Věta 1: Každá cyklická grupa je komutativní.

Důkaz: Uvažujme cyklickou grupu $(G,\cdot)$, kde $G=\{a^k \mid k\in\mathbb{Z}\}$.

Potom:

$$\forall k_1,k_2\in\mathbb{Z}:\ a^{k_1}\cdot a^{k_2}=a^{k_1+k_2}=a^{k_2+k_1}=a^{k_2}\cdot a^{k_1}$$

$\square$

Věta 2: Každá podgrupa cyklické grupy je cyklická.
Navíc, každá podgrupa $(H,\cdot)$, kde $H\neq\{e\}$, grupy $(G,\cdot)$, kde $G=\{a^k \mid k\in\mathbb{Z}\}$ je generována prvkem a^{s_0}, kde $s_0=\min\{s\in\mathbb{N} \mid a^s\in H\}$.

Důkaz: Uvažujme cyklickou grupu $(G,\cdot)$, kde $G=\{a^k \mid k\in\mathbb{Z}\}$

α) $H=\{e\}$ $\Rightarrow$ $(H,\cdot)$ je cyklická grupa, neboť $H=\{e^k \mid k\in\mathbb{Z}\}$.

β) $H\neq\{e\}$ $\Rightarrow$ $\exists\, a^m\in H,\ m\neq 0$. Protože $(H,\cdot)$ je grupa, $a^{-m}\in H$.
Proto můžeme tvrdit, že $\exists\, a^s\in H$, kde $s>0$.
Uvažujme prvek a^{s_0}, kde

$$\boxed{s_0=\min\{s\in\mathbb{N} \mid a^s\in H\}}.$$

Dokážeme, že $H=\langle a^{s_0}\rangle$.

Díky uzavřenosti operace $\cdot$ na H (uvažme, že $a^{s_0}\in H$):

$$\boxed{\langle a^{s_0}\rangle=\{(a^{s_0})^k \mid k\in\mathbb{Z}\}\subseteq H} \qquad (1)$$

Dokážeme platnost opačné inkluze. Uvažujme prvek $a^d \in H$.

$$\boxed{a^d = a^{p\cdot k_0 + r}, \quad \text{kde } p \in \mathbb{Z}, \quad 0 \le r < k_0} \qquad (2)$$

Prvek $a^{k_0} \in H$, $(H,\cdot)$ je grupa $\Rightarrow a^{-k_0} \in H \Rightarrow (a^{-k_0})^p \in H \Rightarrow a^d \cdot a^{-k_0 p} \in H$.
Proto

$$a^d \cdot a^{-k_0 p} = a^{p k_0 + r} \cdot a^{-k_0 p} = a^r \in H$$

Protože $k_0 = \min\{k \in \mathbb{N} \mid a^k \in H\}$ a $0 \le r < k_0$ musí být $r = 0$.
Dosazením do (2) obdržíme:

$$a^d = a^{p\cdot k_0} = (a^{k_0})^p \in \langle a^{k_0} \rangle$$

A proto, že a^d byl libovolný prvek z H, dostáváme:

$$\boxed{H \subseteq \langle a^{k_0} \rangle} \qquad (3)$$

Z (1) a (3) pak plyne $H = \langle a^{k_0} \rangle$. □

Věta 3: V cyklické grupě nekonečného řádu neexistují prvky konečného řádu.

Důkaz: Předpokládejme, že $G = \{a^k \mid k \in \mathbb{Z}\}$, $(G,\cdot)$ je grupa $|a| = \infty$ a prvek $c \in G$ je konečného řádu n.

$c \in G \Rightarrow \exists\, m \in \mathbb{Z}: c = a^m$

c je řádu $n \Rightarrow c^n = (a^m)^n = a^{m\cdot n} = e \Rightarrow |a| \le m\cdot n \in \mathbb{N}$

Spor!

□

Věta 4: Nechť $(G, \cdot)$ je grupa, $a \in G$, $|a| = m$. Potom platí:

$$a^k = e \Leftrightarrow m \mid k$$

Důkaz: $\boxed{\Rightarrow}$ Nechť $k = p \cdot m + r$, kde $p \in \mathbb{Z}$ a $0 \leq r < m$.

$$\Rightarrow \quad a^k = a^{p \cdot m + r} = e$$

$$(a^m)^p \cdot a^r = e$$

$$e^p \cdot a^r = e$$

$$a^r = e \qquad (\; r < m \Rightarrow \qquad)$$

číslo r nemůže být větší než 0, jinak by nastal spor s tím, že $|a| = m$ = nejmenší přirozené číslo takové, že $a^m = e$.

