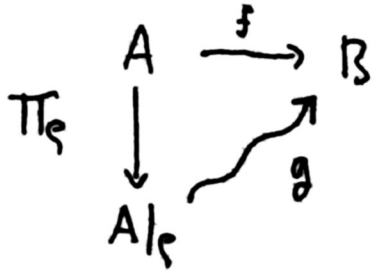
POZNÁMKA: NECH $f: A \to B$ JE ZOBRAZENIE A ρ EKVIVALENCIA NA A. POTOM PLATÍ:

(1) $\ker f$ JE EKVIVALENCIA

(2) f JE PROSTÉ $\Leftrightarrow \ker f = id_A$

(3) $\ker \Pi_\rho = \rho$

(4) ZOBRAZENIE $g: A|_\rho \to B$ EXISTUJE TAKÉ, ŽE $g \cdot \Pi_\rho = f$ EXISTUJE $\Leftrightarrow \rho \subseteq \ker f$



DŮKAZ. (1), (2) SÚ ZREJMÉ $[a_1]_\rho = [a_2]_\rho$

(3) $\ker \Pi_\rho = \{ (a_1, a_2) \in A \times A \mid \Pi_\rho(a_1) = \Pi_\rho(a_2) \}$

$(a_1, a_2) \in \rho \Rightarrow [a_1]_\rho = [a_2]_\rho \Rightarrow (a_1, a_2) \in \ker \Pi_\rho$

NAOPAK $(a_1, a_2) \in \ker \Pi_\rho \Rightarrow [a_1]_\rho = [a_2]_\rho \Rightarrow (a_1, a_2) \in \rho$.

(4) $\Rightarrow$) NECH $g: A|_\rho \to B : g \cdot \Pi_\rho = f$.

KEĎ $(a_1, a_2) \in \rho \Rightarrow g \cdot \Pi_\rho(a_1) = g([a_1]_\rho) =$

$= g \cdot \Pi_\rho(a_2) = g([a_2]_\rho)$

$\Rightarrow f(a_1) = f(a_2) \Rightarrow (a_1, a_2) \in \ker f$

$\Leftarrow$) NECH $\rho \subseteq \ker f$ NÁJDITE $g: A/\rho \to B$:
$g \circ \Pi_\rho = f$.

DEFINUJEME $g([a]_\rho) := f(a)$ PRE $\forall a \in A$.

DOKÁŽEME, ŽE g JE DEF. KOREKTNE:

NECH $(a_1, a_2) \in \rho$, TJ. $[a_1]_\rho = [a_2]_\rho$.

POTOM, KEĎŽE $(a_1, a_2) \in \ker f$, NUTNE $f(a_1) = f(a_2)$. ✓

NECH $a \in A$. POTOM $g \circ \Pi_\rho(a) = g([a]_\rho) = f(a)$,
TJ. $g \circ \Pi_\rho = f$. ■

DEFINÍCIA: BUĎ ρ <u>EKVIVALENCIA</u> NA MNOŽINE A,
α JE n-ÁRNA OPERÁCIA NA A. HOVORÍME, ŽE
ρ JE ZLUČITEĽNÁ S α, KEĎ PLATÍ
$\forall (a_1, \dots, a_n), (b_1, \dots, b_n) \in A^n$,
KEĎ PRE $\forall i$ $(a_i, b_i) \in \rho$, POTOM
$(\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \rho$

HOVORÍME, ŽE EKVIVALENCIA ρ NA MNOŽINE A.
JE KONGRUENCIA, KEĎ JE NA ALGEBRE $A(\alpha_i, i \in I)$
ZLUČITEĽNÁ S KAŽDOU OPERÁCIOU α_i

POZNÁMKA: NECH $f: A \to B$ JE HOMOMORFIZMUS
DVOCH ALGEBIER (NUTNE ROVNAKÉHO TYPU).
POTOM $\ker f$ JE KONGRUENCIA NA A.

DÔKAZ: ZREJME $\ker f$ JE EKVIVALENCIA.
NECH α JE NEJAKÁ OPERÁCIA NA A I NA B. (SAMOZREJME)
NECH $a_1, \dots, a_n, b_1, \dots, b_n \in A$, $(a_i, b_i) \in \ker f$ $\forall i \in \{1, \dots, n\}$,
TJ. $f(a_i) = f(b_i)$ PRE $\forall i \in \{1, \dots, n\}$

$$f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) = \alpha(f(b_1), \dots, f(b_n)) =$$
$$= f(\alpha(b_1, \dots, b_n)) \Rightarrow (\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \ker f.$$ ■

15.10.2007 Tb
PETER ČERNO

MAI062 ALGEBRA I

DEFINÍCIA: NECH $A(\alpha_i, i \in I)$ JE ALGEBRA A ϱ NECH JE KONGRUENCIA NA A.
POTOM NA A/ϱ DEFINUJEME ŠTRUKTÚRU ALGEBRY:
$\forall i \in I \quad \alpha_i([a_1]_\varrho, \dots [a_{n_i}]_\varrho) := [\alpha_i(a_1, \dots, a_n)]_\varrho$,
KDE n_i JE ARITA OPERÁCIE α_i.
(OPÄŤ ZNAČÍME OPERÁCIE ALGEBIER A AJ A/ϱ ROVNAKÝMI SYMBOLMI ...)

VETA: DEFINÍCIA ŠTRUKTÚRY ALGEBRY NA A/ϱ JE KOREKTNÁ, ALGEBRA $A/\varrho(\alpha_i, i \in I)$ JE ROVNAKÉHO TYPU AKO $A(\alpha_i, i \in I)$.
PRIRODZENÁ PROJEKCIA Π_ϱ JE HOMOMORFIZMUS.

DÔKAZ: KOREKTNOSŤ DEFINÍCIE:
NECH $[a_j]_\varrho = [b_j]_\varrho$ PRE $j = 1, \dots, n_i$
TJ. $(a_j, b_j) \in \varrho$ PRE $\forall j \in \{1, \dots, n_i\}$
$\alpha_i([a_1]_\varrho, \dots, [a_n]_\varrho) = [\alpha(a_1, \dots, a_n)]_\varrho$
$\alpha_i([b_1]_\varrho, \dots, [b_n]_\varrho) = [\alpha(b_1, \dots, b_n)]_\varrho$
(PODĽA DEF. KONGRUENCIE)
PRIČOM VIEME, ŽE: $(\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \varrho$,
TAKŽE $[\alpha(a_1, \dots, a_n)]_\varrho = [\alpha(b_1, \dots, b_n)]_\varrho$.

DOKÁŽEME, ŽE Π_ϱ JE HOMOMORFIZMUS.
NECH $a_1, \dots, a_{n_i} \in A$.
$\Pi_\varrho(\alpha_i(a_1, \dots, a_{n_i})) = [\alpha_i(a_1, \dots, a_{n_i})]_\varrho =$ (PODĽA DEF.)
$= \alpha_i([a_1]_\varrho, \dots, [a_{n_i}]_\varrho) =$
$= \alpha_i(\Pi_\varrho(a_1), \dots, \Pi_\varrho(a_{n_i}))$. ∎

PRÍKLAD: $\mathbb{Z}(+,-,\cdot)$. ZVOLME $n \in \mathbb{N}$, $n \geq 1$.
NECH $a, b \in \mathbb{Z}$. DEFINUJME $a \sim_n b \Leftrightarrow n \mid (a-b)$
ZREJME $\sim_n$ JE EKVIVALENCIA.
ĎALEJ $\sim_n$ JE ZLÚČITEĽNÁ S $+$:
NECH $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $a_1 \sim_n b_1$, $a_2 \sim_n b_2$.
TJ. $n \mid (a_1 - b_1)$, $n \mid (a_2 - b_2)$
$\Rightarrow n \mid (a_1 + a_2) - (b_1 + b_2)$ TJ. $a_1 + a_2 \sim_n b_1 + b_2$
PODOBNE PRE $-$ A $\cdot$.

UVAŽUJME ALGEBRU $\mathbb{Z}|_{\sim_n}(+,-,\cdot)$.
ZREJME $\mathbb{Z}|_{\sim_n} = \{[0]_{\sim_n}, \ldots [n-1]_{\sim_n}\} =$
$= \{[a]_{\sim_n} \mid a \in \mathbb{Z}_n\}$

$$[a]_{\sim_n} + [b]_{\sim_n} = [a+b]_{\sim_n} = [(a+b) \bmod n]_{\sim_n}$$

TOTO SÚ V KONGRUENCIE NA $\mathbb{Z}(+,-,\cdot)$
(NETRIVIÁLNE DOKÁZAŤ)

PRÍKLAD: NECH $A(d_i, i \in I)$ JE ALGEBRA,
POTOM id_A AJ $A \times A$ SÚ KONGRUENCIE

PRÍKLAD: NECH A JE MNOŽINA $+$ JE NULÁRNA OP.
NECH ϱ JE EKVIVALENCIA. POTOM ϱ JE
ZLÚČITEĽNÁ S e. $(e, e) \in \varrho$

PRÍKLAD: SÚ $\sim_n$ KONGRUENCIE AJ NA $\mathbb{Z}(+,-,0,1)$?
ÁNO :).

15.10.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

DEFINÍCIA: ALGEBRU $G(\cdot)$ NAZÝVAME GRUPOIDOM, KEĎ JE $\cdot$ BINÁRNA OPERÁCIA.

PRVOK $e \in G$ NAZÝVAME NEUTRÁLNYM PRVKOM OPERÁCIE (GRUPOIDU), KEĎ

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

HOVORÍME, ŽE ALGEBRA $G(\cdot, e)$ (JE MONOID), KEĎ JE:

- ASOCIATÍVNA BINÁRNA OPERÁCIA, TJ.:

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

PODGRUPOID (PODMONOID) JE PODALGEBROU GRUPOIDU (MONOIDU).

POZNÁMKA: MONOID MÁ VEĽMI BLÍZKO K POLOGRUPE.

POZNÁMKA: BUĎ $G(\cdot)$ GRUPOID A e, f JEHO DVA NEUTRÁLNE PRVKY. POTOM $e = f$.

KAŽDÝ GRUPOID OBSAHUJE NAJVIAC JEDEN NEUTRÁLNY PRVOK.

DÔKAZ: f JE NEUTRÁLNY, T.J. $e = e \cdot f$
e JE NEUTRÁLNY, TAKŽE $e \cdot f = f$
$\Rightarrow e = f$.

PRÍKLAD: NECH G JE ĽUBOVOĽNÁ MNOŽINA, KTORÁ MÁ ASPOŇ 2 PRVKY. DEFINUJME $a * b := a$.
POTOM $G(*)$ NEOBSAHUJE ŽIADEN NEUTRÁLNY PRVOK.

17.10.2007 Vk
PETER ČERNO

EX: MAI062 ALGEBRA I

PRÍKLAD: NAD TELESOM T NÁJDITE POLYNÓM $p \in T[x]$ TAK, ABY $a = b \cdot p + r$, KDE $a, b \in T[x]$, $st(r) < st(b)$.

$st\left(\sum_{i=0}^{n} a_i x^i\right) = \max\{ i \in \mathbb{N}_0 \mid a_i \neq 0 \}$ KDE $b \neq 0$

$st(0) = st\left(\sum_{i=0}^{\infty} 0 x^i\right) = -1$

a) $T = \mathbb{Z}_2$ $a = x^4 + x + 1$, $b = x^2 + 1$

$$\begin{array}{l} x^4 + x + 1 : x^2 + 1 = x^2 + 1 \\ -\ x^4 + x^2 \\ \hline x^2 + x + 1 \\ -\ x^2 + 1 \\ \hline x \end{array}$$

$$\underbrace{x^4 + x + 1}_{a} = \underbrace{(x^2 + 1)}_{b}\underbrace{(x^2 + 1)}_{p} + \underbrace{x}_{r}$$

b) $T = \mathbb{Z}_2$ $a = x^5 + x^3 + x$, $b = x^4 + x^2 + 1$

$$x^5 + x^3 + x = (x^4 + x^2 + 1) \cdot x + 0$$

c) $T = \mathbb{Z}_2$ $a = x^5 + x + 1$ $b = x^3 + x^2 + 1$

$$\begin{array}{l} x^5 + x + 1 : x^3 + x^2 + 1 = x^2 + x + 1 \\ x^5 + x^4 + x^2 \\ \hline x^4 + x^2 + x + 1 \\ x^4 + x^3 + x \\ \hline x^3 + x^2 + 1 \\ x^3 + x^2 + 1 \\ \hline 0 \end{array}$$

d) $T = \mathbb{Z}_5 \quad a = 2x^3 + 3x + 4 \quad b = 3x^3 + 2$

$2x^3 + 3x + 4 : 3x^3 + 2 = 4$
$2x^3 + 3$
$3x + 1$

$3x^3 + 2 : 3x + 1 = 4x^2 + 3x + 4$
$3x^3 + x^2$
$4x^2 + 2$
$4x^2 + 3x$
$2x + 2$
$2x + 4$
3

PRÍKLAD: DELENIE SO ~~ZBYTKOM~~ ZVYŠKOM

$DSZ\left(\underbrace{\sum_{i \in \mathbb{N}_0} a_i x^i}_{\alpha}, s_a, \underbrace{\sum_{i \in \mathbb{N}_0} b_i x^i}_{\beta}, s_b\right)$

if $s_a < s_b$ then return $(p = 0, r = \alpha)$
else $w := (a_{s_a} \cdot b_{s_b}^{-1}) \times^{s_a - s_b}$
$zv := \alpha - w \cdot \beta$
~~return~~ $(p', r') := DSZ(zv, \beta)$
return $(w + p', r')$

17.10.2007 Ut
PETER ČERNO

EX: MA1062 ALGEBRA I

PRÍKLAD: EUKLIDOV ALGORITMUS NAD $T[x]$ FUNGUJE ROVNAKO, PO KONEČNOM POČTE KROKOV SKONČÍ A NÁJDE NAJVÄČŠÍ SPOLOČNÝ DELITEĽ DVOCH POLYNÓMOV

PRÍKLAD: NÁJDITE NAJVÄČŠIEHO SPOLOČNÉHO DELITEĽA $\gcd(2x^3+3x+4, 3x^3+2)$ V ALGEBRE $\mathbb{Z}_5[x]$.
a_0 a_1

$a_2 = 3x+1$

$a_3 = 3$

$\rightsquigarrow \gcd(2x^3+3x+4, 3x^3+2) = 1.$

NÁJDITE POLYNÓMY $\xi, \eta \in \mathbb{Z}_5[x]$ TAKÍ, ABY

$\xi(2x^3+3x+4) + \eta(3x^3+2) = 1.$

$2x^3+3x+4 = (3x^3+2)\cdot 4 + 3x+1$

$3x^3+2 = (x^2+3x+4)\cdot(3x+1) + 3$

$3 = (3x^2+2) - (x^2+3x+4)(3x+1) =$

$= (3x^2+2) - (x^2+3x+4)[(2x^3+3x+4) - 4(3x^3+2)] =$

$= (4x^2+2x+1)(2x^3+3x+4) +$

$+ (1+4x^2+2x+1)(3x^3+2) =$

$= (4x^2+2x+1)(2x^3+3x+4) + (4x^2+2x+2)(3x^3+2)$

$\Rightarrow 1 = \overbrace{(3x^2+4x+2)}^{\xi}(2x^3+3x+4) + \overbrace{(3x^2+4x+4)}^{\eta}(3x^3+2)$

$+ 4x^5 + 4x^4 + 2x^3 + 3x^4 + 2x^3 + x^2 + 4x^3 + 4x + 3 +$

$+ 4x^5 + x^3 + 2x^4 + 3x^2 + 2x^3 + 3 = 1$

PRÍKLAD: NECH p JE POLYNÓM NAD TELESOM T. HOVORÍME, ŽE p JE NEROZLOŽITEĽNÝ, KEĎ

$$p = a \cdot b \,,\ a,b \in T[x] \Rightarrow st\,a = st\,p \ \vee\ st\,b = st\,p.$$

KEĎ JE $p \in T[x]$ NEROZLOŽITEĽNÝ

$q \in T[x]$, $st\,q < st\,p$.

OTÁZKA: $gcd(p,q) = ?$

PLATÍ $st(a \cdot b) = st(a) + st(b) \qquad a,b \neq 0$

$\Rightarrow gcd(p,q) = 1.$

$\exists \xi, \eta \in T[x] : \ 1 = \xi p + \eta q$

PRÍKLAD: NÁJDITE NEROZLOŽITEĽNÝ POLYNÓM STUPŇA 3 NAD $\mathbb{Z}_2$.

KEĎ JE p ROZLOŽITEĽNÝ, T.J. $p = a \cdot b$,

$st(a), st(b) < 3$

$\Rightarrow$ BUNO $st(a) = 1$, $st(b) = 2$

$a = \alpha x + \beta$ PRE $x = -\alpha^{-1}\beta$ JE $a(x) = 0$

$\Rightarrow p(-\alpha^{-1}\beta) = 0.$ $\Rightarrow$ EXISTUJE KOREŇ !!

$p_1 = x^3 + x + 1$ A $p_2 = x^3 + x^2 + 1$

SÚ NEROZLOŽITEĽNÉ.

PRÍKLAD: PRE $T[x]$ NECH p JE NEROZLOŽITEĽNÝ POLYNÓM Z $T[x]$. ZAVEDIEME RELÁCIU $\sim_p$

$a \sim_p b \Leftrightarrow p \mid a - b$ PRE $a,b \in T[x]$

$\sim_p$ JE KONGRUENCIA NA ALGEBRE $T[x](+,-,\cdot)$. ??

22.10.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

PRÍKLADY: (1) X množina písmen
$M(X)$ množina všetkých konečných postupností skladajúcich sa z písmen z X.
pre $x_1, \dots, x_k \in X$ píšeme namiesto $(x_1, \dots, x_k)$ kratšie $x_1 \dots x_k$
definujeme bin. operáciu $\cdot$
$x_1 \dots x_k \cdot y_1 \dots y_\ell := x_1 \dots x_k y_1 \dots y_\ell$
~ λ nech je prázdna postupnosť
$M(X)(\cdot, \lambda)$ je monoid

(2) X je množina $T(X) := \{f \mid f: X \to X\}$
definujeme $\cdot$ skladanie zobrazení
$T(X)(\cdot, id_X)$ je monoid $\equiv$ transformačný monoid.

(3) $M_n(T)$ .. štvorcové matice $\in T^{n \times n}$
$M_n(T)(\cdot, I_n)$ je monoid

~ (4) A - algebra (alebo napr. graf, topologický priestor, geometrický objekt)
$\mathrm{End}\, A = \{f: A \to A \mid f$ je homomorfizmus$\} \subseteq T(A)$
$\mathrm{End}\, A (\circ, id_A)$ je monoid

napríklad A je vekt. priestor dimenzie n nad T
(lin. algebra hovorí, že $M_n(T)(\cdot, I_n) \cong \mathrm{End}(A)$
t.j. existuje bijektívny homomorfizmus medzi
$M_n(T)(\cdot, I_n)$ a $\mathrm{End}(A)$

POZNÁMKA: KEĎ JE $S(\cdot, 1)$ MONOID
A PLATÍ $a \cdot b = 1 = c \cdot a$ PRE NEJAKÉ $a, b, c \in S$,
POTOM PLATÍ $b = c$.

DÔKAZ: $c \cdot \underbrace{(a \cdot b)}_{1} = \underbrace{(c \cdot a)}_{1} \cdot b$

PRÍKLAD: UVAŽUJME $T(\mathbb{N})\,(\circ, \underbrace{id_{\mathbb{N}}}_{1})$
NECH $\alpha(k) := 2 \cdot k$, $\beta(k) := \lfloor \frac{k}{2} \rfloor$.

ZREJME $\beta \circ \alpha = id_{\mathbb{N}}$
NA DRUHÚ STRANU $\alpha \circ \beta \neq id_{\mathbb{N}}$
NAVIAC $\alpha \circ \varphi \neq id_{\mathbb{N}}$ PRE $\forall \varphi : \mathbb{N} \to \mathbb{N}$,
PRETOŽE OBRAZ α SÚ VŠETKY IBA PÁRNE ČÍSLA.

DEF.: KEĎ JE $S(\cdot, 1)$ MONOID, POTOM PRVOK $a^{-1} \in S$
PRE NEJAKÉ $a \in S$ NAZÝVAME INVERZNÝM, KEĎ
$a^{-1} \cdot a = 1 = a \cdot a^{-1}$.
a NAZÝVAME TIEŽ INVERTIBILNÝM PRVKOM MONOIDOM.
PODĽA PREDCHÁDZAJÚCEJ POZNÁMKY, KEĎ a^{-1} EXISTUJE,
POTOM JE URČENÝ JEDNOZNAČNE.

POZNÁMKA: $S(\cdot, 1)$ JE MONOID. OZNAČME S^*
MNOŽINU VŠETKÝCH INVERTIBILNÝCH PRVKOV S.
$S^*(\cdot, 1)$ JE PODMONOID MONOIDU $S(\cdot, 1)$.
NAVIAC KAŽDÝ INVERZNÝ PRVOK JE INVERTIBILNÝ.

22.10.2007 M.
PETER ČERNO

MA1062 ALGEBRA I

DÔKAZ: $1 \cdot 1 = 1 \Rightarrow 1 \in S^*$.
$a, b \in S^*$, POTOM $b^{-1} \cdot a^{-1}$ JE INVERZNÝ PRVOK KU $a \cdot b$ Z OBOCH STRÁN

DEF.: ALGEBRU $G(\cdot, ^{-1}, 1)$ NAZVEME GRUPOU, KEĎ JE $G(\cdot, 1)$ MONOID A $^{-1}$ JE UNÁRNA OPERÁCIA, KTORÁ KAŽDÉMU PRVKU PRIRADÍ INVERZNÝ PRVOK MONOIDU $G(\cdot, 1)$.

KOMUTATÍVNOU (ABELOVOU) GRUPOU NAZVEME GRUPU S KOMUTATÍVNOU OPERÁCIOU $\cdot$.

PODGRUPOU ROZUMIEME PODALGEBRU GRUPY.

NORMÁLNOU PODGRUPOU H GRUPY $G(\cdot, ^{-1}, 1)$ BUDEME ROZUMIEŤ PODGRUPU, KTORÁ SPĹŇA PODMIENKU:
$\forall g \in G \; \forall h \in H: \; g \cdot h \cdot g^{-1} \in H$.

POZNÁMKA: NECH $S(\cdot, 1)$ JE MONOID A S^* JE MNOŽINA VŠETKÝCH INVERTIBILNÝCH PRVKOV MONOIDU S.
POTOM $\odot$ JE RESTRIKCIA $\cdot$ NA S^*. $(\odot: S^* \times S^* \to S^*)$
$a \odot b := a \cdot b \quad \forall a, b \in S^*$ (S^* JE UZAVRETÁ NA $\cdot$)
$^{-1}$ NECH JE OPERÁCIA „INVERZNÝ PRVOK" NA S^*.
POTOM $S^*(\odot, ^{-1}, 1)$ JE GRUPA.

PRÍKLAD: (1) $(M(X))^* = \{\lambda\}$
(2) $(T(X))^* = \{f \mid f: X \to X \;\; f \text{ JE BIJEKCIA}\} =: S(X)$
$S(X)(\circ, ^{-1}, \mathrm{id}_X)$ JE GRUPA (SYMETRICKÁ GRUPA)
$S_n := S(\{1, 2, \ldots, n\})$

(3) $(M_n(T))^* =: GL_n(T)$ = INVERTIBILNÉ MATICE $\in T^{n\times n}$.

$GL_n(T)(\cdot, ^{-1}, I_n)$ JE GRUPA.

(4) $(End(A))^* = Aut(A) = \{f : A \to A \mid$ f JE BIJEKTÍVNY HOMOMORFIZMUS $\}$

$Aut(A)(\circ, ^{-1}, id_A)$

NAPR. $Aut(\mathbb{Z}_n) = \{f : \mathbb{Z}_n \to \mathbb{Z}_n \mid +$ JE HOMOMORFIZMUS, PRE $\mathbb{Z}_n(+,-,0)$ f JE BIJEKCIA $\}$

SÚ TO PRÁVE ZOBRAZENIA: $f : \mathbb{Z}_n \to \mathbb{Z}_n$:

$f(x) := (k \cdot x) \bmod n$ PRE $k \in \mathbb{Z}_n$, $\gcd(k,n) = 1$.

POZNÁMKA: KAŽDÁ PODGRUPA KOMUTATÍVNEJ GRUPY JE NORMÁLNA.

NECH H JE PODGRUPA GRUPY $G(\cdot, ^{-1}, 1)$.

$g \in G$, $h \in H$, POTOM $g \cdot h \cdot g^{-1} = h \in H$.

VETA: NECH $G(\cdot, ^{-1}, 1)$ JE GRUPA A ρ JE RELÁCIA NA G.

POTOM ρ JE KONGRUENCIA NA $G \Leftrightarrow$

$[1]_\rho$ JE NORMÁLNOU PODGRUPOU GRUPY G

A $(g,h) \in \rho \Leftrightarrow g^{-1} \cdot h \in [1]_\rho$.

DÔKAZ: $\Rightarrow$) NECH ρ JE KONGRUENCIA.

a) $[1]_\rho$ JE PODGRUPA G.

ZREJME $(1,1) \in \rho$. $\Rightarrow 1 \in [1]_\rho$.

22.10.2007 Ob
PETER ČERNO

MAI062 ALGEBRA I

$a \in [1]_\rho \Rightarrow (1, a) \in \rho$

ρ JE KONGRUENCIA, TJ. ρ JE ZLÚČITEĽNÁ S $\bullet^{-1}$.

$\Rightarrow (1^{-1}, a^{-1}) \in \rho$ PRIČOM $1^{-1} = 1$, TAKŽE $(1, a^{-1}) \in \rho$, TAKŽE $a^{-1} \in [1]_\rho$

$a, b \in [1]_\rho \Rightarrow (1, a), (1, b) \in \rho$.

