NOVý TEXT O GRUPÁCH

DAVID STANOVSKÝ

1. Pojem grupy

1.1. Definice a příklady.

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 poznámky pod ním) 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

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

Říkáme, že H je *uzavřena na grupové operace* a že *tvoří podgrupu* grupy $\mathbf{G}$. Čtveřici $\mathbf{H} = (H, *|_H, '|_H, e)$ pak nazýváme *podgrupou*, přičemž $|_H$ značí restrikci operací na množinu H. Značíme $\mathbf{H} \leq \mathbf{G}$. Podgrupy $\mathbf{G}$ a $\{e\}$ nazýváme *nevlastní*.

V matematice se vyskytují nejrůznější příklady grup, nicméně jsou čtyři základní rodiny, které nacházejí asi největší aplikace: permutační grupy, maticové grupy, grupy geometrických zobrazení a číselné grupy.

Date: 10. června 2019.

Příklad. *Permutační grupy*[1]. Základním příkladem je *symetrická grupa* sestávající 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 $\mathbf{S}_n$. Podgrupy symetrických grup se nazývají permutační grupy, např.

- *alternující grupa* $\mathbf{A}_n$ všech sudých permutací na n prvcích;
- *dihedrální grupa* $\mathbf{D}_{2n}$ všech symetrií pravidelného n-úhelníka; na ni se lze dívat jako na grupu permutací roviny sestávající z izometrií, které zachovávají tento útvar, anebo jako na grupu permutací na množině $1, \ldots, n$ reprezentující jeho vrcholy (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.

Příklad. Speciálním případem permutačních grup jsou grupy zobrazení na různých typech geometrických prostorů (eukleidovské, afinní, projektivní, apod.) zachovávajících jisté vlastnosti (afinní zobrazení, projektivní zobrazení apod.). Příkladem je *Eukleidovská grupa* $E(n)$ sestávající ze všech izometrií (tj. zobrazení zachovávajících vzdálenosti) eukleidovského prostoru $\mathbb{R}^n$. Tzv. *Erlangenský program* formulovaný Felixem Kleinem v roce 1872 klasifikuje různé typy geometrií pomocí odpovídajících grup geometrických zobrazení.

Příklad. *Maticové grupy*[2]. Základním příkladem je *obecná lineární grupa* nad tělesem $\mathbf{T}$ sestávající z regulárních matic dané velikosti s operacemi $\cdot$ maticového násobení, $^{-1}$ maticového invertování a konstantou E, jednotkovou maticí, tj.

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

Podgrupy lineárních grup se nazývají maticové grupy, např.

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

V sekci **??** si ukážeme, že permutační a maticové grupy jsou v jistém smyslu univerzální příklady: každou grupu lze reprezentaovat jako permutační grupu (*Cayleyova reprezentace*) a každou konečnou grupu lze reprezentovat jako maticovou grupu. Ne každou grupu však lze tímto způsobem reprezentovat nějakým přirozeným způsobem: příkladem je osmiprvková kvaternionová grupa.

Příklad. *Kvaternionová grupa* $\mathbf{Q}$ je definovaná na množině $\{\pm 1, \pm i, \pm j, \pm k\}$. Násobení je dáno vzorci

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

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

[1] Typický čtenář by měl znát základní fakta o permutacích z kurzu lineární algebry nebo diskrétní matematiky. Ostatním doporučujeme nahlédnout do sekce 1.3, kde jsou tyto znalosti zopakovány a doplněny.

[2] Typický čtenář by měl znát základní fakta o maticích z kurzu lineární algebry.

Základním zdrojem abelovských grup jsou grupy odvozené od komutativních okruhů, zejména pak *číselné grupy*, odvozené od číselných oborů.

Příklad. Buď $\mathbf{R}$ komutativní okruh. Pak $(R, +, -, 0)$ je abelovská grupa, tzv. *aditivní grupa* okruhu $\mathbf{R}$. Důležité jsou zejména číselné grupy $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, a také grupy $\mathbb{Z}_n = (\{0, 1, \ldots, n-1\}, +-, 0)$ 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 ověřit, že jde skutečně o grupu: inverz invertibilního prvku je invertibilní (protože $(a^{-1}) \cdot a = 1$) a součin dvou invertibilních prvků a, b je invertibilní (protože $(ab)(b^{-1}a^{-1}) = 1$).

- Je-li $\mathbf{R}$ těleso, pak $\mathbf{R}^* = (R \setminus \{0\}, \cdot, ^{-1}, 1)$.
- Pro polynomiální okruhy platí $\mathbf{R}[x]^* = \mathbf{R}^*$, protože invertibilní jsou právě konstantní polynomy invertibilní v $\mathbf{R}$.
- $\mathbb{Z}^* = (\{1, -1\}, \cdot, ^{-1}, 1)$.
- Prvky grupy $\mathbb{Z}_n^*$ 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, uvažujme 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 $a^{-1} = u \bmod n$.

Zajímavé podgrupy číselných grup poskytuje jednotková kružnice v komplexní rovině.

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 $x^n - 1$,
- *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.

Prüferovy grupy jsou oblíbeným protipříkladem na řadu vlastností.

Existuje řada dalších geometrických i algebraických konstrukcí abelovských grup, například grupy odvozené od eliptických křivek nebo třídové grupy prvoideálů v číselných tělesech. Některé z těchto konstrukcí mají významné aplikace v kryptografii.

Posledním příkladem, který uvedeme, bude konstrukce direktního součinu.

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.

V případě, kdy $\mathbf{G}_1 = \cdots = \mathbf{G}_n = \mathbf{G}$, hovoříme o *direktní mocnině* a značíme ji $\mathbf{G}^n$.

Podobně jako v případě komutativních okruhů, definice grupy obsahuje pouze minimální množství podmínek. Následující tvrzení ukazuje několik aritmetických pravidel, které z definice snadno plynou a v dalším textu je budeme používat bez dalších odkazů.

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* $u \in G$, *pak* $u = e$ (jednoznačnost jednotky);
(3) *jestliže* $a * u = e$ *nebo* $u * a = e$ *pro nějaké* $u \in G$, *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 $(a * b)' = b' * a'$. □

1.2. **Mocniny a řád prvku.**

Čtenář si snad již zažil, že grupové operace se značí nejrůznějšími způsoby. Nadále se budeme držet multiplikativního zápisu. Nebude-li výslovně uvedeno jinak, uvažujeme-li grupu $\mathbf{G}$, implicitně rozumíme $\mathbf{G} = (G, \cdot, ^{-1}, 1)$. Ze začátku je dobré si u všech výrazů rozmýšlet, jak bychom je přepsali do ostatních značení.

Důležitou roli hrají v grupách mocniny. Buď $\mathbf{G}$ grupa, $a \in G$, $n \in \mathbb{Z}$. Označme

$$a^n = \begin{cases} 1 & n = 0 \\ \underbrace{a \cdot a \cdot \ldots \cdot a}_{n} & n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{-n} & n < 0 \end{cases}$$

Tvrzení 1.2. *Buď* $\mathbf{G}$ *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 vidíme, 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 značení je mocninou výraz $a + \ldots + a$, resp. $(-a) + \ldots + (-a)$; tyto výrazy zkracujeme jako $n \cdot a$. Tvrzení 1.2 se pak přepíše jako

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

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 $\mathbb{Z}$“, neboli $\mathbb{Z}$-modulů.

Řádem grupy $\mathbf{G}$ se rozumí počet prvků její nosné množiny, značíme jej $|\mathbf{G}|$ (tj., formálně vzato, $|\mathbf{G}| = |G|$).

Řádem prvku a v grupě $\mathbf{G}$ se rozumí nejmenší $n \in \mathbb{N}$ takové, že $a^n = 1$, pokud takové n existuje, resp. ∞ v opačném případě. V Tvrzení 2.5 si ukážeme, že řád prvku je roven řádu jisté podgrupy, ale zatím si vystačíme s definicí pomocí mocnin.

Příklad. Pokud mluvíme o řádu jistého prvku, je třeba říci, v které grupě!

- $\operatorname{ord}(2) = 7$ v grupě $\mathbb{Z}_7$, protože $7 \cdot 2 \equiv 0 \pmod 7$, ale $n \cdot 2 \not\equiv 0 \pmod 7$ pro $n = 1, \ldots, 6$;
- $\operatorname{ord}(2) = 3$ v grupě $\mathbb{Z}_7^*$, protože $2^3 \equiv 1 \pmod 7$, ale $3^n \not\equiv 1 \pmod 7$ pro $n = 1, 2$.

Příklad. V nekonečných grupách mohou řády vycházet všelijak:

- v grupě $\mathbb{Q}$ je $\operatorname{ord}(0) = 1$ a $\operatorname{ord}(a) = \infty$ pro všechna $a \neq 0$;
- v grupě $\mathbb{Q}^*$ je $\operatorname{ord}(1) = 1$, $\operatorname{ord}(-1) = 2$ a $\operatorname{ord}(a) = \infty$ pro všechna $a \neq \pm 1$;
- v grupě $\mathbb{C}^*$ existuje prvek libovolného řádu: $\operatorname{ord}(e^{2\pi i/k}) = k$.

Příklad. V konečných grupách řády nevycházejí všelijak:

- v grupě $\mathbb{Z}_6$ je $\operatorname{ord}(0) = 1$, $\operatorname{ord}(1) = 6$, $\operatorname{ord}(2) = 3$, $\operatorname{ord}(3) = 2$, $\operatorname{ord}(4) = 3$ a $\operatorname{ord}(5) = 6$, čili vyskytují se řády $1, 2, 3, 6$;
- v grupě $\mathbf{S}_3$ je $\operatorname{ord}(id) = 1$, $\operatorname{ord}((i\ j)) = 2$, $\operatorname{ord}((i\ j\ k) = 3$, čili vyskytují se řády $1, 2, 3$.

V posledním příkladu si všimněte, že řád každého prvku dělí řád celé grupy. To není náhoda, nýbrž pravidlo, které je speciálním případem Lagrangeovy věty 2.6, která je náplní příští sekce.

1.3. **Základní vlastnosti permutací.**

V tomto odstavci shrneme poznatky, které by měl typický čtenář mít ze základního kurzu lineární algebry nebo diskrétní matematiky, a doplníme je o pojem konjugace.

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 $X = \{1, \ldots, n\}$, značíme $\mathbf{S}_X = \mathbf{S}_n$.

Cyklus v permutaci π je posloupnost $a_1, \ldots, a_k$ navzájem různých prvků množiny X splňující $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, …, $\pi(a_k) = a_1$. *Rozkladem na cykly* se rozumí zápis

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

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

Tvrzení 1.3. *Řád permutace π v grupě $\mathbf{S}_n$ je roven nejmenšímu společnému násobku délek jejích cyklů.*

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

Transpozicí rozumíme permutaci tvaru $(x\ y)$. 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. Z definice snadno plyne, že

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

Z rozkladu $(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k) \circ \ldots \circ (a_1\ a_3) \circ (a_1\ a_2)$ vidíme, 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* $\mathbf{A}_n$.

Permutaci $\rho \circ \pi \circ \rho^{-1}$ nazýváme *permutací konjugovanou* s permutací π podle permutace ρ. Pro

$$\pi = (a_{11}\ a_{12}\ \ldots\ a_{1k_1}) \cdots (a_{m1}\ a_{m2} \ldots\ a_{mk_m})$$

dostáváme

$$\rho \circ \pi \circ \rho^{-1} = (\rho(a_{11})\ \rho(a_{12})\ \ldots\ \rho(a_{1k_1})) \cdots (\rho(a_{m1})\ \rho(a_{m2})\ \ldots\ \rho(a_{mk_m})),$$

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 podle 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 1.4. *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 výše uvedeného výpočtu.
($\Leftarrow$) Jsou-li

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

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 1.4, 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.