$\Rightarrow$ Číslo r splňuje $0 \leq r < m$ a $r \not> 0$ $\Rightarrow$ $r = 0$ $\Rightarrow$

$$k = p \cdot m + 0$$

$$m \mid k$$

$\boxed{\Leftarrow}$ $m \mid k \Rightarrow a^k = a^{c \cdot m} = (a^m)^c = e^c = e$

$\square$

Důsledek: Nechť $(G, \cdot)$ je grupa, $a \in G$, $|a| = m$. Potom platí:

$$a^i = a^j \Leftrightarrow m \mid (i - j)$$

Věta 5: Nechť $(G,\cdot)$ je grupa generovaná prvkem $a \in G$ řádu $n \in \mathbb{N}$. Potom:

1.) $(G,\cdot)$ je cyklická grupa řádu n, kde $G = \{a^1, a^2, \dots, a^n = e = a^0\}$ a $|G| = n$.

2.) Řád libovolného prvku $g \in G$ je konečný a dělí n. Tzn.

$$|g| \,/\, |G|$$

3.) Nechť $k \in \mathbb{N}$, $k \mid n$. Potom $g = a^{\frac{n}{k}}$ je prvek řádu k a generuje podgrupu $(\langle a^{\frac{n}{k}} \rangle, \cdot)$ řádu k.

4.) V grupě $(G,\cdot)$ existuje podgrupa řádu $k \iff k \mid n$.

5.) Jestliže $g \in G$ je prvek řádu $k \in \mathbb{N}$, pak

$$\langle g \rangle = \langle a^{\frac{n}{k}} \rangle$$

6.) Jestliže $k \mid |G|$, pak v cyklické grupě $(G,\cdot)$ existuje právě jedna podgrupa řádu k (je to $(\langle a^{\frac{n}{k}} \rangle, \cdot)$).

7.) Nechť $g = a^m$, kde $m \geq 1$. Potom $|g| = \dfrac{n}{\gcd(m, |G|)}$

Důkaz:

1.) Je-li grupa $(G,\cdot)$ generovaná jedním prvkem, je podle definice cyklická. Je-li generovaná prvkem $a \in G$ řádu $n \in \mathbb{N}$, potom platí:

$$G = \{a^k \mid k \in \mathbb{Z}\}$$

$\forall k \in \mathbb{Z}\ \exists p, r \in \mathbb{Z} : k = p \cdot n + r$, kde $0 \le r < n$. Proto:

$$a^k = a^{p \cdot n + r} = (a^n)^p \cdot a^r = e^p \cdot a^r = a^r,$$

kde $0 \le r < n$. Ukážeme, že prvky $a^0, a^1, \dots, a^{n-1}$ jsou navzájem disjunktní (sporem). Předpokládejme, že $r_1, r_2 \in \{0, 1, \dots, n-1\}$ a bez újmy na obecnosti $r_1 > r_2$. Potom $n > r_1 - r_2 > 0$. Předpoklad $a^{r_1} = a^{r_2}$ potom podle Důsledku Věty 4 vede k tomu, že $n \mid (r_1 - r_2)$, ale to je spor s tím, že $n > r_1 - r_2 > 0$

$$\Rightarrow \quad G = \{a^0, a^1, \dots, a^{n-1}\}$$

$\square$

2.) $G = \{a^k \mid k \in \mathbb{Z}\} \Rightarrow \forall g \in G\ \exists k_0 \in \mathbb{Z} : g = a^{k_0}$. Potom:

$$g^n = (a^k)^n = (a^n)^k = e^k = e$$

$\Rightarrow$ řád prvku g je menší nebo roven číslu n.

Prvek g generuje množinu $\langle g \rangle = H = \{g^k \mid k \in \mathbb{Z}\}$. Dokážeme, že $(H,\cdot)$ je podgrupa: $(G,\cdot)$ je konečná grupa $\Rightarrow$ stačí ověřit uzavřenost na H:

$$\forall g^{k_1}, g^{k_2} \in H : \quad g^{k_1} \cdot g^{k_2} = g^{k_1 + k_2} = g^k \in H$$

Podle 1.) je $(H,\cdot)$ cyklická grupa řádu $|H| = |g|$ a podle Lagrangeovy věty $|H| \mid |G|$, tzn. $|g| \mid |G|$.