ρ JE ZLÚČITEĽNÁ S $\bullet$, TAKŽE NUTNE $(1 \cdot 1, a \cdot b) \in \rho$.

$\Rightarrow a \cdot b \in [1]_\rho$.

TÝM SME DOKÁZALI, ŽE $[1]_\rho$ JE PODGRUPA.

b) NORMALITA $[1]_\rho$.

$g \in G, h \in [1]_\rho \Rightarrow (1, h) \in \rho$

TAKTIEŽ $(g, g) \in \rho$, $(g^{-1}, g^{-1}) \in \rho$ (ρ JE REFLEXÍVNA)

$\Rightarrow$ (ρ JE ZLÚČITEĽNÉ S $\bullet$)

$(g \cdot 1, g \cdot h) \in \rho$, $(g \cdot 1 \cdot g^{-1}, g \cdot h \cdot g^{-1}) \in \rho$

TJ. $(1, g \cdot h \cdot g^{-1}) \in \rho \Rightarrow g \cdot h \cdot g^{-1} \in [1]_\rho$.

c) $(g, h) \in \rho$, $(g^{-1}, g^{-1}) \in \rho$

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

NAOPAK, KEĎ $g^{-1} \cdot h \in [1]_\rho \Rightarrow (1, g^{-1} \cdot h) \in \rho$

$(g, g) \in \rho \Rightarrow (g \cdot 1, g \cdot g^{-1} \cdot h) \in \rho$ TJ. $(g, h) \in \rho$

$\Leftrightarrow$ H JE NORMÁLNA PODGRUPA GRUPY G.

DEFINUJME ρ: $(a, b) \in \rho \Leftrightarrow a^{-1} \cdot b \in H$.

a) ρ JE EKVIVALENCIA

$g^{-1} \cdot g = 1 \in H \Rightarrow (g, g) \in \rho$ (REFLEXIVITA)

$(g, h) \in \rho \Rightarrow g^{-1} \cdot h \in H$ (SYMETRIA)

$\Rightarrow H$ JE UZAVRETÁ NA $^{-1} \Rightarrow h^{-1} \cdot g \in H \Rightarrow (h, g) \in H$.

$(g, h) \in \rho$, $(h, r) \in \rho$, $g^{-1} \cdot h$, $h^{-1} \cdot r \in H$

$\Rightarrow H$ JE UZAVRETÁ NA $\cdot \Rightarrow g^{-1} \cdot h \cdot h^{-1} \cdot r = g^{-1} \cdot r \in H$

$\Rightarrow (g, r) \in \rho$ (TRANZITIVITA)

b) $[1]_\rho = H$ (ZREJME)

c) ρ JE ZLUČITEĽNÉ SO VŠETKÝMI OPERÁCIAMI

$(1, 1) \in \rho \Rightarrow \rho$ JE ZLUČITEĽNÁ S 1

$(g, h) \in \rho \Rightarrow g^{-1} h \in H \Rightarrow$ NORMALITA H

$g \cdot (g^{-1} \cdot h) \cdot g^{-1} \in H$ T.J. $h \cdot g^{-1} \in H$

$\Rightarrow (h^{-1}, g^{-1}) \in \rho \Rightarrow (g^{-1}, h^{-1}) \in \rho$

ρ JE ZLUČITEĽNÁ S $^{-1}$

$(g_1, h_1) \in \rho$, $(g_2, h_2) \in \rho \Rightarrow g_1^{-1} \cdot h_1 \in H$, $g_2^{-1} \cdot h_2 \in H$

NORMALITA H : $g_2 \cdot (g_2^{-1} \cdot h_2) \cdot g_2^{-1} \in H$

T.J. $h_2 \cdot g_2^{-1} \in H$

$\Rightarrow g_1^{-1} \cdot h_1 \cdot h_2 \cdot g_2^{-1} \in H$ (UZAVRETOSŤ NA $\cdot$)

NORMALITA H : $g_2^{-1} \cdot (g_1^{-1} \cdot h_1 \cdot h_2 \cdot g_2^{-1}) \cdot g_2 \in H$,

T.J. $(g_1 \cdot g_2)^{-1} \cdot (h_1 \cdot h_2) \in H \Rightarrow$

$\Rightarrow (g_1 \cdot g_2, h_1 \cdot h_2) \in \rho$. ■

24.10.2007 Wk
PETER ČERNO

EX: MI062 ALGEBRA I

$p \in T[x]$ T - TELESO $\quad \exists c \in T[x] : a-b = c \cdot p$

$\sim$ - RELÁCIA NA $T[x]$ $\quad a \sim b \Leftrightarrow p \mid \widetilde{a-b}$

ZADANÉ $\sim$ JE EKVIVALENCIA

$\sim$ JE KONGRUENCIA NA $T[x](+, \cdot, 0, 1)$

NECH $a_1 \sim b_1$, $a_2 \sim b_2$ TJ. $a_1 - b_1 = c_1 \cdot p$, $a_2 - b_2 = c_2 \cdot p$

$\Rightarrow$ a) $a_1 + a_2 \sim b_1 + b_2$

b) $a_1 \cdot a_2 \sim b_1 \cdot b_2$

$a_1 + a_2 - (b_1 + b_2) = (c_1 + c_2) p \quad \Rightarrow$ a)

$a_1 \cdot a_2 = b_1 b_2 + b_1 \cdot c_2 \cdot p + b_2 \cdot c_1 \cdot p + c_1 \cdot c_2 \cdot p^2$

$a_1 \cdot a_2 - b_1 \cdot b_2 = (b_1 c_2 + b_2 c_1 + c_1 \cdot c_2 \cdot p) p \quad \Rightarrow$ b)

$\mathcal{L}(a_1, \ldots, a_n)$

$a_1 \sim b_1, \ldots, a_n \sim b_n \Rightarrow \mathcal{L}(a_1, \ldots, a_n) \sim \mathcal{L}(b_1, \ldots, b_n)$

PRÍKLAD: $A(+, \cdot)$ BINÁRNE OPERÁCIE $+, \cdot$,
ς JE KONGRUENCIA NA $A(+, \cdot)$
KEĎ $+, \cdot$ MAJÚ NEJAKÉ VLASTNOSTI VYJADRENÉ ROVNOSŤOU,
POTOM TIETO VLASTNOSTI MAJÚ $+, \cdot$ AJ NA FAKTOROVEJ MNOŽINE $A/\varsigma\,(+, \cdot)$.

NAPR. ASOCIATIVITA:

PLATÍ $\forall a, b, c \in A \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$[a]_\varsigma \square [b]_\varsigma \overset{\text{def}}{:=} [a \square b]_\varsigma$

$\square$ ↑ OPERÁCIA

$a \in \alpha \Rightarrow \alpha = [a]_\varrho$

CHCEME DOKÁZAŤ, ŽE

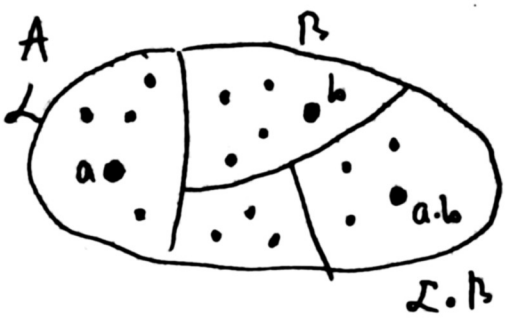
PRE $\forall \alpha, \beta, \gamma \in A/_\varrho (+, \cdot) \quad \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

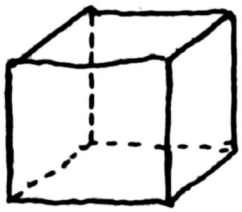
NECH $\alpha, \beta, \gamma \in A/_\varrho (+, \cdot)$,

POTOM $\exists a, b, c \in A : a \in \alpha,\ b \in \beta,\ c \in \gamma$,

T.J. $\alpha = [a]_\varrho,\ \beta = [b]_\varrho,\ \gamma = [c]_\varrho$.

$$([a]_\varrho \cdot [b]_\varrho) \cdot [c]_\varrho = [a \cdot b]_\varrho \cdot [c]_\varrho =$$
$$= [(a \cdot b) \cdot c]_\varrho = [a \cdot (b \cdot c)]_\varrho = [a]_\varrho \cdot [b \cdot c]_\varrho =$$
$$= [a]_\varrho \cdot ([b]_\varrho \cdot [c]_\varrho).$$







PRÍKLAD: DÔSLEDOK : p - POLYNÓM,

$\sim$ DEFINOVANÝ POMOCOU p (KONGRUENCIA)

$T[x]|_\sim (+, \cdot, [0]_\sim, [1]_\sim)$. POTOM:

$+, \cdot$ SÚ ASOC., KOMUT.

$+$ JE VZHĽADOM KU $\cdot$ DISTRIBUTÍVNE

PRÍKLAD: KEĎ p JE NEROZLOŽITEĽNÝ POLYNÓM.

DOKÁŽTE, ŽE $T[x]|_\sim$ JE TELESO VZHĽADOM K $+, \cdot$.

24. 10. 2007 We
PETER ČERNO

EX: MAI062 ALGEBRA I

$[0]_\sim$ JE NULOVÝ PRVOK (NEUTRÁLNÍ PRVOK) VZHLEDEM K $+$

$[1]_\sim$ JE JEDNOTKOVÝ PRVOK (NEUTRÁLNÍ PRVOK) VZHLEDEM K $\cdot$

DOKÁŽEME ŽE PRO KAŽDÉ $[a]_\sim \neq [0]_\sim$
$\exists\, [b]_\sim$: $[a]_\sim \cdot [b]_\sim = [1]_\sim$

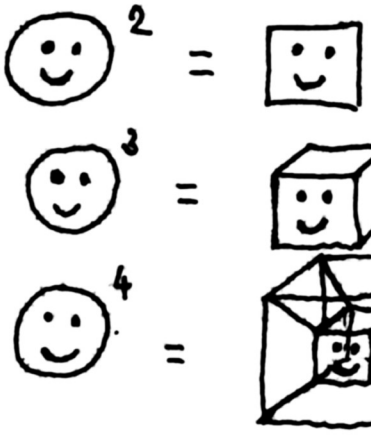
ZNAMÉ $\gcd(a, p) = 1$, PROTOŽE p JE IREDUCIBILNÝ

$\Rightarrow \exists b, c \in T[x]$: $b \cdot a + c \cdot p = 1$

TJ. $[a \cdot b]_\sim = [1]_\sim$

$[a]_\sim \cdot [b]_\sim = [1]_\sim$.







PŘÍKLAD: POPIŠTE TĚLESO $\mathbb{Z}_2[x]/_\sim$

KDE $a \sim b \Leftrightarrow x^3+x+1 \mid a-b$

(x^3+x+1 JE IREDUCIBILNÝ NAD $\mathbb{Z}_2$).

$$\mathbb{Z}_2[x]/_\sim = \{ [0]_\sim, [1]_\sim, [x]_\sim, [x+1]_\sim, [x^2]_\sim, [x^2+1]_\sim, [x^2+x]_\sim, [x^2+x+1]_\sim \}$$

$$[x+1]_\sim \cdot [x^2]_\sim = [x^3+x^2]_\sim = [x^2+x+1]_\sim$$

$$p \mid (x^3+x^2) - (x^2+x+1) = \underline{\underline{x^3+x+1}} = p$$

PŘÍKLAD: NAJDĚTE $[x]_\sim^{-1}$

HLEDÁME $r,s \in T[x]$: $1 = rx + s(x^3+x+1)$

$$x^3+x+1 = x\underbrace{(x^2+1)}_{r} + 1$$

$$[x]_\sim^{-1} = [x^2+1]_\sim$$

NAPIŠTE TABULKY OPERACÍ V TĚLESE

$\mathbb{Z}_2[x]/_\sim$ $\quad\quad \sim : x^2+x+1 = p$

29.10.2007
PETER CERNO

MA1062 ALGEBRA I

UZÁVEROVÉ SYSTÉMY NA ALGEBRE

DEF. Buď A množina. Povieme, že $\mathcal{C} \subseteq \mathcal{P}(A)$ je uzáverový systém na A, keď:

1) $A \in \mathcal{C}$
2) $\mathcal{B} \subseteq \mathcal{C} \Rightarrow \bigcap \mathcal{B} = \bigcap_{B \in \mathcal{B}} B \in \mathcal{C}$

Uzáverom (v uzáverovom systéme $\mathcal{C}$) budeme rozumieť zobrazenie $cl_{\mathcal{C}} : \mathcal{P}(A) \to \mathcal{P}(A)$:

$cl_{\mathcal{C}}(X) = \bigcap \{ C \in \mathcal{C} \mid X \subseteq C \}$ $(\in \mathcal{C})$

Uzáverovým operátorom na A budeme rozumieť $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ spĺňajúce:

1) $\forall B \subseteq A : B \subseteq \alpha(B)$
2) $\forall B \subseteq A : \alpha(\alpha(B)) = \alpha(B)$
3) $\forall B \subseteq C \subseteq A : \alpha(B) \subseteq \alpha(C)$.

Poznámka: Množina všetkých podalgebier ľubovoľnej algebry tvorí uzáverový systém.

Dôkaz: 1) A je algebra a je svojou [vlastnou] podalg.
2) Prienik nejakého systému podalgebier je podalgebra (už máme dokázané)

Veta: (1) Keď je $\mathcal{C}$ uzáverový systém, potom $cl_{\mathcal{C}}$ je uzáverovým operátor.
(2) Keď je $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ uzáverový operátor na A, potom množina $\mathcal{C} = \{ C \in \mathcal{P}(A) : \alpha(C) = C \}$ je uzáverový systém, naviac $cl_{\mathcal{C}} = \alpha$.

Dôkaz: (1) 1) pre $X \subseteq A$, $\{ C \in \mathcal{C} \mid X \subseteq C \} \supseteq X$
$\Rightarrow$ $X \subseteq cl_{\mathcal{C}}(X)$
2) $cl_{\mathcal{C}}(cl_{\mathcal{C}}(X)) \overset{?}{=} cl_{\mathcal{C}}(X)$

PODĽA 1) JE $cl_\ell(X) \subseteq cl_\ell(cl_\ell(X))$

$\supseteq$: $cl_\ell(cl_\ell(X)) = \bigcap \{ C \in \ell \mid cl_\ell(X) \subseteq C \}$

$cl_\ell(X) \in \ell$

$cl_\ell(X) \subseteq cl_\ell(X)$

TJ. $cl_\ell(X) \in \{ C \in \ell \mid cl_\ell(X) \subseteq C \}$

$\Rightarrow cl_\ell(cl_\ell(X)) = cl_\ell(X)$

3) NECH $X \subseteq Y \subseteq A$.

$\{ C \in \ell \mid X \subseteq C \} \supseteq \{ C \in \ell \mid \underbrace{Y \subseteq C}_{X \subseteq Y \subseteq C} \}$

$\Rightarrow \bigcap \{ C \in \ell \mid X \subseteq C \} \subseteq \bigcap \{ C \in \ell \mid Y \subseteq C \}$

$cl_\ell(X) \subseteq cl_\ell(Y)$. □

(2) $\ell = \{ C \in \mathcal{P}(A) \mid \alpha(C) = C \}$

a) DOKÁŽEME, ŽE ℓ JE UZÁVEROVÝ SYSTÉM

1) $A \subseteq \alpha(A)$ AXIÓM UZÁVEROVÉHO OPERÁTORA

ALE $\alpha(A) \in \mathcal{P}(A) \Rightarrow \alpha(A) \subseteq A$

$\Rightarrow A = \alpha(A) \Rightarrow A \in \ell$.

2) $\mathcal{B} \subseteq \ell$. CHCEME DOKÁZAŤ, ŽE

$\alpha(\cap \mathcal{B}) = \cap \mathcal{B}$.

$\forall B \in \mathcal{B} \quad \cap \mathcal{B} \subseteq B, \quad \alpha(B) = B$

$\Rightarrow \alpha(\cap \mathcal{B}) \subseteq \alpha(B) = B$ (3. AXIÓM UZÁVEROVÉHO OPERÁTORU)

$\Rightarrow \underbrace{\bigcap_{B \in \mathcal{B}} \alpha(\cap \mathcal{B})}_{\alpha(\cap \mathcal{B}) \subseteq \cap \mathcal{B}} \subseteq \bigcap_{B \in \mathcal{B}} B$ (1. AXIÓM UZÁV. OP.)

$\Rightarrow \alpha(\cap \mathcal{B}) = \cap \mathcal{B}$, PRETOŽE $\cap \mathcal{B} \subseteq \alpha(\cap \mathcal{B})$.

29.10.2007 No
PETER ČERNO

MA1062 ALGEBRA I

b) $cl_{\mathcal{C}}(X) \overset{!}{=} \mathcal{A}(X) \quad \forall X \subseteq A.$

$\subseteq$: $\bigcap \{C \in \mathcal{C} \mid X \subseteq C\}$

PLATÍ $\mathcal{A}(\mathcal{A}(X)) = \mathcal{A}(X)$ (2. AXIÓM UZ. OPERÁTORU)

$\Rightarrow \mathcal{A}(X) \in \mathcal{C}$, TAKŽE NUTNE:

$\Rightarrow \bigcap \{C \in \mathcal{C} \mid X \subseteq C\} \subseteq \mathcal{A}(X)$

$\supseteq$: $X \subseteq C$, $C \in \mathcal{C}$, TJ. $C = \mathcal{A}(C)$

$\mathcal{A}(X) \subseteq \mathcal{A}(C) = C$

$\Rightarrow \forall C \in \mathcal{C} \mid X \subseteq C \Rightarrow \mathcal{A}(X) \subseteq C$

$\Rightarrow \mathcal{A}(X) \subseteq \bigcap \{C \in \mathcal{C} \mid X \subseteq C\}$ ∎

POZNÁMKA: MNOŽINA VŠETKÝCH UZÁVEROVÝCH SYSTÉMOV NA MNOŽINE A TVORÍ UZÁVEROVÝ SYSTÉM NA MNOŽINE $\mathcal{P}(A)$.

DOKAZ: NECH $\mathcal{C}$ SÚ VŠETKY UZÁVEROVÉ SYSTÉMY NA A. DOKÁŽEME, ŽE $\mathcal{C}$ JE UZÁVEROVÝM SYSTÉMOM NA $\mathcal{P}(A)$.

1) $\mathcal{P}(A) \in \mathcal{C}$, PRETOŽE $\mathcal{P}(A)$ JE UZÁVEROVÝ SYSTÉM NA A.

2) NECH $\mathcal{B} \subseteq \mathcal{C}$, $\forall \Gamma \in \mathcal{B}$ JE Γ UZÁVEROVÝ SYSTÉM NA A.

CHCEME DOKÁZAŤ, ŽE $\boxed{\bigcap \mathcal{B}}$ JE UZÁVEROVÝ SYSTÉM NA A...

1*) $\forall \Gamma \in \mathcal{B}: A \in \Gamma \Rightarrow A \in \bigcap_{\Gamma \in \mathcal{B}} \Gamma = \boxed{\bigcap \mathcal{B}}$

2*) NECH $\mathcal{B} = \{\Gamma_i \mid i \in I\}$, TJ. $\bigcap \mathcal{B} = \bigcap_{i \in I} \Gamma_i$

$B_j \in \bigcap \mathcal{B}$ $j \in J$: $B_j \in \Gamma_i \quad \forall j \in J \ \forall i \in I$

$\xi = \{B_j \mid j \in J\} \subseteq \boxed{\bigcap \mathcal{B}}$. CHCEME DOKÁZAŤ $\bigcap \xi \in \boxed{\bigcap \mathcal{B}}$

$\bigcap \xi = \bigcap_{j \in J} B_j \in \Gamma_i \quad \forall i \in I \Rightarrow \bigcap \xi \in \bigcap_{i \in I} \Gamma_i = \boxed{\bigcap \mathcal{B}}$ ∎

KEĎ $\mathcal{A} \subseteq \mathcal{B}$ SÚ DVA UZÁVEROVÉ SYSTÉMY NA A A $C \subseteq D \subseteq A$, POTOM $cl_{\mathcal{B}}(C) \subseteq cl_{\mathcal{A}}(D)$

DÔKAZ: $cl_{\mathcal{B}}(C) \subseteq cl_{\mathcal{B}}(D)$ ($cl_{\mathcal{B}}$ JE UZÁV. OPERÁTOR) AX. 3 UZ. OP.

$cl_{\mathcal{B}}(D) \subseteq cl_{\mathcal{A}}(D)$

$\{Y \in \mathcal{B} \mid D \subseteq Y\} \supseteq \{Z \in \mathcal{A} \mid D \subseteq Z\}$ PRETOŽE $\mathcal{A} \subseteq \mathcal{B}$

$\Rightarrow \bigcap\{Y \in \mathcal{B} \mid D \subseteq Y\} \subseteq \bigcap\{Z \in \mathcal{A} \mid D \subseteq Z\}$ ■

POZNÁMKA: MNOŽINA VŠETKÝCH REFLEXÍVNYCH (SYMETRICKÝCH, TRANZITÍVNYCH) RELÁCIÍ NA MNOŽINE A, TAKISTO MN. V EKVIVALENCIÍ NA A, TVORÍ UZÁVEROVÝ SYSTÉM NA $A \times A$.

DÔKAZ: 1. $A \times A$ JE REFLEXÍVNA (SYMETRICKÁ, TRANZIT.) RELÁCIA $A \times A \in \mathcal{R}$ ($\in \mathcal{Y}$, $\in \mathcal{T}$, $\in \mathcal{E}$ $\mathcal{E} = \mathcal{R} \cap \mathcal{Y} \cap \mathcal{T}$)

2. NECH $\{\varrho_i \subseteq A \times A \mid i \in I\} \subseteq \mathcal{R}$ ($\subseteq \mathcal{Y}$, $\subseteq \mathcal{T}$, $\subseteq \mathcal{E}$)

a) $\varrho_i \in \mathcal{R}$: $id \subseteq \varrho_i \Rightarrow id \subseteq \bigcap_{i \in I} \varrho_i \Rightarrow \bigcap_{i \in I} \varrho_i \in \mathcal{R}$

b) $\varrho_i \in \mathcal{Y}$: $\varrho_i^{-1} \subseteq \varrho_i \ \forall i \in I$

$(a,b) \in \bigcap_{i \in I} \varrho_i \Rightarrow (b,a) \in \bigcap_{i \in I} \varrho_i \Rightarrow \bigcap_{i \in I} \in \mathcal{Y}$

c) $\varrho_i \in \mathcal{T}$: $(a,b), (b,c) \in \bigcap_{i \in I} \varrho_i \Rightarrow (a,c) \in \bigcap_{i \in I} \varrho_i \Rightarrow \bigcap_{i \in I} \varrho_i \in \mathcal{T}$. ■

EKVIVALENCIA $\mathcal{E} = \underbrace{\mathcal{R} \cap \mathcal{Y} \cap \mathcal{T}}$

$\in$ SYSTÉM $\forall$ UZÁVEROVÝCH SYSTÉMOV NA $A \times A$

JE UZÁVEROVÝ SYSTÉM

$\Rightarrow$ $\mathcal{E}$ JE UZÁVEROVÝ SYSTÉM NA $A \times A$. □

31.10.2007 Ut
PETER ČERNO

MAI062 ALGEBRA I

KAŽDÝ NEROZLOŽITEĽNÝ POLYNÓM STUPŇA n V $\mathbb{Z}_p[x]$ DELÍ POLYNÓM $x^{p^n} - x$.

PRÍKLAD: UVAŽUJME KONEČNÉ TELESO T

$$P = \{\underbrace{1+1+\ldots+1}_{k} \mid k \in \mathbb{N}_0\}$$

a) $|P|$ JE PRVOČÍSLO = CHARAKTERISTIKA TELESA

b) P JE PODALGEBRA ALGEBRY $T(+,\cdot,0,1)$.
A NAVYAC $P(+,\cdot,0,1)$ JE TELESO IZOMORFNÉ SO $\mathbb{Z}_p$.

a) CHARAKT. (KONEČNÉHO) TELESA JE NAJMENŠIE k ($k>0$) TAKÉ, ŽE:

$$\underbrace{1+1+\ldots+1}_{k} = 0$$

$$P = \{0, 1, 1+1, \ldots, \underbrace{1+\ldots+1}_{k-1}\} \quad \text{TAKŽE} \quad |P| = k.$$

PREDPOKLADAJME, ŽE k NIE JE PRVOČÍSLO, TJ. $k = a \cdot b$, $a, b > 1$, POTOM

$$(\underbrace{1+1+\ldots+1}_{a})(\underbrace{1+1+\ldots+1}_{b}) = 0$$

ZREJME $a \neq 0$, $b \neq 0$, TAKŽE $ab = 0$ ŽE SPOR. ↯

b) $0,1 \in P$, UZAVRETOSŤ NA $+$ A $\cdot$ JE ZREJMÁ.

c) $P \cong \mathbb{Z}_p$ $\qquad \underbrace{1+1+\ldots+1}_{k} \leftrightarrow [k]_{n_p} \leftrightarrow k \in \mathbb{Z}_p$

T JE VEKTOROVÝ PRIESTOR NAD TELESOM P.

$\dim_P T = n$ (PRETOŽE T JE KONEČNÁ MNOŽINA)

$\Rightarrow$ ZREJME $|T| = |P|^n$.

NECH $b_1, \ldots, b_n \in T$ JE BÁZA T NAD P.

POTOM PRE KAŽDÉ $x \in T$ $\exists$ PRÁVE JEDNA POSTUPNOSŤ $\alpha_1, \ldots, \alpha_n \in P$: $x = \alpha_1 b_1 + \ldots + \alpha_n b_n$.

TÝCHTO POSTUPNOSTÍ JE PRÁVE $|P|^n$.

05.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

POZNÁMKA: MNOŽINA VŠETKÝCH KONGRUENCIÍ NA NEJAKEJ ALGEBRE TVORÍ UZÁVEROVÝ SYSTÉM NA $A \times A$.

