МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«МИРЭА – Российский технологический университет»**
**РТУ МИРЭА**

---

Институт кибернетики
Базовая кафедра №252 – информационной безопасности

---

# КУРСОВАЯ РАБОТА

По дисциплине «Группы подстановок»

**Тема курсовой работы:** «Порядки классов сопряжённых элементов в конечных группах подстановок»(вариант№14)

| | | |
|---|---|---|
| Студент группы ККСО-03-19 | Николенко В.О. | _____ *(подпись)* |
| Руководитель курсовой работы | к.ф.-м.н., проф. Зязин В.П. | _____ *(подпись)* |
| Консультант | асс. Плешаков А.С. | _____ *(подпись)* |

Работа представлена к защите «__» _____ 2020 г.

Допущен к защите «__» _____ 2020 г.

Москва – 2020

# СОДЕРЖАНИЕ

# 1. ВВЕДЕНИЕ

В мире на данный момент самый важный ресурс это информация. Не даром Натан Ротшильд сказал:"Кто владеет информацией — тот владеет миром". Еще в древние времена, при Юлии Цезаре был придуман один из старейших шифров - "Шифр Цезаря". Хоть он был весьма примитивен, но сумел дать толчок сфере защиты информации, ведь даже, если гонца с важным донесением перехватили, но не сумели прочитать, что написано в послании, то планы великих полководцев и не только не будут подвержены риску быть нарушенными людьми со злыми намерениями. Так постепенно и появился предмет "алгебра". Как писал в своей книге М.М. Глухов,"термин "алгебра" происходит от названия сочинения узбексого математика 9 века Муххамеда ал-Хорезми "Альджебр аль-Мукабала", в котором были систематизированны сведения о правилах действий с числами и общих приёмах решения задач, сводящихся к решению уравнений 1-й и 2-й степеней". Сегодня же "алгебра" - это предмет, без которого невозможно работать в сфере защиты информации. Алгебра даёт понять, какие операции можно производить над числами/цифрами и что в итоге у нас получается.

# 2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

## 2.1. Основы теории групп

**Задание №9(л)**

Найти порядок элемента $g$ в группе $G$.

Решение:

$$G = C^*_{n\times n} g = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

, где $\lambda_1, \lambda_2, \cdots, \lambda_n \in \Gamma_n$

Рассмотрим какую-либо конечную группу $\Gamma_2$, $\{e^{i\Pi}; 1\} \in \Gamma_2$.

Тогда составим матрицу:

$$G = \begin{pmatrix} e^{i\Pi} & 0 \\ 0 & 1 \end{pmatrix}$$

По определению 1, порядком элемента $g$ группы $G$ называется наименьшее из чисел $n \in N$, при котором $g^n = e$, если такие n существуют, и бесконечность - в противном случае.

Результатом перемножения двух матриц является матрица:

$$\begin{pmatrix} e^{i\Pi} & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} e^{i\Pi} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} e^{2i\Pi} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow$ порядок группы $\Gamma_2$ равен 2.

Рассмотрим ещё одну произвольную конечную группу $\Gamma_3$, $\{e^{i\frac{2\Pi}{3}}, e^{i\frac{4\Pi}{3}}, 1\}$.

$$\begin{pmatrix} e^{i\frac{2\Pi}{3}} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{i\frac{4\Pi}{3}} \end{pmatrix}$$

Результатом перемножения уже трёх матриц является матрица:

$$\begin{pmatrix} e^{i\frac{2\Pi}{3}} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{i\frac{4\Pi}{3}} \end{pmatrix} \cdot \begin{pmatrix} e^{i\frac{2\Pi}{3}} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{i\frac{4\Pi}{3}} \end{pmatrix} \cdot \begin{pmatrix} e^{i\frac{2\Pi}{3}} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{i\frac{4\Pi}{3}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Если группа будет увеличиваться, то будет расти и её порядок $\Rightarrow$ можем сказать, что порядок группы $\Gamma_n$ равен $n$.

**Задание №10(д)**

Решение: Рассмотрим мультипликативную группу классов вычетов $\mathbb{Z}_{16}^*$
$\mathbb{Z}_{16}$ ={1,2,3,4,5,...,15};
$\mathbb{Z}_{16}^*$ ={1,3,5,7,9,11,13,15};
Составим таблицу Кэли:

| * | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
| 3 | 3 | 9 | 15 | 5 | 11 | 1 | 7 | 13 |
| 5 | 5 | 15 | 9 | 3 | 13 | 7 | 1 | 11 |
| 7 | 7 | 5 | 3 | 1 | 15 | 13 | 11 | 9 |
| 9 | 9 | 11 | 13 | 15 | 1 | 3 | 5 | 7 |
| 11 | 11 | 1 | 7 | 13 | 3 | 9 | 15 | 5 |
| 13 | 13 | 7 | 1 | 11 | 5 | 15 | 9 | 3 |
| 15 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

Тогда найдём порядки для всех элементов:
$ord(1) = 1$
$ord(3) = 4$
$ord(5) = 4$
$ord(7) = 2$
$ord(9) = 2$
$ord(11) = 4$
$ord(13) = 4$
$ord(15) = 2$
$exp(\mathbb{Z}_{16}^*) = [1, 4, 4, 2, 2, 4, 4, 2] = 4$

**Задание №10(и)**

Решение: Рассмотрим все случаи цикловых структур в группе $S_n$:
$(\cdot)(\cdot)(\cdot)(\cdot)(\cdot) \Rightarrow ordS_5 = 1$
$(\cdot\ \cdot)(\cdot)(\cdot)(\cdot) \Rightarrow ordS_5 = 2$
$(\cdot\ \cdot\ \cdot)(\cdot)(\cdot) \Rightarrow ordS_5 = 3$
$(\cdot\ \cdot)(\cdot\ \cdot\ \cdot) \Rightarrow ordS_5 = 6$
$(\cdot\ \cdot\ \cdot\ \cdot)(\cdot) \Rightarrow ordS_5 = 4$
$(\cdot\ \cdot\ \cdot\ \cdot\ \cdot) \Rightarrow ordS_5 = 5$
$exp(S_n) = n! = 720$

**Задание №38**

$\supset H_1, H_2$ - подгруппы в группе $G$, причём $H_1 \in H_2$. Доказать, что если $|H_2 : H_1| = n$ и $|G : H_2| = m$, то $|G : H_1| = mn$.

