12 Normální faktorizační safari

Řešení
verze ze dne 4. května 2025.

Cíle cvičení: Vydáme se na dobrodružnou faktorizační výpravu, přičemž hlavním cílem naší expedice budou faktorgrupy. Nejprve ovšem důkladně rozvážíme, jak poznat takzvané normální podgrupy, bez jejichž pomoci se neobejdeme, neboť jako jediné disponují platným povolením k lovu faktorgrup.

Úlohy, které bychom určitě měli umět řešit:

Úloha 12.1. Nechť $M = \{\mathrm{id}, (1\,2)(3\,4)\}$ a $\mathbf{K} = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ jsou podmnožiny grupy $\mathbf{S}_4$. Dokažte, že

(a) M není normální podgrupa grupy $\mathbf{A}_4$ ani $\mathbf{S}_4$,

(b) $\mathbf{K}$ je normální podgrupa grupy $\mathbf{S}_4$ a M je normální podgrupa grupy $\mathbf{K}$,

(c) $\mathbf{K}$ je jediná vlastní normální podgrupa grupy $\mathbf{A}_4$,

(d) relace „býti normální podgrupou“ obecně není tranzitivní.

Řešení. (a) Stačí si všimnout konjugace prvku $(1\,2)(3\,4) \in M$ prvkem $(1\,2\,3)$

$$(1\,2\,3) \circ (1\,2)(3\,4) \circ (1\,2\,3)^{-1} = (2\,3)(1\,4) \notin M,$$

což znamená, že M určitě nemůže být normální podgrupou grupy $\mathbf{A}_4$, a tedy ani $\mathbf{S}_4$.

(b) Vidíme, že všechny neidentické prvky obou podgrup jsou řádu dva, proto jsou samy k sobě inverzní. To znamená, že jsou obě množiny uzavřené na inverzní prvky.[1] Dále snadno ověříme, že součin každých dvou různých neidentických prvků $\mathbf{K}$ nám dává zbylý neidentický prvek, čímž jsme dokončili důkaz, že množiny M a $\mathbf{K}$ představují podgrupy grupy $\mathbf{S}_4$. Nyní můžeme přímočaře ověřit pro všechny čtyři permutace $\sigma \in \mathbf{K}$, že

$$\sigma \circ (1\,2)(3\,4) \circ \sigma^{-1} = (1\,2)(3\,4) \in M$$

(pro identitu a $(1\,2)(3\,4)$ je to navíc bezpracné), což znamená, že M je normální podgrupa grupy $\mathbf{K}$; tento výpočet je ovšem zbytečný, uvědomíme-li si, že $\mathbf{K}$ je komutativní grupa, tím pádem jsou všechny její podgrupy normální. Konečně tři neidentické prvky grupy $\mathbf{K}$ jsou právě všechny prvky grupy $\mathbf{S}_4$ sestávající ze dvou nezávislých cyklů, takže konjugování prvky $\mathbf{S}_4$ jenom ony tři prvky permutuje; proto je $\mathbf{K}$ normální podgrupa $\mathbf{S}_4$.

(c) Normální podgrupa alternující grupy musí být uzavřená na všechny konjugace. Jestliže tedy normální podgrupa $G \trianglelefteq \mathbf{A}_4$ obsahuje některý z netriviálních prvků $\mathbf{K}$, pak výpočet jako v (a) ukazuje, že už musí obsahovat celou $\mathbf{K}$. Pokud G obsahuje trojcyklus, pak jeho konjugováním prvky $\mathbf{A}_4$ dostaneme ještě tři další trojcykly (pozor, pouhým konjugováním nedostaneme všechny trojcykly, protože konjugujeme pouze sudými permutacemi) a zbývající čtyři trojcykly jsou právě ty inverzní k těm již získaným, tedy se musí také nalézat v G. Dle Lagrangeovy věty už podgrupa obsahující alespoň 8 prvků musí obsahovat všech 12 prvků, tedy jde o celou $\mathbf{A}_4$. Jediná vlastní podgrupa je tedy $\mathbf{K}$.

