1. Cyklické grupy

Tvrzení 1. *Každá podgrupa cyklické grupy je cyklická.*

Důkaz. Buď $\mathbf{H}$ podgrupa cyklické grupy $\mathbf{G} = (G, *, ', e) = \langle a \rangle$. Je-li $H = \{e\}$, pak $\mathbf{H} = \langle e \rangle$. V opačném případě označme k nejmenší kladné číslo takové, že $k \times a \in H$. Dokážeme, že $\mathbf{H} = \langle k \times a \rangle$. Zřejmě $\langle k \times a \rangle \subseteq H$, pro spor tedy předpokládejme, že existuje nějaký prvek $l \times a \in H \setminus \langle k \times a \rangle$. Označme $q = l \operatorname{div} k$ a $r = l \bmod k$, tj. $l = kq + r$. Samozřejmě $k > r \neq 0$, protože $l \times a \notin \langle k \times a \rangle$. Ovšem

$$r \times a = (l \times a) * (-kq \times a) = \underbrace{(l \times a)}_{\in H} * (-q \times \underbrace{(k \times a)}_{\in H}) \in H,$$

což je ve sporu s výběrem k jako nejmenšího čísla splňujícího $k \times a \in H$. □

Příklady.

- Podgrupy grupy $\mathbb{Z}$ jsou právě $a\mathbb{Z} = \langle a \rangle$, $a \in \mathbb{Z}$. Přitom
$$a\mathbb{Z} = b\mathbb{Z} \;\Leftrightarrow\; a = \pm b.$$
(Všimněte si, že podgrupa grupy $\mathbb{Z}$ je totéž co ideál oboru integrity $\mathbb{Z}$, takže charakterizace podgrup je důsledkem toho, že $\mathbb{Z}$ je obor hlavních ideálů.)
- Podgrupy grupy $\mathbb{Z}_n$ jsou právě $a\mathbb{Z}_n = \langle a \rangle$, $a = 0, \ldots, n-1$. Přitom díky Bézoutově rovnosti je $a\mathbb{Z}_n = \langle \mathrm{NSD}(a, n) \rangle$, tedy
$$a\mathbb{Z}_n = b\mathbb{Z}_n \;\Leftrightarrow\; \mathrm{NSD}(a, n) = \mathrm{NSD}(b, n).$$

Podgrupy obecných cyklických grup se chovají podobně jako ve výše uvedeném příkladu, jak plyne z následujícího tvrzení.

Lemma 2. *Buď $\mathbf{G}$ grupa a a její prvek řádu n. Pak $\langle k \times a \rangle = \langle \mathrm{NSD}(k, n) \times a \rangle$ pro každé $k \in \mathbb{Z}$.*

Důkaz. Označme $u \in \mathbb{Z}$ takové, že $k = u \cdot \mathrm{NSD}(k, n)$. Pak $k \times a = u \times (\mathrm{NSD}(k, n) \times a) \in \langle \mathrm{NSD}(k, n) \times a \rangle$, tedy $\langle k \times a \rangle \subseteq \langle \mathrm{NSD}(k, n) \times a \rangle$.

Na druhou stranu, díky Bézoutově rovnosti existují $u, v \in \mathbb{Z}$ splňující $\mathrm{NSD}(k, n) = uk + vn$, a tedy $\mathrm{NSD}(k, n) \times a = (uk + vn) \times a = (u \times (k \times a)) * (v \times (n \times a)) = (u \times (k \times a)) * (v \times e) = u \times (k \times a) \in \langle k \times a \rangle$, tedy $\langle k \times a \rangle \supseteq \langle \mathrm{NSD}(k, n) \times a \rangle$. □

Tvrzení 3. *Cyklická grupa $\mathbf{G} = \langle a \rangle$ konečného řádu n obsahuje právě jednu podgrupu řádu k pro každé $k \mid n$, konkrétně podgrupu $\langle \frac{n}{k} \times a \rangle$.*

Důkaz. Z jedné strany vidíme, že pokud $d \mid n$, pak $\langle d \times a \rangle$ sestává z prvků tvaru $u \times (d \times a) = ud \times a$, kde $u = 0, \ldots, \frac{n}{d} - 1$, a tedy $|\langle d \times a \rangle| = \frac{n}{d}$. Pro důkaz jednoznačnosti uvažujme podgrupu $\mathbf{H} \leq \mathbf{G}$ řádu k. Podle Tvrzení 1 je $\mathbf{H}$ cyklická, tedy $\mathbf{H} = \langle l \times a \rangle = \langle \mathrm{NSD}(l, n) \times a \rangle$ pro nějaké $l \in \mathbb{Z}$, a tedy $\mathbf{H} = \langle d \times a \rangle$ pro nějaké $d \mid n$. Tyto jsou po dvou různé, neboť jsou různě velké. □

Nekonečné cyklické grupy obsahují pouze prvky nekonečného řádu, s výjimkou jednotky. Mají přesně dva generátory, v případě grupy $\mathbb{Z}$ to jsou prvky ± 1. Pro konečné cyklické grupy je situace mnohem zajímavější. Předně je dobré si uvědomit následující:

Tvrzení 4. *Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa konečného řádu n. Pak $\mathbf{G} = \langle k \times a \rangle$ právě tehdy, když $\mathrm{NSD}(k, n) = 1$.*

Důkaz. Jsou-li k, n nesoudělné, podle Lemmatu 2 platí $\langle k \times a\rangle = \langle 1 \times a\rangle = \langle a\rangle = \mathbf{G}$. Naopak, je-li $\mathrm{NSD}(k,n) = d \neq 1$, pak $\langle k \times a\rangle = \langle d \times a\rangle$ sestává z prvků tvaru $ud \times a$, $u = 0, \ldots, \frac{n}{d} - 1$, a tedy $a \notin \langle k \times a\rangle$. □

Například pro grupy $\mathbb{Z}_n = \langle 1\rangle$ dostáváme, že $\mathbb{Z}_n = \langle k\rangle$ právě tehdy, když $\mathrm{NSD}(k,n) = 1$.

Bezprostředním důsledkem Tvrzení 4 je, že cyklická grupa řádu n má právě $\varphi(n)$ generátorů. Dodefinujme Eulerovu funkci hodnotou $\varphi(1) = 1$.

Věta 5. *Cyklická grupa konečného řádu n obsahuje právě $\varphi(k)$ prvků řádu k, pro každé $k \mid n$.*

Důkaz. Označme tuto grupu $\mathbf{G}$. Tvrzení 3 říká, že v $\mathbf{G}$ existuje právě jedna podgrupa $\mathbf{H}_k$ řádu k. Ta má podle Tvrzení 4 právě $\varphi(k)$ generátorů, neboli prvků řádu k, takže $\mathbf{G}$ obsahuje alespoň $\varphi(k)$ prvků tohoto řádu. Na druhou stranu, je-li prvek $a \in G$ řádu k, pak generuje podgrupu $\mathbf{H}_k$, neboť $|\langle a\rangle| = k$ a taková podgrupa je v $\mathbf{G}$ jenom jedna. Tedy jiné prvky řádu k než generátory $\mathbf{H}_k$ v $\mathbf{G}$ nejsou. □

Větu 5 lze překvapivým způsobem aplikovat na důkaz následující kombinatorické identity.

Tvrzení 6. *Pro každé n platí $\sum_{k|n} \varphi(k) = n$.*

Důkaz. Označme u_k počet prvků řádu k v grupě $\mathbb{Z}_n$. Podle Lagrangeovy věty je $u_k = 0$ kdykoliv $k \nmid n$. Sečteme-li hodnoty u_k přes všechny možné řády $k \mid n$, dostaneme přesně počet prvků grupy $\mathbb{Z}_n$. Podle Věty 5 je $u_k = \varphi(k)$, takže $\sum_{k|n} \varphi(k) = \sum_{k|n} u_k = |\mathbb{Z}_n| = n$. □

Netriviální aplikace výše uvedené teorie poskytuje následující veledůležitá věta.

Věta 7. *Buď $\mathbf{G}$ konečná podgrupa grupy $\mathbf{T}^*$, kde $\mathbf{T}$ je nějaké těleso. Pak $\mathbf{G}$ je cyklická.*

Lemma 8. *Buď $\mathbf{G} = (G, *, ', e)$ konečná grupa a předpokládejme, že pro každé $k \in \mathbb{N}$ existuje nejvýše k prvků a splňujících $k \times a = e$. Pak $\mathbf{G}$ je cyklická.*

Důkaz. Označme u_k počet prvků řádu k v grupě $\mathbf{G}$, položme $n = |G|$. Pokud $k \nmid n$, pak podle Lagrangeovy věty je $u_k = 0$. Naopak, pokud $u_k \neq 0$, uvažujme nějaký prvek a řádu k. Pak $\langle a\rangle_{\mathbf{G}}$ je cyklická grupa řádu k, a tedy všechny prvky $b = u \times a$, $u = 0, \ldots, k-1$, splňují $k \times b = e$. Podle předpokladu jsme nalezli všechna řešení této rovnice, takže $\langle a\rangle_{\mathbf{G}}$ je jediná cyklická podgrupa řádu k v $\mathbf{G}$. Podle Věty 5 má $\varphi(k)$ generátorů, tedy $u_k = \varphi(k)$.

Shrnuto, pro každé $k \mid n$ platí $u_k = 0$ nebo $u_k = \varphi(k)$. Přitom $\sum_{k|n} u_k = n$, a zároveň podle Tvrzení 6 je $\sum_{k|n} \varphi(k) = n$. Tedy $u_k = \varphi(k)$ pro všechna $k \mid n$, speciálně tedy v $\mathbf{G}$ existuje prvek řádu n. □

Důkaz Věty 7. Je-li $\mathbf{T}$ těleso, pak má polynom $x^k - 1$ nejvýše k kořenů v $\mathbf{T}$. Tedy v $\mathbf{G} \leq \mathbf{T}^*$ existuje nejvýše k prvků splňujících $a^k = 1$ a můžeme aplikovat předchozí lemma. □