2.A Konečné cyklické grupy

Předpokládejme, že g je prvek konečné grupy G. Podgrupa $\langle g\rangle = \{g^n\ ;\ n \in \mathbb{N}\}$ je konečná cyklická grupa. Počet jejích prvků se nazývá *řád prvku* g a budeme ho značit $\mathrm{o}(g)$. Podle Lemmatu 2.2 je $\mathrm{o}(g) = k$, kde $k \in \mathbb{N}$ je nejmenší takové, že $g^k = 1$. Prvky $\langle g\rangle$ jsou tedy $g, g^2, g^3, ..., g^{k-1}, 1$. Z Věty 2.6 okamžitě plyne:

Důsledek 2.7 *Ať je g prvek konečné grupy G. Pak $\mathrm{o}(g) \mid |G|$.*

V kapitole 1.B jsme mluvili o množině $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ s operací sčítání modulo n. Není těžké ukázat, že sčítání modulo n je asociativní, tedy že $\mathbb{Z}_n$ je pologrupa. Z dalšího Lemmatu plyne, že $\mathbb{Z}_n$ je grupa.

Lemma 2.8 *Buď C konečná cyklická grupa s generátorem g, $\mathrm{o}(g) = n$. Pak jsou C a $\mathbb{Z}_n$ izomorfní grupy.*

Důkaz. Chceme najít izomorfismus $f : C \to \mathbb{Z}_n$. Pro $a \in C$ položme $\log_g(a) = i$, kde $i \in \mathbb{N} \cup \{0\}$ je nejmenší takové, že $g^i = a$. Definujeme $g^0 = 1$ neutrální prvek C. Podle Lemmatu 2.2 vidíme, že $\log_g$ je bijekce z C do množiny $\{0, 1, 2, ..., n-1\}$. Zbývá ukázat vlastnost homomorfismu. Zvolme $a, b \in C$, $a = g^i$, $b = g^j$, $0 \le i, j < n$. Tedy $a \cdot b = g^{i+j}$ a pokud je $i + j \ge n$, pak $a \cdot b = g^{i+j-n} \cdot g^n = g^{i+j-n} \cdot 1 = g^{(i+j) \bmod n}$. Tedy modulo n platí: $\log_g(a \cdot b) = \log_g(a) + \log_g(b)$. □

Důsledek 2.9 *Je-li g prvek konečné grupy a $k \in \mathbb{Z}$, pak $g^k = 1$ právě když $\mathrm{o}(g) | k$.*

Důkaz. Opět klademe $g^0 = 1$ a pro $k > 0$ považujeme g^{-k} za $(g^k)^{-1} = (g^{-1})^k$. Položme $n = \mathrm{o}(g)$ a počítejme v $\mathbb{Z}_n$. Podle Lemmatu 2.8 je $g^k = 1$ právě když k je kongruentní modulo n s 0, což nastává právě když $n | k$. □

Neutrální prvek 1 grupy C tedy odpovídá neutrálnímu prvku 0 v $\mathbb{Z}_n$, inverzní prvek $(g^i)^{-1} \in C$ odpovídá prvku $-i \bmod n \in \mathbb{Z}_n$.

Budeme dále mluvit o cyklických grupách v obecném tvaru, ale vždy půjde o grupu $\mathbb{Z}_n$ pro vhodné n.

Lemma 2.10 *Ať je H podgrupa konečné cyklické grupy C. Pak je H cyklická. Navíc platí, že $H = \langle g^k\rangle$, kde g je generátor C a $k = |C|/|H|$.*

