2 Grupy

Tuto kapitolu začneme obecnou definicí pojmu operace. Pro množinu X budeme značit $X^n = \{(x_1, x_2, ..., x_n)\ ;\ x_1, x_2, ..., x_n \in X\}$ množinu všech uspořádaných n-tic prvků X.

Definice. Zobrazení $\sigma : X^n \to X$ se nazývá *n-ární operace* na množině X.

Nejčastěji používanými operacemi jsou binární operace, tedy zobrazení $\sigma : X^2 \to X$. Připomeňme dvě základní vlastnosti, které tyto operace mohou mít:

komutativita, tedy pro všechna $x, y \in X$

$$\sigma(x, y) = \sigma(y, x)$$

a *asociativita*, pro všechna $x, y, z \in X$

$$\sigma(x, \sigma(y, z)) = \sigma(\sigma(x, y), z).$$

Obvykle se binární operace značí symboly $\cdot$, $*$ nebo $\circ$ a místo zápisu $\cdot(x, y)$ se používá zápis $x \cdot y$. Zmíněné vlastnosti $\cdot$ pak mají tvar $x \cdot y = y \cdot x$ (x a y komutují) a $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (operace je asociativní na trojici x, y, z). I my se přidržíme tohoto značení.

Pokud bude jasné, se kterou operací v dané chvíli počítáme, budeme symbol operace vynechávat, tedy místo $x \cdot y$ budeme psát pouze xy.

Definice. Množina P spolu s asociativní binární operací $\cdot$ se nazývá *pologrupa*.

Množinu P s binární operací $\cdot$ budeme zapisovat $P(\cdot)$. Pokud bude jasné, o kterou operaci půjde, budeme mluvit pouze o P.

Příklady. Asociativních binárních operací se v matematice objevuje celá řada. Uveďme alespoň několik:

- sčítání přirozených, nezáporných a celých čísel
- sčítání v tělese T (například v racionálních, reálných nebo v komplexních číslech)
- násobení ve zmíněných číselných oborech
- sčítání vektorů
- skládání permutací n-prvkové množiny
- násobení čtvercových matic řádu n.

K posledním dvěma příkladům se ještě podrobněji vrátíme.

Definice. Ať je $P(\cdot)$ pologrupa a S podmnožina P. Řekneme, že S je *podpologrupa* $P(\cdot)$, pokud pro každá $a, b \in S$ je i $a \cdot b \in S$. V tomto případě je $S(\cdot)$ opět pologrupa a říkáme, že S je *uzavřená na operaci* $\cdot$.

Příklad. Množina $k\mathbb{N} = \{kn\ ;\ n \in \mathbb{N}\}$ je podpologrupa $\mathbb{N}$.

Lemma 2.1 *Ať je P pologrupa a X nějaká podmnožina P. Pak existuje $\langle X \rangle$ vzhledem k inkluzi nejmenší podpologrupa P, která obsahuje množinu X.*

Důkaz. Dokážeme tvrzení dvěma způsoby.

1) Uvědomme si, že je-li S_i, $i \in I$, systém podpologrup P, kde I je nějaká, obecně nekonečná, indexová množina, pak je $S = \bigcap_{i \in I} S_i$ opět podpologrupa P. Totiž, je-li $a, b \in S$, pak $a, b \in S_i$ pro všechna $i \in I$, tedy $a \cdot b \in S_i$ pro každé $i \in I$ a proto $a \cdot b \in S$. Položme $\langle X \rangle = \bigcap_{S \text{ podpologrupa } P,\ X \subseteq S} S$, tedy průnik všech podpologrup P, které obsahují X. Našli jsme nejmenší podpologrupu obsahující X.

