Теория групп

prerequisite knowledge: база алгебры: множества, упорядоченные n-ки, декартово произведение, отображения, графики, классы отображений, отношения их их свойства.

Мотивация

Группа - одна из простейших алгебраических структур, свойства которой нам будут очень полезны.

Аксиомы и примеры:

Пусть есть какое-то непустое множество G с заданной на нём бинарной операцией звёздочкой $*: G \times G \to G$.
Такое множество называется **группой**, если выполняются три аксиомы:

1. $\forall a, b, c \in G : a * (b * c) = (a * b) * c$ (ассоциативность операции)
2. $\exists e \in G : a * e = e * a = a$ (существование единицы)
3. $\forall a \in G : \exists a' : a * a' = e$ (существование обратных)

e называют нейтральным элементом, а a' - обратным к a.

Заметим, что не для всех $a, b : a * b \neq b * a$.
Если для всех элементов группы справедлива

коммутативность умножения ($a * b = b * a$), то группа называется **абелевой**.

> Обычно для абелевой группы вместо звездочки пишут плюс, вместо нейтрального элемента - 0, а вместо обратного к a - $-a$. Для неабелевой пишут знак умножения, вместо нейтрального - 1, вместо обратного к a - a^{-1}. Такие записи называются аддитивными и мультипликативными соответственно.

Далее группы обозначаются либо несущим множеством: G; либо парой множества и операции: $(G, *)$.

Примеры групп:

1. $(\mathbb{Z}, +)$ - целые числа по сложению. У каждого элемента есть обратный (он же со знаком минус), нейтральный - 0, ассоциативность сложения выполняется.
2. $(\mathbb{Q} \setminus \{0\},\ \bullet)$ - рациональные числа без нуля по умножению. Обратный - перевернутая дробь, нейтральный - 1, ассоциативность умножения выполняется.
3. $(\mathbb{R}_{>0},\ \bullet)$ - положительные вещественные числа по умножению.
4. $(\{\pm 1\} \in \mathbb{R},\ \bullet)$ - группа из элементов $-1,\ 1$. Нейтральный - 1, обратный - он сам. Построим **таблицу Кэли** операции:

$\bullet$	$\mathbf{1}$	$\mathbf{-1}$
$\mathbf{1}$	1	-1
$\mathbf{-1}$	-1	1

Смотреть так: чтобы получить результат операции двух элементов, надо взять один элемент из первого столбца и один элемент из первой строки. Затем посмотрим на пересечение соответствующих им строки и столбца. Это и есть результат операции этих двух элементов.

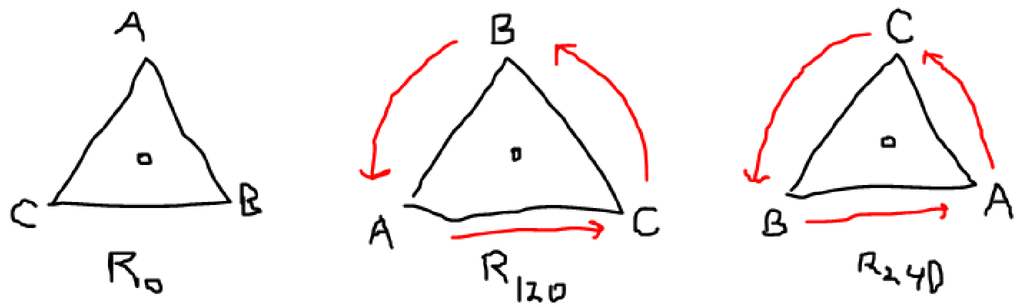
5. Множество поворотов правильного n-угольника на плоскости вокруг его центра на углы $\frac{2\pi k}{n}$.

На пятом примере можно остановиться поподробнее, так как это очень интересная группа. Рассмотрим простейшую из таких групп - группу поворотов правильного треугольника. Элементами группы будут такие повороты, которые оставляют его таким же, если бы мы не знали названия вершин. А именно:

- поворот на 0 градусов вокруг центра
- поворот на 120 градусов вокруг центра
- поворот на 240 градусов вокруг центра

Обозначим эти операции как $R_0,\ R_{120},\ R_{240}$ соответственно.