Důkaz. Zvolme $H \le C = \langle g\rangle$. Na C máme ekvivalenci $\sim_H$ jejíž třídy jsou pravé rozkladové třídy podle H. Zaveďme podobným způsobem relaci $\approx_H$ na $\mathbb{Z}$: pro $n, m \in \mathbb{Z}$ bude $n \approx_H m$ pokud $g^n \sim_H g^m$. Mocninu g^{-k} pro $k \ge 0$ považujeme za $(g^k)^{-1}$. Je hned vidět, že $\approx_H$ je ekvivalence na $\mathbb{Z}$. Ukážeme, že $\approx_H$ je dokonce kongruence (viz kapitola 1.B). Mějme $n_1, n_2, m_1, m_2 \in \mathbb{Z}$ taková, že $n_1 \approx_H n_2$ a $m_1 \approx_H m_2$. Pak $g^{(n_2+m_2)} = g^{n_2} \cdot g^{m_2} = (g^{n_1} \cdot h) \cdot (g^{m_1} \cdot h') = g^{n_1+m_1} \cdot (h \cdot h')$, kde $h, h', h \cdot h' \in H$, a tedy $n_1 + m_1 \approx_H n_2 + m_2$. Uvědomme si, že jsme použili komutativitu násobení v cyklické grupě. Kongruence $\approx_H$ na $\mathbb{Z}$ se musí rovnat $\equiv_k$ pro vhodné $k \in \mathbb{N}$. Přitom má zjevně $\approx_H$ stejný počet tříd jako $\sim_H$ a tudíž je z Lagrangeovy věty $k = |C|/|H|$.

Snadno ukážeme, že H musí být generovaná prvkem g^k. Nejprve $k \equiv_k 0$ a proto $g^k = g^0 \cdot h = 1 \cdot h = h \in H$. Pro $h \in H$ je $h = g^i$ pro nějaké $i \in \mathbb{N}$ a z $g^i = g^0 \cdot h$ plyne $i \equiv_k 0$. To ale znamená, že $i = l \cdot k$ pro nějaké $l \in \mathbb{Z}$ a že $h = g^{l \cdot k} = (g^k)^l$. □

Následující Lemma se dá chápat jako obrácení Lagrangeovy věty pro konečné cyklické grupy.

Důsledek 2.11 *Ať je C konečná cyklická grupa s generátorem g, $\mathrm{o}(g) = n$ a $l \in \mathbb{N}$, $l \mid n$. Pak existuje právě jedna l-prvková podgrupa C. Tato podgrupa je generovaná prvkem g^k, kde $k = n/l$.*

Důkaz. Uvědomme si, že podgrupa generovaná $h = g^{n/l}$ má opravdu l prvků. Platí $h^l = g^{l \cdot n/l} = g^n = 1$ a tedy $\langle h \rangle = \{h, h^2, h^3, ...h^{l-1}, 1\}$ a přitom z $\mathrm{o}(g) = n$ plyne, že l je nejmenší možné.

Naopak, je-li H l-prvková podgrupa, pak podle Lemmatu 2.10 je $H = \langle g^{n/l} \rangle$ a tedy je jednoznačně určená. □

Lemma 2.12 *Počet různých generátorů n-prvkové cyklické grupy je $\varphi(n)$.*

Důkaz. Zvolme $0 \leq i < n$ a ptejme se, kdy je i generátor $\mathbb{Z}_n$. Prvek 1 je generátor $\mathbb{Z}_n$. Podle Lemmatu 2.10 platí, že podgrupa $\langle i \rangle = \{m \cdot i \ ; \ m \in \mathbb{N}\}$ (aditivní zápis!) je generovaná $k \cdot 1$, kde $k = n/l$ a l je počet prvků $\langle i \rangle$. Z rovnosti $\langle i \rangle = \langle k \cdot 1 \rangle$ plyne, že v $\mathbb{Z}_n$ je $i = r \cdot k \cdot 1$ pro vhodné $r \in \mathbb{N}$, tedy $i \equiv_n rk$ a proto $\mathrm{NSD}(i, n) = \mathrm{NSD}(rk, n)$, tudíž $\mathrm{NSD}(k, n) \mid \mathrm{NSD}(i, n)$. Podobně dostaneme $\mathrm{NSD}(i, n) \mid \mathrm{NSD}(k, n)$, tedy $\mathrm{NSD}(i, n) = \mathrm{NSD}(k, n) = k$, neboť $k|n$.