Доказательство:

$\supset$ для конечной группы справедливо:

По т. Лагранжа для конечных групп, а также её подгрупп:

$|H_2 : H_1| = \frac{|H_2|}{|H_1|}$

$|G| = m|H_2|, |H_1| = \frac{H_2}{n} \Rightarrow \frac{G}{H_1} = \frac{m|H_2|n}{|H_2|} = mn.$

В то же время рассмотрим бесконечные группы, которые мы можем разбить на бесконечное число конечный а также идентичных подмножеств, для которых справедливо:

Если для $m$ элементов из $G$ $\exists$ 1 элемент $H_2$, то и для $km$ элементов $G$ $\exists$ $k$ элементов из $H_2$.

## 2.2. Строение групп

### Задание №8

$\sqsupset G$ - произвольная группа. Доказать, что равенство
$|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$
справедливо для всех конечных подгрупп $H, K < G$.

Доказательство:

В силу того, что $\forall x \in K : xK = K$:
$\forall x \in (H \cap K), h \in H : h = const \Leftrightarrow (hx)K = const = hK \Rightarrow$
$\Rightarrow \{hK | h \in H\} \cong H/(H \cap K)| \Rightarrow$
$\Rightarrow \left|\{hK | h \in H\}\right| = \left|H/(H \cap K)\right|$
Рассмотрим элементы множества левых классов:
$\forall h \in H : |hK| = const = K \Rightarrow$
$\Rightarrow$ Основываясь на т. Лагранжа можно сказать, что:
$|HK| = |K| \cdot \left|H/(H \cap K)\right| = \frac{|H|\cdot|K|}{|H\cap K|}$, ч.т.д.

### Задание №21

Доказать, что силовская $p-$подгруппа группы $G$ единственная т. и т. т., когда она нормальна с $G$.

Доказательство:

$\sqsupset$ порядок группы $G$ имеет вид: $|G| = p^n s$,где $(p, s) = 1$.

Опираясь на 1 т. Силова можно сказать, что в группе $G$ $\exists$ подгруппа порядка $p^n$ и по условию она единственна. Поскольку по 2 т. Силова все силовские $p-$подгруппы сопряжены, то верно следующее:

$g^{-1}H_p g = H_p$.

$\Rightarrow$ выполняется определение нормальной подгруппы.

Обратно:

$\sqsupset \exists$ 2 силовские $p-$подгруппы $H_{p_1}$ и $H_{p_2}$, такие, что $H_{p_1}$,$H_{p_2} \in G$. По определению нормальной подгруппы и 2 теоремы Силова будет справедливо следующее:

$$\begin{cases} g^{-1}H_{p_1}g = H_{p_1} \\ g^{-1}H_{p_2}g = H_{p_2} \Rightarrow H_{p_1} = H_{p_2} \Rightarrow H-\text{единственная}. \\ g^{-1}H_{p_1}g = H_{p_2} \end{cases}$$

### Задание №24(e)

Доказать, что любая группа порядка $n \in \mathbb{N}$ коммутативна.

Доказательство: Нам дано число 187, его можно разложить на произведение 11 и 17, тогда найдём количество силовских 11-подгрупп и 17-подгрупп.

$s_{11}|187 \cup s_{11} \equiv 1(mod 11) \Rightarrow s_{11} = 1$

$s_{17}|187 \cup s_{17} \equiv 1(mod 17) \Rightarrow s_{17} = 1$

Силовские подгруппы $H_{11}$ и $H_{17}$ - циклические и имеют тривиальное пересечение из чего можно сделать вывод, что $G = H_{11} \dot{+} H_{17} \cong \mathbb{Z}_{11} \oplus \mathbb{Z}_{17}$. $\Rightarrow$ группа порядка 187 абелева.

## 2.3. Конечные группы подстановок

### Задание №9

Определить, сколько инверсий образует число $n$, стоящее в нижней строке подстановки степени $n$ на $k-$ом месте.

Решение: Рассмотрим каноническую запись подстановки степени 5 и ⊐ k=4:

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

видим, что наше число 5 образует ровно одну инверсию в подстановке 5 степени, тогда (n-k) - формула по которой мы вычисляем число инверсий которые образует число n, расположенное на $k-$ом месте в подстановке степени $n$.

### Задание №10

Показать, что от одной перестановки $(a_1, ..., a_n)$ к другой перестанов- ке $(b_1, ..., b_n)$ тех же элементов можно перейти путём не более чем $n-1$ транспозиций.

Решение: Возьмём группу $S_3$, рассмотрим все её подстановки и найдём число транспозиций благодаря которым мы сможем перейти от одной подстановки к другой:

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Из подстановки (1) мы можем перейти в подстановку (2) при помощи транспозиций (3 2) и (2 1).

Из подстановки (1) мы можем перейти в подстановку (3) при помощи транспозиций (3 1) и (1 2).

Из подстановки (1) мы можем перейти в подстановку (4) при помощи транспозиций (3 2).

Из подстановки (1) мы можем перейти в подстановку (5) при помощи транспозиций (3 1).

Из подстановки (1) мы можем перейти в подстановку (6) при помощи транспозиций (3 2).

Из подстановки (2) мы можем перейти в подстановку (3) при помощи транспозиций (3 2), (1 3).

Из подстановки (2) мы можем перейти в подстановку (4) при помощи транспозиций (2 1).

Из подстановки (2) мы можем перейти в подстановку (5) при помощи транспозиций (3 2).

Из подстановки (2) мы можем перейти в подстановку (6) при помощи транспозиций (3 1).

Из подстановки (3) мы можем перейти в подстановку (4) при помощи транспозиций (3 1).

Из подстановки (3) мы можем перейти в подстановку (5) при помощи транспозиций (1 2).

Из подстановки (3) мы можем перейти в подстановку (6) при помощи транспозиций (3 2).

Из подстановки (4) мы можем перейти в подстановку (5) при помощи транспозиций (3 1) и (1 2).