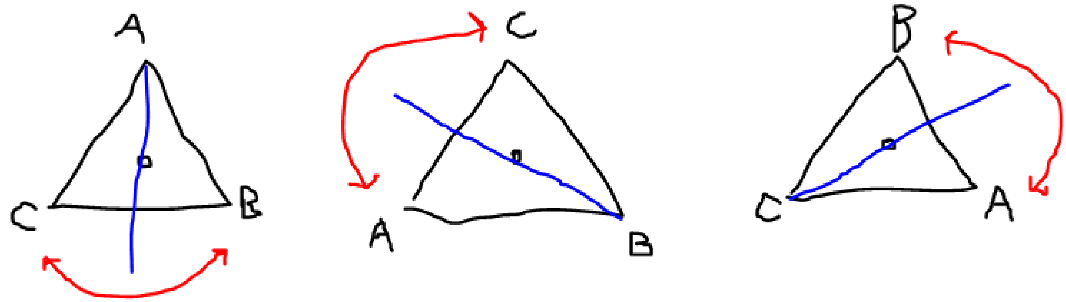
Заметим, что R_0 - тождественное отображение в треугольник до операции. Этот поворот не меняет ничего, поэтому его можно считать нейтральным элементом.



Зададим операцию на множестве поворотов: $\circ$ - операцию композиции. Мы можем применить два поворота:
$R_{120} \circ R_{120} = R_{240}$.
Можете проверить, что любая композиция поворотов - это тоже поворот.
Для каждого поворота есть поворот, который возвращает треугольник в исходное положение. Например проверим, что обратное к R_{120} это R_{240}. Повернём треугольник на 120 градусов и затем на 240: $R_{240} \circ R_{120} = R_0$.
Получается, что у каждого элемента группы есть обратный.
Композиция поворотов ассоциативна.
Получили группу поворотов правильного треугольника вокруг его центра. Таблица Кэли операции:

$\circ$	$\mathbf{R_0}$	$\mathbf{R_{120}}$	$\mathbf{R_{240}}$
$\mathbf{R_0}$	R_0	R_{120}	R_{240}
$\mathbf{R_{120}}$	R_{120}	R_{240}	R_0
$\mathbf{R_{240}}$	R_{240}	R_0	R_{120}

Но не только повороты оставляют треугольник на месте. Можем расширить нашу группу до группы самосовмещений треугольника. Симметрия относительно медианы тоже сохраняет треугольник. Таких симметрий три: $S_a,\ S_b,\ S_c$.



Однако это действие меняет свойство треугольника - его ориентацию. Применив симметрию, мы как бы попали в зазеркалье - там меняется направление. То есть, из элемента симметрии мы не сможем получить элемент поворота, не применив симметрию ещё раз. Таблица Кэли новой группы:

$\circ$	$\mathbf{R_0}$	$\mathbf{R_{120}}$	$\mathbf{R_{240}}$	$\mathbf{S_a}$	$\mathbf{S_b}$	$\mathbf{S_c}$
$\mathbf{R_0}$	R_0	R_{120}	R_{240}	S_a	S_b	S_c
$\mathbf{R_{120}}$	R_{120}	R_{240}	R_0	S_b	S_c	S_a
$\mathbf{R_{240}}$	R_{240}	R_0	R_{120}	S_c	S_a	S_b
$\mathbf{S_a}$	S_a	S_c	S_b	R_0	R_{240}	R_{120}
$\mathbf{S_b}$	S_b	S_a	S_c	R_{120}	R_0	R_{240}
$\mathbf{S_c}$	S_c	S_b	S_a	R_{240}	R_{120}	R_0

Группа поворотов треугольника - **подгруппа** этой более большой группы самосовмещений правильного треугольника на плоскости. Вот она в верхнем левом углу таблицы. О подгруппах поговорим чуточку позднее.

Вообще все эти преобразования можно было бы записать без поворотов и симметрий. Например, заменим элементы группы поворотов треугольника на **перестановки вершин** треугольника:

$$R_0 = id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \ R_{120} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \ R_{240} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

Под каждой вершиной пишется та, в которую она переходит при повороте. И у нас получилась группа не поворотов треугольника, а **группа перестановок**. Это вроде бы разные группы, но они представляют что-то одно по своей сути. Такое явление называется **изоморфизмом** групп, про который поговорим буквально через пункт (в следующем параграфе).