Prvek i je generátor $\mathbb{Z}_n$ právě když $l = n$ právě když $k = 1 = \mathrm{NSD}(k, n) = \mathrm{NSD}(i, n)$. Tedy i je generátor $\mathbb{Z}_n$ právě když je i nesoudělné s n a počet různých generátorů je tudíž hodnota Eulerovy funkce v n. □

Důsledek 2.13 *$\mathbb{Z}_p$ se sčítáním a násobením modulo p je těleso pro $p \in \mathbb{N}$ prvočíslo.*

Důkaz. Nenulové prvky $\mathbb{Z}_p$ značíme $\mathbb{Z}_p^*$. Chceme dokázat, že $\mathbb{Z}_p^*$ s násobením modulo p tvoří grupu. Nejprve dokažme uzavřenost na násobení. Pro $i, j \in \mathbb{Z}_p^*$ jistě platí, že p nedělí i ani j, tedy p nedělí $i \cdot j$ a $i \cdot j \neq 0$ modulo p.

Pro $i \in \mathbb{Z}_p^*$ je i podle Lemmatu 2.12 generátor $\mathbb{Z}_p(+)$. Musí proto existovat $k \in \mathbb{N}$ takové, že $k \cdot i = 1$ modulo p. Našli jsme inverzi k i v násobení modulo p, $k \bmod p = i^{-1} \in \mathbb{Z}_p^*$. □

Úkol. Později uvidíme, že jsou grupy $\mathbb{Z}_p^*$ s násobením modulo p, pro p prvočíslo, rovněž cyklické. Například v $\mathbb{Z}_5^*$ je $\langle 2 \rangle = \{2, 2^2, 2^3, 2^4\} = \{2, 4, 3, 1\}$, tedy číslo 2 generuje $\mathbb{Z}_5^*$. Která čísla jsou generátory $\mathbb{Z}_7^*$? Kolik různých generátorů má grupa $\mathbb{Z}_{29}^*$?

Vlastnosti grupy $\mathbb{Z}_n(+)$, které jsme v této kapitole dokázali, můžeme zpětně aplikovat v elementární teorii čísel.

Lemma 2.14 *Pro přirozené číslo n platí $n = \Sigma_{k|n} \varphi(k)$.*

Důkaz. Pro $k|n$ existuje podle Důsledku 2.11 jediná k-prvková podgrupa $\mathbb{Z}_n(+)$ a ta je cyklická. Počet prvků řádu k v této podgrupě a tudíž i v celém $\mathbb{Z}_n$ je $\varphi(k)$. Každý prvek $\mathbb{Z}_n$ má nějaký řád, který dělí n, a proto platí rovnost $|\mathbb{Z}_n| = n = \Sigma_{k|n}(\text{počet prvků řádu } k) = \Sigma_{k|n}\varphi(k)$. □

Později budeme potřebovat následující charakterizaci cyklických grup.

Věta 2.15 *Ať je C konečná grupa. Pokud pro každé $k \in \mathbb{N}$ obsahuje C nejvýše jednu k-prvkovou podgrupu, pak je C cyklická.*

Důkaz. Pokusme se najít nějaký generátor C. Položme $n = |C|$. Podle Lemmatu 2.14 je $n = \Sigma_{k|n}\varphi(k)$ a také $n = \Sigma_{k|n}p_k$, kde p_k je počet prvků C řádu k. Je-li $p_n = 0$, pak pro nějaké $k|n$ musí být $p_k > \varphi(k)$. Zvolme $a \in C$ prvek řádu k. Podgrupa $\langle a\rangle$ obsahuje pouze $\varphi(k)$ prvků řádu k, tedy musí existovat $b \in C \setminus \langle a\rangle$ řádu k. To ale dává dvě různé k-prvkové podgrupy: $\langle a\rangle$ a $\langle b\rangle$. Proto $p_n \neq 0$ a existuje prvek C řádu n, tedy generátor. □

Grupy permutací. V lineární algebře jste při počítání s determinanty potřebovali některé vlastnosti permutací, jako je asociativita skládání permutací, existence jednotkové a inverzních permutací nebo výpočet znaménka permutace. První tři zmíněné vlastnosti říkají, že množina všech permutací na n bodech je spolu s operací skládání permutací grupa. Zopakujme si potřebné definice.

