Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$.

Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Rozklad grupy G podle podgrupy H je rozklad na množině G, tedy systém neprázdných podmnožin množiny G, které jsou po dvou disjunktní a jejichž sjednocení je G.

Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Rozklad grupy G podle podgrupy H je rozklad na množině G, tedy systém neprázdných podmnožin množiny G, které jsou po dvou disjunktní a jejichž sjednocení je G. Znamená to, že každý prvek $a \in G$ leží v právě jedné levé třídě (totiž třídě $a \cdot G$).

Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Rozklad grupy G podle podgrupy H je rozklad na množině G, tedy systém neprázdných podmnožin množiny G, které jsou po dvou disjunktní a jejichž sjednocení je G. Znamená to, že každý prvek $a \in G$ leží v právě jedné levé třídě (totiž třídě $a \cdot G$).

Inspirace. Zvolme pevně libovolné $m \in \mathbb{N}$ a označme $H = [0]_m = \{mk;\ k \in \mathbb{Z}\}$. Pak H je podgrupa grupy $(\mathbb{Z}, +)$ a odpovídajícím rozkladem je $\mathbb{Z}/H = \mathbb{Z}_m$.

Rozklad grupy podle podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Rozklad grupy G podle podgrupy H je rozklad na množině G, tedy systém neprázdných podmnožin množiny G, které jsou po dvou disjunktní a jejichž sjednocení je G. Znamená to, že každý prvek $a \in G$ leží v právě jedné levé třídě (totiž třídě $a \cdot G$).

Inspirace. Zvolme pevně libovolné $m \in \mathbb{N}$ a označme $H = [0]_m = \{mk;\ k \in \mathbb{Z}\}$. Pak H je podgrupa grupy $(\mathbb{Z}, +)$ a odpovídajícím rozkladem je $\mathbb{Z}/H = \mathbb{Z}_m$. Na $\mathbb{Z}_m$ jsme definovali operaci $+$ pomocí reprezentantů: pro libovolné $a \in \mathbb{Z}$ je totiž $a + H = [a]_m$ a použitou definici sčítání zbytkových tříd $[a]_m + [b]_m = [a + b]_m$ pro libovolná $a, b \in \mathbb{Z}$ lze psát ve tvaru $(a + H) + (b + H) = (a + b) + H$.

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů.

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$.

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$,

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = (1,3,2) \circ H = \{(2,3), (1,3,2)\}$.

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = (1,3,2) \circ H = \{(2,3), (1,3,2)\}$. Protože $\mathrm{id} \circ H = (1,2) \circ H$, musí být $\big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = \big((1,2) \circ H\big) \circ \big((1,3) \circ H\big)$.

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = (1,3,2) \circ H = \{(2,3), (1,3,2)\}$. Protože $\mathrm{id} \circ H = (1,2) \circ H$, musí být
$\big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = \big((1,2) \circ H\big) \circ \big((1,3) \circ H\big)$.
Ale předchozí definice pomocí reprezentantů by dala
$\big((1,2) \circ H\big) \circ \big((1,3) \circ H\big) = (1,3,2) \circ H$,
$\big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = (1,3) \circ H \neq (1,3,2) \circ H$,

Naivní pokus o zavedení operace na rozkladu G/H

Nechť $(G, \cdot)$ je grupa a H její podgrupa. Na rozkladu G/H bychom rádi zavedli operaci $\cdot$ pomocí reprezentantů. Pro libovolné levé třídy $a \cdot H$, $b \cdot H$ zvolíme jejich reprezentanty, například $a \in a \cdot H$, $b \in b \cdot H$, a pro součin těchto reprezentantů v grupě $(G, \cdot)$, tj. $a \cdot b$, najdeme třídu, která jej obsahuje, tj. $(a \cdot b) \cdot H$. O této třídě chceme prohlásit, že je výsledkem nové operace pro třídy $a \in a \cdot H$, $b \in b \cdot H$. Rádi bychom tedy definovali novou operaci $\cdot$ na G/H předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$.

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = (1,3,2) \circ H = \{(2,3), (1,3,2)\}$. Protože $\mathrm{id} \circ H = (1,2) \circ H$, musí být
$\big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = \big((1,2) \circ H\big) \circ \big((1,3) \circ H\big)$.
Ale předchozí definice pomocí reprezentantů by dala
$\big((1,2) \circ H\big) \circ \big((1,3) \circ H\big) = (1,3,2) \circ H$,
$\big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = (1,3) \circ H \neq (1,3,2) \circ H$,
a tedy v tomto případě definici pomocí reprezentantů nelze použít.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$,

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupa** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupa** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupa** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy.
V libovolné komutativní grupě G je každá podgrupa normální.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupa** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy.
V libovolné komutativní grupě G je každá podgrupa normální.
Podgrupa $H = \{\mathrm{id}, (1,2)\}$ není normální podgrupou grupy $\mathbb{S}_3$.

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupa** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy.
V libovolné komutativní grupě G je každá podgrupa normální.
Podgrupa $H = \{\mathrm{id}, (1,2)\}$ není normální podgrupou grupy $\mathbb{S}_3$.

Věta. *Je-li $f : G \to K$ homomorfismus grup, pak jeho jádro* $\ker f$ *je normální podgrupa grupy G.*

Kdy by definice pomocí reprezentantů mohla být použita?

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli na G/H zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupa** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy.
V libovolné komutativní grupě G je každá podgrupa normální.
Podgrupa $H = \{\mathrm{id}, (1,2)\}$ není normální podgrupou grupy $\mathbb{S}_3$.

Věta. *Je-li $f : G \to K$ homomorfismus grup, pak jeho jádro $\ker f$ je normální podgrupa grupy G.*

Důkaz. Víme, že $\ker f$ je podgrupa. Je-li $h \in \ker f$, tj. $f(h) = 1$, pak pro každé $a \in G$ je $f(a \cdot h \cdot a^{-1}) = f(a) \cdot f(h) \cdot f(a)^{-1} = 1$, proto $a \cdot h \cdot a^{-1} \in \ker f$.

Normální podgrupy - shrnutí

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Normální podgrupy - shrnutí

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Definujme zobrazení $\pi : G \to G/H$ předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří).

Normální podgrupy - shrnutí

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Definujme zobrazení $\pi : G \to G/H$ předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří). Zřejmě je π surjektivní.

Normální podgrupy - shrnutí

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Definujme zobrazení $\pi : G \to G/H$ předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří). Zřejmě je π surjektivní. Požadavek zavést novou operaci předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ lze pak psát ve tvaru $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$.

Normální podgrupy - shrnutí

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Definujme zobrazení $\pi : G \to G/H$ předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří). Zřejmě je π surjektivní. Požadavek zavést novou operaci předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ lze pak psát ve tvaru $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$.

Ukážeme si, že v případě, kdy H je normální podgrupa grupy G, pak tímto předpisem operace na rozkladu G/H skutečně vznikne.

Normální podgrupy - shrnutí

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat součin levých tříd $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Definujme zobrazení $\pi : G \to G/H$ předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří). Zřejmě je π surjektivní. Požadavek zavést novou operaci předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ lze pak psát ve tvaru $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$.

Ukážeme si, že v případě, kdy H je normální podgrupa grupy G, pak tímto předpisem operace na rozkladu G/H skutečně vznikne. Dále ukážeme, že G/H s touto operací tvoří grupu a že π je homomorfismus grup, jehož jádro $\ker \pi = H$.

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa.*

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$.*

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Důkaz. Musíme ověřit korektnost definice.

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Důkaz. Musíme ověřit korektnost definice. Pro libovolné $a, b, c, d \in G$ musíme ukázat

$$a \cdot H = c \cdot H,\ b \cdot H = d \cdot H \implies (a \cdot b) \cdot H = (c \cdot d) \cdot H.$$

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Důkaz. Musíme ověřit korektnost definice. Pro libovolné $a, b, c, d \in G$ musíme ukázat

$$a \cdot H = c \cdot H,\ b \cdot H = d \cdot H \implies (a \cdot b) \cdot H = (c \cdot d) \cdot H.$$

Ekvivalentně

$$c^{-1} \cdot a,\ d^{-1} \cdot b \in H \implies (c \cdot d)^{-1} \cdot (a \cdot b) \in H.$$

Ovšem

$$(c \cdot d)^{-1} \cdot (a \cdot b) = d^{-1} \cdot (c^{-1} \cdot a) \cdot b = d^{-1} \cdot (c^{-1} \cdot a) \cdot d \cdot (d^{-1} \cdot b).$$

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Důkaz. Musíme ověřit korektnost definice. Pro libovolné $a, b, c, d \in G$ musíme ukázat

$$a \cdot H = c \cdot H,\ b \cdot H = d \cdot H \implies (a \cdot b) \cdot H = (c \cdot d) \cdot H.$$

Ekvivalentně

$$c^{-1} \cdot a,\ d^{-1} \cdot b \in H \implies (c \cdot d)^{-1} \cdot (a \cdot b) \in H.$$

Ovšem
$(c \cdot d)^{-1} \cdot (a \cdot b) = d^{-1} \cdot (c^{-1} \cdot a) \cdot b = d^{-1} \cdot (c^{-1} \cdot a) \cdot d \cdot (d^{-1} \cdot b)$.
Protože podgrupa H je normální, platí $d^{-1} \cdot (c^{-1} \cdot a) \cdot d \in H$, odkud plyne korektnost definice operace $\cdot$ na G/H.