Свойства групп:

1. **Нейтральный элемент единственный.**

   Доказательство ›

   Пусть есть какие-то два нейтральных e, e'. Тогда $e = e * e' = e'$ по определению нейтрального.

2. **Для каждого элемента обратный единственный.**

   Док-во ›

   Пусть g', g'' - обратные к g. Тогда $g' = g'_e = g'_(g * g'') = g' * g * g'' = (g' * g) * g'' = e * g'' = g''$

3. **Уравнения $ax = b, ya = b$ разрешимы относительно x, y единственным способом.**

   Док-во:

   Рассмотрим $ax = b$. Пусть есть решение x. Домножим на a^{-1} слева:
   $a^{-1}(ax) = a^{-1}bex = a^{-1}bx = a^{-1}b$ - единственность.
   Проверим, что это решение:
   $a(a^{-1}b) = beb = bb = b$. ч.т.д.
   Для y аналогично. Домножаем на a^{-1} справа и получаем $y = ba^{-1}$.

4. **Если $(ax = ay)$ или $(xa = ya)$, то $x = y$. (то есть возможно сокращение слева и справа)**

   D:

   Пусть $ax = ay$. Домножим на a^{-1} слева. $ex = ey, x = y$.
   Аналогично и для $xa = ya$.

Из этих свойств **следует** небольшой факт:
Пусть G - группа, $a \in G$, заданы два отображения:

$$\begin{aligned} \phi_a : G &\to G & \psi_a : G &\to G \\ x &\mapsto ax & y &\mapsto ya \end{aligned}$$

Эти отображения - биекции.

D:

Докажем для ϕ_a:
Сюръективность: $\forall b \in G \quad \phi(x) = ax = b$. По третьему свойству x существует, причем единственный, следовательно для всякого b есть прообраз.
Инъективность следует из четвёртого свойства:
$\phi(x) = \phi(y) \iff ax = ay,\ a^{-1}ax = a^{-1}ay,\ x = y.$
Значит ϕ_a биективно. Аналогично доказывается и для ψ_a.

Далее поговорим про изоморфизм групп.

2. Изоморфизм групп

Пусть есть две группы $(G, *), (H, \circ)$, отображение $f : G \to H$. Это отображение называется **изоморфизмом**, если

1. f биективно
2. $\forall g_1, g_2 \in G : f(g_1 * g_2) = f(g_1) \circ f(g_2)$

Если между двумя группами есть изоморфизм, то они называются **изоморфными**:

$$G \cong H$$

Например

Группа $\{\pm 1\}$ с операцией умножения и группа перестановок $\{a, b\}$ изоморфны.
$f : \begin{cases} 1 & \mapsto id \\ -1 & \mapsto (a \leftrightarrow b) \end{cases}$

(1 переходит в нейтральную перестановку, -1 в единственную отсавшуюся перестановку, которая меняет элемент на другой: a на b, и наоборот)
Можете проверить второе свойство самостоятельно.

Некоторые свойства изоморфизма

1. $G \cong G$ (**группа изоморфна сама себе**)
2. $G \cong H \implies H \cong G$ (**изоморфизм симметричен**)

D:

Пусть есть изоморфизм f из G в H. У биекции есть обрантое: f^{-1}, проверим для него второй критерий изоморфизма: Пусть есть $h_1, h_2 \in H$, $\exists g_1, g_2 \in G$:

$$h_1 = f(g_1) \iff g_1 = f^{-1}(h_1)$$
$$h_2 = f(g_2) \iff g_2 = f^{-1}(h_2)$$
$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2)$$
$$f^{-1}(h_1h_2) = g_1g_2 = f^{-1}(h_1)f^{-1}(h_2)$$

3. $G \cong H, H \cong K \implies G \cong K$. (**композиция изоморфизмов - изоморфизм**)

D:

$f : G \to H,\ d : H \to K$. $d \circ f$ - биекция.
$(d \circ f)(g_1g_2) = d(f(g_1g_2)) = d(f(g_1)f(g_2)) =$
$d(f(g_1))d(f(g_2)) = (d \circ f)(g_1)(d \circ f)(g_2)$

Гомоморфизм:

Пусть всё ещё есть группы $(G, *), (H, \circ)$, но теперь $f : G \to H$ **не биективно**. Тогда f называется **гомоморфизмом**, если

$$\forall g_1, g_2 \in G : f(g_1 * g_2) = f(g_1) \circ f(g_2)$$

Таким образом **изоморфизм** - это биективный гомоморфизм.
Некоторые свойства гомоморфизма:

1. $f(e_G) = e_H$

> **D:**
>
> $$f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G) \quad | \, (f(e_G))^{-1} \circ$$
> $$e_H = e_H \circ f(e_G) \implies e_H = f(e_G)$$

2. $f(g^{-1}) = (f(g))^{-1}$

> **D:**
>
> $$\left.\begin{matrix} e_H = f(e_G) = f(g * g^{-1}) = f(g) \circ f(g^{-1}) \\ e_H = f(e_G) = f(g^{-1} * g) = f(g^{-1}) \circ f(g) \end{matrix}\right\} \implies$$
> $f(g^{-1})$ - обратный к $f(g)$.

3. Подгруппы

В начале главы мы познакомились с примером группы самосовмещений треугольника. В этой группе была подгруппа поворотов относительно центра. Строго определим это понятие.

Пусть есть группа $(G, *)$ и непустое подмножество $\varnothing \neq H \subseteq G$. $(H, *)$ - **подгруппа** G, если H - группа относительно той же самой операции $(*)$:
$(*) : G \times G \to G$
$(*)|_{H \times H} : H \times H \to H$ (сужение операции на H)

Подгруппа обозначается так: $H \leq G$.

Пример:

$(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

Критерий подгруппы

Как понять, подгруппа перед нами или нет?

Пусть есть группа $(G, *)$, $\varnothing \neq H \subset G$. Тогда:

$$H \leq G \iff \begin{cases} \forall h_1, h_2 \in H & : h_1 * h_2 \in H \\ \forall h \in H & : h^{-1} \in H \end{cases}$$

(H - подгруппа G, если H замкнута относительно умножения и замкнута относительно взятия обратного.)

D:

$\boxed{\Rightarrow}$ Пусть H - подгруппа. Значит, H - группа относительно этой же операции. Значит, операция задана на $H \times H \to H$. Получается, что H замкнута относительно умножения, и обратные лежат в H.
$\boxed{\Leftarrow}$ Пусть выполнены оба условия. На H задана операция группы G :
$\forall g_1, g_2, g_3 \in G : g_1(g_2g_3) = (g_1g_2)g_3 \implies$
$\forall g_1, g_2, g_3 \in H : g_1(g_2g_3) = (g_1g_2)g_3$ (ассоциативность)
Возьмём $h \in H$. По второму свойству $h^{-1} \in H$, по первому $h * h^{-1} \in H \implies e_G \in H$.
$\forall g \in G : e_G * g = g * e_G = g \implies$
$\forall g \in H : e_G * g = g * e_G = g$.
e_G будет нейтральным в H. Обратные тоже в H
$\implies H$ - группа относительно той же операции - подгруппа.

Пересечения подгрупп

У подгрупп одной группы есть наверняка что-то общее. Хотя бы нейтральный. Об этом в следующем предложении:

Пусть есть группа $(G, \cdot)$, семейство подгрупп $\{H_i\}_{i \in I},\ H_i \leq G$. Тогда **пересечение подгрупп - группа**:

$$\bigcap_{i \in I} H_i \leq G$$

D: ›

Каждая H_i содержит $e = e_G \implies e \in \bigcap H_i, \ \bigcap H_i \neq \varnothing$.
Рассмотрим $h, g \in \bigcap H_i$. Тогда
$h, g \in H_i$ для всех $i \in I$.
$h \cdot g \in H_i$ (т.к. $H_i \leq G$).
$h^{-1} \in H_i$ (т.к. $H_i \leq G$).
Таким образом, $hg \in \bigcap H_i, \ h^{-1} \in \bigcap H_i$, по выбору h, g это справедливо для всех элементов пересечения, и по критерию подгруппы $\bigcap H_i \leq G$.

Подгруппа, порождённая множеством

Есть группа G, рассмотрим пересечение подгрупп, содержащие множество S: $H = \bigcap\limits_{S \subseteq F \leq G} F$.
H - подгруппа G, т.к. пересечение подгрупп F - группа.
H - наименьшая (по включению) подгруппа G, содержащая S.
H - **подгруппа, порождённая множеством** S:

$$H = \langle S \rangle$$

S - **<u>множество образующих</u>** подгруппы H.