$\square$

3.) Uvažujme prvek $a^{\frac{n}{k}}$, kde k / n. Prvek a je řádu n $\Rightarrow$

$$\left(a^{\frac{n}{k}}\right)^k = a^n = e$$

$\Rightarrow$ Řád prvku $a^{\frac{n}{k}}$ je proto menší, nebo roven, číslu k.
Uvažujme číslo $c \in \mathbb{N}$, $c < k$ (ukážeme, že $|a^{\frac{n}{k}}| \neq c$). Potom:

$$0 < \frac{n}{k} \cdot c < n$$

a tak

$$\left(a^{\frac{n}{k}}\right)^c = a^{\frac{n}{k} \cdot c} \neq e$$

Proto $c < k$ nemůže být řádem prvku $a^{\frac{n}{k}}$ $\Rightarrow$ $|a^{\frac{n}{k}}| = k$

Navíc, podle 1.) je $(\langle a^{\frac{n}{k}} \rangle, \cdot)$ cyklická grupa, jejíž řád je roven řádu prvku $a^{\frac{n}{k}}$.

$\square$

4.) $\boxed{\Leftarrow}$ Tato implikace je tvrzením 3.)

$\boxed{\Rightarrow}$ Tato implikace je tvrzením Lagrangeovy věty.

$\square$

5.) Označme $H = \{a^s \in G \mid (a^s)^k = e\}$.

Dokážeme, že $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$ (ta je konečná, proto stačí ověřit uzavřenost $\cdot$ na H):

$$\forall a^{s_1}, a^{s_2} \in H: \quad (a^{s_1} \cdot a^{s_2})^k = (a^{s_1})^k \cdot (a^{s_1})^k = e \cdot e = e$$

$$\Rightarrow a^{s_1} \cdot a^{s_2} \in H$$

Podle Věty 2 je tedy $(H, \cdot)$ cyklická grupa generovaná prvkem a^{s_0} (tj. $H = \langle a^{s_0} \rangle$), kde

$$s_0 = \min\{s \in \mathbb{N} \mid a^s \in H\} = \min\{s \in \mathbb{N} \mid (a^s)^k = e\}$$

Pro $0 < s < \frac{n}{k}$ je $0 < sk < n$, proto pro $s < \frac{n}{k}$ je $(a^s)^k \neq e$, ale pro $s = \frac{n}{k}$: $(a^s)^k = (a^{\frac{n}{k}})^k = a^n = e$. Proto:

$$s_0 = \frac{n}{k}$$

a tak $H = \langle a^{s_0} \rangle = \langle a^{\frac{n}{k}} \rangle$.

Dále si všimněme, že $\forall g \in G$, kde $|g| = k$ platí $g \in H$ (neboť $g^k = e$).
Díky uzavřenosti $\cdot$ na podgrupě H:

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \subseteq H = \langle a^{\frac{n}{k}} \rangle$$

Ale g je řádu k, proto (podle 1.)) $|\langle g \rangle| = k = |H| = |\langle a^{\frac{n}{k}} \rangle|$.
Proto:

$$\langle g \rangle = \langle a^{\frac{n}{k}} \rangle$$

$\square$

6.) Toto tvrzení je důsledkem tvrzení 5.). Protože $(G, \cdot)$ je cyklická grupa řádu n, musí být každá její podgrupa cyklická grupa řádu k, kde $k | n$. Každá podgrupa řádu k v $(G, \cdot)$ je tedy generovaná prvkem $g \in G$ řádu k. Tvrzení 5.) ale říká, že všechny prvky řádu k z G generují tutéž podgrupu, a to: $(\langle a^{\frac{n}{k}} \rangle, \cdot)$.

7.) $|G| = n$ a tak je třeba dokázat, že řádem prvku a^m je $\frac{n}{\gcd(m,n)}$.
Podle definice řádu prvku

$$|a^m| = r_0 = \min\{ r \in \mathbb{N} \mid (a^m)^r = e \}$$

Všimněme si, že v případě $(a^m)^r = a^{m \cdot r} = e$ z Věty 4 plyne, že

$$n \mid m \cdot r$$

$\forall r \in \mathbb{N}$ splňující $(a^m)^r = e$ proto platí $n \mid mr \wedge m \mid mr \Rightarrow$ číslo mr je společným násobkem čísel m a n. Naopak, pokud mr je společným násobkem čísel m a n, pak $n \mid mr \Rightarrow mr = c \cdot n \Rightarrow a^{mr} = a^{cn} = e$.
Proto:

$$r_0 = \min\{ r \in \mathbb{N} \mid (a^m)^r = e \} = \min\{ r \in \mathbb{N} \mid mr \text{ je spol. náš. } m \text{ a } n\} =$$

$\Rightarrow$ $r = r_0 \Leftrightarrow m r = \operatorname{lcm}(m,n)$ ... nejmenší spol. násobek m a n

$$m r = \frac{m \cdot n}{\gcd(m,n)}$$

$$r = \frac{n}{\gcd(m,n)} = r_0$$

$\square$