Izomorfismy grup

Def (Izomorfismus grup): Bijektivní homomorfismus $f: G_1 \to G_2$ grupy $(G_1, *)$ do $(G_2, \circ)$ nazýváme izomorfismem grupy $(G_1, *)$ a $(G_2, \circ)$.

Příklad: Uvažujme grupu $(\mathbb{Z}_3, +)$ a množinu $Im(\mathbb{Z}_3) = \{\circ, \triangle, \square\}$.

Zobrazení $f: \mathbb{Z}_3 \to Im(\mathbb{Z}_3)$ definujme předpisem:

$$\left.\begin{array}{l} 0 \to \circ \\ 1 \to \triangle \\ 2 \to \square \end{array}\right\} \Rightarrow f \text{ je bijekce (tj. injektivní i surjektivní)}$$

$(\mathbb{Z}_3, +)$:

b

+	0	1	2
0	0	1	2
a= 1	1	2	0 =a+b
2	2	0	1

V tabulce sčítání na $\mathbb{Z}_3$ „nahraďme":

$$\left.\begin{array}{l} 0 \to \circ \\ 1 \to \triangle \\ 2 \to \square \end{array}\right\} \text{bijekce!}$$

a definujme tak operaci $*$ na $Im(\mathbb{Z}_3) = \{\circ, \triangle, \square\}$

f(b)

$*$	$\circ$	$\triangle$	$\square$
$\circ$	$\circ$	$\triangle$	$\square$
f(a)= $\triangle$	$\triangle$	$\square$	$\circ$
$\square$	$\square$	$\circ$	$\triangle$

$\Rightarrow$ Nevytvořili jsme nic nového – jen změnili označení prvků v $\mathbb{Z}_3$

$f(\overset{a+b}{0}) = \circ$, ale také

$\circ = \triangle * \square = f(a) * f(b)$

$$\forall a, b \in \mathbb{Z}_3: \quad f(a+b) = f(a) * f(b) \qquad \Leftrightarrow f \text{ je izomorfismus.}$$

Poznámka: Jestliže existuje izomorfismus grup $(G_1, *)$ a $(G_2, \circ)$, znamená to, že mají úplně stejnou strukturu, tzn. můžeme je chápat jako úplně stejné grupy – lišící se pouze označením prvků a operace. Říkáme, že $(G_1, *)$ a $(G_2, \circ)$ jsou izomorfní a značíme

$$(G_1, *) \approx (G_2, \circ)$$

Pokud je jasné, jaké operace na G_1 a G_2 máme na mysli, značíme pouze $G_1 \approx G_2$.

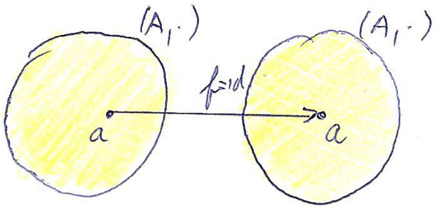
Věta: Relace „býti izomorfní" je relace ekvivalence na množině grup.
Tzn. Nechť $(A,\cdot)$, $(B,*)$, $(C,\circ)$ jsou grupy. Potom platí:

1.) $A \approx A$

2.) $A \approx B \Rightarrow B \approx A$

3.) $(A \approx B \wedge B \approx C) \Rightarrow A \approx C$

Důkaz: 1.) $\boxed{A \approx A}$



Izomorfismem $f: A \to A$ je identita:

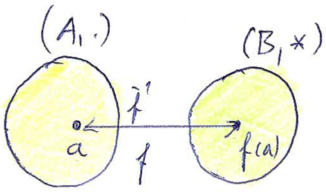
$$f(a) = a$$

1.) Je to homomorfismus: $f(a \cdot b) = a \cdot b = f(a) \cdot f(b)$

2.) f je injektivní: $f(a) = f(b) \Rightarrow a = b$

3.) f je surjektivní: $\forall a \in A \ \exists a \in A: f(a) = a$

2.) $\boxed{A \approx B \Rightarrow B \approx A}$



$A \approx B \Rightarrow \exists f: A \to B$ izomorfismus

Dokážeme, že $f^{-1}: B \to A$ je také izomorfismus

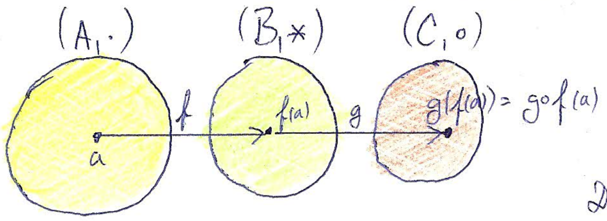
1.) f^{-1} je homomorfismus:

f je surjektivní $\Rightarrow \forall a', b' \in B \ \exists a, b \in A: f(a) = a' \wedge f(b) = b'$

$\Rightarrow f^{-1}(a' * b') = f^{-1}(f(a) * f(b)) = f^{-1}(f(a \cdot b)) = a \cdot b = f^{-1}(a') \cdot f^{-1}(b')$

2.) f^{-1} je bijekce: Zobrazení inverzní k bijekci f je zase bijekce.

3.) $\boxed{(A \approx B \wedge B \approx C) \Rightarrow A \approx C}$



$A \approx B \Rightarrow \exists f: A \to B$ izomorfismus

$B \approx C \Rightarrow \exists g: B \to C$ izomorfismus

Dříve bylo dokázáno, že složení dvou izomorfismů je izomorfismus. Tj.

$g \circ f: A \to C$ je izomorfismus $\Rightarrow A \approx C$

$\square$

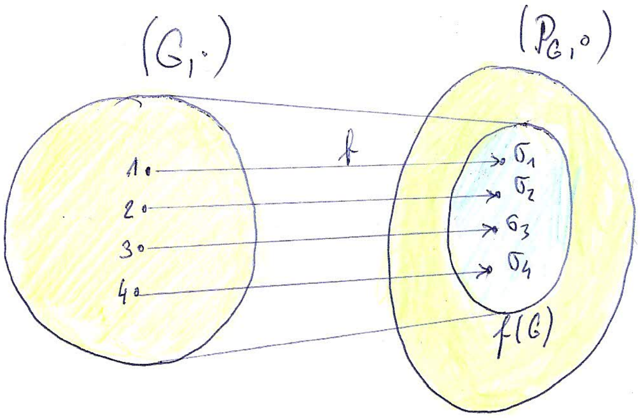
Př: Uvažujme grupu $(G,\cdot)$, kde $G = \mathbb{Z}_5 - \{0\}$ a $\cdot$ je násobení modulo 5. označme P_G množinu permutací prvků z G. $(P_G,\circ)$, kde $\circ$ je skládání zobrazení tvoří grupu.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Prvku 2 přiřadíme permutaci $\sigma_2 : \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 3 \end{pmatrix}$ tj. $\sigma_2(g) = 2g$

Prvku 3 přiřadíme permutaci $\sigma_3 : \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 4 & 2 \end{pmatrix}$ tj. $\sigma_3(g) = 3g$

$$\sigma_3 \circ \sigma_2 : \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{pmatrix} = id = \sigma_1 \left(= \overset{!!!?}{\sigma_{3\cdot 2}}\right)$$



$$(\sigma_3 \circ \sigma_2)(g) = \sigma_3(\sigma_2(g)) = \sigma_3(2g) = 3\cdot 2g = 1g$$

$\Rightarrow \quad \sigma_a \circ \sigma_b = \sigma_{a\cdot b}$

$\Rightarrow \quad f(a) = \sigma_a$ je zobrazení $f : G \to P_G$

$$\left.\begin{aligned} f(a) &= \sigma_a \\ f(b) &= \sigma_b \end{aligned}\right\} \quad f(a) \circ f(b) = \sigma_a \circ \sigma_b = \sigma_{ab} = f(ab)$$

$\Rightarrow$ $\boxed{f \text{ je homomorfismus z } G \to P_G}$

$\Rightarrow$ $\boxed{(f(G),\circ) \text{ je podgrupa grupy permutací prvků z } G.}$

$\underline{f(a) = f(b)} \iff \sigma_a = \sigma_b \iff \forall g \in G : \sigma_a(g) = \sigma_b(g) \iff \forall g \in G : a\cdot g = b \cdot g \Rightarrow \underline{a = b}$

