Základní vlastnosti pologrup, mocnina v pologrupě

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.* [Věta 4.1, str. 23]

Základní vlastnosti pologrup, mocnina v pologrupě

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.* [Věta 4.1, str. 23]

Věta. *Nechť $(G, \cdot)$ je komutativní pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ nezáleží na jejich pořadí.* [Věta 4.2, str. 24]

Základní vlastnosti pologrup, mocnina v pologrupě

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.* [Věta 4.1, str. 23]

Věta. *Nechť $(G, \cdot)$ je komutativní pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ nezáleží na jejich pořadí.* [Věta 4.2, str. 24]

Definice. Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $n \in \mathbb{N}$. **Mocninu** a^n prvku a v pologrupě G definujeme jako součin n exemplářů prvku a:

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$$

(podle výše uvedené věty není nutné specifikovat uzávorkování).

Základní vlastnosti pologrup, mocnina v pologrupě

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.* [Věta 4.1, str. 23]

Věta. *Nechť $(G, \cdot)$ je komutativní pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ nezáleží na jejich pořadí.* [Věta 4.2, str. 24]

Definice. Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $n \in \mathbb{N}$. **Mocninu** a^n prvku a v pologrupě G definujeme jako součin n exemplářů prvku a:

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$$

(podle výše uvedené věty není nutné specifikovat uzávorkování).

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $m, n \in \mathbb{N}$. Pak platí* $a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{m \cdot n}$. [Věta 4.4, str. 24]

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť* $(G, \cdot)$ *je grupa,* $a, b, c \in G$. *Pak platí*

$$a \cdot b = a \cdot c \qquad \Longrightarrow \qquad b = c,$$

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť* $(G, \cdot)$ *je grupa,* $a, b, c \in G$. *Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$

$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c.$$

[Věta 4.17, str. 27]

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť $(G, \cdot)$ je grupa, $a, b, c \in G$. Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$
$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c. \qquad \text{[Věta 4.17, str. 27]}$$

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme nejen pro $n \in \mathbb{N}$, ale i pro nekladný celočíselný exponent n: a^0 definujeme jako neutrální prvek grupy G, tj. $a^0 = 1$,

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť $(G, \cdot)$ je grupa, $a, b, c \in G$. Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$
$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c. \qquad \text{[Věta 4.17, str. 27]}$$

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme nejen pro $n \in \mathbb{N}$, ale i pro nekladný celočíselný exponent n: a^0 definujeme jako neutrální prvek grupy G, tj. $a^0 = 1$, a pro libovolné $n \in \mathbb{N}$ definujeme a^{-n} jako inverzní prvek k prvku a^n, tj. $a^{-n} = (a^n)^{-1}$.

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť $(G, \cdot)$ je grupa, $a, b, c \in G$. Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$
$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c. \qquad \text{[Věta 4.17, str. 27]}$$

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme nejen pro $n \in \mathbb{N}$, ale i pro nekladný celočíselný exponent n: a^0 definujeme jako neutrální prvek grupy G, tj. $a^0 = 1$, a pro libovolné $n \in \mathbb{N}$ definujeme a^{-n} jako inverzní prvek k prvku a^n, tj. $a^{-n} = (a^n)^{-1}$.

Poznámka. Uvědomte si, že oba významy symbolu a^{-1} (inverzní prvek k a, resp. prvek a umocněný na $-1 \in \mathbb{Z}$) znamenají totéž.

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť $(G, \cdot)$ je grupa, $a, b, c \in G$. Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$
$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c. \qquad \text{[Věta 4.17, str. 27]}$$

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme nejen pro $n \in \mathbb{N}$, ale i pro nekladný celočíselný exponent n: a^0 definujeme jako neutrální prvek grupy G, tj. $a^0 = 1$, a pro libovolné $n \in \mathbb{N}$ definujeme a^{-n} jako inverzní prvek k prvku a^n, tj. $a^{-n} = (a^n)^{-1}$.