2. Podgrupy

2.1. Generátory.

Lemma 2.1. *Průnik podgrup je podgrupa.*

Důkaz. Buď $\mathbf{G}$ grupa, uvažujme podgrupy $\mathbf{H}_i$, $i \in I$, a označme $H = \bigcap_{i\in I} H_i$. Dokážeme, že je množina H uzavřená na grupové operace. Protože $1 \in H_i$ pro všechna $i \in I$, bude 1 náležet i jejich průniku. Nyní uvažujme $a, b \in H$. Tyto leží v každém H_i a díky uzavřenosti na operace tam leží 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.

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

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

Tvrzení 2.2. *Buď $\mathbf{G}$ grupa a $\emptyset \neq X \subseteq G$. Pak*

$$\langle X\rangle_{\mathbf{G}} = \{a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n} :\ n \in \mathbb{N},\ a_1, \ldots, a_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Důkaz. Označme M množinu na pravé straně rovnosti. Je potřeba dokázat, že množina M

(1) tvoří podgrupu,
(2) obsahuje X,
(3) je nejmenší podmnožinou grupy $\mathbf{G}$ splňující tyto podmínky.

(1) Součin dvou prvků z M je jistě v M, jednotka $1 = a^0$ je tam také, a uzavřenost na inverzy plyne ze vztahu $(a_1^{k_1} \cdot \ldots \cdot a_n^{k_n})^{-1} = a_n^{-k_n} \cdot \ldots \cdot a_1^{-k_1} \in M$.

(2) Volbou $n = 1, k_1 = 1$ dostaneme libovolný prvek X.

(3) Uvažujme libovolnou podgrupu $\mathbf{H}$ obsahující X. Tato podgrupa musí obsahovat všechny mocniny a^i, $a \in X$, i jejich libovolné násobky, čili celé M. □

Důsledek 2.3. *Buď $\mathbf{G}$ abelovská grupa a $u_1, \ldots, u_n \in G$. Pak*

$$\langle u_1, \ldots, u_n\rangle_{\mathbf{G}} = \{u_1^{k_1} \cdot u_2^{k_2} \cdot \ldots \cdot u_n^{k_n} :\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

V aditivním zápise, tj. pro abelovskou grupu $\mathbf{G} = (G, +, -, 0)$, dostáváme

$$\langle u_1, \ldots, u_n\rangle_{\mathbf{G}} = \{k_1u_1 + k_2u_2 + \ldots + k_nu_n :\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Vidíme, že generování podgrup lze vyjádřit analogicky jako generování vektorových podprostorů (s jednoznačností je to však složitější).

Příklad. Jedním důležitým typem úlohy je, najít k dané grupě $\mathbf{G}$ co nejmenší množinu generátorů, tj. podmnožinu $X \subseteq G$ takovou, že $\mathbf{G} = \langle X\rangle_{\mathbf{G}}$.

- $\mathbb{Z} = \langle 1\rangle$, $\mathbb{Z}_n = \langle 1\rangle$, $\mathbb{Z} \times \mathbb{Z} = \langle (1, 0), (0, 1)\rangle$, $\mathbb{Q} = \langle \frac{1}{n} : n \in \mathbb{N}\rangle$.
- $\mathbb{Z}_7^* = \langle 3\rangle$, ale $\mathbb{Z}_8^*$ nelze generovat jedním prvkem; platí např. $\mathbb{Z}_8^* = \langle 3, 5\rangle$.
- $\mathbf{S}_n = \langle T\rangle$, kde T je množina všech transpozic, viz Tvrzení 2.4.

Příklad. Druhým důležitým typem úlohy je zjistit, jakou podgrupu generuje daná podmnožina.

- $\langle \frac{3}{4}, \frac{1}{3} \rangle_{\mathbb{Q}} = \{k\frac{3}{4} + l\frac{1}{3} : \ k, l \in \mathbb{Z}\} = \{k\frac{1}{12} : \ k \in \mathbb{Z}\} = \langle \frac{1}{12} \rangle_{\mathbb{Q}}$. První a poslední rovnost plynou z Důsledku 2.3. K důkazu prostřední je potřeba si uvědomit, že na jednu stranu $\frac{3}{4}, \frac{1}{3} \in \langle \frac{1}{12} \rangle_{\mathbb{Q}}$, a na druhou stranu $\frac{1}{12} = \frac{3}{4} - 2 \cdot \frac{1}{3}$, a tedy $\frac{1}{12} \in \langle \frac{3}{4}, \frac{1}{3} \rangle_{\mathbb{Q}}$.
- $\langle \frac{3}{4}, \frac{1}{3} \rangle_{\mathbb{Q}^*} = \{(\frac{3}{4})^k \cdot (\frac{1}{3})^l : \ k, l \in \mathbb{Z}\} = \{3^k \cdot 4^l : \ k, l \in \mathbb{Z}\}$.

Tvrzení 2.4. *Grupa $\mathbf{S}_n$ je generovaná množinou všech transpozic. Grupa $\mathbf{A}_n$ je generovaná množinou všech trojcyklů.*

Důkaz. Libovolný cyklus můžeme rozložit následovně:

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

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

Danou sudou permutaci nejprve rozložíme na transpozice, těch je sudý počet, a tak je seskupíme do sousedících dvojic. Pokud jsou sousedící 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. □

Uvedené množiny generátorů nejsou optimální. Například grupu $\mathbf{S}_n$ je možné generovat jednou transpozicí a jedním n-cyklem. Více příkladů najdete v cvičeních.

Příklad. Ukážeme, že

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

Díky Tvrzení 2.4 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

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

Na závěr dokážeme, že řád prvku (definovaný pomocí mocnin) je roven řádu podgrupy jím generované.

Tvrzení 2.5. *Buď $\mathbf{G}$ grupa a $a \in G$. Pak* $\operatorname{ord}(a) = |\langle a \rangle|$.

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. □

2.2. **Lagrangeova věta.**

Věta 2.6 (Lagrangeova věta, konečná varianta)**.** *Buď* $\mathbf{G}$ *konečná grupa a* $\mathbf{H}$ *její podgrupa. Pak* $|\mathbf{H}|$ *dělí* $|\mathbf{G}|$.

Jako speciální případ dostaneme, že $\mathrm{ord}(a)$ dělí $|\mathbf{G}|$ pro každé $a \in G$.

Ještě speciálnějším případem Lagrangeovy věty je *Eulerova věta*. Zvolme $\mathbf{G} = \mathbb{Z}_n^*$ a $a \in \mathbb{Z}_n^*$, tedy a je celé číslo nesoudělné s n. Pak $\mathrm{ord}(a)$ dělí $|\mathbb{Z}_n^*| = \varphi(n)$, čili $\varphi(n) = k \cdot \mathrm{ord}(a)$. Dostáváme

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

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

Myšlenka důkazu není složitá: celou grupu rozložíme na několik podmnožin, které jsou po dvou disjunktní a stejně velké jako daná podgrupa, čili řád celé grupy bude roven řádu podgrupy krát počet těchto podmonžin. Nesamozřejmou částí důkazu je konstrukce tohoto rozkladu.

Definice. Buď $\mathbf{G}$ grupa a $\mathbf{H}$ její podgrupa:

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

$$[\mathbf{G} : \mathbf{H}] = |\{aH : \ a \in G\}|;$$

Poznámka. Pojmy, které jsme definovali, se někdy používají s přívlastkem *levý*, tj. levé rozkladové třídy, levá transverzála, levý index. *Pravými rozkladovými třídami* pak rozumíme množiny $Ha = \{ha : \ h \in H\}$ a ostatní pojmy se definují analogicky. Levé a pravé varianty mohou být stejné či různé (viz příklady níže), ale počet rozkladových tříd, tj. index, vyjde z obou stran stejně. V konečném případě je to zřejmý důsledek Lagrangeovy věty, nicméně tento fakt platí pro grupy libovolné velikosti: mezi levým a pravým rozkladovem je bijekce definovaná

$$aH \mapsto Ha^{-1}.$$

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 2.10

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

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

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

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

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

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

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

Lemma 2.7. *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 2.8. *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. □

Lagrangeovu větu lze formulovat i pro nekonečné grupy, s použitím kardinálních čísel pro označení velikostí množin. Čtenáři, který kardinální čísla neviděl, postačí k porozumění tvrzení vlastnost, že součin velikostí množin je roven velikosti kartézského součinu, tj. $|X| \cdot |Y| = |X \times Y|$. Důkaz věty funguje pro konečné i nekonečné množiny stejně.

Věta 2.9 (Lagrangeova věta, obecná varianta)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pak*

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

Důkaz. Zvolme nějakou transverzálu T a napišme

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

Podle Lemmatu 2.7 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 2.8 a ve čtvrté rovnosti jsme použili vztah $|T| = [\mathbf{G} : \mathbf{H}]$, který plyne z Lemmatu 2.7. □

Na závěr sekce ukážeme důležité kritérium, podle kterého se snadno pozná, zda jsou dvě rozkladové třídy stejné.

Tvrzení 2.10. *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

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

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

3. Grupové homomorfismy

3.1. Základní vlastnosti.

Slovo homomorfismus v matematice označuje zobrazení, která zachovávají základní strukturu matematických objektů. Například v lineární algebře to jsou zobrazení zachovávající sčítání a skalární násobení. V teorii grafů to jsou zobrazení zachovávající hrany. Podobně, v teorii grup to budou zobrazení zachovávající základní grupové operace. Jak si později ukážeme, homomorfismy přenášejí řadu dalších vlastností, např. v obou grupách panuje úzký vztah mezi podgrupami či řády prvků.

V celé sekci budeme uvažovat dvě grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ a $\mathbf{H} = (H, *, ', e)$. Zobrazení $\varphi : G \to H$ je *homomorfismem* těchto grup, pokud pro každé $a, b \in G$ platí

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b), \qquad \varphi(a^{-1}) = \varphi(a)', \qquad \varphi(1) = e.$$

Fakt, že je zobrazení mezi grupami homomorfismem, budeme zapisovat $\varphi : \mathbf{G} \to \mathbf{H}$.

Hned na začátku je dobré si všimnout, že druhá a třetí rovnost plynou z té první, což znatelně zjednodušuje ověřování, zda je dané zobrazení homomorfismem.

Lemma 3.1. *Buď* $\mathbf{G}, \mathbf{H}$ *grupy a* $\varphi : G \to H$ *zobrazení. Pak* φ *je homomorfismem těchto grup právě tehdy, když* $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ *pro všechna* $a, b \in G$*.*

Důkaz. Nejprve dokážeme, že $\varphi(1) = e$. Protože $e * \varphi(1) = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) * \varphi(1)$, krácením dostaneme $\varphi(1) = e$. Dále dokážeme $\varphi(a^{-1}) = \varphi(a)'$ pro každé $a \in G$. Protože $e = \varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a) * \varphi(a^{-1})$, z jednoznačnosti inverzních prvků v grupě $\mathbf{H}$ plyne $\varphi(a^{-1}) = \varphi(a)'$. □

Obrazem homomorfismu nazýváme jeho obor hodnot, tj. množinu

$$\mathrm{Im}(\varphi) = \{b \in H : \ b = \varphi(a) \text{ pro nějaké } a \in G\}.$$

Jádro homomorfismu definujeme jako množinu

$$\mathrm{Ker}(\varphi) = \{a \in G : \ \varphi(a) = e\}.$$

Tvrzení 3.2. *Buď* $\mathbf{G}, \mathbf{H}$ *grupy a* $\varphi : \mathbf{G} \to \mathbf{H}$ *homomorfismus. Pak*

(1) $\mathrm{Im}(\varphi)$ *tvoří podgrupu grupy* $\mathbf{H}$*;*
(2) $\mathrm{Ker}(\varphi)$ *tvoří normální podrupu grupy* $\mathbf{G}$*;*
(3) φ *je prostý právě tehdy, když* $\mathrm{Ker}(\varphi) = \{1\}$.

