NOVÝ ÚVOD DO TEORIE GRUP

DAVID STANOVSKÝ

1. Příklady a základní vlastnosti

Motivací teorie grup je především studium nejrůznějších symetrií matematických objektů. Pojem pochází z Galoisovy teorie a původně označoval množinu (skupinu) permutací G uzavřenou na skládání, tj. splňující $\pi \circ \sigma \in G$ pro všechna $\pi, \sigma \in G$. Abstrakcí tohoto pojmu vznikla rozsáhlá větev algebry, zvaná teorie grup. Aplikace nachází mimo jiné v kombinatorice (zejména teorie konečných grup) a geometrii (zejména teorie reprezentací, zkoumající maticové grupy).

Teorie abelovských grup se výrazně liší od teorie grup obecně nekomutativních. Abelovské grupy připomínají vektorové prostory (viz Tvrzení 1.2) a z tohoto pohledu pochází většina metod k jejich studiu. Aplikace často vedou do teorie čísel.

Definice. *Grupou* rozumíme čtveřici $\mathbf{G} = (G, *, ', e)$, kde G je množina, na které jsou definovány binární operace $*$, unární operace $'$ a konstanta e splňující pro každé $a, b, c \in G$ následující podmínky:

$$a * (b * c) = (a * b) * c, \qquad a * e = e * a = a, \qquad a * a' = a' * a = e.$$

Grupu nazýváme *abelovskou*, pokud navíc pro všechna $a, b \in G$ platí

$$a * b = b * a.$$

Prvku e se říká *jednotka*, prvku a' *inverzní prvek* k prvku a.

Formálně rozlišujeme mezi množinou G, tzv. *nosnou množinou*, a čtveřicí $\mathbf{G} = (G, *, ', e)$, která navíc obsahuje informaci o algebraické struktuře definované na množině G. V konkrétních příkladech bývá typickou trojicí operací buď $+, -, 0$, pak hovoříme o *aditivním zápise* (a místo $x + (-y)$ píšeme $x - y$), anebo trojice $\cdot, ^{-1}, 1$, čemuž říkáme *multiplikativní zápis*.

Definice. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $H \subseteq G$ podmnožina její nosné množiny taková, že $e \in H$ a pro každé $a, b \in H$ platí

$$a' \in H \quad \text{a} \quad a * b \in H.$$

Pak říkáme, že H *tvoří podgrupu* grupy $\mathbf{G}$. Čtveřici $\mathbf{H} = (H, *|_H, '|_H, e)$ pak nazýváme *podgrupou*, přičemž $|_H$ značí restrikci operací na množinu H. Je zřejmé, že podgrupa skutečně splňuje podmínky z definice grupy. Fakt, že $\mathbf{H}$ je podgrupou $\mathbf{G}$, značíme $\mathbf{H} \leq \mathbf{G}$. Podgrupy $\mathbf{G}$ a $\{e\}$ nazýváme *nevlastní*.

Začneme příklady abelovských grup. Důležité příklady jsou odvozeny od komutativních okruhů.

Příklad. Buď $\mathbf{R}$ komutativní okruh s jednotkou. Pak $(R, +, -, 0)$ je abelovská grupa, tzv. *aditivní grupa* okruhu $\mathbf{R}$. Za všechny příklady uveďme např. číselné grupy $\mathbb{Z} = (\mathbb{Z}, +, -, 0)$ a $\mathbb{Z}_n = (\{0, 1, \ldots, n-1\}, +_{\bmod n}, -_{\bmod n}, 0)$ s operacemi $+, -$ modulo n.

Příklad. Buď $\mathbf{R}$ komutativní okruh s jednotkou, označme R^* množinu všech invertibilních prvků v $\mathbf{R}$. Pak $\mathbf{R}^* = (R^*, \cdot, ^{-1}, 1)$ je abelovská grupa, tzv. *multiplikativní grupa* okruhu $\mathbf{R}$. (Je třeba si uvědomit, že 1 je invertibilní prvek, že inverz invertibilního prvku je invertibilní, a především, že součin dvou invertibilních prvků a, b je invertibilní — jeho inverzem je $(ab)^{-1} = a^{-1}b^{-1}$.) Příklady:

- Je-li $\mathbf{R}$ těleso, pak $\mathbf{R}^* = (R \setminus \{0\}, \cdot, ^{-1}, 1)$.
- Pro $\mathbf{R} = \mathbb{Z}$ je $\mathbb{Z}^* = (\{1, -1\}, \cdot, ^{-1}, 1)$.
- Pro polynomiální okruhy platí $\mathbf{R}[x]^* = \mathbf{R}^*$, protože invertibilní jsou právě konstantní polynomy invertibilní v $\mathbf{R}$.
- Důležitým příkladem jsou grupy $\mathbb{Z}_n^*$. Prvky této grupy jsou právě všechna čísla $a \in \{1, \ldots, n-1\}$ nesoudělná s n. Na jednu stranu, soudělná čísla invertibilní nejsou: je-li $d \nmid 1$ společný dělitel a, n, pak $d \mid (ab \bmod n)$ pro libovolné b, takže součin ab nikdy nemůže být 1. Naopak, jsou-li a, n nesoudělná, vezměme Bézoutovy koeficienty u, v splňující $1 = \mathrm{NSD}(a, n) = ua + vn$. Podíváme-li se na rovnost modulo n, dostaneme $1 \equiv ua \pmod{n}$, a tedy
$$a^{-1} = u \bmod n.$$
(Alternativně, inverzní prvek je možné nalézt pomocí Eulerovy věty: vhledem k tomu, že $a^{\varphi(n)} \equiv 1 \pmod{n}$, máme $a^{-1} = a^{\varphi(n)-1} \bmod n$. Tento postup je však výpočetně mnohem náročnější.)

Řadu příkladů lze sestrojit jako podgrupy jiných grup. Spoustu možností nabízí například multiplikativní grupa $\mathbb{C}^*$.

Příklad. Komplexní jednotky, tj. množina $\{z \in \mathbb{C} : |z| = 1\}$, tvoří podgrupu grupy $\mathbb{C}^*$. Mezi jejími podgrupami dále jmenujme např. grupy $\mathbb{C}_n$ sestávající ze všech kořenů polynomu $x^n - 1$ a tzv. *Prüferovu p-grupu* $\mathbb{C}_{p^\infty} = \bigcup_{k=1}^{\infty} \mathbb{C}_{p^k}$ sestávající ze všech komplexních čísel z splňujících $z^{p^k} = 1$ pro nějaké k. Prüferova grupa je v teorii grup oblíbeným protipříkladem na řadu vlastností.

Existuje řada geometrických i algebraických konstrukcí abelovských grup, z nichž některé mají významné aplikace v geometrii, ale také třeba v kryptografii — například grupy odvozené od eliptických křivek (viz Diffie-Hellmanův protokol v Sekci 4.3).

Většina příkladů neabelovských grup je odvozena od dvou základních konstrukcí: *symetrické grupy* všech permutací na dané množině a *lineární grupy* všech regulárních matic daného rozměru nad daným tělesem.

Příklad. *Symetrická grupa* sestává z permutací na dané neprázdné množině X s operacemi $\circ$ skládání permutací, $^{-1}$ invertování permutací a konstantou $id : x \mapsto x$ (identické zobrazení), tj.
$$\mathbf{S}_X = (\{\pi : \pi \text{ je permutace na množině } X\}, \circ, ^{-1}, id).$$
Je-li $X = \{1, \ldots, n\}$, pak místo $\mathbf{S}_X$ píšeme $\mathbf{S}_n$. Mezi podgrupami $\mathbf{S}_n$ zmiňme např.

- *alternující grupu* $\mathbf{A}_n$ všech sudých permutací;
- *dihedrální grupu* $\mathbf{D}_{2n}$ všech symetrií pravidelného n-úhelníka, jakožto grupu permutací na množině jeho vrcholů (tato grupa sestává z n otočení a n osových symetrií, proto značení $\mathbf{D}_{2n}$);
- nejrůznější grupy symetrií geometrických těles, automorfismů grafů a dalších matematických struktur, apod.

Příklad. *Obecná lineární grupa* nad tělesem $\mathbf{T}$ sestává z regulárních matic dané velikosti s operacemi $\cdot$ maticového násobení, $^{-1}$ maticového invertování a konstantou E, jednotkovou maticí, tj.

$$\mathbf{GL}_n(\mathbf{T}) = (\{A : A \text{ je regulární matice } n \times n \text{ nad tělesem } \mathbf{T}\}, \cdot, ^{-1}, E),$$

Mezi jejími podgrupami zmiňme např.

- *speciální lineární grupu* $\mathbf{SL}_n(\mathbf{T})$ všech matic s determinantem 1;
- *ortogonální grupu* $\mathbf{O}_n(\mathbf{T})$ všech ortogonálních matic, tj. takových A, co splňují $AA^T = E$. (Nad tělesem $\mathbb{R}$ to odpovídá maticím, jejichž řádky, resp. sloupce, jsou ortonormální vektory vzhledem k standardnímu skalárnímu součinu.)

Příkladem grupy, která nemá přirozenou definici jako permutační ani lineární grupa, je např. osmiprvková grupa všech jednotkových kvaternionů.

Příklad. *Kvaternionová grupa* $\mathbf{Q}$ na množině $\{\pm 1, \pm i, \pm j, \pm k\}$ s násobením daným předpisy

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j,$$

a dále pravidly $xy = -(yx)$ a $(-x)y = x(-y) = -(xy)$ pro všechna $x, y \in \{i, j, k\}$.

Symetrické a lineární grupy jsou v jistém smyslu charakteristické příklady. Každá grupa je *je izomorfní* (viz Sekce **??**) s nějakou podgrupou nějaké symetrické grupy (*Cayleyova reprezentace*, Věta **??**). A každá konečná grupa je izomorfní s nějakou podgrupou nějaké obecné lineární grupy nad libovolným tělesem (*lineární reprezentace*, Věta **??**).

Definice. *Direktním součinem* grup $\mathbf{G}_i = (G_i, *_i, {}'^i, e_i)$, $i = 1, \ldots, n$, rozumíme grupu

$$\mathbf{G}_1 \times \cdots \times \mathbf{G}_n = (G_1 \times \cdots \times G_n, *, ', e),$$

jejíž operace jsou definovány po složkách, tj.

$$\begin{aligned}(a_1, \ldots, a_n) * (b_1, \ldots, b_n) &= (a_1 *_1 b_1, \ldots, a_n *_n b_n),\\ (a_1, \ldots, a_n)' &= ((a_1)'^1, \ldots, (a_n)'^n),\\ c &= (c_1, \ldots, c_n).\end{aligned}$$

pro všechna $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \ldots \times G_n$. Je snadné ověřit, že direktní součin skutečně splňuje podmínky z definice grupy.

Přestože existuje řada nejrůznějších konstrukcí konečných abelovských grup, ve skutečnosti jich je, *až na izomorfismus*, poměrně málo: Věta **??** říká, že každá konečná abelovská grupa je izomorfní direktnímu součinu cyklických grup

$$\mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_n^{k_n}},$$

kde $p_1^{k_1}, \ldots, p_n^{k_n}$ jsou nějaké mocniny prvočísel. (Nekonečné abelovském grupy jednoduše charakterizovat nelze.)