2) Položíme $\langle X \rangle = \{x_1 \cdot x_2 \cdot ... \cdot x_k \ ;\ k \in \mathbb{N} \text{ a } x_1, x_2, ..., x_k \in X\}$. Množina $\langle X \rangle$ musí být obsažená v každé podpologrupě, která obsahuje X. Zbývá dokázat, že je $\langle X \rangle$ podpologrupa P. To je ale snadné: pro $x_1 \cdot x_2 \cdot ... \cdot x_k$ a $y_1 \cdot y_2 \cdot ... \cdot y_l$ prvky $\langle X \rangle$ je jejich součin $x_1 \cdot x_2 \cdot ... \cdot x_k \cdot y_1 \cdot y_2 \cdot ... \cdot y_l$ opět prvkem X. Zkonstruovali jsme nejmenší podpologrupu obsahující X. □

Definice. Podpologrupa $\langle X \rangle$ z předchozího Lemmatu se nazývá podpologrupa P *generovaná* množinou X. Množina X je *množina generátorů* pologrupy $\langle X \rangle$.

Příklad. Uveďme několik příkladů množin generátorů:
$\mathbb{N}(+) = \langle \{1\} \rangle$, $\mathbb{N} \cup \{0\}(+) = \langle \{1, 0\} \rangle$, $\mathbb{Z}(+) = \langle \{3, -8\} \rangle$, $\mathbb{N}(\cdot) = \langle \{p \in \mathbb{N} \ ;\ p = 1 \text{ nebo } p \text{ je prvočíslo}\} \rangle$.

Úkol. Najděte S podpologrupu $\mathbb{N}(+)$, která má tříprvkovou množinu generátorů, ale nemá dvouprvkovou množinu generátorů. Pro obecné $k \in \mathbb{N}$ najděte S podpologrupu $\mathbb{N}(+)$, která má k-prvkovou množinu generátorů, ale nemá $(k-1)$-prvkovou množinu generátorů.

Pologrupy s jedním generátorem. Ať je P pologrupa s generátorem $g \in P$, tedy $\langle g \rangle = P$ (používáme zkrácené značení $\langle g \rangle$ místo správnějšího $\langle \{g\} \rangle$). Podle druhé části důkazu Lemmatu 2.1 můžeme vypsat všechny prvky P do, obecně nekonečného, seznamu

$$g, g^2, g^3, g^4, ...$$

kde g^i je zkratka za součin $g \cdot g \cdot g \cdot ... \cdot g$ délky i.

Zaveďme graf pologrupy P s jedním pevně zvoleným generátorem g takto: vrcholy grafu budou prvky P a šipky budou $a \to g \cdot a$ pro $a \in P$.

Pokud existují $i, j \in \mathbb{N}$, $i < j$, taková, že $g^i = g^j$, pak $g, g^2, g^3, ..., g^{j-2}, g^{j-1}$ jsou všechny prvky P. Tedy pologrupa P má konečně mnoho prvků, říkáme, že je *konečná*. Proveďme nyní nejmenší možnou volbu i a j.

Lemma 2.2 *Ať je P konečná pologrupa s generátorem g. Zvolme nejmenší $i \in \mathbb{N}$, pro které existuje $j > i$ tak, že $g^i = g^j$. K tomuto i zvolme nejmenší takové j. Pak jsou $g, g^2, g^3, ..., g^{j-1}$ všechny po dvou různé prvky P.*

Důkaz. Pologrupa P je konečná, proto taková i a j musí existovat. Dvojice (i, j) je nejmenší z vhodných dvojic v lexikografickém uspořádání. Je-li $g^k = g^l$ pro $1 \leq k < l \leq j - 1$, pak je jistě $k \geq i$ díky volbě i a $k > i$ díky volbě j. Dále lze všechny prvky P psát ve tvaru $g, g^2, ..., g^k, g^{k+1}, ..., g^{l-1}, g^l = g^k, g^{k+1}, ...$ a tedy $g^j = g^{j'}$ pro vhodné $k \leq j' \leq l - 1$. To je spor s volbou j. □

Graf pologrupy P vzhledem ke generátoru g v tomto případě vypadá takto:

$$g \to g^2 \to g^3 \to ... \to g^i \to g^{i+1} \to ... \to g^{j-2} \to g^{j-1} \to g^i \to g^{i+1} \to ...$$

Je to tedy $(j-i)$-členný cyklus navazující na cestu délky $i-1$.