Из подстановки (4) мы можем перейти в подстановку (6) при помощи транспозиций (3 2) и (1 3).

Из подстановки (5) мы можем перейти в подстановку (6) при помощи транспозиций (3 2) и (3 1).

Видим, что максимально возможное число транспозиций $n-1$ т.е. 2 в нашем случае.Раз это свойство верно для $S_3$, то верно и для $S_n$.

### Задание №16(г)

Пусть $A \subset S_n$ - некоторое множество транспозиций степени $n \in N$. По свойствам графа $\Gamma_A$ описать структуру группы $G = < A >$ и определить, является ли множество A системой образующих или базисом группы $S_n$.

Решение: $A$={(1 9),(2 6),(3 5),(4 8),(5 6),(6 9),(7 9),(8 10),(10 2)}

Видим, что из каждой точки можно перейти в другую притом только одним способом $\Rightarrow$ наша группа является базисом.

### Задание №16(ж)

Пусть $A \subset S_n$ - некоторое множество транспозиций степени $n \in N$. По свойствам графа $\Gamma_A$ описать структуру группы $G = < A >$ и определить, является ли множество A системой образующих или базисом группы $S_n$.

Решение: $A$=$\{(1\,5)$,$(2\,6)$,$(3\,7)$,$(3\,8)$,$(4\,9)$,$(4\,10)$,$(7\,8)$,$(10\,9)\}$

Видим, что мы не можем из любой точки перейти любую в другую $\Rightarrow$ наша группа является системой образующих.

### Задание №21(в)

Найти централизатор подстановки $g \in S_6$.

Решение: Найдём количество всех решений, которые входят в наш нормализатор:

| № | 1 | 3 | 2 | 5 | 3 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 4 | 6 | 2 |
| 2 | 1 | 3 | 4 | 6 | 2 | 5 |
| 3 | 1 | 3 | 6 | 2 | 5 | 4 |
| 4 | 1 | 3 | 2 | 5 | 4 | 6 |
| 5 | 3 | 1 | 5 | 4 | 6 | 2 |
| 6 | 3 | 1 | 4 | 6 | 2 | 5 |
| 7 | 3 | 1 | 6 | 2 | 5 | 4 |
| 8 | 3 | 1 | 2 | 5 | 4 | 6 |

Переведём все наши подстановки в цикловую структуру и запишем их в множество нормализатора:

$G = \{\varepsilon, (2\,5\,4\,6), (4\,2)(6\,5), (2\,6\,4\,5), (1\,3)(2\,5\,4\,6), (1\,3)(4\,2)(6\,5), (1\,3)(2\,6\,4\,5),$
$(1\,3), (2\,5\,4\,6), (4\,2)(6\,5), (2\,6\,4\,5), (1\,3)(2\,5\,4\,6), (1\,3)(4\,2)(6\,5), (1\,3)(2\,6\,4\,5),$
$(1\,3)\}$

### Задание №39(а)

Определить, является ли группа $G < S_n$ транзитивной. Решение: Рассмотрим группу $G =< (1\,2\,3)(4\,5\,6), (1\,3\,4\,6) >$

Найдём орбиты элементов:

$G(1) = (1\,2\,3);$
$G(2) = (2\,3);$

$$\left.\begin{array}{l} G(3) = (3\,1\,4); \\ G(4) = (4\,5\,6); \\ G(5) = (5\,6); \\ G(6) = (6\,4\,1); \end{array}\right| \Rightarrow \text{т.к. орбиты не совпадают, то } G \text{ не транзитивна;}$$

# 3. ИНДИВИДУАЛЬНАЯ ЧАСТЬ

**Задание 1.** Пусть перестановки элементов множества $\overline{1,n}$ задают нижние строки канонических записей подстановок $g, h \in \mathbf{S}_n$.

а) Записать подстановки $g$ и $h$ в каноническом виде. Выписать элементы множеств $\operatorname{Mob} g$ и $\operatorname{Mob} h$, $\operatorname{Fix} g$ и $\operatorname{Fix} h$.

б) Найти подстановки $gh$, $hg$, $g^{-1}$, $h^{-1}$.

в) Разложить подстановки $g$ и $h$ на независимые циклы, указать их цикловые структуры и найти $\operatorname{ord} g$ и $\operatorname{ord} h$.

г) Разложить подстановки $g$ и $h$ в произведение транспозиций и определить их чётность.

Решение: Начнём с пункта А

Выпишем подстановки g и h в каноническом виде:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 13 & 6 & 4 & 16 & 7 & 3 & 10 & 2 & 9 & 11 & 17 & 19 & 5 & 12 & 15 & 14 & 18 & 1 & 8 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 16 & 13 & 18 & 14 & 11 & 7 & 10 & 19 & 1 & 9 & 2 & 17 & 12 & 15 & 6 & 5 & 3 & 8 & 4 \end{pmatrix}$$

Для перестановок справедливы утверждения:
Mob g={1,2,3,4,5,6,7,8,10,11,12,13,14,16,17,18,19}
Fix g={9,15}
Mob h={1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19}
Fix h=∅

Перейдём к пункту Б

$$g{\cdot}h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 12 & 2 & 14 & 5 & 10 & 18 & 9 & 13 & 1 & 2 & 3 & 4 & 11 & 17 & 6 & 15 & 8 & 16 & 19 \end{pmatrix}$$

$$h{\cdot}g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 14 & 5 & 1 & 12 & 17 & 10 & 11 & 8 & 13 & 9 & 6 & 18 & 19 & 15 & 3 & 7 & 4 & 2 & 16 \end{pmatrix}$$

$$g^{-1} = \begin{pmatrix} 13 & 6 & 4 & 16 & 7 & 3 & 10 & 2 & 9 & 11 & 17 & 19 & 5 & 12 & 15 & 14 & 18 & 1 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \end{pmatrix}$$

$$h^{-1} = \begin{pmatrix} 16 & 13 & 18 & 14 & 11 & 7 & 10 & 19 & 1 & 9 & 2 & 17 & 12 & 15 & 6 & 5 & 3 & 8 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \end{pmatrix}$$

