# 5. Grupy a tělesa

**Cv. 5.1** Zjistěte, zda je (Abelovou) grupou:

(a) $(\mathbb{Q}, +)$,

(b) $(\mathbb{Q}, -)$,

(c) $(\mathbb{Q}, \cdot)$,

(d) $(\mathbb{Q} \setminus \{0\}, \circ)$, kde $a \circ b = |ab|$ pro všechna $a, b \in \mathbb{Q}$,

(e) $(\mathbb{Q}, \circ)$, kde $a \circ b = \frac{a+b}{2}$ pro všechna $a, b \in \mathbb{Q}$,

(f) $(\mathbb{Q}, \circ)$, kde $a \circ b = a + b + 3$ pro všechna $a, b \in \mathbb{Q}$,

(g) $(\mathcal{F}, +)$, tj. množina $\mathcal{F}$ všech reálných funkcí jedné proměnné s operací sčítání funkcí,

(h) množina rotací v $\mathbb{R}^2$ kolem počátku s operací skládání zobrazení,

(i) množina posunutí v $\mathbb{R}^2$ s operací skládání zobrazení.

***Řešení:***

(a) $(\mathbb{Q}, +)$ je Abelovou grupou:

- sčítání je komutativní i asociativní operace,
- neutrální prvek je 0
- k racionálnímu číslu $q$ je inverzní prvek $-q$.

(b) $(\mathbb{Q}, -)$ není grupou, protože rozdíl racionálních čísel není asociativní operace. Například $(8 - 6) - 1 = 1 \neq 3 = 8 - (6 - 1)$.

(c) $(\mathbb{Q}, \cdot)$ není grupou. Součin je sice komutativní i asociativní operace a existuje neutrální prvek 1, ale k číslu 0 neexistuje inverzní prvek.

(d) $(\mathbb{Q}\setminus\{0\}, \circ)$ s operací $a \circ b = |ab|$ není grupou, protože není zaručena existence neutrálního prvku. Pro každé $a < 0$ a číslo $e$ je $a \circ e = |ae| > 0 > a$. Tudíž žádné $e$ nemůže splňovat definici neutrálního prvku pro záporná $a$.

(e) $(\mathbb{Q}, \circ)$ s operací $a \circ b = \frac{a+b}{2}$ není grupou, protože aritmetický průměr čísel není asociativní. Například pro $a = 1$, $b = 5$, $c = 7$ máme $a \circ (b \circ c) = \frac{1}{2}\left(1 + \frac{5+7}{2}\right) = 3.5 \neq 5 = \frac{1}{2}\left(\frac{1+5}{2} + 7\right) = (a \circ b) \circ c$.

(f) $(\mathbb{Q}, \circ)$ s operací $a \circ b = a + b + 3$ je Abelovou grupou. Asociativita a komutativita platí z asociativity a komutativity sčítání nad $\mathbb{Q}$. Neutrální prvek je $e = -3$, protože pro každé $a \in \mathbb{Q}$ platí

$$a \circ e = a + (-3) + 3 = a = (-3) + a + 3 = e \circ a.$$

Konečně, inverzní prvek k prvku $a \in \mathbb{Q}$ je $a^{-1} = -a - 6$, protože

$$a \circ a^{-1} = a + (-a - 6) + 3 = -3 = e = -3 = (-a - 6) + a + 3 = a^{-1} \circ a.$$

(g) $(\mathcal{F}, +)$ je grupou. Asociativita plyne z definice součtu funkcí a asociativity sčítání nad $\mathbb{R}$. Pro každé $f, g, h \in \mathcal{F}$ a $x \in \mathbb{R}$ platí $f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)$. Neutrální prvek je identicky nulová funkce $e(x) = 0$ pro všechna $x \in \mathbb{R}$. Inverzní prvek k funkci $f \in \mathcal{F}$ je funkce $-f$.

(h) Množina rotací v $\mathbb{R}^2$ kolem počátku je Abelovou grupou. Asociativita plyne z asociativity skládání zobrazení. Komutativita platí také, protože uvažujeme rotace v rovině. Neutrálním prvkem je například rotace o 360 stupňů. Inverzním prvkem k rotaci o úhel $\alpha$ je rotace o úhel $\alpha$ v opačném směru.