(d) To, že M je normální podgrupa $\mathbf{K}$ a $\mathbf{K}$ je normální podgrupa $\mathbf{S}_4$, plyne z (b), a že M není normální podgrupa grupy $\mathbf{S}_4$ jsme dokázali v (c), což dosvědčuje, že relace „býti normální podgrupou“ není tranzitivní.

Úloha 12.2. Jaké jsou možné faktorgrupy grupy $\mathbf{S}_3$?

[1] Poznamenejme, že tuto podmínku není pro *konečné* podgrupy nutné ověřovat, jestliže ověříme uzavřenost na grupovou operaci.

Řešení. V $\mathbf{S}_3$ máme právě tři normální podgrupy $\mathbf{S}_3$, $\mathbf{A}_3$ a $\{\mathrm{id}\}$. Kromě triviálních faktorů $\{0\} \cong \mathbf{S}_3/\mathbf{S}_3$ a $\mathbf{S}_3 \cong \mathbf{S}_3/\{\mathrm{id}\}$ tudíž zbývá už jen dvouprvkový, tedy cyklický faktor podle alternující grupy $\mathbb{Z}_2 \cong \mathbf{S}_3/\mathbf{A}_3$.

Úloha 12.3. Rozhodněte, které známé grupě je izomorfní daná faktorgrupa:

(a) $\mathbf{S}_n/\mathbf{A}_n$ pro libovolné $n > 2$,

(b) $\mathbb{R}^*/\mathbb{R}^+$, kde $\mathbb{R}^+ = \{r \in \mathbb{R}^* \mid r > 0\}$,

(c) $\mathbb{C}^*/\mathbf{S}^1$, kde $\mathbf{S}^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$.

(Nápověda: Nalezněte vhodný homomorfismus, jehož jádrem bude zadaná podgrupa, a použijte 1. větu o izomorfismu.)

Řešení. (a) Stačí si vzpomenout, že zobrazení znaménko $\mathrm{sgn}\colon \mathbf{S}_n \to \mathbb{Z}^*$ splňuje podmínku $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$, tedy jde o homomorfismus na multiplikativní grupu $\mathbb{Z}^* = \{\pm 1\}$. Protože jeho jádro tvoří právě sudé permutace $\mathbf{A}_n$, dostáváme díky první větě o izomorfismu a faktu, že dvouprvková grupa je nutně cyklická, izomorfismy

$$\mathbf{S}_n/\mathbf{A}_n = \mathbf{S}_n/\operatorname{Ker}(\mathrm{sgn}) \cong \mathbb{Z}^* = \{\pm 1\} \cong \mathbb{Z}_2.$$

(b) Uvážíme homomorfismus $r \mapsto \mathrm{sgn}(r)$ multiplikativních grup $\mathbb{R}^* \to \mathbb{Z}^*$. Jeho jádro je rovno $\mathbb{R}^+$, tudíž podle první věty o izomorfismu dostáváme obdobně jako v úloze (a) $\mathbb{R}^*/\mathbb{R}^+ \cong \mathbb{Z}^* \cong \mathbb{Z}_2$.

(c) Tentokrát vidíme, že $\mathbb{C}^*/\mathbf{S}^1 \cong \mathbb{R}^+$, jak dosvědčuje homomorfismus $z \mapsto |z|$ grupy $\mathbb{C}^*$ na grupu $\mathbb{R}^+$, jehož jádro tvoří právě podgrupa $\mathbf{S}^1$.

Úloha 12.4. Pro podgrupu $H = 3\mathbb{Z} \times 5\mathbb{Z} = \{(3a, 5b) \in \mathbb{Z} \times \mathbb{Z} \mid a, b \in \mathbb{Z}\}$ popište faktorgrupu $(\mathbb{Z} \times \mathbb{Z})/H$ jako součin aditivních grup $\mathbb{Z}_n$. Je tato faktorgrupa cyklická?