DÔKAZ: NECH α JE n-ÁRNA OPERÁCIA NA A, $\mathcal{V}_\alpha$ JE MNOŽINA VŠETKÝCH EKVIVALENCIÍ ZLUČITEĽNÝCH S OPERÁCIOU α. DOKÁŽTE, ŽE $\mathcal{V}_\alpha$ JE UZÁVEROVÝ SYSTÉM.

1. $A \times A$ JE EKVIVALENCIA ZLUČITEĽNÁ S α, TAKŽE $A \times A \in \mathcal{V}_\alpha$.

2. NECH $\rho_j \in \mathcal{V}_\alpha$ $j \in J$, TJ. $\xi = \{\rho_j, j \in J\} \subseteq \mathcal{V}_\alpha$. DOKÁŽTE, ŽE $\cap\xi = \bigwedge_{j \in J} \rho_j \in \mathcal{V}_\alpha$.

   a) UVEDOMTE SI, ŽE $\bigwedge_{j \in J} \rho_j$ JE EKVIVALENCIA

   b) UVAŽUJTE $a_1, \dots, a_n, b_1, \dots, b_n \in A$ A PREDPOKLADAJTE, ŽE $(a_i, b_i) \in \bigwedge_{j \in J} \rho_j$. PRE $\forall i \in \{1, \dots, n\}$

   $\Rightarrow \forall j \in J \ (a_i, b_i) \in \rho_j \Rightarrow (\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \rho_j$

   TAKŽE NUTNE $(\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \bigwedge_{j \in J} \rho_j$

   • TJ. α JE ZLUČITEĽNÁ S $\bigwedge_{j \in J} \rho_j = \cap\xi$. ∎

PRE ALGEBRU $A(\alpha_i, i \in I)$ MÁTE MNOŽINU VŠETKÝCH KONGRUENCIÍ AKO $\bigcap_{i \in I} \mathcal{V}_{\alpha_i}$

$\mathcal{V}_\alpha$ JE UZÁVEROVÝ SYSTÉM

A PRIENIK UZÁVEROVÝCH SYSTÉMOV JE OPÄŤ UZÁVEROVÝ SYSTÉM, TAKŽE $\bigcap_{i \in I} \mathcal{V}_{\alpha_i}$ JE UZÁVEROVÝ SYSTÉM. ∎

POZOROVANIE: NECH $\mathcal{C}$ JE UZÁVEROVÝ SYSTÉM NA A. PRE $X \subseteq A$ JE $cl_{\mathcal{C}}(X)$ NAJMENŠÍ (ABSOLÚTNE) PRVOK (ZHODNÝ K $\subseteq$) UZÁVEROVÉHO SYSTÉMU $\mathcal{C}$

POZNÁMKA: BUĎ ϱ REFLEXÍVNA (SYMETRICKÁ) RELÁCIA, POTOM ϱ^+ A $\varrho \cup \varrho^{-1}$ SÚ OPÄŤ REFLEXÍVNE (SYMETRICKÉ) RELÁCIE.

DÔKAZ.: $\varrho^+ = \{(a,b) \mid \exists\, a=a_0, \dots, a_k=b : \begin{cases} k\geq 0 \\ k \geq 1 \end{cases}$ PRIDÁ REFLEXIVITU $\wedge$

$(a_i, a_{i+1}) \in \varrho \quad \forall i = 0, \dots, k-1 \}$ JE ZREJME TRANZITÍVNA RELÁCIA

- ZREJME $\varrho \subseteq \varrho^+$

$\varrho^{-1} = \{(a,b) \mid (b,a) \in \varrho\}$

1. AK JE ϱ REFLEXÍVNA REL., TJ. $id \subseteq \varrho$

$\Rightarrow id \subseteq \varrho \subseteq \varrho^+$, TAKŽE ϱ^+ JE TIEŽ REFLEXÍVNA

ĎALEJ $id \subseteq \varrho \Rightarrow id^{-1} \subseteq \varrho^{-1}$, ALE $id^{-1} = id$, TAKŽE ϱ^{-1} JE TAKTIEŽ REFLEXÍVNA.

2. AK JE ϱ SYMETRICKÁ

$(a,b) \in \varrho^+$, TJ. $\exists\ a=a_0, \dots, a_k=b \cdot (a_i, a_{i+1}) \in \varrho$

$\Rightarrow (a_{i+1}, a_i) \in \varrho \quad b=a_k, \dots, a_0=a \Rightarrow (b,a) \in \varrho^+$

SYMETRIA ϱ

$(a,b) \in \varrho^{-1} \Rightarrow (b,a) \in \varrho \underset{\text{SYMETRIA } \varrho}{\Rightarrow} (a,b) \in \varrho \Rightarrow (b,a) \in \varrho^{-1}$ ■

VETA: KEĎ JE ϱ RELÁCIA, POTOM $[(\varrho \cup id) \cup (\varrho \cup id)^{-1}]^+ = (\varrho \cup \varrho^{-1} \cup id)^+$ JE NAJMENŠIA EKVIVALENCIA, KTORÁ OBSAHUJE ϱ. (TJ. $= cl_{\mathcal{E}}(\varrho)$, KDE $\mathcal{E}$ JE UZÁVEROVÝ SYSTÉM VŠETKÝCH EKVIVALENCIÍ)

DÔKAZ. $\varrho \cup id$ JE REFLEXÍVNA RELÁCIA.

$(\varrho \cup id) \cup (\varrho \cup id)^{-1}$ ZOSTÁVA REFLEXÍVNA A JE TIEŽ SYMETRICKÁ.

$\Rightarrow$ TRANZITÍVNY OBAL $[(\varrho \cup id) \cup (\varrho \cup id)^{-1}]$ JE POTOM (PODĽA MIESTE UVEDENEJ POZNÁMKY) EKVIVALENCIA.

MAI062 ALGEBRA

NECH ε JE EKVIVALENCIA OBSAHUJÚCA ρ, TJ. $\rho \subseteq \varepsilon$

$\Rightarrow \rho \cup id \subseteq \varepsilon \Rightarrow (\rho \cup id)^{-1} \subseteq \varepsilon^{-1} = \varepsilon$

$\Rightarrow (\rho \cup id) \cup (\rho \cup id)^{-1} \subseteq \varepsilon$

$\Rightarrow [(\rho \cup id) \cup (\rho \cup id)^{-1}]^{+} \subseteq \varepsilon^{+} = \varepsilon$.

TJ. $[(\rho \cup id) \cup (\rho \cup id)^{-1}]^{+}$ JE PRIENIK

$\curvearrowright$ VŠETKÝCH EKVIVALENCIÍ ε, KTORÉ OBSAHUJÚ ρ (TJ. $\rho \subseteq \varepsilon$).

DEFINÍCIA: NECH $A(\alpha_i, i \in I)$ JE ALGEBRA A $X \subseteq A$ (ρ JE RELÁCIA NA A), POTOM HOVORÍME, ŽE X GENERUJE [PODALGEBRU $cl_A(X)$, ZNAČ.: $\langle X \rangle$

(ρ GENERUJE KONGRUENCIU $cl_c(\rho)$) ZNAČ.: $\langle \rho \rangle$

KDE $\mathcal{A}$ SÚ VŠETKY PODALGEBRY (UZÁVER. SYSTÉM)

$\mathcal{C}$ SÚ VŠETKY KONGRUENCIE ALGEBRY $A(\alpha_i, i \in I)$

POZNÁMKA: NECH f, g SÚ HOMOMORFIZMY ALGEBIER $A \to B$ (ROVNAKÉHO TYPU) A NECH $X \subseteq A$ GENERUJE A (TJ. $cl_A(X) = A$).

KEĎ $f(x) = g(x)$ PRE $\forall x \in X$, POTOM $f = g$ NA A.

DÔKAZ: UVAŽUJME $Y = \{a \in A \mid f(a) = g(a)\} \subseteq A$

NECH α JE ĽUBOVOĽNÁ OPERÁCIA ALGEBRY A (RESP. B) ARITY n.

NECH $a_1, \dots, a_n \in Y$. POTOM (f JE HOMOMORFIZMUS)

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

$= \alpha(g(a_1), \dots, g(a_n)) = g(\alpha(a_1, \dots, a_n)) \Rightarrow$

$\alpha(a_1, \dots, a_n) \in Y$. Y JE UZAVRETÁ NA OP. α.

$\Rightarrow$ Y JE PODALGEBRA A.

DALEJ $X \subseteq Y \Rightarrow$ (VZHLADOM K TOMU, ŽE X GEN. A)

NUTNE $\underline{\underline{Y = A}}$.

TO ALE ZNAMENÁ, ŽE $f = g$. ■

PRÍKLAD: UVAŽUJME ALGEBRU $\mathbb{Z}(+, \cdot, -)$

A ALGEBRU $G(+, \cdot, -)$ S BINÁRNYMI OPERÁCIAMI $+, \cdot, -$.

UVAŽUJME $1 \in \mathbb{Z}$. POTOM

$$\langle 1 \rangle \supseteq \{ 1, 1+1, 1+1+1, \ldots 1-(1+1), \ldots \} = \mathbb{Z}$$

NECH f, g SÚ HOMOMORFIZMY $\mathbb{Z} \to G$.

TO ALE ZNAMENÁ, ŽE AK $f(1) = g(1)$, POTOM $f = g$.

IZOMORFIZMY

DEFINÍCIA: KAŽDÝ BIJEKTÍVNY HOMOMORFIZMUS [2 ALGEBIER ROVNAKÉHO TYPU] BUDEME NAZÝVAŤ IZOMORFIZMUS.

O ALGEBRÁCH (ROVNAKÉHO TYPU) A A B POVIEME, ŽE SÚ IZOMORFNÉ, KEĎ EXISTUJE ASPOŇ JEDEN IZOMORFIZMUS $A \to B$. (ZNAČÍME $A \cong B$).

$f : A \to B$, $g : B \to C$

KEĎ SÚ f, g IZOMORFIZMY, POTOM $f^{-1} : B \to A$ JE TIEŽ IZOMORFIZMUS A $g \circ f$ JE TIEŽ IZOMORFIZMUS

$id_A : A \to A$ JE IZOMORFIZMUS

05.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

$\Rightarrow$ $\cong$ JE EKVIVALENCIA NA KAŽDEJ MNOŽINE ALGEBIER ROVNAKÉHO TYPU.

DEFINÍCIA: BUĎ $\rho \subseteq \sigma$ DVE EKVIVALENCIE NA A DEFINUJEME RELÁCIU σ/ρ NA A/ρ NASLEDOVNE:

$([a]_\rho, [b]_\rho) \in \sigma/\rho \overset{\text{def.}}{\Leftrightarrow} (a,b) \in \sigma$.

POZNÁMKA: (1) $\rho \subseteq \sigma$ NECH SÚ EKVIVALENCIE NA A, POTOM σ/ρ JE KOREKTNE DEFINOVANÁ EKVIVALENCIA NA A/ρ.

(2) η JE EKVIVALENCIA NA A/ρ, KDE ρ JE EKVIVALENCIA NA A, POTOM EXISTUJE PRÁVE JEDNA EKVIVALENCIA σ NA A TAKÁ, ŽE $\rho \subseteq \sigma$ A $\eta = \sigma/\rho$.

DÔKAZ. NECH $[a_1]_\rho = [a_2]_\rho$, $[b_1]_\rho = [b_2]_\rho$.

DOKÁŽEME, ŽE $([a_1]_\rho, [b_1]_\rho) \in \sigma/\rho \Leftrightarrow ([a_2]_\rho, [b_2]_\rho) \in \sigma/\rho$

(H) $(a_1, b_1) \in \sigma \Leftrightarrow (a_2, b_2) \in \sigma$

$(a_1, a_2) \in \rho \Rightarrow (a_2, a_1) \in \rho \subseteq \sigma$

$(a_1, b_1) \in \sigma \Rightarrow (a_2, b_1) \in \sigma$

$(b_1, b_2) \in \rho \subseteq \sigma \Rightarrow (a_2, b_2) \in \sigma$

TJ. $(a_1, b_1) \in \sigma \Rightarrow (a_2, b_2) \in \sigma$.

PODOBNE NAOPAK.

σ/ρ JE ZREJME REFLEXÍVNA,
SYMETRICKÁ } PLYNIE
TRANZITÍVNA } Z VLASTNOSTÍ σ
$\Rightarrow$ JE TO EKVIVALENCIA

NECH η JE EKVIV. NA A/ρ

DEFINUJME σ : $(a,b) \in \sigma \overset{\text{def.}}{\Leftrightarrow} ([a]_\rho, [b]_\rho) \in \eta$

DOKÁŽTE, ŽE σ JE EKVIVALENCIA TAKÁ, ŽE $\rho \subseteq \sigma$ A $\eta = \sigma/\rho$.

KOREKTNOSŤ SA ZREJME.

TO, ŽE σ JE EKVIVALENCIA VYPLÝVA Z TOHO, ŽE η JE EKVIVALENCIA

$\rho \subseteq \sigma$: $(a,b) \in \rho \Rightarrow [a]_\rho = [b]_\rho$

Z REFLEXIVITY η JE $([a]_\rho, [b]_\rho) \in \eta$.

TO ALE ZNAMENÁ, ŽE $(a,b) \in \sigma$.

TO, ŽE $\eta = \sigma/\rho$ VYPLÝVA PRIAMO Z DEFINÍCIE σ.

21.10.2007 16
PETER ČERNO

ALGEBRA I - TEST

(18)

1. $98x + 68y = 10$
$49x + 34y = 5$ /:2

49
34
$15 = 49 - 34$
$4 = 34 - 2.15$
$3 = 15 - 3.4$
$1 = 4 - 3 = 34 - 2.15 - 15 + 3.4 =$
$= 34 - 2.(49-34) - 49 + 34 + 3.(34 - 2.15) =$
$= 34 - 2.49 + 2.34 - 49 + 34 + 3.34$
$- 6.49 + 6.34 =$
$= 13.34 - 9.49$

$34 \cdot 13 = 102 + 34 = 442$

$49 \cdot 9 = 441$

$\gcd(34, 49) = 1$

$\Rightarrow (-5.9).49 + (5.13).34 = 5$

VŠETKY RIEŠENIA SÚ TVARU

$(-45 - 34k).49 + (65 + 49k).34 = 5 \qquad k \in \mathbb{Z}$

2. (2 body)

$P_0 = x^3 - x^2 - x - 2$

$P_1 = x^3 - 3x^2 + x + 2$

$P_2 = 2x^2 - 2x - 4$

$P_3 = \frac{1}{2} \cdot (x - 2)$

$P_4 = (x + 1)$

$P_{5} = 0$

$\gcd(x^3 - x^2 - x - 2,\ x^3 - 3x^2 + x + 2) =$

$= x + 2$

$x^3 - x^2 - x - 2 : x^3 - 3x^2 + x + 2 = 1$

$-(x^3 - 3x^2 + x + 2)$

$2x^2 - 2x - 4$

$x^3 - 3x^2 + x + 2 : x^2 - x - 2 = x - 2$

$-(x^3 - x^2 - 2x)$

$-2x^2 + 3x + 2$

$-(-2x^2 + 2x + 4)$

$x - 2$

$x^2 - x - 2 : x - 2 = x + 1$

$-(x^2 - 2x)$

$x - 2$

$-(x - 2)$

0

3. (4 body)

$a_n x^n + \ldots + a_0 : b_m x^m + \ldots + b_0 = c_{n-m} x^{n-m} + \ldots + c_0$

MÔŽEME PREDPOKLADAŤ $n \geq m$

INPUT: $a[0..n]$, $b[0..m]$, p PRVOČÍSLO, $a[n] \neq 0$, $b[m] \neq 0$

OUTPUT: $c[0..n-m]$, $a[0..n]$ JE ZVYŠOK

```
for i := n-m downto 0 do begin
    c[i] := a[i+m] . (b[m])^-1 mod p
    for j := 0 to m do begin
        a[i+j] := (a[i+j] - c[i] * b[j]) mod p
    end;
end;
```

ZVYŠOK PO DELENÍ JE v POLI a.

$(b[m])^{-1}$ JE TAKÝ PRVOK ZO $\mathbb{Z}_p$, ŽE

$b[m] * (b[m])^{-1} \bmod p = 1$

NÁJDEME HO POMOCOU EUKLIDOVHO ALGORITMU

31.10.2007 Ve
PETER ČERNO

ALGEBRA I – TEST

(4.) 3

PŘEDPOKLADÁME, ŽE:

$$x^3+2x+1 = P_1(x)\cdot P_2(x)$$

KDE:

$st\,P_1 + st\,P_2 = 3, \quad st\,P_1, st\,P_2 \geq 1$

BÚNO $st\,P_1 = 1, \quad st\,P_2 = 2$

$$x^3+2x+1 = (x+a)(x^2+bx+c) =$$
$$= x^3 + bx^2 + cx + ax^2 + abx + ac =$$
$$= x^3 + (a+b)x^2 + (ab+c)x + ac$$

MUSÍ BÝT: $a+b=0 \Rightarrow b=-a$

$ab+c=2 \Rightarrow -a^2+c=2$

$ac=1 \qquad ac=1$

$\Rightarrow c = 2+a^2 = a^{-1} \quad /\cdot a$

$2a+a^3=1$

$a^3+2a+6=0$

x	0	1	2	3	4	5	6
x^3	0	1	1	6	1	6	6
$2x$	0	2	4	6	1	3	5
x^3+2x+6	6	2	4	4	1	1	3

TENTO ROVNICI NEVYHOVUJE ŽÁDNÉ $a \in \mathbb{Z}_7$ (VID TABULKA)

$\Rightarrow$ x^3+2x+1 JE IREDUCIBILNÍ V $\mathbb{Z}_7$.

(5.) $q = 3^2$

NAJSKÔR SI VEZMEME IREDUCIBILNÝ POLYNÓM STUPŇA 2 V $\mathbb{Z}_3$. NAPRÍKLAD $P(x) = x^2+1$.

KEBY $x^2+1 = (x+a)(x+b)$, POTOM:

$a+b=0$

$ab=1$

a	1	2
b	1	2
$a+b$	2	1

Z TABUĽKY VIDIEŤ, ŽE TÁTO SÚSTAVA NEMÁ V $\mathbb{Z}_3$ RIEŠENIE!

VIDÍME, ŽE x^2+1 JE IREDUCIBILNÝ V $\mathbb{Z}_3$.

DEFINUJEME KONGRUENCIU $\sim$ NA $\mathbb{Z}_3[x]$ AKO

$$\forall P_1, P_2 \in \mathbb{Z}_3[x]: \quad P_1 \sim P_2 \Leftrightarrow x^2+1 \mid (P_1 - P_2)$$

ĽAHKO NAHLIADNUŤ, ŽE

$$\mathbb{Z}_3[x]|_\sim = \{ [0]_\sim, [1]_\sim, [2]_\sim, [x]_\sim, [x+1]_\sim, [x+2]_\sim, [2x]_\sim, [2x+1]_\sim, [2x+2]_\sim \}$$

TJ. $\mathbb{Z}_3[x]|_\sim$ MÁ PRÁVE 9 ROZKLADOVÝCH TRIED

A STAČÍ S OPERÁCIAMI $+, \cdot, 0, 1$

$[a]_\sim + [b]_\sim := [a+b]_\sim$, $[a]_\sim \cdot [b]_\sim := [a \cdot b]_\sim$

$0 := [0]_\sim$, $1 := [1]_\sim$

$-[a]_\sim := [-a]_\sim$, PRE $[a]_\sim \neq [0]_\sim$

VIEME NÁJSŤ $([a]_\sim)^{-1}$ PODĽA EUKLIDOVHO ALGORITMU

$\Rightarrow$ DOSTÁVAME TELESO O 9 PRVKOCH.

07.11.2007 14
PETER ČERNO

EX: MAI062 ALGEBRA I

PRÍKLAD: $A = \{a, b, c\}$, BINÁRNA OPERÁCIA $\circ$

$\circ$	a	b	c
a	c	b	a
b	b	a	b
c	a	b	c

NÁJDITE VŠETKY PODALGEBRY ALGEBRY $A(\circ)$:

$\emptyset$, $\{a, c\}$, $\{a, b, c\}$, $\{c\}$ JE TO UZÁVEROVÝ SYSTÉM!

↳ NEVIEME ŽIADNU NULÁRNU OPERÁCIU

$\langle\{a\}\rangle$ = BUDEME ZNAČIŤ $\langle a\rangle = \{a, c\}$

$\langle\{c\}\rangle = \langle c\rangle = \{c\}$

PRÍKLAD: NÁJDITE VŠETKY PODALGEBRY ALGEBRY $A(\circ, a)$: $\{a, c\}$, $\{a, b, c\}$

PRÍKLAD:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

NÁJDITE VŠETKY PODALGEBRY ALGEBRY $A(\circ, *)$:

$\emptyset$, $\{a, b, c\}$

PRÍKLAD: VŠETKY PODALGEBRY ALGEBRY $A(\circ, *, a)$:

IBA $\{a, b, c\}$.

PRÍKLAD: NÁJDITE ∀ KONGRUENCIE NA $A(\cdot)$

EKVIVALENCIE BUDEME POPISOVAŤ POMOCOU ROZKLADOV MNOŽINY A.

(a)(b)(c) ✓

(a b c) ✓

(a b)(c) ⊗ $a \circ a = c,\ a \circ b = b$

(a)(b c) ✓

(a)(b)(c) ✗ $b \circ a = b,\ c \circ a = a$

AKO VYZERÁ KONGRUENCIA OBSAHUJÚCA (b,c)

TJ. HĽADÁME $\langle (b,c) \rangle$

$b \sim c$
$a \sim a \Rightarrow b \circ a \sim c \circ a \Rightarrow b \sim a \Rightarrow \langle (b,c) \rangle = A \times A$

$\cdot$	a	$b \sim c$
a	c	$b \sim a$
b	b	$a \sim b$
$\wr$	$\wr$	$\wr$ $\wr$
c	a	$b \sim c$

POMÔCKA !!!

$A \times A = \{ (a,a), (a,b), \ldots$
$\ldots (c,c) \}$

$a \sim b \sim c$

07.11.2007 Ut
PETER ČERNO

EX: MAI062 ALGEBRA I

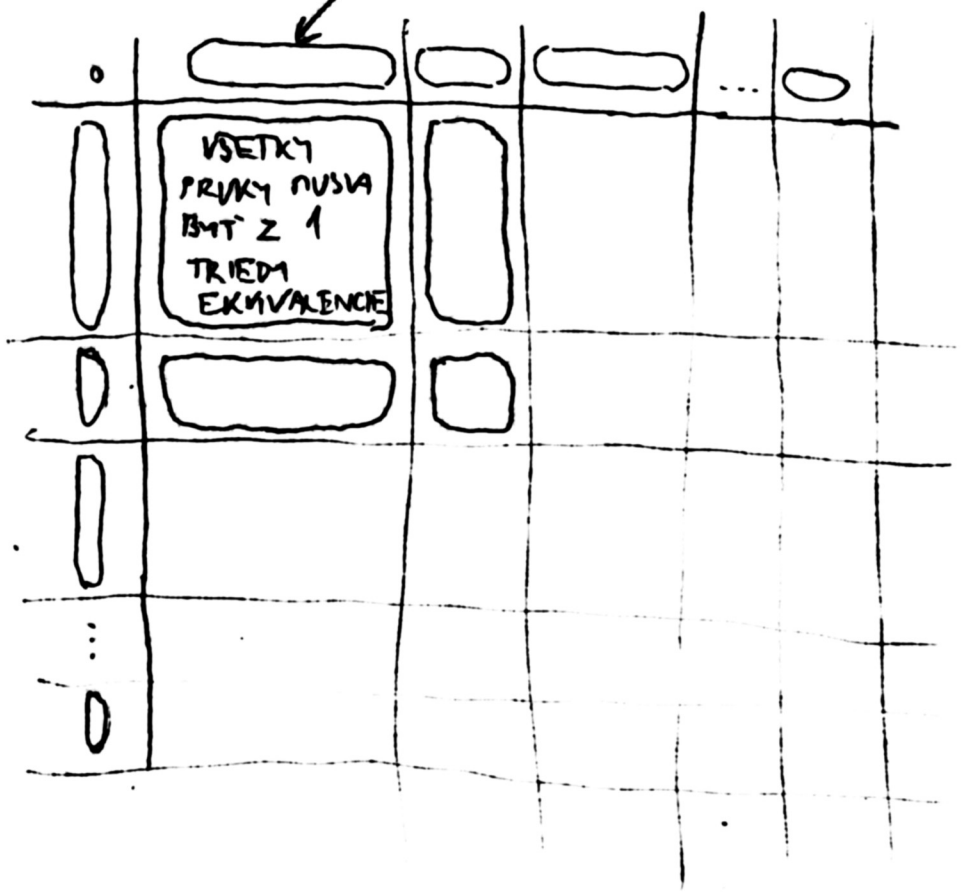
∘	a ~ b	c
a	c ~ b	a
≀	≀ ≀	≀
b	b ~ a	b
c	a ~ b	c

$\langle (a,b) \rangle = A \times A$

∘	a ~ c	b
a ≀ c	c ~ a ≀ ≀ a ~ c	b ≀ b
b	b ~ b	a

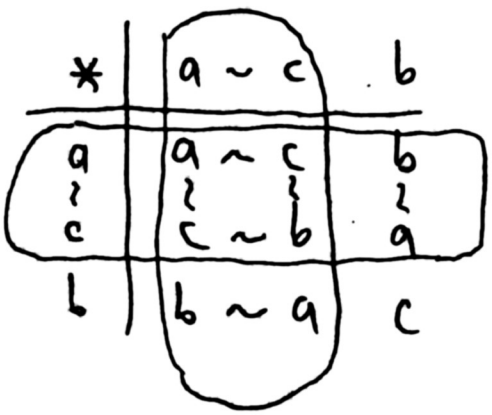
$\langle (a,c) \rangle = id \cup \{(a,c), (c,a)\}$

VŠEOBECNE — TRIEDA EKVIVALENCIE



PRÍKLAD: $A(\circ, a)$ MÁ KONGRUENCIE ROVNAKÉ AKO V PREDCHÁDZAJÚCOM PRÍPADE, TJ. $A(\circ)$.