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Důkaz. Musíme ověřit korektnost definice. Pro libovolné $a, b, c, d \in G$ musíme ukázat

$$a \cdot H = c \cdot H,\ b \cdot H = d \cdot H \implies (a \cdot b) \cdot H = (c \cdot d) \cdot H.$$

Ekvivalentně

$$c^{-1} \cdot a,\ d^{-1} \cdot b \in H \implies (c \cdot d)^{-1} \cdot (a \cdot b) \in H.$$

Ovšem
$(c \cdot d)^{-1} \cdot (a \cdot b) = d^{-1} \cdot (c^{-1} \cdot a) \cdot b = d^{-1} \cdot (c^{-1} \cdot a) \cdot d \cdot (d^{-1} \cdot b)$.
Protože podgrupa H je normální, platí $d^{-1} \cdot (c^{-1} \cdot a) \cdot d \in H$,
odkud plyne korektnost definice operace $\cdot$ na G/H.
Snadno se ověří, že tato operace je asociativní, má neutrální prvek $1 \cdot H$ a že pro libovolné $a \in G$ je inverzní prvek k prvku $a \cdot H$ prvek $a^{-1} \cdot H$.

Rozklad grupy podle normální podgrupy

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Důkaz. Musíme ověřit korektnost definice. Pro libovolné $a, b, c, d \in G$ musíme ukázat

$$a \cdot H = c \cdot H,\ b \cdot H = d \cdot H \implies (a \cdot b) \cdot H = (c \cdot d) \cdot H.$$

Ekvivalentně

$$c^{-1} \cdot a,\ d^{-1} \cdot b \in H \implies (c \cdot d)^{-1} \cdot (a \cdot b) \in H.$$

Ovšem
$(c \cdot d)^{-1} \cdot (a \cdot b) = d^{-1} \cdot (c^{-1} \cdot a) \cdot b = d^{-1} \cdot (c^{-1} \cdot a) \cdot d \cdot (d^{-1} \cdot b)$.
Protože podgrupa H je normální, platí $d^{-1} \cdot (c^{-1} \cdot a) \cdot d \in H$,
odkud plyne korektnost definice operace $\cdot$ na G/H.
Snadno se ověří, že tato operace je asociativní, má neutrální prvek $1 \cdot H$ a že pro libovolné $a \in G$ je inverzní prvek k prvku $a \cdot H$ prvek $a^{-1} \cdot H$. Proto $(G/H, \cdot)$ je grupa.

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří)*

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$. [Věta 9.5, str. 46]

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$. [Věta 9.5, str. 46]

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$. [Věta 9.5, str. 46]

Důkaz. Definice operace $\cdot$ na G/H dává $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$, a tedy π je homomorfismus grup.

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro $\ker \pi = H$.* [Věta 9.5, str. 46]

Důkaz. Definice operace $\cdot$ na G/H dává $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$, a tedy π je homomorfismus grup. Libovolný prvek $a \in G$ splňuje $a \in \ker \pi$, právě když $\pi(a) = 1 \cdot H$, tj. $a \cdot H = 1 \cdot H$, neboli $a \in H$.

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro $\ker \pi = H$.* [Věta 9.5, str. 46]

Důkaz. Definice operace $\cdot$ na G/H dává $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$, a tedy π je homomorfismus grup. Libovolný prvek $a \in G$ splňuje $a \in \ker \pi$, právě když $\pi(a) = 1 \cdot H$, tj. $a \cdot H = 1 \cdot H$, neboli $a \in H$.

Definice. Toto π se nazývá **projekce grupy G na faktorgrupu G/H**.

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro $\ker \pi = H$.* [Věta 9.5, str. 46]

Důkaz. Definice operace $\cdot$ na G/H dává $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$, a tedy π je homomorfismus grup. Libovolný prvek $a \in G$ splňuje $a \in \ker \pi$, právě když $\pi(a) = 1 \cdot H$, tj. $a \cdot H = 1 \cdot H$, neboli $a \in H$.

Definice. Toto π se nazývá **projekce grupy G na faktorgrupu G/H**.

Důsledek. *Normální podgrupy grupy G jsou právě jádra homomorfismů $G \to K$ grupy G do vhodných grup K.*

Faktorgrupa

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa $(G/H, \cdot)$ z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro $\ker \pi = H$.* [Věta 9.5, str. 46]

Důkaz. Definice operace $\cdot$ na G/H dává $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$, a tedy π je homomorfismus grup. Libovolný prvek $a \in G$ splňuje $a \in \ker \pi$, právě když $\pi(a) = 1 \cdot H$, tj. $a \cdot H = 1 \cdot H$, neboli $a \in H$.

Definice. Toto π se nazývá **projekce grupy G na faktorgrupu G/H**.

Důsledek. *Normální podgrupy grupy G jsou právě jádra homomorfismů $G \to K$ grupy G do vhodných grup K.*

Věta. *Nechť $(G, \cdot)$ je komutativní grupa, pak je každá podgrupa H grupy G normální a faktorgrupa G/H je komutativní.* [Věta 9.8, str. 47]

Rozklad grupy podle jádra homomorfismu

Věta. *Nechť* $f : G \to K$ *je homomorfismus grup,* $\ker f$ *jeho jádro. Pak pro libovolné* $a, b \in G$ *platí* $f(a) = f(b)$, *právě když* $a^{-1} \cdot b \in \ker f$, *tj. právě když* $a \cdot (\ker f) = b \cdot (\ker f)$.

Rozklad grupy podle jádra homomorfismu

Věta. *Nechť* $f : G \to K$ *je homomorfismus grup,* $\ker f$ *jeho jádro. Pak pro libovolné* $a, b \in G$ *platí* $f(a) = f(b)$, *právě když* $a^{-1} \cdot b \in \ker f$, *tj. právě když* $a \cdot (\ker f) = b \cdot (\ker f)$.

Důkaz. Víme, že pro libovolnou podgrupu H grupy G platí
$a^{-1} \cdot b \in H \quad \Leftrightarrow \quad a \cdot H = b \cdot H$,

Rozklad grupy podle jádra homomorfismu

Věta. *Nechť* $f : G \to K$ *je homomorfismus grup,* $\ker f$ *jeho jádro. Pak pro libovolné* $a, b \in G$ *platí* $f(a) = f(b)$, *právě když* $a^{-1} \cdot b \in \ker f$, *tj. právě když* $a \cdot (\ker f) = b \cdot (\ker f)$.

Důkaz. Víme, že pro libovolnou podgrupu H grupy G platí
$a^{-1} \cdot b \in H \quad \Leftrightarrow \quad a \cdot H = b \cdot H$,
proto to platí i pro $H = \ker f$.

Rozklad grupy podle jádra homomorfismu

Věta. *Nechť* $f : G \to K$ *je homomorfismus grup,* $\ker f$ *jeho jádro. Pak pro libovolné* $a, b \in G$ *platí* $f(a) = f(b)$, *právě když* $a^{-1} \cdot b \in \ker f$, *tj. právě když* $a \cdot (\ker f) = b \cdot (\ker f)$.

Důkaz. Víme, že pro libovolnou podgrupu H grupy G platí
$a^{-1} \cdot b \in H \quad \Leftrightarrow \quad a \cdot H = b \cdot H$,
proto to platí i pro $H = \ker f$.

Jestliže platí $f(a) = f(b)$, pak
$f(a^{-1} \cdot b) = f(a^{-1}) \cdot f(b) = f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(1) = 1$,
a tedy $a^{-1} \cdot b \in \ker f$.

Rozklad grupy podle jádra homomorfismu

Věta. *Nechť* $f : G \to K$ *je homomorfismus grup,* $\ker f$ *jeho jádro. Pak pro libovolné* $a, b \in G$ *platí* $f(a) = f(b)$, *právě když* $a^{-1} \cdot b \in \ker f$, *tj. právě když* $a \cdot (\ker f) = b \cdot (\ker f)$.

Důkaz. Víme, že pro libovolnou podgrupu H grupy G platí
$a^{-1} \cdot b \in H \quad \Leftrightarrow \quad a \cdot H = b \cdot H$,
proto to platí i pro $H = \ker f$.

Jestliže platí $f(a) = f(b)$, pak
$f(a^{-1} \cdot b) = f(a^{-1}) \cdot f(b) = f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(1) = 1$,
a tedy $a^{-1} \cdot b \in \ker f$.

Jestliže naopak platí $a^{-1} \cdot b \in \ker f$, pak $f(a^{-1} \cdot b) = 1$, proto
$f(a) = f(a) \cdot 1 = f(a) \cdot f(a^{-1} \cdot b) = f(a \cdot a^{-1} \cdot b) = f(b)$.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.

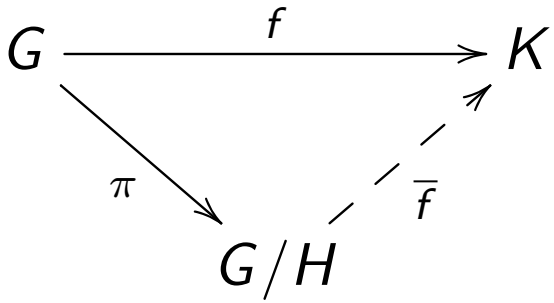
Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

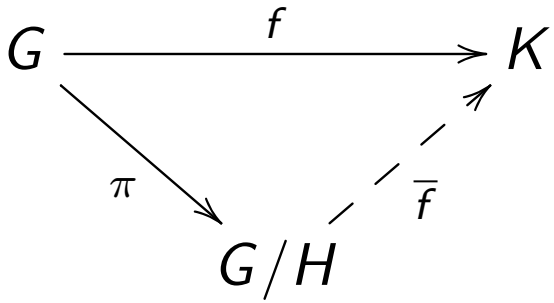
To můžeme znázornit diagramem takto:



Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

To můžeme znázornit diagramem takto:

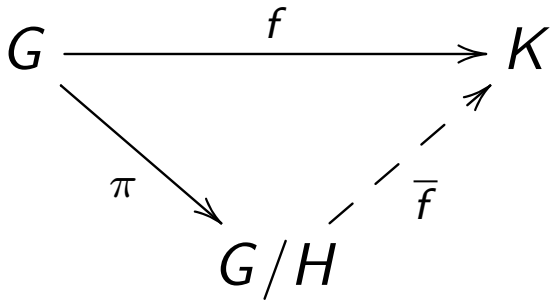


Pro každý prvek $h \in H$ platí $\pi(h) = h \cdot H = 1 \cdot H = \pi(1)$.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

To můžeme znázornit diagramem takto:



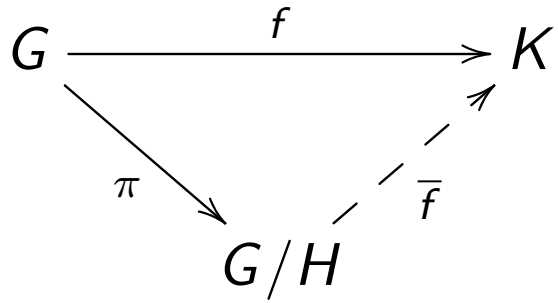
Pro každý prvek $h \in H$ platí $\pi(h) = h \cdot H = 1 \cdot H = \pi(1)$.