Důkaz. (1) $e \in \mathrm{Im}(\varphi)$, protože $e = \varphi(1)$. Pokud $\varphi(a), \varphi(b) \in \mathrm{Im}(\varphi)$, pak $\varphi(a)' = \varphi(a^{-1}) \in \mathrm{Im}(\varphi)$ a $\varphi(a) * \varphi(b) = \varphi(a \cdot b) \in \mathrm{Im}(\varphi)$.

(2) $1 \in \mathrm{Ker}(\varphi)$, protože $\varphi(1) = e$. Pokud $a, b \in \mathrm{Ker}(\varphi)$, pak a^{-1} a $a \cdot b$ také, protože $\varphi(a^{-1}) = \varphi(a)' = e' = e$ a $\varphi(a{\cdot}b) = \varphi(a){*}\varphi(b) = e{*}e = e$. Normalita plyne z toho, že pro libovolné $u \in G$ platí $\varphi(uau^{-1}) = \varphi(u){*}\varphi(a){*}\varphi(u)' = \varphi(u){*}\varphi(u)' = e$.

(3) Je-li φ prosté, dva různé prvky se nemohou zobrazovat na e, takže $\mathrm{Ker}(\varphi)$ musí obsahovat jen jeden prvek, a tím je 1. Naopak, $\varphi(a) = \varphi(b)$ právě tehdy, když $e = \varphi(a) * \varphi(b)' = \varphi(ab^{-1})$, takže neprostá zobrazení obsahují nejednotkový prvek v jádru. □

Příklad. Řada známých zobrazení v matematice je homomorfismem jistých grup.

- Uvažujme zobrazení $z \mapsto |z|$ na komplexních číslech. Toto zobrazení je homomorfismem grup $\mathbb{C}^* \to \mathbb{R}^*$, protože $|a \cdot b| = |a| \cdot |b|$. Jeho jádrem je podgrupa komplexních jednotek, jeho obrazem podgrupa kladných čísel. Naopak, toto zobrazení není homomorfismem grup $\mathbb{C} \to \mathbb{R}$, protože obecně $|a + b| \neq |a| + |b|$.
- Uvažujme zobrazení $z \mapsto e^z$ na komplexních číslech. Toto zobrazení je homomorfismem grup $\mathbb{C} \to \mathbb{C}^*$, protože $e^{a+b} = e^a \cdot e^b$. Jeho jádrem je podgrupa $\langle 2\pi i \rangle = \{k \cdot 2\pi i : \ k \in \mathbb{Z}\}$, jeho obrazem celé $\mathbb{C}^*$.
- Uvažujme zobrazení $A \mapsto \det(A)$ na maticích. Toto zobrazení je homomorfismem grup $\mathbf{GL}_n(\mathbf{T}) \to \mathbf{T}^*$, protože $\det(A \cdot B) = \det(A) \cdot \det(B)$. Jeho jádrem je podgrupa $\mathbf{SL}_n(\mathbf{T})$, jeho obrazem celé $\mathbf{T}^*$.
- Uvažujme zobrazení $\pi \mapsto \mathrm{sgn}(\pi)$ na permutacích. Toto zobrazení je homomorfismem grup $\mathbf{S}_n \to \mathbb{Z}^*$, protože $\mathrm{sgn}(\pi \circ \sigma) = \mathrm{sgn}(\pi) \cdot \mathrm{sgn}(\sigma)$. Jeho jádrem je podgrupa $\mathbf{A}_n$, jeho obrazem celé $\mathbb{Z}^*$.

Tvrzení 3.3. *Buď* $\mathbf{G}, \mathbf{H}, \mathbf{K}$ *grupy a* $\varphi : \mathbf{G} \to \mathbf{H}$*,* $\psi : \mathbf{H} \to \mathbf{K}$ *homomorfismy. Pak*

(1) $\psi \circ \varphi$ *je homomorfismus* $\mathbf{G} \to \mathbf{K}$*,*
(2) *je-li* φ *bijektivní, pak* φ^{-1} *je homomorfismus* $\mathbf{H} \to \mathbf{G}$.

Důkaz. (1) Označme $\mathbf{K} = (K, +, -, 0)$. Pro $a, b \in G$ platí

$$(\psi{\circ}\varphi)(a{\cdot}b) = \psi(\varphi(a{\cdot}b)) = \psi(\varphi(a){*}\varphi(b)) = \psi(\varphi(a)){+}\psi(\varphi(b)) = (\psi{\circ}\varphi)(a){+}(\psi{\circ}\varphi)(b)$$

postupným použitím faktu, že φ a ψ jsou homomorfismy.

(2) Napišme $u, v \in H$ jako $u = \varphi(a)$ a $v = \varphi(b)$ pro jistá $a, b \in G$. Pak

$$\varphi^{-1}(u * v) = \varphi^{-1}(\varphi(a) * \varphi(b)) = \varphi^{-1}(\varphi(a \cdot b)) = a \cdot b = \varphi^{-1}(u) \cdot \varphi^{-1}(v)$$

použitím faktu, že φ je homomorfismus a $\varphi^{-1} \circ \varphi = id$. □

3.2. **Izomorfismus.**

Homomorfismy, které jsou bijekce, nazýváme *izomorfismy*.

Na izomorfismus je možné pohlížet jako na „kopírování“: máme-li grupu $\mathbf{G}$ a bijektivní zobrazení $\varphi : G \to H$, můžeme na množinu H „překopírovat“ grupové operaci předpisem

$$e = \varphi(1), \qquad a' = \varphi((\varphi^{-1}(a))^{-1}), \qquad a * b = \varphi(\varphi^{-1}(a) \cdot \varphi^{-1}(b)).$$

Vidíme, že zobrazení φ^{-1}, a tedy podle Tvrzení 3.3 i zobrazení φ, bude izomorfismus staré grupy $\mathbf{G}$ a nové grupy $\mathbf{H} = (H, *, ', e)$. Jedna grupa je kopií druhé, došlo pouze k přejmenování prvků kopírovacím zobrazením φ. Na každý izormofismus lze pohlížet tímto způsobem.

Dvě grupy $\mathbf{G}, \mathbf{H}$ nazveme *izomorfní*, pokud existuje izomorfismus $\mathbf{G} \to \mathbf{H}$. Tento fakt značíme $\mathbf{G} \simeq \mathbf{H}$. Neformálně, jedna grupa je „kopií“ druhé. Tvrzení 3.3 implikuje, že izomorfismus dává ekvivalenci na třídě všech grup:

- reflexivita: $\mathbf{G} \simeq \mathbf{G}$ je zaručeno izomorfismem $id : \mathbf{G} \to \mathbf{G}$;
- symetrie: je-li $\mathbf{G} \simeq \mathbf{H}$ pomocí izomorfismu φ, pak $\mathbf{H} \simeq \mathbf{G}$ pomocí izomorfismu φ^{-1};
- tranzitivita: je-li $\mathbf{G} \simeq \mathbf{H}$ pomocí izomorfismu φ a $\mathbf{H} \simeq \mathbf{K}$ pomocí izomorfismu ψ, pak $\mathbf{G} \simeq \mathbf{K}$ pomocí izomorfismu $\psi \circ \varphi$.

Na prosté homomorfismy lze nahlížet jako na izomorfismy mezi výchozí grupou a obrazem, tj. prostý homomorfismus $\varphi : \mathbf{G} \to \mathbf{H}$ je izomorfismem $\mathbf{G} \simeq \mathbf{Im}(\varphi)$. Takovým homomorfismům se říká *vnoření* grupy $\mathbf{G}$ do grupy $\mathbf{H}$, tj. grupa $\mathbf{H}$ obsahuje izomorfní kopii $\mathbf{G}$ jako podgrupu.

Příklad. Grupy $\mathbb{Z}_2$ a $\mathbb{Z}^*$ jsou izomorfní. Podívejme se na tabulky jejich operací:

$+$	0	1
0	0	1
1	1	0

$\cdot$	1	-1
1	1	-1
-1	-1	1

Tyto tabulky vypadají podobně: jedna je kopií druhé, pokud přepíšeme $0 \mapsto 1$, $1 \mapsto -1$. Toto zobrazení, které můžeme vyjádřit také jako $a \mapsto (-1)^a$, je grupový izomorfismus.

Příklad. Grupy $\mathbb{C}$ a $\mathbb{R} \times \mathbb{R}$ jsou izomorfní. Intuitivně, komplexní čísla odpovídají dvojicím reálných čísel, v obou interpretacích se sčítají jednotlivé složky. Není těžké ověřit, že zobrazení $a + bi \mapsto (a, b)$ je grupový izomorfismus $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$.

Příklad. Grupy $\mathbb{Z}_n$ a $\mathbb{C}_n = \langle \omega \rangle_{\mathbb{C}^*}$, kde $\omega = e^{2\pi i/n}$, jsou izomorfní. Intuitivně, $\omega^n = 1$ a komplexní čísla tvaru ω^k se násobí tak, že se exponenty sčítají modulo n. Není těžké ověřit, že zobrazení $k \mapsto \omega^k$ je grupový izomorfismus $\mathbb{Z}_n \simeq \mathbb{C}_n$.

Příklad. Všechny tři grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8^*$ a $\{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq \mathbf{S}_4$ jsou navzájem izomorfní. Není to vidět na první pohled, ale intuice se dá vybudovat přes generátory: všechny tři grupy lze napsat jako $\mathbf{G} = \langle a, b \rangle$, kde $a^2 = 1$, $b^2 = 1$ a $ab = ba$ je ten třetí prvek různý od jednotky. Formální důkaz si udělejte jako cvičení.

Důležitým příkladem izomorfismu je modulární zobrazení z čínské věty o zbytcích.

Tvrzení 3.4. *Buďte $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla a označme $M = m_1 \cdot \ldots \cdot m_n$. Zobrazení*

$$\begin{aligned} \varphi : \mathbb{Z}_M &\to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \\ x &\mapsto (x \bmod m_1, \ldots, x \bmod m_n). \end{aligned}$$

je izomorfismem těchto grup.

Důkaz. Pohledem do důkazu čínské věty o zbytcích zjistíme, že je zobrazení φ bijektivní. Ověříme, že to je homomorfismus:

$$\begin{aligned} \varphi(x) + \varphi(y) &= (x \bmod m_1, \ldots, x \bmod m_n) + (y \bmod m_1, \ldots, y \bmod m_n) \\ &= ((x+y) \bmod m_1, \ldots, (x+y) \bmod m_n) = \varphi(x + y \bmod M), \end{aligned}$$

přičemž v poslední rovnosti využíváme faktu, že všechna m_i dělí M. □

3.3. **Neizomorfismus.**

Čínská věta o zbytcích tvrdí, že pro m, n nesoudělná je $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. Jak je tomu pro m, n soudělná? Zobrazení $x \mapsto (x \pmod m), x \pmod n))$ není ani prosté, ani na: čísla 0 i $\mathrm{NSN}(m, n)$ se zobrazí na dvojici $(0, 0)$. Nemohly by ale být izomorfní použitím nějakého jiného izomorfismu?

Podobně, viděli jsme, že zobrazení $a + bi \mapsto (a, b)$ je izomorfismus $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$, ale není to izomorfismus grup $\mathbb{C}^*$ a $\mathbb{R}^* \times \mathbb{R}^*$. Nemohly by být izomorfní použitím nějakého jiného izomorfismu?

Obecným principem, který umožňuje řešit takové úlohy, jsou *invarianty*. Vlastnost V nazveme invariantem, pokud pro každou dvojici izomorfních grup $\mathbf{G} \simeq \mathbf{H}$ platí, že pokud má grupa $\mathbf{G}$ vlastnost V, pak má i grupa $\mathbf{H}$ vlastnost V. Příkladem invariantů je počet prvků daného řádu nebo minimální počet generátorů, jak si nyní dokážeme.