PRÍKLAD: NÁJDITE ∀ KONGRUENCIE ALGEBRY $A(\circ, *, a)$



⊛ KONGRUENCIE SÚ IBA id a $A \times A$.

PRÍKLAD: $C = \{1, 2, 3, 4\}$

□	1	2	3	4
1	2	1	1	1
2	1	4	1	1
3	4	1	4	1
4	3	4	4	2

$\langle 1 \rangle = \{1, 2, 4, 3\}$

$\langle \{3,4\} \rangle = \{1, 2, 3, 4\}$

∀ PODALGEBRY: $\emptyset$, C

07.11.2007 Uk
PETER ČERNO

EX: MAI062 ALGEBRA I

PRÍKLAD:

□	1 ~ 4	2 3
1	2 ~ 3	1 1
4	3 2	4 4
2	1 1	4 1
3	4 1	1 4

$\langle (1,4) \rangle =$

$= id \cup \{(1,4),(4,1),(2,3),(3,2)\} \subseteq C \times C$

$\leftrightarrow$



$C|_{\sim}$ (□) PRE KONGRUENCIU $\{\{1,4\},\{2,3\}\}$

ROZKLADOVÉ TRIEDY

□	{1,4}	{2,3}
{1,4}	{2,3}	{1,4}
{2,3}	{1,4}	{1,4}

$X = \{1,4\}$

$Y = \{2,3\}$

□	x	y
x	y	x
y	x	x

PRÍKLAD: DOKÁŽTE TVRDENIE:

NECH P JE KONEČNÁ MNOŽINA $\neq \emptyset$
A $\circ$ JE ASOCIATÍVNA BINÁRNA OPERÁCIA.

POTOM $\exists e \in P$ TAKÝ, ŽE $e \circ e = e$.
$\Rightarrow$ EXISTUJE 1-PRVKOVÁ PODALGEBRA

$\Rightarrow$ V PREDCHÁDZAJÚCOM PRÍKLADE II NIE JE ASOCIATÍVNA

e = IDEMPOTENTNÝ PRVOK

POZNÁMKA: ČASTOKRÁT SA OPLATÍ OVEROVAŤ TÚTO PODMIENKU NA PODALGEBRU.

$a^m = a^n$ NECH $m > 2n$

$a^{r+km} = a^{r+kn}$ HĽADÁME r, k TAK, ABY

$r+km = 2(r+kn)$

$r = km - 2kn$

STAČÍ POLOŽIŤ $r = m - 2n$ A MÁME

$a^{(m-2n)+m} = a^{m-2n+n}$

TJ. $(a^{m-n})^2 = a^{m-n}$

$\square$

12.11.2007 Mo
PETER CEANO

MA1062 ALGEBRA I

POZNÁMKA: BUĎ ρ KONGRUENCIA NA ALGEBRE A, $\rho \subseteq \sigma$, σ JE EKVIVALENCIA NA A.
POTOM σ JE KONGRUENCIA NA ALGEBRE $A \Leftrightarrow$ σ/ρ JE KONGRUENCIA NA ALGEBRE A/ρ.

DÔKAZ: α NECH JE n-ÁRNA OPERÁCIA NA A. $(A/\rho|$.

σ JE ZLUČITEĽNÁ S $\alpha \Leftrightarrow$
$\forall a_1, \dots, a_n, b_1, \dots, b_n \in A \quad \forall i \in [n] \ (a_i, b_i) \in \sigma \Rightarrow$
$(\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \sigma$ $\quad x \sim y \Leftrightarrow (x,y) \in \sigma$

EKVIVALENTNÉ DEF.

σ/ρ JE ZLUČITEĽNÁ S $\alpha \Leftrightarrow$
$\forall [a_1]_\rho, \dots, [a_n]_\rho, [b_1]_\rho, \dots, [b_n]_\rho \in A/\rho$
$([a_i]_\rho, [b_i]_\rho) \in \sigma/\rho \Rightarrow$
↳ TOTO JE EKVIVALENTNÉ S $(a_i, b_i) \in \sigma$
$(\alpha([a_1]_\rho, \dots, [a_n]_\rho), \alpha([b_1]_\rho, \dots, [b_n]_\rho)) \in \sigma/\rho$
$\Leftrightarrow ([\alpha(a_1, \dots, a_n)]_\rho, [\alpha(b_1, \dots, b_n)]_\rho) \in \sigma/\rho$
$\Leftrightarrow (\alpha(a_1, \dots, a_n), \alpha(b_1, \dots, b_n)) \in \sigma$

VETA O HOMOMORFIZME: NECH $f: A \to B$ JE HOMOMORFIZMUS (ALGEBIER ROVNAKÉHO TYPU) A ρ JE KONGRUENCIA NA ALGEBRE A. POTOM EXISTUJE TAKÝ HOMOMORFIZMUS $g: A/\rho \to B$, ŽE $f = g \circ \Pi_\rho \Leftrightarrow \rho \subseteq \ker f$.

KEĎ EXISTUJE TAKÉ g, POTOM g JE IZOMORFIZMUS $\Leftrightarrow$ f JE ZOBRAZENIE NA A $\rho = \ker f$.

DOKAZ. a) PODĽA VIAC UVEDENÉHO TVRDENIA PLATÍ IMPLIKÁCIA $\Rightarrow$)
(HOMOMORFIZMUS JE ZOBRAZENIE)
$\Leftarrow$) PODĽA TEJ VIEM AK $\rho \subseteq \ker f$, POTOM EXISTUJE ZOBRAZENIE $g : A/\rho \to B$, TAKÉ, ŽE $f = g \cdot \Pi_\rho$.
DOKÁŽEME, ŽE g JE HOMOMORFIZMUS.
NECH α JE n-ÁRNA OPERÁCIA NA A (A) NA B)

$g(\alpha([a_1]_\rho, \dots, [a_n]_\rho)) =$ PODĽA DEFINÍCIE α NA A/ρ

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

$= f(\alpha(a_1, \dots, a_n)) =$ f JE ZÚŽENÍM $\subset \alpha$, T.J.

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

$= \alpha(g([a_1]_\rho), \dots g([a_n]_\rho))$.

b) g JE na $\Leftrightarrow$ f JE na, PRETOŽE Π_ρ JE na.
STAČÍ DOKÁZAŤ, ŽE g JE PROSTÉ $\Leftrightarrow$ $\rho = \ker f$.
$\Rightarrow$) g JE PROSTÉ. PODĽA a) JE $\rho \subseteq \ker f$.
NECH $(a,b) \in \ker f$, T.J. $f(a) = f(b)$
T.J. $g([a]_\rho) = g([b]_\rho) \Rightarrow [a]_\rho = [b]_\rho \Rightarrow (a,b) \in \rho$.
(g JE PROSTÉ)

12.11.2007/6
PETER ČERNO

MA1062 ALGEBRA I

$\Leftarrow$ $\rho = \ker f$, $g([a]_\rho) = g([b]_\rho)$

TJ. $f(a) = f(b)$

$\Rightarrow$ PODĽA DEFINÍCIE $\ker f$ JE $(a,b) \in \ker f = \rho$.

$\Rightarrow [a]_\rho = [b]_\rho \Rightarrow$ g JE PROSTÉ ZOBRAZENIE. ■

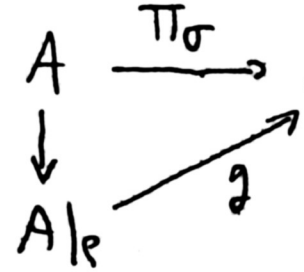
VETA (1. VETA O HOMOMORFIZME):
NECH $f: A \to B$ JE HOMOMORFIZMUS ALGEBIER ROVNAKÉHO TYPU. POTOM $f(A)$ JE ALGEBROU ROVNAKÉHO TYPU AKO A AJ B A JE TO PODAL. B. A $A/\ker f \cong f(A)$

DÔKAZ: f JE HOMOMORFIZMUS NA $f(A)$.
POUŽIJEME TVRDENIE UVEDENÉ VYŠŠIE PRE $\rho := \ker f$
$\Rightarrow$ EXISTUJE HOMOMORFIZMUS $g: \underbrace{A/\rho}_{A/\ker f} \to f(A)$

KEĎŽE PLATÍ $\rho = \ker f$, g JE IZOMORFIZMUS. □

VETA (2. VETA O IZOMORFIZME). NECH $\rho \subseteq \sigma$ SÚ KONGRUENCIE NA ALGEBRE A, POTOM
$A/\rho|_{\sigma/\rho} \cong A/\sigma$.

DÔKAZ:



$\ker \pi_\rho = \rho$, $\ker \pi_\sigma = \sigma$
PREDPOKLAD: $\rho \subseteq \sigma$

$g([a]_\rho) = \pi_\sigma(a) = [a]_\sigma$ JE HOMOMORFIZMUS NA A/σ.

PODĽA 1. VETY O HOMOMORFIZME

PRE HOMOMORFIZMUS g PLATÍ

$$A|_\varrho / \ker g \cong g(A|_\varrho) = A|_\sigma \qquad g \text{ je na}$$

$$\ker g = \{([a]_\varrho, [b]_\varrho) \in A|_\varrho^2 : \underbrace{g([a]_\varrho) = g([b]_\varrho)}_{\parallel \quad \parallel \quad [a]_\sigma \quad [b]_\sigma} \}$$

$$(a,b) \in \sigma$$

= PODĽA DEFINÍCIE σ/ϱ =

$= \sigma/\varrho$.

PRÍKLAD: $f_n : \mathbb{Z} \to \mathbb{Z}_n \quad f_n(k) := (k) \bmod n \quad n > 1$

f_n JE HOMOMORFIZMUS ALGEBIER

$\mathbb{Z}(+, \cdot, -, 0)$ A $\mathbb{Z}_n(+, \cdot, -, 0)$

PRVÁ VETA O IZOMORFIZME HOVORÍ, ŽE

$$\mathbb{Z}/\ker f_n \cong f_n(\mathbb{Z}) = \mathbb{Z}_n$$

$(x,y) \in \ker f_n \Leftrightarrow x \equiv_n y \Leftrightarrow n \mid (x-y)$

NECH $n = a \cdot b, \ a, b > 1$

NA $\mathbb{Z}/\ker f_n$ SI MÔŽEME VZIAŤ KONGRUENCIU

$\eta_a \leftrightarrow \equiv_a$  $\eta_a = \equiv_a / \equiv_n$

ZREJME $\equiv_n \subseteq \equiv_a$.

$$\mathbb{Z}_n|_{\equiv_n} / \eta_a \cong \mathbb{Z}/\equiv_a \cong \mathbb{Z}_a$$

12.11.2007 Mo
PETER ČERNO

MA1062 ALGEBRA I

ZVÄZY

ČIASTOČNÉ USPORIADANIE

DEFINÍCIA: RELÁCIU $\leq$ NA MNOŽINE S NAZVEME USPORIADANÍM, KEĎ JE REFLEXÍVNA, TRANZITÍVNA A SLABO ANTISYMETRICKÁ ($\forall a,b \in S \quad a \leq b \wedge b \leq a \Rightarrow a = b$)

PRÍKLADY: 1) $\leq$ NA $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Q}$ TVORIA USPORIAD.
2) X - MNOŽINA, $\subseteq$ (INKLÚZIA) NA $\mathcal{P}(X)$
3) RELÁCIA DELENIA $|$ NA $\mathbb{N}$
4) id_A NA A

DEFINÍCIA: NECH S JE MNOŽINA S USPORIADANÍM $\leq$. HOVORÍME, ŽE $s \in S$ JE NAJMENŠÍ (NAJVÄČŠÍ) PRVOK $A \subseteq S \Leftrightarrow s \in A$ A $\forall a \in A : s \leq a$ ($a \leq s$)

INFIMOM (SUPRÉMOM) MNOŽINY $A \subseteq S$ NAZVEME NAJVÄČŠÍ (NAJMENŠÍ) PRVOK MNOŽINY $\{s \in S \mid s \leq a \ \forall a \in A\}$ ($\{s \in S \mid a \leq s \ \forall a \in A\}$)

ZNAČÍME $\inf_{\leq}(A)$ ($\sup_{\leq}(A)$).

DVOJICU $(S, \leq)$ NAZVEME ZVÄZOM, KEĎ EXISTUJE inf A sup PRE VŠETKY DVOJPRVKOVÉ PODMNOŽINY A MNOŽINY S.

ZNAČÍME $\inf_{\leq}(\{a,b\}) = a \wedge b$ (PRIESEK)
$\sup_{\leq}(\{a,b\}) = a \vee b$ (SPOJENIE).

ÚPLNÝM ZVÄZOM BUDEME ROZUMIEŤ ZVÄZ, KDE EXISTUJE inf A sup PRE KAŽDÚ $A \subseteq S$.

PRÍKLADY: 1) $(\mathbb{N}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$
SÚ ZVÄZY, ALE NIE ÚPLNE ZVÄZY.

2) $(\mathcal{P}(X), \subseteq)$ JE ZVÄZ (DOKONCA ÚPLNÝ)
$\inf_{\subseteq}(\{A,B\}) = A \cap B$
$\sup_{\subseteq}(\{A,B\}) = A \cup B$.

3) $(\mathbb{N}, |)$ JE ZVÄZ (ALE NIE ÚPLNÝ)
$\inf_{|}(\{a,b\}) = \gcd(a,b)$
$\sup_{|}(\{a,b\}) = \operatorname{lcm}(a,b)$

4) (A, id_A) NIE JE ZVÄZ

14.11.2007 We
PETER ČERNO

EX: MAIB G2 ALGEBRA I

PRÍKLAD: NÁJDITE ∀ PODALGEBRY ALGEBRY $S_3(\circ, ^{-1}, id)$

$\circ$	(1,2,3)	(1,3,2)	(2,1,3)	(2,3,1)	(3,1,2)	(3,2,1)
(1,2,3)	(1,2,3)	(1,3,2)	(2,1,3)	(2,3,1)	(3,1,2)	(3,2,1)
(1,3,2)	(1,3,2)	(1,2,3)	(2,3,1)	(2,1,3)	(3,2,1)	(3,1,2)
(2,1,3)						
(2,3,1)						
(2,1,2)						
(3,2,1)						

NEVÝHODNÝ POSTUP

$\langle \emptyset \rangle = \{id\}$
$\langle S_3 \rangle = S_3$

POZOR! NÁJDENIA PODALGEBRA $A \subseteq S_3$ TAKÁ, ŽE $\emptyset \subseteq A$, MUSÍ OBSAHOVAŤ id !!!
UZAVRETOSŤ NA NULÁRNU OPERÁCIU

PRI PERMUTÁCIACH JE VHODNÉ POUŽÍVAŤ CYKLICKÝ ZÁPIS
BUDEME VYNECHÁVAŤ PEVNÉ BODY

$\langle (12) \rangle = \{id, (12)\}$
$\langle (13) \rangle = \{id, (13)\}$
$\langle (23) \rangle = \{id, (23)\}$
$\langle (123) \rangle = \{id, (123), (321)\} = A_3$ ALTERNUJÚCA GRUPA
$\langle (132) \rangle = \{id, (132), (123)\}$"

$\langle \{(12), (23)\} \rangle = \{id, (12), (23), (13)$

$(13) = (12) \cdot (23) \cdot (12)$ TOTO SÚ VŠETKY TRANSPOZÍCIE $\Rightarrow$ Z LIN. ALGEBRY $= S_3$.

$\langle \{(12), (123)\} \rangle = \{id, (12), (123), (13), \ldots\}$

$= S_3$

$(12) \cdot (123) = (23)$

NAŠLI SME CELKOVO 6 PODGRÚP.

NÁJDITE VŠETKY KONGRUENCIE:

$p, q \in S_n : \quad q(a) = b \qquad q = (\ldots)\ldots(\ldots \widehat{ab} \ldots)\ldots$

$(p \circ q \circ p^{-1})(p(a)) = p(b)$

TJ. $p \circ q \circ p^{-1} = \ldots(\ldots)\ldots(\ldots p(a)\, p(b) \ldots)\ldots$

$p = (127)(5346)$

$q = (14)(23)(576)$

$p \circ q \circ p^{-1} = (p(1)\ p(4))(p(2)\ p(3))(p(5)\ p(7)\ p(6)) =$

$= (26)(74)(315)$

$q \circ p \circ q^{-1} = (4362)(7215)$

14.11.2007/16
PETER ČERNO

EX: MA1062 ALGEBRA I

EXISTUJE PERMUTÁCIA $p \in S_8$ TAKÁ, ŽE

$$p \circ (1\ 7\ 5)(2\ 3\ 4\ 8) \circ p^{-1} =$$

$$= (1\ 2\ 4\ 5)(3\ 6\ 7)$$

NAPR.

$$p = (2\ 1\ 3)(8\ 5\ 7\ 6)$$

DVE PERMUTÁCIE SÚ KONJUGOVANÉ $\Leftrightarrow$ MAJÚ ROVNAKÝ TYP, TJ. CYKLY ROVNAKÝCH DĹŽOK. VO VŠEOBECNOSTI EXISTUJE VIACEJ TAKÝCH p.

NAPR. VO VYŠŠIE UVEDENOM PRÍKLADE MÁME (12) $3 \cdot 4 = 12$ TAKÝCH PERMUTÁCIÍ.

NÁJDITE PERMUTÁCIU $p \in S_9$:

$$(1\ 3\ 4)(5\ 9)(7\ 6\ 8) \circ p = p \circ (12)(345)(697)$$

$$p \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 9 & 1 & 3 & 4 & 7 & 6 & 8 & 2 \end{pmatrix} \circ p^{-1} =$$

$$= (5\ 9)(1\ 3\ 4)(7\ 6\ 8)(2)$$

$$p = (1\ 5\ 4\ 3)(2\ 9\ 6\ 7\ 8)$$

MÁME $2 \cdot 3 \cdot 3 \cdot 2 = 36$ MOŽNOSTÍ

GRUPA
$S_3(0, ^{-1}; id)$

PRÍKLAD: NÁJDITE VŠETKY KONGRUENCIE NA S_3.

VETA: KONGRUENCII ρ JEDNOZNAČNE ZODPOVEDÁ NORMÁLNA PODGRUPA H. (PRE GRUPU G)

a) $\rho \to [Id]_\rho$ JE NORMÁLNA PODGRUPA H

b) AK H JE NORMÁLNA PODGRUPA, POTOM ρ_H MOŽNO DEFINOVAŤ AKO

$$(p,q) \in \rho_H \Leftrightarrow p^{-1}q \in H.$$

PRE S_3 PLATÍ, ŽE:

$\rho = id$ JE KONGRUENCIA $\to$ PRÍSLUŠNÁ NORMÁLNA PODGRUPA JE ROZKLADOVÁ TRIEDA $[Id]_\rho = \{Id\}$

$\rho = S_3 \times S_3$ JE KONGRUENCIA $\to$ PRÍSLUŠNÁ NORMÁLNA PODGRUPA JE $[Id]_\rho = S_3$

H JE NORMÁLNA $\Leftrightarrow \forall s \in S_3 \; \forall h \in H : s \cdot h \cdot s^{-1} \in H$

ZREJME $\{Id\}$ A S_3 SÚ NORMÁLNE PODGRUPY.

ZOSTÁVA VYŠETRIŤ NORMALITU PODGRÚP:

$\langle (12) \rangle = \{id, (12)\}$ NIE JE NORMÁLNA PODGRUPA

$$(13) \cdot (12) \cdot (13)^{-1} = (32) \notin \langle (12) \rangle$$

V S_n NORMÁLNA PODGRUPA OBSAHUJÚCA TRANSPOZÍCIU $(a\ b)$ OBSAHUJE VŠETKY TRANSPOZÍCIE $(p(a)\ p(b))$

$\Rightarrow = S_n$.

14.11.2007 We
PETER ČERNO

EX: MAI062 ALGEBRA I

ZOSTÁVA NÁJSŤ PODGRUPU

$\{ id, (123), (132) \} = A_3$

$p \cdot id \circ p^{-1} = id$

MÁME TU VŠETKY PROJEKCIE,
VŠETKY PERMUTÁCIE MAJÚ + ZNAMIENKO

$sgn(p \circ q \circ p^{-1}) = sgn(p) \cdot sgn(q) \cdot sgn(p^{-1}) = sgn(q)$

$\Rightarrow$ $\{ id, (123), (132) \}$ JE NORMÁLNA PODGRUPA.

POPÍŠME PRÍSLUŠNÚ KONGRUENCIU ρ.

$(p, q) \in \rho \Leftrightarrow p^{-1} \circ q \in A_3$

ZREJME $p^{-1} \circ q \in A_3 \Leftrightarrow sgn(p) = sgn(q)$

PRÍKLAD: AKO VYZERÁ S_3/ρ_{A_3} (POPR. S_n/ρ_{A_n})?

$\{ A_n, (12) \cdot A_n \}$

$\circ$	$[id]_{\rho_{A_n}}$	$(12) \cdot A_n$
$A_n = [id]_{\rho_{A_n}}$	A_n	$[(12)]_{\rho_{A_n}}$
$(12) \cdot A_n$	$[(12)]_{\rho_{A_n}}$	A_n

JE IZOMORFNÁ S $\mathbb{Z}_2(+, -, 0)$ ↓ UNÁRNE $-$.

PRÍKLAD: DOKÁŽTE, ŽE ZOBRAZENIE GRUPY

$G(\bullet, ^{-1}, 1)$ DO GRUPY $\underbrace{S(G)}_{\text{PERMUTÁCIE } G \to G}(\circ, ^{-1}, Id)$

$g \longmapsto L_g \qquad L_g : G \to G \qquad L_g(h) \overset{def}{:=} g \circ h.$

a) DOKÁŽTE, ŽE TOTO ZOBRAZENIE PROSTÝ HOMOMORFIZMUS GRÚP ●.

KOREKTNOSŤ DEFINÍCIE L_g:

ZREJME L_g JE PROSTÉ A NA

$(L_g)^{-1} = L_{g^{-1}}$.

19.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

POZOROVANIE: M - MNOŽINA S USPORIADANÍM $\leq$
$\inf_{\leq}(\{m\}) = \sup_{\leq}(\{m\}) = m$.

$m \wedge m \qquad m \vee m$

POZNÁMKA: NECH $(M, \leq)$ JE ZVÄZ, POTOM
$\forall a,b,c \in M$ A PRE BINÁRNE OPERÁCIE $\wedge$ a $\vee$
NA M ($a \wedge b = \inf_{\leq}(\{a,b\})$, $a \vee b = \sup_{\leq}(\{a,b\})$)
PLATÍ:

(S1): $a \wedge b = b \wedge a$, $\quad a \vee b = b \vee a$
(S2): $a = a \wedge a = a \vee a$
(S3): $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
$a \vee (b \vee c) = (a \vee b) \vee c$
(S4): $a \vee (b \wedge a) = a$
$a \wedge (b \vee a) = a$

DÔKAZ: (S1) $\{a,b\} = \{b,a\}$
(S2) VID POZOROVANIE
(S3) DOKÁŽEME, ŽE $a \wedge (b \wedge c) = \inf_{\leq}(\{a,b,c\})$.
OZNAČME $d = a \wedge (b \wedge c)$.
PLATÍ $a \wedge$ ČOKOĽVEK $\leq a$ (VID DEF. $\wedge$)
$\Rightarrow d \leq a$
$b \wedge c \leq b, c$ Z TRANZITIVITY
ČOKOĽVEK $\wedge (b \wedge c) \leq b, c \Rightarrow d \leq b, c$.
VIDÍME, ŽE d JE DOLNÝ ODHAD MNOŽINY $\{a,b,c\}$.

BUĎ e PRVOK TAKÝ, ŽE $e \leq a, b, c$.

KEĎŽE $b \wedge c = \inf_{\leq}(\{b, c\})$ A e JE DOLNÝ ODHAD PRVKOV b A c, NUTNE (2 DEF. INFÍMA) $e \leq b \wedge c$.

MÁME $e \leq a, b \wedge c$ A PODOBNOU ÚVAHOU DOSTANEME $e \leq a \wedge (b \wedge c) = d$.

$\Rightarrow$ d JE NAJVÄČŠÍ DOLNÝ ODHAD MNOŽINY $\{a, b, c\}$, TJ. $d = a \wedge (b \wedge c) = \inf_{\leq}(\{a, b, c\})$.

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

$\Rightarrow$ $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

PODOBNE $a \vee (b \vee c) = (a \vee b) \vee c$. □

(S4) $a \leq a \vee$ KOKOĽVEK, TAKŽE $a \leq a \vee (b \wedge a)$

ĎALEJ $b \wedge a \leq a$, $a \leq a$, TJ.

a JE HORNÝ ODHAD PRVKOV a, $b \wedge a$

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

ZO SLABEJ SYMETRIE DOSTÁVAME $a = a \vee (b \wedge a)$.

POZNÁMKA: NECH $M(\wedge, \vee)$ JE ALGEBRA S BINÁRNYMI OPERÁCIAMI $\wedge$, $\vee$ SPĹŇAJÚCIMI (S1), ..., (S4). KED DEFINUJEME NA M RELÁCIU $\leq$ PREDPISOM: $a \leq b \Leftrightarrow b = a \vee b$, POTOM $(M, \leq)$ JE ZVÄZOM, PRE KTORÝ PLATÍ, ŽE PRE $\forall a, b \in M$: $a \wedge b = \inf_{\leq}(\{a, b\})$, $a \vee b = \sup_{\leq}(\{a, b\})$.

19.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

DÔKAZ: NAJSKÔR DOKÁŽEME, ŽE $b = a \vee b \Leftrightarrow a = a \wedge b$.

