Podgrupy

Definice: Grupa $(H, \bullet)$ je *podgrupa* grupy $(G, \circ)$ jestliže $H \subseteq G$ a $\forall a, b \in H : a \bullet b = a \circ b$. Píšeme $(H, \bullet) \leq (G, \circ)$.
V obou grupách se obvykle používá stejný operační symbol.

Ukázky: Aditivní podgrupy: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$,
(sudá celá čísla, $+) \leq (\mathbb{Z}, +)$.

Multiplikativní podgrupy:

$$\begin{array}{ccccc}
(\mathbb{Q}^+, \cdot) & \leq & (\mathbb{R}^+, \cdot) & & \\
\wedge| & & \wedge| & & \\
(\mathbb{Q} \setminus \{0\}, \cdot) & \leq & (\mathbb{R} \setminus \{0\}, \cdot) & \leq & (\mathbb{C} \setminus \{0\}, \cdot) \\
\vee| & & & & \vee| \\
(\{-1, 1\}, \cdot) & & \leq & & (\{z \in \mathbb{C} : |z| = 1\}, \cdot)
\end{array}$$

(permutační matice, $\cdot) \leq$ (regulární matice, $\cdot$) ... obě z $\mathbb{R}^{n \times n}$.

Grupy permutací: $(\{\mathrm{id}, p_1\}, \circ) \leq \mathsf{S}_3$,
$\mathsf{A}_n =$ (sudé permutace $\mathsf{S}_n, \circ) \leq \mathsf{S}_n$ ... tzv. *alternující* grupa.

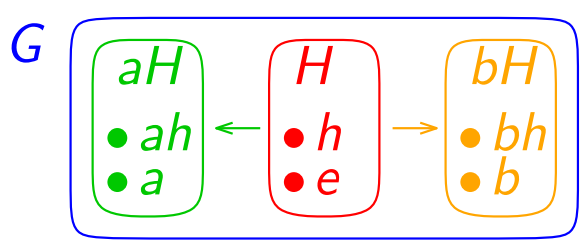
Pozorování: Je-li $(H, \circ)$ podgrupa $(G, \circ)$, pak
$e_H = e_G \in H$ a $\forall a \in H : a_H^{-1} = a_G^{-1} \in H$.

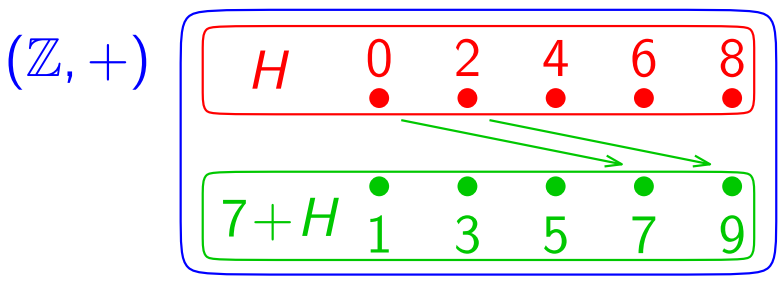
Kosety (rozkladové třídy)

Značení: V této lekci budeme grupovou operaci $\circ$ většinou pro stručnost vynechávat, čili gh znamená $g \circ h$.

Definice: Nechť H je podgrupa G. Pro jakékoli $a \in G$ nazveme množinu $aH = \{ah : h \in H\}$ *levým kosetem* H v G daným a a množinu $Ha = \{ha : h \in H\}$ *pravým kosetem* H v G daným a.

Ukázka:
Pro $G = (\mathbb{Z}, +)$ a podgrupu H sudých čísel dostaneme dva kosety. Jeden koset je samotná H (pro $a = e = 0$), tj. sudá čísla; druhý koset je tvořen lichými čísly (např. pro $a = 7$).
Tento koset $7 + H$ *není podgrupa!*





Kosety (rozkladové třídy)

Značení: V této lekci budeme grupovou operaci $\circ$ většinou pro stručnost vynechávat, čili gh znamená $g \circ h$.

Definice: Nechť H je podgrupa G. Pro jakékoli $a \in G$ nazveme množinu $aH = \{ah : h \in H\}$ *levým kosetem* H v G daným a a množinu $Ha = \{ha : h \in H\}$ *pravým kosetem* H v G daným a.