Označme S_n množinu všech bijekcí na množině $\{1, 2, ..., n\}$, tedy bijekcí $\pi : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$. Prvky S_n je možné zapisovat do matice typu $2 \times n$, kde do horního řádku píšeme čísla $i \in \{1, 2, ..., n\}$ a do spodního jejich obrazy $\pi(i)$:

$$\begin{pmatrix} 1 & 2 & 3 & ..... & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & ..... & \pi(n-1) & \pi(n) \end{pmatrix}$$

Množina S_n je spolu s operací skládání zobrazení grupa. Její neutrální prvek je identické zobrazení $1 = 1_{\{1,2,...,n\}}$:

$$\begin{pmatrix} 1 & 2 & 3 & ..... & n-1 & n \\ 1 & 2 & 3 & ..... & n-1 & n \end{pmatrix}$$

a inverzní prvky jsou inverzní zobrazení, tedy

$$\begin{pmatrix} 1 & 2 & 3 & ..... & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & ..... & \pi(n-1) & \pi(n) \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & ..... & \pi(n-1) & \pi(n) \\ 1 & 2 & 3 & ..... & n-1 & n \end{pmatrix}$$

V našem zápisu nehraje žádnou roli, že horní řádek u inverzní permutace není uspořádán podle velikosti. Prvky S_n se nazývají *permutace* a S_n se nazývá *grupa permutací na n bodech.*

Někdy je efektivnější zapisovat permutace pomocí cyklů. Zaveďme graf zobrazení $f : X \to X$ na množině X takto: vrcholy budou prvky X a šipky budou tvaru $x \to f(x)$ pro $x \in X$.

Úkol. Popište graf obecného zobrazení. Popište graf $f : X \to X$ v případě, že f je bijekce (a X nějaká, obecně nekonečná, množina).

Uvědomme si, že v této kapitole již definovaný graf pologrupy P s vybraným generátorem g je graf zobrazení $P \to P$, $a \mapsto g \cdot a$ pro $a \in P$.

Nyní nás bude zajímat graf $\pi : X \to X$, kde π je bijekce a X konečná množina. Začněme například s číslem 1:

$$1 \to \pi(1) \to \pi^2(1) \to .....$$

Množina X je konečná, nějaké číslo se tedy musí v dané posloupnosti zopakovat. Uvědomme si, že se nejdřív musí zopakovat 1: pokud se zopakuje číslo $\pi^i(1)$, $i \geq 1$, tedy $\pi^i(1) = \pi^j(1)$ pro $j > i$, pak má číslo $\pi^i(1)$ dva vzory: $\pi^{i-1}(1)$ a $\pi^{j-1}(1)$ (definujeme $\pi^0(1) = 1$). Zobrazení π je prosté, tedy $\pi^{i-1}(1) = \pi^{j-1}(1)$ a takto indukcí dojdeme k $1 = \pi^{j-i}$. V prostém zobrazení π má každý prvek jednoznačně určený obraz i vzor a proto je souvislá komponenta grafu π obsahující číslo 1 právě tento cyklus:

$$1 \to \pi(1) \to \pi^2(1) \to ..... \to \pi^{-2}(1) \to \pi^{-1}(1) \to 1$$

Vidíme, že graf π se rozkládá na disjunktní (=nezávislé) cykly. Dokázali jsme fakt, že každá permutace má rozklad na složení nezávislých cyklů. Přitom jsme použili pouze, že π je prosté zobrazení, ale uvědomme si, že prosté zobrazení na konečné množině musí být bijekce.

