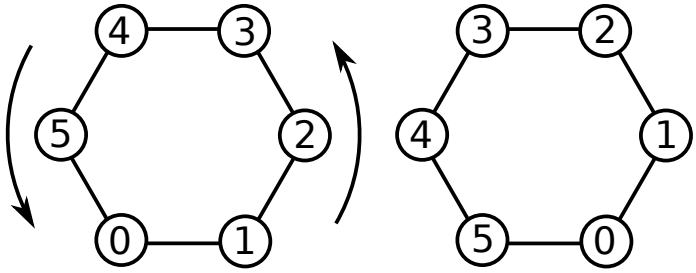
1. Grupa $\mathbb{Z}_n$ – zoznámte sa, prosím

Grupa v nadpise tohoto dielu je najjednoduchšou a zároveň najdôležitejšou grupou. Preto si zaslúži, aby jej bola venovaná celá kapitola. Nájdeme ju úplne všade, takže určite nikoho neprekvapí, že sa najprv pozrieme na symetrie mnohouholníkov.

1.1. Symetrie pravidelného n-uholníka

Pre začiatok nebudeme vyšetrovať úplne všetky symetrie, ale len také, ktoré zachovávajú orientáciu, tj. vynecháme zrkadlenia. Zostanú nám teda len natočenia o $\frac{k}{n} \times 360°$ pre ľubovoľné $k \in \mathbb{Z}$. Skrátene – natočenia o k. Ako vyzerá natočenie o 1 si môžete pozrieť na obrázku.



Hneď si všimneme, že natočenia, ktoré sa líšia o n sú totožné. Druhá dôležitá vec je, že natočenie o k_1 a následne o k_2 je to isté ako natočenie o $k_1 + k_2$. Inými slovami, táto grupa je v podstate rovnaká ako grupa celých čísel modulo n s operáciou sčítania $(\mathbb{Z}_n, +)$ (skrátene $\mathbb{Z}_n$, ak bude jasné, že máme na mysli sčítanie). Presnejšie povedané, tieto grupy sú izomorfné.

Definícia 1.1.1. Homomorfizmu $f : H \to G$, ktorý je zároveň bijekciou (tj. zobrazením jedna k jednej medzi dvoma množinami) hovoríme *izomorfizmus*. O grupách H a G potom povieme, že sú *izomorfné* a píšeme $H \cong G$.

Rozmyslite si, že aj inverzné zobrazenie f^{-1} je homomorfizmus.

1.2. Cyklická grupa

Prvá dôležitá vlastnosť grupy $\mathbb{Z}_n$ je, že sa celá dá vygenerovať z jediného prvku. Čo presne sa tým myslí?

Definícia 1.2.1. *Mocniny* prvku a budeme značiť $a^k \equiv \underbrace{a \circ \cdots \circ a}_{k}$, kde $k > 0$ a $\circ$ je grupová operácia. Ďalej identitu v grupe zapíšeme ako a^0 a záporné mocniny vyhradíme pre inverzné prvky $a^{-k} \equiv (a^{-1})^k$ pre $k > 0$.

Definícia 1.2.2. Grupa G sa nazýva *cyklická*, ak existuje prvok $g \in G$ tak, že $G = \langle g \rangle \equiv \{g^n | n \in \mathbb{Z}\}$.

Grupa $\mathbb{Z}_n$ pochopiteľne cyklická je, lebo každý jej prvok k vyjadríme ako $k = \underbrace{1 + \cdots + 1}_{k}$.

Naopak, každá n-prvková cyklická grupa sa dá interpretovať ako grupa $\mathbb{Z}_n$, pretože pre generátor g platí $g^n = g^0 = e$ (viď úlohu 1). Príslušný izomorfizmus medzi týmito grupami je daný pomocou $a = g^k \leftrightarrow k$ pre $a \in G$ a $k \in \mathbb{Z}_n$ (viď úlohu 2).

Zdá sa, že táto grupa sa vyskytuje v mnohých podobách a obsadeniach. Ako uvidíme neskôr, je to zároveň fundamentálny stavebný blok množstva ďalších grúp, a preto má zmysel pozrieť sa na ňu ešte viac do hĺbky.

1.3. Podgrupa

Ako sa taká grupa vlastne skúma? Obvykle, keď človek dostane do ruky novú grupu, tak sa snaží zistiť, či v nej nie je ukrytá nejaká menšia grupa, ktorú už pozná, a tým si trochu zjednodušiť (obvykle dosť ťažkú) úlohu skúmania celej grupy.

Definícia 1.3.1. Uvažujme podmnožinu H grupy $(G, \circ)$. Nech ďalej pre všetky $a, b \in H$ je aj $a \circ b \in H$, takže $\circ$ sa dá uvažovať aj ako operácia na množine H. Ak $(H, \circ)$ je navyše grupa, tak ju nazveme *podgrupou* grupy G.