Перейдём к пункту В

$g = (1\,13\,5\,7\,10\,11\,17\,18)(2\,6\,3\,4\,16\,14\,12\,19\,8)$

$h = (1\,16\,5\,11\,2\,13\,12\,17\,3\,18\,8\,19\,4\,14\,15\,6\,7\,10\,9)$

$[g] = [8^1, 9^1, 1^2] \Rightarrow$ ord g=72

$[h] = [19^1] \Rightarrow$ ord h=19

Перейдём к пункту Г

Разложим наши подстановки на произведение транспозиций:

g=(1 18)(13 18)(5 18)(7 18)(10 18)(11 18)(17 18)(2 8)(6 8)(3 8)(4 18)(16 8)(14 8)(12

Видим, что у нас нечётное количество транспозиций $\Rightarrow$ перестановка g нечётная

h=(1 9)(16 9)(5 9)(11 9)(2 9)(13 9)(12 9)(17 9)(3 9)(18 9)(19 9)(4 9)(14 9)(15 9)(6 9)

Видим, что у нас чётное количество транспозиций $\Rightarrow$ перестановка h чётная

**Задание 2.** Пусть перестановки элементов множества $\overline{1,n}$ задают нижние строки канонических записей подстановок $g, h \in \mathbf{S}_n$.

а) Доказать, что подстановки $g$ и $h$ сопряжены в $S_n$.

б) Определить число решений уравнений $x^{-1}gx = h$ и $y^{-1}hy = g$.

в) Составить таблицы, описывающие множества всех решений каждого из уравнений.

г) Выписать по два произвольных решения каждого из уравнений и осуществить их проверку.

Решение: Начнём с пункта А

Выпишем нижние строки подстановок g и h:

g=(1,2,6,3,9,4,5,7,8)

h=(6,2,8,4,9,5,3,7,1)

Разложим подстановки g и h на цикловые структуры:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 6 & 3 & 9 & 4 & 5 & 7 & 8 \end{pmatrix} = (7,5,9,8)(3,6,4)$$

Где $[g] = [4^1, 3^1, 1^2]$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 8 & 4 & 1 & 9 & 3 & 7 & 5 \end{pmatrix} = (1,6,9,5)(3,8,7)$$

Где $[h] = [4^1, 3^1, 1^2]$

Перейдём к пункту Б

Число решений для уравнений $x^{-1}gx = h$ и $y^{-1}hy = g$ одинаково так как в g и h одинаковые цикловые структуры.

Поскольку цикловые структуры подстановок g и h совпадают, то согласно следствию теоремы о порядке нормализатора, множество всех решений заданного уравнения есть правый смежный класс $N_{S_n}(g) \cdot f$, где f - произвольное решение. Тогда справедлива формула: $|N_{S_n}(g)| = \prod_{i=1}^{r}(k_i)! \cdot l_i^{k^i}$, где $k_i$ - число циклов заданной длины $l_i$.

$\Rightarrow$ число решений равно $(1! \cdot 4^1) \cdot (1! \cdot 3^1) \cdot (2! \cdot 1^2) = 24$

Перейдём к пункту В

Составим таблицу для уравнения $x^{-1}gx = h$ со всеми его решениями:

| № | 7 | 5 | 9 | 8 | 3 | 6 | 4 | 1 | 2 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 6 | 5 | 9 | 3 | 8 | 7 | 4 | 2 |
| 2 | 1 | 6 | 5 | 9 | 8 | 7 | 3 | 4 | 2 |
| 3 | 1 | 6 | 5 | 9 | 7 | 3 | 8 | 4 | 2 |
| 4 | 6 | 5 | 9 | 1 | 3 | 8 | 7 | 4 | 2 |
| 5 | 6 | 5 | 9 | 1 | 8 | 7 | 3 | 4 | 2 |
| 6 | 6 | 5 | 9 | 1 | 7 | 3 | 8 | 4 | 2 |
| 7 | 5 | 9 | 1 | 6 | 3 | 8 | 7 | 4 | 2 |
| 8 | 5 | 9 | 1 | 6 | 8 | 7 | 3 | 4 | 2 |
| 9 | 5 | 9 | 1 | 6 | 7 | 3 | 8 | 4 | 2 |
| 10 | 9 | 1 | 6 | 5 | 3 | 8 | 7 | 4 | 2 |
| 11 | 9 | 1 | 6 | 5 | 8 | 7 | 3 | 4 | 2 |
| 12 | 9 | 1 | 6 | 5 | 7 | 3 | 8 | 4 | 2 |
| 13 | 1 | 6 | 5 | 9 | 3 | 8 | 7 | 2 | 4 |
| 14 | 1 | 6 | 5 | 9 | 8 | 7 | 3 | 2 | 4 |
| 15 | 1 | 6 | 5 | 9 | 7 | 3 | 8 | 2 | 4 |
| 16 | 6 | 5 | 9 | 1 | 3 | 8 | 7 | 2 | 4 |
| 17 | 6 | 5 | 9 | 1 | 8 | 7 | 3 | 2 | 4 |
| 18 | 6 | 5 | 9 | 1 | 7 | 3 | 8 | 2 | 4 |
| 19 | 5 | 9 | 1 | 6 | 3 | 8 | 7 | 2 | 4 |
| 20 | 5 | 9 | 1 | 6 | 8 | 7 | 3 | 2 | 4 |
| 21 | 5 | 9 | 1 | 6 | 7 | 3 | 8 | 2 | 4 |
| 22 | 9 | 1 | 6 | 5 | 3 | 8 | 7 | 2 | 4 |
| 23 | 9 | 1 | 6 | 5 | 8 | 7 | 3 | 2 | 4 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 24 | 9 | 1 | 6 | 5 | 7 | 3 | 8 | 2 | 4 |