Tvrzení 3.5. *Buď $\varphi : \mathbf{G} \to \mathbf{H}$ izomorfismus grup. Pak pro každé $a \in G$*

$$\mathrm{ord}(a) = \mathrm{ord}(\varphi(a)).$$

Důkaz. Pokud $a^k = 1$, pak $\varphi(a)^k = \varphi(a^k) = \varphi(1) = e$, čili $\mathrm{ord}(\varphi(a)) \leq \mathrm{ord}(a)$. Použitím téhož principu na izomorfismus φ^{-1} dostaneme opačnou nerovnost. □

Příklad.

- Grupa $\mathbb{Z}_{mn}$ obsahuje prvek řádu mn. Avšak v grupě $\mathbb{Z}_m \times \mathbb{Z}_n$ mají všechny prvky řád nejvýše $\mathrm{NSN}(m, n)$. Čili pokud jsou m, n soudělné, tyto grupy nemohou být izormofní.
- Grupa $\mathbb{C}^*$ obsahuje prvky libovolného řádu, avšak grupa $\mathbb{R}^* \times \mathbb{R}^*$ obsahuje pouze prvky řádu $1, 2, \infty$. Čili tyto grupy nejsou izomorfní.
- Kvaternionová grupa $\mathbf{Q}$ i dihedrální grupa $\mathbf{D}_8$ obsahují prvky řádů $1, 2, 4$. Avšak $\mathbf{Q}$ obsahuje šest prvků řádu 4, zatímco $\mathbf{D}_8$ pouze dva, takže nemohou být izomorfní.

Tvrzení 3.6. *Buď $\varphi : \mathbf{G} \to \mathbf{H}$ izomorfismus grup. Je-li $\mathbf{G} = \langle u_1, \ldots, u_n \rangle$, pak $\mathbf{H} = \langle \varphi(u_1), \ldots, \varphi(u_n) \rangle$.*

Důkaz. Prvek $b \in H$ napíšeme jako $b = \varphi(a)$, prvek a vyjádříme v generátorech jako $a = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$, kde $a_i \in \{u_1, \ldots, u_n\}$, a prvek b pak dostaneme jako $b = \varphi(a) = \varphi(a_1)^{k_1} * \ldots * \varphi(a_n)^{k_n}$. □

Na rozdíl od vektorových prostorů, v grupách mohou být minimální generující množiny různě velké, např. $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$. Invariantem je nejmenší počet prvků, který je potřeba k nagenerování dané grupy.

Příklad. Grupy $\mathbb{Z}$ a $\mathbb{Z}\times\mathbb{Z}$ nejsou izormorfní, protože grupu $\mathbb{Z}\times\mathbb{Z}$ nelze nagenerovat jedním prvkem: podgrupa $\langle (a,b) \rangle = \{(ka, kb) : k \in \mathbb{Z}\}$ obsahuje dvojici $(1,1)$ pouze pro $(a,b) = \pm(1,1)$, ale ani jedna z těchto dvojic $\mathbb{Z}\times\mathbb{Z}$ negeneruje. O něco složitější argument by prošel i pro $\mathbb{Z}_{mn} \not\cong \mathbb{Z}_m \times \mathbb{Z}_n$ pro soudělná m, n.

Tyto dva invarianty umožnují prokázat neizomorfismus ve spoustě případů, ale ne ve všech. Příkladem je dvojice grup $\mathbb{Q}$ a $\mathbb{Q}^+ = \{a \in \mathbb{Q} : a > 0\} \leq \mathbb{Q}^*$.

Příklad. Existence odmocnin, tj. vlastnost „pro každé a existuje b takové, že $a = b^2$“, je invariantem. Mějme izomorfismus $\varphi : \mathbf{G} \to \mathbf{H}$ a předpokládejme, že tato vlastnost platí v grupě $\mathbf{G}$. Prvek $u \in H$ napíšeme jako $u = \varphi(a)$, vezmeme $b \in G$ takové, že $a = b \cdot b$ a položíme $v = \varphi(b)$. Vidíme, že $u = \varphi(a) = \varphi(b^2) = \varphi(b)^2 = v^2$.

Tento invariant je splněn v grupě $\mathbb{Q}$, kde jde o vlastnost „pro každé $a \in \mathbb{Q}$ existuje $b \in \mathbb{Q}$ takové, že $a = 2b$“. Ale není splněn v grupě $\mathbb{Q}^+$, kde jde o vlastnost „pro každé $0 \neq a \in \mathbb{Q}$ existuje $0 \neq b \in \mathbb{Q}$ takové, že $a = b^2$“.

Obecně lze říci, že invariantem je každá vlastnost, kterou lze zformulovat pomocí operací dané struktury, rovnosti, logických spojek a kvantifikátorů (tzv. formule prvního řádu).

3.4. **Klasifikační věty.**

Jedním ze základních cílů každé algebraické teorie je tzv. *klasifikace* objektů, tj. *úplný seznam* všech příkladů *až na izomorfismus*. Obvykle není možné provést takovou klasifikace kompletně, ale často je možné klasifikovat objekty s nějakou speciální, nicméně důležitou vlastností.

Asi nejjednodušším příkladem je *klasifikace cyklických grup*: každá cyklická grupa, tj. grupa s jedním generátorem, je izomorfní právě jedné z grup $\mathbb{Z}$ nebo $\mathbb{Z}_n$. Jinými slovy, $\mathbb{Z}$ a $\mathbb{Z}_n$ jsou, až na izomorfismus, všechny příklady cyklických grup.

Věta 3.7. *Buď $\mathbf{G}$ cyklická grupa. Je-li $\mathbf{G}$ nekonečná, pak je izomorfní grupě $\mathbb{Z}$. Je-li $\mathbf{G}$ konečná řádu n, pak je izomorfní grupě $\mathbb{Z}_n$.*

Důkaz. Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa. Nejprve předpokládejme, že je $\mathbf{G}$ nekonečná, tedy $\operatorname{ord}(a) = \infty$, a uvažujme zobrazení

$$\mathbb{Z} \to \mathbf{G}, \qquad k \mapsto a^k.$$

Toto zobrazení je homomorfismus, neboť $a^k \cdot a^l = a^{k+l}$. Přitom jádro je triviální, protože $a^k \neq 1$ pro všechna $k \neq 0$, takže podle Tvrzení 3.2 jde o prosté zobrazení. Podle Tvrzení 2.2 je toto zobrazení na $\mathbf{G}$.

Nyní předpokládejme, že je $\mathbf{G}$ řádu n, tedy $\operatorname{ord}(a) = n$, a uvažujme zobrazení

$$\mathbb{Z}_n \to \mathbf{G}, \qquad k \mapsto a^k.$$

Toto zobrazení je homomorfismus, neboť $a^k \cdot a^l = a^{k+l} = a^{k+l \bmod n}$, přičemž druhá rovnost plyne z následující úvahy: pokud $k + l < n$, tvrzení je triviální; pokud $k+l \geq n$, pak $k+l \bmod n = k+l-n$, a tedy $a^{k+l \bmod n} = a^{k+l} \cdot a^{-n} = a^{k+l} \cdot 1^{-1} = a^{k+l}$. Podobně jako pro nekonečnou grupu dostáváme, že jádro je triviální a že jde o zobrazení na $\mathbf{G}$. □

Mnohem komplikovanější je *klasifikace konečně generovaných abelovských grup*, která říká, že každá abelovská grupa s konečnou množinou generátorů je, až na izomorfismus, direktním součinem konečně mnoha cyklických grup. Navíc, použitím čínské věty o zbytcích ve formě Tvrzení 3.4, konečné cyklické grupy stačí uvažovat pouze ty řádu mocniny prvočísla. Tyto komponenty jsou navíc jednoznačně určené (až na pořadí), tj. volbou neizomorfních cyklických grup dostaneme neizomorfní direktní součin.

Věta 3.8. *Buď* $\mathbf{G}$ *konečně generovaná abelovská grupa,* $|\mathbf{G}| > 1$*. Pak existují* $m, n \geq 0$*, prvočísla* $p_1, \ldots, p_m$ *(ne nutně po dvou různá) a přirozená čísla* $k_1, \ldots, k_m$ *taková, že*

$$\mathbf{G} \simeq \mathbb{Z}^n \times \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

Čísla m, n *jsou určena jednoznačně a čísla* $p_1, \ldots, p_m$ *a* $k_1, \ldots, k_m$ *jednoznačně až na pořadí.*

Důkaz této věty nevyžaduje žádnou složitou teorii, ale je poměrně zdlouhavý, proto jej přenecháme do některého navazujícího kurzu.

Příklad. Podle Věty 3.8 je každá čtyřprvková abelovská grupa izomorfní buď grupě $\mathbb{Z}_4$, nebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- Grupa $\mathbb{Z}_5^*$ je také čtyřprvková. Vidíme, že $\operatorname{ord}(2) = 4$, takže $\mathbb{Z}_5^* \simeq \mathbb{Z}_4$.
- Grupa $\mathbb{Z}_8^*$ je také čtyřprvková. Vidíme, že $\operatorname{ord}(3) = \operatorname{ord}(5) = \operatorname{ord}(7) = 2$, takže $\mathbb{Z}_8^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Oblíbenou kratochvílí v historii teorie grup bylo a je hledání malých grup, což je svým způsobem také klasifikační věta. Následující tabulka obsahuje klasifikaci všech grup řádu n pro $n \leq 15$ a pro $n = p$, $2p$, p^2, kde p je prvočíslo. V současné době je znám seznam všech grup až do velikosti $2047 = 2^{11} - 1$.

n	grupy řádu n
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	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbf{D}_8,\ \mathbf{Q}$
	$\ldots$
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p$
$2p$	$\mathbb{Z}_{2p},\ \mathbf{D}_{2p}$
12	$\mathbb{Z}_4 \times \mathbb{Z}_3,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \mathbf{A}_4, \mathbf{D}_{12}, \mathbf{X}$
15	$\mathbb{Z}_3 \times \mathbb{Z}_5$

Případ $n = p$ je důsledkem Lagrangeovy věty: grupa prvočíselné velikosti nemůže mít vlastní podgrupy, takže musí být generovaná libovolným svým prvkem $\neq 1$ a podle klasifikace cyklických grup musí být izomorfní $\mathbb{Z}_p$.

4. Cyklické grupy

Grupa $\mathbf{G}$ se nazývá *cyklická*, pokud je generovaná jedním prvkem, tj. $\mathbf{G} = \langle a \rangle_{\mathbf{G}}$ pro nějaké $a \in G$. Její prvky lze díky Tvrzení 2.2 vyjádřit jako mocniny generátoru,

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

Z Tvrzení 2.5 plyne, že je-li řád a nekonečný, pak jsou tyto mocniny po dvou různé, a je-li $\mathrm{ord}(a) = n$ konečný, pak $G = \{a^0, a^1, \ldots, a^{n-1}\}$. Odsud pochází název pro cyklické grupy: při násobení daným prvkem a cyklicky procházíme přes všechny prvky grupy $\mathbf{G}$.

Klasifikace cyklických grup (Věta 3.7) říká, že každá cyklická grupa je izomorfní jedné z grup $\mathbb{Z}$, $\mathbb{Z}_n$. Přirozených příkladů je však více.

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, $\mathbb{C}_n = \langle e^{2\pi i/n} \rangle$.
- Grupy $\mathbb{Z}_p^*$ jsou cyklické pro každé prvočíslo p, jak plyne z Věty 4.6. 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. grupa $\mathbb{Z}_8^*$ cyklická není.
- Každá grupa $\mathbf{G}$ prvočíselného řádu je cyklická. Uvažujme podgrupu $\langle a \rangle$, $a \neq 1$. Podle Lagrangeovy věty je $|\langle a \rangle|$ dělí $|\mathbf{G}|$, přitom $|\langle a \rangle| > 1$, tedy $|\langle a \rangle| = |\mathbf{G}|$ 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 $a^n \in H \setminus \langle a^k \rangle$. Nutně $k \nmid n$, jinak bychom měli $a^n = (a^k)^{n/k} \in \langle a^k \rangle$. Napišme $n = kq + r$, kde $0 < r < k$. Pak

$$a^r = a^{n-kq} = a^n \cdot (a^k)^{-q} \in H,$$

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

Tvrzení nelze obrátit: Prüferova grupa $\mathbb{C}_{p^\infty}$ je příkladem grupy, která není cyklická (ani konečně generovaná), přestože všechny její vlastní podgrupy cyklické jsou.

