# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

*Poznámka.* Podle definice je levá třída $a \cdot H$ podmnožinou grupy $G$, je to množina všech součinů pevně zvoleného prvku $a$ postupně se všemi prvky $h \in H$.

# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

*Poznámka.* Podle definice je levá třída $a \cdot H$ podmnožinou grupy $G$, je to množina všech součinů pevně zvoleného prvku $a$ postupně se všemi prvky $h \in H$.

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

# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

*Poznámka.* Podle definice je levá třída $a \cdot H$ podmnožinou grupy $G$, je to množina všech součinů pevně zvoleného prvku $a$ postupně se všemi prvky $h \in H$.

*Věta. Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa, $a, b \in G$ libovolné. Následující podmínky jsou ekvivalentní:*

- $a \cdot H = b \cdot H$,

# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

*Poznámka.* Podle definice je levá třída $a \cdot H$ podmnožinou grupy $G$, je to množina všech součinů pevně zvoleného prvku $a$ postupně se všemi prvky $h \in H$.

*Věta.* *Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa, $a, b \in G$ libovolné. Následující podmínky jsou ekvivalentní:*

- $a \cdot H = b \cdot H$,
- $a \in b \cdot H$,

# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

*Poznámka.* Podle definice je levá třída $a \cdot H$ podmnožinou grupy $G$, je to množina všech součinů pevně zvoleného prvku $a$ postupně se všemi prvky $h \in H$.

*Věta. Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa, $a, b \in G$ libovolné. Následující podmínky jsou ekvivalentní:*

- $a \cdot H = b \cdot H$,
- $a \in b \cdot H$,
- $b^{-1} \cdot a \in H$.

# Levé třídy rozkladu grupy podle podgrupy

*Definice.* Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ grupy $G$ podle podgrupy $H$ předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

*Poznámka.* Podle definice je levá třída $a \cdot H$ podmnožinou grupy $G$, je to množina všech součinů pevně zvoleného prvku $a$ postupně se všemi prvky $h \in H$.

*Věta.* *Nechť $(G, \cdot)$ je grupa, $H$ její podgrupa, $a, b \in G$ libovolné. Následující podmínky jsou ekvivalentní:*

- $a \cdot H = b \cdot H$,
- $a \in b \cdot H$,
- $b^{-1} \cdot a \in H$.

[Věta 7.2, str. 37]

*Označení.* Označme $G/H$ množinu všech levých tříd grupy $G$ podle podgrupy $H$, tj. $G/H = \{a \cdot H;\ a \in G\}$.

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

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

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

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

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

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

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

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

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

*Příklad.* Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H$, $(1,3) \circ H = \{(1,3) \circ \mathrm{id}, (1,3) \circ (1,2)\} = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = \{(2,3) \circ \mathrm{id}, (2,3) \circ (1,2)\} = \{(2,3), (1,3,2)\}$. Podle předchozí věty odtud plyne $(1,2) \circ H = \mathrm{id} \circ H = H$, $(1,2,3) \circ H = (1,3) \circ H$, $(1,3,2) \circ H = (2,3) \circ H$. Je tedy $G/H = \big\{\{\mathrm{id}, (1,2)\}, \{(1,3), (1,2,3)\}, \{(2,3), (1,3,2)\}\big\}$.

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

*Příklad.* Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H$, $(1,3) \circ H = \{(1,3) \circ \mathrm{id}, (1,3) \circ (1,2)\} = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = \{(2,3) \circ \mathrm{id}, (2,3) \circ (1,2)\} = \{(2,3), (1,3,2)\}$. Podle předchozí věty odtud plyne $(1,2) \circ H = \mathrm{id} \circ H = H$, $(1,2,3) \circ H = (1,3) \circ H$, $(1,3,2) \circ H = (2,3) \circ H$. Je tedy $G/H = \big\{\{\mathrm{id}, (1,2)\}, \{(1,3), (1,2,3)\}, \{(2,3), (1,3,2)\}\big\}$.

*Poznámka.* Připomeňme, že rozkladem na množině $M$ rozumíme systém neprázdných podmnožin množiny $M$, které jsou po dvou disjunktní a jejichž sjednocení je rovno celé množině $M$.

# Rozklad grupy podle podgrupy

*Příklad.* Pro libovolné $m \in \mathbb{N}$ tvoří množina $H$ všech celých čísel dělitelných číslem $m$ podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

*Příklad.* Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H$, $(1,3) \circ H = \{(1,3) \circ \mathrm{id}, (1,3) \circ (1,2)\} = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = \{(2,3) \circ \mathrm{id}, (2,3) \circ (1,2)\} = \{(2,3), (1,3,2)\}$. Podle předchozí věty odtud plyne $(1,2) \circ H = \mathrm{id} \circ H = H$, $(1,2,3) \circ H = (1,3) \circ H$, $(1,3,2) \circ H = (2,3) \circ H$. Je tedy $G/H = \big\{\{\mathrm{id}, (1,2)\}, \{(1,3), (1,2,3)\}, \{(2,3), (1,3,2)\}\big\}$.