Pokud takové $\overline{f}$ existuje, musí pro každý prvek $h \in H$ platit
$f(h) = (\overline{f} \circ \pi)(h) = \overline{f}(\pi(h)) = \overline{f}(\pi(1)) = (\overline{f} \circ \pi)(1) = f(1) = 1$,

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

To můžeme znázornit diagramem takto:



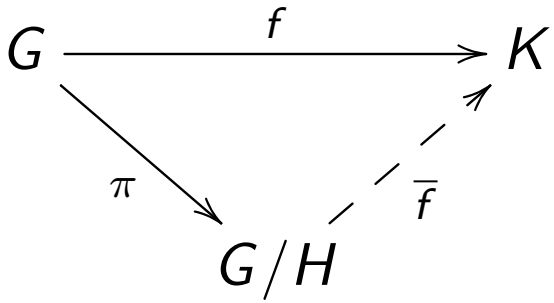
Pro každý prvek $h \in H$ platí $\pi(h) = h \cdot H = 1 \cdot H = \pi(1)$.

Pokud takové $\overline{f}$ existuje, musí pro každý prvek $h \in H$ platit
$f(h) = (\overline{f} \circ \pi)(h) = \overline{f}(\pi(h)) = \overline{f}(\pi(1)) = (\overline{f} \circ \pi)(1) = f(1) = 1$,
a tedy $h \in \ker f$.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

To můžeme znázornit diagramem takto:



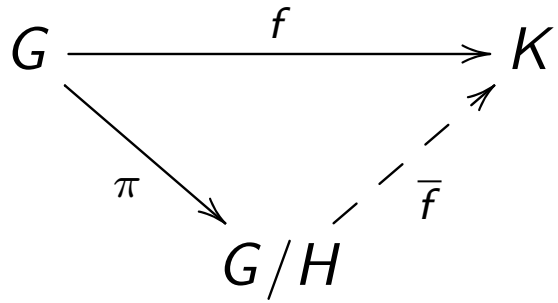
Pro každý prvek $h \in H$ platí $\pi(h) = h \cdot H = 1 \cdot H = \pi(1)$.

Pokud takové $\overline{f}$ existuje, musí pro každý prvek $h \in H$ platit
$f(h) = (\overline{f} \circ \pi)(h) = \overline{f}(\pi(h)) = \overline{f}(\pi(1)) = (\overline{f} \circ \pi)(1) = f(1) = 1$,
a tedy $h \in \ker f$.
Pokud tedy není splněna podmínka $H \subseteq \ker f$, nemůže takové $\overline{f}$ existovat.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

To můžeme znázornit diagramem takto:



Pro každý prvek $h \in H$ platí $\pi(h) = h \cdot H = 1 \cdot H = \pi(1)$.

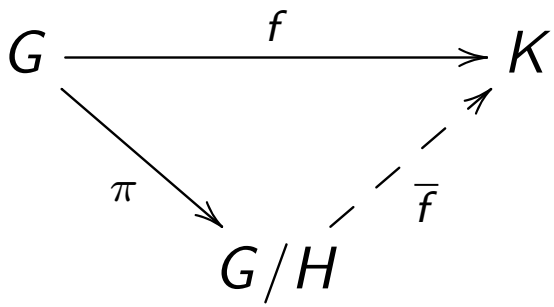
Pokud takové $\overline{f}$ existuje, musí pro každý prvek $h \in H$ platit
$f(h) = (\overline{f} \circ \pi)(h) = \overline{f}(\pi(h)) = \overline{f}(\pi(1)) = (\overline{f} \circ \pi)(1) = f(1) = 1$,
a tedy $h \in \ker f$.
Pokud tedy není splněna podmínka $H \subseteq \ker f$, nemůže takové $\overline{f}$ existovat.
Ale stačí tato podmínka, aby byla existence $\overline{f}$ zaručena?

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.*

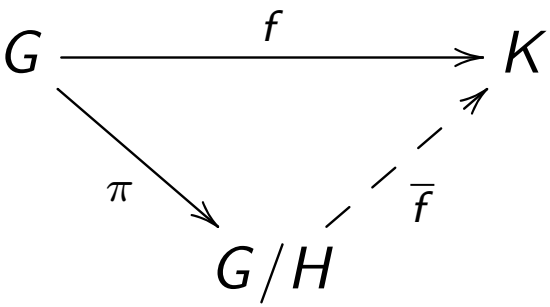
Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*



Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*

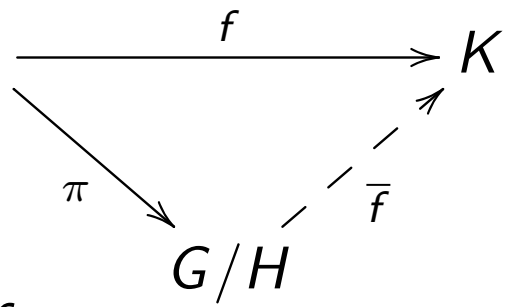


Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*

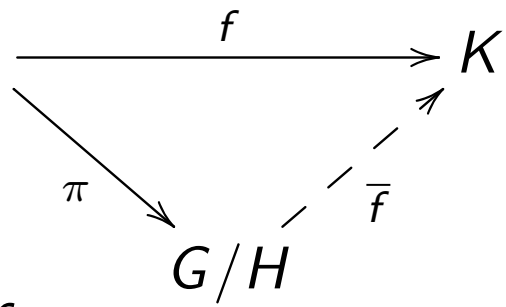


Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*
- *$\overline{f}$ je injekce, právě když $H = \ker f$,*

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*

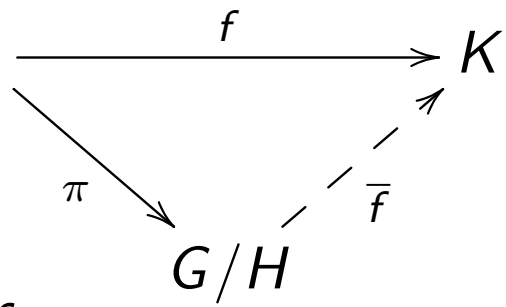


Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*



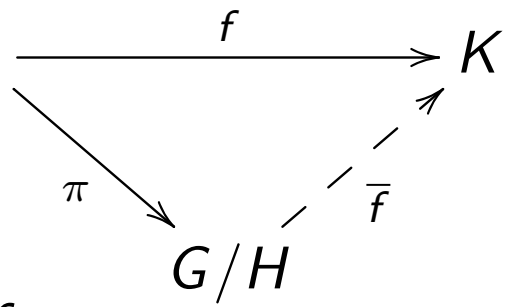
Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*
- *$\overline{f}$ je injekce, právě když $H = \ker f$,*
- *$\overline{f}$ je surjekce, právě když f je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$.

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*



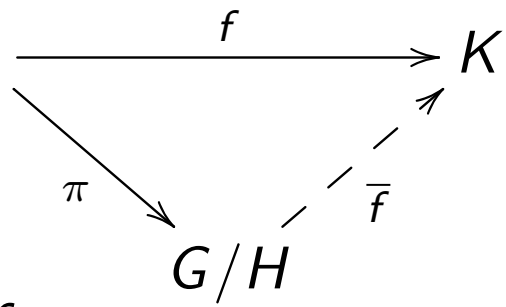
Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*
- *$\overline{f}$ je injekce, právě když $H = \ker f$,*
- *$\overline{f}$ je surjekce, právě když f je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$. Pak pro libovolné zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$ musí platit $\overline{f}(a \cdot H) = \overline{f}(\pi(a)) = (\overline{f} \circ \pi)(a) = f(a)$.

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*



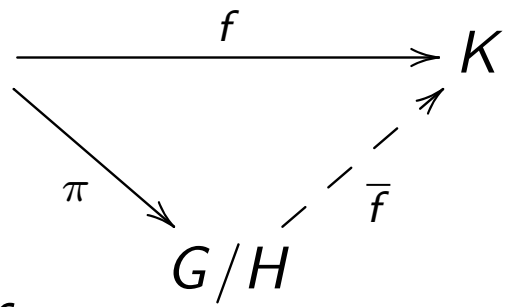
Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*
- *$\overline{f}$ je injekce, právě když $H = \ker f$,*
- *$\overline{f}$ je surjekce, právě když f je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$. Pak pro libovolné zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$ musí platit $\overline{f}(a \cdot H) = \overline{f}(\pi(a)) = (\overline{f} \circ \pi)(a) = f(a)$. Jediná možnost, jak definovat $\overline{f}$, je předpisem $\overline{f}(a \cdot H) = f(a)$.