Lemma 4.2. *Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa. Pak*

(1) $\langle a^k, a^l \rangle = \langle a^{\mathrm{NSD}(k,l)} \rangle$,
(2) *je-li $|\mathbf{G}| = n$, pak $\langle a^k \rangle = \langle a^{\mathrm{NSD}(k,n)} \rangle$.*

Důkaz. (1) Protože $\mathrm{NSD}(k, l)$ dělí k i l, platí $a^k, a^l \in \langle a^{\mathrm{NSD}(k,l)} \rangle$, čímž máme prokázánu inkluzi $\subseteq$. Naopak, podle Bézoutovy rovnosti je $\mathrm{NSD}(k, l) = uk + vl$ pro nějaká $u, v \in \mathbb{Z}$, a tedy

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

čímž máme prokázánu inkluzi $\supseteq$.

(2) dostaneme dosazením $l = n$: pak $\langle a^{\mathrm{NSD}(k,n)}\rangle = \langle a^k, a^n\rangle = \langle a^k\rangle$, protože $a^n = 1$. □

Příklad. Grupa $\mathbb{Z}$ je cyklická, čili její podgrupy jsou cyklické, tedy 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 $k = \pm l$. Podgrupy jsou tedy ve vzájemně jednoznačné korepondenci s nezápornými čísly a $k\mathbb{Z} \subseteq l\mathbb{Z}$ právě tehdy, když $l \mid k$. Čili podgrupy jsou uspořádány vzhledem k inkluzi opačně než množina $\mathbb{N} \cup \{0\}$ dělitelností.

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

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

Z Lemmatu 4.2(2) s volbou $a = 1$ plyne, že $k\mathbb{Z}_n = \mathrm{NSD}(k,n)\mathbb{Z}_n$, tedy $k\mathbb{Z}_n = l\mathbb{Z}_n$ právě tehdy, když $\mathrm{NSD}(k,n) = \mathrm{NSD}(l,n)$. Podgrupy jsou tedy ve vzájemně jednoznačné korepondenci s děliteli čísla n. Přitom $k\mathbb{Z}_n \subseteq l\mathbb{Z}_n$ právě tehdy, když $l \mid k$. Čili pogrupy jsou uspořádány vzhledem k inkluzi opačně než množina všech dělitelů čísla n dělitelností.

Nyní se budeme věnovat generátorům cyklických grup.

Tvrzení 4.3. *Buď $\mathbf{G} = \langle a\rangle$ cyklická grupa. Pokud je nekonečná, generátorem jsou pouze prvky a, a^{-1}. Pokud je konečná řádu n, generátorem jsou právě prvky a^k pro $k \in \{1, \dots, n-1\}$ nesoudělná s n.*

Důkaz. Nejpve rozebereme nekonečný případ. Oba prvky a, a^{-1} grupu $\mathbf{G}$ generují, protože $\{a^k :\ k \in \mathbb{Z}\} = \{a^{-k} :\ k \in \mathbb{Z}\}$. Žádný jiný generátor grupa $\mathbf{G}$ nemá: kdyby $\mathbf{G} = \langle a^n\rangle$ pro nějaké n, pak by existovalo $m \in \mathbb{Z}$ takové, že $a = (a^n)^m$, a dostali bychom $1 = (a^n)^m \cdot a^{-1} = a^{mn-1}$; řád a je ovšem nekonečný, a tedy $mn = 1$, čili $n = \pm 1$.

Nyní uvažujme konečnou cyklickou grupu řádu n. Podle Lemmatu 4.2 je $\langle a^k\rangle = \langle a^{\mathrm{NSD}(k,n)}\rangle$. Pokud $\mathrm{NSD}(k,n) = 1$, pak $\langle a^k\rangle = \langle a\rangle = \mathbf{G}$. Pokud $\mathrm{NSD}(k,n) = d \neq 1$, pak $\langle a^k\rangle = \langle a^d\rangle = \{a^d, a^{2d}, \dots, a^{\frac{n}{d}d}\}$ je vlastní podgrupa. □

Z tvrzení plyne, že cyklická grupa řádu n má právě $\varphi(n)$ generátorů, kde φ značí Eulerovu funkci.

O něco obecnější úlohou je spočítat počet prvků daného řádu. V nekonečných cyklických grupách mají všechny prvky kromě jednotky řád nekonečný. V konečných grupách dává Lagrangeova věta omezení na přípustné řády. Ukážeme si, že v cyklických grupách prvky všech přípustných řádů existují a jejich počet je dán Eulerovou funkcí.

Tvrzení 4.4. *Cyklická grupa konečného řádu n obsahuje právě $\varphi(d)$ prvků řádu d pro každé $d \mid n$.*

Důkaz. Buď $\mathbf{G}$ cyklická grupa konečného řádu n. Každý prvek řádu $d \mid n$ je generátorem nějaké cyklické podgrupy řádu d. Taková podgrupa však v $\mathbf{G}$ existuje pouze jedna: podle Lemmatu 4.2 jsou všechny podgrupy v $\mathbf{G}$ tvaru $\langle a^k\rangle$, $k \mid n$. Přitom $|\langle a^k\rangle| = \frac{n}{k}$, čili $\langle a^{\frac{n}{d}}\rangle$ je jediná podgrupa řádu d. Ta má podle Tvrzení 4.3 právě $\varphi(d)$ generátorů. □

Tvrzení o počtu prvků daného řádu lze použít k důkazu následující kombinatorické identity.

Tvrzení 4.5. *Pro každé $n \in \mathbb{N}$ platí $\sum_{d|n} \varphi(d) = n$.*

Důkaz. Budeme počítat počet prvků grupy $\mathbb{Z}_n$ dvěma způsoby. Jeden způsob je 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 $|\mathbb{Z}_n| = \sum_{d|n} u_d$, kde u_d značí počet prvků řádu d. Tvrzení 4.4 říká, že $u_d = \varphi(d)$. □

Následující věta má dalekosáhlé důsledky v teorii konečných těles.

Věta 4.6. *Buď $\mathbf{T}$ těleso a $\mathbf{G}$ konečná podgrupa grupy $\mathbf{T}^*$. Pak $\mathbf{G}$ je cyklická.*

Speciálním případem je fakt, že 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 právě jedním způsobem jako $b = a^k \bmod p$ pro nějaké $k \in \{0, \ldots, p-2\}$.

Důsledkem Věty 4.6 je, že každé konečné těleso $\mathbf{T}$ lze napsat jako $\mathbf{T} = \mathbb{Z}_p(a)$ pro jisté $a \in T$, konkrétně pro libovolný generátor a grupy $\mathbf{T}^*$. Pozor, v tělese $\mathbf{T} = \mathbb{Z}_p[\alpha]/(m)$ není prvek α nutně generátorem $\mathbf{T}^*$: například v $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ generuje α pouze čtyřprvkovou podgrupu.

K důkazu věty použijeme následující kritérium cykličnosti.

Lemma 4.7. *Buď $\mathbf{G}$ konečná grupa a předpokládejme, že pro každé k existuje v $\mathbf{G}$ nejvýše k prvků a splňujících $a^k = 1$. Pak je grupa $\mathbf{G}$ cyklická.*

Důkaz. Označme $n = |\mathbf{G}|$ a u_k počet prvků řádu k v grupě $\mathbf{G}$. Podle Lagrangeovy věty je $u_k = 0$ pro všechna $k \nmid n$, a tedy $n = \sum_{d|n} u_d$ (počítáme prvky $\mathbf{G}$ podle jejich řádu jako v Tvrzení 4.5).

Uvažujme nějaký prvek a řádu k v $\mathbf{G}$. Podgrupa $\langle a \rangle$ je cyklická řádu k a všechny prvky $b \in \langle a \rangle$ splňují $b^k = 1$. Podle předpokladu v $\mathbf{G}$ žádné jiné prvky s touto vlastností nejsou, takže $\langle a \rangle$ je jediná cyklická podgrupa řádu k v $\mathbf{G}$. Podle Tvrzení 4.3 má $\varphi(k)$ generátorů, a tedy $u_k = \varphi(k)$.

Čili pro každé $d \mid n$ platí $u_d = 0$ nebo $u_d = \varphi(d)$. Přitom podle Tvrzení 4.5 je $\sum_{d|n} \varphi(d) = n = \sum_{d|n} u_d$, takže $u_d = \varphi(d)$ pro všechna $d \mid n$. Speciálně v $\mathbf{G}$ existuje prvek řádu n, neboli generátor. □

Důkaz Věty 4.6. 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. □

DISKRÉTNÍ LOGARITMUS A KRYPTO-APLIKACE VIZ STARÁ SKRIPTA

5. Grupy symetrií

5.1. **Symetrie geometrických objektů.**

Jednou z původních motivací pro rozvoj teorie grup bylo studium symetrií geometrických objektů. Pro jednoduchost se soustředíme na eukleidovskou geometrii, ačkoliv podobné úvahy lze provádět i v jiných geometriích.

Z kurzu lineární algebry si připomeňme větu, která říká, že izometrie na eukleidovském prostoru $\mathbb{R}^n$ jsou právě ortogonální afinní zobrazení, tj. zobrazení

$$\mathbb{R}^n \to \mathbb{R}^n, \quad x \mapsto Ax + b,$$

kde A je ortogonální matice a $b \in \mathbb{R}^n$. Izometrie roviny jsou rotace (otočení) se středem v počátku složené s posunutím a reflexe (osové symetrie) podle osy procházející počátkem složené z posunutím. Izometrie třidimenzionálního prostoru jsou

rotace kolem osy procházející počátkem složené z posunutím a dále tato zobrazení složená s reflexí podle roviny procházející počátkem.

Je-li dána podmnožina X eukleidovského prostoru $\mathbb{R}^n$, uvažujme prvky eukleidovské grupy $\mathbf{E}_n$ zachovávající tuto množinu, tj.

$$\mathrm{Sym}(X) = \{\varphi \in E_n : \varphi(X) = X\}.$$

Je snadné ověřit, že $\mathrm{Sym}(X)$ tvoří podgrupu v $\mathbf{E}_n$. Podgrupa $\mathbf{Sym}(X)$ se nazývá *grupa symetrií objektu* X.

Příklad. Uvažujme n-dimenzionální kouli $X = \{(x_1, \ldots, x_n) : \sum x_i \leq 1\} \subset \mathbb{R}^n$. Grupa $\mathbf{Sym}(X) = \mathbf{Sym}(\{0\})$ sestává z izometrií, které zachovávají nulu, tj. ze zobrazení $x \mapsto Ax$, kde A je ortogonální matice. Vidíme, že $\mathbf{Sym}(X) \simeq \mathbf{O}_n(\mathbb{R})$.

Příklad. Uvažujme pravidelný n-úhelník $X \subset \mathbb{R}^2$ se středem v nule. Grupa $\mathbf{Sym}(X)$ sestává z rotací se středem v nule o úhly $k \cdot 2\pi/n$, $k = 0, \ldots, n-1$, a z reflexí, jejichž osy procházejí

- pro liché n, vrcholem a středem protilehlé strany,
- pro sudé n, protilehlými vrcholy a protilehlými středy stran.

Vidíme, že $\mathbf{Sym}(X) \simeq \mathbf{D}_{2n}$, kde dané izometrii odpovídá příslušná permutace na očíslovaných vrcholech.