Je-li P nekonečná, pak musí být mocniny $g^i, i \in \mathbb{N}$, po dvou různé a graf P je nekonečná cesta:

$g \to g^2 \to g^3 \to .....$

Definice. Pologrupa C s jedním generátorem g taková, že $g = g^j$ pro nějaké $j \in \mathbb{N}, j > 1$, se nazývá *konečná cyklická grupa.*

Uvědomme si, že definice nezávisí na volbě generátoru. Je-li h nějaký generátor C, pak $h = g^k$ pro vhodné $k \geq 1$ a tedy $h = g^k = (g^j)^k = g^{jk},\ jk > 1$.

Konečná cyklická grupa C má podle předchozího odstavce opravdu konečně mnoho prvků. Pro generátor g můžeme zvolit $i = 1$ a $j > 1$ nejmenší takové, že $g = g^j$. Pak má C podle Lemmatu 2.2 $(j-1)$-prvků a cyklický graf:

$$g \to g^2 \to g^3 \to ... \to g^{j-1} \to g \to ...$$

Příklad. Ať $\mathbb{C}(\cdot)$ je pologrupa násobení komplexních čísel. Zvolme $k \in \mathbb{N}$ a označme $c_k = \cos 2\pi/k + i \sin 2\pi/k$ komplexní číslo na jednotkové kružnici. Platí $c_k^k = 1$ a $c_k^{k+1} = c_k$. Podpologrupa $\langle c_k \rangle$ pologrupy $\mathbb{C}(\cdot)$ je tedy konečná cyklická grupa s k prvky. Obvykle se $\langle c_k \rangle$ nazývá grupa k-tých odmocnin z jedné.

Definice. Prvek a pologrupy P se nazývá *neutrální*, pokud pro každé $b \in P$ platí $a \cdot b = b \cdot a = b$.

Prvek a pologrupy P se nazývá *inverzní* k prvku b, pokud $ab = ba = 1$, kde 1 je neutrální prvek P. Řekneme, že v P *existují inverzní prvky*, pokud ke každému prvku P existuje inverze.

Příklad. Označme $Z(\mathbb{R})$ pologrupu všech zobrazení $\mathbb{R} \to \mathbb{R}$ s operací skládání zobrazení. $Z(\mathbb{R})$ je pologrupa s neutrálním prvkem $1_{\mathbb{R}}$ (identické zobrazení, $1_{\mathbb{R}}(x) = x$ pro všechna $x \in \mathbb{R}$). Funkce e^x nemá v $Z(\mathbb{R})$ inverzi. Dodefinujme libovolně přirozený logaritmus $\ln : \mathbb{R}^+ \to \mathbb{R}$ v nule a záporných číslech, například $\ln(y) = 0$ pro $y \leq 0$. Pak je $\ln \circ e^x = 1_{\mathbb{R}}$ ale $e^x \circ f \neq 1_{\mathbb{R}}$ pro žádné zobrazení $f : \mathbb{R} \to \mathbb{R}$.

Lemma 2.3 *Ať je C pologrupa s jedním generátorem. Pak C je konečná cyklická grupa právě když má neutrální prvek a existují v ní inverzní prvky.*

Důkaz. Předpokládejme, že C je konečná cyklická grupa s generátorem g, a $j \in \mathbb{N}, j > 1$, ať je takové, že $g = g^j$. Počítejme pro $k \in \mathbb{N}$: $g^{j-1} \cdot g^k = g^j \cdot g^{k-1} = g \cdot g^{k-1} = g^k$ a podobně $g^k \cdot g^{j-1} = g^k$. Našli jsme neutrální prvek $1 = g^{j-1}$. Zbývá pro $a \in C$ najít inverzi. Musí být $a = g^l$ pro nějaké $l = 1, 2, ..., j-1$. Pokud je $l = j-1$, pak $a = 1$ a je samo k sobě inverzní. Je-li $l < j-1$, položme $b = g^{j-1-l}$ a máme $a \cdot b = g^l \cdot g^{j-1-l} = g^{l+j-1-l} = g^{j-1} = 1 = b \cdot a$.