Poznámka. Uvědomte si, že oba významy symbolu a^{-1} (inverzní prvek k a, resp. prvek a umocněný na $-1 \in \mathbb{Z}$) znamenají totéž.

Věta. *Nechť $(G, \cdot)$ je grupa, $a \in G$, $m, n \in \mathbb{Z}$. Pak platí*
$a^m \cdot a^n = a^{m+n}$, $\quad (a^m)^n = a^{m \cdot n}$. [Věta 4.9, str. 25]

Základní vlastnosti grup, mocnina v grupě

Věta (zákony o krácení). *Nechť $(G, \cdot)$ je grupa, $a, b, c \in G$. Pak platí*

$$a \cdot b = a \cdot c \quad \Longrightarrow \quad b = c,$$
$$b \cdot a = c \cdot a \quad \Longrightarrow \quad b = c.$$

[Věta 4.17, str. 27]

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme nejen pro $n \in \mathbb{N}$, ale i pro nekladný celočíselný exponent n: a^0 definujeme jako neutrální prvek grupy G, tj. $a^0 = 1$, a pro libovolné $n \in \mathbb{N}$ definujeme a^{-n} jako inverzní prvek k prvku a^n, tj. $a^{-n} = (a^n)^{-1}$.

Poznámka. Uvědomte si, že oba významy symbolu a^{-1} (inverzní prvek k a, resp. prvek a umocněný na $-1 \in \mathbb{Z}$) znamenají totéž.

Věta. *Nechť $(G, \cdot)$ je grupa, $a \in G$, $m, n \in \mathbb{Z}$. Pak platí*
$a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{m \cdot n}$. [Věta 4.9, str. 25]

Věta. *Nechť $(G, \cdot)$ je komutativní grupa, $a, b \in G$, $m \in \mathbb{Z}$. Pak platí $(a \cdot b)^m = a^m \cdot b^m$.* [Věta 4.10, str. 26]

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G.

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ [Věta 4.13 (3), str. 26]

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ [Věta 4.13 (3), str. 26]

Důsledek. *Nechť řád prvku a v grupě G je $n \in \mathbb{N}$. Nechť r je zbytek po dělení čísla $k \in \mathbb{Z}$ číslem n, pak $a^k = a^r$.*

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ [Věta 4.13 (3), str. 26]

Důsledek. *Nechť řád prvku a v grupě G je $n \in \mathbb{N}$. Nechť r je zbytek po dělení čísla $k \in \mathbb{Z}$ číslem n, pak $a^k = a^r$. Prvky $a^0 = 1$, $a^1 = a$, $a^2, \ldots, a^{n-1}$ jsou po dvou různé.*

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ [Věta 4.13 (3), str. 26]

Důsledek. *Nechť řád prvku a v grupě G je $n \in \mathbb{N}$. Nechť r je zbytek po dělení čísla $k \in \mathbb{Z}$ číslem n, pak $a^k = a^r$. Prvky $a^0 = 1$, $a^1 = a$, a^2, $\ldots$, a^{n-1} jsou po dvou různé.*

Důsledek. *Řád prvku a v grupě G tedy udává, kolik existuje různých mocnin prvku a.*

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ [Věta 4.13 (3), str. 26]

Důsledek. *Nechť řád prvku a v grupě G je $n \in \mathbb{N}$. Nechť r je zbytek po dělení čísla $k \in \mathbb{Z}$ číslem n, pak $a^k = a^r$. Prvky $a^0 = 1$, $a^1 = a$, a^2, $\ldots$, a^{n-1} jsou po dvou různé.*

Důsledek. *Řád prvku a v grupě G tedy udává, kolik existuje různých mocnin prvku a. V konečné grupě má každý prvek konečný řád.*

Důsledky věty

Věta. Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$.

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$. Nechť pro $t \in \mathbb{N}$ platí $(a \cdot b)^t = 1$.