*Poznámka.* Připomeňme, že rozkladem na množině $M$ rozumíme systém neprázdných podmnožin množiny $M$, které jsou po dvou disjunktní a jejichž sjednocení je rovno celé množině $M$.

*Věta.* *Množina $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ tvoří rozklad na množině $G$.* [Věta 7.2, str. 37]

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**.

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

*Věta.* *Nechť $(G, \cdot)$ je konečná grupa, $H$ její podgrupa. Pak platí* $|G| = |G/H| \cdot |H|$. [Věta 7.6, str. 38]

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

*Věta.* *Nechť $(G, \cdot)$ je konečná grupa, $H$ její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* [Věta 7.6, str. 38]

*Důsledek (Lagrangeova věta).* *Řád libovolné podgrupy konečné grupy $G$ je dělitelem řádu grupy $G$.*

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

*Věta.* *Nechť $(G, \cdot)$ je konečná grupa, $H$ její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* [Věta 7.6, str. 38]

*Důsledek (Lagrangeova věta).* *Řád libovolné podgrupy konečné grupy $G$ je dělitelem řádu grupy $G$.*

*Důsledek.* *Řád libovolného prvku konečné grupy $G$ je dělitelem řádu grupy $G$.* [Řád libovolného $a \in G$ je roven řádu podgrupy $\langle a \rangle$, kterou generuje.]

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

*Věta.* *Nechť $(G, \cdot)$ je konečná grupa, $H$ její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* [Věta 7.6, str. 38]

*Důsledek (Lagrangeova věta).* *Řád libovolné podgrupy konečné grupy $G$ je dělitelem řádu grupy $G$.*

*Důsledek.* *Řád libovolného prvku konečné grupy $G$ je dělitelem řádu grupy $G$.* [Řád libovolného $a \in G$ je roven řádu podgrupy $\langle a \rangle$, kterou generuje.]

*Důsledek.* *Libovolná grupa prvočíselného řádu je cyklická.* [Důsledek 7.9, str. 39]

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

*Věta.* *Nechť $(G, \cdot)$ je konečná grupa, $H$ její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* [Věta 7.6, str. 38]

*Důsledek (Lagrangeova věta).* *Řád libovolné podgrupy konečné grupy $G$ je dělitelem řádu grupy $G$.*

*Důsledek.* *Řád libovolného prvku konečné grupy $G$ je dělitelem řádu grupy $G$.* [Řád libovolného $a \in G$ je roven řádu podgrupy $\langle a \rangle$, kterou generuje.]

*Důsledek.* *Libovolná grupa prvočíselného řádu je cyklická.* [Důsledek 7.9, str. 39]

*Důsledek.* *Nechť $G$ je konečná grupa řádu $n = |G|$. Pak pro libovolný prvek $a \in G$ platí $a^n = 1$.*

# Lagrangeova věta a její důsledky

*Definice.* Množinu $G/H$ všech levých tříd grupy $G$ podle podgrupy $H$ nazýváme **rozklad grupy $G$ podle podgrupy $H$**. Je-li množina $G/H$ konečná, pak počet $|G/H|$ všech levých tříd grupy $G$ podle podgrupy $H$ se nazývá **index** podgrupy $H$ v grupě $G$.

*Věta.* *Nechť $(G, \cdot)$ je konečná grupa, $H$ její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* [Věta 7.6, str. 38]

*Důsledek (Lagrangeova věta).* *Řád libovolné podgrupy konečné grupy $G$ je dělitelem řádu grupy $G$.*

*Důsledek.* *Řád libovolného prvku konečné grupy $G$ je dělitelem řádu grupy $G$.* [Řád libovolného $a \in G$ je roven řádu podgrupy $\langle a \rangle$, kterou generuje.]

*Důsledek.* *Libovolná grupa prvočíselného řádu je cyklická.* [Důsledek 7.9, str. 39]

*Důsledek.* *Nechť $G$ je konečná grupa řádu $n = |G|$. Pak pro libovolný prvek $a \in G$ platí $a^n = 1$. Jinými slovy: exponent konečné grupy $G$ je dělitelem řádu grupy $G$.*

# Eulerova věta a malá Fermatova věta

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

# Eulerova věta a malá Fermatova věta

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

*Věta (Eulerova).* *Nechť* $m \in \mathbb{N}$, $a \in \mathbb{Z}$ *jsou libovolná nesoudělná čísla. Pak platí* $a^{\varphi(m)} \equiv 1 \pmod{m}$. [Věta 7.11, str. 39]

# Eulerova věta a malá Fermatova věta

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

*Věta (Eulerova).* *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná nesoudělná čísla. Pak platí* $a^{\varphi(m)} \equiv 1 \pmod{m}$. [Věta 7.11, str. 39]

*Příklad.* V situaci, kdy v Eulerově větě za přirozené číslo $m$ dosadíme prvočíslo $p$, vzhledem k tomu, že $\varphi(p) = p - 1$, dostaneme, že pro každé celé číslo $a$, které je nesoudělné s $p$, platí $a^{p-1} \equiv 1 \pmod{p}$.