Ať je naopak C pologrupa s jedním generátorem g, která má neutrální prvek, označme ho 1. Musí existovat $k \in \mathbb{N}$, $k \geq 1$, tak, že $g^k = 1$. Pak je ale $g^{k+1} = g^k \cdot g = 1 \cdot g = g$, $k+1 > 1$, a podle definice je C konečná cyklická grupa. □

Předchozí tvrzení vede k obecné definici grupy.

Definice. Pologrupa G se nazývá *grupa*, pokud má G neutrální prvek a v G existují inverzní prvky.

Příklady. 1) Pologrupy $\mathbb{Z}(+)$, sčítání v tělesech a sčítání ve vektorových prostorech jsou grupy. Používá se pro ně aditivní zápis, tedy neutrální prvek značíme 0 a inverzní prvek k a značíme $-a$.

2) Pologrupy $(T \setminus \{0\})(\cdot)$ násobení nenulových prvků tělesa T, dále skládání permutací n-prvkové množiny nebo násobení *regulárních* matic řádu n jsou grupy. Zapisujeme je multiplikativně, tedy neutrální prvek je 1 a prvek inverzní k a je a^{-1}.

V grupě jsou neutrální prvek i inverzní prvky *jednoznačně určené*. Ať a, a' jsou dva neutrální prvky grupy G. Musí být $a' = a \cdot a' = a$. Jsou-li b a b' prvky inverzní k a, pak $b = b \cdot 1 = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = 1 \cdot b' = b'$.

Definice. Ať je G grupa a H podmnožina G. Řekneme, že H je *podgrupa* G, pokud je H podpologrupa G, $1 \in H$ a pro každé $a \in H$ je i $a^{-1} \in H$, kde 1 značí neutrální prvek a a^{-1} inverzi k a v G. V tomto případě říkáme, že H je *uzavřená na* $\cdot$, 1 a inverzní prvky, a píšeme $H \leq G$.

Lemma 2.4 *Ať je G konečná grupa a H podpologrupa G. Pak je H podgrupa G.*

Důkaz. Chceme ukázat, že $1 \in H$ a $a^{-1} \in H$ pro každé $a \in H$. Zvolme $a \in H$. Množina $\{a^i \ ; \ i \in \mathbb{N}\} \subseteq H$ je konečná a tudíž $a^i = a^j$ pro nějaké $i < j$. V G existuje $a^{-i} = (a^i)^{-1}$ a můžeme krátit $1 = a^{j-i} \in H$. Pokud je $j - i = 1$, pak $a = 1 = a^{-1}$. Pro $j - i > 1$ z rovnosti $1 = a^{j-i} = a \cdot a^{j-i-1} = a^{j-i-1} \cdot a$ plyne $a^{-1} = a^{j-i-1} \in H$. □

V konečných grupách tedy podpologrupy splývají s podgrupami a můžeme podle předchozího Lemmatu a Lemmatu 2.1 mluvit o *podgrupě generované podmnožinou* $X \subseteq G$, která má tvar ukázaný v druhé části důkazu Lemmatu 2.1. Vidíme také, že v konečných grupách jsou *grupové generátory* totéž co pologrupové generátory.

Definice konečné cyklické grupy má proto podle Lemmat 2.3 a 2.4 ekvivalentní tvar:

Grupa C je konečná cyklická právě když je konečná a má jeden generátor.

Ať je nyní H podgrupa grupy G. Definujme na G relaci $\sim_H$ takto: $g \sim_H k$, pokud existuje $h \in H$ tak, že $gh = k$. Můžeme říci, že se g a k "liší zprava o prvek H". Uvědomme si, že $\sim_H$ je ekvivalence. Nejprve $g \cdot 1 = g$ a tedy $g \sim_H g$, dále je-li $gh = k$, pak $g = kh^{-1}$ a proto z $g \sim_H k$ plyne $k \sim_H g$. Zbývá tranzitivita: z $g = kh$ a $k = lh'$ dostaneme $g = (lh')h = l(h'h)$. Využili jsme všechny tři vlastnosti podgrupy.