Již Leonardo da Vinci si všiml, že pokud má rovinný objekt konečně mnoho symetrií, tyto tvoří buď cyklickou nebo dihedrální grupu. Dokažte si jako cvičení, že je-li $\mathbf{G}$ konečná podgrupa eukleidovské grupy $\mathbf{E}_2$, pak $\mathbf{G} \simeq \mathbb{Z}_n$ nebo $\mathbf{G} \simeq \mathbf{D}_{2n}$ pro nějaké n. [Návod: translace mají nekonečný řád; složením $ghg^{-1}h^{-1}$ lze z rotací v různých bodech dostat translaci; podobně pro rotaci a reflexi podle osy neprocházející jejím středem; čili $\mathbf{G}$ je izomorfní podgrupě $\mathbf{O}_2(\mathbb{R})$; nyní si stačí rozmyslet, jaký řád má daná rotace a jaká rotace vznikne složením dvou reflexí.]

Z druhého příkladu si lze vzít obecné ponaučení: jsou-li izometrie zachovávající daný objekt X určeny hodnotami v n bodech, lze se na grupu $\mathbf{Sym}(X)$ dívat jako na podgrupu grupy $\mathbf{S}_n$. Tento duální pohled budeme používat často, nejen pro dihedrální grupy.

Příklad. Uvažujme krychli $X \subset \mathbb{R}^3$ se středem v nule. Zřejmě $\mathbf{Sym}(X) \leq \mathbf{Sym}(\{0\})$. Jak vypadají rotace, které zachovávají krychli?

Nejprve ukážeme, že existuje nejvýše 24 rotací zachovávajících danou krychli. Zvolme vrchol. Ten lze otočit na libovolný z osmi vrcholů krychle. Jeho tři sousedi se ovšem musí zobrazit na sousedy obrazu, a to ve stejném pořadí, čili jsou nejvýše tři možnosti, jak to udělat. Obrazy protilehlých vrcholů jsou těmito čtyřmi jednoznačně určeny, nemůže tedy být více než $8 \cdot 3 = 24$ rotací.

Je snadné nahlédnout, že následujících 24 rotací krychli zachovává:

- identita,
- rotace s osou přes středy protilehlých stěn o úhly 90, 180 a 270 stupňů,
- rotace s osou přes středy protilehlých hran o úhel 180 stupňů,
- rotace s osou přes protilehlé vrcholy o úhly 120 a 240 stupňů.

Čili podgrupa rotací $\mathbf{R} \leq \mathbf{Sym}(X)$ má 24 prvků. Všimněte si, že různé rotace permutují různým způsobem tělesové úhlopříčky, čili grupa $\mathbf{R}$ je izomorfní nějaké podgrupě grupy $\mathbf{S}_4$ (rotaci přiřaďte permutaci na očíslovaných úhlopříčkách). Protože mají obě grupy 24 prvků, nutně musí platit $\mathbf{R} \simeq \mathbf{S}_4$.

Zvolme pevně jednu reflexi $\sigma_0 \in \mathrm{Sym}(X)$. Pro každou další reflexi $\sigma \in \mathrm{Sym}(X)$ platí $\sigma \circ \sigma_0^{-1} \in R$, protože složením reflexí (determinant příslušné matice je -1) dostaneme rotaci (determinant 1), čili podle Tvrzení 2.10 patří σ do rozkladové třídy $\sigma_0 R$. Dokázali jsme, že všechny reflexe tvoří jednu rozkladovou třídu, čili $[\mathbf{Sym}(X) : \mathbf{R}] = 2$, a tedy $\mathbf{Sym}(X)$ má 48 prvků. V pokročilejším kurzu teorie grup se dozvíte, jak tuto grupu reprezentovat pomocí konstrukce zvané semidirektní součin.

5.2. **Působení grupy na množině a Burnsideova věta.**

Často se hodí interpretovat danou grupu jako grupu permutací na jisté 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.

Působením grupy $\mathbf{G}$ *na množině* X rozumíme libovolný homomorfismus $\pi : G \to S_X$. Hodnotu permutace $\pi(g)$ na prvku $x \in X$ budeme značit krátce $g(x)$. Z definice homomorfismu 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 jak se prvky v $\mathbf{G}$ násobí, tak se příslušné „pohyby“ skládají.

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

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

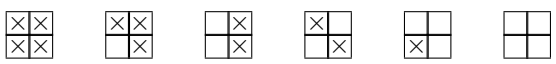
$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} \cos(k \cdot 2\pi/n) & -\sin(k \cdot 2\pi/n) \\ \sin(k \cdot 2\pi/n) & \cos(k \cdot 2\pi/n) \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}.$$

Příklad. Maticové grupy lze interpretovat 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.

Jako motivaci, proč uvažovat abstraktní koncept působení grupy na množině, si ukážeme jednu pěknou aplikaci v kombinatorice. Jak spočítat jistý typ objektů až na dané symetrie? 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? Pro jednoduchost budeme metodu ilustrovat v dvojrozměrném případě.

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

Tuto úlohu je 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 (čili $|X| = 2^4 = 16$), kde $\pi(g)$ je permutace, která otočí tabulku o příslušný úhel i s daným obarvením.

Nyní zpět k teorii. V celém zbytku sekce budeme uvažovat libovolné působení grupy $\mathbf{G}$ 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 prvek x na prvek y.

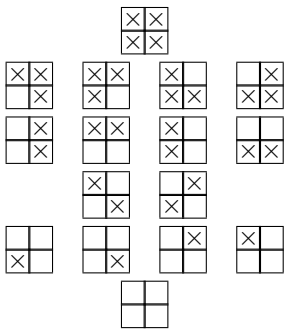
Lemma 5.1. *Relace $\sim$ je ekvivalence na množině X.*

Důkaz. Reflexivita: jednotka působí jako identita, tj. $1(x) = id(x) = x$. Symetrie: inverz prvku působí jako inverzní permutace, tj. $g(x) = y$ implikuje $g^{-1}(y) = x$. Tranzitivita: násobení odpovídá skládání permutací, čili pokud $x \sim y \sim z$, tj. $g(x) = y$ a $h(y) = z$ pro nějaká $g, h \in G$, 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 $\sim$ právě ty dvojice obravení, kde lze jedno z druhého dostat otočením. Množina všech obarvení se tedy rozpadne na šest orbit následujícím způsobem:



Řešením motivační 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.

Lemma 5.2. *Stabilizátor $\mathbf{G}_x$ tvoří podgrupu grupy $\mathbf{G}$.*

Důkaz. Jednotka náleží G_x, neboť $1(x) = id(x) = x$. Pokud $g(x) = x$, pak také $g^{-1}(x) = x$. A pokud $g, h \in G_x$, tj. platí $g(x) = h(x) = x$, pak $(gh)(x) = g(h(x)) = g(x) = x$, čili $gh \in G_x$. □

Zásadní význam má následující pozorování, které dává do souvislosti velikost stabilizátoru a velikost orbity.

Tvrzení 5.3. *Nechť grupa* $\mathbf{G}$ *působí na množině* X*. Pak pro každé* $x \in X$ *platí*

$$\big|[x]\big| = [\mathbf{G} : \mathbf{G}_x].$$

Důkaz. Index $[\mathbf{G} : \mathbf{G}_x]$ značí počet rozkladových tříd podgrupy $\mathbf{G}_x$, stačí tedy najít bijekci mezi prvky orbity a množinou rozkladových tříd. 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 dobře definovali zobrazení: mohlo by se stát, že tutéž rozkladovou třídu máme označenu dvěma různými způsoby, tj. že $gG_x = hG_x$, a přitom se jí snažíme přiřadit různé hodnoty $g(x) \neq h(x)$. Ovšem podle Tvrzení 2.10 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. □

Je-li grupa $\mathbf{G}$ konečná, kombinací Tvrzení 5.3 a Lagrangeovy věty dostáváme vztah

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

Speciálně, velikost každé orbity dělí řád grupy $\mathbf{G}$ (všimněte si, že to je splněno v naší motivační úloze).

Označme $X/\!\sim$ množinu všech bloků ekvivalence $\sim$ na množině X. V našem kontextu bude $|X/\!\sim|$ značit počet orbit daného působení.

Věta 5.4 (Burnsideova věta)**.** *Nechť konečná grupa* $\mathbf{G}$ *působí na konečnou množinu* X*. Pak*

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

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

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:

$$\frac{1}{|G|}\cdot\sum_{g\in G}|X_g| \;=\; \frac{1}{|G|}\cdot\sum_{x\in X}|G_x| \overset{5.3}{=} \frac{1}{|G|}\cdot\sum_{x\in X}\frac{|G|}{\big|[x]\big|} \;=\; \sum_{x\in X}\frac{1}{\big|[x]\big|} \;=$$

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

Výsledek je tedy roven velikosti množiny $X/\sim$. □

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 $\mathbb{Z}_4$ interpretovaná jako otočení čtverce, (b) grupa $\mathbf{D}_8$ všech symetrií čtverce. 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 (rozumí se, že prvky „podobného typu“ mají stejně velké množiny pevných bodů), 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) $\frac{1}{8}\cdot(1680+2\cdot 0+1\cdot 0+2\cdot 36+2\cdot 36) = 228$.

□

DALŠÍ ŘEŠENÉ ÚLOHY VIZ STARÁ SKRIPTA

5.3. **Cauchyova věta.**

Tvrzení 5.3 lze použít k důkazu spousty užitečných tvrzení o konečných grupách. Jedno takové si nyní ukážeme.

Lagrangeova věta říká, že řád každého prvku dělí řád celé grupy. Naopak, pokud k dělí $|G|$, prvek řádu k v grupě $\mathbf{G}$ existovat nemusí. Leda by k bylo prvočíslo, pak musí, jak ukazuje následující věta, kterou má řadu důsledků v teorii konečných grup a i my ji budeme potřebovat v kapitole o Galoisově teorii k důkazu, že jisté polynomy stupně 5 nemají vzorec na vyjádření kořenů.

Věta 5.5 (Cauchyova věta)**.** *Buď* $\mathbf{G}$ *konečná grupa a* p *prvočíslo, které dělí* $|G|$*. Pak v* $\mathbf{G}$ *existuje prvek řádu* p*.*

Důkaz. Označme

$$X = \{(a_1, \ldots, a_p) \in G^p : \ a_1 \cdot \ldots \cdot a_p = 1\}.$$

Prvních $p-1$ prvků v každé p-tici můžeme zvolit libovolně a poslední je jimi jednoznačně určen, čili $|X| = |G|^{p-1}$ a vidíme, že $p \mid |X|$. Grupa $\mathbb{Z}_p$ působí na X rotací složek. Podle Tvrzení 5.3 velikost každé orbity dělí řád působící grupy, čili možné velikosti orbit jsou pouze 1 a p. Přitom aspoň jedna orbita velikosti 1 existuje, konkrétně $\{(1, \ldots, 1)\}$. Protože je velikost $|X|$ dělitelná p, musí existovat ještě aspoň $p-1$ jednoprvkových orbit. Přitom v jednoprvkové orbitě může být pouze konstantní p-tice, nějaká $(a, \ldots, a)$, která splňuje $a^p = a \cdot \ldots \cdot a = 1$, čímž jsme objevili hledaný prvek řádu p. □

6. Faktorgrupy a řešitelnost

6.1. **Normální podgrupy.**

Tvrzení 6.1. *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Následující tvrzení jsou ekvivalentní:*

(1) $aH = Ha$ *pro každé* $a \in G$*.*
(2) $aha^{-1} \in H$ *pro každé* $h \in H$ *a každé* $a \in G$*;*

Důkaz. (1) $\Rightarrow$ (2). Buď $h \in H$ a $a \in G$. Pak $ah \in aH = Ha$, a tedy existuje $k \in H$ takové, že $ah = ka$. Dostáváme $aha^{-1} = k \in H$.

(2) $\Rightarrow$ (1). Dokážeme obě inkluze v rovnosti $aH = Ha$. Nejprve uvažujme $ah \in aH$. Pak $k = aha^{-1} \in H$, a tedy $ah = ka \in Ha$. Nyní uvažujme $ha \in Ha$. Pak $l = a^{-1}ha \in H$, tedy $ha = al \in aH$. □

Podgrupy splňující vlastnosti z Tvrzení 6.1 se nazývají *normální podgrupy*, značíme $\mathbf{H} \trianglelefteq \mathbf{G}$.