Oblíbenou kratochvílí je hledání malých grup. Následující tabulka obsahuje úplný seznam (až na izomorfismus) všech n-prvkových grup pro $n \leq 11$ a $n = p, 2p, p^2$, kde p je prvočíslo. V současné době je znám seznam všech grup až do velikosti $2047 = 2^{11} - 1$.

n	grupy s n prvky
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ \mathbf{S}_3 = \mathbf{D}_6$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbf{D}_8,\ \mathbf{Q}$
	$\dots$
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p$
$2p$	$\mathbb{Z}_{2p},\ \mathbf{D}_{2p}$

Podobně jako u oborů integrity, definice grupy obsahuje minimální množství podmínek. Následující tvrzení ukazuje několik aritmetických pravidel, které z definice snadno plynou a v dalším textu je budeme zcela automaticky používat.

Tvrzení 1.1. *Buď* $\mathbf{G} = (G, *, ', e)$ *grupa a* $a, b, c \in G$. *Pak*

(1) *jestliže* $a * c = b * c$ *nebo* $c * a = c * b$, *pak* $a = b$ (krácení);
(2) *jestliže* $a * u = a$ *nebo* $u * a = a$ *pro nějaké* $u \in A$, *pak* $u = e$ (jednoznačnost jednotky);
(3) *jestliže* $a * u = e$ *nebo* $u * a = e$ *pro nějaké* $u \in A$, *pak* $u = a'$ (jednoznačnost inverzních prvků);
(4) $(a')' = a$;
(5) $(a * b)' = b' * a'$.

Důkaz. (1) Je-li $a * c = b * c$, pak také $(a * c) * c' = (b * c) * c'$ a použitím všech tří axiomů dostaneme $(a * c) * c' = a * (c * c') = a * e = a$ a podobně $(b * c) * c' = b$. Tedy $a = b$. Analogicky pro $c * a = c * b$.

(2) Je-li $a * u = a = a * e$, krácením dostáváme $u = e$. Analogicky pro $u * a = a$.

(3) Je-li $a * u = e = a * a'$, krácením dostáváme $u = a'$. Analogicky pro $u * a = e$.

(4) Protože $a' * a = e$, z jednoznačnosti inverzních prvků dostáváme $a = (a')'$.

(5) Protože $(a*b)*(b'*a') = a*(b*b')*a' = a*e*a' = a*a' = e$, z jednoznačnosti inverzních prvků dostáváme $(a * b)' = b' * a'$. □

Důležitou roli hrají v grupách mocniny. Buď $\mathbf{G} = (G, *, ', e)$ grupa, $a \in G$, $n \in \mathbb{Z}$. Označme

$$n \times a = \begin{cases} e & n = 0 \\ \underbrace{a * a * \cdots * a}_{n} & n > 0 \\ \underbrace{a' * a' * \cdots * a'}_{-n} & n < 0 \end{cases}$$

Uvědomte si, co tento zápis znamená v aditivním nebo multiplikativním zápise:

- v aditivním případě je mocninou $n \cdot a = a + \ldots + a$, resp. $(-a) + \ldots + (-a)$,
- v multiplikativním případě je mocninou $a^n = a \cdot \ldots \cdot a$, resp. $a^{-1} \cdot \ldots \cdot a^{-1}$.

Od tohoto místa dále budeme ve všech tvrzeních a důkazech uvažovat grupy v multiplikativním zápise. U tvrzení, kde by překlad do aditivní formy mohl činit obtíže, situaci vysvětlíme.

Tvrzení 1.2. *Buď* $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *grupa,* $a, b \in G$ *a* $k, l \in \mathbb{Z}$*. Pak*

$$a^{k+l} = a^k \cdot a^l, \qquad a^{kl} = (a^k)^l = (a^l)^k$$

a je-li $\mathbf{G}$ *abelovská, pak navíc*

$$(ab)^k = a^k b^k.$$

Důkaz. Pokud $k, l > 0$, ihned vidímě, že počet prvků a ve výrazu na obou stranách každé rovnosti je stejný. V případě záporných exponentů je třeba vzít v úvahu, že a a a^{-1} se navzájem pokrátí. Např. v první rovnosti, pro $k > 0 > l$, $|l| < |k|$, máme na levé straně součin $k + l$ prvků a, zatímco na pravé straně součin k prvků a a $-l$ prvků a^{-1}. Po vykrácení dostaneme rovnost obou výrazů. Ostatní případy se rozeberou podobně. □

V aditivním zápise Tvrzení 1.2 říká následující:

$$(k + l) \cdot a = k \cdot a + l \cdot a, \qquad (kl) \cdot a = k \cdot (l \cdot a), \qquad k \cdot (a + b) = k \cdot a + k \cdot b,$$

poslední rovnost samozřejmě platí pouze pro abelovské grupy. Pokud vám tyto podmínky připomínají definici vektorového prostoru, jste na správně stopě. Jak bylo řečeno výše, teorie abelovských grup je skutečně teorií „vektorových prostorů nad $\mathbb{Z}$“, odborně $\mathbb{Z}$-modulů (viz Sekce **??**).

2. Podgrupy a řády prvků

2.1. Generátory.

Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa. Připomeňme, že podmnožina $H \subseteq G$ tvoří podgrupu, pokud $e \in H$, $a^{-1} \in H$ a $a \cdot b \in H$ pro každé $a, b \in H$.

Lemma 2.1. *Průnik podgrup je podgrupa.*

Důkaz. Uvažujme podgrupy $\mathbf{H}_i$, $i \in I$, dané grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$. Označme $H = \bigcap_{i \in I} H_i$. Dokážeme, že množina H splňuje výše uvedenou podmínku. Protože $e \in H_i$ pro všechna $i \in I$, bude e náležet i jejich průniku H. Nyní uvažujme $a, b \in H$. Tyto leží v každém H_i a díky uzavřenosti na operace tam náleží také prvky a^{-1} a $a \cdot b$. Takže tyto prvky leží i v průniku všech H_i, čili v H. □

Uvažujme podmnožinu $X \subseteq G$ grupy $\mathbf{G}$. Podgrupou *generovanou množinou* X rozumíme nejmenší podgrupu (vzhledem k inkluzi) grupy $\mathbf{G}$ obsahující podmnožinu X, značíme ji $\langle X \rangle_{\mathbf{G}}$. Taková podgrupa jistě existuje: stačí vzít průnik všech podgrup obsahujících množinu X, tj.

$$\langle X \rangle_{\mathbf{G}} = \bigcap_{X \subseteq H \leq G} H.$$

Podle předchozího lemmatu jde skutečně o podgrupu, mezi všemi podgrupami obsahujícími množinu X bude nejmenší.

Tvrzení 2.2. *Buď* $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *grupa a* $\emptyset \neq X \subseteq G$*. Pak*

$$\langle X \rangle_{\mathbf{G}} = \{x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n} : \ n \in \mathbb{N},\ x_1, \ldots, x_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Důkaz. Označme M množinu z pravé strany uvedené rovnosti. Každý prvek M je obsažen v každé podgrupě $\mathbf{H}$, která obsahuje množinu X, protože $x_i \in X \subseteq H$ pro všechna i, tedy $x_i^{k_i} \in H$, a tudíž také $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \in H$. Tedy M je obsaženo v průniku všech takových podgrup H. Zbývá ověřit, že M skutečně tvoří podgrupu. Součin dvou prvků z M je jistě v M, jednotka $1 = x \cdot x^{-1}$ je tam také, a pro $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \in M$ platí $(x_1^{k_1} \cdot \ldots \cdot x_n^{k_n})^{-1} = x_n^{-k_n} \cdot \ldots \cdot x_1^{-k_1} \in M$. □

Uvědomte si, že v aditivním zápise, tj. pro grupu $\mathbf{G} = (G, +, -, 0)$, dostáváme

$$\langle X\rangle_{\mathbf{G}} = \{k_1x_1 + k_2x_2 + \ldots + k_nx_n : \ n \in \mathbb{N},\ x_1, \ldots, x_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Je-li $\mathbf{G}$ abelovská grupa a $X = \{a_1, \ldots, a_n\}$ konečná množina, prvky podgrupy generované množinou X lze vyjádřit jednodušším způsobem: díky komutativitě můžeme sečíst mocniny stejných prvků a dostaneme (v aditivním zápise)

$$\langle a_1, \ldots, a_n\rangle_{\mathbf{G}} = \{k_1a_1 + k_2a_2 + \ldots + k_na_n : \ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Příklady. Jedním typem úlohy je zjistit, jaké prvky obsahuje podgrupa dané grupy generovaná danou podmnožinou.

- $\langle 1+i, 3-i\rangle_{\mathbb{C}} = \{k(1+i)+l(3-i) : k, l \in \mathbb{Z}\} = \{(k+3l)+(k-l)i : k, l \in \mathbb{Z}\}$.
- $\langle 1+i, 3-i\rangle_{\mathbb{C}^*} = \{(1+i)^k \cdot (3-i)^l : k, l \in \mathbb{Z}\}$.
- $\langle a, b\rangle_{\mathbb{Z}} = \{ka + lb : k, l \in \mathbb{Z}\} = \langle \mathrm{NSD}(a, b)\rangle_{\mathbb{Z}}$ díky Bézoutově rovnosti.

Příklady. Druhým typem úlohy je, dána grupa $\mathbf{G}$, najděte co nejmenší množinu generátorů, tj. podmnožinu $X \subseteq G$ takovou, že $\mathbf{G} = \langle X\rangle_{\mathbf{G}}$.

- $\mathbb{Z} = \langle 1\rangle$, $\mathbb{Z}_n = \langle 1\rangle$.
- $\mathbb{Z}_7^* = \langle 3\rangle$, ale $\mathbb{Z}_8^*$ nelze generovat jedním prvkem; platí $\mathbb{Z}_8^* = \langle 3, 5\rangle$.
- $\mathbf{S}_n = \langle T\rangle$, kde T je množina všech transpozic, viz Tvrzení 3.2.

2.2. Řád prvku.

Řádem grupy $\mathbf{G}$ rozumíme počet prvků její nosné množiny, značíme jej $|\mathbf{G}|$ (tj., formálně vzato, $|\mathbf{G}| = |G|$). *Řádem prvku* a v grupě $\mathbf{G}$ se rozumí řád grupy $\langle a\rangle_{\mathbf{G}}$ a značí se $\mathrm{ord}(a)$. Je-li tato podgrupa nekonečná, rozumí se $\mathrm{ord}(a) = \infty$.