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$. Nechť pro $t \in \mathbb{N}$ platí $(a \cdot b)^t = 1$. Pak $1 = (a \cdot b)^{tm} = (a^m)^t \cdot b^{tm} = b^{tm}$,

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$. Nechť pro $t \in \mathbb{N}$ platí $(a \cdot b)^t = 1$. Pak $1 = (a \cdot b)^{tm} = (a^m)^t \cdot b^{tm} = b^{tm}$, a tedy $n \mid tm$, což vzhledem k $(m, n) = 1$ dává $n \mid t$.

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$. Nechť pro $t \in \mathbb{N}$ platí $(a \cdot b)^t = 1$. Pak $1 = (a \cdot b)^{tm} = (a^m)^t \cdot b^{tm} = b^{tm}$, a tedy $n \mid tm$, což vzhledem k $(m, n) = 1$ dává $n \mid t$. Analogicky $m \mid t$.

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$. Nechť pro $t \in \mathbb{N}$ platí $(a \cdot b)^t = 1$. Pak $1 = (a \cdot b)^{tm} = (a^m)^t \cdot b^{tm} = b^{tm}$, a tedy $n \mid tm$, což vzhledem k $(m, n) = 1$ dává $n \mid t$. Analogicky $m \mid t$. Celkem z $(m, n) = 1$ dostaneme $mn \mid t$.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6,

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, exponent grupy $\mathbb{S}_4$ je 12,

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, exponent grupy $\mathbb{S}_4$ je 12, exponent grupy $\mathbb{D}_4$ je roven 4.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, exponent grupy $\mathbb{S}_4$ je 12, exponent grupy $\mathbb{D}_4$ je roven 4.

Příklad. Pokud v grupě G existuje prvek řádu ∞, pak je exponent této grupy ∞.

Exponent grupy

Definice. Nechť $(G, \cdot)$ je grupa. Existuje-li přirozené číslo e tak, že pro každé $a \in G$ platí $a^e = 1$, pak nejmenší přirozené číslo e s touto vlastností se nazývá **exponent** grupy G. Jestliže žádné přirozené číslo e s touto vlastností neexistuje, říkáme, že exponent grupy G je ∞.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, exponent grupy $\mathbb{S}_4$ je 12, exponent grupy $\mathbb{D}_4$ je roven 4.

Příklad. Pokud v grupě G existuje prvek řádu ∞, pak je exponent této grupy ∞. Opačná implikace však neplatí, například množina $\{\alpha \in \mathbb{C};\ \exists n \in \mathbb{N} : \alpha^n = 1\}$ spolu s operací násobení tvoří nekonečnou komutativní grupu, ve které má každý prvek konečný řád, avšak exponent této grupy je ∞.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$.
Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Protože $p^r \mid k \in S$, existuje v G prvek řádu k, jeho $\frac{k}{p^r}$-tá mocnina má řád p^r, proto $p^r \in S$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Protože $p^r \mid k \in S$, existuje v G prvek řádu k, jeho $\frac{k}{p^r}$-tá mocnina má řád p^r, proto $p^r \in S$. Podobně z $n \mid m \in S$ plyne $n \in S$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Protože $p^r \mid k \in S$, existuje v G prvek řádu k, jeho $\frac{k}{p^r}$-tá mocnina má řád p^r, proto $p^r \in S$. Podobně z $n \mid m \in S$ plyne $n \in S$.
V komutativní grupě G existují prvky řádů p^r a n, přitom $(p^r, n) = 1$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Protože $p^r \mid k \in S$, existuje v G prvek řádu k, jeho $\frac{k}{p^r}$-tá mocnina má řád p^r, proto $p^r \in S$. Podobně z $n \mid m \in S$ plyne $n \in S$.
V komutativní grupě G existují prvky řádů p^r a n, přitom $(p^r, n) = 1$. Proto podle předchozí věty v G existuje prvek řádu $p^r \cdot n \in S$, ovšem $p^r \cdot n > m$, což je spor s $m = \max S$.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Protože $p^r \mid k \in S$, existuje v G prvek řádu k, jeho $\frac{k}{p^r}$-tá mocnina má řád p^r, proto $p^r \in S$. Podobně z $n \mid m \in S$ plyne $n \in S$.
V komutativní grupě G existují prvky řádů p^r a n, přitom $(p^r, n) = 1$. Proto podle předchozí věty v G existuje prvek řádu $p^r \cdot n \in S$, ovšem $p^r \cdot n > m$, což je spor s $m = \max S$.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, přitom v $\mathbb{S}_3$ prvek řádu 6 není.