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť* $f : G \to K$ *je homomorfismus grup,* H *normální podgrupa grupy* G *splňující* $H \subseteq \ker f$. *Nechť* $\pi : G \to G/H$ *je projekce grupy* G *na faktorgrupu* G/H. *Pak existuje, a to jediné, zobrazení* $\overline{f} : G/H \to K$ *splňující* $\overline{f} \circ \pi = f$.



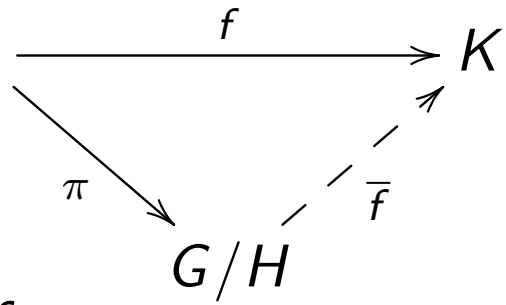
Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$. Pak pro libovolné zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$ musí platit $\overline{f}(a \cdot H) = \overline{f}(\pi(a)) = (\overline{f} \circ \pi)(a) = f(a)$. Jediná možnost, jak definovat $\overline{f}$, je předpisem $\overline{f}(a \cdot H) = f(a)$. Ale $a \cdot H = b \cdot H \Leftrightarrow a^{-1} \cdot b \in H \Rightarrow a^{-1} \cdot b \in \ker f \Leftrightarrow f(a) = f(b)$.

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť* $f : G \to K$ *je homomorfismus grup,* H *normální podgrupa grupy* G *splňující* $H \subseteq \ker f$. *Nechť* $\pi : G \to G/H$ *je projekce grupy* G *na faktorgrupu* G/H. *Pak existuje, a to jediné, zobrazení* $\overline{f} : G/H \to K$ *splňující* $\overline{f} \circ \pi = f$.



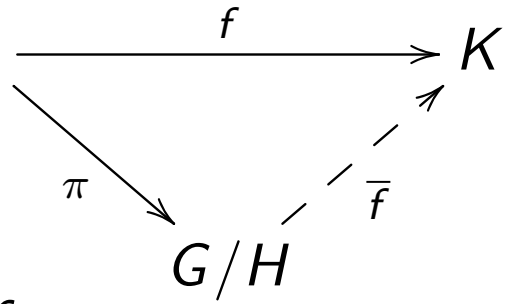
Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$. Pak pro libovolné zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$ musí platit $\overline{f}(a \cdot H) = \overline{f}(\pi(a)) = (\overline{f} \circ \pi)(a) = f(a)$. Jediná možnost, jak definovat $\overline{f}$, je předpisem $\overline{f}(a \cdot H) = f(a)$. Ale $a \cdot H = b \cdot H \Leftrightarrow a^{-1} \cdot b \in H \Rightarrow a^{-1} \cdot b \in \ker f \Leftrightarrow f(a) = f(b)$. Odtud nejen korektnost definice $\overline{f}$, ale také $H = \ker f \Leftrightarrow \overline{f}$ injekce.

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*



Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*
- *$\overline{f}$ je injekce, právě když $H = \ker f$,*
- *$\overline{f}$ je surjekce, právě když f je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$. Pak pro libovolné zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$ musí platit $\overline{f}(a \cdot H) = \overline{f}(\pi(a)) = (\overline{f} \circ \pi)(a) = f(a)$. Jediná možnost, jak definovat $\overline{f}$, je předpisem $\overline{f}(a \cdot H) = f(a)$. Ale $a \cdot H = b \cdot H \Leftrightarrow a^{-1} \cdot b \in H \Rightarrow a^{-1} \cdot b \in \ker f \Leftrightarrow f(a) = f(b)$. Odtud nejen korektnost definice $\overline{f}$, ale také $H = \ker f \Leftrightarrow \overline{f}$ injekce. Dále $\{\overline{f}(a \cdot H);\ a \in G\} = \{f(a);\ a \in G\}$, tj. f surjekce $\Leftrightarrow$ $\overline{f}$ surjekce.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$,

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\, a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\, a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\, a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$,

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$,

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\, a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$,

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$, je homomorfismus grupy $(\mathbb{R}^*, \cdot)$ do sebe

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$, je homomorfismus grupy $(\mathbb{R}^*, \cdot)$ do sebe s jádrem $\ker \mathrm{abs} = \{1, -1\}$

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$, je homomorfismus grupy $(\mathbb{R}^*, \cdot)$ do sebe s jádrem $\ker \mathrm{abs} = \{1, -1\}$ a obrazem $\mathrm{abs}(\mathbb{R}^*) = \mathbb{R}^+$,

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$, je homorfismus grupy $(\mathbb{R}^*, \cdot)$ do sebe s jádrem $\ker \mathrm{abs} = \{1, -1\}$ a obrazem $\mathrm{abs}(\mathbb{R}^*) = \mathbb{R}^+$, proto faktorgrupa $(\mathbb{R}^*/\{1, -1\}, \cdot) \cong (\mathbb{R}^+, \cdot)$.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\ a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\ a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$, je homorfismus grupy $(\mathbb{R}^*, \cdot)$ do sebe s jádrem $\ker \mathrm{abs} = \{1, -1\}$ a obrazem $\mathrm{abs}(\mathbb{R}^*) = \mathbb{R}^+$, proto faktorgrupa $(\mathbb{R}^*/\{1, -1\}, \cdot) \cong (\mathbb{R}^+, \cdot)$. Zde třída $\{a, -a\} \mapsto |a|$.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup,

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$,

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$,

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{C}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{C}^*$,

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{C}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{C}^*$, je homorfismus grupy $(\mathbb{C}^*, \cdot)$ do grupy $(\mathbb{R}^*, \cdot)$

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{C}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{C}^*$, je homorfismus grupy $(\mathbb{C}^*, \cdot)$ do grupy $(\mathbb{R}^*, \cdot)$ s jádrem $\ker \mathrm{abs} = \{a \in \mathbb{C};\ |a| = 1\}$

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{C}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{C}^*$, je homorfismus grupy $(\mathbb{C}^*, \cdot)$ do grupy $(\mathbb{R}^*, \cdot)$ s jádrem $\ker \mathrm{abs} = \{a \in \mathbb{C};\ |a| = 1\}$ a obrazem $\mathrm{abs}(\mathbb{C}^*) = \mathbb{R}^+$,

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{C}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{C}^*$, je homorfismus grupy $(\mathbb{C}^*, \cdot)$ do grupy $(\mathbb{R}^*, \cdot)$ s jádrem $\ker \mathrm{abs} = \{a \in \mathbb{C};\ |a| = 1\}$ a obrazem $\mathrm{abs}(\mathbb{C}^*) = \mathbb{R}^+$, proto faktorgrupa $(\mathbb{C}^*/\{a \in \mathbb{C};\ |a| = 1\}, \cdot) \cong (\mathbb{R}^+, \cdot)$.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G. Každá podgrupa grupy $(G, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot \ell;\ k \in K, \ell \in L\},$$

což obecně nemusí být podgrupa grupy $(G, \cdot)$.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G. Každá podgrupa grupy $(G, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot \ell;\ k \in K, \ell \in L\},$$

což obecně nemusí být podgrupa grupy $(G, \cdot)$. Ukažme, že je-li K dokonce normální podgrupa grupy $(G, \cdot)$, pak je $K \cdot L$ podgrupa grupy $(G, \cdot)$.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G. Každá podgrupa grupy $(G, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot \ell;\ k \in K, \ell \in L\},$$

což obecně nemusí být podgrupa grupy $(G, \cdot)$. Ukažme, že je-li K dokonce normální podgrupa grupy $(G, \cdot)$, pak je $K \cdot L$ podgrupa grupy $(G, \cdot)$. Jistě $1 = 1 \cdot 1 \in K \cdot L$.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G. Každá podgrupa grupy $(G, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot \ell;\ k \in K, \ell \in L\},$$

což obecně nemusí být podgrupa grupy $(G, \cdot)$. Ukažme, že je-li K dokonce normální podgrupa grupy $(G, \cdot)$, pak je $K \cdot L$ podgrupa grupy $(G, \cdot)$. Jistě $1 = 1 \cdot 1 \in K \cdot L$. Pro libovolné $k \in K$, $\ell \in L$ platí

$$(k \cdot \ell)^{-1} = \ell^{-1} \cdot k^{-1} = (\ell^{-1} \cdot k^{-1} \cdot \ell) \cdot \ell^{-1} \in K \cdot L,$$

neboť $\ell^{-1} \cdot k^{-1} \cdot \ell \in K$ díky tomu, že K je normální podgrupa grupy $(G, \cdot)$.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G. Každá podgrupa grupy $(G, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot \ell;\ k \in K, \ell \in L\},$$

což obecně nemusí být podgrupa grupy $(G, \cdot)$. Ukažme, že je-li K dokonce normální podgrupa grupy $(G, \cdot)$, pak je $K \cdot L$ podgrupa grupy $(G, \cdot)$. Jistě $1 = 1 \cdot 1 \in K \cdot L$. Pro libovolné $k \in K$, $\ell \in L$ platí

$$(k \cdot \ell)^{-1} = \ell^{-1} \cdot k^{-1} = (\ell^{-1} \cdot k^{-1} \cdot \ell) \cdot \ell^{-1} \in K \cdot L,$$

neboť $\ell^{-1} \cdot k^{-1} \cdot \ell \in K$ díky tomu, že K je normální podgrupa grupy $(G, \cdot)$. Podobně pro libovolné $k_1, k_2 \in K$, $\ell_1, \ell_2 \in L$ platí

$$(k_1 \cdot \ell_1) \cdot (k_2 \cdot \ell_2) = k_1 \cdot (\ell_1 \cdot k_2 \cdot \ell_1^{-1}) \cdot (\ell_1 \cdot \ell_2) \in K \cdot L,$$

neboť opět $\ell_1 \cdot k_2 \cdot \ell_1^{-1} \in K$.