$\Rightarrow$) NECH $b = a \vee b$. POTOM $a \wedge b =$
$= a \wedge (a \vee b) \overset{S1}{=} a \wedge (b \vee a) \overset{S4}{=} a$.

$\Leftarrow$) NECH $a = a \wedge b$. POTOM $a \vee b =$
$= b \vee (a \wedge b) \overset{S4}{=} b$.

a) DOKÁŽEME, ŽE $\leq$ JE USPORIADANIE.

REFLEXIVITA: $a \vee a \overset{S2}{=} a \Rightarrow a \leq a$

TRANZITIVITA: $a \leq b$, $b \leq c$

TJ. $b = a \vee b$, $c = b \vee c$

STAČÍ DOKÁZAŤ, ŽE $a \vee c = c$:

$a \vee c = a \vee (b \vee c) \overset{S3}{=} (a \vee b) \vee c = b \vee c = c$. $\Rightarrow a \leq c$

ANTISYMETRIA (SLABÁ): $a \leq b$, $b \leq a$

$b = a \vee b$, $a = b \vee a$

$a = b \vee a \overset{S1}{=} a \vee b = b \Rightarrow a = b$. □

b) DOKÁŽEME, ŽE $x \vee y = \sup_{\leq}(\{x, y\})$ PRE $\forall x, y \in M$.

DOKÁŽEME, ŽE $x \vee y$ JE HORNÝ ODHAD $\{x, y\}$

$x \vee (x \vee y) \overset{S3}{=} (x \vee x) \vee y \overset{S2}{=} x \vee y$,

$\Rightarrow$ PODĽA DEF. $\leq$: $x \leq x \vee y$.

PODOBNE $y \vee (x \vee y) \overset{S1}{=} y \vee (y \vee x) \overset{S3}{=} (y \vee y) \vee x =$
$\overset{S1}{=} x \vee (y \vee y) \overset{S2}{=} x \vee y \Rightarrow y \leq x \vee y$.

NECH c JE HORNÝ ODHAD $\{x, y\}$, TJ. $x, y \leq c$.

DOKÁŽEME, ŽE $x \vee y \leq c$, TJ. $(x \vee y) \vee c = c$

PLATÍ $c = x \vee c$, $c = y \vee c$.

$c \vee (x \vee y) = (c \vee x) \vee y = c \vee y = c$. □ $\Rightarrow x \vee y = \sup_{\leq}(\{x, y\})$

PRÍKLAD: 1)  $(\mathbb{N}, \leq)$, ...

ZODPOVEDÁ ALGEBRA $\mathbb{N}(\underbrace{\min}_{\wedge}, \underbrace{\max}_{\vee})$ A NAOPAK.

2) $(\mathcal{P}(X), \subseteq)$ ZODPOVEDÁ ALGEBRA $\mathcal{P}(X)(\cap, \cup)$

3) $(\mathbb{N}, |)$ ZODPOVEDÁ ALGEBRA $\mathbb{N}(gcd, lcm)$

VETA: KEĎ JE $\mathcal{C}$ UZÁVEROVÝ SYSTÉM, POTOM $(\mathcal{C}, \subseteq)$ TVORÍ ÚPLNÝ ZVÄZ, KDE $\inf_{\subseteq} \mathcal{B} = \bigcap \mathcal{B}$ A $\sup_{\subseteq}(\mathcal{B}) = cl_{\mathcal{C}}(\bigcup \mathcal{B})$ $\boxed{\forall \mathcal{B} \subseteq \mathcal{C}}$

DÔKAZ. $\subseteq$ JE ZREJME USPORIADANIE.

PRE $\forall \mathcal{B} \subseteq \mathcal{C}$ $\bigcap \mathcal{B} \in \mathcal{C}$ A JE TO ZREJME INFIMUM.

PODOBNE $cl_{\mathcal{C}}(\bigcup \mathcal{B}) \in \mathcal{C}$

$\forall B \in \mathcal{B}$ $B \subseteq cl_{\mathcal{C}}(\bigcup \mathcal{B}) \Rightarrow \bigcup \mathcal{B} \subseteq cl_{\mathcal{C}}(\bigcup \mathcal{B})$

A $B \subseteq \bigcup \mathcal{B} \subseteq cl_{\mathcal{C}}(\bigcup \mathcal{B})$, TJ. $cl_{\mathcal{C}}(\bigcup \mathcal{B})$ JE HORNÝ ODHAD.

$cl_{\mathcal{C}}(\bigcup \mathcal{B})$ JE NAJMENŠÍ PRVOK OBSAHUJÚCI $\bigcup \mathcal{B}$.

$\Rightarrow$ DOSTÁVAME, ŽE $cl_{\mathcal{C}}(\mathcal{B})$ JE SUPRÉMUM.

PRÍKLAD: 1)  $A(d_i, i \in I)$ JE ALGEBRA

$\mathcal{A}$ = VŠETKY PODALGEBRY A

$\Rightarrow (\mathcal{A}, \subseteq)$ JE ZVÄZ, KTORÉMU ZODPOVEDÁ ALGEBRA $\mathcal{A}(\cap, \langle .. \cup .. \rangle)$

2) $A(d_i, i \in I)$ A $\mathcal{C}$ SÚ VŠETKY KONGRUENCIE NA A, POTOM $(\mathcal{C}, \subseteq)$ JE ZVÄZ, KT. ZODPOVEDÁ ALGEBRA $\mathcal{C}(\cap, \langle .. \cup .. \rangle)$.

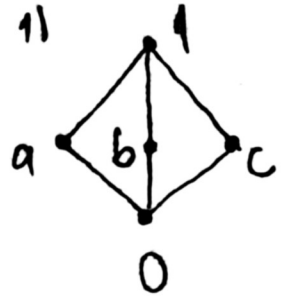
19.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

POZNÁMKA: KEĎ JE $M(\wedge, \vee)$ ZVÄZ $(M, \leq)$, POTOM AJ $M(\vee, \wedge)$ JE ZVÄZ $(M, \geq)$. (TZV. OPAČNÝ)
DÔKAZ. ZREJMÝ.

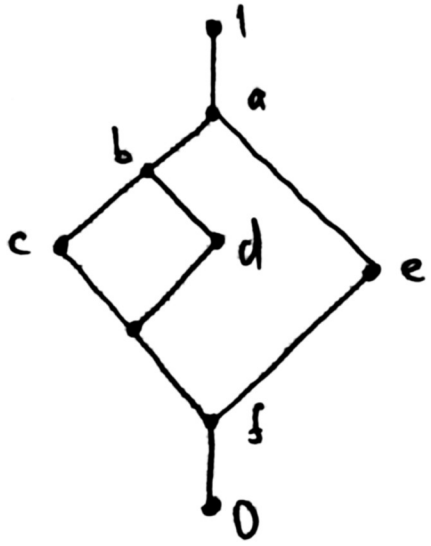
DEFINÍCIA: BUĎ $(M, \leq)$ ZVÄZ. POVIEME, ŽE PRE $a, b \in M$ a POKRÝVA b: $a \prec\cdot b$ KEĎ $a \neq b$, $a \leq b$ A PLATÍ $\forall c \in M$
$a \leq c \leq b \Rightarrow a = c \vee b = c$.
NECH e JE NAJMENŠÍ PRVOK M (NEMUSÍ EXISTOVAŤ) A f JE NAJVÄČŠÍ PRVOK M, POTOM ATÓMOM (KOATÓMOM) NAZVEME KAŽDÝ PRVOK $a \in M$ ($c \in M$): $e \prec\cdot a$ ($c \prec\cdot f$)
HASSEOVSKÝ DIAGRAM KONEČNÉHO ZVÄZU NAZVEME ORIENTOVANÝ GRAF, KDE $a \longrightarrow b$ (ALEBO $\overset{b}{|}_{a}$) $\Leftrightarrow a \prec\cdot b$.
VRCHOLY TVORIA PRVKY ZVÄZU.

PRÍKLAD:



$M = \{0, 1, a, b, c\}$
$a \vee c = 1$
$a \wedge b = 0$

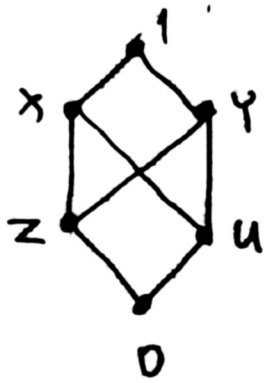
VŠIMNITE SI, ŽE $x \vee 0 = x$, $x \wedge 0 = 0$
$x \vee 1 = 1$, $x \wedge 1 = x$



$c \wedge e = f$

$c \vee d = b$

2) TOTO NIE JE HASSOV DIAGRAM ZVÄZU

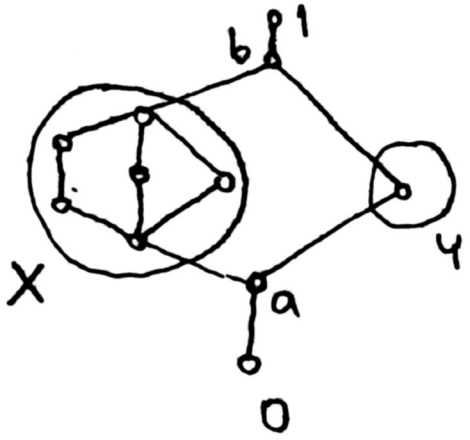


$\inf_c(\{x,y\})$ NEEXISTUJE

29. 11. 2007 We
PETER ČERNO

EX: MAI062 ALGEBRA I

HASSEOV DIAGRAM MNOŽINY $(S, \leq)$



$x \in X, y \in Y$

$\inf_{\leq}(x,y) = a$

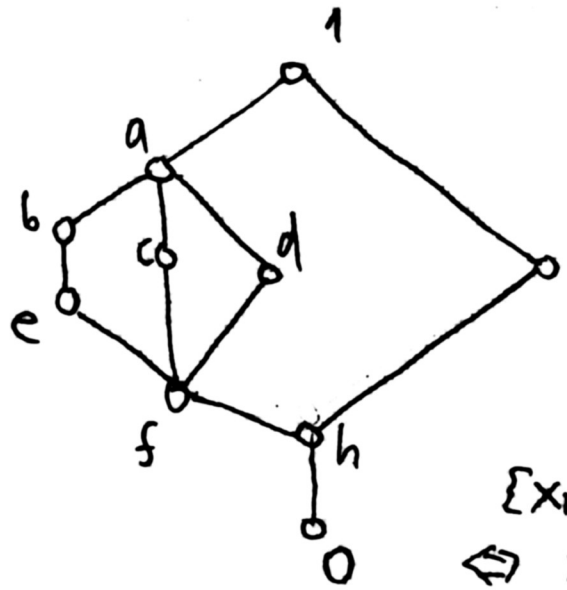
$\sup_{\leq}(x,y) = b$

ZREJME SA JEDNÁ O ZVÄZ

PRE POROVNATEĽNÉ VRCHOLY $x \leq y$
PLATÍ $\inf_{\leq}(\{x,y\}) = x$, $\sup_{\leq}(\{x,y\}) = y$.

KONEČNÝ ZVÄZ MÁ URČITE NAJVÄČŠÍ A NAJMENŠÍ PRVOK.

PRÍKLAD: NÁJDITE VŠETKY PODALGEBRY ALGEBRY $S(\wedge, \vee)$.



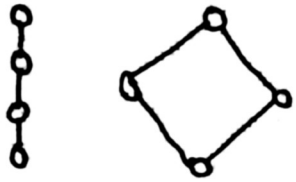
$\forall x \in S$
JE $\{x\}(\wedge, \vee)$
PODALGEBROU S.

$x \wedge x = x \vee x = x$

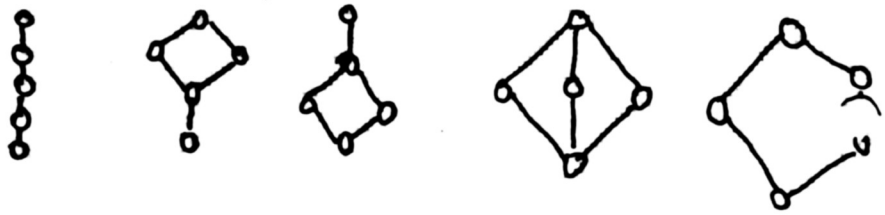
$\forall x, y \in S \; x \neq y$ JE
$\{x,y\}(\wedge, \vee)$ PODALGEBROU S
$\Leftrightarrow$ x A y SÚ POROVNATEĽNÉ

HASSEOV DIAGRAM $\{x,y\}$ JE

3-PRVKOVÉ ZVÄZY 

4-PRVKOVÉ ZVÄZY 

POZOR! $\{0, 1, g, b\}$ NIE JE PODZVÄZ, PRETOŽE $g \wedge b = h$.

5-PRVKOVÉ ZVÄZY 

6-PRVKOVÉ ZVÄZY ... ZAČNE BYŤ KOMPLIKOVANÉ

KAŽDÝ UZÁVEROVÝ SYSTÉM TVORÍ ZVÄZ.

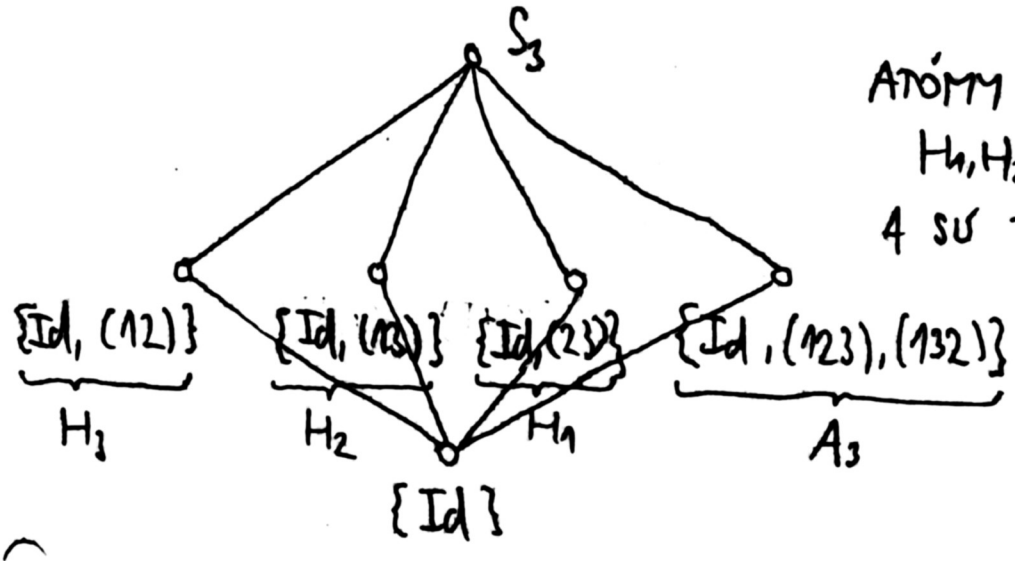
PRÍKLAD: NAKRESLITE HASSEOV DIAGRAM ZVÄZU VŠETKÝCH PODGRÚP GRUPY S_3.

$$\mathcal{G} = \{ \{Id\}, S_3, \{Id, (12)\}, \{Id, (13)\}, \{Id, (23)\}, A_3 \}$$
$$A_3 = \{Id, (123), (132)\}$$

CHCEME NAKRESLIŤ HASSEOV DIAGRAM $(\mathcal{G}, \subseteq)$.

21. 11. 2007 Ut
PETER ČERN

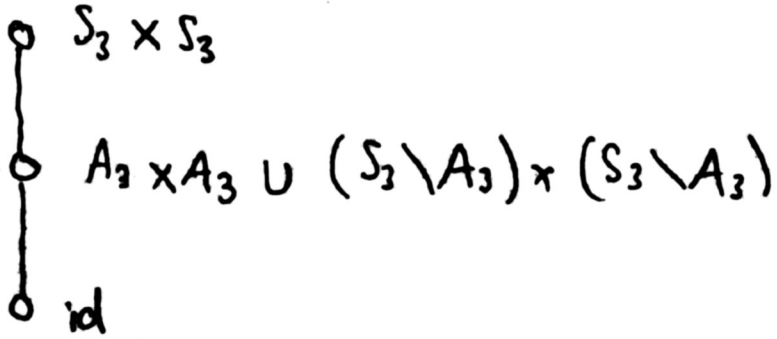
EX: MA1062 ALGEBRA I



ATÓMY SÚ PRÁVE ALGEBRY:
H_1, H_2, H_3, A_3
4 SÚ TO TIEŽ KOATÓMY

NAKRESLITE HASSEOV DIAGRAM ZVÄZU VŠETKÝCH KONGRUENCIÍ GRUPY S_3.

MÁME 3 KONGRUENCIE



NÁJDITE ATÓMY VO ZVÄZE $(\mathbb{N}, |)$.
PRÍSLUŠNÁ ALGEBRA JE $\mathbb{N}$ (gcd, lcm)

SÚ TO PRÁVE PRVOČÍSLA. PRE PRVOČÍSLO p PLATÍ:
$1 | k \wedge k | p \Rightarrow k = 1 \vee k = p$

A NAOPAK KAŽDÝ ATÓM JE ZREJME PRVOČÍSLO.

PRÍKLAD: NÁJDITE HASSEOV DIAGRAM ZVÄZU VŠETKÝCH KONGRUENCIÍ ALGEBRY $\mathbb{Z}_{12}(+,-,0)$.

UNÁRNA OPERÁCIA

ZREJME $\mathbb{Z}_{12}(+,-,0)$ JE GRUPA.

$\Rightarrow$ KAŽDÁ KONGRUENCIA JEDNOZNAČNE ZODPOVEDÁ NORMÁLNEJ PODGRUPE

KEĎŽE + JE KOMUTATÍVNA OPERÁCIA $\Rightarrow$
KAŽDÁ PODGRUPA GRUPY $\mathbb{Z}_{12}(+,-,0)$ JE NORMÁLNA.

PODGRUPY

$\{0\}$, $\mathbb{Z}_{12}$

$\updownarrow$ $\updownarrow$

id $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$

$\langle\{1\}\rangle = \mathbb{Z}_{12}$

$\langle\{2\}\rangle = \{0,2,4,6,8,10\}$

$\langle\{3\}\rangle = \{0,3,6,9\}$

$\langle\{4\}\rangle = \{0,4,8\}$

$\langle\{5\}\rangle = \mathbb{Z}_{12}$ PLATÍ $\langle a\rangle = \langle \gcd(a,12)\rangle$

$\langle\{6\}\rangle = \{0,6\}$

$\langle\{7\}\rangle = \mathbb{Z}_{12}$

$\langle\{8\}\rangle = \{0,4,8\}$

$\langle\{9\}\rangle = \{0,3,6,9\}$

$\langle\{10\}\rangle = \langle\{2\}\rangle$

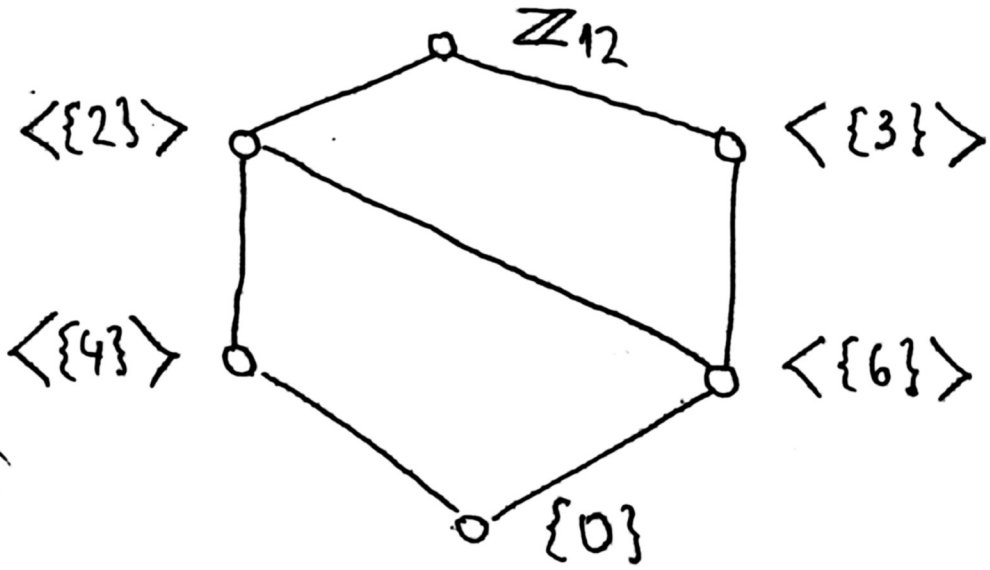
$\langle\{11\}\rangle = \mathbb{Z}_{12}$

ZREJME $\langle\{a,b\}\rangle = \langle\{\gcd(a,b)\}\rangle$

PODOBNE PRE n-GENEROVANÉ PODGRUPY

21.11.2007 Mo
PETER ČERNO

EX: MA1062 ALGEBRA I



26.11.2007Mo
PETER ČERNO

MAI062 ALGEBRA I

POZNÁMKA: BUĎ $(S, \leq)$ SVAZ A $a,b,c \in S$.
KEĎ $a \leq c$, POTOM $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

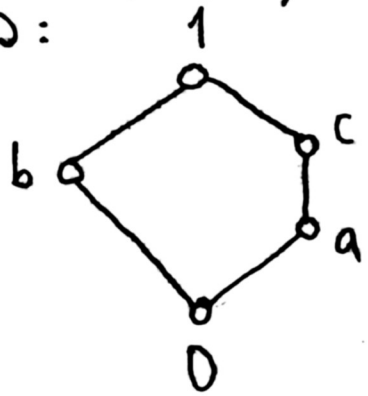
DÔKAZ: $a \leq a \vee b$
$b \wedge c \leq b \leq a \vee b$ $\Big\}$ $a \vee (b \wedge c) \leq a \vee b$

$a \leq c$ (PODĽA PREDPOKLADU)
$b \wedge c \leq c$ $\Big\}$ $a \vee (b \wedge c) \leq c$ $\Big\}$ QED.

DEFINÍCIA: O ZVÄZE $(S, \leq)$ POVIEME, ŽE JE MODULÁRNY, KEĎ PRE $\forall a,b,c$ PLATÍ: $a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$.

PRÍKLAD: 1) ZVÄZ V PODPRIESTOROV VEKTOROVÉHO PRIESTORU $(\subseteq)$.
2) $(\mathcal{P}(X), \subseteq)$
3) $(\mathbb{N}, |)$
4) AKÝKOĽVEK LINEÁRNE USPORIADANÝ ZVÄZ.
NAPR. $(\mathbb{Z}, \leq)$.

PRÍKLAD:



$a \leq c$

$a \vee \underbrace{(b \wedge c)}_{0} = a$ ≠

$\underbrace{(a \vee b)}_{1} \wedge c = c$

DEFINÍCIA: BUĎ $(A, \leq)$ A $(B, \leq)$ ZVÄZY A $f: A \to B$.
POVIEME, ŽE f JE MONOTÓNNE, KEĎ PLATÍ
$a_1 \leq a_2 \Rightarrow f(a_1) \leq f(a_2) \quad \forall a_1, a_2 \in A$.

POZOROVANIE: ⟲ HOMOMORFIZMUS ZVÄZOV JE MONOTÓNNY.

DÔKAZ: $f: A \to B$ HOMOMORFIZMUS

$a_1 \leq a_2 \Rightarrow a_2 = a_1 \vee a_2 \Rightarrow f(a_2) = f(a_1 \vee a_2) =$ f JE HOM.
$= f(a_1) \vee f(a_2) \Rightarrow f(a_1) \leq f(a_2)$. ■

VETA: BIJEKCIA ZVÄZOV f JE IZOMORFIZMUS ⟺
f A f^{-1} SÚ MONOTÓNNE.

DÔKAZ: ⇒) AK JE f IZOMORFIZMUS ⇒ f^{-1} JE IZOMORFIZMUS
⇒ f AJ f^{-1} SÚ PODĽA VYŠŠIE UVEDENEJ POZNÁMKY MONOTÓNNE.

⇐) DOKÁŽEME ZLUČITEĽNOSŤ S $\vee$. $f: S_1 \to S_2$

$a, b \in S_1$. ZREJME $a, b \leq a \vee b$.

⇒ Z MONOTÓNIE f PLATÍ

$$\left.\begin{array}{l} f(a) \leq f(a \vee b) \\ f(b) \leq f(a \vee b) \end{array}\right\} f(a) \vee f(b) \leq f(a \vee b)$$

$$\left.\begin{array}{l} f(a) \leq f(a) \vee f(b) \\ f(b) \leq f(a) \vee f(b) \end{array}\right\} \begin{array}{l} f^{-1} \text{ JE TIEŽ MONOTÓNNE} \\ \text{ZOBRAZENIE} \end{array}$$

$$\underbrace{f^{-1}(f(a))}_{a}, \underbrace{f^{-1}(f(b))}_{b} \leq f^{-1}(f(a) \vee f(b)) \leq a \vee b$$

↳ $a \vee b \leq f^{-1}(f(a) \vee f(b))$

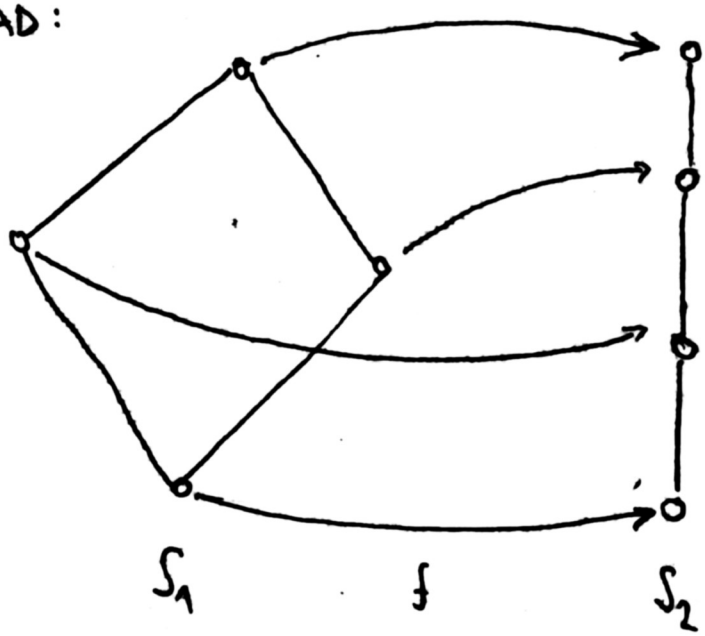
⇒ NUTNE $f^{-1}(f(a) \vee f(b)) = a \vee b$

⇒ $f(a) \vee f(b) = f(a \vee b)$.