Пример

$\langle \varnothing \rangle = \{e\}$
$\langle e \rangle = \{e\}$
$\langle -1 \rangle = (\{\pm 1\}, \cdot)$

Пусть F - любая подгруппа, содержащая S.
В F есть $e, \ s \in S, \ s^{-1} \in S$.

Можем рассматривать всевозможные следующие произведения: $s_1^{n_1}, s_2^{n_2}, \ldots, s_k^{n_k} \in F$, где $s_i \in S,\ n_i \in \{\pm 1\},\ k \geq 0.$

Предложение. $\langle S \rangle = \{s_1^{n_1} \cdot \ldots \cdot s_k^{n_k} \mid k \geq 0,\ n_i \in \{\pm 1\},\ s_i \in S\}.$

---

4. Теорема о делении с остатком в $\mathbb{Z}$.

Пусть $a, b \in \mathbb{Z},\ b \neq 0.$ Тогда

$$\exists! q, r \in \mathbb{Z} : a = bq + r,\ 0 \leq r \leq |b|$$

q - **неполное частное**, r - **остаток от деления** a на b.

---

5. Циклические группы

Группа, порождённая одним элементом, - **циклическая**.

Примеры

1. $\langle e \rangle = \{e\}$
2. $\mathbb{Z}, + \quad \langle 1 \rangle = (\mathbb{Z}, +)$
3. Группы поворотов плоскости вокруг нуля на углы $\frac{2\pi n}{k}, k \in \mathbb{Z}$ порождаются поворотом на $\frac{2\pi}{n}$.

Назовём группу из примера номер 3 C_n.

Теорема. Всякая циклическая группа изоморфна либо группе целых чисел по сложению, либо $C_n,\ n \geq 1$.

Порядок группы

$a \in (G, \cdot)$.
Если $a^k \neq a^j \quad \forall k \neq j$ (т.е. $\langle a \rangle \cong (\mathbb{Z}, +)$), то говорят, что у a **бесконечный порядок**.
В противном случае, существует наименьшее положительное n, что $a^n = e_G$. Тогда n - **порядок** a.

Порядок группы - её мощность - $|G|$.

Порядок a совпадает с порядком $\langle a \rangle$.

6. Классы смежности

#todo мотивацию и примеры

G - группа, $H \leq G$.
$a, b \in G$.

Левый класс смежности

$a \underset{L}{\equiv} b \iff b^{-1}a \in H$.

Лемма. $\underset{L}{\equiv}$ - отношение эквивалентости.

$[a]_L$ - **левый класс смежности** по подгруппе H.

$[a]_L = \{b \in G \mid b^{-1}a = h,\ h \in H\} = \{b \in G \mid b = ah^{-1},\ h \in H\} = \underline{aH}$

Правый класс смежности

$a \underset{R}{\equiv} b \iff ab^{-1} \in H.$

Лемма. $\underset{R}{\equiv}$ - отношение эквивалентности.

D:

Аналогично предыдущей лемме.

$[a]_R$ - **<u>правый класс смежности</u>** по подгруппе H.
$[a]_R = \{b \in G \mid b = h^{-1}a,\ h \in H\} = Ha$

В общем случае $aH \neq Ha$. Равенство в случае абелевой группы.

Если $H = G$, то только 1 класс смежности.
Если $H = \langle e \rangle$, то каждый класс смежности содержит 1 элемент.

7. Теорема Лагранжа

Лемма. $(G, \cdot)$ - группа, $H \leq G,\ a \in G$.
Множества H и aH равномощны и множества H и Ha равномощны.

Все левые классы смежности образуют разбиение множества G на подмножества aH, равномощные H.

Равномощны ли фактормножества $G/_{\underset{L}{\equiv}}$ и $G/_{\underset{R}{\equiv}}$?

Лемма 2. Фактормножества $G/_{\underset{L}{\equiv}}$ и $G/_{\underset{R}{\equiv}}$ равномощны.
(неформально: число левых классов равно числу правых)

Индекс подгруппы H в G - это мощность $G/_{\underset{L}{\equiv}}$ (или тоже самое, что $G/_{\underset{R}{\equiv}}$). *(количество левых классов смежности)*
Индекс подгруппы обозначается так: $[G : H]$.
Далее будем различать индекс конечный и бесконечный.