Příklad. Mějme permutaci

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 7 & 2 & 6 & 4 \end{pmatrix} \in \mathrm{S}_7$$

Rozklad π na složení nezávislých cyklů je:

$$\pi = (1\ 5\ 2) \circ (3) \circ (4\ 7) \circ (6) = (1\ 5\ 2) \circ (4\ 7),$$

kde v maticovém zápisu:

$$(1\ 5\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 4 & 2 & 6 & 7 \end{pmatrix}.$$

Spočítejme řád π. Nejdříve označme $C_1 = (1\ 5\ 2)$ a $C_2 = (4\ 7)$, tedy $\pi = C_1 \circ C_2 = C_2 \circ C_1$ díky nezávislosti cyklů. Dále $\pi^k = C_1^k \circ C_2^k$ (používáme nezávislost!) a proto je $\pi^k = 1$ právě když $C_1^k = 1$ a zároveň $C_2^k = 1$. Tedy $\pi^k = 1$ právě když $\mathrm{o}(C_1)|k$ a zároveň $\mathrm{o}(C_2)|k$. Nejmenší možnou volbou dostaneme $\mathrm{o}(\pi) = \mathrm{NSN}(\mathrm{o}(C_1), \mathrm{o}(C_2))$. Snadno zjistíme řády cyklů: $\mathrm{o}(C_1) = 3$ a $\mathrm{o}(C_2) = 2$. Máme $\mathrm{o}(\pi) = \mathrm{NSN}(3, 2) = 6$.

Pro $C \in \mathrm{S}_n$ cyklus délky l snadno zjistíme jeho řád. Ať je $C = (i_0 i_1 ... i_{l-1})$, $1 \leq i_0, i_1, ..., i_{l-1} \leq n$ po dvou různá čísla. Pro $0 \leq j \leq l-1$ platí $C^k(i_j) = i_{(j+k \bmod l)}$. Tedy l je nejmenší takové, že $C^l = 1$, a $\mathrm{o}(C) = l$.

Mějme $\pi = C_1 \circ C_2 \circ ... \circ C_r$ rozklad permutace π na složení nezávislých cyklů, označme l_i délku cyklu C_i, $i = 1, ..., r$, a předpokládejme, že je $l_i > 1$ pro všechna $i = 1, ..., r$. Neuspořádaná r-tice $[l_1, l_2, ..., l_r]$ se nazývá *typ permutace* π a budeme ji značit $\mathrm{t}(\pi)$. Pro $\pi = 1$ položíme $\mathrm{t}(1) = \emptyset$.

Úkol. Uvažte pro C cyklus délky l podgrupu $\langle C \rangle = \{C, C^2, C^3, ..., C^{l-1}, 1\}$. Jaké typy mají permutace z $\langle C \rangle$?

Lemma 2.16 *Ať je* $\mathrm{t}(\pi) = [l_1, l_2, ..., l_r]$ *typ permutace* $\pi \in \mathrm{S}_n$. *Pak pro řád* π *platí* $\mathrm{o}(\pi) = \mathrm{NSN}(l_1, l_2, ..., l_r)$.

Důkaz. Ať je $\pi = C_1 \circ C_2 \circ ... \circ C_r$ je rozklad π na složení nezávislých cyklů. Nezávislé cykly ve skládání komutují, proto $\pi^k = C_1^k \circ C_2^k \circ ... \circ C_r^k$. Z toho snadno plyne, že $\pi^k = 1$ právě když $C_i^k = 1$ pro všechna $i = 1, ..., r$. To podle Důsledku 2.9 dává $\pi^k = 1$ právě když $\mathrm{o}(C_i) | k$ pro všechna $i = 1, ..., r$. Nejmenší možná volba je tedy $\mathrm{o}(\pi) = \mathrm{NSN}(\mathrm{o}(C_1), \mathrm{o}(C_2), ..., \mathrm{o}(C_r))$. Řád cyklu je ovšem roven jeho délce a proto je $\mathrm{o}(\pi) = \mathrm{NSN}(l_1, l_2, ..., l_r)$. □