26.11.2007 Mo
PETER ČERNO

MA1062 ALGEBRA I

PRÍKLAD:



f JE MONOTÓNNA BIJEKCIA
A ZÁROVEŇ f NIE JE IZOMORFIZMUS
ZVÄZOV $(S_1, \leq)$, $(S_2, \leq)$.
[$\Leftrightarrow$ f^{-1} NIE JE MONOTÓNNE]

POZNÁMKA: NECH $\mathcal{C}$ JE UZÁVEROVÝ SYSTÉM
OBSAHNÚTÝ V MNOŽINE $\forall$ EKVIVALENCIÍ NA A,
NECH $\mathcal{N} \subseteq \mathcal{P}(A)$, $\varrho \in A$, TAK, ŽE PLATÍ: $\forall \varrho, \eta \in \mathcal{C}$:

1) $[e]_\varrho \in \mathcal{N}$
2) $\forall N \in \mathcal{N}\ \exists \xi \in \mathcal{C}: N = [e]_\xi$
3) $[e]_\varrho \subseteq [e]_\eta \Rightarrow \varrho \subseteq \eta$

POTOM $\mathcal{N}$ TVORÍ UZÁVEROVÝ SYSTÉM (TEDA ZV'Z)
A $\varphi: \mathcal{C} \to \mathcal{N}$: $\varphi(\varrho) \overset{\text{def.}}{=} [e]_\varrho$ JE
IZOMORFIZMUS ZVÄZOV $(s \subseteq)$

DÔKAZ: $\mathcal{C}$ JE UZÁVEROVÝ SYSTÉM (EKVIVALENCIÍ) NAD $A \times A$.

$\Rightarrow A \times A \in \mathcal{C}$. $A = [e]_{A\times A} \overset{(1)}{\in} \mathcal{N}$.

NECH $N_i \in \mathcal{N}\ \forall i \in I \overset{(2)}{\Rightarrow} \exists \xi_i \in \mathcal{C} : N_i = [e]_{\xi_i}$

KEĎŽE $\mathcal{C}$ JE UZÁV. SYS., NUTNE $\bigcap \xi_i \in \mathcal{C}$.

ĽAHKO NAHLIADNUŤ, ŽE $\bigcap N_i = \bigcap [e]_{\xi_i} =$

$= [e]_{\bigcap \xi_i} \overset{(1)}{\in} \mathcal{N}$

$\Rightarrow$ TÝM SME DOKÁZALI, ŽE $\mathcal{N}$ JE UZÁVEROVÝ SYSTÉM.

ĎALEJ DOKÁŽEME, ŽE φ JE DOBRE DEFINOVANÉ.

TO JE VIDIEŤ Z PODMIENKY (1)

Z PODMIENKY (2) VIDÍME, ŽE φ JE NA.

ĎALEJ φ JE PROSTÉ $\Leftrightarrow$ $\varphi(\rho) \overset{\in}{=} \varphi(\xi) \Rightarrow \rho \overset{\subseteq}{=} \xi$

TO DOSTÁVAME, KEĎ ZX POUŽIJEME PODMIENKU (3).

$\Rightarrow$ DOKÁZALI SME, ŽE φ JE BIJEKCIA.

ZOSTÁVA DOKÁZAŤ, ŽE φ AJ φ^{-1} SÚ MONOTÓNNE (VZHĽADOM K $\subseteq$).

ZREJME $\rho \subseteq \xi \Rightarrow [e]_\rho \subseteq [e]_\xi$. MONOTÓNNOSŤ φ

MONOTÓNNOSŤ φ^{-1} PLYNIE Z (3).

$\Rightarrow$ φ JE IZOMORFIZMUS.

VETA: MNOŽINA VŠETKÝCH NORMÁLNYCH PODGRUP ĽUBOVOĽNEJ PEVNEJ GRUPY G TVORÍ ZVÄZ, KTORÝ JE IZOMORFNÝ ZVÄZU VŠETKÝCH KONGRUENCIÍ NA GRUPE G.

26.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

DÔKAZ: $G(\cdot, ^{-1}, 1)$ GRUPA, POLOŽÍME $e = 1$

ℓ = ZVÄZ VŠETKÝCH KONGRUENCIÍ NA $G(\cdot, ^{-1}, 1)$

η = ZVÄZ NORMÁLNYCH PODGRÚP GRUPY $G(\cdot, ^{-1}, 1)$.

(1) $[1]_\rho$ JE NORMÁLNA PODGRUPA GRUPY G $\forall \rho \in \ell$.

(2) $\forall N \in \eta$ VYROBÍME KONGRUENCIU ξ

$(a,b) \in \xi \overset{\text{def.}}{\Leftrightarrow} a^{-1}b \in N$. (VIĎ VETA ...)

PLATÍ $[1]_\xi = N$.

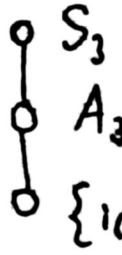
(3) $[1]_\rho \subseteq [1]_\xi \Rightarrow$

$(a,b) \in \rho \Rightarrow a^{-1}b \in [1]_\rho \subseteq [1]_\xi \Rightarrow a^{-1}b \in [1]_\xi$

$\Rightarrow (a,b) \in \xi$, t.j. $\rho \subseteq \xi$.

OVERILI SME VŠETKY PODMIENKY VYŠŠIE UVEDENEJ POZNÁMKY. $\varphi(\rho) \overset{\text{def}}{=} [1]_\rho$ JE IZOMORFIZMUS ℓ A η

PRÍKLAD: HASSEOV DIAGRAM ZVÄZU VŠETKÝCH KONGRUENCIÍ GRUPY $S_3(\circ, ^{-1}, id)$ JE ROVNAKÝ AKO HASSEOV DIAGRAM ZVÄZU NORMÁLNYCH PODGRÚP GRUPY $S_3(\circ, ^{-1}, id)$.



PRÍKLAD: O - OBJEKTY, V - VLASTNOSTI OBJEKTOV,
$\rho \subseteq O \times V$ $\quad (o,v) \in \rho \overset{def.}{\Leftrightarrow}$ OBJEKT o MÁ VLASTNOSŤ v

$\alpha_\rho : \mathcal{P}(O) \to \mathcal{P}(V)$, $\beta_\rho : \mathcal{P}(V) \to \mathcal{P}(O)$

$X \subseteq O : \alpha_\rho(X) \overset{def}{=} \{v \in V \mid (o,v) \in \rho \ \forall o \in X\}$

$Y \subseteq V : \beta_\rho(Y) \overset{def}{=} \{o \in O \mid (o,v) \in \rho \ \forall v \in Y\}$

α_ρ A β_ρ SÚ PRÍKLADOM TZV. GALOISOVEJ KORESPOND.

GALOISOVA KOREJP. : $\alpha : \mathcal{P}(O) \to \mathcal{P}(V)$, $\beta : \mathcal{P}(V) \to \mathcal{P}(O)$

(1) $X_1 \subseteq X_2 \subseteq O \Rightarrow \alpha(X_1) \supseteq \alpha(X_2)$

$Y_1 \subseteq Y_2 \subseteq V \Rightarrow \beta(Y_1) \supseteq \beta(Y_2)$

(2) $[X_1 \subseteq X_2 \subseteq O \Rightarrow \beta\cdot\alpha(X_1) \subseteq \beta\cdot\alpha(X_2)]$

$X \subseteq O \Rightarrow X \subseteq \beta\cdot\alpha(X)$

$Y \subseteq V \Rightarrow Y \subseteq \alpha\cdot\beta(Y)$

VLASTNOSTI GALOISOVEJ KORESPONDENCIE:

a) $\underbrace{\alpha\cdot\beta}_{\mathcal{B}}$ A $\underbrace{\beta\cdot\alpha}_{\mathcal{A}}$ SÚ UZÁVEROVÉ OPERÁTORY

b) $\mathcal{B}$ $\quad$ $\mathcal{A}$ SÚ ZODPOVEDAJÚCE UZÁVEROVÉ SYST.

b) $\alpha(\mathcal{A}) \subseteq \mathcal{B}$

$\beta(\mathcal{B}) \subseteq \mathcal{A}$

c) RESTRIKCIA α NA $\mathcal{A} \to \mathcal{B}$ SÚ BIJEKCIE

β NA $\mathcal{B} \to \mathcal{A}$

$\beta\cdot\alpha$ A $\alpha\cdot\beta$ SÚ IDENTITY NA $\mathcal{A}$, RESP. $\mathcal{B}$.

26.11.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I ZÁP. PÍSOMKA

NECH $G(\cdot, ^{-1}, 1)$ JE GRUPA, ρ ~~EKVIVALENCIA~~ RELÁCIA NA G.

POTOM ρ JE KONGRUENCIA $\Leftrightarrow$

$[1]_\rho$ JE NORMÁLNA PODGRUPA GRUPY G

A $(a,b) \in \rho \Leftrightarrow a^{-1}b \in [1]_\rho$

DÔKAZ: PREDPOKLADAJME, ŽE ρ JE KONGRUENCIA NA G, TJ. ρ JE EKVIVALENCIA ZLÚČITEĽNÁ S OPERÁCIAMI $\cdot$ A $^{-1}$ (A TAKTIEŽ AUTOMATICKY S 1).

DOKÁŽTE, ŽE $[1]_\rho$ JE [redacted] PODGRUPA GRUPY G.

NECH $a,b \in [1]_\rho$, TJ. $(1,a), (1,b) \in \rho$

DOKÁŽTE, ŽE $a \cdot b \in [1]_\rho$. (TJ. UZAVRETOSŤ NA $\cdot$)

ZREJME $(1 \cdot 1, a \cdot b) \in \rho$ (ZLÚČITEĽNOSŤ $\cdot$ S ρ)

$\Rightarrow a \cdot b \in [1]_\rho$

DOKÁŽTE, ŽE $a^{-1} \in [1]_\rho$. $(1,a) \in \rho \Rightarrow (1^{-1}, a^{-1}) \in \rho$

TAKŽE $a^{-1} \in [1]_\rho$. (ZLÚČITEĽNOSŤ $^{-1}$ S ρ)

NAKONIEC $(1,1) \in \rho \Rightarrow 1 \in [1]_\rho$.

DOKÁŽTE, ŽE $[1]_\rho$ JE NORMÁLNA PODGRUPA GRUPY G.

NECH $h \in [1]_\rho$, TJ. $(1,h) \in \rho$, $g \in G$.

DOKÁŽTE, ŽE $g \cdot h \cdot g^{-1} \in [1]_\rho$,

TJ. $(1, g \cdot h \cdot g^{-1}) \in \rho$

$(g,g), (1,h) \in \rho \Rightarrow (g \cdot 1, g \cdot h) \in \rho$

$(g, g \cdot h), (g^{-1}, g^{-1}) \in \rho \Rightarrow (g \cdot g^{-1}, g \cdot h \cdot g^{-1}) \in \rho$

$\Rightarrow g \cdot h \cdot g^{-1} \in [1]_\rho$.

NAKONIEC DOKÁŽTE $(a,b) \in \rho \Leftrightarrow a^{-1}b \in [1]_\rho$

$(a^{-1}, a^{-1}), (a,b) \in \rho \Leftrightarrow (1, a^{-1}b) \in \rho$ □

NECH N JE NORMÁLNA PODGRUPA GRUPY G

DEFINUJME ρ: $(a,b) \in \rho \Leftrightarrow a^{-1}b \in N$.

DOKÁŽTE, ŽE ρ JE EKVIVALENCIA NA G

$1 \in N \quad \forall a \in G \quad a^{-1}a = 1 \in N \Rightarrow (a,a) \in \rho$

$(a,b) \in \rho \Rightarrow a^{-1}b \in N \Rightarrow (a^{-1}b)^{-1} \in N$, t.j.

$b^{-1}a \in N \Rightarrow (b,a) \in \rho$

$(a,b) \in \rho \wedge (b,c) \in \rho \Rightarrow a^{-1}b \in N \wedge b^{-1}c \in N$

$\Rightarrow (a^{-1}b)\cdot(b^{-1}c) = a^{-1}c \in N \Rightarrow (a,c) \in \rho$

DOKÁŽTE, ŽE ρ JE ZLUČITEĽNÁ S $\cdot$

NECH $(a_1, a_2), (b_1, b_2) \in \rho$. DOKÁŽTE, ŽE $(a_1 \cdot b_1, a_2 \cdot b_2) \in \rho$.

$a_1^{-1}a_2 \in N, \quad b_1^{-1}b_2 \in N$.

CHCEME DOKÁZAŤ, ŽE $(a_1 \cdot b_1)^{-1} \cdot (a_2 \cdot b_2) =$

$= b_1^{-1} \cdot a_1^{-1} \cdot a_2 \cdot b_2 \in N$

N JE NORMÁLNA T. $\forall h \in N \; \forall g \in G : g \cdot h \cdot g^{-1} \in N$.

$a_1^{-1} \cdot a_2 \in N \Rightarrow b_1^{-1} \cdot a_1^{-1} \cdot a_2 \cdot b_1 \in N, \quad b_1^{-1} \cdot b_2 \in N \Rightarrow$

$b_1^{-1} \cdot a_1^{-1} \cdot a_2 \cdot b_2 \in N$ □

DOKÁŽTE, ŽE ρ JE ZLUČITEĽNÁ S $^{-1}$

NECH $(a,b) \in \rho$. DOKÁŽTE, ŽE $(a^{-1}, b^{-1}) \in \rho$.

$a^{-1}b \in N \Rightarrow ba^{-1} \in N$

$a^{-1}b \in N \Rightarrow ba^{-1}bb^{-1} \in N$ T. $ba^{-1} \in N$

ZREJME ρ JE ZLUČITEĽNÁ S 1

NAKONIEC DOKÁŽEME, ŽE $N = [1]_\rho$, T. $\forall a \in N : (1,a) \in \rho$.

$a \in N \Leftrightarrow 1^{-1}a \in N \Leftrightarrow (1,a) \in \rho$ ■

27.11.2007 Tu
PETER ČERNO

MAI062 ALGEBRA I – ZÁP. PÍSOMKA

PRÍKLAD:

o	a	b	c
a	c	b	a
b	b	a	b
c	a	b	c

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

1) V PODALGEBRY ALGEBRY $A(o)$

$\emptyset$, $\{c\}$, $\{a,c\}$, $\{a,b,c\}$

$\langle a \rangle = \{a, c\}$

$\langle b \rangle = \{b, a, c\}$

$\langle c \rangle = \{c\}$

2) PODALGEBRY ALG. $A(o,a)$: $\{a,c\}$, $\{a,b,c\}$

3) PODALG. ALG. $A(*)$

$\langle a \rangle = \{a\}$

$\langle b \rangle = \{b, c, a\}$

$\langle c \rangle = \{c, b, a\}$

4) KONGRUENCIE $A(o)$

Id, $A \times A$

$a \sim b \Rightarrow c \sim b$

$b \sim c \Rightarrow a \sim b$

$a \sim a$, $a \sim b \Rightarrow a \circ a \sim a \circ b$

o	a	c	b
a	c	a	b
c	a	c	b
b	b	b	a

NÁJDITE VŠETKY KONGRUENCIE GRUPY $S_3(\circ, ^{-1}, Id)$

NAJSKÔR PODGRUPY: $\{Id\}, S_3$

$\langle (12) \rangle = \{Id, (12)\}$ $\quad (12)\circ(12) = Id$

$\langle (13) \rangle = \{Id, (13)\}$

$\langle (23) \rangle = \{Id, (23)\}$

$(12)\circ(23) = (123)$

~~$(123)\circ(23) = (12)$~~ MÁME V TRANSPOZÍCIE

$(123)\circ(12) = (13)$ $\Rightarrow$ GEN. S_3

$\langle (123) \rangle = \{Id, (123), (132)\} = A_3$

$(123)\circ(123) = (132)$

$(123)\circ(132) = Id$

HĽADÁME NORMÁLNE PODGRUPY:

$\{Id\}$, S_3 SÚ NORMÁLNE

$(12)\circ(13)\circ(12)^{-1} = (23)$ TJ. $\{Id, (ab)\}$ NIE SÚ N.

$(12)\circ(123)\circ(12)^{-1} = (213)$ ... A_3 JE NORMÁLNA

MÁME 3 N. PODGRUPY: $\{Id\}, A_3, S_3$

27.11.2007 Ty
PETER ČERNO

MAI062 ALGEBRA I – ZÁP. PÍSOMKA

KEĎ N JE NORMÁLNA PODGRUPA GRUPY G,
POTOM ZODPOVEDAJÚCA KONGRUENCIA NA G JE
DEFINOVANÁ AKO $(a,b) \in \rho \Leftrightarrow a^{-1}b \in N$.

PRE $N = \{id\}$ $a^{-1}b = id \Leftrightarrow a = b$, T. $\rho = id$
PRE $N = S_3$ JE VŽDY $a^{-1}b \in N \Rightarrow \rho = S_3 \times S_3$
NAKONIEC $a^{-1}b \in A_3 \Leftrightarrow sgn(a^{-1}b) = 1$
$\Leftrightarrow sgn\, a = sgn\, b$

1) V PODALGEBRE A KONGRUENCIE ALG. $C = \{a, b, c, d, e, f\}$
$x \odot y = x$. $C(\odot)$
ZREJME KAŽDÁ $D \subseteq C$ JE PODALG. $x, y \in D \Rightarrow x \odot y = x \in D$.
NECH ρ JE EKV. NA C.
$(x_1, y_1)\, \theta_1\, (x_2, y_2) \in \rho \Rightarrow (x_1 \odot x_2, y_1 \odot y_2) =$
$= (x_1, y_1) \in \rho \Rightarrow \rho$ JE KONGR.

2) PRE $\mathbb{Z}_n(+)$ ZREJME IBA 2 PODALGEBRY $\emptyset$ A $\mathbb{Z}_n$
NECH $(x,y) \in \rho \Rightarrow (x^+, y^+)$ MUSÍ PATRIŤ DO $\rho \Rightarrow$
id, $\mathbb{Z}_n \times \mathbb{Z}_n$ SÚ KONGR. $(0, y-x) \in \rho$

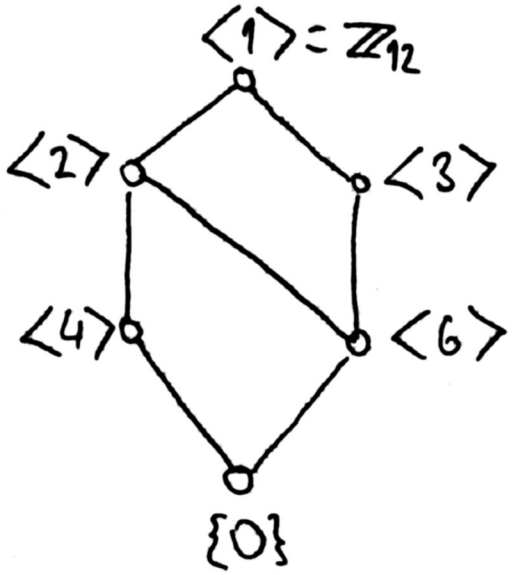
PRE KAŽDÉHO DELITEĽA n VIEME URČIŤ
1 KONGRUENCIU

$n = p_1^{e_1} \dots p_m^{e_m}$ MÁ PRÁVE $(e_1+1) \dots (e_m+1)$ KONGR.

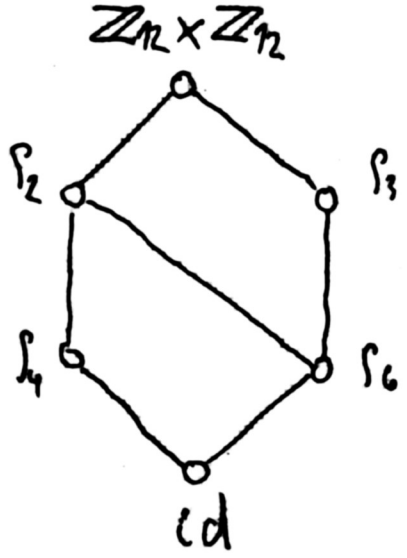
28.11.2007 Wk
PETER ČERNO

EX: MA1062 ALGEBRA I

VŠETKY PODALGEBRY ALGEBRY $\mathbb{Z}_{12}(+,-,0)$ SÚ NORMÁLNE, HASSEOV DIAGRAM JE IZOMORFNÝ ...



$\cong$



ZVÄZ NORMÁLNYCH PODGRUP

ZVÄZ KONGRUENCIÍ

$(a,b) \in \rho_k \Leftrightarrow a^{-1}b \in \langle k \rangle$

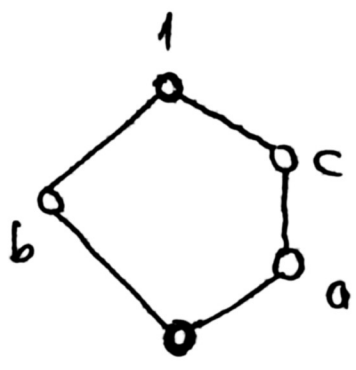
$b-a \in \langle k \rangle \Leftrightarrow k \mid b-a$

ZVÄZ S JE MODULÁRNY: $\forall a,b,c$

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

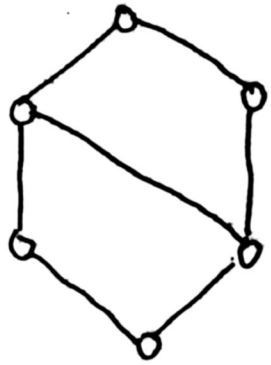
$\leq$ PLATÍ VŠEOBECNE

ZVÄZ



NIE JE MODULÁRNY !!

$a \vee \underbrace{(b \wedge c)}_{0} = a \qquad \underbrace{(a \vee b)}_{1} \wedge c = c$

POZOR: ZVÄZ  JE NEMODULÁRNY !!!

DOKÁŽTE, ŽE ZVÄZ NORMÁLNYCH PODGRUP $(\mathcal{N}, \subseteq)$ GRUPY $G(\circ, ^{-1}, 1)$ JE MODULÁRNY.

PRÍSLUŠNÁ ALGEBRA JE $\mathcal{N}(\cap, \cdot)$,

KDE PRE $A, B \in \mathcal{N}$ JE $A \cdot B \overset{def}{=} \{ab \mid a \in A, b \in B\}$

DOKÁŽTE, ŽE $A \cdot B = \sup_{\subseteq} \{A, B\}$ V $\mathcal{N} = cl_{\mathcal{N}}(A \cup B)$.

ZREJME $A \subseteq A \cdot B$, $B \subseteq A \cdot B$.

DOKÁŽTE: $A \cdot B$ JE UZAVRETÁ NA $\cup$ OPERÁCIE.

A ŽE $A \cdot B \in \mathcal{N}$

1) $A \cdot B \overset{!}{=} B \cdot A$

$\supseteq$

$a \in A, b \in B \quad bab^{-1} \in A, b \in B$

$ba \in BA \quad \Rightarrow ba \in A \cdot B$

$1 \cdot 1 \in AB \qquad (ab)^{-1} = b^{-1}a^{-1} \in BA = AB$

$a_1 b_1 \cdot a_2 b_2 = a_1 \cdot \bar{a}_2 \cdot \bar{b}_1 \cdot b_2 \in AB$

$\exists \bar{a}_2, \bar{b}_1 : b_1 a_2 = \bar{a}_2 \bar{b}_1$, PRETOŽE $AB = BA$

$g \in G \quad g^{-1}(a \cdot b) \cdot g = (g^{-1} a\, g)(g^{-1} b\, g) \in AB$ ■

03.12.2007 Mo
PETER ČERNO

MAL062 ALGEBRA I

GRUPY

POZNÁMKA: BUĎ $f: G \to H$, KDE $G(\cdot, ^{-1}, 1)$ A $H(\cdot, ^{-1}, 1)$ SÚ GRUPY, ZLUČITEĽNÉ S $\cdot$.
POTOM f JE HOMOMORFIZMUS.
DÔKAZ: $f(1) = f(1.1) = f(1) \cdot f(1)$ (ZLUČITEĽNOSŤ S $\cdot$)
KEĎŽE V H EXISTUJE $(f(1))^{-1}$, NUTNE:
$1 = f(1)$. (ASOCIATIVITA $\cdot$)
NECH $g \in G$. CHCEME DOKÁZAŤ $f(g^{-1}) = (f(g))^{-1}$
$f(1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$
PODOBNE $f(1) = f(g^{-1} \cdot g) = f(g^{-1}) \cdot f(g)$
$\Rightarrow$ $f(g^{-1})$ JE INVERZNÝ PRVOK K $f(g)$.

DEFINÍCIA: $G(\cdot, ^{-1}, 1)$ JE GRUPA, $H, K \subseteq G$ A $g \in G$. $HK = \{h \cdot k \mid h \in H, k \in K\}$
ĎALEJ $gH = \{g \cdot h \mid h \in H\}$,
$Hg = \{h \cdot g \mid h \in H\}$.

DEFINÍCIA: RELÁCIA NA G PRE KAŽDÚ PODGRUPU $H \subseteq G$
a) $r \bmod H$: $(a,b) \in r \bmod H \Leftrightarrow a \cdot b^{-1} \in H$.
b) $l \bmod H$: $(a,b) \in l \bmod H \Leftrightarrow a^{-1} \cdot b \in H$.