Exponent konečné komutativní grupy

Věta. *Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.*

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Dokažme sporem, že m je dělitelný každým prvkem množiny S, pak bude nejmenším společným násobkem všech prvků této množiny, a tedy exponentem grupy G.
Předpokládejme tedy, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Protože $p^r \mid k \in S$, existuje v G prvek řádu k, jeho $\frac{k}{p^r}$-tá mocnina má řád p^r, proto $p^r \in S$. Podobně z $n \mid m \in S$ plyne $n \in S$.
V komutativní grupě G existují prvky řádů p^r a n, přitom $(p^r, n) = 1$. Proto podle předchozí věty v G existuje prvek řádu $p^r \cdot n \in S$, ovšem $p^r \cdot n > m$, což je spor s $m = \max S$.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, přitom v $\mathbb{S}_3$ prvek řádu 6 není. Předpoklad, že G je komutativní, je v předchozí větě nutný.

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Věta. *Nechť H je podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H, přičemž H je grupa vzhledem k této operaci.*

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Věta. *Nechť H je podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H, přičemž H je grupa vzhledem k této operaci. Je-li grupa G komutativní, pak je i grupa H komutativní.* [Věta 5.3, str. 29]

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Věta. *Nechť H je podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H, přičemž H je grupa vzhledem k této operaci. Je-li grupa G komutativní, pak je i grupa H komutativní.* [Věta 5.3, str. 29]

Označení. Zmiňovanou operaci na podgrupě budeme označovat stejným symbolem jako původní operaci na celé grupě, přestože tyto operace nejsou stejné.

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Věta. *Nechť H je podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H, přičemž H je grupa vzhledem k této operaci. Je-li grupa G komutativní, pak je i grupa H komutativní.* [Věta 5.3, str. 29]

Označení. Zmiňovanou operaci na podgrupě budeme označovat stejným symbolem jako původní operaci na celé grupě, přestože tyto operace nejsou stejné.

Věta. *Jestliže H je podgrupa grupy G a K je podgrupa grupy H, pak je K také podgrupou grupy G.* [To je zřejmé.]

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností. Podgrupu $\langle M \rangle$ nazýváme **podgrupa generovaná množinou** M, množinu M nazýváme **množina generátorů podgrupy** $\langle M \rangle$.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností. Podgrupu $\langle M \rangle$ nazýváme **podgrupa generovaná množinou** M, množinu M nazýváme **množina generátorů podgrupy** $\langle M \rangle$.

Označení. Je-li $M = \{a_1, \ldots, a_n\}$, lze psát stručně $\langle a_1, \ldots, a_n \rangle$ místo $\langle M \rangle$.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností. Podgrupu $\langle M \rangle$ nazýváme **podgrupa generovaná množinou** M, množinu M nazýváme **množina generátorů podgrupy** $\langle M \rangle$.

Označení. Je-li $M = \{a_1, \ldots, a_n\}$, lze psát stručně $\langle a_1, \ldots, a_n \rangle$ místo $\langle M \rangle$.

Poznámka. Zřejmě $\langle G \rangle = G$, $\langle \emptyset \rangle = \{1\}$.

Podgrupa grupy generovaná podmnožinou grupy

Označení. Pro libovolné $n \in \mathbb{N}$ označme $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n;\ p(\sigma) = 1\}$ množinu všech sudých permutací v $\mathbb{S}_n$.