Tvrzení 2.3. *Buď* $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *grupa a* $a \in G$. *Pak* $\mathrm{ord}(a)$ *je rovno nejmenšímu* $n \in \mathbb{N}$ *takovému, že* $a^n = 1$, *pokud takové* n *existuje, resp.* ∞ *v opačném případě.*

Důkaz. Podle Tvrzení 2.2 je

$$\langle a\rangle_{\mathbf{G}} = \{a^{k_1} \cdot a^{k_2} \cdot \ldots \cdot a^{k_n} : n \in \mathbb{N},\ k_1, \ldots, k_n \in \mathbb{Z}\} = \{a^k : k \in \mathbb{Z}\}.$$

Všimněte si, že $a^i = a^j$ právě tehdy, když $a^{i-j} = 1$. Pokud tedy žádné $n \in \mathbb{N}$ s vlastností $a^n = 1$ neexistuje, uvedené prvky podgrupy $\langle a\rangle_{\mathbf{G}}$ jsou po dvou různé a tato podgrupa je nekonečná. Uvažujme nadále nejmenší $n \in \mathbb{N}$ takové, že $a^n = 1$. Pak $a^0, a^1, \ldots, a^{n-1}$ jsou po dvou různé prvky podgrupy $\langle a\rangle_{\mathbf{G}}$. Na druhou stranu, každá mocnina a^m je rovna některému z těchto prvků: pro $q = m \operatorname{div} n$, $r = m \bmod n$ platí

$$a^m = a^{qn+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = a^r.$$

Tedy $\langle a\rangle_{\mathbf{G}} = \{a^0, a^1, \ldots, a^{n-1}\}$ obsahuje přesně n prvků. □

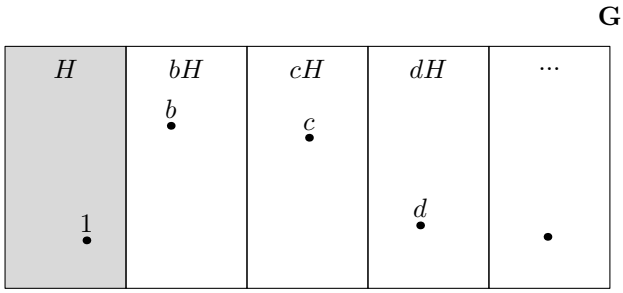
V aditivním zápise je tedy řád prvku a roven nejmenšímu n takovému, že $n \cdot a = 0$. Pozor, řád prvku záleží na zvolené grupě! Např.

- $\mathrm{ord}(3) = 8$ v grupě $\mathbb{Z}_8$, protože $8 \cdot 3 \equiv 0 \pmod 8$, ale $n \cdot 3 \not\equiv 0 \pmod 8$ pro $n = 1, \ldots, 7$;
- $\mathrm{ord}(3) = 2$ v grupě $\mathbb{Z}_8^*$, protože $3^2 \equiv 1 \pmod 8$, ale $3^1 \not\equiv 1 \pmod 8$.

Příklady. V nekonečných grupách mohou řády vycházet všelijak:

- v grupě $\mathbb{Z}$ platí $\mathrm{ord}(0) = 1$ a $\mathrm{ord}(a) = \infty$ pro všechna $a \neq 0$;
- v grupě $\mathbb{C}^*$ existuje prvek libovolného řádu: $\mathrm{ord}(e^{2\pi i/k}) = k$ a $\mathrm{ord}(z) = \infty$ kdykoliv $|z| \neq 1$.

Příklady. V konečných grupách nikoliv:



Obrázek 1. Rozklad grupy **G** podle podgrupy **H** a jeho transverzála.

- v grupě $\mathbb{Z}_6$ je $\mathrm{ord}(0) = 1$, $\mathrm{ord}(1) = 6$, $\mathrm{ord}(2) = 3$, $\mathrm{ord}(3) = 2$, $\mathrm{ord}(4) = 3$ a $\mathrm{ord}(5) = 6$;
- v grupě $\mathbb{Z}_7^*$ je $\mathrm{ord}(1) = 1$, $\mathrm{ord}(2) = 3$, $\mathrm{ord}(3) = 6$, $\mathrm{ord}(4) = 3$, $\mathrm{ord}(5) = 6$ a $\mathrm{ord}(6) = 2$.

Všimněte si, že v uvedených příkladech konečných grup řád každého prvku dělí řád celé grupy. To není náhoda, nýbrž pravidlo, které je speciálním případem Lagrangeovy věty 2.4, kterou si nyní ukážeme. Další restrikce ohledně řádů prvků se pak dozvíme v sekci o cyklických grupách.

2.3. **Lagrangeova věta.**

Lagrangeova věta říká, že řád podgrupy dělí řád celé grupy. Myšlenka důkazu je jednoduchá: celou grupu rozložíme na několik podmnožin, které jsou po dvou disjunktní a stejně velké jako daná podgrupa. Nesamozřejmou částí důkazu je konstrukce tohoto rozkladu.

Definice. Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa a **H** její podgrupa:

- množiny $aH = \{ah : h \in H\}$, $a \in G$, se nazývají *rozkladové třídy* podgrupy **H**;
- množina všech rozkladových tříd $\{aH : a \in G\}$ se nazývá *rozkladem* grupy **G** podle podgrupy **H**;
- počet rozkladových tříd se nazývá *index* podgrupy **H** v grupě **G** a značí se $[\mathbf{G} : \mathbf{H}] = |\{aH : a \in G\}|$;
- podmnožina $T \subseteq G$ s vlastností $|T \cap aH| = 1$ pro každé $a \in G$ se nazývá *transverzála* rozkladu **G** podle **H**.

Pojmy, které jsme definovali, se někdy používají s přívlastkem *levý*, tj. levé rozkladové třídy, levý rozklad, levá transverzála. Pravými rozkladovými třídami pak rozumíme množiny $Ha = \{ha : h \in H\}$ a ostatní pojmy se definují analogicky. Z Lemmatu 2.9 plyne, že velikost levého a pravého rozkladu je stejná, tedy index podgrupy nezávisí na volbě strany.

Příklad. Buď $\mathbf{G} = \mathbb{Z}$ a $\mathbf{H} = \{x \in \mathbb{Z} : n \mid x\}$. Rozkladovou třídu určenou prvkem $a \in \mathbb{Z}$ můžeme vyjádřit jako

$$aH = \{a + h : \ h \in H\} = \{a + nk : \ k \in \mathbb{Z}\} = \{x \in \mathbb{Z} : \ x \equiv a \pmod{n}\}.$$

Dvě rozkladové třídy aH, bH jsou buď stejné, nebo disjunktní, přičemž $aH = bH$ právě tehdy, když $n \mid (a-b)$, tedy $a \equiv b \pmod{n}$. Dostáváme tak n různých rozkladových tříd, tedy $[\mathbf{G} : \mathbf{H}] = n$. Jako transverzálu lze zvolit např. $T = \{0, \ldots, n-1\}$, množinu všech možných zbytků po dělení n.

Příklad. Buď $\mathbf{G} = \mathbf{S}_n$ a $\mathbf{H} = \mathbf{A}_n$. Pak $\pi \circ A_n = A_n \circ \pi = A_n$ pro libovolnou π sudou a $\pi \circ A_n = A_n \circ \pi$ sestává ze všech lichých permutací pro libovolnou π lichou. Grupa $\mathbf{S}_n$ se tedy rozkládá na dvě rozkladové třídy (levé i pravé jsou stejné), $[\mathbf{S}_n : \mathbf{A}_n] = 2$ a jako transverzálu lze zvolit např. $T = \{id, (1\ 2)\}$.

Levé a pravé rozkladové třídy nemusí být vždy stejné, nejmenším příkladem je následující situace.

Příklad. Buď $\mathbf{G} = \mathbf{S}_3$ a $\mathbf{H} = \{id, (1\ 2)\}$. Snadno spočteme, že levý i pravý rozklad obsahuje tři dvouprvkové třídy, avšak

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}, \quad \text{ale} \quad H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}.$$

Nyní můžeme zformulovat slibovanou Lagrangeovu větu.

Věta 2.4 (Lagrangeova)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pak*

$$|\mathbf{G}| = |\mathbf{H}| \cdot [\mathbf{G} : \mathbf{H}].$$

Znění věty dává smysl i pro nekonečné grupy, s použitím kardinálních čísel pro označení velikostí množin. I bez znalosti kardinální aritmetiky lze tvrzení interpretovat tak, že existuje bijekce mezi prvky grupy $\mathbf{G}$ a kartézským součinem $H \times \{aH : a \in G\}$, tj. že tyto množiny jsou stejně velké. Pro konečné grupy můžeme zformulovat tento okamžitý důsledek:

Důsledek 2.5. *Buď* $\mathbf{G}$ *konečná grupa a* $\mathbf{H}$ *její podgrupa. Pak* $|\mathbf{H}|$ *dělí* $|\mathbf{G}|$ *a* $\operatorname{ord}(a)$ *dělí* $|\mathbf{G}|$ *pro každé* $a \in G$.

Důkaz. Aplikujte Lagrangeovu větu na podgrupu $\mathbf{H} = \langle a \rangle$. □

Lagrangeovu větu dokážeme pomocí dvou základních vlastností rozkladů: za prvé, dvě různé rozkladové třídy jsou disjunktní, a za druhé, všechny rozkladové třídy jsou stejně velké. Analogická tvrzení platí i pro pravé rozkladové třídy.

Lemma 2.6. *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pro každé* $a, b \in G$ *platí buď* $aH = bH$*, nebo* $aH \cap bH = \emptyset$.

Důkaz. Předpokládejme $aH \cap bH \neq \emptyset$, dokážeme, že $aH = bH$. Uvažujme $c \in aH \cap bH$ a napišme $c = ah_1 = bh_2$ pro nějaká $h_1, h_2 \in H$. Pak pro každé $ah \in aH$ platí

$$ah = ch_1^{-1}h = b\underbrace{h_2h_1^{-1}h}_{\in H} \in bH$$

a podobně pro každé $bh \in bH$ platí

$$bh = ch_2^{-1}h = a\underbrace{h_1h_2^{-1}h}_{\in H} \in aH.$$

Tedy $aH = bH$. □

Lemma 2.7. *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pro každé* $a \in G$ *platí* $|aH| = |H|$.

Důkaz. Uvažujme zobrazení $f : G \to G$ definované $f(x) = ax$. Toto zobrazení je prosté: kdyby $ax = f(x) = f(y) = ay$, krácením dostaneme $x = y$. Přitom $f(H) = aH$, tedy $f|_H$ je bijekce mezi H a aH, takže jsou tyto množiny stejně velké. □

Důkaz Lagrangeovy věty. Zvolme nějakou transverzálu T a napišme

$$G = \bigcup_{a \in T} aH.$$

Podle Lemmatu 2.6 jde o disjunktní sjednocení, takže počet prvků lze spočítat jako součet velikostí jednotlivých podmnožin:

$$|\mathbf{G}| = \sum_{a \in T} |aH| = \sum_{a \in T} |H| = |T| \cdot |H| = [\mathbf{G} : \mathbf{H}] \cdot |\mathbf{H}|.$$

V druhé rovnosti jsme použili Lemma 2.7 a ve čtvrté rovnosti jsme použili vztah $|T| = [\mathbf{G} : \mathbf{H}]$, který plyne z Lemmatu 2.6. □

Speciálním případem Lagrangeovy věty je *Eulerova věta*, kterou jsme diskutovali v Sekci **??**. Buď $\mathbf{G} = \mathbb{Z}_n^*$ a $a \in \mathbb{Z}_n^*$, tedy a je celé číslo splňující $\mathrm{NSD}(a, n) = 1$. Pak $\mathrm{ord}(a)$ dělí $|\mathbb{Z}_n^*| = \varphi(n)$. Protože $a^{\mathrm{ord}(a)} = 1$, tím spíše bude

$$a^{\varphi(n)} = 1 \text{ v } \mathbb{Z}_n^*,$$

jinými slovy $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Ve zbytku sekce ukážeme další dvě vlastnosti rozkladů. Začneme důležitým kritériem, podle kterého se snadno ověří, za jakých podmínek jsou dvě rozkladové třídy stejné. Toto kritérium se nám bude hodit při důkazu Burnsideovy věty nebo v sekci o faktorgupách.

