UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

Přírodovědecká fakulta
Katedra matematiky

# Základy matematiky KMA/ZAM
# Teoretické základy informatiky I KI/TZI1

## Přednáška 09
## Binární operace

jiri.cihlar@ujep.cz

# O čem budeme hovořit:

- Definice a příklady binárních operací
- Vlastnosti binárních operací
- Definice a příklady grup

# Definice a příklady binárních operací

# Příklad binární operace - sčítání

**Při sčítání přirozených čísel je ke dvojici libovolně zvolených čísel (tzv. sčítanců) jednoznačně přiřazen výsledek (tzv. součet).**

Například:

$2 + 3 = 5$ ..... $[2 ; 3] \rightarrow 5$

$4 + 2 = 6$ ..... $[4 ; 2] \rightarrow 6$

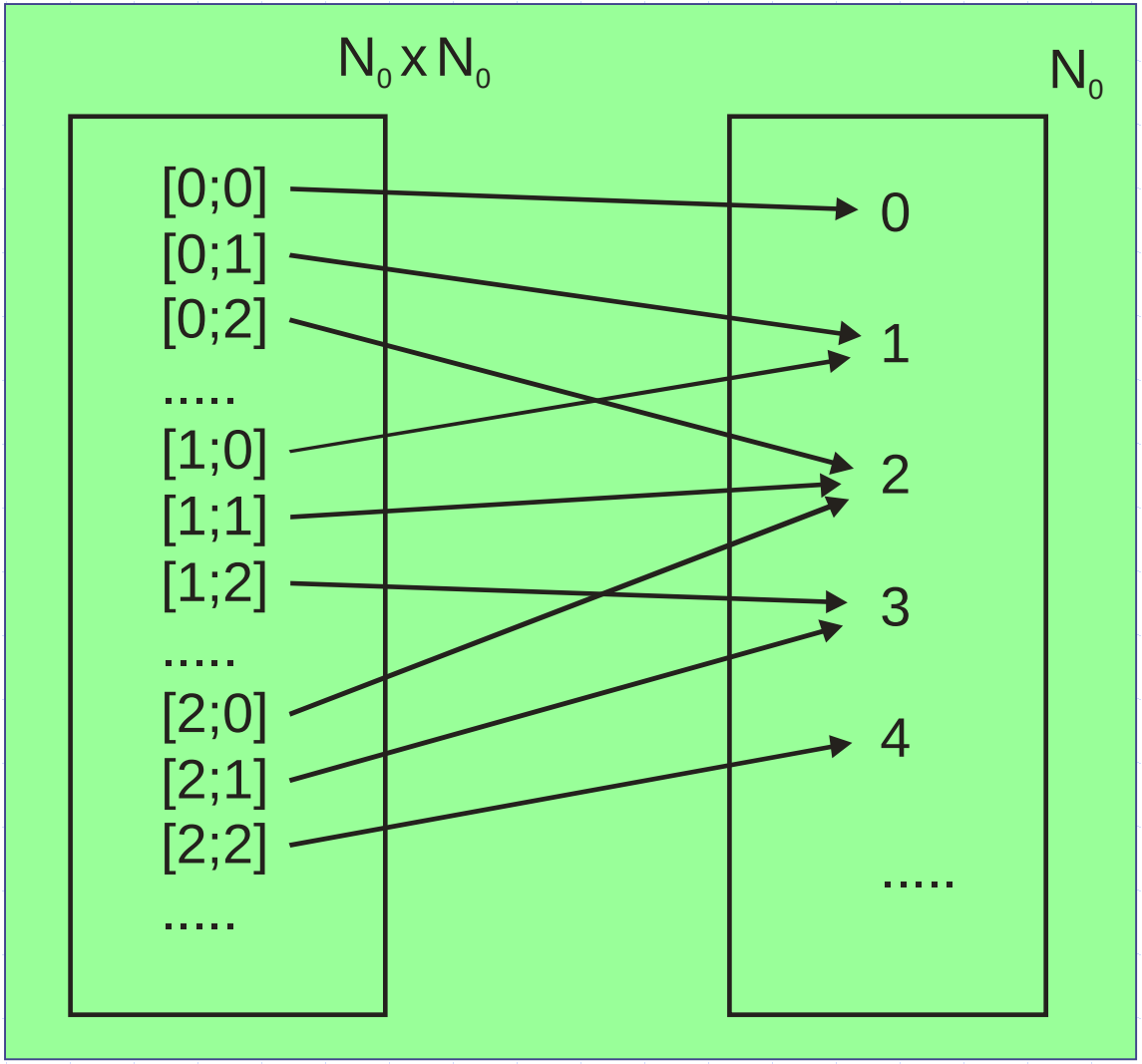
$9 + 0 = 9$ ..... $[9 ; 0] \rightarrow 9$