(i) Množina posunutí v $\mathbb{R}^2$ je Abelovou grupou. Asociativita plyne z asociativity skládání zobrazení a komutativita z komutativity sčítání vektorů. Neutrálním prvkem je identické zobrazení $e((x_1, x_2)^T) = (x_1, x_2)^T$ (tj. posunutí vektorem $(0,0)^T$) a inverzím prvkem k posunutí $t((x_1, x_2)^T) = (x_1, x_2)^T + (a, b)^T$ je posunutí $t^{-1}((x_1, x_2)^T) = (x_1, x_2)^T - (a, b)^T$.

**Cv. 5.2** Vyplňte tabulku pro binární operaci $\circ$ na $G$ tak aby $(G, \circ)$ byla grupou s neutrálním prvkem 0. Výsledek zdůvodněte.

(a)

| $\circ$ | 0 | 1 |
|---|---|---|
| 0 | | |
| 1 | | |

(b)

| $\circ$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | | | |
| 2 | | | |

(c)

| $\circ$ | 0 |
|---|---|
| 0 | |

(d)

| $\circ$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | | | | |
| 1 | | 0 | | |
| 2 | | | | |
| 3 | | | | |

***Řešení:***
Všechny tabulky až na poslední jsou určeny jednoznačně. Fakt, že 0 je neutrálním prvkem pro $\circ$ určuje první řádek i sloupec tabulky. Existence levé i pravé inverze omezuje pozice 0 na diagonále nebo symetricky podle diagonály. Asociativita vynutí zbylé pozice. Dostáváme:

(a)

| $\circ$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

… aditivní grupa modulo 2, tj. $(\mathbb{Z}_2, +)$

(b)

| $\circ$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

… aditivní grupa modulo 3, tj. $(\mathbb{Z}_3, +)$

(c)

| $\circ$ | 0 |
|---|---|
| 0 | 0 |

… triviální grupa,

(d)

| $\circ$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 0 | 3 | 2 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 2 | 1 | 0 |

, anebo

| $\circ$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 0 | 3 | 2 |
| 2 | 2 | 3 | 1 | 0 |
| 3 | 3 | 2 | 0 | 1 |

.

První je Kleinova grupa symetrií obdélníka, a to druhé je $(\mathbb{Z}_4, +)$ s přejmenovanými čísly (prohozena 1 a 2).

**Cv. 5.3** Rozhodněte a zdůvodněte, zda je Abelovou grupou množina

$$\left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}; z \in \mathbb{Z} \right\} \text{ s maticovým součinem.}$$

***Řešení:***

Ano. Nejdříve ukážeme, že maticový součin je uzavřený pro danou množinu. Pro všechna $a, b \in \mathbb{Z}$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}, \tag{1}$$

což je matice náležející do zadané množiny (neboť celá čísla jsou uzavřená na součet).

Asociativita maticového součinu na dané množině plyne z asociativity maticového součinu pro obecné čtvercové matice stejných rozměrů.

Neutrálním prvkem je jednotková matice řádu dva, jež patří do zadané množiny (volbou $z := 0 \in \mathbb{Z}$).

Inverzním prvkem pro matici $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ je celočíselná matice $\left(\begin{smallmatrix} 1 & -z \\ 0 & 1 \end{smallmatrix}\right)$, což plyne z rovnosti (1).

Zadaná množina matic spolu s maticovým součinem tvoří grupu. Zbývá ověřit, zda je maticový součin pro tyto matice komutativní. Komutativita maticového součinu plyne z rovnosti (1) a komutativity sčítání nad $\mathbb{Z}$. I když obecně součin matic není komutativní, pro naši třídu matic komutativita splněna jest.

Ověřili jsme tedy, že se jedná o Abelovskou grupu.

**Cv. 5.4** Mějme grupu $(G, \circ)$ s neutrálním prvkem $e$ a inverze k prvku $a$ nechť je $a^{-1}$. Proveďte:

(a) najděte $e^{-1}$,

(b) upravte $(a \circ b)^{-1}$.

***Řešení:***

(a) $e^{-1} = e$, neboť $e \circ e = e$.