Ukázka:
Pro $G = (\mathbb{Z}, +)$ a podgrupu H sudých čísel dostaneme dva kosety. Jeden koset je samotná H (pro $a = e = 0$), tj. sudá čísla; druhý koset je tvořen lichými čísly (např. pro $a = 7$). Tento koset $7 + H$ *není podgrupa!*

Pozorování: Je-li G Abelovská, pak se levý a pravý koset dané libovolným $a \in G$ shodují: $aH = Ha$, jako v naší ukázce.

Kosety dané e se vždy shodují $eH = He = H$, dokonce i v neabelovských grupách.

Rozdělení na levé a na pravé kosety se nemusejí shodovat

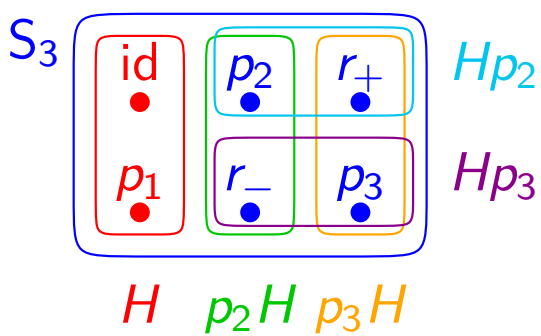
Nechť $H = \{\mathrm{id}, p_1\}$.

H je podgrupa S_3, neboť
$\mathrm{id}\ \mathrm{id} = p_1 p_1 = \mathrm{id}$ a
$p_1\ \mathrm{id} = \mathrm{id}\ p_1 = p_1$.

Levé kosety jsou:
$\mathrm{id}\, H = p_1 H = \{\mathrm{id}, p_1\}$
$p_2 H = r_- H = \{p_2, r_-\}$
$p_3 H = r_+ H = \{p_3, r_+\}$

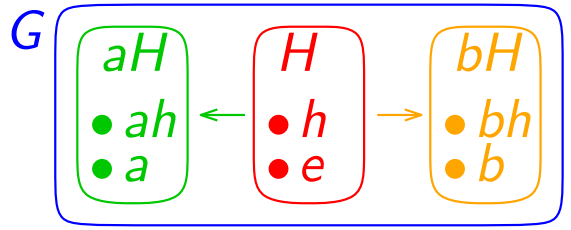
Pravé kosety jsou:
$H\,\mathrm{id} = H p_1 = \{\mathrm{id}, p_1\}$
$H p_2 = H r_+ = \{p_2, r_+\}$
$H p_3 = H r_- = \{p_3, r_-\}$

	id	p_1	p_2	p_3	r_+	r_-
id	id	p_1	p_2	p_3	r_+	r_-
p_1	p_1	id	r_+	r_-	p_2	p_3
p_2	p_2	r_-	id	r_+	p_3	p_1
p_3	p_3	r_+	r_-	id	p_1	p_2
r_+	r_+	p_3	p_1	p_2	r_-	id
r_-	r_-	p_2	p_3	p_1	id	r_+

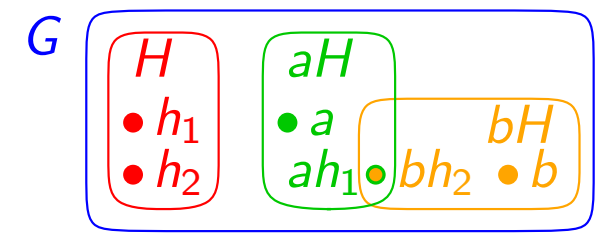


Vlastnosti kosetů

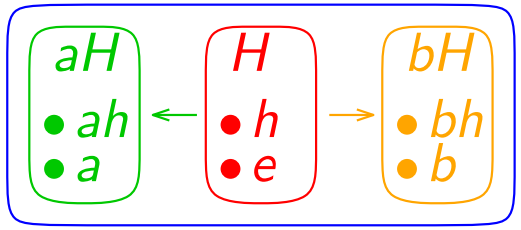
Lemma: Nechť H je podgrupa G, pak
$\forall a, b \in G$: buď $aH = bH$ nebo $aH \cap bH = \emptyset$.