Operace z podmínky (2) se nazývá *konjugace*. Formálně, buď $\mathbf{G}$ grupa a $a, b \in G$. Prvky a, b nazýváme *konjugované* v $\mathbf{G}$, pokud existuje $c \in G$ takové, že $a = cbc^{-1}$. Je vidět, že relace konjugace je ekvivalencí. Její bloky se nazývají *třídy konjugace*.

Příklad. Dvě permutace jsou konjugované v grupě $\mathbf{S}_n$ právě tehdy, když mají stejnou strukturu cyklů, viz Tvrzení 1.4.

Příklad. V lineární algebře se konjugovaným maticím se říká *podobné*. Konjugace odpovídá změně báze lineárního zobrazení, tj. dvě matice jsou konjugované v grupě $\mathbf{GL}_n(\mathbf{T})$ právě tehdy, když jsou maticí téhož lineárního zobrazení vzhledem k různým bázím.

V abelovských grupách je každá podgrupa normální, obě ekvivalentní podmínky jsou triviálně splněny. Z triviálních důvodů platí $\{1\} \trianglelefteq \mathbf{G}$ a $\mathbf{G} \trianglelefteq \mathbf{G}$. Vlastní podgrupy být normální mohou i nemusí.

Příklad.

- Podgrupa $\mathbf{SL}_n(\mathbf{T})$ matic s determinantem 1 je normální v grupě $\mathbf{GL}_n(\mathbf{T})$, jak plyne z podmínky (2) užitím součinového vzorce pro determinanty: $\det(AHA^{-1}) = (\det A)(\det H)(\det A)^{-1} = \det H$.
- Podgrupa $\mathbf{A}_n$ sudých permutací je normální v grupě $\mathbf{S}_n$, jak plyne ze součinového vzorce pro znaménko: $\operatorname{sgn}(aha^{-1}) = (\operatorname{sgn} a)(\operatorname{sgn} h)(\operatorname{sgn} a)^{-1} = \operatorname{sgn} h$.
- Podgrupa $\mathbf{D}_{2n}$ není normální v grupě $\mathbf{S}_n$, což je ihned vidět z Tvrzení 1.4.

Příklad. Jediné normální podgrupy v $\mathbf{S}_n$, $n \neq 4$, jsou $\{1\}$, $\mathbf{A}_n$, $\mathbf{S}_n$. Grupa $\mathbf{S}_4$ navíc obsahuje čtyřprvkovou normální podgrupu

$$\{id, (12)(34), (13)(24), (14)(23)\}.$$

Není těžké nahlédnout, že to je podgrupa, a z Tvrzení 1.4 plyne její normalita.

6.2. **Faktorgrupy.**
KONSTRUKCE A PŘÍUKLADY VIZ STARÁ SKRIPTA

Věta 6.2 (1. o izomorfismu)**.** *Buď $\varphi : \mathbf{G} \to \mathbf{H}$ homomorfismus grup.*

(1) *Je-li $\mathbf{N} \leq \mathbf{Ker}(\varphi)$ normální podgrupa grupy $\mathbf{G}$, pak je zobrazení*

$$\psi : \mathbf{G}/\mathbf{N} \to \mathbf{H}, \qquad [a] \mapsto \varphi(a)$$

dobře definované a je to grupový homomorfismus.

(2) $\mathbf{G}/\mathbf{Ker}(\varphi) \simeq \mathbf{Im}(\varphi)$.

Důkaz. (1) Předně je třeba ověřit, že je zobrazení ψ dobře definované: mohlo by se stát, že máme tentýž blok označen dvěma různými způsoby, tj. že $[a] = [b]$ pro nějaká $a \neq b$, a přitom se těmto blokům snažíme přiřadit dvě různé hodnoty $\varphi(a) \neq \varphi(b)$. Ovšem

$$[a] = [b] \;\Leftrightarrow\; a \cdot b^{-1} \in N \;\Rightarrow\; a \cdot b^{-1} \in \operatorname{Ker}(\varphi) \;\Leftrightarrow\; \varphi(a \cdot b^{-1}) = 1 \;\Leftrightarrow\; \varphi(a) = \varphi(b),$$

tedy ψ je dobře definované zobrazení, a protože $\psi([a \cdot b]) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = = \psi([a]) \cdot \psi([b])$, je to homomorfismus.

(2) Použijeme (1) pro $\mathbf{N} = \mathbf{Ker}(\varphi)$. Výsledný homomorfismus je prostý, neboť

$$[a] = [b] \;\Leftrightarrow\; a \cdot b^{-1} \in \operatorname{Ker}(\varphi) \;\Leftrightarrow\; \varphi(a \cdot b^{-1}) = 1 \;\Leftrightarrow\; \varphi(a) = \varphi(b),$$

a uvažujeme-li jej jako zobrazení $\mathbf{G}/\mathbf{Ker}(\varphi) \to \mathbf{Im}(\psi) = \mathbf{Im}(\varphi)$, pak je také na. □

Tvrzení 6.3 (2. věta o izomorfismu)**.** *Buď $\mathbf{G}$ grupa a $\mathbf{N}$ její normální podgrupa.*

(1) *Je-li $\mathbf{N} \leq \mathbf{H} \trianglelefteq \mathbf{G}$, pak $\mathbf{H}/\mathbf{N}$ je normální podgrupa v $\mathbf{G}/\mathbf{N}$.*

(2) *Je-li $\mathbf{K} \trianglelefteq \mathbf{G}/\mathbf{N}$, pak existuje normální podgrupa $\mathbf{H} \trianglelefteq \mathbf{G}$ taková, že $\mathbf{K} = \mathbf{H}/\mathbf{N}$.*

(3) *Pro $\mathbf{N} \leq \mathbf{H} \trianglelefteq \mathbf{G}$ platí*

$$(\mathbf{G}/\mathbf{N})/(\mathbf{H}/\mathbf{N}) \simeq \mathbf{G}/\mathbf{H}.$$

Důkaz. (1) Buď $[a], [b]$ prvky $\mathbf{H}/\mathbf{N}$, čili $a, b \in H$, a buď $[g]$ prvek $\mathbf{G}/\mathbf{N}$. Pak $[a][b] = [ab]$ je prvek $\mathbf{H}/\mathbf{N}$, protože $ab \in H$, a ze stejného důvodu jsou i $[1]$, $[a]^{-1} = [a^{-1}]$ i $[g][a][g]^{-1} = [gag^{-1}]$ prvky $\mathbf{H}/\mathbf{N}$.

(2) Buď $H = \{a \in G : \ [a] \in K\}$. Pro $a, b \in H$ a $g \in G$ platí $ab \in H$, protože $[ab] = [a][b] \in K$, a ze stejného jsou prvky H také 1, a^{-1} a gag^{-1}. Zjevně $\mathbf{K} = \mathbf{H}/\mathbf{N}$.

(3) Uvažujme homomorfismus $\varphi : \mathbf{G}/\mathbf{N} \to \mathbf{G}/\mathbf{H}$, $[a]_{\mathbf{N}} \mapsto [a]_{\mathbf{H}}$. Je dobře deifnovaný, protože $\mathbf{N} \leq \mathbf{H}$, a tedy $[a]_{\mathbf{N}} = [b]_{\mathbf{N}}$ implikuje $[b]_{\mathbf{H}} = [b]_{\mathbf{H}}$. Je to homomorfismus, $\varphi([a]_{\mathbf{N}}[b]_{\mathbf{N}}) = \varphi([ab]_{\mathbf{N}}) = [ab]_{\mathbf{H}} = [a]_{\mathbf{H}}[b]_{\mathbf{H}} = \varphi([a]_{\mathbf{N}})\varphi([b]_{\mathbf{N}})$. Jeho obraz je celé $\mathbf{G}/\mathbf{H}$ a jeho jádro sestává z těch $[a]_{\mathbf{N}}$, pro které je $a \in H$, tedy $\mathbf{Ker}(\varphi) = \mathbf{H}/\mathbf{N}$. Aplikací 1. věta o izomorfismu dostaneme uvedený vztah. □

Tvrzení 6.4 (3. věta o izomorfismu)**.** *Buď* $\mathbf{G}$ *grupa,* $\mathbf{N}$ *její normální podgrupa a* $\mathbf{H}$ *její libovolná podgrupa. Pak* HN *tvoří podgrupu grupy* $\mathbf{G}$*,* $H \cap N$ *tvoří normální podgrupu grupy* $\mathbf{H}$ *a*

$$\mathbf{HN}/\mathbf{N} \simeq \mathbf{H}/(\mathbf{H} \cap \mathbf{N}).$$

Důkaz je snadným cvičením v podobném stylu, jako jsme dokazovali 2. větu o izomorfismu.

6.3. Řešitelné grupy.

Pojem řešitelnosti vychází z Galoisovy věty, která říká, že polynom f lze řešit v radikálech, tj. jeho kořeny lze vyjádřit pomocí jeho koeficientů pomocí sčítání, odčítání, násobení, dělení a odmocnin, právě tehdy, když je tzv. Galoisova grupa tohoto polynomu řešitelná.

Definice. Grupa $\mathbf{G}$ se nazývá *řešitelná*, pokud existuje číslo k a normální podgrupy $\mathbf{N}_0, \ldots, \mathbf{N}_k \trianglelefteq \mathbf{G}$ takové, že $\{1\} = \mathbf{N}_0 \leq \mathbf{N}_1 \leq \ldots \leq \mathbf{N}_k = \mathbf{G}$ a každá faktorgrupa $\mathbf{N}_i/\mathbf{N}_{i-1}$, $i = 1, \ldots, k$, je abelovská. Nejmenšímu k, pro které taková řada podgrup existuje, se říká *stupeň řešitelnosti* grupy $\mathbf{G}$.

Vidíme, že grupa je řešitelná stupně 1 právě tehdy, když je abelovská. Řešitelné grupy stupně ≤ 2 se nazývají *metabelovské*.

Příklady.

- Grupa $\mathbf{S}_3$ je metabelovská, jak prokazuje řada podgrup
$$\{1\} \leq \mathbf{A}_3 \leq \mathbf{S}_3.$$
Obě faktorgrupy $\mathbf{A}_3/\{1\} \simeq \mathbf{A}_3 \simeq \mathbb{Z}_3$ a $\mathbf{S}_3/\mathbf{A}_3 \simeq \mathbb{Z}_2$ jsou abelovské.
- Obecněji, dihedrální grupy $\mathbf{D}_{2n}$ jsou metabelovské, jak prokazuje řada podgrup
$$\{1\} \leq \mathbf{R} \leq \mathbf{D}_{2n},$$
kde $\mathbf{R}$ sestává ze všech otočení. Obě faktorgrupy $\mathbf{R}/\{1\} \simeq \mathbf{R} \simeq \mathbb{Z}_n$ a $\mathbf{D}_{2n}/\mathbf{R} \simeq \mathbb{Z}_2$ jsou abelovské.
- Grupa $\mathbf{S}_4$ je řešitelná stupně 3, jak prokazuje řada podgrup
$$\{1\} \leq \mathbf{K} \leq \mathbf{A}_4 \leq \mathbf{S}_4,$$
kde $\mathbf{K}$ je Kleinova podgrupa. Je snadné ověřit, že všechny faktorgrupy $\mathbf{K}/\{1\} \simeq \mathbf{K} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbf{A}_4/\mathbf{K} \simeq \mathbb{Z}_3$ a $\mathbf{S}_4/\mathbf{A}_4 \simeq \mathbb{Z}_2$ jsou abelovské.

Příklad. Grupy $\mathbf{S}_n$, $n \geq 5$, nejsou řešitelné. Stačí dokázat, že $\mathbf{S}_n$ má jedinou vlastní normální podgrupu $\mathbf{A}_n$, tedy že jediná možná řada je $\{1\} \leq \mathbf{A}_n \leq \mathbf{S}_n$, avšak podgrupa $\mathbf{A}_n$ není abelovská.

