ДОМАШНЯ РОБОТА №4
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

1. Таблиця 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

2. Порядки елементів σ_3 :
   $\pi_0 = e \Longrightarrow \text{ ord } (\pi_0) = 1, \quad \pi_1 \cdot \pi_1 = e \Longrightarrow \text{ ord } (\pi_1) = 2$
   $\pi_2 \cdot \pi_2 = e \Longrightarrow \text{ ord } (\pi_2) = 2, \quad \pi_3 \cdot \pi_3 = \pi_4, \pi_4 \cdot \pi_3 = e \Longrightarrow \pi_3^3 = e \Longrightarrow$
   $\text{ ord } (\pi_3) = 3, \quad \pi_4 \cdot \pi_4 = \pi_3, \pi_3 \cdot \pi_4 = e \Longrightarrow \text{ ord } (\pi_4) = 3,$
   $\pi 5 \cdot \pi_5 = e \Longrightarrow \text{ ord } (\pi_5) = 2$

3. Знайти усі підгрупи σ_3 :
   Дві тривіальні підрупи це $\{e\}$ і σ_3. Підгрупи порядку 2: $\{e, \pi_1\}, \{e, \pi_2\}, \{e, \pi_5\}$. Підгрупа порядку 3: $\{e, \pi_3, \pi_4\}$.

4. $\langle a \rangle_{18}$:
   $\text{ ord } (a^1) = \text{ ord } (a^5) = \text{ ord } (a^7) = \text{ ord } (a^{11}) = \text{ ord } (a^{13}) = \text{ ord } (a^{17}) = \dfrac{18}{1} = 18,$
   $\text{ ord } (a^2) = \text{ ord } (a^4) = \text{ ord } (a^8) = \text{ ord } (a^{10}) = \text{ ord } (a^{14}) = \text{ ord } (a^{16}) = \dfrac{18}{2} = 9$
   $\text{ ord } (a^3) = \text{ ord } (a^{15}) = \dfrac{18}{3} = 6, \quad \text{ ord } (a^6) = \text{ ord } (a^{12}) = \dfrac{18}{6} = 3,$
   $\text{ ord } (a^9) = \dfrac{18}{9} = 2, \quad \text{ ord } (a^{18}) = \dfrac{18}{18} = 1$
   Підгрупи: тривіальні $\{e = a_{18}\}, \langle a \rangle_{18}$, порядок 18: $\{a^1, a^5, a^7, a^{11}, a^{13}, a^{17}\}$, порядок 9: $\{e, a_2, a_4, a_8, a_{10}, a_{14}, a_{16}\}$, порядок 6: $\{e, a_3, a_{15}\}$, порядок 3: $\{e, a_6, a_{12}\}$, порядок 2: $\{e, a_9\}$.
   $\phi(18) = 6$, отже кількість твірних елементів 6 і їх порядок 18,
   $\varphi(9) = 6$, у підгрупі порядку 9 - 6 твірних елементів, $\varphi(6) = 2$, у підгрупі порядку 6 - 2 твірних елементів, $\varphi(3) = 2$, у підгрупі порядку 3 - 2 твірних елементів, $\varphi(2) = 1$, у підгрупі порядку 2 - 1 твірний елементів.

5.

[реф.] Нехай $a \in H \Longrightarrow aa^{-1} = e \in H$, бо H підгрупа H. Тоді $a \equiv a \mod H \quad \forall a \in G$. Відношення рефлексивне.

[сим.] $a, b \in G : \quad a \equiv b \mod H \Longrightarrow ab^{-1} \in H \Longrightarrow (ab^{-1})^{-1} \in H \Longrightarrow ba^{-1} \in H \Longrightarrow b \equiv a \mod H$. Відношення симетричне.

[транз.] $\forall a, b, c \in G : \quad a \equiv b \mod H, b \equiv c \mod H \Longrightarrow ab^{-1} \in H, bc^{-1} \in H \Longrightarrow (ab^{-1})^{-1}(bc^{-1})^{-1} \in H \Longrightarrow ac^{-1} \in H \Longrightarrow a \equiv c \mod H$. Відношення транзитивне.