Svaz všech normálních podgrup dané grupy

Věta. *Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech normálních podgrup grupy G uspořádaná inkluzí je modulární svaz.*

Důkaz. Nechť K, L jsou podgrupy grupy G. Každá podgrupa grupy $(G, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot \ell;\ k \in K, \ell \in L\},$$

což obecně nemusí být podgrupa grupy $(G, \cdot)$. Ukažme, že je-li K dokonce normální podgrupa grupy $(G, \cdot)$, pak je $K \cdot L$ podgrupa grupy $(G, \cdot)$. Jistě $1 = 1 \cdot 1 \in K \cdot L$. Pro libovolné $k \in K$, $\ell \in L$ platí

$$(k \cdot \ell)^{-1} = \ell^{-1} \cdot k^{-1} = (\ell^{-1} \cdot k^{-1} \cdot \ell) \cdot \ell^{-1} \in K \cdot L,$$

neboť $\ell^{-1} \cdot k^{-1} \cdot \ell \in K$ díky tomu, že K je normální podgrupa grupy $(G, \cdot)$. Podobně pro libovolné $k_1, k_2 \in K$, $\ell_1, \ell_2 \in L$ platí

$$(k_1 \cdot \ell_1) \cdot (k_2 \cdot \ell_2) = k_1 \cdot (\ell_1 \cdot k_2 \cdot \ell_1^{-1}) \cdot (\ell_1 \cdot \ell_2) \in K \cdot L,$$

neboť opět $\ell_1 \cdot k_2 \cdot \ell_1^{-1} \in K$. Dokázali jsme, že $K \cdot L$ je podgrupa grupy $(G, \cdot)$, a to ta nejmenší obsahující K i L.

Přitom platí, že pokud jsou obě K i L normálními podgrupami grupy $(G, \cdot)$, pak je $K \cdot L$ též normální podgrupou grupy $(G, \cdot)$.

Přitom platí, že pokud jsou obě K i L normálními podgrupami grupy $(G, \cdot)$, pak je $K \cdot L$ též normální podgrupou grupy $(G, \cdot)$. Totiž pro libovolné $h \in G$ a libovolné $k \in K$, $\ell \in L$ platí

$$h \cdot (k \cdot \ell) \cdot h^{-1} = (h \cdot k \cdot h^{-1}) \cdot (h \cdot \ell \cdot h^{-1}) \in K \cdot L,$$

což bylo třeba dokázat.

Přitom platí, že pokud jsou obě K i L normálními podgrupami grupy $(G, \cdot)$, pak je $K \cdot L$ též normální podgrupou grupy $(G, \cdot)$. Totiž pro libovolné $h \in G$ a libovolné $k \in K$, $\ell \in L$ platí

$$h \cdot (k \cdot \ell) \cdot h^{-1} = (h \cdot k \cdot h^{-1}) \cdot (h \cdot \ell \cdot h^{-1}) \in K \cdot L,$$

což bylo třeba dokázat.
Označme S množinu všech normálních podgrup grupy $(G, \cdot)$.

Přitom platí, že pokud jsou obě K i L normálními podgrupami grupy $(G, \cdot)$, pak je $K \cdot L$ též normální podgrupou grupy $(G, \cdot)$. Totiž pro libovolné $h \in G$ a libovolné $k \in K$, $\ell \in L$ platí

$$h \cdot (k \cdot \ell) \cdot h^{-1} = (h \cdot k \cdot h^{-1}) \cdot (h \cdot \ell \cdot h^{-1}) \in K \cdot L,$$

což bylo třeba dokázat.
Označme S množinu všech normálních podgrup grupy $(G, \cdot)$. Protože G je největší svá normální podgrupa a průnikem libovolného neprázdného systému normálních podgrup grupy G je normální podgrupa grupy G, je $(S, \subseteq)$ úplný svaz, v němž pro libovolné $K, L \in S$ platí

$$K \wedge L = K \cap L, \qquad K \vee L = K \cdot L.$$

Přitom platí, že pokud jsou obě K i L normálními podgrupami grupy $(G, \cdot)$, pak je $K \cdot L$ též normální podgrupou grupy $(G, \cdot)$. Totiž pro libovolné $h \in G$ a libovolné $k \in K$, $\ell \in L$ platí

$$h \cdot (k \cdot \ell) \cdot h^{-1} = (h \cdot k \cdot h^{-1}) \cdot (h \cdot \ell \cdot h^{-1}) \in K \cdot L,$$

což bylo třeba dokázat.
Označme S množinu všech normálních podgrup grupy $(G, \cdot)$. Protože G je největší svá normální podgrupa a průnikem libovolného neprázdného systému normálních podgrup grupy G je normální podgrupa grupy G, je $(S, \subseteq)$ úplný svaz, v němž pro libovolné $K, L \in S$ platí

$$K \wedge L = K \cap L, \qquad K \vee L = K \cdot L.$$

Dokážeme, že je tento svaz modulární.

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$.

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$. Platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$. Platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Máme tedy ukázat, že platí

$$(K \cap L) \cdot M \supseteq K \cap (L \cdot M),$$

neboť opačná inkluze je modulární nerovnost platná v každém svazu.

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$. Platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Máme tedy ukázat, že platí

$$(K \cap L) \cdot M \supseteq K \cap (L \cdot M),$$

neboť opačná inkluze je modulární nerovnost platná v každém svazu.
Nechť je tedy $k \in K \cap (L \cdot M)$ libovolné.

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$. Platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Máme tedy ukázat, že platí

$$(K \cap L) \cdot M \supseteq K \cap (L \cdot M),$$

neboť opačná inkluze je modulární nerovnost platná v každém svazu.
Nechť je tedy $k \in K \cap (L \cdot M)$ libovolné. Pak existují $\ell \in L$, $m \in M$ takové, že platí $\ell \cdot m = k$.

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$. Platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Máme tedy ukázat, že platí

$$(K \cap L) \cdot M \supseteq K \cap (L \cdot M),$$

neboť opačná inkluze je modulární nerovnost platná v každém svazu.
Nechť je tedy $k \in K \cap (L \cdot M)$ libovolné. Pak existují $\ell \in L$, $m \in M$ takové, že platí $\ell \cdot m = k$. Z $M \subseteq K$ plyne $m \in K$, odkud $\ell = k \cdot m^{-1} \in K$.

Zvolme libovolně $K, L, M \in S$ tak, že $M \subseteq K$ a ukažme, že $(K \wedge L) \vee M = K \wedge (L \vee M)$. Platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Máme tedy ukázat, že platí

$$(K \cap L) \cdot M \supseteq K \cap (L \cdot M),$$

neboť opačná inkluze je modulární nerovnost platná v každém svazu.
Nechť je tedy $k \in K \cap (L \cdot M)$ libovolné. Pak existují $\ell \in L$, $m \in M$ takové, že platí $\ell \cdot m = k$. Z $M \subseteq K$ plyne $m \in K$, odkud $\ell = k \cdot m^{-1} \in K$. Je tedy $\ell \in (K \cap L)$ a platí $k = \ell \cdot m \in (K \cap L) \cdot M$, což jsme chtěli dokázat.

Další příklady modulárních svazů uvedené dříve bez důkazu

Důsledek. *Svaz všech podgrup libovolné komutativní grupy je modulární.*

Další příklady modulárních svazů uvedené dříve bez důkazu

Důsledek. *Svaz všech podgrup libovolné komutativní grupy je modulární.*

Důkaz. V komutativní grupě je každá podgrupa normální.

Další příklady modulárních svazů uvedené dříve bez důkazu

Důsledek. *Svaz všech podgrup libovolné komutativní grupy je modulární.*

Důkaz. V komutativní grupě je každá podgrupa normální.

Důsledek. *Pro libovolný vektorový prostor V nad tělesem T platí, že množina všech podprostorů vektorového prostoru V uspořádaná inkluzí je modulární svaz.*

Další příklady modulárních svazů uvedené dříve bez důkazu

Důsledek. *Svaz všech podgrup libovolné komutativní grupy je modulární.*

Důkaz. V komutativní grupě je každá podgrupa normální.

Důsledek. *Pro libovolný vektorový prostor V nad tělesem T platí, že množina všech podprostorů vektorového prostoru V uspořádaná inkluzí je modulární svaz.*

Důkaz. Protože podsvaz libovolného modulárního svazu je modulární, stačí ověřit, že svaz všech podprostorů vektorového prostoru V nad tělesem T je podsvazem svazu všech podgrup grupy vektorů V, která je komutativní.

Další příklady modulárních svazů uvedené dříve bez důkazu

Důsledek. *Svaz všech podgrup libovolné komutativní grupy je modulární.*

Důkaz. V komutativní grupě je každá podgrupa normální.

Důsledek. *Pro libovolný vektorový prostor V nad tělesem T platí, že množina všech podprostorů vektorového prostoru V uspořádaná inkluzí je modulární svaz.*

Důkaz. Protože podsvaz libovolného modulárního svazu je modulární, staří ověřit, že svaz všech podprostorů vektorového prostoru V nad tělesem T je podsvazem svazu všech podgrup grupy vektorů V, která je komutativní.
K tomu si stačí uvědomit, že každý podprostor je podgrupou, a ověřit, že infima i suprema se ve svazu všech podprostorů počítají stejně jako ve svazu podgrup: infimem dvou podprostorů je jejich množinový průnik a jejich supremem je jejich součet.