Tvrzení 2.8. *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pro každé* $a, b \in G$ *platí*

(1) $aH = bH$ *právě tehdy, když* $a^{-1}b \in H$*;*
(2) $Ha = Hb$ *právě tehdy, když* $ab^{-1} \in H$*.*

Důkaz. (1) ($\Rightarrow$) Protože $aH = bH$, máme $b \in aH$, a tedy $b = ah$ pro nějaké $h \in H$. Tudíž $a^{-1}b = h \in H$. ($\Leftarrow$) Jestliže $a^{-1}b \in H$, pak pro každé $ah \in aH$ platí

$$ah = bb^{-1}ah = b\underbrace{(a^{-1}b)^{-1}h}_{\in H} \in bH$$

a podobně pro každé $bh \in bH$ platí

$$bh = a\underbrace{a^{-1}bh}_{\in H} \in aH.$$

Tedy $aH = bH$. (2) se dokáže analogicky. □

Na závěr ukážeme, že levé a pravé rozklady jsou stejně velké.

Lemma 2.9. *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Levý i pravý rozklad* $\mathbf{G}$ *podle* $\mathbf{H}$ *mají stejný počet prvků.*

Důkaz. Dokážeme, že zobrazení $aH \mapsto Ha^{-1}$ je bijekcí mezi levým a pravým rozkladem. Nejprve musíme dokázat, že jsme korektně definovali zobrazení: mohlo by se stát, že téže rozkladové třídě $aH = bH$ se snažíme přiřadit dvě různé hodnoty $Ha^{-1} \neq Hb^{-1}$. Podle Tvrzení 2.8

$$aH = bH \;\Leftrightarrow\; a^{-1}b \in H \;\Leftrightarrow\; (a^{-1}b)^{-1} = b^{-1}a \in H \;\Leftrightarrow\; Ha^{-1} = Hb^{-1},$$

a tedy zobrazení je nejen dobře definované, ale také prosté. Evidentně je i na. □

3. Permutační grupy

3.1. **Základní vlastnosti permutací.**

Permutací na množině X rozumíme bijekci (vzájemně jednoznačné zobrazení) $X \to X$. Pro permutace π, σ na X definujeme operace $\circ$, $^{-1}$, id předpisy

- $\pi \circ \sigma : x \mapsto \pi(\sigma(x))$,
- $\pi^{-1} : x \mapsto$ ten (jediný) prvek y splňující $\pi(y) = x$,
- $id : x \mapsto x$.

Označíme-li S_X množinu všech permutací na množině X, pak $\mathbf{S}_X = (S_X, \circ, ^{-1}, id)$ je tzv. *symetrická grupa* na X. Podgrupám této grupy se říká *permutační grupy*. Je-li $X = \{1, \dots, n\}$, značíme $\mathbf{S}_X = \mathbf{S}_n$.

Cyklus v permutaci π je posloupnost $x_1, \dots, x_k$ navzájem různých prvků množiny X splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, …, $\pi(x_k) = x_1$. *Rozkladem na cykly* se rozumí zápis

$$(x_{11}\ x_{12}\ \dots\ x_{1k_1})(x_{21}\ x_{22}\ \dots\ x_{2k_2}) \cdots (x_{m1}\ x_{m2}\ \dots\ x_{mk_m}),$$

kde $x_{i1}, x_{i2}, \dots, x_{ik_i}$ jsou navzájem různé prvky pro všechna i. Cykly délky 1 se ze zápisu zpravidla vynechávají. (Je-li X konečná množina, pak rozklad na cykly jistě existuje; pro nekonečné množiny bychom museli povolit „nekonečné cykly“.)

Tvrzení 3.1. *Řád permutace π v grupě $\mathbf{S}_n$ je roven nejmenšímu společnému násobku délek jejích cyklů.*

Důkaz. Cyklus délky n má zřejmě řád n a jsou-li $C_1, \dots, C_m$ disjunktní cykly, pak $(C_1 \circ \dots \circ C_m)^k = C_1^k \circ \dots \circ C_m^k$. Z toho plyne, že $(C_1 \circ \dots \circ C_m)^k = id$ právě tehdy, když je k násobkem všech délek cyklů. Čili řád je roven nejmenšímu společnému násobku. □

Transpozicí rozumíme permutaci tvaru $(x\ y)$.

Tvrzení 3.2. *Grupa $\mathbf{S}_n$ je generovaná množinou všech transpozic.*

Jinými slovy, každou permutaci (na konečné množině) lze napsat jako složení transpozic.

Důkaz. Libovolný cyklus můžeme rozložit jako

$$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_k) \circ \dots \circ (a_1\ a_3) \circ (a_1\ a_2).$$

Danou permutaci pak můžeme napsat jako složení rozkladů všech jejích cyklů. □

Permutace (na konečné množině) se nazývá *sudá*, pokud se skládá ze sudého počtu transpozic, *lichá* v opačném případě (máme-li dva různé rozklady jedné permutace, mohou mít různé délky, ale, jak lze snadno nahlédnout, stejnou paritu). Definujeme *znaménko permutace*: $\operatorname{sgn}\pi = 1$, je-li π sudá, a $\operatorname{sgn}\pi = -1$, je-li π lichá. Přímo z definice plyne, že

$$\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}\pi \cdot \operatorname{sgn}\sigma \quad \text{a} \quad \operatorname{sgn}\pi^{-1} = \operatorname{sgn}\pi.$$

(První tvrzení je očividné, druhé plyne ze vztahu $((a_1\ b_1) \circ \dots \circ (a_n\ b_n))^{-1} = (a_n\ b_n) \circ \dots \circ (a_1\ b_1)$.) Z důkazu Tvrzení 3.2 navíc můžeme vyčíst, že

$$\operatorname{sgn}\pi = (-1)^{n - \text{počet cyklů v } \pi} = (-1)^{\text{počet sudých cyklů v } \pi}.$$

Díky uvedeným vztahům tvoří sudé permutace podgrupu v $\mathbf{S}_n$, tzv. *alternující grupu* $\mathbf{A}_n$.

Tvrzení 3.3. *Grupa $\mathbf{A}_n$ je generovaná množinou všech trojcyklů.*

Jinými slovy, každou sudou permutaci lze napsat jako složení trojcyklů.

Důkaz. Danou sudou permutaci nejprve rozložíme na transpozice, a ty seskupíme do dvojic. Pokud jsou dvě sousední transpozice stejné, můžeme je vypustit. Pokud mají společný jeden prvek, pak $(i\ j) \circ (j\ k) = (i\ j\ k)$. A jsou-li disjunktní, pak $(i\ j) \circ (k\ l) = (k\ i\ l) \circ (i\ j\ k)$. Tímto způsobem přepíšeme rozklad na transpozice na složení trojcyklů. □

Důležitým konceptem v teorii grup je tzv. *konjugace*.

Definice. Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa a $a, b \in G$. Prvky a, b nazýváme *konjugované* v $\mathbf{G}$, pokud existuje $c \in G$ takové, že $a = c \cdot b \cdot c^{-1}$.

Je vidět, že relace konjugace je ekvivalencí. Její bloky se nazývají *třídy konjugace*.

Příklad. V lineární algebře se konjugovaným maticím se říká *podobné*. Konjugace odpovídá zmeně báze daného lineárního zobrazení, tj. dvě matice jsou podobné právě tehdy, když jsou maticí téhož lineárního zobrazení vzhledem k různým bázím. Připomeňme například *Jordanovu větu*, která říká, že matice A, B jsou konjugované v grupě $\mathbf{GL}_n(\mathbb{C})$ právě tehdy, když mají stejný Jordanův kanonický tvar.

Příklad. Pojem konjugace je velmi důležitý v permutačních grupách. Uvažujme permutaci

$$\pi = (a_{11}\ a_{12}\ \dots\ a_{1k_1})(a_{21}\ a_{22}\ \dots\ a_{2k_2}) \cdots (a_{m1}\ a_{m2} \dots\ a_{mk_m}),$$

a libovolnou permutaci ρ. Pak $\rho \circ \pi \circ \rho^{-1}$ je rovno

$$(\rho(a_{11})\ \rho(a_{12})\ \dots\ \rho(a_{1k_1}))(\rho(a_{21})\ \rho(a_{22})\ \dots\ \rho(a_{2k_2})) \cdots (\rho(a_{m1})\ \rho(a_{m2})\ \dots\ \rho(a_{mk_m})),$$

neboť pro každé i, j platí

$$(\rho \circ \pi \circ \rho^{-1})(\rho(a_{ij})) = \rho(\pi(a_{ij})) = \rho(a_{i(j \oplus 1)}),$$

kde $j \oplus 1 = j + 1$ pro $j < k_j$ a $k_j \oplus 1 = 1$. Konjugace permutací ρ tedy funguje jako „kopírování“ zápisu podle pravidel daných permutací ρ, každý prvek a v zápise permutace π se přepíše na $\rho(a)$, přičemž struktura cyklů zůstane zachována.

Tvrzení 3.4. *Permutace π, σ jsou konjugované v grupě $\mathbf{S}_n$ právě tehdy, když mají stejný počet cyklů každé délky (říká se* stejný typ*).*

Důkaz. ($\Rightarrow$) Plyne bezprostředně z výpočtu v předchozím příkladu.
($\Leftarrow$) Jsou-li

$$\pi = (a_{11}\ a_{12}\ \dots\ a_{1k_1})(a_{21}\ a_{22}\ \dots\ a_{2k_2}) \cdots (a_{m1}\ a_{m2} \dots\ a_{mk_m}),$$
$$\sigma = (b_{11}\ b_{12}\ \dots\ b_{1k_1})(b_{21}\ b_{22}\ \dots\ b_{2k_2}) \cdots (b_{m1}\ b_{m2} \dots\ b_{mk_m}),$$

dvě permutace stejného typu, definujeme $\rho(a_{ij}) = b_{ij}$ a výše uvedeným výpočtem dostaneme $\sigma = \rho \circ \pi \circ \rho^{-1}$. □

Příklad. Permutace (1 2 3) a (2 3 4) jsou konjugované v grupě $\mathbf{S}_4$, protože obě mají jeden cyklus délky 1 a jeden cyklus délky 3. Tyto permutace ovšem nejsou konjugované v grupě $\mathbf{A}_4$: jak plyne z důkazu Tvrzení 3.4, jediné permutace ρ splňující $(2\ 3\ 4) = \rho \circ (1\ 2\ 3) \circ \rho^{-1}$ jsou (1 4), (1 2 3 4) a (1 3 2 4). Žádná z nich ovšem není sudá.