Důkaz provedeme pro $n = 5$ rozborem případů podle typu permutací. Podobně lze provést důkaz i pro obecné n, ale diskuse je komplikovanější. Uvažujme normální podgrupu $\{1\} \neq \mathbf{N} \trianglelefteq \mathbf{S}_5$.

(1) Pokud $\mathbf{N}$ obsahuje transpozici, pak obsahuje všechny transpozice, protože $\mathbf{N}$ je uzavřená na konjugaci, a tedy $\mathbf{N} = \mathbf{S}_5$, neboť transpozice generují celou grupu $\mathbf{S}_5$.
(2) Pokud $\mathbf{N}$ obsahuje trojcyklus, pak obsahuje všechny trojcykly, a tedy $\mathbf{A}_5 \leq \mathbf{N}$, neboť trojcykly generují celou grupu $\mathbf{A}_5$. Z Lagrangeovy věty plyne, že $\mathbf{N} = \mathbf{A}_5$ nebo $\mathbf{N} = \mathbf{S}_5$.
(3) Pokud $\mathbf{N}$ obsahuje permutaci složenou ze dvou disjunktních transpozic, pak obsahuje všechny takové a složení $(1\ 2)(3\ 4) \circ (1\ 2)(3\ 5) = (3\ 5\ 4)$ převádí problém na bod (2).
(4) Pokud $\mathbf{N}$ obsahuje permutaci složenou z trojcyklu a dvojcyklu, pak obsahuje všechny takové a složení $((1\ 2\ 3)(4\ 5))^2 = (1\ 3\ 2)$ převádí problém na bod (2).
(5) Pokud $\mathbf{N}$ obsahuje čtyřcyklus, pak obsahuje všechny takové a složení $(1\ 2\ 3\ 4) \circ (1\ 2\ 4\ 3) = (1\ 3\ 2)$ převádí problém na bod (2).
(6) Pokud $\mathbf{N}$ obsahuje pěticyklus, pak obsahuje všechny takové a složení $(1\ 2\ 3\ 4\ 5) \circ (1\ 2\ 3\ 4\ 5) = (1\ 3)(2\ 4)$ převádí problém na bod (3).

S abelovskostí faktorgrupy úzce souvisí následující pojem: pro danou grupu $\mathbf{G}$ definujeme *derivovanou podgrupu*

$$\mathbf{G}' = \langle aba^{-1}b^{-1} : a, b \in G.$$

Lemma 6.5. *Buď $\mathbf{G}$ grupa a $\mathbf{N}$ její normální podgrupa.*

(1) *$\mathbf{N}'$ je normální podgrupa v $\mathbf{G}$.*
(2) *$\mathbf{G}/\mathbf{N}$ je abelovská právě tehdy, když $\mathbf{G}' \leq \mathbf{N}$.*

Důkaz. (1) Generátory grupy $\mathbf{N}'$ jsou uzavřeny na konjugaci: pro $a, b \in N$ a $g \in G$ platí

$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}),$$

přičemž všechny čtyři prvky v závorkách jsou v $\mathbf{N}$, protože je tato podgrupa normální. Z Tvrzení **??** pak stejným argumentem plyne, že pokud je množina generátorů X uzavřena na konjugaci, podgrupa jimi generovaná je normální: pro prvek $a_1^{k_1} \dots a_n^{k_n}$, kde $a_i \in X$, platí

$$g(a_1^{k_1} \dots a_n^{k_n})g^{-1} = (ga_1g^{-1})^{k_1} \dots (ga_ng^{-1})^{k_n},$$

přičemž všechny prvky v závorkách jsou v X.

(2) Faktorgrupa $\mathbf{G}/\mathbf{N}$ je abelovská právě tehdy, když pro všechna $a, b \in G$ platí $[a][b] = [b][a]$, neboli $[1] = [a][b][a]^{-1}[b]^{-1} = [aba^{-1}b^{-1}]$, tj. $aba^{-1}b^{-1} \in N$. Nejmenší taková podgrupa je z definice $\mathbf{G}'$, všechny ostatní $\mathbf{N}$ ji musí obsahovat. □

Stěžejní vlastností řešitelných grup je následující charakterizace, která dává do souvislosti řešitelnost dané grupy a jejích podgrup a faktorgrup. Tvrzení se několikrát využije v důkazu Galoisovy věty.

Tvrzení 6.6. *Buď $\mathbf{G}$ grupa.*

(1) *Je-li $\mathbf{G}$ řešitelná a $\mathbf{H}$ její pogrupa, pak je $\mathbf{H}$ řešitelná.*
(2) *Je-li $\mathbf{G}$ řešitelná a $\mathbf{K}$ její normální podgrupa, pak je $\mathbf{G}/\mathbf{K}$ řešitelná.*
(3) *Pokud $\mathbf{G}$ obsahuje normální podgrupu $\mathbf{N}$ takovou, že jsou obě grupy $\mathbf{N}$ i $\mathbf{G}/\mathbf{N}$ řešitelné, pak je $\mathbf{G}$ řešitelná.*

Důkaz. (1) Uvažujme řadu normálních podgrup $\{1\} = \mathbf{N}_0 \leq \mathbf{N}_1 \leq \ldots \leq \mathbf{N}_k = \mathbf{G}$, kde je každá faktorgrupa $\mathbf{N}_i/\mathbf{N}_{i-1}$ abelovská. Dokážeme, že

$$\{1\} = \mathbf{N}_0 \cap \mathbf{H} \leq \mathbf{N}_1 \cap \mathbf{H} \leq \ldots \leq \mathbf{N}_k \cap \mathbf{H} = \mathbf{H}$$

je řada prokazující řešitelnost grupy $\mathbf{H}$. Pomocí 3. věty o izomorfismu upravíme

$$\begin{aligned}(\mathbf{N}_i \cap \mathbf{H})\big/(\mathbf{N}_{i-1} \cap \mathbf{H}) &= (\mathbf{N}_i \cap \mathbf{H})\big/((\mathbf{N}_i \cap \mathbf{H}) \cap \mathbf{N}_{i-1}) \\ &\simeq (\mathbf{N}_{i-1}(\mathbf{N}_i \cap \mathbf{H}))\big/\mathbf{N}_{i-1} \leq \mathbf{N}_i/\mathbf{N}_{i-1},\end{aligned}$$

což je abelovská grupa a její podgrupa je nutně také abelovská.

(2) Vyjdeme ze stejné řady a dokážeme, že

$$\mathbf{K}/\mathbf{K} = \mathbf{N}_0\mathbf{K}/\mathbf{K} \leq \mathbf{N}_1\mathbf{K}/\mathbf{K} \leq \ldots \leq \mathbf{N}_k\mathbf{K}/\mathbf{K} = \mathbf{G}/\mathbf{K}$$

je řada prokazující řešitelnost grupy $\mathbf{G}/\mathbf{K}$. Použijeme postupně 2., 3. a 2. větu o izomorfismu a dostaneme

$$\begin{aligned}(\mathbf{N}_i\mathbf{K}/\mathbf{N})\big/(\mathbf{N}_{i-1}\mathbf{K}/\mathbf{K}) &\simeq \mathbf{N}_i\mathbf{K}\big/\mathbf{N}_{i-1}\mathbf{K} = \mathbf{N}_i(\mathbf{N}_{i-1}\mathbf{K})\big/\mathbf{N}_{i-1}\mathbf{K} \\ &\simeq \mathbf{N}_i\big/(\mathbf{N}_{i-1}\mathbf{K}) \cap \mathbf{N}_i \simeq (\mathbf{N}_i/\mathbf{N}_{i-1})\big/\left((\mathbf{N}_{i-1}\mathbf{K}) \cap \mathbf{N}_i/\mathbf{N}_{i-1}\right).\end{aligned}$$

Poslední krok dává smysl, protože $\mathbf{N}_{i-1} \leq (\mathbf{N}_{i-1}\mathbf{K}) \cap \mathbf{N}_i$. Vidíme, že původní faktorgrupa je faktorgrupou abelovské grupy $\mathbf{N}_i/\mathbf{N}_{i-1}$, čili je abelovská.

(3) Uvažujme řadu $\mathbf{N}/\mathbf{N} = \mathbf{L}_0/\mathbf{N} \leq \mathbf{L}_1/\mathbf{N} \leq \ldots \leq \mathbf{L}_l/\mathbf{N} = \mathbf{G}/\mathbf{N}$, kde je každá faktorgrupa $(\mathbf{L}_i/\mathbf{N})\big/(\mathbf{L}_{i-1}/\mathbf{N}) \simeq \mathbf{L}_i/\mathbf{L}_{i-1}$ abelovská (takový zápis podgrup je možný díky 2. větě o izomorfismu, bod (2)). Tvrzení dokážeme indukcí podle stupně řešitelnosti grupy $\mathbf{N}$.

Je-li $\mathbf{N}$ řešitelná stupně 1, tedy abelovská, pak

$$\{1\} \leq \mathbf{N} = \mathbf{L}_0 \leq \mathbf{L}_1 \leq \ldots \leq \mathbf{L}_l = \mathbf{G},$$

je řada prokazující řešitelnost grupy $\mathbf{G}$.

Nyní předpokládejme, že tvrzení platí, kdykoliv je $\mathbf{N}$ řešitelná stupně $< k$, a uvažujme situaci, kdy je stupeň řešitelnosti roven k. Uvažujme řadu $\{1\} = \mathbf{K}_0 \leq \mathbf{K}_1 \leq \ldots \leq \mathbf{K}_k = \mathbf{N}$, kde je každá faktorgrupa $\mathbf{K}_i/\mathbf{K}_{i-1}$ abelovská. Vidíme, že předposlední člen řady, grupa $\mathbf{K} = \mathbf{K}_{k-1}$, je řešitelná stupně $< k$ a $\mathbf{N}/\mathbf{K}$ je abelovská. Z Lemmatu 6.5 plyne, že $\mathbf{N}' \leq \mathbf{K}$ a že $\mathbf{N}'$ je normální v $\mathbf{G}$. Podobně jako v bodu (1) vidíme, že grupa $\mathbf{N}'$ je řešitelná stupně $< k$, jak prokazuje řada

$$\{1\} = \mathbf{K}_0 \cap \mathbf{N}' \leq \mathbf{K}_1 \cap \mathbf{N}' \leq \ldots \leq \mathbf{K}_{k-1} \cap \mathbf{N}' = \mathbf{N}'.$$

Také $\mathbf{G}/\mathbf{N}'$ je řešitelná grupa, což prokazuje řada

$$\mathbf{N}'/\mathbf{N}' \leq \mathbf{N}/\mathbf{N}' = \mathbf{L}_0/\mathbf{N}' \leq \mathbf{L}_1/\mathbf{N}' \leq \ldots \leq \mathbf{L}_l/\mathbf{N}' = \mathbf{G}/\mathbf{N}'.$$

Z indukčního předpokladu plyne, že $\mathbf{G}$ je řešitelná. □

Důsledek 6.7. *Buď $\mathbf{G}$ grupa a $\mathbf{N}_0, \ldots, \mathbf{N}_k \trianglelefteq \mathbf{G}$ takové, že $\{1\} = \mathbf{N}_0 \leq \mathbf{N}_1 \leq \ldots \leq \mathbf{N}_k = \mathbf{G}$ a každá faktorgrupa $\mathbf{N}_i/\mathbf{N}_{i-1}$, $i = 1, \ldots, k$, je řešitelná. Pak je $\mathbf{G}$ řešitelná.*

Důkaz. Snadno indukcí podle k: $\mathbf{N}_1 \simeq \mathbf{N}_1/\mathbf{N}_0$ je řešitelná z předpokladu a je-li řešitelná $\mathbf{N}_{i-1}$, pak je $\mathbf{N}_i$ řešitelná také díky Tvrzení 6.6(3). □