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty.*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$.*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$.*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathbb{S}_n$.*

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathbb{S}_n$.* [Věta 8.14, str. 43]

Poznámka. V předchozí větě jsme každý prvek a grupy $(G, \cdot)$ reprezentovali permutací r_a nosné množiny G.

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathbb{S}_n$.* [Věta 8.14, str. 43]

Poznámka. V předchozí větě jsme každý prvek a grupy $(G, \cdot)$ reprezentovali permutací r_a nosné množiny G. Tuto situaci lze zobecnit, můžeme prvky grupy $(G, \cdot)$ reprezentovat permutacemi nějaké jiné množiny X, kterou můžeme libovolně zvolit.

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathbb{S}_n$.* [Věta 8.14, str. 43]

Poznámka. V předchozí větě jsme každý prvek a grupy $(G, \cdot)$ reprezentovali permutací r_a nosné množiny G. Tuto situaci lze zobecnit, můžeme prvky grupy $(G, \cdot)$ reprezentovat permutacemi nějaké jiné množiny X, kterou můžeme libovolně zvolit. Budeme tedy studovat homomorfismy $G \to \mathbb{S}(X)$.

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathbb{S}_n$.* [Věta 8.14, str. 43]

Poznámka. V předchozí větě jsme každý prvek a grupy $(G, \cdot)$ reprezentovali permutací r_a nosné množiny G. Tuto situaci lze zobecnit, můžeme prvky grupy $(G, \cdot)$ reprezentovat permutacemi nějaké jiné množiny X, kterou můžeme libovolně zvolit. Budeme tedy studovat homomorfismy $G \to \mathbb{S}(X)$. Této situaci říkáme reprezentace grupy G permutacemi na množině X anebo stručně **akce grupy G na množině X**.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y,

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$:

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$: platí-li $f(y) = y$, je $O_y = \{y\}$, v opačném případě je O_y množina všech prvků z cyklu, v němž vystupuje y.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$: platí-li $f(y) = y$, je $O_y = \{y\}$, v opačném případě je O_y množina všech prvků z cyklu, v němž vystupuje y. Stabilizátorem S_y prvku y je množina všech mocnin f^k permutace f, které ponechávají y na místě, tj. splňují $f^k(y) = y$.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$: platí-li $f(y) = y$, je $O_y = \{y\}$, v opačném případě je O_y množina všech prvků z cyklu, v němž vystupuje y. Stabilizátorem S_y prvku y je množina všech mocnin f^k permutace f, které ponechávají y na místě, tj. splňují $f^k(y) = y$. Jde o podgrupu grupy G generovanou permutací $f^{|O_y|}$, tj. $S_y = \langle f^{|O_y|} \rangle$.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$: platí-li $f(y) = y$, je $O_y = \{y\}$, v opačném případě je O_y množina všech prvků z cyklu, v němž vystupuje y. Stabilizátorem S_y prvku y je množina všech mocnin f^k permutace f, které ponechávají y na místě, tj. splňují $f^k(y) = y$. Jde o podgrupu grupy G generovanou permutací $f^{|O_y|}$, tj. $S_y = \langle f^{|O_y|} \rangle$. Platí proto $|G/S_y| = |O_y|$.

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

[Věta 8.17, str. 44]

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.*

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

[Věta 8.17, str. 44]

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.*

Věta. *Předpokládejme navíc, že X je konečná množina. Pak pro každé $y \in X$ je počet prvků v orbitě O_y roven indexu stabilizátoru S_y, tj. $|O_y| = |G/S_y|$.*

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

[Věta 8.17, str. 44]

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.*

Věta. *Předpokládejme navíc, že X je konečná množina. Pak pro každé $y \in X$ je počet prvků v orbitě O_y roven indexu stabilizátoru S_y, tj. $|O_y| = |G/S_y|$.* [Věta 8.19, str. 45]

Důsledek. *Nechť je navíc X konečná množina a $y_1, \ldots, y_m \in X$ jsou takové, že v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$ (a tedy m je počet orbit). Pak platí $|X| = \sum_{i=1}^{m} |G/S_{y_i}|$.*

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

[Věta 8.17, str. 44]

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.*

Věta. *Předpokládejme navíc, že X je konečná množina. Pak pro každé $y \in X$ je počet prvků v orbitě O_y roven indexu stabilizátoru S_y, tj. $|O_y| = |G/S_y|$.* [Věta 8.19, str. 45]

Důsledek. *Nechť je navíc X konečná množina a $y_1, \ldots, y_m \in X$ jsou takové, že v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$ (a tedy m je počet orbit). Pak platí $|X| = \sum_{i=1}^{m} |G/S_{y_i}|$.* [Důsledek 8.20, str. 45]

Věta (Burnsidovo lemma). *Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$.*

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

[Věta 8.17, str. 44]

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.*

Věta. *Předpokládejme navíc, že X je konečná množina. Pak pro každé $y \in X$ je počet prvků v orbitě O_y roven indexu stabilizátoru S_y, tj. $|O_y| = |G/S_y|$.* [Věta 8.19, str. 45]

Důsledek. *Nechť je navíc X konečná množina a $y_1, \ldots, y_m \in X$ jsou takové, že v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$ (a tedy m je počet orbit). Pak platí $|X| = \sum_{i=1}^{m} |G/S_{y_i}|$.* [Důsledek 8.20, str. 45]

Věta (Burnsidovo lemma). *Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.*

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right|$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y|$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y|$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|}$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|}$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|} =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_{y_i}|}$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|} =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |O_{y_i}| \frac{|G|}{|O_{y_i}|}$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|} =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |O_{y_i}| \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |G|$$

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|} =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |O_{y_i}| \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |G| = m|G|.$$

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek. Abychom zjistili, která obarvení dávají stejný náramek, užijme grupu $\mathbb{D}_7$ všech symetrií pravidelného 7úhelníka a definujme $\varphi : \mathbb{D}_7 \to \mathbb{S}(X)$ takto: pro symetrii $a \in \mathbb{D}_7$ a obarvení $y \in X$ je $\varphi(a)(y)$ to obarvení, které z y vznikne, aplikujeme-li na 7úhelník symetrii a.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek. Abychom zjistili, která obarvení dávají stejný náramek, užijme grupu $\mathbb{D}_7$ všech symetrií pravidelného 7úhelníka a definujme $\varphi : \mathbb{D}_7 \to \mathbb{S}(X)$ takto: pro symetrii $a \in \mathbb{D}_7$ a obarvení $y \in X$ je $\varphi(a)(y)$ to obarvení, které z y vznikne, aplikujeme-li na 7úhelník symetrii a. Pak dvě obarvení z množiny X odpovídají témuž náramku, právě když patří do stejné orbity.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek. Abychom zjistili, která obarvení dávají stejný náramek, užijme grupu $\mathbb{D}_7$ všech symetrií pravidelného 7úhelníka a definujme $\varphi : \mathbb{D}_7 \to \mathbb{S}(X)$ takto: pro symetrii $a \in \mathbb{D}_7$ a obarvení $y \in X$ je $\varphi(a)(y)$ to obarvení, které z y vznikne, aplikujeme-li na 7úhelník symetrii a. Pak dvě obarvení z množiny X odpovídají témuž náramku, právě když patří do stejné orbity. Pro identitu id je $|F_{\mathrm{id}}| = |X| = n^7$, pro libovolnou ze 6 zbylých rotací $r \in \mathbb{D}_7$ je $|F_r| = n$ a pro každou ze 7 osových souměrností s je $|F_s| = n^4$.

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek. Abychom zjistili, která obarvení dávají stejný náramek, užijme grupu $\mathbb{D}_7$ všech symetrií pravidelného 7úhelníka a definujme $\varphi : \mathbb{D}_7 \to \mathbb{S}(X)$ takto: pro symetrii $a \in \mathbb{D}_7$ a obarvení $y \in X$ je $\varphi(a)(y)$ to obarvení, které z y vznikne, aplikujeme-li na 7úhelník symetrii a. Pak dvě obarvení z množiny X odpovídají témuž náramku, právě když patří do stejné orbity. Pro identitu id je $|F_{\mathrm{id}}| = |X| = n^7$, pro libovolnou ze 6 zbylých rotací $r \in \mathbb{D}_7$ je $|F_r| = n$ a pro každou ze 7 osových souměrností s je $|F_s| = n^4$. Podle Burnsidova lemmatu je hledaný počet $\frac{1}{14}(n^7 + 7n^4 + 6n)$.

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Důkaz. Pro libovolné $a, b, g \in G$ platí $(\rho_a \circ \rho_b)(g) = \rho_a(\rho_b(g)) = \rho_a(b \cdot g \cdot b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \rho_{ab}(g)$.

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Důkaz. Pro libovolné $a, b, g \in G$ platí $(\rho_a \circ \rho_b)(g) = \rho_a(\rho_b(g)) = \rho_a(b \cdot g \cdot b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \rho_{ab}(g)$. Zřejmě $\rho_1(g) = 1 \cdot g \cdot 1^{-1} = g = \mathrm{id}(g)$, a tedy $\rho_1 = \mathrm{id}$.

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Důkaz. Pro libovolné $a, b, g \in G$ platí $(\rho_a \circ \rho_b)(g) = \rho_a(\rho_b(g)) = \rho_a(b \cdot g \cdot b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \rho_{ab}(g)$.
Zřejmě $\rho_1(g) = 1 \cdot g \cdot 1^{-1} = g = \mathrm{id}(g)$, a tedy $\rho_1 = \mathrm{id}$.
Odtud plyne, že $\rho_a \circ \rho_{a^{-1}} = \mathrm{id}$ a $\rho_{a^{-1}} \circ \rho_a = \mathrm{id}$, tedy ρ_a je bijekce a platí $\rho_a^{-1} = \rho_{a^{-1}}$.