$\Rightarrow f$ je injektivní zobrazení $\Rightarrow f : G \to f(G)$ je bijekce $\Rightarrow$ $\boxed{(G,\cdot) \text{ je izomorfní s } (f(G),\circ)}$

Věta: Nechť $(G,\cdot)$ je grupa, $a \in G$. Definujme zobrazení $\lambda_a : G \to G$ předpisem:

$$\forall x \in G: \quad \lambda_a(x) = ax$$

Potom $\lambda_a(x)$ je bijektivní. Tzn. λ_a je permutace prvků G, tj. $\lambda_a \in \mathrm{Perm}\,G$.

Důkaz: I.) λ_a je injektivní:

$$\forall x,y \in G: \quad \lambda_a(x) = \lambda_a(y) \Rightarrow$$
$$\Rightarrow \quad ax = ay \quad \Rightarrow$$
$$\Rightarrow \quad x = y$$

II.) λ_a je surjektivní:

$$\forall y \in G \;\; \exists a^{-1}y \in G: \quad \lambda_a(a^{-1}y) = aa^{-1}y = y$$

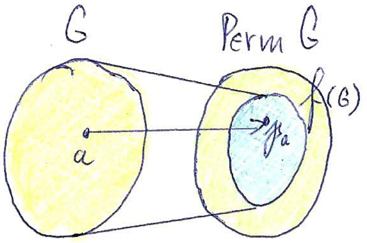
$\square$

Věta: Nechť $(G,\cdot)$ je grupa a zobrazení $\lambda_a : G \to G$ je dáno předpisem $\forall x \in G: \lambda_a(x) = ax$.
Potom zobrazení $f: G \to \mathrm{Perm}\,G$ dané předpisem

$$f(a) = \lambda_a$$

je injektivní homomorfismus grupy $(G,\cdot)$ do grupy $(\mathrm{Perm}\,G, \circ)$.

Důkaz:



I.) f je homomorfismus:

$$\forall a,b \in G: \quad f(a\cdot b) = \lambda_{ab} \qquad \forall x \in G: \lambda_{ab}(x) = ab\,x$$

$$f(a) \circ f(b) = \lambda_a \circ \lambda_b \qquad \forall x \in G: \lambda_a \circ \lambda_b(x) = \lambda_a(\lambda_b(x)) =$$
$$= \lambda_a(bx) = abx$$

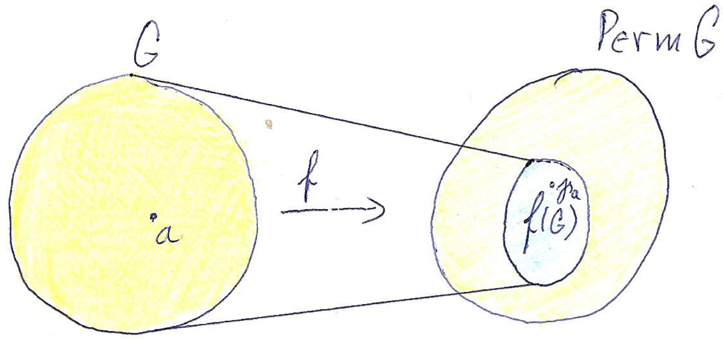
$$\Rightarrow \quad \lambda_{ab} = \lambda_a \circ \lambda_b \quad \Rightarrow \quad f(a\cdot b) = f(a) \circ f(b)$$

II.) f je injektivní:

$$f(a) = f(b) \Rightarrow \lambda_a = \lambda_b \Rightarrow \forall x \in G: ax = bx \Rightarrow (\text{zvolme } x = e) \; a = b$$

$\square$

Důsledek: (Cayleyho věta): Každá grupa je izomorfní s nějakou podgrupou grupy permutací svých prvků.



$f(a) = \rho_a \in \text{Perm } G$

$f: G \to \text{Perm } G$ je injektivní homomorfismus $\Rightarrow$

$\Rightarrow f: G \to f(G)$ je bijektivní homomorfismus = izomorfismus

navíc $(f(G), \circ)$ je podgrupa grupy $(\text{Perm } G, \circ)$