# Eulerova věta a malá Fermatova věta

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

*Věta (Eulerova).* *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná nesoudělná čísla. Pak platí* $a^{\varphi(m)} \equiv 1 \pmod{m}$. [Věta 7.11, str. 39]

*Příklad.* V situaci, kdy v Eulerově větě za přirozené číslo $m$ dosadíme prvočíslo $p$, vzhledem k tomu, že $\varphi(p) = p - 1$, dostaneme, že pro každé celé číslo $a$, které je nesoudělné s $p$, platí $a^{p-1} \equiv 1 \pmod{p}$.

*Věta (malá Fermatova).* *Nechť $p$ je prvočíslo, $a \in \mathbb{Z}$. Pak platí* $a^p \equiv a \pmod{p}$. [Pro $p \mid a$ zřejmé. Pro $p \nmid a$, plyne z kongruence získané v předchozím příkladu.]

# Eulerova věta a malá Fermatova věta

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

*Věta (Eulerova).* *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná nesoudělná čísla. Pak platí* $a^{\varphi(m)} \equiv 1 \pmod{m}$. [Věta 7.11, str. 39]

*Příklad.* V situaci, kdy v Eulerově větě za přirozené číslo $m$ dosadíme prvočíslo $p$, vzhledem k tomu, že $\varphi(p) = p - 1$, dostaneme, že pro každé celé číslo $a$, které je nesoudělné s $p$, platí $a^{p-1} \equiv 1 \pmod{p}$.

*Věta (malá Fermatova).* *Nechť $p$ je prvočíslo, $a \in \mathbb{Z}$. Pak platí* $a^p \equiv a \pmod{p}$. [Pro $p \mid a$ zřejmé. Pro $p \nmid a$, plyne z kongruence získané v předchozím příkladu.]

*Příklad.* Pro ukázku, jak můžeme použít uvedené věty, nalezněme zbytek po dělení čísla $3^{50} + 7^{65}$ číslem 17. Protože čísla 3 i 7 jsou nesoudělná s číslem 17, platí $3^{16} \equiv 7^{16} \equiv 1 \pmod{17}$, tedy $3^{50} + 7^{65} = 3^{3 \cdot 16 + 2} + 7^{4 \cdot 16 + 1} \equiv 3^2 + 7 = 16 \pmod{17}$, hledaný zbytek po dělení je 16.

# 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 $\ker f$ je podgrupa grupy $G$ a 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 $\ker f$ je podgrupa grupy $G$ a 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 $\ker f$ je podgrupa grupy $G$ a 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 $\ker f$ je podgrupa grupy $G$ a 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
$f(a) = f(a) \cdot 1 = f(a) \cdot f(a^{-1} \cdot b) = f(a \cdot a^{-1} \cdot b) = f(b)$.

# 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 $\ker f$ je podgrupa grupy $G$ a 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
$f(a) = f(a) \cdot 1 = f(a) \cdot f(a^{-1} \cdot b) = f(a \cdot a^{-1} \cdot b) = f(b)$.

*Důsledek.* *Nechť* $f : G \to K$ *je homomorfismus grup,* $f(G) = \{f(a);\ a \in G\}$ *jeho obraz. Je-li* $f(G)$ *konečná množina, pak pro index podgrupy* $\ker f$ *v grupě* $G$ *platí* $|G/\ker f| = |f(G)|$.

# 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 $\ker f$ je podgrupa grupy $G$ a 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
$f(a) = f(a) \cdot 1 = f(a) \cdot f(a^{-1} \cdot b) = f(a \cdot a^{-1} \cdot b) = f(b)$.

*Důsledek.* *Nechť* $f : G \to K$ *je homomorfismus grup,* $f(G) = \{f(a);\ a \in G\}$ *jeho obraz. Je-li* $f(G)$ *konečná množina, pak pro index podgrupy* $\ker f$ *v grupě* $G$ *platí* $|G/\ker f| = |f(G)|$. *Je-li navíc* $G$ *konečná grupa, pak* $|f(G)| \cdot |\ker f| = |G|$.

# 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 $\ker f$ je podgrupa grupy $G$ a 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
$f(a) = f(a) \cdot 1 = f(a) \cdot f(a^{-1} \cdot b) = f(a \cdot a^{-1} \cdot b) = f(b)$.

*Důsledek.* *Nechť* $f : G \to K$ *je homomorfismus grup,* $f(G) = \{f(a);\ a \in G\}$ *jeho obraz. Je-li* $f(G)$ *konečná množina, pak pro index podgrupy* $\ker f$ *v grupě* $G$ *platí* $|G/\ker f| = |f(G)|$. *Je-li navíc* $G$ *konečná grupa, pak* $|f(G)| \cdot |\ker f| = |G|$.

[Podle předchozí věty předpis $F(a \cdot (\ker f)) = f(a)$ korektně definuje bijekci $F : G/\ker f \to f(G)$.]