Příklad. Ukážeme, že

$$\mathbf{S}_n = \langle (1\ 2), (1\ 2\ \ldots\ n) \rangle.$$

Díky Tvrzení 3.2 stačí dokázat, že lze nagenerovat všechny transpozice. Nejprve nagenerujeme transpozice $(k\ k+1)$, $k = 1, \ldots, n-1$: induktivně

$$(k+1\ k+2) = (1\ 2\ \ldots\ n)(k\ k+1)(1\ 2\ \ldots\ n)^{-1}.$$

Dále, pro každé k nagenerujeme ostatní transpozice $(k\ k+i)$, $i > 0$: opět induktivně

$$(k\ k+i+1) = (k+i\ k+i+1)(k\ k+i)(k+i\ k+i+1)^{-1}.$$

3.2. **Působení grupy na množině.**

V řada případů se hodí danou abstraktní grupu interpretovat jako grupu permutací na nějaké množině. Například grupu $\mathbb{Z}_n$ lze interpretovat jako grupu permutací roviny, kde číslu k odpovídá otočení o o úhel $k \cdot 2\pi/n$. Součet dvou čísel modulo n odpovídá složení příslušných otočení, opačné číslo odpovídá opačnému otočení a nula odpovídá identické permutaci. Toto pozorování motivuje následující definici.

Definice. *Působením grupy* $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *na množině* X rozumíme zobrazení $\pi : G \to S_X$ splňující následující podmínky pro všechna $g, h \in G$:

- $\pi(1) = id$,
- $\pi(g^{-1}) = \pi(g)^{-1}$,
- $\pi(g \cdot h) = \pi(g) \circ \pi(h)$.

Hodnotu permutace $\pi(g)$ na prvku $x \in X$ budeme značit krátce $g(x)$. Z definice plyne, že jednotka v $\mathbf{G}$ působí jako identita, g^{-1} působí jako inverzní permutace k $\pi(g)$ a platí vztah $(g \cdot h)(x) = g(h(x))$. Můžeme si představovat, že prvky grupy $\mathbf{G}$ „hýbou“ s prvky množiny X, přičemž tak, jak se prvky v $\mathbf{G}$ násobí, tak se příslušné „pohyby“ skládají.

Příklad. Působení z úvodního odstavce odpovídá následující konfiguraci: $\mathbf{G} = \mathbb{Z}_n$, $X = \mathbb{R}^2$ a $\pi(k)$ je permutace na X daná předpisem

$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} \cos(k \cdot 2\pi/n) & -\sin(k \cdot 2\pi/n) \\ \sin(k \cdot 2\pi/n) & \cos(k \cdot 2\pi/n) \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}.$$

Příklad. Podobným způsobem lze interpretovat maticové grupy jako permutace příslušného vektorového prostoru dané příslušným lineárním zobrazením: zde $\mathbf{G} \leq \mathbf{GL}_n(\mathbf{T})$, $X = T^n$ a $\pi(A)$ je permutace množiny T^n, která vektor v zobrazí na součin Av.

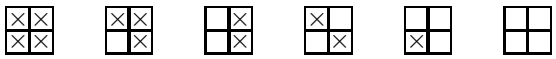
Příklad. Triviálním případem je přirozené působení permutační grupy $\mathbf{G} \leq \mathbf{S}_X$ na množinu X, kde $\pi(g) = g$.

3.3. **Burnsideova věta.**

Jako ukázku, k čemu je dobrá teorie permutačních grup, si ukážeme jednu pěknou aplikaci v kombinatorice. Jak spočítat počet nějakých objektů až na danou symetrii? Například, kolika způsoby je možné obarvit stěny krychle dvěma barvami až na otočení, tj. když dvě obarvení považujeme za totožná, pokud jedno z druhého dostaneme otočením krychle? Jako motivaci použijeme následující jednodušší úlohu.

Úloha. Kolika způsoby je možné obarvit políčka čtverce 2×2 dvěma barvami až na otočení? Tj. dvě obarvení považujeme za totožná, pokud jedno z druhého dostaneme otočením čtverce.

Tuto úlohu je samozřejmě snadné řešit prostým výčtem všech možných obarvení, vyjde nám následujících šest:



Ale při větším počtu barev nebo větším počtu políček bychom se nedopočítali. Nejprve si ujasněme, co přesně znamená počítání „až na danou symetrii“. Dva objekty považujeme za totožné, pokud jeden z druhého dostaneme pomocí nějakého povoleného zobrazení. V naší úloze jsou to otočení, která zachovávají daný čtverec, tj. otočení roviny o 0, 90, 180 a 270 stupňů. Uvažujme tedy působení grupy $\mathbf{G}$ sestávající z těchto čtyřech otočení na množině X sestávající ze včech možných obarvení čtverce 2×2 dvěma barvami (tj. $|X| = 2^4 = 16$), kde $\pi(g)$ je permutace, která čtverec otočí o příslušný úhel i s daným obarvením.

Nyní zpět k teorii. V celém zbytku této sekce uvažujme libovolné působení grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ na množinu X. Budeme potřebovat několik užitečných definic a vlastností.

Zavedeme tzv. *relaci tranzitivity* $\sim$ na množině X: definujeme $x \sim y$, pokud existuje $g \in G$ takové, že $g(x) = y$. Volně řečeno, $x \sim y$, pokud nějaká permutace přesouvá x na y.

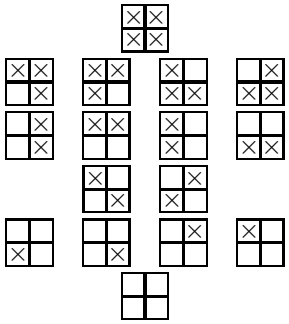
Pozorování 3.5. *Relace $\sim$ je ekvivalence na X.*

Důkaz. Reflexivita plyne z toho, že $1(x) = id(x) = x$. Symetrie z toho, že $g(x) = y$ implikuje $g^{-1}(y) = x$. Tranzitivita: pokud $x \sim y \sim z$, tedy $g(x) = y$ a $h(y) = z$ pro nějaká g, h, pak $(h \cdot g)(x) = h(g(x)) = h(y) = z$, a tedy $x \sim z$. □

Bloky ekvivalence $\sim$ nazýváme *orbity*. Orbitu obsahující prvek x budeme značit

$$[x] = \{y \in X : x \sim y\} = \{g(x) : g \in G\}.$$

Příklad. V motivační úloze jsou v relaci $\sim$ každá dvě obarvení taková, že jedno z druhého lze dostat otočením. Množina všech obarvení se tedy rozpadne na šest orbit následujícím způsobem:



Vidíme, že řešením úlohy je *počet orbit* v tomto působení.

Bod $x \in X$ se nazývá *pevným bodem* prvku $g \in G$, pokud $g(x) = x$. Množinu všech pevných bodů prvku $g \in G$ budeme značit

$$X_g = \{x \in X : g(x) = x\}$$

a *stabilizátorem prvku* $x \in X$ nazveme množinu

$$G_x = \{g \in G : g(x) = x\}.$$

Příklad. Stabilizátorem obou jednobarevných obarvení je celá grupa $\mathbf{G}$. Stabilizátor obarvení  obsahuje pouze identitu. Stabilizátor obarvení  obsahuje identitu a otočení o 180 stupňů.

Pozorování 3.6. *Stabilizátor tvoří podgrupu grupy* $\mathbf{G}$.

Důkaz. Jednotka náleží G_x, neboť $1(x) = id(x) = x$. Je-li $g, h \in G_x$, tj. platí $g(x) = h(x) = x$, pak $g^{-1}(x) = x$ a $(g \cdot h)(x) = g(h(x)) = g(x) = x$. □

Lemma 3.7. *Pro každé* $x \in X$ *platí* $|\mathbf{G}| = |\mathbf{G}_x| \cdot |[x]|$.

Důkaz. Protože je $\mathbf{G}_x$ podgrupa grupy $\mathbf{G}$, Lagrangeova věta říká, že

$$|G| = |G_x| \cdot [\mathbf{G} : \mathbf{G}_x].$$

Stačí tedy dokázat, že $\big|[x]\big| = [\mathbf{G} : \mathbf{G}_x] = \big|\{gG_x : g \in G\}\big|$. Uvažujme zobrazení

$$\varphi : \{gG_x : g \in G\} \to [x], \qquad gG_x \mapsto g(x).$$

Dokážeme, že to je bijekce. Předně je třeba ověřit, že jsme skutečně definovali zobrazení: mohlo by se stát, že tutéž rozkladovou třídu máme označenu dvěma různými způsoby, tj. že $gG_x = hG_x$ pro nějaká $g \neq h$, a přitom se jí snažíme přiřadit dvě různé hodnoty $g(x), h(x)$. Ovšem podle Tvrzení 2.8 platí

$$gG_x = hG_x \;\Leftrightarrow\; h^{-1}g \in G_x \;\Leftrightarrow\; h^{-1}g(x) = x \;\Leftrightarrow\; g(x) = h(x),$$

a tedy φ je nejen dobře definované, ale také prosté. Navíc pro každý prvek $y \in [x]$ existuje $g \in G$ splňující $g(x) = y$, tedy φ je bijekce. □

Z lemmatu plyne, že velikosti orbit dělí počet prvků grupy $\mathbf{G}$. (Všimněte si, že to je splněno v naší motivační úloze.)

Připomeňme, že $X/\!\sim$ značí množinu všech bloků ekvivalence $\sim$, tj. $|X/\!\sim|$ značí počet orbit daného působení.

Věta 3.8 (Burnsideova věta)**.** *Nechť konečná grupa* $\mathbf{G}$ *působí na konečnou množinu* X*. Pak*

$$\big|X/\!\sim\big| = \frac{1}{|G|} \cdot \sum_{g \in G} \big|X_g\big|.$$

Důkaz. Označme

$$M = \big\{(g, x) \in G \times X : g(x) = x\big\}.$$

Prvky této množiny můžeme spočítat dvěma způsoby: buď ke každému g spočítáme počet x takových, že $(g, x) \in M$, nebo naopak, ke každému x spočítáme počet g takových, že $(g, x) \in M$. Dostaneme tak následující rovnost:

$$|M| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

Použitím této rovnosti dopočítáme uvedený vzorec:

$$\frac{1}{|G|} \cdot \sum_{g \in G} |X_g| \;=\; \frac{1}{|G|} \cdot \sum_{x \in X} |G_x| \;\overset{3.7}{=}\; \frac{1}{|G|} \cdot \sum_{x \in X} \frac{|G|}{\big|[x]\big|} \;=\; \sum_{x \in X} \frac{1}{\big|[x]\big|} \;=$$

$$\sum_{O \in (X/\sim)} \sum_{x \in O} \frac{1}{\big|[x]\big|} \;=\; \sum_{O \in (X/\sim)} \sum_{x \in O} \frac{1}{|O|} \;=\; \sum_{O \in (X/\sim)} |O| \cdot \frac{1}{|O|} \;=\; \sum_{O \in (X/\sim)} 1.$$

Výsledek je tedy roven velikosti množiny $X/\!\sim$, tj. počtu orbit. □

Vzorec lze interpretovat tak, že *počet orbit je roven průměrnému počtu pevných bodů*, kde průměr počítáme přes všechny prvky grupy $\mathbf{G}$.

