1 Инверсия

Определение. Говорят, что i_s, i_t перестановка $\sigma = \begin{pmatrix} 1..s..t..n \\ ..i_s..i_t.. \end{pmatrix}$ образует инверсию, если $s < t, i_s > i_t$

Число всех инверсий $\sigma = inv(\sigma)$

Теорема. Если перестановка σ - четная (нечетная) $\Leftrightarrow inv(\sigma)$ - четно (нечетно).

$\sigma = (23) \quad \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 3\ 2\ 4 \end{pmatrix} inv(23) = 1 \quad$ нечетно.

$\sigma = (234) \quad \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 3\ 4\ 2 \end{pmatrix} inv(234) = 2$ четно.

Пример. $\begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 4\ 2\ 1 \end{pmatrix} \underset{(13)}{\to} \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 4\ 2\ 3 \end{pmatrix} \underset{(24)}{\to} \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 4\ 3 \end{pmatrix} \underset{(34)}{\to} \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 3\ 4 \end{pmatrix}$

$(13)(24)(34) = (1234)$

Доказательство.

1. Транспозиция соседних чисел меняет число инверсий на одну.
$\begin{pmatrix} 1\ ..\ i\ j\ ..\ n \\ ..\ ..\ j\ i\ ..\ .. \end{pmatrix}$
1) Рассмотрим пары, не содержащие $i, j \Rightarrow$ число инверсий не меняется.

2) Рассмотрим пары содержащие либо i, либо $j \Rightarrow (k, i), (k, j), (i, k), (j, k)$ либо обратна инверсия, как раньше $\Rightarrow$ число инверсий не меняется.

3) $(i, j) \to (j, i)$ - число инверсия изменяется на одну.

2. Транспозиция $\forall i, j$ меняет четность числа инверсий.
$\left(i\underbrace{ab..cd}_{m}j\right) \to \left(..aib..cdj\right) \to \left(ab..cdij\right) \to \left(ab..cdji\right) \to \left(jab..cdi\right)$
m транспозиций соседних чисел.
$\Rightarrow$ всего $2m+1$ транспозиций соседних чисел $\Rightarrow$ четность $inv(\sigma)$ измен.

3. σ - четное (нечетное) $\Leftrightarrow \sigma =$ четное (нечетное) число транспозиций $\Leftrightarrow inv(\sigma)$ - четное (нечетное).

2 Теорема Лагранжа

Определение. G - группа, $H \leq G$, $x \in G$, тогда xH - левым смежным классом по подгруппе H (Hx - правый смежный класс).

Пример. $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$
$H = A_3 = \{e, (123), (132)\}$
$(12)H = \{(12), (12)(123), (12)(132)\} = \{(12), (23), (13)\}$

Лемма. $\forall$ два смежных класса (левых) либо совпадают, либо не пересекаются.

Доказательство. $x, y \in G \quad xH \cap yH \neq \varnothing$
$xh_1 = yh_2 \Rightarrow x = yh_2h_1^{-1} \Rightarrow$
$xH = yh_2h_1^{-1}H = yH$

Определение. Число различных смежных классов (левых)
$H \leq G$ называется индексом подгруппы H в G и обозначается

$$[G : H]$$

Теорема Лагранжа.
G - конечная группа, $H \leq G$
$\Rightarrow |G| = [G : H] * |H|$

Доказательство.
1.Количетсво элементов в каждом смежном классе одинаково $\quad |xH| = |H| \quad \forall x \in G$
2. $G = x_1H \cup x_2H \cup ... \cup x_kH \Rightarrow |G| = k * |H|,\ k = [G : H]$

Следствие. G_3 - конечное группа $H \leq G \Rightarrow |G| \vdots |H|$

Пример.
$S_3 = A_3 \cup (12)A_3 \quad |S_3| = [S_3 : A_3] * |A_3|$

Определение. Подгруппа вида $H = \{e, a, a^2, ..., a^n = e\}$ называется циклической.

Определение. Наименьшее натуральное $n \in \mathbb{N} : a^n = e$ называется порядком элемента a.

Следствие. Порядок элемента делит $|G|$
Доказательство. $a \in G, a^n = e, n$ - порядок a.

Рассмотрим $H = \{e, a, ..., a^n\},\ |H| = n,\ |G| \vdots n$, по теореме Лагранжа.