(b) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ neboť

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e$$

a analogicky v opačném pořadí.

**Cv. 5.5** Najděte různé příklady podgrup grupy matic $(\mathbb{R}^{n\times n}, +)$.

***Řešení:***
Příkladů je nespočet. Podgrupou je taková (neprázdná) podmnožina matic $\mathbb{R}^{n\times n}$, která je uzavřená na násobky a součty. Přikladem je tak například podgrupa symetrických matic. Dalšími příklady jsou trojúhelníkové matice, horní trojúhelníkové matice, diagonální matice, matice s racionálními čísly, matice s celými čísly, atp.

**Cv. 5.6** Vyjádřete jako prvky daného tělesa výrazy:

(a) $((2^{-1}+1)4)^{-1}$ a $4/3$ v tělese $\mathbb{Z}_5$,

(b) $6+7$, $-7$, $6\cdot 7$, $7^{-1}$ a $6/7$ v tělese $\mathbb{Z}_{11}$.

***Řešení:***

(a) Těleso $\mathbb{Z}_5$ je definováno jako množina všech zbytků v $\mathbb{Z}$ po dělení 5 spolu s operacemi součtu a součinu modulo 5. Pro názornost uvádíme tabulky pro obě operace.

| $\mathbb{Z}_5,+$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

,

| $\mathbb{Z}_5,\cdot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Podle definice tělesa má množina $\mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ se součinem modulo 5 tvořit Abelovu grupu; zde je to takzvaná multiplikativní grupa modulo 5. V tabulce můžeme některé vlastnosti grupy snadno nahlédnout, například komutativitu nebo existenci neutrálního a inverzního prvku.

Nyní můžeme vyhodnotit zadané výrazy v $\mathbb{Z}_5$, kde při výpočtu nalezneme multiplikativní inverzi k libovolnému $a \in \mathbb{Z}_5 \setminus \{0\}$ v tabulce tak, že v řádku s $a$ najdeme hodnotu 1 a index $b$ odpovídajícího sloupce musí být hledaná multiplikativní inverze $a^{-1}$, protože $a \cdot b = 1$ v $\mathbb{Z}_5$. Dostáváme:

$$((2^{-1}+1)4)^{-1} = ((3+1)4)^{-1} = (4\cdot 4)^{-1} = (1)^{-1} = 1 \text{ v } \mathbb{Z}_5$$

a

$$4/3 = 4\cdot 3^{-1} = 4\cdot 2 = 3 \text{ v } \mathbb{Z}_5.$$

(b) Postupujeme podobně jako pro $\mathbb{Z}_5$, ale nebudeme konstruovat celou tabulku pro součin v $\mathbb{Z}_{11}$. Dostáváme:

$$\begin{aligned} 6+7 &= 6+7 \pmod{*}11 = 13 \pmod{*}11 = 2 \text{ v } \mathbb{Z}_{11}, \\ -7 &= 11-7 \pmod{*}11 = 4 \text{ v } \mathbb{Z}_{11}. \\ 6\cdot 7 &= 6\cdot 7 \pmod{*}11 = 42 \pmod{*}11 = 9 \text{ v } \mathbb{Z}_{11}. \end{aligned}$$

Při hledání multiplikativní inverze k prvku 7 můžeme postupovat jako při výpočtu řádku odpovídajícího 7 v tabulce pro součin v $\mathbb{Z}_{11}$. Výpočet zastavíme v momentě, kdy uvidíme na pravé straně číslo 1:

$$\begin{aligned}7 \cdot 1 &= 7,\\ 7 \cdot 2 &= 3,\\ 7 \cdot 3 &= 10,\\ 7 \cdot 4 &= 6,\\ 7 \cdot 5 &= 2,\\ 7 \cdot 6 &= 9,\\ 7 \cdot 7 &= 5,\\ 7 \cdot 8 &= 1.\end{aligned}$$

Vidíme, že

$$7^{-1} = 8 \text{ v } \mathbb{Z}_{11}.$$

Tuto hodnotu využijeme i při posledním výpočtu:

$$6/7 = 6 \cdot 7^{-1} = 6 \cdot 8 = 48 \pmod{*} 11 = 4 \text{ v } \mathbb{Z}_{11}.$$

**Cv. 5.7** Nad $\mathbb{Z}_5$ najděte množinu všech řešení soustavy rovnic

$$\begin{aligned}3x + 2y + z &= 1,\\ 4x + y + 3z &= 3\end{aligned}$$

a spočítejte její mohutnost.