Řešení. I tentokrát zkonstruujeme zobrazení

$$\rho\colon Z \times \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \text{předpisem} \quad \rho(a, b) = (a \bmod 3, b \bmod 5)$$

Vidíme, že jde o zobrazení na $\mathbb{Z}_3 \times \mathbb{Z}_5$, a díky vlastnostem modulu se jedná o grupový homomorfismus. Než využijeme 1. větu o izomorfismu, spočítáme si jádro

$$\operatorname{Ker}(\rho) = \{(u, v) \in \mathbb{Z} \times \mathbb{Z} \mid u \equiv 0 \pmod 3,\ v \equiv 0 \pmod 5\} = \{(3a, 5b) \in \mathbb{Z} \times \mathbb{Z} \mid a, b \in \mathbb{Z}\} = H.$$

Nyní podle 1. věty o izomorfismu dostaneme

$$\mathbb{Z}_3 \times \mathbb{Z}_5 = \rho(\mathbb{Z} \times \mathbb{Z}) \cong (\mathbb{Z} \times \mathbb{Z})/\operatorname{Ker}(\rho) = (\mathbb{Z} \times \mathbb{Z})/H.$$

Protože podle čínské věty o zbytcích $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$, tedy grupy $\mathbb{Z}_3 \times \mathbb{Z}_5$ i $(\mathbb{Z} \times \mathbb{Z})/H$ jsou cyklické.

Úloha 12.5. Pro aditivní grupu $\mathbb{Z}_{12}$

(a) dokažte, že platí $\mathbb{Z}_{12}/\langle 3\rangle \cong \mathbb{Z}_3$ a $\mathbb{Z}_{12}/\langle 4\rangle \cong \mathbb{Z}_4$,

(b) vysvětlete, proč $\mathbb{Z}_{12}/\langle 5\rangle \not\cong \mathbb{Z}_4$ a rozhodněte, jaké cyklické grupě $\mathbb{Z}_n$ je $\mathbb{Z}_{12}/\langle 5\rangle$ izomorfní.

Řešení. (a) Jako obvykle zkonstruujeme homomorfismy $f\colon \mathbb{Z}_{12} \to \mathbb{Z}_3$ a $g\colon \mathbb{Z}_{12} \to \mathbb{Z}_4$ podmínkami $f(a) = a \bmod 3$ a $g(a) = a \bmod 4$, o nichž přímočaře ověříme, že jde o surjektivní homomorfismy. Poté spočítáme jádra

$$\operatorname{Ker}(f) = \{a \in \mathbb{Z}_{12} \mid f(a) = 0\} = \{a \in \mathbb{Z}_{12} \mid a \equiv 0 \pmod 3\} = \langle 3\rangle,$$
$$\operatorname{Ker}(g) = \{a \in \mathbb{Z}_{12} \mid g(a) = 0\} = \{a \in \mathbb{Z}_{12} \mid a \equiv 0 \pmod 4\} = \langle 4\rangle.$$

Nyní nám 1. věta o izomorfismu říká, že

$$\mathbb{Z}_{12}/\langle 3\rangle = \mathbb{Z}_{12}/\operatorname{Ker}(f) \cong \mathbb{Z}_3 \quad \text{a} \quad \mathbb{Z}_{12}/\langle 4\rangle = \mathbb{Z}_{12}/\operatorname{Ker}(f) \cong \mathbb{Z}_4.$$

(b) Prvek 5 nedělí řád grupy, dokonce $\mathrm{NSD}(5, 12) = 1$ a je tedy generátorem celé cyklické grupy $\mathbb{Z}_{12}$. To znamená, že $\mathbb{Z}_{12}/\langle 5\rangle = \mathbb{Z}_{12}/\mathbb{Z}_{12} \cong \{0\}$ (přičemž triviální grupa je cyklická).

Když se člověk rozfaktorizuje, (může, ale) nechce přestat:

Úloha 12.6. Určete řád prvku $P = ((1\,2\,3\,4)\,(5\,6\,7\,8\,9))\mathbf{A}_9$ v grupě $\mathbf{S}_9/\mathbf{A}_9$. Lze prvky (levé) rozkladové třídy P popsat pomocí znaménka a kolik jich je? Co tvoří třídu P^{-1}?