POZNÁMKA: BUĎ $G(\cdot, ^{-1}, 1)$ GRUPA A H JEJ PODGRUPA. POTOM PLATÍ
(1) $r \bmod H$ A $l \bmod H$ SÚ EKVIVALENCIE NA G.
(2) $(a,b) \in r \bmod H \Leftrightarrow (a^{-1}, b^{-1}) \in l \bmod H \quad \forall a,b \in G$.

(3) $|G/_{r\mathrm{mod}H}| = |G|_{\ell\mathrm{mod}H}|$ NEJEDNÁ SA (VO VŠEOB.) O GRUPY

(4) $[a]_{r\mathrm{mod}H} = H \cdot a \quad \forall a \in G$

$[a]_{\ell\mathrm{mod}H} = a \cdot H \quad \forall a \in G$

(5) $|H| = |[a]_{r\mathrm{mod}H}| = |[a]_{\ell\mathrm{mod}H}|$

DOKAZ: (1) UŽ JE TO DOKÁZANÉ VYŠŠIE PRE $\ell\mathrm{mod}H$, PRE $r\mathrm{mod}H$ JE TO PODOBNÉ (SYMETRICKÉ)

(2) $\Rightarrow$) $(a,b) \in r\mathrm{mod}H \Rightarrow a \cdot b^{-1} \in H \Rightarrow$
$(a \cdot b^{-1})^{-1} \in H$ T.J. $(b^{-1})^{-1} \cdot a^{-1} \in H \Rightarrow (b^{-1}, a^{-1}) \in \ell\mathrm{mod}H$
A ZO SYMETRIE $(a^{-1}, b^{-1}) \in \ell\mathrm{mod}H$

$\Leftarrow$) PODOBNE

(3) ZOBRAZENIE $(\ )^{-1} : G \to G$ JE BIJEKCIA
$((\ )^{-1})^{-1} = id : G \to G$ JE IDENTITA.
TÁTO BIJEKCIA PREVÁDZA $r\mathrm{mod}H$ NA $\ell\mathrm{mod}H$.
T.J. $[\ ]_{r\mathrm{mod}H} \to [(\ )^{-1}]_{\ell\mathrm{mod}H}$ JE BIJEKCIA.

(4) $[a]_{r\mathrm{mod}H} = \{g \in G \mid \underbrace{(a,g)}_{a \cdot g^{-1} \in H \Leftrightarrow \exists h \in H : h = a \cdot g^{-1}} \in r\mathrm{mod}H\}$

$\Leftrightarrow \exists h : g = h^{-1} \cdot a \Leftrightarrow g \in H \cdot a$

$[a]_{\ell\mathrm{mod}H} = a \cdot H$

(5) $b : H \to [a]_{r\mathrm{mod}H} = H \cdot a \quad h \mapsto h \cdot a$.
ZREJME b JE BIJEKCIA
$\Rightarrow |H| = |[a]_{r\mathrm{mod}H}|$

03.12.2007 Mo
PETER ČERNO

MA1062 ALGEBRA I

DEFINÍCIA: Buď $G(\cdot, ^{-1}, 1)$ grupa H je jej podgrupa. Indexom podgrupy H v grupe G budeme rozumieť číslo $[G:H] := |G/_r \mathrm{mod}\, H| = |G/_l \mathrm{mod}\, H|$

Rádom grupy G rozumieme počet prvkov grupy G.

VETA (LAGRANGEOVA): Keď je G grupa $G(\cdot, ^{-1}, 1)$ a H je jej podgrupa, potom $|G| = [G:H] \cdot |H|$.

DÔKAZ: $|G| = |\dot{\bigcup}_{A \in G/_r \mathrm{mod}\, H} A| = \sum_{A \in G/_r \mathrm{mod}\, H} |A| = \sum_{A \in G/_r \mathrm{mod}\, H} |H| = [G:H] \cdot |H|$.

DÔSLEDOK: Keď je $G(\cdot, ^{-1}, 1)$ konečná grupa a H jej podgrupa, potom $|H| \,|\, |G|$

PRÍKLAD: A_4 = všetky párne permutácie na $\{1,2,3,4\}$ zrejme $|A_4| = 12$. V A_4 nie je žiadna podgrupa rádu 6.

DEFINÍCIA: O grupe G povieme, že je cyklická, keď existuje $g \in G : \langle \{g\} \rangle = G$.

PRÍKLAD: 1) $\mathbb{Z}(+, -, 0)$, $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$

2) $n \in \mathbb{N}$ $\mathbb{Z}_n(+, -, 0)$, $\langle a \rangle = \mathbb{Z}_n$ pre $\gcd(a, n) = 1$.

POZNÁMKA: Buď $G(\cdot, ^{-1}, 1)$ grupa a $\varphi : \mathbb{Z} \to G$, $g \in G$ také, že $\varphi(z) = g^z$. Potom φ je homomorfizmus grup $\mathbb{Z}(+, -, 0)$ a $G(\cdot, ^{-1}, 1)$.

$\varphi(\mathbb{Z}) = \{g^z / z \in \mathbb{Z}\} = \langle g \rangle$.

DÔKAZ: Stačí dokázať, že $\varphi(k+l) = \varphi(k) \cdot \varphi(l)$. (Vychádzal z definície umocňovania g^n)

DÔSLEDOK: KEĎ JE $G(\cdot, ^{-1}, 1)$ GRUPA, $g \in G$, $m, n \in \mathbb{Z}$, POTOM $\underbrace{(g^{-1})^n = (g^n)^{-1} = g^{-n}}$ A $(g^n)^m = g^{nm}$.

DÔKAZ: φ JE ZLÚČITEĽNÉ S OPERÁCIOU $^{-1}$.
TJ $- \longleftrightarrow {}^{-1}$.

10.12.2007 M.
PETER ČERNO

MAI062 ALGEBRA I

ZNAČENIE: $\mathbb{Z}(+,-,0)$, $\mathbb{Z}_n(+,-,0)$

V $\mathbb{Z}$ JE $\langle k\rangle = k.\mathbb{Z}$

V $\mathbb{Z}_n$ JE $\langle k\rangle = k.\mathbb{Z}_n$

POZNÁMKA: (1) NECH $A \subseteq \mathbb{Z}$. POTOM A JE PODGRUPOU GRUPY $\mathbb{Z}(+,-,0) \Leftrightarrow$ $\exists k \in \mathbb{Z}, k \geq 0 : A = \langle k\rangle = k.\mathbb{Z}$.

(2) TO ISTÉ PLATÍ AJ PRE $\mathbb{Z}_n$ S TÝM ROZDIELOM, ŽE $\exists k \in \mathbb{Z}_n : k=0 \vee k \mid n$.

DOKAZ: $\Leftarrow$) PRE (1) A (2) SÚ ZREJMÉ.

$\Rightarrow$) (1) PRE $A = \{0\}$, POTOM ZREJME $A = 0.\mathbb{Z}$.

KEĎ $A \neq \{0\}$. A NUTNE OBSAHUJE NENULOVÝ PRVOK, A VZHĽADOM K TOMU, ŽE A JE UZAVRETÁ NA OPERÁCIU $-$ $\Rightarrow$ OBSAHUJE KLADNÉ CELÉ ČÍSLO. NECH k OZNAČUJE NAJMENŠIE KLADNÉ CELÉ ČÍSLO V MNOŽINE A.

ZREJME $\langle k\rangle = k.\mathbb{Z} \subseteq A$.

ZOSTÁVA UKÁZAŤ, ŽE $A \subseteq k.\mathbb{Z}$. NECH $a \in A$.

ZREJME $\exists x,y \in \mathbb{Z} : a = x.k + y \quad 0 \leq y < k$.

$\Rightarrow \quad y = a - x.k \in A$. NUTNE $y=0$. $\Rightarrow a \in k\mathbb{Z}$.

(2) PODOBNE AKO VYŠŠIE

PRE $A \neq \{0\}$ JE $a = x.k + y \Rightarrow y = a - x.k \in A$

NUTNE $y=0$, T.J. $a = x.k$

OZNAČME $c = \gcd(k,n) = k.\alpha + n.\beta$, T.J.

$c \equiv k.\alpha \bmod n \Rightarrow c \in A \Rightarrow c = k \quad (k \mid c \wedge c \mid k)$

VETA: NECH $G(\cdot, ^{-1}, 1)$ JE CYKLICKÁ GRUPA.

(1) KEĎ JE G NEKONEČNÁ, POTOM

$$G(\cdot, ^{-1}, 1) \cong \mathbb{Z}(+, -, 0)$$

(2) $|G| = n \Rightarrow G(\cdot, ^{-1}, 1) \cong \mathbb{Z}_n(+, -, 0)$

DÔKAZ: [PRE KOMUTATÍVNU GRUPU JE KAŽDÁ PODGRUPA NORMÁLNA]. NECH

ρ JE KONGRUENCIA NA $\mathbb{Z}(+, -, 0)$

A JEJ PRÍSLUŠNÁ PODGRUPA $[0]_\rho = n\mathbb{Z}$.

UVAŽUJME $f: \mathbb{Z} \to \mathbb{Z}_n : f(k) := \underbrace{1+1+\ldots+1}_{k}$

$f(k) = (k) \bmod n$.

f JE HOMOMORFIZMUS GRUP, KTORÉ JE NA $\mathbb{Z}_n$.

PODĽA PRVEJ VETY O HOMOMORFIZME PLATÍ

$$\mathbb{Z}|_{\ker f} \cong f(\mathbb{Z}) = \mathbb{Z}_n.$$

ZREJME $[0]_{\ker f} = \{k \in \mathbb{Z} : f(k) = f(0)\} = n\mathbb{Z}$

VŠETKY MOŽNÉ KONGRUENCIE $\neq id$ NA $\mathbb{Z}$ POSTAČUJÚ AKO $\ker f$

ZÁVER: $\mathbb{Z}|_\rho \cong \begin{cases} \mathbb{Z} & \text{PRE } \rho = id \\ \mathbb{Z}_n & \text{PRE } \rho \text{ TAKÚ, ŽE } [0]_\rho = n\mathbb{Z}. \end{cases}$

NECH $\varphi: \mathbb{Z} \to G$. G JE CYKLICKÁ

$\Rightarrow \exists g \in G : G = \langle g \rangle$, $\varphi(z) := g^z$.

10.12.2007 Mo
PETER ČERNO

MA1062 ALGEBRA I

PLATÍ $\varphi(\mathbb{Z}) = \langle g \rangle = G$, KDE φ JE HOMOMORFIZMUS NA G, TJ $\varphi(\mathbb{Z}) = G$

ĎALEJ $\mathbb{Z}/\ker\varphi \cong G$.

ALE PODĽA MYŠLIENKY UVEDENÉHO JE

$$\mathbb{Z}/\ker\varphi \cong \begin{cases} \mathbb{Z} \\ \mathbb{Z}_n \end{cases}$$

DÔSLEDOK: KAŽDÁ PODGRUPA I FAKTOROVÁ GRUPA CYKLICKEJ GRUPY JE OPÄŤ CYKLICKÁ.

DÔKAZ: a) PRE PODGRUPY G, NECH φ JE IZOMORFIZMUS G A $\mathbb{Z}$ (RESP. $\mathbb{Z}_n$) NECH H JE PODGRUPA GRUPY G.

$\Rightarrow$ $\varphi(H)$ JE PODGRUPA GRUPY $\mathbb{Z}$ (RESP. $\mathbb{Z}_n$), KTORÉ SÚ (AKO UŽ VIEME) CYKLICKÉ.

$H = \langle \varphi^{-1}(k) \rangle$.

b) ρ - KONGRUENCIA NA $G(\cdot, ^{-1}, 1)$,

G JE CYKLICKÁ, TJ. $G = \langle g \rangle$. POTOM:

$G/\rho = \langle [g]_\rho \rangle$, PRETOŽE $[g^k]_\rho = [g]^k_\rho$

(PRE $k > 0$ JE TO ZREJMÉ, PRE $k \leq 0$ PLATÍ TIEŽ)

DÔSLEDOK: PRE KAŽDÚ KONEČNÚ GRUPU $G(\cdot, ^{-1}, 1)$
$\forall g \in G$ PLATÍ, ŽE $g^{|G|} = 1$.

DÔKAZ: $\langle g \rangle$ JE CYKLICKÁ GRUPA, $n = |\langle g \rangle|$.
ZREJME $\langle g \rangle \cong \mathbb{Z}_n$.

$1 = g^n \leftrightsquigarrow \underbrace{1+1+\ldots+1}_{n} = 0.$

T.J. $g^n = 1$.

PODĽA LAGRANGEOVEJ VETY $n \mid |G|$.

$\Rightarrow \quad g^{|G|} = (g^n)^{|G|/n} = 1.$

VETA: NECH G JE KONEČNÁ CYKLICKÁ GRUPA.
POTOM PRE $\forall k \in \mathbb{N} : k \mid |G|$ $\exists!$ PODGRUPA RÁDU k.

DÔKAZ: STAČÍ DOKÁZAŤ PRE $\mathbb{Z}_n(+, -, 0)$, $n = |G|$.
PRE $k = 1$ JE $\{0\}$ JEDINÁ PODGRUPA GRUPY $\mathbb{Z}_n$ RÁDU 1.
PRE $k > 1$ ZVOĽME $H = \{0 \cdot \frac{n}{k}, 1 \cdot \frac{n}{k}, \ldots, (k-1) \cdot \frac{n}{k}\} = \frac{n}{k} \cdot \mathbb{Z}_n$. VIDÍME, ŽE H JE PODGRUPA GRUPY G, KTORÁ MÁ PRÁVE k PRVKOV.

JEDNOZNAČNOSŤ: K NECH JE PODGRUPA $\mathbb{Z}_n(+, -, 0)$, TAKÁ ŽE $|K| = k$. NECH $a \in \mathbb{Z}_n$: $K = \langle a \rangle$.

(STAČÍ POKÁZAŤ $a \in H$. POTOM TOTIŽ $K = \langle a \rangle \subseteq H$, $|K| = |H| = k \Rightarrow K = H$).

VIEME, ŽE $|K| = |\langle a \rangle| = k \Rightarrow \underbrace{a+a+\ldots+a}_{k} = 0$. (V $\mathbb{Z}_n$)

10.12.2007 Mo
PETER ČERNO

MAI062 ALGEBRA I

V $\mathbb{Z}$ JE $k \cdot a = x \cdot n$, PRIČOM $k \mid n$
$\Rightarrow a = x \cdot \left(\frac{n}{k}\right) \in H$, ČO BOLO TREBA DOKÁZAŤ. □

POZNÁMKA: NECH $n \in \mathbb{N}$ A $k \in \mathbb{Z}_n \setminus \{0\}$.
(1) $a = \gcd(k, n) \in \mathbb{Z}_n \setminus \{0\}$.
$\Rightarrow \langle a \rangle = \langle k \rangle$, T.J. $a\mathbb{Z}_n = k\mathbb{Z}_n$.
(2) $k \cdot \mathbb{Z}_n = \mathbb{Z}_n \Leftrightarrow \gcd(k, n) = 1$.

DÔKAZ: (1) $k = a \cdot x \Rightarrow k \in \langle a \rangle \Rightarrow \langle k \rangle \subseteq \langle a \rangle$.
PODĽA EUKLIDOVHO ALGORITMU MÁME ZARUČENÉ,
ŽE $\exists x, y \in \mathbb{Z} : a = x \cdot k + y \cdot n$, T.J. $a \equiv k \cdot x \pmod{n}$
$\Rightarrow a \in \langle k \rangle \Rightarrow \langle a \rangle \subseteq \langle k \rangle$. □
(2) $\Leftarrow$) VYPLÝVA Z (1) PRE $a = 1$.
$\Rightarrow$) $k\mathbb{Z}_n = \mathbb{Z}_n \Rightarrow 1 = (k \cdot x) \bmod n$
$\Rightarrow \exists y \in \mathbb{Z} : 1 = k \cdot x + n \cdot y \Rightarrow \gcd(k, n) = 1$. □

DEFINÍCIA: NECH $n \in \mathbb{N}$, $\varphi(n) = |\{k \in \mathbb{N}, 0 < k < n, \gcd(k, n) = 1\}|$.
$\varphi: \mathbb{N} \to \mathbb{N}$ SA TIEŽ NAZÝVA EULEROVÁ FUNKCIA.

POZNÁMKA: $n \in \mathbb{N}$, $\varphi(n)$ UDÁVA POČET VŠETKÝCH GENERÁTOROV GRUPY $\mathbb{Z}_n(+, -, 0)$ A TAKTIEŽ POČET V ⓐ INVERTIBILNÝCH PRVKOV MONOIDU $\mathbb{Z}_n(\cdot, 1)$.

VETA (MALÁ FERMATOVA): NECH $a, n \in \mathbb{N}$
$\gcd(a, n) = 1$. POTOM $(a^{\varphi(n)}) \bmod n = 1$.

DOKAZ: $a \in \mathbb{Z}_n^*(\cdot, ^{-1}, 1)$

PLATÍ $1 = (a^{|\mathbb{Z}_n^*|}) \bmod n = (a^{\varphi(n)}) \bmod n$.

12.12.2007 We
PETER ČERNO

EX: MAI062 ALGEBRA I

PRÍKLAD: NAKRESLITE HASSEOV DIAGRAM ZVÄZU PODGRÚP CYKLICKEJ GRUPY RÁDU 35.

$G \cong \mathbb{Z}_{35}$ $(+,-,0)$

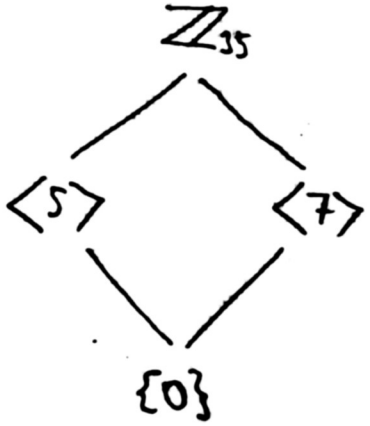
$\forall k \mid 35 \; \exists!$ PODGRUPA H GRUPY $\mathbb{Z}_{35}$ TAKÁ, ŽE $|H| = k$.

$$H = \begin{cases} \{0\} & \text{PRE } k = 1 \\ \langle \frac{35}{k} \rangle = \frac{35}{k} \cdot \mathbb{Z}_{35} \end{cases}$$

$35 = 5 \cdot 7$

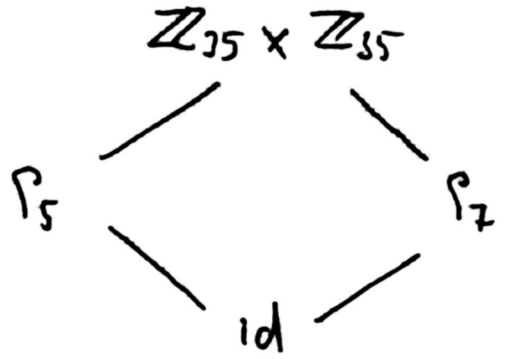
DELITELIA $35 = \{1, 5, 7, 35\}$

$\{0\}$ $\langle 7 \rangle$ $\langle 5 \rangle$ $\mathbb{Z}_{35}$



PRÍKLAD: NAKRESLITE HASSEOV DIAGRAM ZVÄZU KONGRUENCIÍ CYKLICKEJ GRUPY RÁDU 35.

CYKL. GRUPA JE KOMUTATÍVNA $\Rightarrow$ KAŽDÁ PODGRUPA JE NORMÁLNA $\Rightarrow$ DOSTÁVAME TEN ISTÝ ZVÄZ.



$(a,b) \in \rho_5 \Leftrightarrow -a+b \in \langle 5 \rangle \Leftrightarrow 5 \mid b-a$

PODOBNE ρ_7.

PRÍKLAD: NÁJDITE NAJMENŠIU KONGRUENCIU CYKLICKEJ GRUPY $\mathbb{Z}_{64}(+,-,0)$ OBSAHUJÚCU $\{(7,23),(5,61)\}$.

$\underbrace{(7,23)}_{16}$, $\underbrace{(5,61)}_{56}$

$\gcd(56,16) = 8$

56
16
8
0

$\rho \leftrightarrow \langle \{16,56\} \rangle = \langle \gcd(16,56) \rangle = \langle 8 \rangle$

PRÍKLAD: NÁJDITE NAJMENŠIU PODGRUPU GRUPY $\mathbb{Z}_{64}(+,-,0)$ OBSAHUJÚCU PRVOK

(i) 40

(ii) 50

(i) $\gcd(40,64) = 8$ $\quad \langle 40 \rangle = \langle 8 \rangle$ $\quad$ 8 PRVKOV

(ii) $\gcd(50,64) = 2$ $\quad \langle 50 \rangle = \langle 2 \rangle$ $\quad$ 32 PRVKOV

12.12.2007 We
PETER ČERNO

EX: MA1062 ALGEBRA I

V $\mathbb{Z}_n$ $\quad \rho \to [0]_\rho$.

$k|n \quad \langle k \rangle \to \rho \quad (a,b) \in \rho \Leftrightarrow k | b-a$

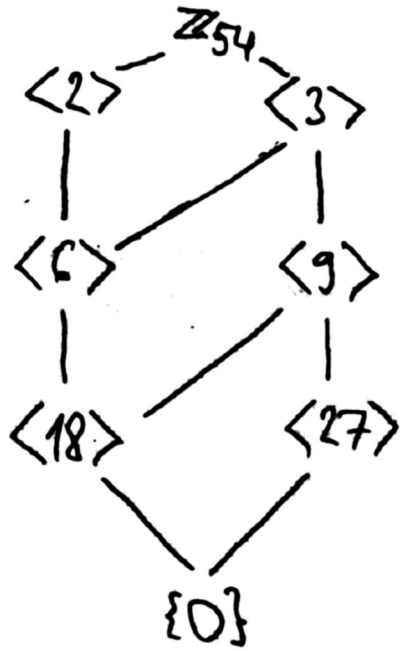
PRÍKLAD: NAKRESLITE HASSEOV DIAGRAM ZVÄZU KONGRUENCIÍ CYKLICKEJ GRUPY $\mathbb{Z}_{54}(+,-,0)$.

TENTO ZVÄZ JE IZOMORFNÝ SO ZVÄZOM VŠ. PODGRÚP

DELITEĽA $54 = 3.3.3.2$

SÚ $\{1, 2, 3, 6, 9, 18, 27, 54\}$

$\{0\}$ $\langle 27 \rangle$ $\langle 18 \rangle$ $\langle 9 \rangle$ $\langle 6 \rangle$ $\langle 3 \rangle$ $\langle 2 \rangle$ $\mathbb{Z}_{54}$



PRÍKLAD: NÁJDITE NAJMENŠIU KONGRUENCIU NA $\mathbb{Z}_{54}(+,-,0)$ OBSAHUJÚCU

a) $\{(7,11)\}$

b) $\{(5,23),\ (7,43)\}$

c) $\{(n,2n) \mid n \in \{0,2,\dots,10\}\}$

a) PRÍSLUŠNÁ PODGRUPA OBSAHUJE PRVOK $11-7=4$

$\gcd(4,54)=2$, T.J. PODGRUPA $\langle 2\rangle$.

T.J. KONGRUENCIA $\underline{\underline{\int_2}}$

b) $\langle\{23-5,\ 43-7\}\rangle = \langle\{18,36\}\rangle = \langle 18\rangle =$

$= \langle \gcd(18,54)\rangle = \underline{\underline{\langle 18\rangle}}$

KONGRUENCIA $\underline{\underline{\int_{18}}}$

c) PRE $n=1$ $\int$ OBSAHUJE $(1,2)$

$\Rightarrow \int = \mathbb{Z}_{54} \times \mathbb{Z}_{54}$

$\underline{\underline{\quad}}$

PRÍKLAD: POPÍŠTE VŠETKY IZOMORFIZMY GRUPY $\mathbb{Z}_{10}(+,-,0)$ DO SEBA (AUTOMORFIZMY)

$f_k: \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ HOMOMORFIZMUS

$\cup \qquad \cup$

$1 \longrightarrow f(1) = k$

$1+1 \longrightarrow f(1)+f(1) = 2k$

$x \longrightarrow (kx) \bmod 10$

ZREJME $\forall f_k$ $k \in \{0,\dots,9\}$ SÚ HOMOMORFIZMY.

IZOMORFIZMUS JE TO $\Leftrightarrow$ OBRAZ 1 $f(1)$ JE GENERÁTOR $\mathbb{Z}_{10}$, T.J. $\Leftrightarrow \gcd(k,10)=1$

12.12.2007 Ut
PETER ČERNO

EX: MA1062 ALGEBRA I

PRÍKLAD: KOĽKO AUTOMORFIZMOV $\mathbb{Z}_{10} \to \mathbb{Z}_{10}$ EXISTUJE ?

ODPOVEĎ: $\varphi(10) = 4$

PRÍKLAD: KOĽKO EXISTUJE AUTOMORFIZMOV CYKLICKEJ GRUPY RÁDU 53_{10}?

$\varphi(53) = 52$

PRÍKLAD: DOKÁŽTE, ŽE:

a) $\mathrm{Aut}(\mathbb{Z}_n(+,-,0)) =$

$= \{ f : \mathbb{Z}_n \to \mathbb{Z}_n$ AUTOMORFIZMUS $\}$

JE PODGRUPOU $S(\mathbb{Z}_n)(\circ, ^{-1}, \mathrm{id})$. ZREJME :)

b) $\mathrm{Aut}(\mathbb{Z}_n(+,-,0))\ (\circ, ^{-1}, \mathrm{id})$

$\cong \mathbb{Z}_n^*(\cdot, ^{-1}, 1)$

INVERTIBILNÉ PRVKY MONOIDU $\mathbb{Z}_n(\cdot, 1)$.