Příklad. Vraťme se k motivační úloze. Otočení o 0 stupňů (tj. identita) zachovává všechna obarvení, tedy $|X_0| = |X| = 16$. Otočení o 90 stupňů zobrazuje levé dolní políčko na levé horní, levé horní na pravé horní, atd., čili abychom dostali stejné obarvení, musí mít všechna čtyři políčka stejnou barvu. Tedy $|X_{90}| = 2$. Podobně $|X_{270}| = 2$. Otočení o 180 stupňů zaměňuje levé dolní políčko za pravé horní a levé horní za pravé dolní. Tyto dvě dvojice tedy musí být stejnobarevné, a to lze provést čtyřmi způsoby. Tedy $|X_{180}| = 4$. Podle Burnsideovy věty je počet obarvení až na otočení $\frac{1}{4} \cdot (16 + 2 + 4 + 2) = 6$.

Metodu ilustrujeme na několika dalších úlohách.

Úloha. a) Dětská stavebnice obsahuje tři červené, tři zelené a tři modré čtvercové destičky. Kolika způsoby je lze sestavit do velkého čtverce 3×3? Dvě sestavy považujeme za totožné, pokud jednu z druhé dostaneme otočením. b) Jak se výsledek změní, pokud je možné dílky pevně spojovat? Tedy pokud dvě sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením a převrácením.

Řešení. Místo sestav budeme uvažovat barvení jednotlivých políček čtverce. Čili X bude množina všech obarvení čtverce 3×3 daným počtem barev a $\mathbf{G}$ bude a) grupa všech otočení čtverce, b) grupa všech symetrií čtverce (tj. $\mathbf{G} = \mathbf{D}_8$). Grupa $\mathbf{G}$ působí na X tak, že příslušná permutace otočí/převrátí čtverec i s jeho obarvením. Řešením úlohy je počet orbit tohoto působení (dvě obarvení jsou v jedné orbitě právě tehdy, když jedno z druhého dostaneme otočením, resp. převrácením).

Napíšeme tabulku, v jejímž prvním sloupci bude seznam prvků grupy $\mathbf{G}$, přičemž zobrazení „podobného typu“ budeme sdružovat, v druhém sloupci bude počet prvků daného typu a ve třetím počet pevných bodů těchto prvků. Pevným bodem se rozumí takové obarvení, které po daném otočení/převrácení vypadá stejně.

g	#	$\lvert X_g \rvert$
id	1	1680
otočení o $\pm 90°$	2	0
otočení o $180°$	1	0
osa přes vrcholy	2	36
osa středem hran	2	36

Podle Burnsideovy věty je počet obarvení

a) $\frac{1}{4} \cdot (1680 + 2 \cdot 0 + 1 \cdot 0) = 420$,
b) $\frac{1}{8} \cdot (1680 + 2 \cdot 0 + 1 \cdot 0 + 2 \cdot 36 + 2 \cdot 36) = 228$.

□

Úloha. Kolik náhrdelníků lze sestavit a) ze tří červených, tří zelených a tří modrých kuliček, b) z šesti žlutých a tří černých kuliček? (Nezáleží na poloze náhrdelníku, je možno jej převracet či otáčet.)

Řešení. Místo náhrdelníků budeme uvažovat barvení vrcholů pravidelného devítiúhelníka. Čili X, resp. Y, bude množina všech obarvení vrcholů pravidelného devítiúhelníka danými barvami a $\mathbf{G} = \mathbf{D}_{18}$ bude grupa všech symetrií pravidelného devítiúhelníka, která působí na X, resp. Y, tak, že příslušná permutace otočí/převrátí devítiúhelník i s jeho obarvením. Každé orbitě tohoto působení odpovídá právě

jeden náhrdelník (jehož kuličky jsou uspořádány podle toho obarvení). Napíšeme tabulku podobně jako v předchozí úloze.

g	#	$\lvert X_g\rvert$	$\lvert Y_g\rvert$
id	1	1680	84
otočení o ± 1 vrchol	2	0	0
otočení o ± 2 vrcholy	2	0	0
otočení o ± 3 vrcholy	2	6	3
otočení o ± 4 vrcholy	2	0	0
osové symetrie	9	0	4

Podle Burnsideovy věty je počet náhrdelníků a) $\frac{1}{18} \cdot (1680 + 2 \cdot 6) = 94$, resp. b) $\frac{1}{18} \cdot (84 + 2 \cdot 3 + 9 \cdot 4) = 7$. □

Úloha. Kolika způsoby je možné obarvit stěny krychle dvěma barvami? Kolika způsoby lze přiřadit stěnám čísla 1 až 6? A kolik existuje hracích kostek, tj. kolika způsoby lze přiřadit čísla 1 až 6 tak, že součet protilehlých stěn je sedm? Dvě obarvení/přiřazení považujeme za totožná, pokud lze jedno z druhého dostat otočením krychle.

Řešení. Buď X množina všech obarvení stěn krychle dvěma barvami, Y množina všech přiřazení čísel 1 až 6 stěnám a Z množina těch přiřazení z Y, jejichž protilehlé stěny dávají součet sedm. $\mathbf{G}$ bude grupa všech otočení krychle působící na X, Y i Z tak, že příslušná permutace otočí krychli i s jejím obarvením/přiřazením. Napíšeme tabulku podobně jako v předchozí úloze.

g	#	$\lvert X_g\rvert$	$\lvert Y_g\rvert$	$\lvert Z_g\rvert$
identita	1	2^6	6!	48
osa přes středy protilehlých stěn, $\pm 90°$	6	2^3	0	0
osa přes středy protilehlých stěn, $+180°$	3	2^4	0	0
osa přes středy protilehlých hran, $+180°$	6	2^3	0	0
osa přes protilehlé vrcholy, $\pm 120°$	8	2^2	0	0

Tedy počty orbit jsou

- $\lvert X/{\sim}\rvert = \frac{1}{24} \cdot (2^6 + 3 \cdot 2^4 + 12 \cdot 2^3 + 8 \cdot 2^2) = 10$,
- $\lvert Y/{\sim}\rvert = \frac{1}{24} \cdot 6! = 30$,
- $\lvert Z/{\sim}\rvert = \frac{1}{24} \cdot 48 = 2$.

Jak známo, hrací kostky jsou dvě, pravotočivá a levotočivá, podle pořadí stěn 1, 2, 3 při pohledu na příslušný roh kostky. □

Burnsideovu větu lze použít v řadě dalších aplikací, např. pokud chceme zjistit *počet nějakých struktur dané velikosti až na izomorfismus*. Metodu ilustrujeme na grafech s čtyřmi vrcholy. Buď X množina všech grafů s vrcholy $1, 2, 3, 4$. Dva grafy jsou izomorfní, pokud existuje permutace z $\mathbf{S}_4$, která převádí hrany na hrany a mezery na mezery. Uvažujme tedy působení grupy $\mathbf{S}_4$ na X tak, že daná permutace přehází vrcholy i s hranami. Orbity tohoto působení budou obsahovat právě všechny navzájem izomorfní grafy, počet neizomorfních grafů je tedy roven počtu

orbit. Řešením je tabulka

g	#	$\lvert X_g\rvert$
id	1	2^6
(..)	6	2^4
(..)(..)	3	2^4
(...)	8	2^2
(....)	6	2^2

Vidíme, že čtyřprvkových grafů je 11.

Na závěr jedna poučná aplikace v teorii permutačních grup. Permutační grupa se nazývá tranzitivní, má-li jen jednu orbitu (ve svém přirozeném působení). Např. grupy $\mathbf{S}_n$, $\mathbf{A}_n$, $\mathbf{D}_{2n}$ jsou tranzitivní, grupa $\langle (1\ 2)(3\ 4)\rangle_{\mathbf{S}_4}$ není.

Věta 3.9 (Jordanova věta)**.** *Každá alespoň dvouprvková konečná tranzitivní grupa obsahuje alespoň jednu permutaci bez pevného bodu.*

Důkaz. Podle Burnsideovy věty je počet orbit roven průměrnému počtu pevných bodů. Tranzitivita říká, že počet orbit je 1. Přitom identita má alespoň dva pevné body, tedy *nadprůměrné* množství, takže musí existovat permutace, která má *podprůměrné* množství pevných bodů. Protože je počet pevných bodů nezáporné celé číslo, jediná podprůměrná hodnota je 0. Tedy existuje permutace bez pevného bodu. □

4. Cyklické grupy

4.1. Podgrupy a řády prvků.

Definice. Grupa $\mathbf{G}$ se nazývá *cyklická*, pokud je generovaná jedním prvkem, tj. $\mathbf{G} = \langle a\rangle_{\mathbf{G}}$ pro nějaké $a \in G$.

Tvrzení 2.2 říká, že prvky cyklické grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1) = \langle a\rangle$ lze vyjádřit jako

$$\mathbf{G} = \{a^k : k \in \mathbb{Z}\}.$$

Z Tvrzení **??** plyne, že je-li řád a nekonečný, pak jsou tyto mocniny po dvou různé, a je-li $\mathrm{ord}(a) = n$ konečný, pak $\mathbf{G} = \{a^0, a^1, \ldots, a^{n-1}\}$. Odsud je odvozen název pro cyklické grupy: při násobení daným prvkem a cyklicky procházíme přes všechny prvky grupy $\mathbf{G}$.

Příklady.

- Grupy $\mathbb{Z}$ a $\mathbb{Z}_n$, $n \in \mathbb{N}$, jsou cyklické, generované prvkem 1.
- Grupy $\mathbb{C}_n \leq \mathbb{C}^*$ sestávající ze všech komplexních kořenů polynomu $x^n - 1$ jsou cyklické, $\mathbb{C}_n = \langle e^{2\pi i/n}\rangle$. Prüferova grupa $\mathbb{C}_{p^\infty}$ cyklická není (není ani konečně generovaná), přestože všechny její vlastní podgrupy cyklické jsou.
- Grupy $\mathbb{Z}_p^*$ jsou cyklické pro každé prvočíslo p, jak plyne z Věty 4.5. Například $\mathbb{Z}_5^* = \langle 2\rangle$, $\mathbb{Z}_7^* = \langle 3\rangle$, $\mathbb{Z}_{11}^* = \langle 2\rangle$.
- Některé grupy $\mathbb{Z}_n^*$, n složené, jsou cyklické, např. $\mathbb{Z}_6^* = \{1, 5\} = \langle 5\rangle$, ale některé ne, např. $\mathbb{Z}_8^*$ cyklická není.
- Každá grupa $\mathbf{G}$ prvočíselného řádu je cyklická. Uvažujme podgrupu $\langle a\rangle$, $a \neq 1$. Podle Lagrangeovy věty je $\lvert\langle a\rangle\rvert$ dělí $\lvert\mathbf{G}\rvert$, přitom $\lvert\langle a\rangle\rvert > 1$, tedy $\lvert\langle a\rangle\rvert = \lvert\mathbf{G}\rvert$ a prvek a tuto grupu generuje.

Nejprve se podíváme, jak vypadají podgrupy cyklických grup.

