Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования   
**Национальный исследовательский университет «МЭИ»**

**Лабораторная работа №8**

по курсу«**Методы и средства защиты информации**»

**«Введение в теорию групп»**

Выполнил:

студент группы А-07-18

Востриков Р.В.

Вариант 8

Москва  
2020

**1. Задание**

**Задание 1**  
Выяснить, образует ли группу следующее множество при указанной операции над элементами:  
Вариант 8: матрицы порядка n с целыми элементами и определителем, равным ±1 относительно умножения

**Задание 2**  
Найти в группе S3  
Вариант 3  
А)

Б) Две подгруппы порядка 2

**Задание 3**  
В группе S3 найти  
А) левые и правые смежные классы по любой подгруппе порядка 2  
Б) левые и правые смежные классы по любой подгруппе порядка 3  
Найти подгруппы порядка 2 и 3 в S3

**Задание 4**  
Составить программу, которая для любой подстановки порядка n определяет она четная или нечётная.

**2. Описание результатов**

Задание 1

Множество образует группу, если выполняются следующие условия:  
1) Ассоциативность  
2) Наличие нейтрального элемента  
3) Наличие обратного элемента

Проверим на выполнение условия ассоциативности:

По свойству определителя произведения:

Условие выполняется.

Проверим на выполнение условие наличия нейтрального элемента:

Можно показать, что нейтральным элементом является единичная матрица порядка n:

Определитель произведения .

Проверим на выполнение условие наличия обратного элемента:

Так как , то для любой матрицы *a* с определителем, равным ±1 будет существовать обратная, с определителем, равным ±1

Так как все условия выполняются, то множество образует группу.

Задание 2

А) По определению:   
  
 Отсюда видно, что

Б) Запишем определение подгруппы:  
 1) если a, b ∈ H, то ab ∈ H;  
 2) если a ∈ H, то a−1 ∈ H;  
 3) e ∈ H.

Найдем первую подгруппу.

Положим,   
 Проверим выполнение условий из определения:  
 1)

2) 3)   
 Все условия выполняются, следовательно, H является подгруппой порядка 2 группы S3.

Найдем вторую подгруппу.

Положим,   
 Проверим выполнение условий из определения:  
 1)

2) 3)   
 Все условия выполняются, следовательно, H является подгруппой порядка 2 группы S3.

Получившиеся подгруппы:

Задание 3

Для начала рассмотрим группу S3 и найдём все её подгруппы порядка 2 и 3.

Подгруппы порядка 2:

Подгруппы порядка 3:

А) Найдём левый и правый смежные классы по подгруппе H1.  
 В качестве порождающего элемента возьмём x = a4:

Левый смежный класс группы S3 по подгруппе H1:

Правый смежный класс группы S3 по подгруппе H1:

Б) Найдём левый и правый смежные классы по подгруппе H4:  
 В качестве порождающего элемента также возьмём x = a4:

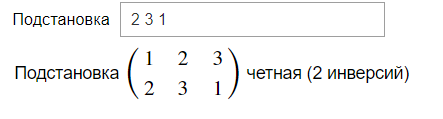
Левый смежный класс группы S3 по подгруппе H4:

Правый смежный класс группы S3 по подгруппе H4:

Задание 4

Была написана программа, принимающая на вход подстановку порядка n в виде строки из чисел, разделенных пробелами. Далее программа вычисляет количество инверсий в подстановке, на основе количества инверсий выводится сообщение о четности подстановки (и количество инверсий для наглядности).

Интерфейс програмы:



**3. Код программы (к заданию 4)**

# определение количества инверсий в подстановке  
def inversions(s):  
 count = 0  
 for i in range(len(s)):  
 for j in range(i + 1, len(s)):  
 if (s[i] > s[j]):  
 count += 1  
 return count

import ipywidgets as widgets  
from ipywidgets import interact  
from IPython.display import Latex

@interact(Подстановка = "2 1 3")  
def is\_even(Подстановка):   
 sub = parse(Подстановка)  
 inv = inversions(sub)  
 res = 'четная' if inv % 2 == 0 else 'нечетная'  
 out = rf'Подстановка {print\_sub(sub)} {res} ({inv} инверсий)'  
 return Latex(out)

**Вывод**

В данной лабораторной работе на примере группы подстановок были разобраны базовые понятия теории групп, такие как группы, подгруппы, левые и правые смежные классыТакже был составлен алгоритм определения чётности подстановки.