Řešení. Protože je grupa $\mathbf{S}_9/\mathbf{A}_9$ podle Lagrangeovy věty řádu $\frac{|\mathbf{S}_9|}{|\mathbf{A}_9|} = [\mathbf{S}_9 : \mathbf{A}_9] = 2$ a prvek $P \neq \mathbf{A}_9$, tedy není jednotkou faktorové grupy, nutně musí jít o prvek řádu 2 a $P = \mathbf{S}_9 \setminus \mathbf{A}_9$, tedy ho tvoří všechny liché permutace. Vidíme, že $|P| = |\mathbf{A}_9| = \frac{9!}{2}$ a $P^{-1} = P$, neboť každý prvek řádu dva je sám k sobě inverzní.

Úloha 12.7. Rozmyslete si, jak se počítá v aditivní abelovské grupě $\mathbb{Q}/\mathbb{Z}$, jejíž prvky můžeme reprezentovat jako rozkladové třídy racionálních čísel z intervalu $[0, 1)$:

(a) Spočítejte $\left[\frac{1}{2}\right] + \left[\frac{1}{2}\right]$, $5 \cdot \left[\frac{1}{3}\right]$ a najděte opačný prvek k $\left[\frac{1}{3}\right]$,

(b) vyřešte rovnici $3 \cdot x = \left[\frac{1}{2}\right]$,

(c) ukažte, že pro každé prvočíslo p a $k \in \mathbb{N}$ existuje v $\mathbb{Q}/\mathbb{Z}$ prvek řádu p^k. Kolik jich je?

Řešení. Nejprve uvážíme, že čitatel výsledného zlomku každého výpočtu je třeba upravit modulo jmenovatel, tedy $[\frac{a}{b}] = [\frac{a \bmod b}{b}]$.

(a) Nyní už snadno spočítáme

$$\left[\frac{1}{2}\right] + \left[\frac{1}{2}\right] = \left[\frac{2}{2}\right] = [0]\,, \quad 5 \cdot \left[\frac{1}{3}\right] = \left[\frac{5}{3}\right] = \left[\frac{2}{3}\right], \quad -\left[\frac{1}{3}\right] = \left[\frac{-1}{3}\right] = \left[\frac{2}{3}\right].$$

(b) Hledáme $3 \cdot \left[\frac{a}{b}\right] = \cdot \left[\frac{3a}{b}\right] = \left[\frac{1}{2}\right]$, kde předpokládáme, že jsou a a b nesoudělné a $0 \leq a < b$. Potom nutně $b \in \{2, 6\}$. Pokud $b = 2$, pak $3a \equiv 1 \pmod 2$, tedy $a = 1$ a pokud $b = 6$, pak $3a \equiv 3 \pmod 6$, tedy opět $3a \equiv 1 \pmod 2$, tedy $a = 1, 3$. Dostáváme 3 řešení $\left[\frac{1}{2}\right]$, $\left[\frac{1}{6}\right]$ a $\left[\frac{5}{6}\right]$.

(c) Snadno uvážíme, že prvek tvaru $\left[\frac{a}{p^k}\right]$ pro celé a je řádu p^k, právě když $p \nmid a$. Různá řešení úlohy potom reprezentují prvky $\frac{a}{p^k}$ z intervalu $[0, 1)$, tedy a splňující podmínku $0 \leq a < p^k$. Vidíme tudíž, že máme v $\mathbb{Q}/\mathbb{Z}$ právě $\varphi(p^k)$ prvků řádu p^k.

Úloha 12.8. Dokažte existenci izomorfismu $\mathbf{D}_{12}/\{\mathrm{id}, \mathrm{rot}_\pi\} \cong \mathbf{S}_3$ pro dihedrální grupu $\mathbf{D}_{12}$, kde rot_π značí rotaci o úhel π. (Nápověda: Nalezněte tři vhodné „objekty“, které standardní geometrické působení $\mathbf{D}_{12}$ permutuje.)