Составим таблицу для уравнения $y^{-1}hy = g$ со всеми его решениями:

| № | 1 | 6 | 5 | 9 | 3 | 8 | 7 | 4 | 2 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 7 | 5 | 9 | 8 | 3 | 6 | 4 | 1 | 2 |
| 2 | 7 | 5 | 9 | 8 | 6 | 4 | 3 | 1 | 2 |
| 3 | 7 | 5 | 9 | 8 | 4 | 3 | 6 | 1 | 2 |
| 4 | 5 | 9 | 8 | 7 | 3 | 6 | 4 | 1 | 2 |
| 5 | 5 | 9 | 8 | 7 | 6 | 4 | 3 | 1 | 2 |
| 6 | 5 | 9 | 8 | 7 | 4 | 3 | 6 | 1 | 2 |
| 7 | 9 | 8 | 7 | 5 | 3 | 6 | 4 | 1 | 2 |
| 8 | 9 | 8 | 7 | 5 | 6 | 4 | 3 | 1 | 2 |
| 9 | 9 | 8 | 7 | 5 | 4 | 3 | 6 | 1 | 2 |
| 10 | 8 | 7 | 5 | 9 | 3 | 6 | 4 | 1 | 2 |
| 11 | 8 | 7 | 5 | 9 | 6 | 4 | 3 | 1 | 2 |
| 12 | 8 | 7 | 5 | 9 | 4 | 3 | 6 | 1 | 2 |
| 13 | 7 | 5 | 9 | 8 | 3 | 6 | 4 | 2 | 1 |
| 14 | 7 | 5 | 9 | 8 | 6 | 4 | 3 | 2 | 1 |
| 15 | 7 | 5 | 9 | 8 | 4 | 3 | 6 | 2 | 1 |
| 16 | 5 | 9 | 8 | 7 | 3 | 6 | 4 | 2 | 1 |
| 17 | 5 | 9 | 8 | 7 | 6 | 4 | 3 | 2 | 1 |
| 18 | 5 | 9 | 8 | 7 | 4 | 3 | 6 | 2 | 1 |
| 19 | 9 | 8 | 7 | 5 | 3 | 6 | 4 | 2 | 1 |
| 20 | 9 | 8 | 7 | 5 | 6 | 4 | 3 | 2 | 1 |
| 21 | 9 | 8 | 7 | 5 | 4 | 3 | 6 | 2 | 1 |
| 22 | 8 | 7 | 5 | 9 | 3 | 6 | 4 | 2 | 1 |
| 23 | 8 | 7 | 5 | 9 | 6 | 4 | 3 | 2 | 1 |
| 24 | 8 | 7 | 5 | 9 | 4 | 3 | 6 | 2 | 1 |

Перейдём к пункту Г

Проведём проверку двух произвольных решений (под номерами 1 и 2 в обоих случаях) наших уравнений:

$$x = \begin{pmatrix} 7 & 5 & 9 & 8 & 3 & 6 & 4 & 1 & 2 \\ 1 & 6 & 5 & 9 & 3 & 8 & 7 & 4 & 2 \end{pmatrix} = (1,4,7)(5,6,8,9)$$

$$x^{-1} = \begin{pmatrix} 1 & 6 & 5 & 9 & 3 & 8 & 7 & 4 & 2 \\ 7 & 5 & 9 & 8 & 3 & 6 & 4 & 1 & 2 \end{pmatrix} = (7,4,1)(9,8,6,5)$$

$x^{-1}gx = (7,4,1)(9,8,6,5) \cdot (7,5,9,8)(3,6,4) \cdot (1,4,7)(5,6,8,9) =$
$= (7,3,8)(1,6,5,9) = h$

$$x = \begin{pmatrix} 7 & 5 & 9 & 8 & 3 & 6 & 4 & 1 & 2 \\ 1 & 6 & 5 & 9 & 8 & 7 & 3 & 4 & 2 \end{pmatrix} = (7,1,4,3,8,9,5,6)$$

$$x^{-1} = \begin{pmatrix} 1 & 6 & 5 & 9 & 8 & 7 & 3 & 4 & 2 \\ 7 & 5 & 9 & 8 & 3 & 6 & 4 & 1 & 2 \end{pmatrix} = (1,7,6,5,9,8,3,4)$$

$x^{-1}gx = (1,7,6,5,9,8,3,4) \cdot (7,5,9,8)(3,6,4) \cdot (7,1,4,3,8,9,5,6) =$
$= (1,6,5,9)(3,8,7) = h$

$$y = \begin{pmatrix} 1 & 6 & 5 & 9 & 3 & 8 & 7 & 4 & 2 \\ 7 & 5 & 9 & 8 & 3 & 6 & 4 & 1 & 2 \end{pmatrix} = (1,7,4)(6,5,9,8)$$

$$y^{-1} = \begin{pmatrix} 7 & 5 & 9 & 8 & 3 & 6 & 4 & 1 & 2 \\ 1 & 6 & 5 & 9 & 3 & 8 & 7 & 4 & 2 \end{pmatrix} = (4,7,1)(8,9,5,6)$$

$y^{-1}hy = (7,1,4)(5,6,8,9) \cdot (1,6,5,9)(3,8,7) \cdot (1,7,5)(6,5,9,8) =$
$= (7,5,9,8)(4,3,6) = g$

$$y = \begin{pmatrix} 1 & 6 & 5 & 9 & 3 & 8 & 7 & 4 & 2 \\ 7 & 5 & 9 & 8 & 6 & 4 & 3 & 1 & 2 \end{pmatrix} = (1,7,3,6,5,9,8,4)$$

$$y^{-1} = \begin{pmatrix} 7 & 5 & 9 & 8 & 6 & 4 & 3 & 1 & 2 \\ 1 & 6 & 5 & 9 & 3 & 8 & 7 & 4 & 2 \end{pmatrix} = (4,8,9,5,6,3,7)$$

$y^{-1}hy = (4,8,9,5,6,3,7) \cdot (1,6,5,9)(3,8,7) \cdot (1,7,3,6,5,9,8,4) =$
$= (7,5,9,8)(4,3,6) = g$

**Задание 3.** Определить какую цикловую структуру и чётность могут иметь подстановки порядка $k$ в группе $S_n$. Найти количество подстановок каждого из описанных типов.

Решение: Имеем порядок $k = 8$ в группе $S_{17}$, т.к. порядок группы это НОК длин всех циклов нашей подстановки, то в любом из представлений данной перестановки будет фигурировать хотя бы один цикл длины 8 и все остальные не больше 8.