Důkaz:
Pokud $aH \cap bH \neq \emptyset$, zvolme $h_1, h_2 \in H$, aby $ah_1 = bh_2 \in aH \cap bH$.
Pak $a = bh_2 h_1^{-1}$, tedy $\forall h \in H$: $ah = bh_2 h_1^{-1} h \in bH$, čili $aH \subseteq bH$.
Pak $b = ah_1 h_2^{-1}$, tedy $\forall h \in H$: $bh = ah_1 h_2^{-1} h \in aH$, čili $bH \subseteq aH$.



Vlastnosti kosetů



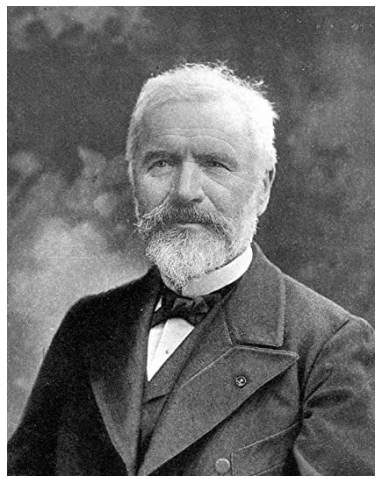
Lemma: Nechť H je podgrupa G, pak
$\forall a, b \in G$: buď $aH = bH$ nebo $aH \cap bH = \emptyset$.

Důsledky: $H = eH = aH$ pro všechna $a \in H$.
Též $a \notin H$ právě když $aH \cap H = \emptyset$. Dů: $ah_1 = h_2 \Leftrightarrow a = h_2 h_1^{-1} \in H$.

Lagrangeova věta: [Camille Jordan, 1861]
Je-li H podgrupou konečné grupy G, pak $|H|$ dělí $|G|$.

Důkaz: Zobrazení $h \to ah$ je bijekce mezi H a aH, čili $|H| = |aH|$.

Giuseppe Lodovico Lagrangia
1736 – 1813



Marie Ennemond Camille Jordan
1838 – 1922

Foto: Wikipedie

Normální podgrupa

Otázka: Kdy se grupová operace přenáší na kosety
jako například sčítání na množinách sudých a lichých celých čísel?

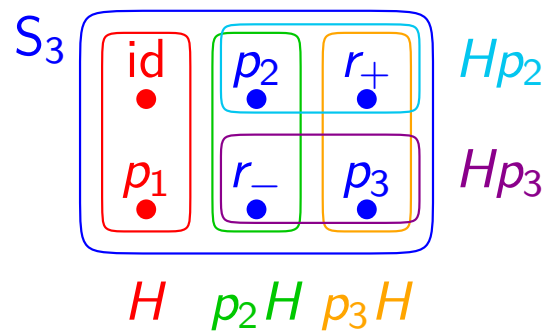
Formálně: Pro které podgrupy H platí, že:
$x \in aH \wedge y \in bH \Longrightarrow xy \in (ab)H$ pro všechna $a, b, x, y \in G$?

Definice: Podgrupa H v G je *normální*, pokud $\forall a \in G : aH = Ha$.

Ukázky: Každá podgrupa Abelovské grupy je normální.

Podgrupa $H = (\{\mathrm{id}, p_1\}, \circ) \leq \mathrm{S}_3$ není normální.

Levé a pravé kosety se neshodují.



Na kosety H, p_2H a p_3H se operace skládání nepřenese:
$r_- \in p_2H$, ale $r_-r_- = r_+ \notin (p_2p_2)H = H$

Normální podgrupa

Otázka: Kdy se grupová operace přenáší na kosety
jako například sčítání na množinách sudých a lichých celých čísel?

Formálně: Pro které podgrupy H platí, že:
$x \in aH \wedge y \in bH \Longrightarrow xy \in (ab)H$ pro všechna $a, b, x, y \in G$?

Definice: Podgrupa H v G je *normální*, pokud $\forall a \in G : aH = Ha$.

Ukázky: Každá podgrupa Abelovské grupy je normální.

Podgrupa $H = (\{\mathrm{id}, p_1\}, \circ) \leq \mathrm{S}_3$ není normální.