$12 + 9 = 21$ ..... $[12 ; 9] \rightarrow 21$

atd.

# Příklad binární operace - sčítání

Operaci sčítání přirozených čísel tedy můžeme chápat jako určité zobrazení kartézského součinu $N_0 \times N_0$ na množinu $N_0$ .



# Definice binární operace

**Binární operací v množině M nazýváme zobrazení z kartézského součinu $M \times M$ do množiny M .**

Další příklady operací s přirozenými čísly:

- Binární operace násobení přirozených čísel je zobrazení množiny $N_0 \times N_0$ na množinu $N_0$ .
- Binární operace odčítání přirozených čísel je zobrazení z množiny $N_0 \times N_0$ na množinu $N_0$ .
- Binární operace dělení přirozených čísel je zobrazení z množiny $N_0 \times N_0$ na množinu $N_0$ .

# Další příklady binárních operací

- konjunkce (disjunkce, implikace, ekvivalence) dvou výroků
- průnik (sjednocení, rozdíl) dvou množin
- střed dvojice bodů
- největší společný dělitel dvou přirozených čísel
- nejmenší společný násobek dvou přirozených čísel
- umocňování přirozených čísel
- skládání translací (posunutí) v rovině

atd.

# Sčítání a násobení zbytkových tříd

Pro modul $m = 3$ máme tři třídy rozkladu množiny Z:

$$T_0 = \{\cdots, -6, -3, 0, 3, 6, 9, 12, \cdots\}$$
$$T_1 = \{\cdots, -5, -2, 1, 4, 7, 10, 13, \cdots\}$$
$$T_2 = \{\cdots, -4, -1, 2, 5, 8, 11, 14, \cdots\}$$

Tyto třídy se sčítají tak, že z obou tříd se vybere libovolné číslo, ta dvě čísla se sečtou, a součtem obou tříd je ta třída, do které patří vypočítaný součet čísel.

$T_1 + T_2 = T_0$ , protože například $4 + 8 = 12$ ,
$T_2 + T_0 = T_2$ , protože například $5 + 3 = 8$ ,
$T_0 + T_1 = T_1$ , protože například $-3 + 7 = 4$ ,
atd.

Obdobně se dvě zbytkové třídy násobí.

# Sčítání a násobení zbytkových tříd

Výsledky sčítání a násobení zbytkových tříd pro modul $m = 3$ jsou v těchto tabulkách:

| $+$ | $T_0$ | $T_1$ | $T_2$ |
|---|---|---|---|
| $T_0$ | $T_0$ | $T_1$ | $T_2$ |
| $T_1$ | $T_1$ | $T_2$ | $T_0$ |
| $T_2$ | $T_2$ | $T_0$ | $T_1$ |

| $\cdot$ | $T_0$ | $T_1$ | $T_2$ |
|---|---|---|---|
| $T_0$ | $T_0$ | $T_0$ | $T_0$ |
| $T_1$ | $T_0$ | $T_1$ | $T_2$ |
| $T_2$ | $T_0$ | $T_2$ | $T_1$ |

# Skládání permutací

- Existuje 6 permutací množiny $\{1, 2, 3\}$ :

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$k = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$l = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$m = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$n = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$o = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Tabulka ukazuje výsledky jejich skládání:

| $\bullet$ | $e$ | $k$ | $l$ | $m$ | $n$ | $o$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $k$ | $l$ | $m$ | $n$ | $o$ |
| $k$ | $k$ | $l$ | $e$ | $o$ | $m$ | $n$ |
| $l$ | $l$ | $e$ | $k$ | $n$ | $o$ | $m$ |
| $m$ | $m$ | $n$ | $o$ | $e$ | $k$ | $l$ |
| $n$ | $n$ | $o$ | $m$ | $l$ | $e$ | $k$ |
| $o$ | $o$ | $m$ | $n$ | $k$ | $l$ | $e$ |

# Vlastnosti binárních operací

# Motivační příklad

U binárních operací je důležité, zda je operace zobrazením **(celé) množiny M × M do množiny M** , nebo pouze **z množiny M × M do množiny M** .