Иначе говоря, $ordg = [l_1^{k_1}, l_2^{k_2}, ..., l_r^{k_r}]$

Мы можем найти число решений этих уравнений по формуле:
$|N_{s_n}(g)| = \frac{n!}{\prod_{i=1}^{r}(k_i)! \cdot l_i^{k^i}}$

Составим список всех возможных циклов в виде которых может быть представлена наша подстановка:

1) $[8^2, 1^1] \Rightarrow \frac{17!}{(2! \cdot 8^2)(1! \cdot 1^1)} = 2778808032000$

2) $[8^1, 4^2, 1^1] \Rightarrow \frac{17!}{(1!\cdot 8^1)(2!\cdot 4^2)(1!\cdot 1^1)} = 1389404016000$
3) $[8^1, 2^4, 1^1] \Rightarrow \frac{17!}{(1!\cdot 8^1)(4!\cdot 2^4)(1!\cdot 1^1)} = 115783668000$
4) $[8^1, 4^1, 2^2, 1^1] \Rightarrow \frac{17!}{(1!\cdot 8^1)(1!\cdot 4^1)(2!\cdot 2^2)(1!\cdot 1^1)} = 1389404016000$
5) $[8^1, 4^1, 2^1, 1^3] \Rightarrow \frac{17!}{(1!\cdot 8^1)(1!\cdot 4^1)(1!\cdot 2^1)(3!\cdot 1^3)} = 926269344000$
6) $[8^1, 4^1, 1^5] \Rightarrow \frac{17!}{(1!\cdot 8^1)(1!\cdot 4^1)(5!\cdot 1^5)} = 92626934400$
7) $[8^1.2^2, 1^5] \Rightarrow \frac{17!}{(1!\cdot 8^1)(2!\cdot 2^2)(5!\cdot 1^5)} = 46313467200$
8) $[8^1, 2^1, 1^7] \Rightarrow \frac{17!}{(1!\cdot 8^1)(1!\cdot 2^1)(7!\cdot 1^7)} = 4410806400$
9) $[8^1, 1^9] \Rightarrow \frac{17!}{(1!\cdot 8^1)(9!\cdot 1^9)} = 122522400$

**Задание 4.** Доказать, что отбражение$\varphi : G \to G$ является гомоморфизмом групп. Найти его образ и ядро. Вычислить порядок факторгруппы $G/Ker\varphi$и определить, какой группе она изоморфна.

Решение: Докажем, что отображение $\varphi : G \to G$ - гомоморфизм групп.
$G = \mathbb{Z}_{14} \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_{25}$; отображение $\varphi : (g_1, g_2, g_3) \mapsto (9g_1, 16g_2, 15g_3)$
$\varphi\big((a,b,c)+(d,e,f)\big) = \varphi(a+d, b+e, c+f) = \big(9(a+d), 16(b+e), 15(c+f)\big)$
$\varphi\big((a,b,c)\big)+\varphi\big((d,e,f)\big) = (9a, 16b, 15c)+(9d, 16e, 15f) = \big(9(a+d), 16(b+e), 15(c+f)\big)$
$\Rightarrow \varphi : G \to G$ - гомоморфизм.
Порядок группы $G : |G| = 14 \cdot 18 \cdot 25 = 6300$
$Im\varphi = \{(9a, 16b, 15c) \big| a \in \mathbb{Z}_{14}, b \in \mathbb{Z}_{18}, c \in \mathbb{Z}_{25}\}$
$\mathbb{Z}_{14} = \{\mathbf{0}, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
$9\mathbb{Z}_{14} = \{0, 9, 4, 13, 8, 3, 12, 7, 2, 11, 6, 1, 10, 5\}$
$\mathbb{Z}_{18} = \{\mathbf{0}, 1, 2, 3, 4, 5, 6, 7, 8, \mathbf{9}, 10, 11, 12, 13, 14, 15, 16, 17\}$
$16\mathbb{Z}_{18} = \{0, 16, 14, 12, 10, 8, 6, 4, 2\}$
$\mathbb{Z}_{25} = \{\mathbf{0}, 1, 2, 3, 4, \mathbf{5}, 6, 7, 8, 9, \mathbf{10}, 11, 12, 13, 14, \mathbf{15}, 16, 17, 18, 19, \mathbf{20}, 21, 22, 23, 24\}$
$15\mathbb{Z}_{25} = \{0, 15, 5, 20, 10\}$
Ker$\varphi$ = {(0,0,0) (0,9,0) (0,0,5) (0,9,5) (0,0,10) (0,9,10) (0,0,15) (0,9,15) (0,0,20) (0,9,20)} ⇒всего 10 сочетаний.
$|G/Ker\varphi| = \frac{|G|}{|Ker\varphi|} = \frac{|\mathbb{Z}_{14}\cdot\mathbb{Z}_{18}\cdot\mathbb{Z}_{25}|}{10} = \frac{6300}{10} = 630$
По теореме о гомоморфизме групп, $|G/Ker\varphi| \cong Im\varphi = 9\mathbb{Z}_{14} \oplus \oplus 6\mathbb{Z}_{18} \oplus 15\mathbb{Z}_{25}$;
$9\mathbb{Z}_{14} = \mathbb{Z}_{14}$;
$16\mathbb{Z}_{18} = 2\mathbb{Z}_{18} \cong \mathbb{Z}_9$;
$15\mathbb{Z}_{25} = 3\mathbb{Z}_{25} \cong \mathbb{Z}_5$;
$\Rightarrow |G/Ker\varphi| \cong Im\varphi = \mathbb{Z}_{14} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

**Задание 5.** Пусть $G$ и $H$– конечные абелевы группы.

а) Вычислить порядки групп $G$ и $H$.

б) Выписать канонические разложения групп $G$ и $H$.

в) Найти *typ* $G$ и *typ* $H$ и определить, изоморфны ли группы $G$ и $H$.