***Řešení:***
Postupujeme podobně jako pro soustavy rovnic nad $\mathbb{R}$. Využijeme toho, že eliminovat prvky pod pivotem můžeme přičtením vhodného násobku řádku s pivotem. Přičtením 2-násobku prvního řádku k druhému dostáváme

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 4 & 1 & 3 & 3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Za volné proměnné zvolíme parametry $y, z \in \mathbb{Z}_5$ a vyjádříme

$$x = 3^{-1}(1 - 2y - z) = 2(1 + 3y + 4z) = 2 + y + 3z.$$

Množina všech řešení dané soustavy je tedy

$$\{(2,0,0)^T + y(1,1,0)^T + z(3,0,1)^T \mid y, z \in \mathbb{Z}_5\}.$$

Máme $25 = 5 \cdot 5$ různých voleb parametrů $y$ a $z$ a mohutnost množiny řešení je tedy 25.

**Cv. 5.8** V $\mathbb{Z}_7$ spočítejte mocninu matice $A^{100}$ pro matici $A = \left(\begin{smallmatrix} 3 & 2 \\ 1 & 4 \end{smallmatrix}\right)$.

***Řešení:***

Nad konečným tělesem musí být posloupnost matic $A^i$ pro $i = 1, \dots, \infty$ cyklická. Spočtěme několik prvních členů této posloupnosti:

$$\begin{aligned}
A = A^1 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}, \\
A^2 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \\
A^3 &= \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix}, \\
A^4 &= \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \\
A^5 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix}, \\
A^6 &= \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
A^7 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = A.
\end{aligned}$$

Vidíme, že perioda této posloupnost je 6. Hledanou mocninu matice tedy spočítáme jako

$$A^{100} = A^{100 \pmod *6} = A^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

*Poznámka.* Trochu práce si můžeme ušetřit tím, že si uvědomíme, že druhá mocnina má tvar $A^2 = 4I_2$. Tudíž

$$A^{100} = (A^2)^{50} = (4I_2)^{50} = 4^{50} I_n.$$

Tím jsme maticový problém zredukovali na skalární problém. Z Malé Fermatovy věty víme, že $4^6 = 1$ v $\mathbb{Z}_7$, čili

$$4^{50} I_n = 4^{50 \pmod *6} I_n = 4^2 I_n = 2I_n.$$

**Cv. 5.9** Spočítejte $20^{3332}$ v tělese $\mathbb{Z}_{31}$.

***Řešení:***

Z Malé Fermatovy věty víme, že v tělese $\mathbb{Z}_{31}$ je $20^{30} = 1$. Proto

$$20^{3332} = 20^{3332 \pmod *30} = 20^2 = 28.$$

# 6. Permutace

**Cv. 6.1** Mějme permutace

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}, \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 6 & 4 \end{pmatrix}.$$

Najděte jejich cykly, znaménka, inverze a složte permutace $p, q$ mezi sebou v obou pořadích.

***Řešení:***

Permutace $p$ zobrazuje $1 \to 2$, dále $2 \to 3$, $3 \to 4$ a $4 \to 1$. Tudíž jeden cyklus je $(1, 2, 3, 4)$, analogicky druhý cyklus je $(5, 6)$. Tudíž zápis permutace pomoci cyklů je $p = (1, 2, 3, 4)(5, 6)$.

Podobně pro permutaci $q$ máme $1 \to 1$ (první cyklus), $2 \to 3$, $3 \to 2$ (druhý cyklus) a $4 \to 5$, $5 \to 6$, $6 \to 4$ (třetí cyklus). Permutaci $q$ lze zapsat pomocí cyklů jako $q = (1)(2, 3)(4, 5, 6)$.