$\psi : \mathrm{Aut}(\mathbb{Z}_n(+,-,0)) \to \mathbb{Z}_n^*$

$f \mapsto f(1)$

ZREJME ψ JE HOMOMORFIZMUS:

$\psi(f_k \circ f_\ell) = \ldots = k \cdot \ell = \psi \ldots$

ZREJME $|\mathrm{Aut}(\ldots)| = |\mathbb{Z}_n^*| = \varphi(n)$

$k \in \mathbb{Z}_n^* \Rightarrow f_k \in \mathrm{Aut}(\ldots)$ $f_k(1) = k$, TJ. ψ JE NA.

06.01.2008 Su
PETER ČERNO

MA1062 ALGEBRA I

DEFINÍCIA: NECH $A_j\ (\alpha_i, i \in I)$ SÚ ALGEBRY ROVNAKÉHO TYPU PRE $j = 1, \dots, k$. NA $\prod_{j=1}^{k} A_j$ DEFINUJEME ŠTRUKTÚRU ALGEBRY ROVNAKÉHO TYPU.

AK JE α_i n-ÁRNA OPERÁCIA, DEFINUJEME

$$\alpha_i : \left(\prod_{j=1}^{k} A_j\right)^n \to \prod_{j=1}^{k} A_j$$

AKO: $\alpha_i\left(\overset{\in A_1}{(a_{11}, \dots, a_{1k})}, \dots, \overset{\in A_k}{(a_{n1}, \dots, a_{nk})} \right) \overset{\text{def}}{:=}$

$$:= \left(\alpha_i(a_{11}, \dots, a_{n1}), \dots, \alpha_i(a_{1k}, \dots, a_{nk})\right) .$$

PRÍKLAD: $\mathbb{Q}(+, \cdot, 1)$, $\mathbb{Z}(+, \cdot, 1)$

A PRE $\mathbb{Q} \times \mathbb{Z}$ JE $(q_1; z_1) + (q_2, z_2) \overset{\text{def}}{:=} (q_1 + q_2, z_1 + z_2)$.

POZNÁMKA: (ČÍNSKA VETA O ZVYŠKOCH): MAJME $n_1, \dots, n_k \in \mathbb{N}$ PO DVOCH NESÚDELITEĽNÉ ČÍSLA, $n = \prod_{i=1}^{k} n_i$. POTOM ZOBRAZENIE $f: \mathbb{Z}_n \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ DANÉ AKO $f(a) \overset{\text{def}}{:=} ((a) \bmod n_1, \dots, (a) \bmod n_k)$ JE IZOMORFIZMUS ALGEBIER $\mathbb{Z}_n(+, \cdot, -, 0, 1)$ A $\prod_{i=1}^{k} \mathbb{Z}_{n_i}(+, \cdot, -, (0, \dots, 0), (1, \dots, 1))$.

DÔKAZ: $f(a) + f(b) = ((a) \bmod n_1, \dots, (a) \bmod n_k) +$

$+ ((b) \bmod n_1, \dots, (b) \bmod n_k) =$

$= ((a+b) \bmod n_1, \dots, (a+b) \bmod n_k) = f(a+b)$.

$f(0) = (0, \dots, 0)$, $f(1) = (1, \dots, 1)$

NECH $f(a) = f(b)$

BÚNO NECH $a \leq b$. PLATÍ $(a) \bmod n_i = (b) \bmod n_i$

$\Rightarrow n_i \mid b-a \quad \forall i \in \{1, \dots, k\}$

$\Rightarrow \operatorname{lcm}(n_1, \dots, n_k) \mid b-a$ TJ. $n \mid b-a$

$\Rightarrow (a) \bmod n = (b) \bmod n$. f JE PROSTÉ.

$\Rightarrow f$ JE BIJEKCIA, PRETOŽE $|\mathbb{Z}_n| = |\prod_{i=1}^{k} \mathbb{Z}_{n_i}|$. □

POZNÁMKA:

(1) $n, m \in \mathbb{N}$ $\gcd(n,m)=1$, POTOM $\varphi(n \cdot m) = \varphi(n)\varphi(m)$

(2) p JE PRVOČÍSLO, $n \in \mathbb{N}$, POTOM $\varphi(p^n) = p^{n-1}(p-1)$.

DÔKAZ: UVAŽUJME $\mathbb{Z}_n(\cdot, 1)$, $\mathbb{Z}_m(\cdot, 1)$ A

„SÚČINOVÝ MONOID" $\mathbb{Z}_n \times \mathbb{Z}_m$.

$(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m$ JE INVERTIBILNÝ $\Leftrightarrow \exists (c,d)$:

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

TJ. $a \cdot c = 1$, $b \cdot d = 1$, $\Big\}$ (+)

a JE INVERTIBILNÝ V $\mathbb{Z}_n$,

b JE INVERTIBILNÝ V $\mathbb{Z}_m$.

$$\varphi(n \cdot m) = |\mathbb{Z}^*_{n \cdot m}| = |(\mathbb{Z}_n \times \mathbb{Z}_m)^*| \overset{(+)}{\simeq} |\mathbb{Z}_n^* \times \mathbb{Z}_m^*| =$$

$$= |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_m^*| = \varphi(n) \cdot \varphi(m).$$

VETA: BUĎ $p_1 < p_2 < \dots < p_k$ POSTUPNOSŤ PRVOČÍSIEL, $r_1, \dots, r_n \in \mathbb{N}$. POTOM $\varphi(\prod_{i=1}^{k} p_i^{r_i}) = \prod_{i=1}^{k} (p_i - 1) p_i^{r_i - 1}$.

DÔKAZ: $\varphi(p_1^{r_1} \cdots p_k^{r_k}) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = \prod_{i=1}^{k} (p_i - 1) p_i^{r_i - 1}$.

06.01.2008 Su
PETER CERNO

MAI062 ALGEBRA I

PRÍKLAD: (1) RSA p_1, p_2 RÔZNE PRVOČÍSLA, $n = p_1 p_2$

$\varphi(p_1 p_2) = (p_1 - 1)(p_2 - 1) =$

$\gcd(a, p_1, p_2) = 1 \Rightarrow a^{(p_1-1)(p_2-1)} \equiv 1 \pmod{p_1 p_2}$

NECH e JE ĽALEŽ NEPÁRNE ČÍSLO NESÚDELITEĽNÉ S $(p_1-1)(p_2-1)$, d JEHO INVERZNÝ PRVOK mod $(p_1-1)(p_2-1)$.

(e, n) JE PUBLIC KEY
(d, n) JE SECRET KEY. KEĎ M JE MESSAGE

$P(M) := M^e \bmod n = C$ CIPHER TEXT
$S(C) := C^d \bmod n$

ZREJME $S(P(M)) = M^{ed} \bmod n = M$
PRE $M \in \{0, \dots, n-1\}$.

(2) KOĽKO GENERÁTOROV OBSAHUJE CYKLICKÁ GRUPA RÁDU 50 $(g \in G \mid \langle g \rangle = G)$.
$G \cong \mathbb{Z}_{50}$, $\varphi(50) = (2-1).(5-1).5 = 20$

OKRUHY A IDEÁLY

DEFINÍCIA: ALGEBRU $R(+, \cdot, -, 0, 1)$ NAZVEME OKRUHOM, AK $R(+, -, 0)$ JE KOMUTATÍVNA GRUPA, $R(\cdot, 1)$ JE MONOID A PLATÍ:

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

KOMUTATÍVNY OKRUH MÁ NAVYŠE KOMUTATÍVNU OP. $\cdot$.

PRÍKLADY: 1) $\mathbb{Z}(+,\cdot,-,0,1)$, $\mathbb{Z}_n(+,\cdot,-,0,1)$ SÚ KOMUTATÍVNE OKRUHY.

2) $T(+,\cdot)$ - TELESO, $T(+,\cdot,-,0,1)$ - OKRUH.

3) $M_n(T)$ - MATICE $n \times n$ NAD TELESOM T
$M_n(T)(+,\times,-,O_n,I_n)$ - OKRUH.

POZNÁMKA: NECH $a,b \in R$. POTOM PLATÍ:

1) $0 \cdot a = a \cdot 0 = 0$
2) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$
3) $(-1)\cdot b = b\cdot(-1) = -b$
4) $(-a)\cdot(-b) = a\cdot b$
5) $0 \neq 1 \Leftrightarrow |R| > 1$

DÔKAZ: 1) $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$
$\Rightarrow 0 = 0\cdot a$

2) $0 = 0\cdot b = (a+(-a))\cdot b = a\cdot b + (-a)\cdot b$
$\Rightarrow -(a\cdot b) = (-a)\cdot b$

3) 2) $a = 1$

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

5) $\Leftarrow$ $1 = 0$
$\forall r \in R \quad r = 1\cdot r = 0\cdot r = 0 \Rightarrow R = \{0\}$

06.01.2008 Su
PETER ČERNO

MA1062 ALGEBRA I

DEFINÍCIA: MNOŽINA $I \subseteq R$ JE PRAVÝ (ĽAVÝ) IDEÁL OKRUHU $R(+,\cdot,-,0,1)$, AK I JE PODGRUPA GRUPY $R(+,-,0)$ A PRE $\forall i \in I$ A $\forall r \in R$: $i \cdot r \in I$ $(r \cdot i \in I)$.

IDEÁLOM NAZVEME I, AK JE PRAVÝM AJ ĽAVÝM IDEÁLOM.

PRÍKLADY: 1) $\{0\}$, R - IDEÁLY

2) $a \in R$, $aR = \{a \cdot r \mid r \in R\}$ JE HLAVNÝ PRAVÝ IDEÁL
$Ra = \{r \cdot a \mid r \in R\}$ HLAVNÝ ĽAVÝ IDEÁL

3) $\mathbb{Z}(+,\cdot,-,0,1)$ - V TOMTO OKRUHU SÚ VŠETKY IDEÁLY HLAVNÉ TVARU $a \cdot \mathbb{Z}$.

VETA: MNOŽINA VŠETKÝCH IDEÁLOV TVORÍ UZÁVEROVÝ SYSTÉM A ZOBRAZENIE $\rho \to [0]_\rho$ JE IZOMORFIZMUS ZVÄZU VŠETKÝCH KONGRUENCIÍ OKRUHU A IDEÁLOV NA OKRUHU. NAVYAC $(a,b) \in \rho \Leftrightarrow (b-a) \in [0]_\rho \Leftrightarrow \rho$ JE KONGRUENCIA.

DÔKAZ. NECH ρ JE KONGRUENCIA NA $R(+,\cdot,-,0,1)$. ZREJME $[0]_\rho$ JE PODGRUPA $R(+,-,0)$.

$$\left.\begin{array}{l} i \in [0]_\rho \\ r \in R \end{array}\right\} \Rightarrow \left.\begin{array}{l} (i,0) \in \rho \\ (r,r) \in \rho \end{array}\right\} \Rightarrow (i \cdot r, r \cdot 0) \in \rho$$

$$\Rightarrow i \cdot r \in [0]_\rho .$$

NECH I JE IDEÁL V $R(+,\cdot,-,0,1)$. ZREJME $b-a \in I \Leftrightarrow (a,b) \in \rho$ DEFINUJE KONGRUENCIU NA $R(+,-,0)$ (KOMUTATÍVNA GRUPA). ZOSTÁVA DOKÁZAŤ ZLUČITEĽNOSŤ S $\cdot$:

$(a,b) \in \varrho$, $(c,d) \in \varrho$, $\quad b-a,\ d-c \in I$

KEĎŽE I JE IDEÁL, TAKTIEŽ $\quad b\cdot(d-c) \in I$

$(b-a)\cdot c \in I$

$\Rightarrow b\cdot d - a\cdot c \in I \Rightarrow (a\cdot c, b\cdot d) \in \varrho$. □

POZNÁMKA : $\mathcal{I}$ = IDEÁLY

$\mathcal{C}$ = KONGRUENCIE NA $R(+,\cdot,-,0,1)$

KDE $\mathcal{C}$ JE UZÁVEROVÝ SYSTÉM OBSIAHNUTÝ V MNOŽINE VŠETKÝCH EKVIVALENCIÍ NA R, $\mathcal{I} \subseteq \mathcal{P}(R)$ A $0 \in R$ TAK, ŽE PLATÍ :

$\forall \varrho, \eta \in \mathcal{C}$:

(1) $[0]_\varrho \in \mathcal{I}$

(2) $\forall N \in \mathcal{I}\ \exists\, \xi \in \mathcal{C} : N = [0]_\xi$

(3) $[0]_\varrho \subseteq [0]_\eta \Rightarrow \varrho \subseteq \eta$.

07.01.2008 M6
PETER ČERNO

MAI062 ALGEBRA I

$R(+,\cdot,-,0,1)$ - OKRUH

ZNAČENIE: I - IDEÁL $\longleftrightarrow$ ϱ_I - KONGRUENCIA

$(a,b) \in \varrho_I \Leftrightarrow a-b \in I$

NAMIESTO $R|_{\varrho_I}$ BUDEME PÍSAŤ $R|_I$.

DEFINÍCIA: INVERTIBILNÝM PRVKOM OKRUHU $R(+,\cdot,-,0,1)$ BUDEME ROZUMIEŤ INVERTIBILNÝ PRVOK MONOIDU $R(\cdot,1)$.

OKRUH NAZVEME TELESOM, KEĎ JE KAŽDÝ JEHO NENULOVÝ PRVOK INVERTIBILNÝ. (POZOR! • NEMUSÍ BYŤ KOMUT.)

TJ. $R^* = R \setminus \{0\}$.

IDEÁL I JE MAXIMÁLNY, KEĎ I JE KOATOM V ZVÄZE IDEÁLOV.

PRÍKLAD: KEĎ JE p PRVOČÍSLO, POTOM NAPR. $p.\mathbb{Z}$ JE MAXIMÁLNY IDEÁL V OKRUHU $\mathbb{Z}(+,\cdot,-,0,1)$.

VETA: NASLEDUJÚCE JE PRE OKRUH EKVIVALENTNÉ:

(1) $R(+,\cdot,-,0,1)$ JE TELESO

(2) $\{0\}$, R SÚ JEDINÉ PRAVÉ IDEÁLY

(3) ——"—— ĽAVÉ IDEÁLY.

DÔKAZ: (1) $\Rightarrow$ (2): BUĎ I PRAVÝ IDEÁL RÔZNY OD $\{0\}$.

$\Rightarrow \exists i \in I: i \neq 0$. V R EXISTUJE i^{-1}.

$1 = i \cdot i^{-1}$
$\in I \quad \in R$ Z DEFINÍCIE PRAVÉHO IDEÁLU

$\forall r \in R \quad r = 1 \cdot r \in I \Rightarrow I = R.$
$\in I \quad \in R$

(2)⇒(1): NECH $a \neq 0 \in R$. DOKÁŽEME, ŽE $\exists a^{-1} \in R$.

$a \cdot R$ JE PRAVÝ IDEÁL. ZREJME $0 \neq a = a \cdot 1 \in a \cdot R$.
TO ALE ZNAMENÁ, ŽE (PODĽA PREDPOKLADU) $a \cdot R = R$,
PRETOŽE $a \cdot R \neq \{0\}$.
$\Rightarrow \exists b \in R : \underline{a \cdot b = 1}$.
TAKISTO $b \neq 0$ (PREDPOKLADÁME, ŽE $0 \neq 1$)

ROVNAKÝM ARGUMENTOM DOSTANEME, ŽE $b \cdot R = R$
$\Rightarrow \exists c \in R : \underline{b \cdot c = 1}$.

$\Rightarrow$ (UŽ SME RAZ DOKÁZALI), $\underline{a = c}$, TAKŽE $b = a^{-1}$.

VETA: KEĎ JE $R(+, \cdot, -, 0, 1)$ KOMUTATÍVNY OKRUH,
I NECH JE IDEÁL (PRAVÝ = ĽAVÝ NA KOMUT. OKRUHU)
$R|_I(+, \cdot, -, 0, 1)$ JE TELESO (KOMUTATÍVNE)
$\Leftrightarrow$ I JE MAXIMÁLNY IDEÁL.

DOKAZ: VIEME, ŽE J-IDEÁL $\longleftrightarrow$ ς_J - KONGRUENCIA
J JE KOAXIÓN $\Leftrightarrow$ ς_J JE KOAXIÓN

STAČÍ DOKÁZAŤ, ŽE $R|_I$ JE TELESOM $\Leftrightarrow$
ς_I JE KOAXIÓN A ZVÄČŠE KONGRUENCIÍ
NA $R(+, \cdot, -, 0, 1)$. (TJ. $\underline{\exists \text{KON. } \varrho}$: $\varsigma_I \subset \varrho \subset R \times R$)

~~EX/ NECH/ R/I/ JE/ TELESO/~~
NA $R|_I(+, \cdot, -, 0, 1)$ MÁME IBA
KONGRUENCIE id_A A $R/I \times R/I$.

07.01.2008/6
PETER ČERNO

MA1062 ALGEBRA I

PODĽA PREDCHÁDZAJÚCEHO TVRDENIA
$R|_I(+,\cdot,-,0,1)$ JE TELESO
↓
KOMUTATÍVNE NÁSOBENIE, T.J.
PRAVÉ = ĽAVÉ IDEÁLY

$\Leftrightarrow$ $\{[0]_{\sim_I}\}$ A $R|_I$ SÚ JEDINÉ IDEÁLY.

$\not\Leftrightarrow$ NA $R|_I$ MÁME PRÁVE KONGRUENCIE
$id,\ R|_I \times R|_I$

ZNAČENIE: $a \in R,\ n \in \mathbb{Z}$.

$0 \times a = 0 \in R$

$n \times a = (n-1) \times a + a. \quad \forall n > 0$

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

POZNÁMKA: DEFINUJME ZOBRAZENIE $\varphi : \mathbb{Z} \to R$ PREDPISOM $\varphi(n) = n \times 1$. POTOM φ JE OKRUHOVÝ HOMOMORFIZMUS $\mathbb{Z}(+,\cdot,-,0,1)$ A $R(+,\cdot,-,0,1)$. $\varphi(\mathbb{Z})$ JE NAJMENŠÍ PODOKRUH R OBSAHUJÚCI 1 A EXISTUJE JEDNOZNAČNE URČENÉ ČÍSLO $p \in \mathbb{N}_0$ TAKÉ, ŽE $\{n \in \mathbb{Z} \mid \varphi(n) = 0\} = p.\mathbb{Z}$.

DEFINÍCIA: CHARAKTERISTIKOU OKRUHU $R(+,\cdot,-,0,1)$ ROZUMIEME p Z PREDCH. POZNÁMKY.
ZODPOVEDÁ TO CHARAKTERISTIKE TELESA.

DÔKAZ: UŽ MÁME DOKÁZANÉ (PODĽA VIET UVEDENÝCH VYŠŠIE), ŽE φ JE HOMOMORFIZMUS GRÚP $\mathbb{Z}(+,-,0)$, $R(+,-,0)$ A $\varphi(\mathbb{Z})$ JE NAJMENŠIA PODGRUPA OBSAHUJÚCA 1.

$\varphi(1) = 1$ PODĽA DEFINÍCIE

ĎALEJ $\varphi(a)\cdot\varphi(b) = (a\times 1)\cdot(b\times 1) = $ Z DISTRIBUTÍVIT
$= a\times(b\times 1) = (a\cdot b)\times 1 = \varphi(a\cdot b)$.

$\varphi(\mathbb{Z})$ JE PODOKRUH $\Rightarrow$ $\varphi(\mathbb{Z})$ JE NAJMENŠÍ PODOKRUH.

$I = \{n\in\mathbb{Z} \mid \varphi(n)=0\}$ OBSAHUJE 0. $\varphi(0)=0$ $0\in I$

ĎALEJ $\varphi(-n) = -\varphi(n) = 0$ $-n\in I$

$\varphi(n+m) = \varphi(n)+\varphi(m) = 0+0=0$ $n+m\in I$

$\Rightarrow$ I JE PODGRUPA $\mathbb{Z}(+,-,0)$

$\Rightarrow \exists p : p\cdot\mathbb{Z} = I$ (PODĽA VIET UVEDENÝCH VYŠŠIE).

POZNÁMKA: NECH $R(+,\cdot,-,0,1)$ JE KOMUTATÍVNY OKRUH, $a,b\in R$, $n\in\mathbb{N}$.

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

(BINOMICKÁ VETA)

DÔKAZ: ROVNAKO AKO V $\mathbb{R}$ (INDUKCIOU)

DÔSLEDOK: BUĎ $R(+,\cdot,-,0,1)$ KOM. OKRUH PRVOČ./SEL. CHARAKTERISTIKY p. POTOM ZOBR. $R\to R$ $a\mapsto a^p$ JE OKRUHOVÝ HOMOMORFIZMUS. (FROBENIOV)

DÔKAZ: $(a+b)^p = a^p+\dots+b^p = a^p+b^p$ ... ATĎ.

07.01.2008 Po
PETER ČERNO

MAI062 ALGEBRA I

DALEJ VIEME, ŽE $a \mapsto a^p$ JE MONOMORFIZMUS
$R(+,\cdot,-,0) \to R(+,\cdot,-,0)$.

$1^p = 1$, $(a \cdot b)^p = a^p \cdot b^p$.

VETA: NECH $R(+,\cdot,-,0,1)$ JE KOMUTATÍVNE TELESO A G JE KONEČNÁ PODGRUPA GRUPY $R \setminus \{0\}(\cdot, ^{-1}, 1)$. POTOM G JE CYKLICKÁ.

DÔKAZ: VID ALGEBRA II

DEFINÍCIA: POVIEME, ŽE $R(+,\cdot,-,0,1)$ JE OBOR INTEGRITY, KEĎ JE TO KOMUTATÍVNY OKRUH A PRE $\forall a,b \in R$ PLATÍ

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0.$$

PRÍKLAD: OBORY INTEGRITY: 1) $\mathbb{Z}(+,\cdot,-,0,1)$,
2) $\mathbb{R}[x](+,\cdot,-,0,1)$ REÁLNE POLYNÓMY

KONŠTRUKCIA: $R(+,\cdot,-,0,1)$ JE OBOR INTEGRITY

$F = R \times (R \setminus \{0\})$, $(a,b), (c,d) \in F$

$(a,b) + (c,d) = (a \cdot d + b \cdot c, b \cdot d)$

$-(a,b) = (-a, b)$

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

$\underline{0} = (0,1)$

$\underline{1} = (1,1)$

DEFINUJEME RELÁCIU $\sim$

$$(a,b) \sim (c,d) \Leftrightarrow a \cdot d = b \cdot c .$$

POZNÁMKA:

(1) $F(+, \underline{0})$, $F(\cdot, \underline{1})$ SÚ KOMUTATÍVNE MONOIDY.

(2) $\sim$ JE KONGRUENCIA NA ALGEBRE $F(+, \cdot, -, \underline{0}, \underline{1})$

(3) $(0,1) \sim (0,a) \quad \forall a \neq 0$

$(1,1) \sim (a,a)$

(4) $F|_\sim \left(+, \cdot, -, [\underline{0}]_\sim, [\underline{1}]_\sim\right)$ JE KOMUTATÍVNE TELESO

(5) $R \to F|_\sim \quad r \mapsto [(r,1)]_\sim$

JE PROSTÝ OKRUHOVÝ HOMOMORFIZMUS

DEFINÍCIA: $F|_\sim (+, \cdot, -, [\underline{0}]_\sim, [\underline{1}]_\sim)$ NAZÝVAME PODIELOVÉ TELESO.

BEŽNE PÍŠEME $[(a,b)]_\sim = \frac{a}{b}$.

09.01.2008 16
PETER ČERNO

EX: MAIOG2 ALGEBRA I

PRÍKLAD: NECH $T(+,\cdot,-,0,1)$ JE TELESO. (NEKOMUTATÍVNE)
POPÍŠTE VŠETKY KONGRUENCIE.

NA TELESE T SÚ PRÁVE DVA ĽAVÉ A PRÁVE DVA PRAVÉ IDEÁLY : $\{0\}, R$ = IDEÁLY
$\Rightarrow$ 2 KONGRUENCIE.

$\{0\} \rightsquigarrow id$
$R \rightsquigarrow T \times T$

PRÍKLAD: NECH T JE TELESO $n \in \mathbb{N}$
$M_n(T)$ SÚ ŠTVORCOVÉ MATICE $T^{n \times n}$.
$M_n(T)\,(+,\cdot,-,O_n,I_n)$ JE ZREJME OKRUH
POPÍŠTE KONGRUENCIE TOHTO OKRUHU
IDEÁLY $M_n(T)$

NECH I JE IDEÁL $\neq \{O_n\}$
STAČÍ DOKÁZAŤ, ŽE $I_n \in I$
NECH $A \neq O_n$ $a_{ij} \neq 0$

$$a_{ij}^{-1} E_{ii} A E_{jj} = \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix} \begin{matrix} \\ i \\ \\ \end{matrix} = E_{ij} \in I$$
$$\qquad\qquad\qquad\qquad\qquad\quad j$$

$E_{kj} = E_{ki} \cdot E_{ij}$
$E_{kk} = E_{kj} \cdot E_{jk} = E_{ki} \cdot E_{ij} \cdot E_{jk} \in I$
$\Rightarrow I_n \in I$ □

$\Rightarrow$ MÁME PRÁVE DVA HOMOMORFIZMY. JADRO HOMOMORFIZMU JE KONGRUENCIA

PRÍKLAD: $\mathbb{Z}_p$ JE TELESO (p JE PRVOČÍSLO)

$\mathbb{Z}_p[x]$ OKRUH POLYNÓMOV NAD $\mathbb{Z}_p$ (KOMUTATÍVNY

PRE $q \in \mathbb{Z}_p[x]$

KEDY JE $q\mathbb{Z}_p[x]$ MAXIMÁLNY IDEÁL

$q\mathbb{Z}_p[x]$ JE MAXIMÁLNY IDEÁL $\Leftrightarrow$

$\mathbb{Z}_p[x] \Big|_{q\mathbb{Z}_p[x]}$ JE TELESO

$\Leftrightarrow$ q JE IREDUCIBILNÝ