V prvním případě je výsledek operace definován pro libovolnou dvojici [x ; y] ∈ M × M a je prvkem množiny M, v druhém případě není některým dvojicím [x ; y] ∈M × M přiřazen obraz z množiny M.

**Příklad:**
Učí-li se děti sčítat například jen v množině M = {1;2;3;4;5}, je operace sčítání v M tzv. **neúplná**.

| + | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | |
| 2 | 3 | 4 | 5 | | |
| 3 | 4 | 5 | | | |
| 4 | 5 | | | | |
| 5 | | | | | |

# Definice úplnosti binární operace

**Binární operaci □ v množině M nazýváme úplnou právě tehdy, když platí**

$$(\forall x,y \in M)(\exists z \in M)\ x \square y = z\ .$$

Příklady:

- operace **sčítání** je úplná v $\mathbf{N_0}$ ,
- operace **odčítání** není úplná v $\mathbf{N_0}$,
- operace **odčítání** je úplná v **Z**,
- operace **dělení** není úplná v **Z**,

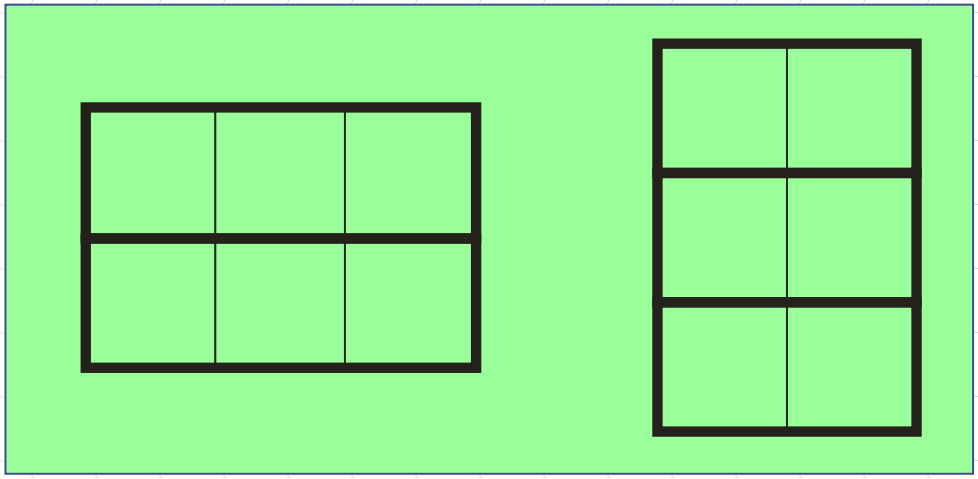
atd.

# Motivační příklad

Při nácviku násobení přirozených čísel se děti učí, že výsledek nezávisí na pořadí činitelů, například:

$$2 \cdot 3 = 3 \cdot 2$$

Tento fakt můžeme odůvodnit na „modelu násobení“:



V těchto situacích užíváme tzv. **komutativitu násobení**:

$$x \cdot y = y \cdot x$$

# Definice komutativnosti binární operace

**Binární operaci □ v množině M nazýváme komutativní právě tehdy, když platí**

$$(\forall x,y \in M)\ \ x \square y = y \square x\ .$$

Příklady:

- operace **sčítání** je komutativní v $\mathbf{N_0}$ ,
- operace **odčítání** není komutativní v $\mathbf{N_0}$,
- operace **střed dvojice bodů** je komutativní,
- operace **průnik množin** je komutativní,
- operace **skládání permutací** není komutativní,

atd.