Permutace $p$ je zadána na $n = 6$ prvcích a skládá se ze $c = 2$ cyklů, proto má znaménko $\operatorname{sgn}(p) = (-1)^{n-\text{počet cyklů}} = (-1)^{6-2} = 1$. Podobně spočítáme $\operatorname{sgn}(q) = (-1)^{6-3} = -1$.

Inverzní permutaci k permutaci $p$ můžeme najít několika způsoby. Pokud vyjdeme z tabulkového zadání $p$, tak stačí prohodit oba řádky, čímž se ze vzorů stanou obrazy a naopak, a pak jen setřídit sloupce od nejmenšího po největší. Dostaneme $p^{-1}$ vyjádřené tabulkou

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}.$$

Pokud využijeme zápisu $p$ pomocí cyklů, stačí pouze prohodit pořadí čísel v každém cyklu, tj. $p^{-1} = (4, 3, 2, 1)(6, 5)$. Zde si můžeme uvědomit, že cykly délek 1 a 2 nemusíme invertovat, protože jsou sami sobě inverzní.

Permutace skládáme jako každé jiné zobrazení, tedy $p \circ q$ zobrazí prvek $i$ na $p(q(i))$. Tabulkově vyjádřeno

$$\begin{array}{ccccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ q & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 & 5 & 6 & 4 \\ p & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 3 & 6 & 5 & 1 \end{array}$$

čili

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}.$$

Podobně můžeme postupovat pomocí popisu přes cykly a dospějeme k vyjádření $p \circ q = (1, 2, 4, 6)(3)(5)$. Pro srovnání, složení v opačném pořadí je $q \circ p = (1, 3, 5, 4)(2)(6)$. To ilustruje, že skládání permutací není komutativní.

**Cv. 6.2** Mějme permutaci
$$p = (1,3,4)(2,5)(6,11,10,9,8,7).$$

Spočítejte permutace $p^9$ a $p^{-14}$.

Pro jakou nejmenší mocninu $k \geq 1$ dostaneme $p^k = id$?

***Řešení:***
Naivní způsob spočítání $p^9$ je složit postupně permutaci $p^9 = p \circ p \circ p \circ p \circ p \circ p \circ p \circ p \circ p$.

Efektivnější způsob počítání vysokých mocnin (čehokoli) je využití dvojkového zápisu exponentu a iterovaného mocnění na druhou. Konkrétně k permutaci $p^9$ se dostaneme tak, že spočítáme $p^2 = p \circ p$, následně $p^4 = p^2 \circ p^2$, $p^8 = p^4 \circ p^4$ a nakonec $p^9 = p^8 \circ p$.

V našem případě, kdy mocníme permutace, můžeme využít ještě rozkladu na cykly. Cyklus $p = (u_1, \ldots, u_k)$ délky $k$ se při mocnění chová tak, že $p^k = id$ a $p^{k+1} = p$. To nás vede k metodě, kdy budeme mocnit každý cyklus zvlášť a mocninu daného cyklu spočítáme efektivně s využitím modula jeho délky. Konkrétně, $(1,3,4)^9 = id$, $(2,5)^9 = (2,5)^1 = (2,5)$ a $(6,11,10,9,8,7)^9 = (6,11,10,9,8,7)^3 = (6,9)(7,10)(8,11)$ Tudíž
$$p^9 = (1)(2,5)(3)(4)(6,9)(7,10)(8,11).$$

Permutaci $p^{-14}$ určíme stejným způsobem s tím, že uvažujeme i záporné exponenty. Tudíž $(1,3,4)^{-14} = (1,3,4)^1$, $(2,5)^{-14} = (2,5)^0 = id$, $(6,11,10,9,8,7)^{-14} = (6,11,10,9,8,7)^4 = (6,8,10)(7,9,11)$. Nakonec dostáváme
$$p^{-14} = (1,3,4)(2)(5)(6,8,10)(7,9,11).$$

Abychom určili nejmenší mocninu $k \geq 1$ takovou, že $p^k = id$, podíváme se na jednotlivé cykly a zjistíme, jaké mocniny dají identitu. První cyklus má délku 3, tedy třetí mocnina a jakýkoli její celý násobek dají identitu. Podobně druhý cyklus má délku 2, čili identitu dostaneme pro sudé mocniny, a konečně třetí cyklus délky 6 vede na mocninu 6. Nejmenší společný násobek čísel $2,3,6$ je 6, tedy hledané $k = 6$. Při šesté mocnině se první cyklus *protočí* 2-krát, druhý 3-krát a poslední 1-krát.