Tvrzení 4.1. *Každá podgrupa cyklické grupy je cyklická.*

Důkaz. Buď $\mathbf{H}$ podgrupa cyklické grupy $\mathbf{G} = \langle a \rangle$. Je-li $H = \{1\}$, pak $\mathbf{H} = \langle 1 \rangle$. V opačném případě označme k nejmenší kladné číslo takové, že $a^k \in H$ (všechny prvky $\mathbf{G}$ jsou mocniny a, takové k tedy existuje). Dokážeme, že $\mathbf{H} = \langle a^k \rangle$. Inkluze $\langle a^k \rangle \subseteq H$ je zřejmá. Pro spor tedy předpokládejme, že existuje nějaký prvek $a^n \in H \setminus \langle a^k \rangle$. Pak $k \nmid n$, jinak bychom měli $a^n = (a^k)^{n/k}$. Dostáváme

$$a^{n \bmod k} = a^{n-k(n \operatorname{div} k)} = a^n \cdot (a^k)^{n \operatorname{div} k} \in H,$$

protože a^n i a^k leží v H, což je spor s volbou k jako nejmenšího kladného čísla s vlastností $a^k \in H$. □

Příklad. Grupa $\mathbb{Z}$ je cyklická, a tedy její podgrupy jsou tvaru

$$\mathbf{H} = \langle k \rangle = k\mathbb{Z} = \{a \in \mathbb{Z} : k \mid a\}.$$

Přitom $k\mathbb{Z} = l\mathbb{Z}$ právě tehdy, když $k = \pm l$. Podgrup je tedy nekonečně mnoho, všechny tvaru $k\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$, tyto jsou po dvou různé. Přitom $k\mathbb{Z} \subseteq l\mathbb{Z}$ právě tehdy, když $l \mid k$, tedy pogrupy jsou vzhledem k inkluzi uspořádány opačně než množina $\mathbb{N} \cup \{0\}$ dělitelností.

Pro grupy $\mathbb{Z}_n$ bychom mohli postupovat podobně, ale není tak jasné, za jakých podmínek jsou dvě podgrupy totožné. Pomůže nám následující vlastnost.

Lemma 4.2. *Buď $\mathbf{G} = \langle a \rangle$ konečná cyklická grupa řádu n. Pak $\langle a^k \rangle = \langle a^{\mathrm{NSD}(k,n)} \rangle$.*

Důkaz. Vzhledem k tomu, že $\mathrm{NSD}(k,n) \mid k$, ihned vidíme, že $a^k \in \langle a^{\mathrm{NSD}(k,n)} \rangle$, a tedy $\langle a^k \rangle \subseteq \langle a^{\mathrm{NSD}(k,n)} \rangle$. K opačné inkluzi využijeme Bézoutovu rovnost: $\mathrm{NSD}(k,n) = uk + vn$, tedy

$$a^{\mathrm{NSD}(k,n)} = a^{uk+vn} = (a^k)^u \cdot (a^n)^v = (a^k)^u \cdot 1^v = (a^k)^u \in \langle a^k \rangle,$$

z čehož plyne dokazovaná inkluze. □

Příklad. Grupa $\mathbb{Z}_n$ je cyklická, a tedy její podgrupy jsou tvaru

$$\mathbf{H} = \langle k \rangle = k\mathbb{Z}_n = \{ku \bmod n : u = 0, \ldots, n-1\}.$$

Podle Lemmatu 4.2 s volbou $a = 1$ dostáváme, že $k\mathbb{Z}_n = \mathrm{NSD}(k,n)\mathbb{Z}_n$, tedy $k\mathbb{Z}_n = l\mathbb{Z}_n$ právě tehdy, když $\mathrm{NSD}(k,n) = \mathrm{NSD}(l,n)$. Podgrup je tedy tolik, kolik je dělitelů čísla n, všechny tvaru $k\mathbb{Z}$, $k \mid n$. Přitom $k\mathbb{Z}_n \subseteq l\mathbb{Z}_n$ právě tehdy, když $l \mid k$, tedy pogrupy jsou vzhledem k inkluzi uspořádány opačně než množina všech dělitelů čísla n dělitelností.

Nyní prodiskutujeme počty generátorů. Je-li $\mathbf{G} = \langle a \rangle$ cyklická grupa nekonečného řádu, má právě dva generátory, a a a^{-1}. Oba tuto grupu generují, protože $\{a^k : k \in \mathbb{Z}\} = \{a^{-k} : k \in \mathbb{Z}\}$. Kdyby $\mathbf{G} = \langle a^n \rangle$ pro nějaké n, pak $a = (a^n)^m$ pro nějaké m, a dostáváme $1 = (a^n)^m \cdot a^{-1} = a^{mn-1}$, a díky tomu, že řád a je nekonečný, $mn = 1$, tedy $n = \pm 1$. Pro konečné cyklické grupy to je složitější, jak uvidíme za chvíli.

O něco obecnější úloha je spočítat počet prvků daného řádu. Pro nekonečné cyklické grupy nutně $\mathrm{ord}(1) = 1$ a $\mathrm{ord}(b) = \infty$ pro každé $b \neq 1$. Pro konečné cyklické grupy můžeme použít Lagrangeovu větu, která říká, že přípustné řády dělí řád celé grupy. Počty prvků jednotlivých přípustných řádů popisuje následující tvrzení.

Tvrzení 4.3. *Buď* $\mathbf{G}$ *cyklická grupa konečného řádu* n*. Pak* $\mathbf{G}$ *obsahuje právě* $\varphi(d)$ *prvků řádu* $d \mid n$*.*

Prvky řádu n jsou právě generátory této grupy, tedy cyklická grupa řádu n má právě $\varphi(n)$ generátorů. (Sluší se dodat, že Eulerova funkce počítá počet čísel nesoudělných s n v intervalu $1, \ldots, n$, a tedy $\varphi(1) = 1$.)

Důkaz. Označme $\mathbf{G} = \langle a \rangle$. Nejprve uvažujme $d = n$. Podle Lemmatu 4.2 $\langle a^k \rangle = \langle \mathrm{NSD}(k, n) \rangle$. Pokud tedy $\mathrm{NSD}(k, n) = 1$, dostáváme $\langle a^k \rangle = \mathbf{G}$, v opačném případě $a \notin \langle a^k \rangle = \{(a^k)^l : l \in \mathbb{Z}\} = \{a^{kl \bmod n} : l \in \mathbb{Z}\}$, protože $\mathrm{NSD}(k, n) \mid kl \bmod n$. Čili generátorů je tolik, kolik čísel nesoudělných s n, tedy $\varphi(n)$.

Nyní uvažujme $d \mid n$ obecné. Nejprve si všimneme, že pro každé $k \mid n$ existuje právě jedna podgrupa velikosti k: všechny podgrupy jsou cyklické, podle Lemmatu 4.2 tvaru $\langle a^l \rangle$, $l \mid n$, přičemž tyto jsou po dvou různé, protože mají různé velikosti $|\langle a^l \rangle| = n/l$. Přitom tato jediná k-prvková podgrupa obsahuje právě $\varphi(k)$ generátorů, tedy prvků řádu k. □

Tvrzení o počtu generátorů lze použít k pěknému důkazu následující kombinatorické identity.

Tvrzení 4.4. *Pro každé* $n \in \mathbb{N}$ *platí* $\sum_{d \mid n} \varphi(d) = n$*.*

Důkaz. Budeme počítat počet prvků grupy $\mathbb{Z}_n$ dvěma způsoby. Jeden je způsob triviální: grupa obsahuje čísla $0, \ldots, n-1$, tedy $|\mathbb{Z}_n| = n$. Podruhé spočítáme prvky podle řádů: přípustné řády jsou $d \mid n$, tedy $|\mathbb{Z}_n| = \sum_{d \mid n} u_d$, kde u_d značí počet prvků řádu d. Tvrzení 4.3 říká, že $u_d = \varphi(d)$. □

4.2. Multiplikativní grupy konečných těles jsou cyklické.

Následující věta má dalekosáhlé důsledky v teorii konečných těles i v teorii čísel.

Věta 4.5. *Buď* $\mathbf{G}$ *konečná podgrupa grupy* $\mathbf{T}^*$*, kde* $\mathbf{T}$ *je nějaké těleso. Pak* $\mathbf{G}$ *je cyklická.*

Speciálně grupy $\mathbb{Z}_p^*$ jsou cyklické pro každé prvočíslo p. Toto tvrzení lze interpretovat čistě v jazyce elementární teorie čísel tak, že pro každé prvočíslo p existuje číslo a (generátor té grupy) takové, že každé $b \in \{1, \ldots, p-1\}$ lze vyjádřit jako $b = a^k \bmod p$ pro nějaké $k \in \mathbb{N}$. (Viz též sekce o diskrétním logaritmu níže.)

K důkazu věty použijeme následující kritérium cykličnosti.

Lemma 4.6. *Buď* $\mathbf{G}$ *konečná grupa a předpokládejme, že pro každé* $k \in \mathbb{N}$ *existuje v* $\mathbf{G}$ *nejvýše* k *prvků a splňujících* $a^k = 1$*. Pak je grupa* $\mathbf{G}$ *cyklická.*

Důkaz. Označme u_k počet prvků řádu k v grupě $\mathbf{G}$. Označme $n = |\mathbf{G}|$. Pokud $k \nmid n$, podle Lagrangeovy věty $u_k = 0$. Naopak, pokud $u_k \neq 0$, uvažujme nějaký prvek a řádu k. Podgrupa $\langle a \rangle$ je cyklická řádu k, a tedy všechny prvky $b \in \langle a \rangle$ splňují $b^k = 1$. Podle předpokladu jsme nalezli všechna řešení této rovnice, takže $\langle a \rangle$ je jediná cyklická podgrupa řádu k v $\mathbf{G}$. Podle Tvrzení 4.3 má $\varphi(k)$ generátorů, tedy $u_k = \varphi(k)$.

Shrnuto, pro každé $d \mid n$ platí $u_d = 0$ nebo $u_d = \varphi(d)$. Přitom $\sum_{d \mid n} u_d = n$, a zároveň podle Tvrzení 4.4 je $\sum_{d \mid n} \varphi(d) = n$. Tedy $u_d = \varphi(d)$ pro všechna $d \mid n$, speciálně tedy v $\mathbf{G}$ existuje prvek řádu n, neboli generátor. □

Důkaz Věty 4.5. Podle Věty **??** má polynom $x^k - 1$ nejvýše k kořenů v tělese $\mathbf{T}$. Tedy grupa $\mathbf{G} \leq \mathbf{T}^*$ může obsahovat nejvýše k prvků a splňujících $a^k = 1$ a můžeme aplikovat předchozí kritérium. □

4.3. **Diskrétní logaritmus a aplikace v kryptografii.**

Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa konečného řádu n. Pro každé $b \in G$ existuje právě jeden exponent $k \in \{0, \ldots, n-1\}$ splňující $b = a^k$. Toto číslo nazýváme *diskrétní logaritmus* prvku b o základu a v grupě $\mathbf{G}$ a značíme $\log_a b$. Vidíme, že zobrazení $k \mapsto a^k$ a zobrazení $b \mapsto \log_a b$ jsou navzájem inverzní bijekce mezi množinami $\{0, \ldots, n-1\}$ a G.