# Motivační příklad

Při nácviku sčítání přirozených čísel „přes desítku“ naučíme děti rozkládat čísla na dva sčítance, a pak postupujeme například takto:

$$8 + 7 = 8 + ( 2 + 5 ) = ( 8 + 2 ) + 5 = 10 + 5 = 15$$

Užíváme přitom tzv. **asociativitu sčítání**:

$$x + ( y + z ) = ( x + y ) + z$$

# Definice asociativnosti binární operace

**Binární operaci $\square$ v množině M nazýváme asociativní právě tehdy, když platí**

$$(\forall x,y,z \in M)\ (x \square y) \square z = x \square (y \square z).$$

Příklady:

- operace **sčítání** je asociativní v $\mathbf{N_0}$,
- operace **odčítání** není asociativní v $\mathbf{N_0}$,
- operace **umocňování** není asociativní v $\mathbf{N_0}$,
- operace **sjednocování množin** je asociativní,
- operace **skládání permutací** je asociativní,

atd.

# Motivační příklad

U některých binárních operací v množině M existuje jistý význačný prvek v množině M s touto vlastností:

**„je-li tento prvek jedním z operandů, pak vůbec neovlivňuje výsledek operace, tj. výsledek je vždy roven druhému operandu“.**

**Příklad**:

U sčítání přirozených čísel je takovým prvkem nula, protože $5 + 0 = 5$ , $12 + 0 = 12$ , $0 + 4 = 4$ , atd.

Budeme říkat, že číslo 0 je **neutrálním prvkem** operace sčítání přirozených čísel.

# Definice neutrálního prvku binární operace

**U binární operace $\square$ v množině M budeme nazývat prvek n neutrálním prvkem právě tehdy, když platí**

$$(\forall x \in M)\ \ x \square n = x \ \ \wedge \ \ n \square x = x\ .$$

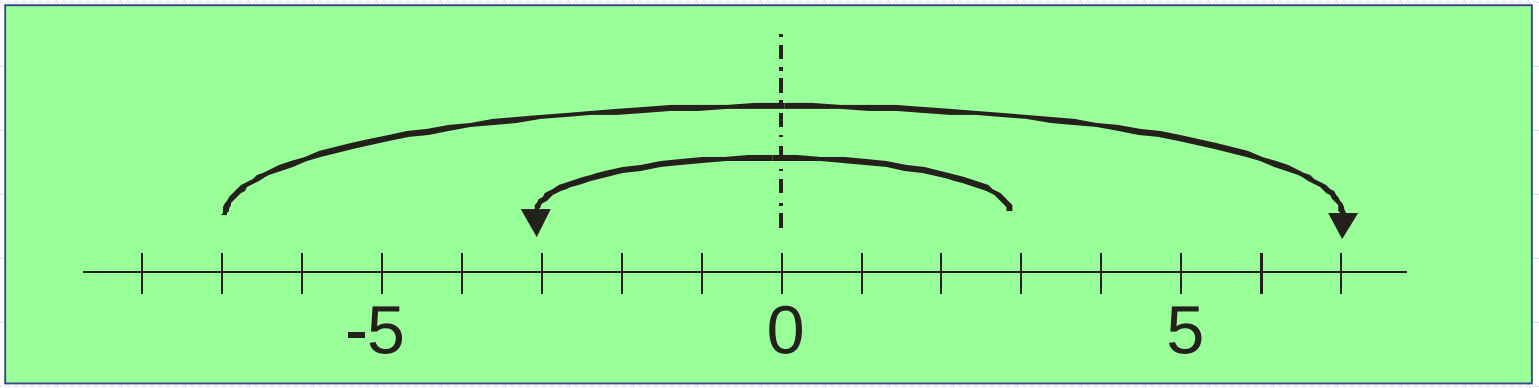
Příklady:

- u operace **sčítání** v $\mathbf{N_0}$ je neutrálním prvkem 0,
- operace **odčítání** v **Z** nemá neutrální prvek,
- u operace **sjednocení** je neutrálním prvkem $\varnothing$,
- u operace **násobení zbytkových tříd při modulu 3** je neutrálním prvkem třída $T_1$,
- u operace **translace** je neutrálním prvkem translace určená nulovým vektorem, atd.