Řešení. Opět zkonstruujeme grupový homomorfismus, který symetrii šestiúhelníku přiřadí permutace tří úhlopříček šestiúhelníka (po očíslování úhlopříček dostáváme grupu $\mathbf{S}_3$). Vidíme, že jádro je právě $\{\mathrm{id}, rot_\pi\}$ a obraz celé $\mathbf{S}_3$, proto díky první větě o izomorfismu máme izomorfismus $\mathbf{D}_{12}/\left\{\mathrm{id}, \mathrm{rot}_\pi\right\} \cong \mathbf{S}_3$.

Úloha 12.9. Označme $I \subseteq \mathbb{Z}[i]$ ideál generovaný prvkem $1 + 3i$ a buď $\mathbf{R} = \mathbb{Z}[\mathrm{i}]/I$. Postupně ukažte, že:

(a) v $\mathbf{R}$ platí $[\mathrm{i}] = [3]$, $[10] = [0]$,

(b) pro každý okruh $\mathcal{S}$ existuje jediný homomorfismus $\phi\colon \mathbb{Z} \to \mathcal{S}$ a toto ϕ je pro $\mathcal{S} = \mathbf{R}$ surjektivní

(c) 2 ani 5 nejsou v $\mathbb{Z}[i]$ dělitelné prvkem $1 + 3i$,

(d) $\mathbf{R} \simeq \mathbb{Z}_{10}$,

(e) I není maximální, najděte nějaký maximální ideál $J \supsetneq I$ a popište $\mathbb{Z}[i]/J$.

Řešení. (a) Spočítáme, že $[i] = [3]$, protože $i - 3 = i(1+3i) \in I$ a $[10] = [0]$, neboť $10 = (1+3i)(1-3i) \in I$.

(b) Tento homomorfismus je určen jednoznačně právě obrazem prvku 1, který se musí zobrazit na jednotkový prvek okruhu $\mathcal{S}$, potom $\phi(z) = z \cdot 1$.

V případě homomorfismu si úvahou z (a) uvědomíme, že pro každý prvek $a + bi \in \mathbb{Z}[i]$ máme

$$[a + bi] = [a + 3b] = \phi(a + 3b) \in \phi(\mathbb{Z}).$$

(c) Plyne z pozorování, že normy $4 = |2|^2$ ani $25 = |5|^2$ nejsou dělitelné normou $|1 + 3i|^2 = 10$.

(d) Stačí spočítat pro homomorfismus ϕ z úlohy (a) jádro $\ker(\phi) = \{n \in \mathbb{Z} \mid 3 + i \mid n\} = 10\mathbb{Z}$ a využít 1. věty o izomorfismu pro okruhy (věta 20.7):

$$\mathbf{R} = \phi(\mathbb{Z}) \cong \mathbb{Z}/\ker(\phi) = \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}_{10}.$$

(e) Podle (d) máme $\mathbb{Z}[i]/I = \mathbf{R} \cong \mathbb{Z}_{10}$, což není těleso. Věta 20.10 potom říká, že I není maximální ideál. Pro nalezení maximálních ideálů si stačí vzít ireducibilní rozklad generátoru

$$1 + 3i = (1 + i)(2 + i)$$

Potom oba ideály $J = (1 + i)\mathbb{Z}[i]$ a $K = (2 + i)\mathbb{Z}[i]$ obsahují ideál I, a protože

$$\mathbb{Z}[i]/J \cong \mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}_2, \quad \mathbb{Z}[i]/K \cong \mathbb{Z}[i]/(2 + i) \cong \mathbb{Z}_5$$

faktory představují dvouprvkové a pětiprvkové těleso, tudíž jsou ideály J a K opět díky větě 20.10 maximální.

Úloha 12.10. Pro grupu $\mathbb{R}/\mathbb{Z}$

(a) popište prvky konečného řádu a řád každého takového prvku určete,

(b) dokažte, že je izomorfní podgrupě $\mathbf{S}^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$ grupy $\mathbb{C}^*$.

Řešení. (a) Protože prvek $[r] \in \mathbb{R}/\mathbb{Z}$ je konečného řádu, právě když existuje přirozené číslo n, pro něž $nr \in \mathbb{Z}$, jde právě o rozkladové třídy racionálních čísel. Prvek $\left[\frac{a}{b}\right]$ má pro a, b nesoudělná řád roven b.