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Důkaz. Pro libovolné $a, b, g \in G$ platí $(\rho_a \circ \rho_b)(g) = \rho_a(\rho_b(g)) = \rho_a(b \cdot g \cdot b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \rho_{ab}(g)$.
Zřejmě $\rho_1(g) = 1 \cdot g \cdot 1^{-1} = g = \mathrm{id}(g)$, a tedy $\rho_1 = \mathrm{id}$.
Odtud plyne, že $\rho_a \circ \rho_{a^{-1}} = \mathrm{id}$ a $\rho_{a^{-1}} \circ \rho_a = \mathrm{id}$, tedy ρ_a je bijekce a platí $\rho_a^{-1} = \rho_{a^{-1}}$.
Konečně pro libovolné $a, g, h \in G$ platí
$\rho_a(g) \cdot \rho_a(h) = a \cdot g \cdot a^{-1} \cdot a \cdot h \cdot a^{-1} = a \cdot g \cdot h \cdot a^{-1} = \rho_a(g \cdot h)$,
je tedy ρ_a homomorfismus.

Vnitřní automorfismy grupy G

Definice. Nechť G je grupa. Libovolný izomorfismus $f : G \to G$ nazýváme **automorfismus** grupy G.

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Důkaz. Pro libovolné $a, b, g \in G$ platí $(\rho_a \circ \rho_b)(g) = \rho_a(\rho_b(g)) = \rho_a(b \cdot g \cdot b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \rho_{ab}(g)$.
Zřejmě $\rho_1(g) = 1 \cdot g \cdot 1^{-1} = g = \mathrm{id}(g)$, a tedy $\rho_1 = \mathrm{id}$.
Odtud plyne, že $\rho_a \circ \rho_{a^{-1}} = \mathrm{id}$ a $\rho_{a^{-1}} \circ \rho_a = \mathrm{id}$, tedy ρ_a je bijekce a platí $\rho_a^{-1} = \rho_{a^{-1}}$.
Konečně pro libovolné $a, g, h \in G$ platí
$\rho_a(g) \cdot \rho_a(h) = a \cdot g \cdot a^{-1} \cdot a \cdot h \cdot a^{-1} = a \cdot g \cdot h \cdot a^{-1} = \rho_a(g \cdot h)$,
je tedy ρ_a homomorfismus.

Definice. Izomorfismy z předchozí věty nazýváme **vnitřní automorfismy** grupy G.

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G;\ \forall g \in G : a \cdot g = g \cdot a\}$.

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G; \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G; \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G; \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G; \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro* $\ker \rho = Z(G)$.

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G; \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj. $O_g = \{g\} \quad \Leftrightarrow \quad g \in Z(G)$.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G;\ \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj. $O_g = \{g\} \quad \Leftrightarrow \quad g \in Z(G)$.*

Důsledek. *Centrum $Z(G)$ je normální podgrupa grupy G.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G;\ \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj. $O_g = \{g\} \quad \Leftrightarrow \quad g \in Z(G)$.*

Důsledek. *Centrum $Z(G)$ je normální podgrupa grupy G. Obraz $\rho(G)$ grupy G v homomorfismu ρ je izomorfní s faktorgrupou $G/Z(G)$.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G;\ \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj. $O_g = \{g\} \quad \Leftrightarrow \quad g \in Z(G)$.*

Důsledek. *Centrum $Z(G)$ je normální podgrupa grupy G. Obraz $\rho(G)$ grupy G v homomorfismu ρ je izomorfní s faktorgrupou $G/Z(G)$. Grupa G má tedy právě $\frac{|G|}{|Z(G)|}$ vnitřních automorfismů.*

Akce grupy G na množině G vnitřními automorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím **centrem** $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G;\ \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní automorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj. $O_g = \{g\} \quad \Leftrightarrow \quad g \in Z(G)$.*

Důsledek. *Centrum $Z(G)$ je normální podgrupa grupy G. Obraz $\rho(G)$ grupy G v homomorfismu ρ je izomorfní s faktorgrupou $G/Z(G)$. Grupa G má tedy právě $\frac{|G|}{|Z(G)|}$ vnitřních automorfismů.*

Poznámka. Je-li H podgrupa grupy G taková, že $H \subseteq Z(G)$, pak H je normální podgrupa grupy G. [$\forall a \in G\ \forall h \in H$: $a \cdot h \cdot a^{-1} = h \cdot a \cdot a^{-1} = h \in H$.]

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru,

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$a \in Z(G) \qquad \Leftrightarrow \qquad |O_a| = 1,$$

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$\begin{aligned} a \in Z(G) \quad &\Leftrightarrow \quad |O_a| = 1, \\ a \notin Z(G) \quad &\Rightarrow \quad p \mid |O_a|. \end{aligned}$$

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$\begin{aligned} a \in Z(G) \quad &\Leftrightarrow \quad |O_a| = 1, \\ a \notin Z(G) \quad &\Rightarrow \quad p \mid |O_a|. \end{aligned}$$

Každý prvek z G patří do právě jedné orbity, počet prvků grupy $|G|$ je dělitelný číslem p.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$\begin{aligned} a \in Z(G) \quad &\Leftrightarrow \quad |O_a| = 1, \\ a \notin Z(G) \quad &\Rightarrow \quad p \mid |O_a|. \end{aligned}$$

Každý prvek z G patří do právě jedné orbity, počet prvků grupy $|G|$ je dělitelný číslem p. Sečtením právě $|Z(G)|$ jedniček a několika sčítanců dělitelných p dostaneme součet dělitelný p.

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$\begin{aligned} a \in Z(G) \quad &\Leftrightarrow \quad |O_a| = 1, \\ a \notin Z(G) \quad &\Rightarrow \quad p \mid |O_a|. \end{aligned}$$

Každý prvek z G patří do právě jedné orbity, počet prvků grupy $|G|$ je dělitelný číslem p. Sečtením právě $|Z(G)|$ jedniček a několika sčítanců dělitelných p dostaneme součet dělitelný p. Proto je počet těchto jedniček dělitelný p, tedy $p \mid |Z(G)|$.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu. Pak existuje $a \in G - Z(G)$, a tedy $M = Z(G) \cup \{a, a^{-1}\}$ má více než p prvků, proto podle Lagrangeovy věty $\langle M \rangle = G$.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu. Pak existuje $a \in G - Z(G)$, a tedy $M = Z(G) \cup \{a, a^{-1}\}$ má více než p prvků, proto podle Lagrangeovy věty $\langle M \rangle = G$. Ovšem podle věty o podgrupě generované množinou je libovolný prvek $\langle M \rangle$ součinem několika prvků z M.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu. Pak existuje $a \in G - Z(G)$, a tedy $M = Z(G) \cup \{a, a^{-1}\}$ má více než p prvků, proto podle Lagrangeovy věty $\langle M \rangle = G$. Ovšem podle věty o podgrupě generované množinou je libovolný prvek $\langle M \rangle$ součinem několika prvků z M. Protože prvky z centra $Z(G)$ komutují s každým prvkem grupy G, je

$$G = \langle M \rangle = \{a^n \cdot h \mid n \in \mathbb{Z}, h \in Z(G)\}.$$

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu. Pak existuje $a \in G - Z(G)$, a tedy $M = Z(G) \cup \{a, a^{-1}\}$ má více než p prvků, proto podle Lagrangeovy věty $\langle M \rangle = G$. Ovšem podle věty o podgrupě generované množinou je libovolný prvek $\langle M \rangle$ součinem několika prvků z M. Protože prvky z centra $Z(G)$ komutují s každým prvkem grupy G, je

$$G = \langle M \rangle = \{a^n \cdot h \mid n \in \mathbb{Z}, h \in Z(G)\}.$$

Pro libovolná $h, h' \in Z(G)$ a $n, n' \in \mathbb{Z}$ pak platí $(a^n \cdot h) \cdot (a^{n'} \cdot h') = a^{n+n'} \cdot h \cdot h' = (a^{n'} \cdot h') \cdot (a^n \cdot h)$.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu. Pak existuje $a \in G - Z(G)$, a tedy $M = Z(G) \cup \{a, a^{-1}\}$ má více než p prvků, proto podle Lagrangeovy věty $\langle M \rangle = G$. Ovšem podle věty o podgrupě generované množinou je libovolný prvek $\langle M \rangle$ součinem několika prvků z M. Protože prvky z centra $Z(G)$ komutují s každým prvkem grupy G, je

$$G = \langle M \rangle = \{a^n \cdot h \mid n \in \mathbb{Z}, h \in Z(G)\}.$$

Pro libovolná $h, h' \in Z(G)$ a $n, n' \in \mathbb{Z}$ pak platí $(a^n \cdot h) \cdot (a^{n'} \cdot h') = a^{n+n'} \cdot h \cdot h' = (a^{n'} \cdot h') \cdot (a^n \cdot h)$. Je tedy grupa G komutativní, tudíž $Z(G) = G$, spor.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p. Nechť zobrazení $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ je určené předpisem $f(([n]_p, [m]_p)) = a^n \cdot b^m$.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p. Nechť zobrazení $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ je určené předpisem $f(([n]_p, [m]_p)) = a^n \cdot b^m$. Protože řády obou prvků a, b jsou p, je toto zobrazení definováno korektně.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p. Nechť zobrazení $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ je určené předpisem $f(([n]_p, [m]_p)) = a^n \cdot b^m$. Protože řády obou prvků a, b jsou p, je toto zobrazení definováno korektně.
Protože G je komutativní, je f homomorfismus grup.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p. Nechť zobrazení $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ je určené předpisem $f(([n]_p, [m]_p)) = a^n \cdot b^m$. Protože řády obou prvků a, b jsou p, je toto zobrazení definováno korektně.
Protože G je komutativní, je f homomorfismus grup. Přitom obraz $f(\mathbb{Z}_p \times \mathbb{Z}_p)$ obsahuje všechny mocniny prvku a i prvek b, je to tedy podgrupa grupy G mající více než p prvků, tedy f je surjektivní.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p. Nechť zobrazení $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ je určené předpisem $f(([n]_p, [m]_p)) = a^n \cdot b^m$. Protože řády obou prvků a, b jsou p, je toto zobrazení definováno korektně.
Protože G je komutativní, je f homomorfismus grup. Přitom obraz $f(\mathbb{Z}_p \times \mathbb{Z}_p)$ obsahuje všechny mocniny prvku a i prvek b, je to tedy podgrupa grupy G mající více než p prvků, tedy f je surjektivní. Protože $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2 = |G|$, je f bijekce, tudíž izomorfismus.