Alternující grupa A_n je normální podgrupa S_n:

- Pokud je p sudé, pak $p\mathrm{A}_n = \mathrm{A}_n p = \mathrm{A}_n$ ... kladná znaménka
- Pokud je p liché, pak $p\mathrm{A}_n = \mathrm{A}_n p = \mathrm{S}_n \setminus \mathrm{A}_n$ ... záporná zn.

Konkrétně pro $\mathrm{A}_3 = \{\mathrm{id}, r_+, r_-\}$,
jsou levé a pravé kosety stejné, proto je A_3 normální podgrupa:

$\mathrm{id}\,\mathrm{A}_3 = \mathrm{A}_3\,\mathrm{id} = r_+\mathrm{A}_3 = \mathrm{A}_3 r_+ = r_-\mathrm{A}_3 = \mathrm{A}_3 r_- = \{\mathrm{id}, r_+, r_-\} = \mathrm{A}_3$
$p_1\mathrm{A}_3 = \mathrm{A}_3 p_1 = p_2\mathrm{A}_3 = \mathrm{A}_3 p_2 = p_3\mathrm{A}_3 = \mathrm{A}_3 p_3 = \{p_1, p_2, p_3\}$

Normální podgrupa

Věta: Grupová operace se přenese na kosety H v G
právě když je podgrupa H normální.

Důkaz: $\Leftarrow$: Shodují-li se kosety $bH = Hb$ a jsou-li $x \in aH, y \in bH$, pak $\exists h_1, h_2 \in H : x = ah_1, y = h_2 b$. Odtud už dostaneme $xy = ah_1 h_2 b = ah_3 b = abh_4 \in (ab)H$ pro vhodná $h_3, h_4 \in H$.

$\Rightarrow$: Pro spor předpokládejme, že existuje $a \in G : aH \neq Ha$.

- Je-li $aH \not\subseteq Ha$, pak existuje $h \in H$ takové, že $ah \notin Ha$.
  Pak $aha^{-1} \notin H$, protože $aha^{-1} = h' \in H \Rightarrow ah = h'a \in Ha$.

  Grupová operace se podle předpokladu přenáší na levé kosety, čili $aha^{-1} = aha^{-1}e \in (aa^{-1})H = eH = H$, což je spor.
- Případ $Ha \not\subseteq aH$ plyne podobně otočením pořadí operandů.
  Je-li $Ha \not\subseteq aH$, pak existuje $h \in H$ takové, že $ha \notin aH$.
  Pak $a^{-1}ha \notin H$, protože $a^{-1}ha = h' \in H \Rightarrow ha = ah' \in aH$.
  Grupová operace se podle předpokladu přenáší na levé kosety, čili $a^{-1}ha = a^{-1}hae \in (a^{-1}a)H = eH = H$, což je spor.

Normální podgrupa

Věta: Grupová operace se přenese na kosety H v G
právě když je podgrupa H normální.

Důkaz: $\Leftarrow$: Shodují-li se kosety $bH = Hb$ a jsou-li $x \in aH, y \in bH$,
pak $\exists h_1, h_2 \in H : x = ah_1, y = h_2 b$. Odtud už dostaneme
$xy = ah_1 h_2 b = ah_3 b = abh_4 \in (ab)H$ pro vhodná $h_3, h_4 \in H$.

$\Rightarrow$: Pro spor předpokládejme, že existuje $a \in G : aH \neq Ha$.

- Je-li $aH \not\subseteq Ha$, pak existuje $h \in H$ takové, že $ah \notin Ha$.
  Pak $aha^{-1} \notin H$, protože $aha^{-1} = h' \in H \Rightarrow ah = h'a \in Ha$.

  Grupová operace se podle předpokladu přenáší na levé kosety,
  čili $aha^{-1} = aha^{-1}e \in (aa^{-1})H = eH = H$, což je spor.
- Případ $Ha \not\subseteq aH$ plyne podobně otočením pořadí operandů.
- Ukázali jsme, že se grupová operace nepřenáší na levé kosety.
  Obdobnou záměnou pořadí by šlo ukázat, že se
  tato operace nepřenáší ani na pravé kosety.