(b) Stačí uvážit zobrazení $\rho\colon \mathbb{R} \to \mathbb{C}^*$ dané předpisem $\rho(r) = e^{2\pi ir}$; z vlastností exponenciály vidíme, že se jedná o homomorfismus, a zřejmě jde i o zobrazení na $\mathbf{S}^1$. Jádrem tohoto homomorfismu jsou reálná čísla r splňující $e^{2\pi ir} = 1$, tedy přesně celá čísla. Z 1. věty o izomorfismu tedy máme $\mathbb{R}/\mathbb{Z} \cong \mathbf{S}^1$.

Úloha 12.11. Popište všechny homomorfismy $\mathbf{S}_3 \to \mathbb{Z}_n$ v závislosti na $n \in \mathbb{N}$.

Řešení. Podle 1. věty o izomorfismu představuje homomorfní obraz $\mathbf{S}_3$ vždy podgrupu komutativní grupy $\mathbb{Z}_n$, která je izomorfní faktoru podle jádra příslušného homomorfismu. Protože je jádro vždy normální podgrupa, připadají v úvahu pouze jádra $\mathbf{S}_3$ a $\mathbf{A}_3$. Pro jádro $\mathbf{S}_3$ dostáváme triviální homomorfismus $\mathbf{S}_3 \to 0$ a pro sudá n ještě existuje homomorfismus, který obdržíme složením přirozené projekce a vnoření $\mathbf{S}_3 \to \mathbf{S}_3/\mathbf{A}_3 \to \mathbb{Z}_n$ daný podmínkou $(12)\mathbf{A}_3 \mapsto \frac{n}{2}$ s jádrem $\mathbf{A}_3$ a obrazem $\operatorname{Im} f = \left\langle \frac{n}{2} \right\rangle$.

⋆ **Úloha 12.12.** Dokažte, že grupa $\mathbf{A}_5$ neobsahuje žádné vlastní normální podgrupy. (Nápověda: Dokažte, že v každé netriv. normální podgrupě musí být obsažen trojcyklus.)

Řešení. Nechť $N \neq \{\mathrm{id}\}$ je normální podgrupa $\mathbf{A}_5$. Pokud N obsahuje jeden trojcyklus, díky konjugování a uzavřenosti na inverzy obsahuje i všechny ostatní trojcykly, které už generují celé $\mathbf{A}_5$. Obsahuje-li permutaci tvaru $(ab)(cd)$, obsahuje i trojcyklus

$$(cde) = (ab)(cd) \circ (ab)(ce) = (ab)(cd) \circ ((cde) \circ (ab)(cd) \circ (cde)^{-1}),$$

proto podle předchozí úvahy opět $N = \mathbf{A}_5$. Konečně pokud $(abcde) \in N$, pak

$$(aec) = (abcde) \circ (badce) = (abcde) \circ ((ab)(cd) \circ (abcde) \circ ((ab)(cd))^{-1}),$$

tedy znovu $N = \mathbf{A}_5$.

Úloha 12.13. Uvažme podgrupy $\mathbf{G} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{R},\, a > 0 \right\}$ a $\mathbf{H} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R},\, a > 0 \right\}$ grupy $\mathbf{GL}_2(\mathbb{R})$.

(a) Ověřte, že vskutku jde o podgrupy $\mathbf{GL}_2(\mathbb{R})$.

(b) Popište levé a pravé rozkladové třídy $\mathbf{H}$ jakožto podgrupy $\mathbf{G}$. (Pro jednodušší popis lze uvažovat geometrickou reprezentaci matice $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ jako bodu (a, b) v reálné rovině $\mathbb{R}^2$.)

(c) Je $\mathbf{H}$ normální podgrupou $\mathbf{G}$?

(d) Najděte nějakou levou a pravou transversálu rozkladu.

Řešení. (a) Obě množiny obsahují jednotkovou matici, tj. jednotkový prvek $\mathbf{GL}_2(\mathbb{R})$. Pro $\mathbf{H}$ jsou ostatní podmínky na podgrupu splněny takřka očividně, u $\mathbf{G}$ ověříme, že

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & b + ad \\ 0 & 1 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix},$$

přičemž pro $a, c > 0$ je v levém horním rohu výsledných matic také vždy kladné číslo.