To znamená, že ak vieme, že H je podgrupa a $a, b \in H$ tak potom nutne aj $a \circ b \in H$. To kladie pomerne silné obmedzenia na to, ktoré podmnožiny majú šancu byť podgrupami. Presnejšie

Lemma 1.3.2. *Nech H je podgrupa grupy G. Ak prvok $g \in H$, tak už nutne $\langle g \rangle \subset H$.*

Dôkaz je priamočiary (pomocou sporu s definíciou podgrupy) a prenecháme ho čitateľovi (viď úlohu 3).

Platí tiež, že samotné $\langle g \rangle$ už tvorí podgrupu. Budeme ju volať celkom prirodzene *cyklická podgrupa generovaná prvkom g*.

Lemma 1.3.3. *Pre všetky $g \in G$ je $\langle g \rangle$ podgrupou grupy G.*

Dôkaz: Musíme overiť, že sú splnené všetky predpoklady definície 1.3.1. Ak $g^n, g^m \in \langle g \rangle$, tak potom zrejme aj $g^n \circ g^m = g^{n+m} \in \langle g \rangle$. Musíme ešte overiť, že $\langle g \rangle$ je grupa. Zrejme násobenie je asociatívne

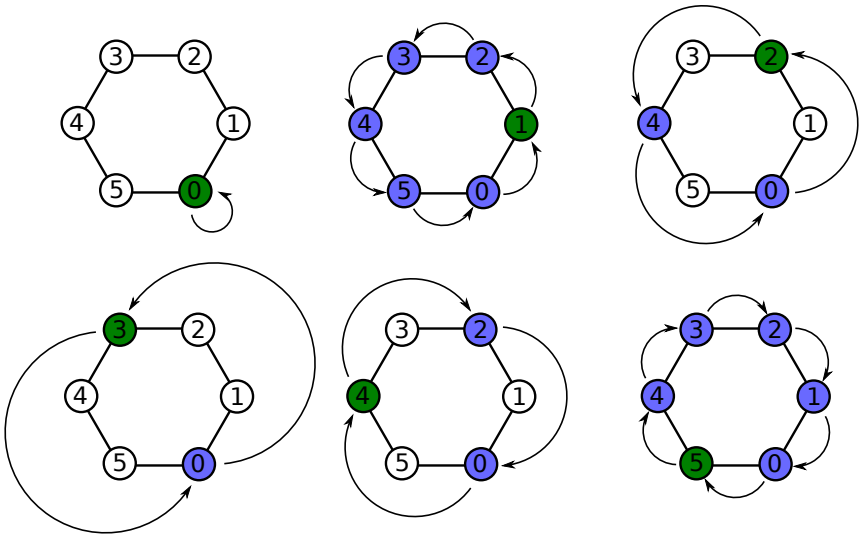
$$(g^n \circ g^m) \circ g^k = g^{n+m} \circ g^k = g^{n+m+k} = g^n \circ g^{m+k} = g^n \circ (g^m \circ g^k)$$

Identitu tiež nájdeme ľahko, pretože $e = g^0 \in \langle g \rangle$. Ďalej, ak $g^n \in G$, tak ľahko nájdeme inverzný prvok a to $g^{-n} \in G$, pretože $g^n \circ g^{-n} = g^0 = e$. □

Pozrime sa, čo nám toto tvrdenie hovorí o podgrupách grupy $\mathbb{Z}_6$. Ak zoberieme 0, tak z nej už nič nového nevygenerujeme (lebo $0 + 0 = 0$), čiže dostaneme jednoprvkovú podgrupu pozostávajúcu len z identity. Takáto sa nachádza v každej grupe a nie je veľmi zaujímavá. Preto sa jej hovorí *triviálna*. Postúpme ďalej. Ak vezmeme 1, tak z horeuvedeného už vieme, že tento prvok generuje celú grupu $\mathbb{Z}_n$. Opäť to nie je zaujímavý prípad, lebo sme nedostali nič nové. Táto podgrupa sa zasa nazýva *nevlastná*. Má $\mathbb{Z}_6$ aj nejaké zaujímavejšie tzv. *vlastné* grupy? Rýchlo prídeme na to, že prvky 2 aj 4 vygenerujú množinu $\{0, 2, 4\} \cong \mathbb{Z}_3$, prvok 3 množinu $\{0, 3\} \cong \mathbb{Z}_2$ a prvok 5 opäť celú $\mathbb{Z}_6$. Našli sme teda celkovo 4 podgrupy. Môžu v $\mathbb{Z}_6$ existovať ešte nejaké iné? Rozmyslite si. Chvíle premýšľania si môžete skrátiť pohľadom na obrázok č. 2, kde máte nakreslené všetky podgrupy, ktoré sme doteraz našli.