# Motivační příklad

U některých binárních operací v množině M, které mají neutrální prvek, můžeme často **k prvku x ∈ M** nalézt (obecně) jiný, tzv. **inverzní prvek x´∈ M .**
**Výsledkem operace s těmito prvky je neutrální prvek.**

**Příklad**: U sčítání celých čísel je neutrální prvek 0 a tedy
k číslu 3 je inverzním prvkem (-3), protože 3 + (-3) = 0 ,
k číslu (-7) je inverzním prvkem 7, protože (-7) + 7 = 0 ,
k číslu 0 je inverzním prvkem 0, protože 0 + 0 = 0 , atd.



# Definice inverzních prvků binární operace

**U binární operace □ v množině M s neutrálním prvkem n budeme nazývat prvek x′ inverzním prvkem k prvku x právě tehdy, když platí**

$$x \square x' = n \quad \wedge \quad x' \square x = n.$$

Příklady:

- u operace **sčítání v Z** je k číslu 3 inverzním prvkem číslo (–3) ,
- u operace **násobení v Q** je k číslu 3 inverzním prvkem číslo 1/3 ,
- u operace **sčítání modulo 3** je k třídě $T_2$ inverzním prvkem třída $T_1$ ,

atd.

# Motivační příklad

V aritmetice čísel je často používáno dobře známé pravidlo o „roznásobování závorky“.

**Příklad**:

Máme-li zpaměti vypočítat součin 3 .12 , postupujeme asi v myšlenkách takto:

$$\mathbf{3 \,.\, 12 = 3 \,.\, (10 + 2) = 3 \,.\, 10 + 3 \,.\, 2 = 30 + 6 = 36}$$

Zde používáme tzv. **distributivitu násobení vůči sčítání**, tedy platnost vztahu

$$\mathbf{x \,.\, (y + z) = x \,.\, y + x \,.\, z}$$

# Definice distributivnosti binárních operací

**Nechť jsou dány dvě binární operace □ a # v množině M. Budeme říkat, že operace # je distributivní vzhledem k operaci □ právě tehdy, když platí**

$$(\forall x,y,z \in M)\ (x \square y) \# z = (x \# z) \square (y \# z) \wedge$$
$$\wedge\ z \# (x \square y) = (z \# x) \square (z \# y)\ .$$

Příklady:

- násobení je distributivní vzhledem ke sčítání,
- sčítání není distributivní vzhledem k násobení,
- sjednocení je distributivní vzhledem k průniku,
- průnik je distributivní vzhledem ke sjednocení,

atd.

# Grupa

# Definice grupy

**Strukturu [ M; □ ], kde □ je operace na množině M, budeme nazývat grupou právě tehdy, když současně platí tyto čtyři podmínky:**

$(\forall x,y \in M)(\exists! z \in M)\ \ x \square y = z$

$(\forall x,y,z \in M)\ \ (x \square y) \square z = x \square (y \square z)$

$(\exists z \in M)(\forall x \in M)\ \ x \square n = x \ \wedge\ n \square x = x$

$(\forall x \in M)(\exists x' \in M)\ x \square x' = n \ \wedge\ x' \square x = n$

**Slovně řečeno:**
**v grupě je operace uzavřená, je asociativní, má neutrální prvek, a ke každému prvku existuje prvek inverzní.**

# Definice komutativní grupy

**Grupu [ M; □ ], kde □ je operace na množině M, budeme nazývat komutativní grupou právě tehdy, když navíc platí tato pátá podmínka:**

$$(\forall x,y \in M)\ \ x \square y = y \square x\ .$$

**Slovně řečeno:**
**v komutativní grupě je operace uzavřená, je asociativní i komutativní, má neutrální prvek, a ke každému prvku existuje prvek inverzní.**

# Příklady z číselných oborů

- $[\mathbf{N_0}\ ;\ +\ ]$ není grupa, protože ke kladným celým číslům neexistují v $N_0$ inverzní prvky
- $[\ \mathbf{Z}\ ;\ +\ ]$ je komutativní grupa
- $[\ \mathbf{Z}\ ;\ \cdot\ ]$ není grupa, protože jen čísla 1 a (-1) mají v Z inverzní prvky
- $[\ \mathbf{Q}\ ;\ +\ ]$ je komutativní grupa
- $[\ \mathbf{Q}\ ;\ \cdot\ ]$ není grupa, protože číslo 0 nemá v Q inverzní prvek
- $[\ \mathbf{Q} - \{\mathbf{0}\}\ ;\ \cdot\ ]$ je komutativní grupa

# Další příklady

- Operace umocňování na přirozených číslech netvoří grupu, protože není asociativní.
- Operace nejmenší společný násobek na množině N netvoří grupu, protože tato operace nemá neutrální prvek.
- **[ Pot(A) ; ∪ ]** , kde A je neprázdná množina, není grupa, protože neprázdné podmnožiny množiny A nemají inverzní prvky.
- Množina všech translací v rovině spolu s operací skládání tvoří komutativní grupu.