(b) Dostáváme, že

$$\mathbf{H} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} ac & bc \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{R}^+ \right\}, \quad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mathbf{H} = \left\{ \begin{pmatrix} ac & b \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{R}^+ \right\},$$

tedy pravá rozkladová třída odpovídá polopřímce z počátku se směrnicí $\frac{a}{b}$ ležící vpravo od osy y a levá rozkladová třída odpovídá vodorovné přímce $y = b$.

(c) Jelikož jsme v (b) nahlédli, že levé a pravé rozkladové třídy se liší, $\mathbf{H}$ není normální podgrupou grupy $\mathbf{G}$ podle tvrzení 19.1 z přednášky.

(d) Díky (b) vidíme, že pravou transversálu tvoří například

$$\left\{ \begin{pmatrix} \cos\alpha & \sin\alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \left(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\right) \right\},$$

neboť nám určuje všechny polopřímky z počátku ležící vpravo od osy y. Levou transversálu představuje například

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\},$$

odpovídající levé rozkladové třídy nám jednoznačně určují všechny přímky $y = b$.

Úloha 12.14. Nechť m, n jsou nesoudělná celá čísla a označme N podgrupu aditivní grupy $\mathbb{Z} \times \mathbb{Z}$ generovanou dvojicí (m, n). Dokažte, že $(\mathbb{Z} \times \mathbb{Z})/N$ je izomorfní $\mathbb{Z}$.

Řešení. Definujme $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ předpisem $f((x, y)) = nx - my$. Jelikož jsou m a n nesoudělná, z Bézoutovy věty nalezneme $x, y \in \mathbb{Z}$ taková, že $f((x, y)) = 1$, takže obrazem f je celé $\mathbb{Z}$. Na druhou stranu, je-li $(x, y) \in \operatorname{Ker} f$, pak $nx - my = 0$, což lze (pro nenulová x, y) přepsat jako

$$\frac{x}{y} = \frac{m}{n}.$$

Jelikož jsou m a n nesoudělná, je zlomek na pravé straně v základním tvaru, takže (x, y) musí být násobkem (m, n). Jinak řečeno, $\operatorname{Ker} f$ je přesně podgrupa generovaná (m, n). První věta o izomorfismu dává požadovaný izomorfismus.

⋆ **Úloha 12.15.** Buď T libovolné těleso. Dokažte, že faktor grupy $\mathbf{GL}_2(T)$ podle podgrupy tvořené skalárními násobky jednotkové matice je izomorfní grupě výrazů tvaru

$$\frac{ax+b}{cx+d},$$

kde $a, b, c, d \in T$, $ad \neq bc$ a grupová operace je „skládání funkcí“ (přičemž kde jsou výrazy definované neřešíme).

Řešení. Uvažme zobrazení

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{ax+b}{cx+d};$$

díky regularitě matice je splněna podmínka $ad \neq bc$ a vzorem „identického zobrazení“ $x/1$ jsou právě skalární násobky jednotkové matice. Že jde o homomorfismus, lze ověřit čistě mechanicky, ale lze to nahlédnout i tak, že pro vektor $\mathbf{x} = (r, s) \in T^2$ s poměrem složek $x = r/s$ je výraz $(ax + b)/(cx + d)$ přesně poměrem složek vektoru $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \mathbf{x}$ (což platí i pro „nekonečný poměr“).

⋆ **Úloha 12.16.** Dokažte, že volbou $T = \mathbb{Z}_3$ v úloze 12.15 dostaneme grupu izomorfní grupě $\mathbf{S}_4$.

Řešení. Uvedená grupa působí na (čtyřprvkové) množině jednodimenzionálních podprostorů vektorového prostoru $\mathbb{Z}_3^2$ (neboli bodech projektivní přímky), přičemž standardní výpočet ukáže, že jde o grupu o 24 prvcích, tedy musí jít o všechny permutace těchto čtyř objektů.