1.4. Podgrupy $\mathbb{Z}_n$

Hotovo? Takže už viete, že všetky podgrupy grupy $\mathbb{Z}_6$ sú opäť len nejaké $\mathbb{Z}_k$ a žiadne iné tam už nie sú. Je to špecifikum len $\mathbb{Z}_6$, alebo to platí pre všetky $\mathbb{Z}_n$? Po chvíli



Cyklické podgrupy grupy $\mathbb{Z}_6$

skúšania človek príde k presvedčeniu, že by toto tvrdenie malo platiť a začne zisťovať, ako by sa dalo dokázať. Takmer určite sa pritom nevyhne nasledujúcemu pozorovaniu

Lemma 1.4.1. *Majme nenulové čísla $m, n \in \mathbb{Z}$. Potom existujú čísla $s, t \in \mathbb{Z}$ tak, že $ms + nt = \gcd(m, n)$, kde* gcd *je najväčší spoločný deliteľ.*

Dôkaz tohoto tvrdenia spočíva na Euklidovom algoritme pre hľadanie najväčšieho spoločného deliteľa. Je to veľmi pekná teória, ktorá funguje v každom tzv. euklidovskom okruhu (ktorým sú aj celé čísla $\mathbb{Z}$), ale je to mimo rámec nášho seriálu o grupách. Prikročme teda radšej k dôkazu hlavného bodu dnešného programu

Veta 1.4.2. *Každá podgrupa H cyklickej grupy G je cyklická.*

Dôkaz: Chce sa po nás, aby sme našli prvok $h \in H$ taký, že $H = \langle h \rangle$. Vieme, že G je cyklická, takže ak máme prvky $a, b \in H$, tak ich môžeme vyjadriť ako $a = g^m$, $b = g^n$ pre nejaké n a m. Vďaka lemme 1.3.2 vieme, že do H patria aj všetky mocniny prvkov a a b. Z definície podgrupy zasa vieme, že do H musia patriť aj všetky možné súčiny týchto mocnín. Lemma 1.4.1 nám teda dá podstatný výsledok a to, že do H musí patriť aj $a^s \circ b^t = g^{ms+nt} = g^{\gcd(m,n)}$. Označme tento prvok h_2. Tým pádom môžeme písať $a = h_2^{m/\gcd(m,n)}$ a $b = h_2^{n/\gcd(m,n)}$. Zoberme si teraz všetky prvky grupy $H = \{g^{n_1}, \ldots, g^{n_k}\}$. Predchádzajúcu úvahu môžeme priamočiaro zovšeobecniť aj pre viac než dva prvky a dostávame, že hľadaným generátorom H je $h \equiv g^{\gcd(n_1,\ldots,n_k)}$. □

Dokázali sme veľmi užitočnú vec. Napr. už vieme, že sme skutočne našli úplne všetky podgrupy grupy $\mathbb{Z}_6$. Tým to však zďaleka nekončí. Táto vetička je totiž dosť silná na to, aby sme našli všetky podgrupy ľubovoľnej grupy $\mathbb{Z}_n$.

Vieme teda, že všetky takéto podgrupy budú cyklické, čiže každá zodpovedá nejakému prvku grupy. Tým pádom podgrúp môže byť najviac toľko, koľko je prvkov grupy. Ale môže ich byť aj menej, ako ukazuje náš príklad so $\mathbb{Z}_6$, lebo tam prvky 2 aj 4 vygenerovali grupu $\mathbb{Z}_3$ a podobne 1 aj 5 grupu $\mathbb{Z}_6$. S čím to súvisí?

Opäť si rýchlo všimneme, že v tom má prsty náš starý známy gcd. V každej podgrupe grupy $\mathbb{Z}_n$ máme totiž 0, čo môžeme písať aj ako n. Zároveň vieme, že tá podgrupa musí byť cyklická a nejaké k je jej generátorom. Lenže potom tam už nutne musí patriť aj

$\gcd(n, k)$ (jednoduchá aplikácia lemmy 1.4.1). To znamená, že všetkých podgrúp je práve toľko, koľko je rôznych čísel $\gcd(k, n)$ pre $1 \leq k \leq n$.

1.5. Úlohy

1. Overiť, že v n-prvkovej cyklickej grupe s generátorom g platí $g^n = g^0 = e$.
2. Overiť, že n-prvková cyklická grupa je izomorfná grupe $\mathbb{Z}_n$, tj. nájsť príslušné zobrazenie medzi nimi a overiť, že je to izomorfizmus.
3. Dokázať lemmu 1.3.2.
4. Nájsť explicitný vzorec pre počet podgrúp grupy $\mathbb{Z}_n$.
5. Nájsť grupu, ktorá má práve 42 podgrúp.