# Další příklady

- Operace střed dvojice bodů na množině všech bodů roviny netvoří grupu, protože tato operace není asociativní.
- Tříprvková množina zbytkových tříd modulo 3 tvoří spolu se sčítáním komutativní grupu, zatímco spolu s násobením netvoří grupu, protože třída $T_0$ nemá inverzní prvek.
- Množina šesti možných permutací tříprvkové množiny se označuje $S_3$, a spolu s operací skládání permutací tvoří nekomutativní grupu (říká se jí symetrická grupa).

# Poznámka o krácení v grupě

Uvažujme grupu **[ M; □ ]** s neutrálním prvkem **n .** Rovnost je vzhledem k operaci □ invariantní, tedy platí:

$$(\forall x,y,z \in N_0)\ \ x = y \rightarrow x \square z = y \square z \ \wedge$$
$$\wedge \ \ x = y \rightarrow z \square x = z \square y .$$

Lze dokázat i obrácená tvrzení, tedy že platí (tzv. krácení):

$$(\forall x,y,z \in N_0)\ \ x \square z = y \square z \rightarrow x = y \ \wedge$$
$$\wedge \ \ z \square x = z \square y \rightarrow x = y .$$

Důkaz: Z předpokladu $x \square z = y \square z$

pomocí invariance $(x \square z) \square z' = (y \square z) \square z'$

a pomocí asociativity $x \square ( z \square z' ) = y \square ( z \square z' )$

získáme $x \square n = y \square n$

a tedy $x = y$

**Závěr: V grupě lze krátit (zprava i zleva).**

# Poznámka k neutrálnímu prvku

Uvažujme grupu **[ M; □ ]** a budeme předpokládat, že v množině existují **M** dva různé neutrální prvky $\mathbf{n_1}$ a $\mathbf{n_2}$ operace □ .

Platí tedy, že:

$$(\forall x \in M)\ \ x \square n_1 = x \ \wedge\ n_1 \square x = x\,, \qquad (1)$$

a současně

$$(\forall x \in M)\ \ x \square n_2 = x \ \wedge\ n_2 \square x = x\,. \qquad (2)$$

Z druhé části (1) plyne, že $n_1 \square n_2 = n_2$ ,
a z první části (2) plyne, že $n_1 \square n_2 = n_1$ .
Z těchto rovností vyplývá, že $n_1 = n_2$ ,
oba neutrální prvky tedy splynou.

**Závěr: Grupa má právě jeden neutrální prvek.**

# Poznámka k inverzním prvkům

Uvažujme grupu **[ M; □ ]** s neutrálním prvkem **n** a budeme předpokládat, že k nějakému prvku **x∈M** existují v **M** dva inverzní prvky $x_1'$ **a** $x_2'$ .

Operace □ je tedy asociativní a platí současně:

$$x \square x_1' = n \wedge x_1' \square x = n$$
$$x \square x_2' = n \wedge x_2' \square x = n$$

Pak: $x_1' = x_1' \square n = x_1' \square (x \square x_2') =$

$$= (x_1' \square x) \square x_2' = n \square x_2' = x_2' ,$$

a oba inverzní prvky tedy splynou.

**Závěr: V grupě existuje ke každému prvku právě jeden inverzní prvek.**

# Co je třeba znát a umět?

- **Znát definici binární operace,**
- **znát příklady binární operací z různých částí matematiky, speciálně operace se zbytkovými třídami a operaci skládání permutací,**
- **znát a umět poznat vlastnosti binárních operací (úplnost, komutativita, asociativita, existence neutrálního prvku a inverzních prvků),**
- **znát pojem (komutativní) grupy a příklady grup.**

# Děkuji za pozornost