**Cv. 6.3** Rozložte permutaci $(1,2,3,4,5)$ na složení transpozic, a to alespoň dvěma různými způsoby. Jaký je nejmenší možný počet transpozic, které k rozkladu potřebujeme?

***Řešení:***
Dvě možná řešení jsou:
$$(1,2,3,4,5) = (1,2)(2,3)(3,4)(4,5) = (1,5)(1,4)(1,3)(1,2).$$

Transpozic musí být alespoň 4. Každá nová transpozice sníží počet cyklů maximálně o 1, takže abychom z identity zkonstruovali cyklus délky 5, potřebujeme alespoň 4 transpozice.

**Cv. 6.4** Dokažte, že každou permutaci $p \in S_n$ lze složit pomocí $n-2$ nebo $n-1$ transpozic.

***Řešení:***
V předchozím cvičení 6.3 jsme viděli, že každý cyklus délky $c$ lze složit pomocí $c-1$ transpozic. Pokud se tedy permutace $p$ skládá z právě $k$ cyklů, tak ji umíme složit z právě $n-k$ transpozic. Tím pádem každou permutaci lze zložit z maximálně $n-1$ transpozic. Pokud počet transpozic je menší než $n-2$, tak přidáme příslušný počet dodatečných (a v zásadě zbytečných) párů transpozic $(i,j)(i,j)$ tak, abychom počet transpozic navýšili na požadovaný počet.

**Cv. 6.5** Určete znaménko permutace $r$ zadané tabulkou:

$$r = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}$$

***Řešení:***
Permutaci $r$ můžeme pomocí cyklů zapsat jako

$$r = \begin{cases} (1,n)(2,n-1)\dots(\frac{n}{2},\frac{n+2}{2}) & \text{pro } n \text{ sudé,} \\ (1,n)(2,n-1)\dots(\frac{n-1}{2},\frac{n+3}{2})(\frac{n+1}{2}) & \text{pro } n \text{ liché.} \end{cases}$$

V prvním případě máme $\frac{n}{2}$ cyklů, v druhém $\frac{n-1}{2}$ cyklů. Celkově tedy dostáváme, že

$$\operatorname{sgn}(r) = (-1)^{n-\text{počet cyklů}} = \begin{cases} (-1)^{n-\frac{n}{2}} = (-1)^{\frac{n}{2}} & \text{pro } n \text{ sudé,} \\ (-1)^{n-\frac{n-1}{2}} = (-1)^{\frac{n-1}{2}} & \text{pro } n \text{ liché.} \end{cases}$$

Souhrnně můžeme též psát $\operatorname{sgn}(r) = (-1)^{\lfloor \frac{n}{2} \rfloor}$.

**Cv. 6.6** Najděte všechny permutace splňující $p \in S_{10}$ a $p^2 = (1,3)(2,4)(7,8,9,10)$.

***Řešení:***
Podívejme se nejprve, jak může vzniknout cyklus $(1,3)$. Aby se 1 zobrazilo na 3 v $p^2$, musí v $p$ být součástí nějaké cyklu $(\dots,1,a,3,\dots)$. Podobně aby se 3 zobrazilo na 1, musí být $(\dots,3,b,1,\dots)$. Spojením obou úseků dostáváme $(\dots,1,a,3,b,1,\dots)$, tedy nutně cyklus $(1,a,3,b)$. V permutaci $p^2$ se tento cyklus rozpadne na 2 podcykly $(1,3)(a,b)$. Ze struktury $p^2$ je jediná možnost, že $a = 2, b = 4$ nebo symetricky $a = 4, b = 2$.