Faktorizace normální podgrupou

Definice: Nechť $(H, \circ)$ je normální podgrupa $(G, \circ)$ pak $G/H = (\{aH \colon a \in G\}, \bullet)$, kde $aH \bullet bH = (a \circ b)H$ je *podílová grupa* G podle H. (Nazývána též *faktorgrupa, kvocient*.)

Ukázka: Podílová grupa S_n podle A_n má dva prvky (kosety), jmenovitě podgrupu A_n a její doplněk $\mathsf{S}_n \setminus \mathsf{A}_n$.

Operace $\circ$ se přenese z grupy S_n na podílovou grupu $\mathsf{S}_n/\mathsf{A}_n$:

$\bullet$	A_n	$\mathsf{S}_n \setminus \mathsf{A}_n$
A_n	A_n	$\mathsf{S}_n \setminus \mathsf{A}_n$
$\mathsf{S}_n \setminus \mathsf{A}_n$	$\mathsf{S}_n \setminus \mathsf{A}_n$	A_n

Podílová grupa $\mathsf{S}_n/\mathsf{A}_n$ je izomorfní s $(\{1, -1\}, \cdot)$ (tzn. operace se v obou grupách chovají stejně, jen se operace a prvky grup jinak nazývají), neboť znaménka reprezentují kosety a $\bullet$ odpovídá $\cdot$.

$\cdot$	1	-1
1	1	-1
-1	-1	1

Zbytkové třídy modulo 6 jako podílová grupa $(\mathbb{Z}, +)$

Označme $6\mathbb{Z} = \{6k, k \in \mathbb{Z}\} = \{\dots, -6, 0, 6, 12, \dots\}$

$(6\mathbb{Z}, +)$ je podgrupou $(\mathbb{Z}, +)$, protože $(6|a \ \wedge \ 6|b) \Longrightarrow 6|(a+b)$.
Navíc $6\mathbb{Z}$ je *normální* podgrupa, protože $+$ je komutativní.

Levé kosety $6\mathbb{Z}$ v $\mathbb{Z}$ jsou $T_i = \{x \in \mathbb{Z} : x \equiv i \pmod 6\}$, čili:
$T_0 = 6\mathbb{Z} = \{\dots, -6, 0, 6, 12, \dots\}$, $T_1 = \{\dots, -5, 1, 7, 13, \dots\}$,
$T_2 = \{\dots, -4, 2, 8, 14, \dots\}$, $T_3 = \{\dots, -3, 3, 8, 15, \dots\}$,
$T_4 = \{\dots, -2, 4, 10, 16, \dots\}$, $T_5 = \{\dots, -1, 5, 11, 17, \dots\}$.

Těchto šest kosetů spolu s odvozenou operací $+$ tvoří podílovou grupu $\mathbb{Z}/6\mathbb{Z}$.

Sčítání se přenáší, protože
$a \in T_i, b \in T_j \Longrightarrow$
$\Longrightarrow a + b \in T_i + T_j$.

$+$	T_0	T_1	T_2	T_3	T_4	T_5
T_0	T_0	T_1	T_2	T_3	T_4	T_5
T_1	T_1	T_2	T_3	T_4	T_5	T_0
T_2	T_2	T_3	T_4	T_5	T_0	T_1
T_3	T_3	T_4	T_5	T_0	T_1	T_2
T_4	T_4	T_5	T_0	T_1	T_2	T_3
T_5	T_5	T_0	T_1	T_2	T_3	T_4

Otázky k porozumění tématu přednášky

- Proč každý prvek náleží do nějakého kosetu?
- Proč v podílové grupě platí všechny axiomy z definice grupy?
- Mějme pravidelný šestiúhelník H na vrcholech $A, \ldots, F$. Nechť G je grupa geometrických transformací roviny (rotace, osové a středové souměrnosti), které zachovávají H.
  1. Kolik prvků má G?
  2. Kolik prvků má podgrupa fixující vrchol A?
  3. Kolik levých a kolik pravých kosetů má podgrupa fixující A?
  4. Je to normální podgrupa?
  5. Tvoří rotace o úhel $0, 60, 120, 180, 240$ a 300 stupňů po směru hodinových ručiček normální podgrupu grupy G?