Na tomto místě je opět důležité zdůraznit, co je diskrétní logaritmus v aditivním zápise: zde se ptáme po inverzením zobrazení k bijekci $k \mapsto k \cdot a$, tedy $\log_a b$ je to jediné $k \in \{0, \ldots, n-1\}$ splňující $k \cdot a = b$.

Příklad. Uvažujme grupu $\mathbb{Z}_n = \langle a \rangle$, tj. $\mathrm{NSD}(a, n) = 1$ (viz Lemma 4.2). Logaritmus $\log_a b$ je roven tomu (jedinému) $k \in \{0, \ldots, n-1\}$, pro které

$$ka \equiv= b \pmod{n}.$$

Např. v $\mathbb{Z}_{11}$ je $\log_7 4 = 10$, protože $7 \cdot 10 \equiv 4 \pmod{11}$.

Takové k najdeme snadno Eukleidovým algoritmem: spočteme Bézoutovy koeficienty $1 = \mathrm{NSD}(a, n) = ua + vn$ a vidíme, že $b = uab + vnb \equiv ub \cdot a \pmod{n}$, čili $\log_a b = ub \bmod n$.

Příklad. Uvažujme grupu $\mathbb{Z}_p^* = \langle a \rangle$, p prvočíslo. Logaritmus $\log_a b$ je roven tomu (jedinému) $k \in \{0, \ldots, p-2\}$, pro které

$$a^k \equiv b \pmod{p}.$$

Např. v $\mathbb{Z}_{11}^*$ je $\log_7 4 = 6$, protože $7^6 \equiv 4 \pmod{11}$.

Na rozdíl od předchozího příkladu není znám žádný efektivní algoritmus (pracující v čase, který je polynomiální vzhledem k počtu cifer prvočísla p) na výpočet $\log_a b$.

Celý zbytek sekce je míněn jako nástin myšlenek, které jsou za aplikací diskrétního logaritmu v kryptografii. Většina informací je v nějakém smyslu zjednodušená, zájemce o přesný výklad odkazujeme na kryptografickou literaturu, např. [Kob94], [Sch96].

Základní myšlenkou moderní kryptografie je pojem *jednosměrné funkce*. Velmi zjednodušeně řečeno, je to bijektivní zobrazení f takové, že hodnoty $f(x)$ se dají počítat rychle, ale není znám postup, kterým by bylo možné počítat rychle hodnoty inverzního zobrazení $f^{-1}(y)$. S jedním příkladem jsme se právě seznámili: výpočet mocniny o daném základu vs. diskrétní logaritmus v grupě $\mathbb{Z}_p^*$. Druhý nejpoužívanější příklad je založen na výpočtu mocniny o daném exponentu vs. výpočet odmocniny.

- Buď p velké prvočíslo (podle současných standardů $p > 2^{1000}$) a a generátor grupy $\mathbb{Z}_p^*$. Funkce
$$\{0, \ldots, p-2\} \to \{1, \ldots, p-1\}, \quad x \mapsto a^x \bmod p$$
je jednosměrná. Inverzní funkcí je diskrétní logaritmus v grupě $\mathbb{Z}_p^*$.
- Buď N součin dvou přibližně stejně velkých různých prvočísel (podle současných standardů $N > 2^{1000}$) a $k > 1$. Funkce
$$\{0, \ldots, N-1\} \to \{0, \ldots, N-1\}, \quad x \mapsto x^k \bmod N$$
je jednosměrná. Inverzní funkcí je „k-tá odmocnina modulo N“.

Mocnění a diskrétní logaritmus lze uvažovat i v řadě jiných grup, nejsilnější aplikace mají grupy odvozené z eliptických křivek. Pro ilustraci ukážeme dva kryptografické protokoly založené na diskrétním logaritmu (*Diffie-Hellmanův protokol* pro výměnu klíče a *El Gamalův protokol* pro kryptografii s veřejným klíčem) a pro srovnání jeden založený na odmocnině (asi nejznámější protokol s veřejným klíčem *RSA*). V současné době jde patrně o nejpoužívanější kryptosystémy.

Začneme velmi jednoduchou aplikací, pro kterou je možné využít jakoukoliv jednosměrnou funkci.

Hod mincí. Alice a Bob si chtějí na dálku (třeba po telefonu) zahrát hru „panna nebo orel“. Alice bude házet mincí, Bob hádat. Jak to ale udělat, aby Alice Boba nepodvedla, když se Bob nemůže na minci podívat? Zvolme nějakou jednosměrnou funkci f na množině $\{1, \ldots, n\}$. Pokud Alice hodí orla, zvolí náhodné liché číslo x, v opačném případě zvolí sudé číslo. Bobovi pošle hodnotu $f(x)$. Protože je f jednosměrná, Bob neumí spočítat, co padlo, zvolí tedy odpověď náhodně. Nyní Alice zveřejní číslo x a Bob ihned vidí, zda vyhrál nebo ne. Může Alice podvádět? Dejme tomu, že padl orel a to samé si tipnul Bob. Aby Alice Boba podvedla, musela by Bobovi ukázat sudé y takové, že $f(y) = f(x)$. Jenže takové y neexistuje, když je f bijekce.

Diffie-Hellman. Jednou ze základních kryptografických úloh je následující: Alice a Bob se potřebují dohodnout na nějakém společném hesle (odborně *klíči*), přičemž k dispozici mají pouze veřejný kanál (např. odposlouchávaný telefon). Jak to provést?

Nejprve se Alice a Bob dohodnou na nějaké cyklické grupě $\mathbf{G} = \langle a \rangle$, ve které je mocnění rychlé, ale výpočet diskrétního logaritmu pomalý, třeba $\mathbb{Z}_p^*$ pro velké p. (Tato informace nepříteli nepomůže, mohou se domluvit libovolným veřejným kanálem.) Dále si Alice zvolí číslo m a Bob číslo n z intervalu $0, \ldots, |G| - 1$, přičemž každý bude svoje číslo držet v tajnosti. Pak provedou následující operace: Alice spočte $x = a^m$ a pošle x Bobovi, Bob spočte $y = a^n$ a pošle y Alici. Poté Alice spočte $y^m = (a^n)^m = a^{mn}$ a Bob spočte $x^n = (a^m)^n = a^{mn}$. Oba tedy získali stejný prvek a^{mn} a ten prohlásí za hledaný klíč.

Kdyby nepřítel poslouchal jejich komunikaci, co zjistí? Bude znát grupu $\mathbf{G}$, generátor a a hodnoty $x = a^m$ a $y = a^n$; chtěl by spočítat prvek a^{mn}. Tomuto problému se říká *Diffie-Hellmanův problém*. V současné době je známo jediné řešení: použitím diskrétního logaritmu získat z hodnot x, y čísla m, n, vynásobit je a dopočítat a^{mn}.

RSA (Rivest-Shamir-Adleman). Problém je následující: Alice (nebo kdokoliv jiný) chce poslat zprávu Bobovi tak, aby nikdo jiný nepřečetl, co v ní je. Bob publikuje tzv. *veřejný klíč*, pomocí něhož může Alice (nebo kdokoliv jiný) zašifrovat svoji zprávu a poslat ji Bobovi. Pouze Bob ovšem zná *soukromý klíč*, pomocí něhož lze zprávu dešifrovat. Popíšeme, jak generovat klíče a jak šifrovat a dešifrovat zprávu.

Na začátku Bob vygeneruje dvě různá přibližně stejně velká prvočísla p, q a spočte $N = pq$. Dále náhodně zvolí číslo e nesoudělné s $\varphi(N) = (p-1)(q-1)$ a pomocí Eukleidova algoritmu spočte číslo d splňující

$$de \equiv 1 \pmod{\varphi(N)}.$$

Čísla N, e budou *veřejným klíčem* (ten Bob rozhlásí do světa), čísla d, p, q budou *soukromým klíčem* (ten bude Bob držet v tajnosti).

Nyní kdykoliv chce někdo poslat Bobovi zprávu, provede následující (pro jednoduchost budeme předpokládat, že zprávu tvoří nějaké přirozené číslo $0 < x < N$

nesoudělné s N): vypočítá

$$y = x^e \bmod N$$

a výsledek pošle libovolným komunikačním kanálem Bobovi.

I když y zachytí nepřítel, nejsou v současné době známy prostředky, jak získat z čísel N, e, y číslo x: je-li N dostatečně velké, neumí se v rozumném čase spočítat ani e-tá odmocnina mod N, ani prvočísla p, q (pomocí nichž by šlo rychle dopočítat soukromý klíč d), a není znám ani jiný způsob, jak RSA prolomit.

Bob, se znalostí soukromého klíče d, ovšem dešifruje snadno: protože $ed \equiv 1 \pmod{\varphi(N)}$, podle Eulerovy věty je

$$y^d \equiv \left(x^e\right)^d = x^{ed} \equiv x^1 = x \pmod{N},$$

takže Bob získá x výpočtem

$$x = y^d \bmod N.$$

Protokol RSA využívá tzv. *zadní vrátka* (*trapdoor*) pro funkci odmocňování modulo N. Obecně se zadními vrátky rozumí dodatečná informace, která činí jednosměrnou funkci obousměrnou. V tomto případě jde o znalost d splňujícího $de \equiv 1 \pmod{\varphi(N)}$, které umožňuje počítat $\sqrt[e]{y}$ jako y^d. Útok proti RSA tak lze vést dvěma způsoby: proti jednosměrné funkci (najít rychlý algoritmus na výpočet odmocniny) i proti zadním vrátkům (nalezení rychlého způsobu výpočtu d bez znalosti p, q).

El Gamal. Tento protokol řeší stejnou úlohu jako RSA, ale je založen na diskrétním logaritmu, nikoliv odmocňování. Bob zvolí *vhodnou* cyklickou grupu $\mathbf{G} = \langle a \rangle$, náhodné číslo $k \in \{0, \ldots, |G| - 1\}$ a spočte $b = a^k$. *Veřejným klíčem* bude $\mathbf{G}, a, b$, *soukromým klíčem* bude k.

Odesílatel zprávy zvolí náhodné číslo $l \in \{0, \ldots, |G| - 1\}$ (které bude držet v tajnosti) a zprávu $x \in G$ zašifruje jako dvojici

$$y = (c_1, c_2),$$

kde $c_1 = a^l$ a $c_2 = x \cdot b^l$. Dešifrování pomocí k je snadné:

$$c_2 \cdot c_1^{-k} = x \cdot b^l \cdot (a^l)^{-k} = x \cdot (a^l)^k \cdot (a^l)^{-k} = x.$$

Je vidět, že kdybychom uměli rychle počítat diskrétní logaritmus, okamžitě získáme soukromý klíč. Bohužel to není jediný známý způsob útoku na El Gamalův protokol, například byl nalezen způsob, jak jej prolomit v případě grup $\mathbb{Z}_p^*$. Někdy se tento algoritmus používá s grupami odvozenými z eliptických křivek.

(Znovu zopakujme, že bezpečnost žádného z uvedených protokolů není prokazatelná: spočívá v tom, že přes veškerou mnohaletou snahu *nikdo dosud nenašel* způsob, jak rychle spočítat tajnou informaci bez znalosti informace soukromé.)