Aby se dále prvky 5 a 6 zobrazily v $p^2$ sami na sebe, musí se buď oba zobrazit sami na sebe už v $p$, nebo tvořit cyklus o dvou prvcích $(5,c),(6,d)$. Pokud by libovolné z čísel byl součástí delšího cyklu, složením permutace sama se sebou bychom už nedostali $(5)$, resp. $(6)$. Ze struktury $p^2$ dále nutně vyplývá, že $c = 6$ a $d = 5$, jinak by $(d)$ a $(c)$ nebyly cykly z $p^2$.

Zbývá určit $p(7),\dots,p(10)$. Podobně jako v případě prvků 1, 3 odvodíme, že musí existovat úsek $(\dots,7,e,8,f,9,g,10,h,7,\dots)$, resp. cyklus $(7,e,8,f,9,q,10,h,7)$, který ale nejsme schopni pouze s pomocí prvků $7,\dots,10$ zkonstruovat. Z toho důvodu žádná permutace $p$ nesplňuje zadání.

*Poznámka.* Znaménko permutace $p^2$ je vždy sudé (pro libovolnou permutaci $p$), neboť platí $\operatorname{sgn}(p^2) = \operatorname{sgn}(p)\operatorname{sgn}(p) = \operatorname{sgn}(p)^2 = 1$. Ale zadaná permutace $(1,3)(2,4)(7,8,9,10)$ má znaménko $(-1)^{10-5} = -1$, tudíž nemůže být druhou mocninou žádné permutace.

**Cv. 6.7** Dokažte, že složením permutací dostaneme permutaci.

***Řešení:***
Abychom dokázali toto tvrzení, stačí ukázat, že složení dvou permutací $p, q \in S_n$ je *prosté* a *na*. Poté se bude jednat o bijekci na konečné množině, což odpovídá definici permutace. Toto půjde jednoduše dokázat z faktu, že obě permutace tyto vlastnosti splňují.

**Prosté**: Mějme $x, y \in \{1, \ldots, n\}$ a nechť platí

$$(p \circ q)(x) = p(q(x)) = p(q(y)) = (p \circ q)(y).$$

Protože zobrazení $p$ je prosté, platí, že nutně $q(x) = q(y)$. Nyní využijeme toho, že je prosté $q$ a tedy platí, že $x = y$. Tedy i zobrazení $(p \circ q)$ je prosté.

**Na**: Aby platila tato vlastnost, musí pro každé $x \in \{1, \ldots n\}$ existovat prvek $y \in \{1, \ldots, n\}$ takový, že $(p \circ q)(y) = p(q(y)) = x$. Protože zobrazení $p$ je „na“, tak existuje $z \in \{1, \ldots, n\}$ takové, že $p(z) = x$. Zároveň z vlastnosti na permutace $q$ existuje $y$, že $q(y) = z$. Toto $y$ splňuje tedy vztah $q(p(y)) = x$.

**Cv. 6.8** Najděte všechny symetrie obdélníku, popište je permutacemi a ověřte, že tvoří podgrupu grupy $(S_4, \circ)$.

***Řešení:***
Obdélník má čtyři symetrie:

- identita, která odpovídá permutaci $id = (1)(2)(3)(4)$,
- překlopení podle svislé osy odpovídá permutaci $(1, 2)(3, 4)$,
- překlopení podle vodorovné osy odpovídá permutaci $(1, 3)(2, 4)$,
- otočení o 180° odpovídá permutaci $(1, 4)(2, 3)$.

Snadno ověříme, že tato množina permutací je uzavřená na inverze a skládání, čili tvoří podgrupu.

**Cv. 6.9** Najděte všechny symetrie čtverce, popište je permutacemi a ověřte, že tvoří podgrupu grupy $(S_4, \circ)$.

***Řešení:***
Analogické předchozímu cvičení 6.8. Kromě tamějších symetrií zde máme navíc:

- překlopení podle diagonály, což odpovídá permutaci $(1, 4)(2)(3)$,
- překlopení podle šikmé diagonály, což odpovídá permutaci $(1)(4)(2, 3)$,
- otočení o 90° ve směru hodinových ručiček, což odpovídá $(1, 2, 4, 3)$,
- otočení o 90° proti směru hodinových ručiček, což odpovídá $(1, 3, 4, 2)$.

Opět ověříme, že tato množina osmi permutací je uzavřená na inverze a skládání, takže tvoří podgrupu.