Motivace následujících vět

Poznámka. Pro libovolnou konečnou grupu G nám Lagrangeova věta říká, že řád každé podgrupy grupy G dělí řád grupy G.

Motivace následujících vět

Poznámka. Pro libovolnou konečnou grupu G nám Lagrangeova věta říká, že řád každé podgrupy grupy G dělí řád grupy G. Naopak se můžeme ptát, jestli pro každého dělitele d řádu grupy G existuje podgrupa H grupy G mající řád d.

Motivace následujících vět

Poznámka. Pro libovolnou konečnou grupu G nám Lagrangeova věta říká, že řád každé podgrupy grupy G dělí řád grupy G.
Naopak se můžeme ptát, jestli pro každého dělitele d řádu grupy G existuje podgrupa H grupy G mající řád d.
Takto obecně to pravda není, je možné ukázat, že například grupa $\mathbb{A}_4$ řádu 12 nemá žádnou podgrupu řádu 6.

Motivace následujících vět

Poznámka. Pro libovolnou konečnou grupu G nám Lagrangeova věta říká, že řád každé podgrupy grupy G dělí řád grupy G.
Naopak se můžeme ptát, jestli pro každého dělitele d řádu grupy G existuje podgrupa H grupy G mající řád d.
Takto obecně to pravda není, je možné ukázat, že například grupa $\mathbb{A}_4$ řádu 12 nemá žádnou podgrupu řádu 6.
Pomocí akce grupy na množině v následujících větách ukážeme, že to je pravda, pokud je d mocnina prvočísla.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X. Pro libovolné $x = (y_1, \ldots, y_p) \in X$ orbita O_x má jediný prvek, je-li $y_1 = \cdots = y_p$, a právě p prvků jinak.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X. Pro libovolné $x = (y_1, \ldots, y_p) \in X$ orbita O_x má jediný prvek, je-li $y_1 = \cdots = y_p$, a právě p prvků jinak. Protože orbity tvoří rozklad množiny X, je $|X|$ součtem několika sčítanců, z nichž každý je 1 nebo p.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X. Pro libovolné $x = (y_1, \ldots, y_p) \in X$ orbita O_x má jediný prvek, je-li $y_1 = \cdots = y_p$, a právě p prvků jinak. Protože orbity tvoří rozklad množiny X, je $|X|$ součtem několika sčítanců, z nichž každý je 1 nebo p. Přitom počet jedniček je dělitelný p a alespoň jedna jednička tam je: máme orbitu $\{(1, \ldots, 1)\}$.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X. Pro libovolné $x = (y_1, \ldots, y_p) \in X$ orbita O_x má jediný prvek, je-li $y_1 = \cdots = y_p$, a právě p prvků jinak. Protože orbity tvoří rozklad množiny X, je $|X|$ součtem několika sčítanců, z nichž každý je 1 nebo p. Přitom počet jedniček je dělitelný p a alespoň jedna jednička tam je: máme orbitu $\{(1, \ldots, 1)\}$. Proto existuje orbita $\{(g, \ldots, g)\}$ pro nějaké $g \in G$, $g \neq 1$.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X. Pro libovolné $x = (y_1, \ldots, y_p) \in X$ orbita O_x má jediný prvek, je-li $y_1 = \cdots = y_p$, a právě p prvků jinak. Protože orbity tvoří rozklad množiny X, je $|X|$ součtem několika sčítanců, z nichž každý je 1 nebo p. Přitom počet jedniček je dělitelný p a alespoň jedna jednička tam je: máme orbitu $\{(1, \ldots, 1)\}$. Proto existuje orbita $\{(g, \ldots, g)\}$ pro nějaké $g \in G$, $g \neq 1$. Pak řád g je roven p a $\langle g \rangle$ je hledaná p-prvková podgrupa grupy G.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). *Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.*

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). *Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.*

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). *Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.*

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.
Rozlišíme dva případy, nejprve předpokládejme, že $p \mid |Z(G)|$.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). *Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.*

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.
Rozlišíme dva případy, nejprve předpokládejme, že $p \mid |Z(G)|$.
Podle Cauchyho věty existuje podgrupa $H \subseteq Z(G)$ řádu p.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.
Rozlišíme dva případy, nejprve předpokládejme, že $p \mid |Z(G)|$.
Podle Cauchyho věty existuje podgrupa $H \subseteq Z(G)$ řádu p. Pak H je normální podgrupa grupy G, faktorgrupa G/H má $\frac{n}{p} < n$ prvků, a tedy pro ni platí indukční předpoklad.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.
Rozlišíme dva případy, nejprve předpokládejme, že $p \mid |Z(G)|$.
Podle Cauchyho věty existuje podgrupa $H \subseteq Z(G)$ řádu p. Pak H je normální podgrupa grupy G, faktorgrupa G/H má $\frac{n}{p} < n$ prvků, a tedy pro ni platí indukční předpoklad. Protože $p^{k-1} \mid \frac{n}{p}$, existuje podgrupa K grupy G/H řádu $|K| = p^{k-1}$.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.
Rozlišíme dva případy, nejprve předpokládejme, že $p \mid |Z(G)|$.
Podle Cauchyho věty existuje podgrupa $H \subseteq Z(G)$ řádu p. Pak H je normální podgrupa grupy G, faktorgrupa G/H má $\frac{n}{p} < n$ prvků, a tedy pro ni platí indukční předpoklad. Protože $p^{k-1} \mid \frac{n}{p}$, existuje podgrupa K grupy G/H řádu $|K| = p^{k-1}$. Její vzor $\pi^{-1}(K)$ v projekci $\pi : G \to G/H$ je podgrupa grupy G řádu p^k.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách. Víme, že $p \mid |G|$ a $p \nmid |Z(G)|$, existuje tedy i tak, že $p \nmid t_i$.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách. Víme, že $p \mid |G|$ a $p \nmid |Z(G)|$, existuje tedy i tak, že $p \nmid t_i$. Protože $t_i = |O_x|$ pro vhodné $x \in G$, je t_i index stabilizátoru S_x, tedy $|G| = |S_x| \cdot t_i$.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách. Víme, že $p \mid |G|$ a $p \nmid |Z(G)|$, existuje tedy i tak, že $p \nmid t_i$. Protože $t_i = |O_x|$ pro vhodné $x \in G$, je t_i index stabilizátoru S_x, tedy $|G| = |S_x| \cdot t_i$. Pak $p^k \mid |S_x|$ a $|S_x| < n$.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách. Víme, že $p \mid |G|$ a $p \nmid |Z(G)|$, existuje tedy i tak, že $p \nmid t_i$. Protože $t_i = |O_x|$ pro vhodné $x \in G$, je t_i index stabilizátoru S_x, tedy $|G| = |S_x| \cdot t_i$. Pak $p^k \mid |S_x|$ a $|S_x| < n$. Podle indukčního předpokladu má grupa S_x podgrupu H řádu p^k.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách. Víme, že $p \mid |G|$ a $p \nmid |Z(G)|$, existuje tedy i tak, že $p \nmid t_i$. Protože $t_i = |O_x|$ pro vhodné $x \in G$, je t_i index stabilizátoru S_x, tedy $|G| = |S_x| \cdot t_i$. Pak $p^k \mid |S_x|$ a $|S_x| < n$. Podle indukčního předpokladu má grupa S_x podgrupu H řádu p^k. Protože H je také podgrupa grupy G, jsme hotovi.

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$.

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$.

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Věta (Sylow). Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme r počet p-Sylowských podgrup grupy G.

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Věta (Sylow). Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme r počet p-Sylowských podgrup grupy G. Pak platí

- $r \equiv 1 \pmod{p}$, $\quad r \mid m$;

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Věta (Sylow). Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme r počet p-Sylowských podgrup grupy G. Pak platí

- $r \equiv 1 \pmod{p}$, $\quad r \mid m$;
- *libovolná podgrupa grupy G, jejíž řád je mocnina p, je podgrupou některé p-Sylowské podgrupy grupy G;*

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Věta (Sylow). Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme r počet p-Sylowských podgrup grupy G. Pak platí

- $r \equiv 1 \pmod{p}$, $\quad r \mid m$;
- *libovolná podgrupa grupy G, jejíž řád je mocnina p, je podgrupou některé p-Sylowské podgrupy grupy G;*
- *jestliže H, K jsou p-Sylowské podgrupy grupy G, pak existuje $g \in G$ tak, že předpis $h \mapsto g \cdot h \cdot g^{-1}$ určuje izomorfismus $H \to K$.* [První vlastnost viz [Věta 10.10, str. 51], zbytek Dummit, Foote: Abstract algebra, str. 139.]