ДОМАШНЯ РОБОТА №5
З ПРЕДМЕТУ
"МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ"

ФІ-12 Бекешева Анастасія

1. Спочатку покажемо що $(A, \cdot)$ - група.

   (a) асоціативність. Множення матриць асоціативне за означенням.

   (b) нейтральний елемент. У множині A є нейтральний елемент: $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

   (c) обернений елмент. $a_1 \cdot a_1 = e, \quad a_2 \cdot a_2 = e, \quad a_3 \cdot a_4 = e, \quad a_4 \cdot a_3 = e, \quad a_5 \cdot a_5 = e.$

   Отже $(A, \cdot)$ є групою. Побудуємо таблицю Келі для A. Також візьмемо $\mod 2$ від кожного множення, шоб у відповіді отримати елементи з множини A. Тобто $a_1 \cdot a_3$ рахуватиметься так: $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \mod 2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = a_2$.
   Отже таблиця Келі:

$\cdot$	e	a_1	a_2	a_3	a_4	a_5
e	e	a_1	a_2	a_3	a_4	a_5
a_1	a_1	e	a_3	a_2	a_5	a_4
a_2	a_2	a_4	e	a_5	a_1	a_3
a_3	a_3	a_5	a_1	a_4	e	a_2
a_4	a_4	a_2	a_5	e	a_3	a_1
a_5	a_5	a_3	a_4	a_1	a_2	e

   Згадаємо таблицю Келі для σ_3 :

$\cdot$	e	π_1	π_2	π_3	π_4	π_5
e	e	π_1	π_2	π_3	π_4	π_5
π_1	π_1	e	π_3	π_2	π_5	π_4
π_2	π_2	π_4	e	π_5	π_1	π_3
π_3	π_3	π_5	π_1	π_4	e	π_2
π_4	π_4	π_2	π_5	e	π_3	π_1
π_5	π_5	π_3	π_4	π_1	π_2	e

   З даних таблиць Келі легко бачити, що $A \cong \sigma_3$

2. (a) Доведемо що $f(e_H) = e_G$. Скористаємося тим, що $e_H \cdot e_H = e_H$:

   $$f(e_H) = f(e_H \cdot e_H) = f(e_H) \times f(e_H)$$

   Тепер домножимо на оберенене до $f(e_H)$:

   $$f(e_H) \times f^{-1}(e_H) = (f(e_H) \times f(e_H)) \times f^{-1}(e_H)$$

   Так як $\times$ - асоціативна, можемо сказати, що

   $$f(e_H) = e_G$$

   (b) Доведемо що $f(a^{-1}) = f(a)^{-1}$. Вже знаємо, що $e_G = f(e_h)$. Отже

   $$e_G = f(e_h) = f(a \cdot a^{-1})$$

   За означенням гомомрфізму

   $$e_G = f(e_h) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1})$$

   Перепишемо і отримаємо:

   $$f(a)^{-1} = f(a)^{-1} \times e_H = f(a)^{-1} \times f(a) \times f(a^{-1}) = e_H \times f(a^{-1}) = f(a^{-1})$$

3. Порахуємо порядки елементів $\langle a \rangle$: $\operatorname{ord}(a^1) = \operatorname{ord}(a^5) = \operatorname{ord}(a^7) = \operatorname{ord}(a^{11}) = 12$, $\operatorname{ord}(a^2) = \operatorname{ord}(a^{10}) = 6$, $\operatorname{ord}(a^3) = \operatorname{ord}(a^9) = 4$, $\operatorname{ord}(a^4) = \operatorname{ord}(a^8) = 3$, $\operatorname{ord}(a^6) = 2$, $\operatorname{ord}(a^{12} = e) = 1$.

   Запишемо підгрупи: порядок 1: $H_1 = \{e\}$, порядок 12: $H_{12} = \langle a \rangle$, порядок 6: $H_6 = \{e, a^2, a^4, a^6, a^8, a^{10}\}$, порядок 4: $H_4 = \{e, a^3, a^6, a^9\}$, порядок 3: $H_3 = \{e, a^4, a^8\}$, порядок 2: $H_2 = \{e, a^6\}$.

(H_1.) $aH_1 = \{a\}, \quad a^2H_1 = \{a^2\}, \quad \cdots, \quad a^{11}H_1 = \{a^{11}\}$
$\langle a \rangle = H_1 \cup aH_1 \cup \cdots \cup a^{11}H_1, \quad \langle a \rangle / H_1 \cong (Z_{12}, \oplus)$

(H_2.) $aH_2 = \{a^1, a^7\}, \quad a^2H_2 = \{a^2, a^8\}, \quad a^3H_2 = \{a^3, a^9\}, \quad a^4H_2 = \{a^4, a^{10}\}, \quad a^5H_2 = \{a^5, a^{11}\}, \quad \langle a \rangle = H_2 \cup aH_2 \cup a^2H_2 \cup a^3H_2 \cup a^4H_2 \cup a^5H_2, \quad \langle a \rangle / H_2 \cong (\mathbb{Z}_6, \oplus)$

(H_3.) $aH_3 = \{a, a^5, a^9\}, \quad a^2H_3 = \{a^2, a^6, a^{10}\}, \quad a^3H_3 = \{a^3, a^7, a^{11}\},$
$\langle a \rangle = H_4 \cup aH_3 \cup a^2H_3 \cup a^3H_3, \quad \langle a \rangle / H_3 \cong (\mathbb{Z}_4, \oplus)$

(H_4.) $aH_4 = \{a, a^4, a^7, a^{10}\}, \quad a^2H_4 = \{a^2, a^5, a^8, a^{11}\},$
$\langle a \rangle = H_4 \cup aH_4 \cup a^2H_4, \quad \langle a \rangle / H_4 \cong (\mathbb{Z}_3, \oplus)$

(H_6.) $aH_6 = \{a, a^3, a^5, a^7, a^9, a^{11}\}$
$\langle a \rangle = H_6 \cup aH_6, \quad \langle a \rangle / H_6 \cong (\mathbb{Z}_2, \oplus)$

(H_{12}.) $\langle a \rangle = H_{12}, \quad \langle a \rangle / H_{12} \cong (\mathbb{Z}_0, \oplus)$