1 Нека је $\mathbb{G}_1 = (G, \cdot, ^{-1}, e)$ група. Дефинишимо на G операцију $\circ$ са: $(\forall a, b \in G)\ a \circ b = b \cdot a$.
(а) Показати да је структура $\mathbb{G}_2 = (G, \circ, ^{-1}, e)$ група.
(б) Показати да је пресликавање $f : \mathbb{G}_1 \to \mathbb{G}_2$, дефинисано са $f(a) = a^{-1}$ изоморфизам група.

Решење: **(а)** Проверавамо аксиоме групе. Групоидност је лака, јер важи групоидност за $\mathbb{G}_1$, тј. $a \circ b = b \cdot a \in G$. Асоцијативност важи јер је $a \circ (b \circ c) = (b \circ c) \cdot a = (c \cdot b) \cdot a$. Даље, пошто у $\mathbb{G}_1$ важи асоцијативност имамо једнакост $(c \cdot b) \cdot a = c \cdot (b \cdot a) = (b \cdot a) \circ c = (a \circ b) \circ c$ што доказује асоцијативност у $\mathbb{G}_2$. Из $a \circ e = e \cdot a = a$ и $e \circ a = a \cdot e = a$ видимо да се неутрал наслеђује, а исто из $a \circ a^{-1} = a^{-1} \cdot a = e$ и $a^{-1} \circ a = a \cdot a^{-1} = e$ наслеђује се инверз. Дакле $\mathbb{G}_2$ јесте група.
(б) Треба проверити да је f бијекција и да је хомоморфизам. Да је "на" је лако, јер се у елемент a слика a^{-1}, јер $f(a^{-1}) = (a^{-1})^{-1} = a$. Да је "1-1" је такође лако, јер из $f(a) = f(b)$ следи $a^{-1} = b^{-1}$, па је $(a^{-1})^{-1} = (b^{-1})^{-1}$, тј. $a = b$. И коначно је хомоморфизам јер имамо $f(a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = a^{-1} \circ b^{-1} = f(a) \circ f(b)$. □

2 Нека су $g_1 = (12)(27)(35)(36)(47)$, $g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 6 & 5 & 1 & 3 & 4 \end{pmatrix} \in \mathbb{S}_7$.
(а) У групи $\mathbb{S}_7$ наћи једну пермутацију f реда 12. Одредити парност пермутације f.
(б) Ако постоје, одредити пермутације h_1, h_2, тако да је $f = h_1 g_1 h_1^{-1}$, односно $f = h_2 g_2 h_2^{-1}$.

Решење: Најпре запишимо g_1 и g_2 као производ дисјунктних циклуса: $g_1 = (1274)(365)$ и $g_2 = (12745)(36)$.
(а) Како је ред пермутације, која је записана као производ дисјунктних циклуса, једнак НЗС дузина тих циклуса, пермутација је реда 12 ако је производ циклуса дужине 3 и 4. Нпр. узмимо $f = (1234)(567)$. Како је f производ парног и непарног циклуса, то је непарна пермутација.
(б) Како је конјугат од f, hfh^{-1}, такође производ дисјунктних циклуса дужине 4 и 3, и ово запажање је ако и само ако, тражено h_1 постоји, док тражено h_2 не. За h_1 узимимо $h_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 4 & 7 & 6 & 3 \end{pmatrix}$. □

3 Одредити последње две цифре броја 2007^{2008}.

Ресење: Задатак лако можемо решити применом Ојлерове теореме, али можемо да приметимо да је $2007^{2008} =_{100} 7^{2008} =_{100} (7^4)^{502} =_{100} (2401)^{502} =_{100} 1^{502} = 1$. Дакле, две последње цифре су 01. □

4 Абелова група $\mathbb{G}$ је дата генераторима a, b, c и релацијама:

$$\begin{array}{rrrcl} 4a & -12b & -4c & = & 0, \\ 5a & -10b & -2c & = & 0, \\ 3a & -14b & -6c & = & 0. \end{array}$$

(а) Одредити нормалну форму групе $\mathbb{G}$.
(б) Колико група $\mathbb{G}$ има елемената коначног реда?

Решење: **(а)** Сводимо на нормалну форму:

$$\begin{pmatrix} 4 & -12 & -4 \\ 5 & -10 & -2 \\ 3 & -14 & -6 \end{pmatrix} \sim \begin{pmatrix} 4 & -12 & -4 \\ 1 & 2 & 2 \\ 3 & -14 & -6 \end{pmatrix} \sim \begin{pmatrix} 0 & -20 & -12 \\ 1 & 2 & 2 \\ 0 & -20 & -12 \end{pmatrix} \sim \begin{pmatrix} 0 & -20 & -12 \\ 1 & 0 & 0 \\ 0 & -20 & -12 \end{pmatrix} \sim \begin{pmatrix} 0 & -20 & -12 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim$$
$$\begin{pmatrix} 0 & -8 & -12 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & -8 & -4 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & -4 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$ Дакле, $\mathbb{G} = \mathbb{Z}_4 \times \mathbb{Z}$.

(б) Из нормалне форме је јасно да група $\mathbb{G}$ има четири елемента коначног реда. □

5 Дат је полином $f(x) = x^3 + 3x^2 + 2x + 3 \in \mathbb{Z}_5[x]$.
(а) Показати да је $f(x)$ несводљив над $\mathbb{Z}_5$.
(б) Нека је $\mathbb{E}$ скуп остатака полинома из $\mathbb{Z}_5[x]$ по модулу полинома $f(x)$. Показати да је $\mathbb{E}$ поље.
(в) У пољу $\mathbb{E}$ израчунати $\frac{x+4}{x^2+3x+2}$.

Решење: **(а)** Полином је трећег степена, па кад би био сводљив, имао би нулу у $\mathbb{Z}_5$. Како је $f(0) = 3$, $f(1) = 4$, $f(2) = 2$, $f(3) = 3$, $f(4) = 3$, то је $f(x)$ несводљива над $\mathbb{Z}_5$.
(б) Знамо да је $\mathbb{E}$ прстен, показујемо да сваки елемент из њега има инверз за множење. Нека је $g(x) \in \mathbb{E}$. Тада је $deg(g(x)) < deg(f(x)) = 3$, па како је $f(x)$ несводљив мора бити $(f(x), g(x)) = 1$. Одатле је $p(x)f(x) + q(x)g(x) = 1$, за неке $p(x), q(x) \in \mathbb{Z}[x]$. Нека је $\overline{q}(x)$ остатак од $q(x)$ при дељењу са $f(x)$, тј. $\overline{q}(x)$ припада $\mathbb{E}$. Уочену релацију сведимо по модулу $f(x)$: $1 =_{f(x)} p(x)f(x) + q(x)g(x) =_{f(x)} \overline{q}(x)g(x)$, тј. у $\mathbb{E}$ важи $\overline{q}(x)g(x) = 1$, па је $\overline{q}(x)$ иверз за $g(x)$ у $\mathbb{E}$. Дакле, $\mathbb{E}$ је поље.
(в) Нека је $h(x) = x^2 + 3x + 2$. Како је $f(x) = h(x)x + 3$, имамо у $\mathbb{E}$ да је $\frac{x+4}{x^2+3x+2} = \frac{x+4}{h(x)} = \frac{(x+4)x}{h(x)x} = \frac{x^2+4x}{f(x)+2} = \frac{3(x^2+4x)}{3 \cdot 2} = 3x^2 + 2x$. □

6 (Теоријско питање)
(а) Подгрупе цикличних група.
(б) Навести и доказати $n!$ теорему.