Решение: $G = \mathbb{Z}_{51} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{187}$

$ordG = 572220$

$H = \mathbb{Z}_{45} \oplus \mathbb{Z}_{187} \oplus \mathbb{Z}_{17} \oplus \mathbb{Z}_4$

$ordH = 572220$

Для G справедливо следующее:

$51 = 17 \cdot 3; 15 = 3 \cdot 5; 187 = 17 \cdot 11$

Для H справедливо следующее:

$45 = 9 \cdot 5; 187 = 17 \cdot 11;$

Канонические записи G и H:

$\mathbb{Z}_4 =< 1 >$

$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 =< 5 > \dot{+} < 3 >$

$\mathbb{Z}_{51} \cong \mathbb{Z}_{17} \oplus \mathbb{Z}_3 =< 3 > \dot{+} < 17 >$

$\mathbb{Z}_{187} \cong \mathbb{Z}_{17} \oplus \mathbb{Z}_{11} =< 11 > \dot{+} < 17 >$

$G =< (17,0,0,0) > \dot{+} < (3,0,0,0) > \dot{+} < (0,3,0,0) > \dot{+}$
$\dot{+} < (0,5,0,0) > \dot{+} < (0,0,1,0) > \dot{+} < (0,0,0,17) > \dot{+}$
$\dot{+} < (0,0,0,11) > \cong \mathbb{Z}_{17} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{17} \oplus \mathbb{Z}_{11}$

$\mathbb{Z}_4 =< 1 >$

$\mathbb{Z}_{17} =< 1 >$

$\mathbb{Z}_{45} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_5 =< 5 > \dot{+} < 9 >$

$\mathbb{Z}_{187} \cong \mathbb{Z}_{17} \oplus \mathbb{Z}_{11} =< 11 > \dot{+} < 17 >$

$H =< (9,0,0,0) > \dot{+} < (5,0,0,0) > \dot{+} < (0,17,0,0) > \dot{+}$
$\dot{+} < (0,11,0,0) > \dot{+} < (0,0,1,0) > \dot{+} < (0,0,0,1) > \cong$
$\cong \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{17} \oplus \mathbb{Z}_{17} \oplus \mathbb{Z}_4$

$typG = [3^1, 3^1, 2^2, 5^1, 11^1 17^1, 17^1]$

$typH = [3^2, 2^2, 5^1, 11^1 17^1, 17^1]$

$\Rightarrow G \ncong H$

**Задание 6.** Пусть $G = < g_1, g_2 >$ - группа подстановок степени $n \in N$, порождённая элементами $g_1, g_2 \in S_n$.

а) Определить, является ли группа $G$ абелевой, и выписать все её элементы.

б) Выписать орбиты и стабилизаторы для каждой из точек a $\in \overline{1,n}$ в группе $G$.

в) Определить, является ли группа $G$ транзитивной ($k-$транзитивной)или регулярной ($k-$регулярной).

г) Определить, является ли группа $G$ примитивной или импримитивной.

Решение: $G =< g_1, g_2 >, g_1 = (1\,4\,6\,2\,5\,3), g_2 = (1\,2)(3\,5)(4\,6)$

Начнём с пункта А

Найдём все элементы группы G:

По образующей $g_1$:

$$g_1 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} = g_3$$

$$g_1 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 5 & 1 \end{pmatrix} = g_4$$

$$g_1 \cdot g_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = g_5$$

$$g_1 \cdot g_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = g_6$$

$$g_1 \cdot g_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix} = g_7$$

$$g_1 \cdot g_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix} = g_8$$

$$g_1 \cdot g_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 2 & 4 \end{pmatrix} = g_9$$

$$g_1 \cdot g_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix} = g_{10}$$

$$g_1 \cdot g_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon$$

$$g_1 \cdot g_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = g_{11}$$

$$g_1 \cdot g_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix} = g_2$$

$$g_1 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} = g_3$$

$$g_2 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = g_{11}$$

$$g_3 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = g_5$$

$$g_4 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix} = g_2$$

$$g_5 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix} = g_7$$

$$g_6 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 5 & 1 \end{pmatrix} = g_4$$

$$g_7 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 2 & 4 \end{pmatrix} = g_9$$

$$g_8 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = g_6$$

$$g_9 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon$$

$$g_{10} \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix} = g_8$$

$$g_{11} \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix} = g_{10}$$

По образующей $g_2$:

$$g_2 \cdot g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = g_{11}$$

$$g_2 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon$$

$$g_2 \cdot g_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix} = g_{10}$$

$$g_2 \cdot g_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 2 & 4 \end{pmatrix} = g_9$$

$$g_2 \cdot g_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix} = g_8$$

$$g_2 \cdot g_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix} = g_7$$

$$g_2 \cdot g_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = g_6$$

$$g_2 \cdot g_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = g_5$$

$$g_2 \cdot g_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 5 & 1 \end{pmatrix} = g_4$$

$$g_2 \cdot g_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} = g_3$$

$$g_2 \cdot g_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 6 & 3 & 2 \end{pmatrix} = g_1$$

$$g_1 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 5 & 1 \end{pmatrix} = g_4$$

$$g_2 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon$$

$$g_3 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = g_6$$

$$g_4 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 6 & 3 & 2 \end{pmatrix} = g_1$$

$$g_5 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 6 & 5 \end{pmatrix} = g_8$$

$$g_6 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} = g_3$$

$$g_7 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix} = g_{10}$$

$$g_8 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = g_5$$

$$g_9 \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = g_{11}$$

$$g_{10} \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = g_7$$

$$g_{11} \cdot g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 1 & 2 & 4 \end{pmatrix} = g_9$$