Příklad. $\mathbb{A}_n$ je podgrupa grupy $(\mathbb{S}_n, \circ)$ pro každé $n \in \mathbb{N}$.

Věta. Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G. [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností. Podgrupu $\langle M \rangle$ nazýváme **podgrupa generovaná množinou** M, množinu M nazýváme **množina generátorů podgrupy** $\langle M \rangle$.

Označení. Je-li $M = \{a_1, \ldots, a_n\}$, lze psát stručně $\langle a_1, \ldots, a_n \rangle$ místo $\langle M \rangle$.

Poznámka. Zřejmě $\langle G \rangle = G$, $\langle \emptyset \rangle = \{1\}$. Pro každou $M \subseteq G$ platí

$$\langle M \rangle = \langle M \cup \{a^{-1};\ a \in M\} \rangle.$$

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$.*

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.
Pro libovolné $c = a_1 \cdot \ldots \cdot a_n \in X$ je $c^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in X$.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.
Pro libovolné $c = a_1 \cdot \ldots \cdot a_n \in X$ je $c^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in X$.
Protože součin n prvků z M vynásobený součinem m prvků z M je součinem $n + m$ prvků z M, je X uzavřeno na operaci $\cdot$.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.
Pro libovolné $c = a_1 \cdot \ldots \cdot a_n \in X$ je $c^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in X$.
Protože součin n prvků z M vynásobený součinem m prvků z M je součinem $n + m$ prvků z M, je X uzavřeno na operaci $\cdot$.
Je tedy X podgrupa grupy G.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.
Pro libovolné $c = a_1 \cdot \ldots \cdot a_n \in X$ je $c^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in X$.
Protože součin n prvků z M vynásobený součinem m prvků z M je součinem $n + m$ prvků z M, je X uzavřeno na operaci $\cdot$.
Je tedy X podgrupa grupy G.

Naopak libovolná podgrupa Y grupy G obsahující M obsahuje také libovolný součin prvků z M, proto $X \subseteq Y$.

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.
Pro libovolné $c = a_1 \cdot \ldots \cdot a_n \in X$ je $c^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in X$.
Protože součin n prvků z M vynásobený součinem m prvků z M je součinem $n + m$ prvků z M, je X uzavřeno na operaci $\cdot$.
Je tedy X podgrupa grupy G.

Naopak libovolná podgrupa Y grupy G obsahující M obsahuje také libovolný součin prvků z M, proto $X \subseteq Y$.

Je tedy X nejmenší podgrupa grupy G obsahující M, tj. $X = \langle M \rangle$.

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$.*

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Definice. Řádem konečné grupy $(G, \cdot)$ rozumíme počet prvků této grupy, značíme $|G|$.

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$.* [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Definice. Řádem konečné grupy $(G, \cdot)$ rozumíme počet prvků této grupy, značíme $|G|$.

Důsledek. *Řád konečné cyklické grupy je roven řádu jejího generátoru.*

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$.* [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Definice. Řádem konečné grupy $(G, \cdot)$ rozumíme počet prvků této grupy, značíme $|G|$.

Důsledek. *Řád konečné cyklické grupy je roven řádu jejího generátoru. Konečná grupa řádu n je cyklická, právě když obsahuje prvek řádu n.*

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Definice. Řádem konečné grupy $(G, \cdot)$ rozumíme počet prvků této grupy, značíme $|G|$.

Důsledek. *Řád konečné cyklické grupy je roven řádu jejího generátoru. Konečná grupa řádu n je cyklická, právě když obsahuje prvek řádu n.*

[Obsahuje-li konečná grupa řádu n prvek a řádu n, má podgrupa $\langle a \rangle$ stejný počet prvků jako G, tedy $\langle a \rangle = G$.]

Důsledek. *Nechť H, K jsou podgrupy komutativní grupy $(G, \cdot)$. Pak platí $\langle H \cup K \rangle = \{h \cdot k;\ h \in H,\ k \in K\}$.* [Důsledek 5.9, str. 30]