Definice. Třídy ekvivalence $\sim_H$ se nazývají *pravé rozkladové třídy* grupy G podle podgrupy H. Pro $g \in G$ lze tedy pravou rozkladovou třídu g podle H zapsat ve tvaru $gH = \{gh\ ;\ h \in H\}$.

Lemma 2.5 *Pro H podgrupu konečné grupy G a $g \in G$ platí rovnosti $|gH| = |Hg| = |H|$.*

Důkaz. Stačí se zabývat pravými rozkladovými třídami, pro levé rozkladové třídy Hg je situace symetrická. Stačí dokázat, že zobrazení $h \to gh$ je bijekce množin H a gH. Toto zobrazení je jistě *na*, zbývá uvědomit si, že pokud $gh = gh'$, pak $g^{-1}(gh) = g^{-1}(gh')$ a $h = h'$. □

Věta 2.6 (Lanrangeova věta) *Pro H podgrupu konečné grupy G platí $|H| \mid |G|$.*

Důkaz. Všechny (pravé) rozkladové třídy podle H mají $|H|$-prvků, tedy $|H| \mid |G|$ a $|G|/|H|$ je počet (pravých) rozkladových tříd G podle H. □

Příklad. Z lineární algebry víte, že $\mathbb{Z}_p$ je těleso pro p prvočíslo. Násobení na tělese je asociativní (a komutativní), má neutrální prvek 1 a k nenulovým prvkům existují inverze. Množina $\{1, 2, ..., p-1\}$ s násobením modulo p je tedy grupa, označme ji $\mathbb{Z}_p^*$. Pro $a \in \mathbb{Z}_p^*$ je $\langle a \rangle \leq \mathbb{Z}_p^*$ konečná cyklická grupa s j prvky, kde j je nejmenší takové, že $a^j = 1$ (modulo p). Podle Lagrangeovy věty musí být $|\mathbb{Z}_p^*| = p - 1 = j \cdot l$ pro vhodné $l \in \mathbb{N}$. Dostáváme $a^{p-1} = a^{jl} = (a^j)^l = 1^l = 1$ pro $a \in \mathbb{Z}_p^*$. Jinými slovy:

$$a^{p-1} \equiv_p 1$$

pro p prvočíslo, $a \in \mathbb{N}$, p nedělí a. Dokázané tvrzení se nazývá Malá Fermatova věta.

Definice. Zobrazení $f : P(\cdot) \to S(\circ)$ pologrup $P(\cdot)$ a $S(\circ)$ se nazývá *homomorfismus*, pokud platí pro všechna $a, b \in P$ rovnost $f(a \cdot b) = f(a) \circ f(b)$. Prostý homomorfismus nazýváme *monomorfismus*, homomorfismus na *epimorfismus* a bijektivní homomorfismus *izomorfismus*.

Úkol. Ukažte, že pologrupa, která je izomorfní grupě, musí být také grupa.

Příklady. 1) Znaménko permutace je zobrazení z množiny všech permutací na n prvcích do množiny $\{1, -1\}$. Je to homomorfismus vzhledem k operacím skládání permutací a násobení celých čísel. Příslušné pravidlo je:

$$\mathrm{sgn}(\sigma \circ \pi) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\pi).$$

2) Determinant přiřazuje dané matici (nad tělesem, například $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$) skalár z tělesa. Je to homomorfismus vzhledem k násobení matic a násobení skalárů v tělese, tedy:

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

3) Zobrazení $a + ib \mapsto a - ib = \overline{a + ib}$, které danému komplexnímu číslu přiřadí komplexně sdružené číslo, je homomorfismus vzhledem ke sčítání i vzhledem k násobení komplexních čísel. Jinými slovy:

$$\overline{c + d} = \overline{c} + \overline{d}$$

$$\overline{c \cdot d} = \overline{c} \cdot \overline{d}.$$

Zobrazení $|| \; || : \mathbb{C} \to \mathbb{R}$, které danému komplexnímu číslu přiřadí jeho velikost, $||a+ib|| = \sqrt{a^2 + b^2}$, je homomorfismus vzhledem k operacím násobení na $\mathbb{C}$ a $\mathbb{R}$:

$$||c \cdot d|| = ||c|| \cdot ||d||.$$