Построим неполную таблицу Кэли, заполнив лишь те столбцы и строки, которые соответствуют $g$ и $g_2$:

| $\cdot$ | $\varepsilon$ | $g_1$ | $g_2$ | $g_3$ | $g_4$ | $g_5$ | $g_6$ | $g_7$ | $g_8$ | $g_9$ | $g_{10}$ | $g_{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\varepsilon$ | | $g_1$ | $g_2$ | | | | | | | | | |
| $g_1$ | $g_1$ | $g_3$ | $g_4$ | $g_5$ | $g_6$ | $g_7$ | $g_8$ | $g_9$ | $g_{10}$ | $\varepsilon$ | $g_{11}$ | $g_2$ |
| $g_2$ | $g_2$ | $g_{11}$ | $\varepsilon$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_1$ |
| $g_3$ | | $g_5$ | $g_6$ | | | | | | | | | |
| $g_4$ | | $g_2$ | $g_1$ | | | | | | | | | |
| $g_5$ | | $g_7$ | $g_8$ | | | | | | | | | |
| $g_6$ | | $g_4$ | $g_3$ | | | | | | | | | |
| $g_7$ | | $g_9$ | $g_{10}$ | | | | | | | | | |
| $g_8$ | | $g_6$ | $g_5$ | | | | | | | | | |
| $g_9$ | | $\varepsilon$ | $g_{11}$ | | | | | | | | | |
| $g_{10}$ | | $g_8$ | $g_7$ | | | | | | | | | |
| $g_{11}$ | | $g_{10}$ | $g_9$ | | | | | | | | | |

$G = \{\varepsilon, (1\,4\,6\,2\,5\,3), (1\,2)(3\,5)(4\,6), (1\,6\,5)(2\,3\,4), (1\,6)(2\,3),$
$(1\,2)(3\,6)(4\,5), (1\,4)(2\,5)(3\,6), (1\,5\,6)(2\,4\,3), (3\,4)(5\,6),$
$(1\,3\,5\,2\,6\,4), (1\,3)(2\,6)(4\,5), (1\,5)(2\,4)\}$

Группа G не абелева, что следует из таблицы. В качестве примера рассмотрим результаты произведений $g_1 \cdot g_2$ и $g_2 \cdot g_1$.

Переходим к пункту Б

Выпишем орбиты для всех элементов:

$G(1) = \{1, 4, 2, 6, 3, 5\} = G(2) = G(3) = G(4) = G(5) = G(6)$

Выпишем стабилизаторы для всех элементов:

$St_G(1) = \{\varepsilon, (3\,4)(5\,6)\}$

$St_G(2) = \{\varepsilon, (3\,4)(5\,6)\}$

$St_G(3) = \{\varepsilon, (1\,5)(2\,4)\}$

$St_G(4) = \{\varepsilon, (1\,6)(2\,3)\}$

$St_G(5) = \{\varepsilon, (1\,6)(2\,3)\}$

$St_G(6) = \{\varepsilon, (1\,5)(2\,4)\}$

Перейдём к пункту В

Группа G является транзитивной, т.к. существует ровно одна орбита для всех элементов, но не является регулярной, т.к. $|G| = 12; n = 6 \Rightarrow |G| \neq n$.

Выпишем орбиты для стабилизаторов:

$St_G(1) : \{1\}, \{2\}, \{3, 4\}, \{5, 6\}$

$St_G(2) : \{1\}, \{2\}, \{3, 4\}, \{5, 6\}$

$St_G(3) : \{1, 5\}, \{2, 4\}, \{3\}, \{6\}$

$St_G(4) : \{4\}, \{5\}, \{1, 6\}, \{2, 3\}$

$St_G(5) : \{4\}, \{5\}, \{1, 6\}, \{2, 3\}$

$St_G(6) : \{1, 5\}, \{2, 4\}, \{3\}, \{6\}$

Так же группа G не является k-транзитивной (при $k \geq 2$), т.к не выполняется условие: $|G| \nmid n(n-1)$ (и соответственно не является k-регулярной).

Перейдём к пункту Г

Найдём все делители |G|=12: 1,2,3,4,6,12;

$|St_G(1)| = ... = |St_G(6)| = 2$;

Нам нужно придерживаться условия максимальности подгрупп:

$St_G(a) < H < G$

Тогда рассмотрим циклическую подгруппу $H$, образующими которой являются 2 элемента из стабилизатора:

$H =< (3\,4)(5\,6), (1\,5)(2\,4) >=$

$= \{\varepsilon, (3\,4)(5\,6), (1\,5)(2\,4), (1\,5\,6)(2\,4\,3), (1\,6\,5)(2\,3\,4)\} < G \Rightarrow$

$\Rightarrow$ т.к. $St_G(1), ..., St_G(6)$ не является максимальной подгруппой (содержится в $H < G$), то $G$ - импримитивна.

# 4. ЗАКЛЮЧЕНИЕ

Группы подстановок – весьма серьезный раздел математики, к которому нужно относиться с полной серьёзностью и постоянно совершенствовать себя в этом направлении, если желаешь не отставать от развития криптографии и новых тенденций информационной безопасности.

К сожалению, не у всех людей найдётся достаточное количество умственных ресурсов для осознания всех криптографических основ. Однако освоение подобного рода материала может значительно упростить понимание основных математических и криптографических моделей. Эти знания смогут помочь в освоении сложнейших шифров и методов дешифрования, найти путь к новейшим методам шифрования, которые смогут стать революционными.

# 5. СПИСОК ЛИТЕРАТУРЫ

1.Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: Учебник. — 2-ое, испр.

2.и доп. изд. — СПб : Издательство «Лань», 2020 — 608 с.

3.Куликов Л.Я. Алгебра и теория чисел: Учебное пособие для педагогических институтов. — М : Высшая школа, 1979 — 559 с.

4.Применко Э.А. Алгебраические основы криптографии: Учебное пособие. — 2-ое, испр. изд. — М : ЛЕНАНД, 2018 — 288 с.

5.Кострикин А.И. Введение в алгебру. Ч. I: Основы алгебры. — 3-ое, стереотип. изд. — М : МЦНМО, 2018 — 272 с.

6.Куликов Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и тео- рии чисел: Учеб. пособие для студентов физ.-мат. спец. пед. ин-тов. — М : Про- свещение, 1993 — 288 с.

7.Сборник задач по алгебре / Под ред. Кострикина А.И. — 2-ое, стереотип. изд. — М : МЦНМО, 2015 — 416 с.

8.Фадеев Д.К., Соминский И.С. Задачи по высшей алгебре. — 17-ое, стереотип. изд. — СПб : Издательство «Лань», 2008 — 288 с.

9.Ляпин Е.С., Айзенштат А.Я., Лесохин М.М. Упражнения по теории групп: Учебное пособие. — 2-ое, стереотип. изд. — СПб : Издательство «Лань», 2010 — 272 с.