Теорема Лагранжа. G - конечная группа, $H \leq G$.

$$|G| = |H| \cdot [G : H]$$

Следствие 1. $|H|$ делит $|G|$.
Следствие 2. $a \in G$. Порядок a делит $|G|$.

8. Симметрические группы

Пусть есть какое-то множество $X = \{1, 2, \dots, n\}$.
$S(X)$ - **множество всех биекций** на X.
S_n - **симметрическая группа, группа перестановок** степени n. Элементы группы - **перестановки**:

$$\sigma \in S_n \quad \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Иногда пишут только вторую строку.
σ^{-1} - та же перестановка, только надо поменять строки местами.

Мощность группы перестановок: $|S_n| = n!$

Цикл длины k - переводит каждый элемент в следующий, а последний (k-тый) - в первый. Пишут $(i_1\, i_2 \dots i_k)$.

Количество различных циклов длины k в S_n : $\frac{n(n-1)\dots(n-k+1)}{k}$.

Цикл длины два - **транспозиция**: $(i\; j)$
Два цикла называются **незацепляющимися**, если у них нет общих элементов из X.

$x \in X$ - **неподвижная точка** для σ, если $\sigma(x) = x$.

Лемма 1. Произведение двух незацепляющихся циклов не зависит от порядка сомножителей.

Теорема. Всякая перестановка представляется в виде произведения попарно незацепляющихся циклов, и такое представление единственно с точностью до перестановок сомножителей.

Перестановки $\sigma,\ \sigma'$ **сопряженные**, если существует $\tau \in S_n : \sigma' = \tau\sigma\tau^{-1},\ \sigma = \tau^{-1}\sigma'\tau$.

Некоторые семейства образующих S_n:

1. S_n порождается циклами.

2. Все транспозиции пораждают $S_n,\ n \geq 2$.

3. S_n пораждаются транспозициями, меняющих два соседних элемента

9. Чётность перестановок

$\sigma \in S_n, \quad 1 \leq i, j \leq n.$

i, j - **<u>инверсия</u>** для σ, если $i < j,\ \sigma(i) < \sigma(j)$.

$I(\sigma)$ - **множество всех инверсий** перестановки σ.
$|I(\sigma)| = \#\sigma.$

Пример:

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ - инверсии, любые два элемента - инверсия.

$\#id = 0$
$\# \begin{pmatrix} 1 \dots n \\ n \dots 1 \end{pmatrix} = \frac{n(n-1)}{2}$

Определим $l(\sigma) = n - \text{число циклов в цикловом типе}$. *(это не тире, а минус)*
(считаем неподвижные точки как циклы длины 1).

Пример:

Цикловый тип σ': $(5\ 5\ 3\ 2\ 2\ 1\ 1\ 1)$ - цикл длины 5, цикл длины 5, цикл длины 3, $\ldots$
$l(\sigma') = 20 - 8 = 12$

Наша цель: $\sigma = \tau_1\tau_2\ldots\tau_m, \quad \tau_i$ - транспозиции. Хотим докажем, что $m,\ l(\sigma),\ \#\sigma$ имеют одну чётность.

Теорема 1. $\sigma \in S_n,\ \tau$ - транспозиция. Тогда $l(\sigma),\ l(\sigma\tau)$ имеют разную чётность.

Теорема 2. τ - транспозиция. Тогда $\#\sigma$ и $\#(\sigma\tau)$ имеют разную чётность.

Лемма. $\tau = (i\ \ i+1)$. Тогда $\#\tau$ и $\#(\sigma\tau)$ имеют разную чётность.

Теорема. Пусть $\sigma = \tau_1\ldots\tau_m, \quad \tau_i \in S_n,\ \tau_i$ - транспозиции.
Тогда три числа имеют одинаковую чётность:

$$\#\sigma \qquad l(\sigma) \qquad m$$

Следствие. $\sigma \in S_n,\ \tau$ - транспозиция. Тогда $\#\sigma$ и $\#\tau\sigma$ имеют разную чётность. И $l(\sigma)$и $l(\tau\sigma)$ имеют разную чётность.

Перестановка σ называется <u>**чётной**</u>, если выполнено любое из трёх равносильных условий:

1. σ - произведение чётного числа транспозиций.
2. $\#\sigma$ чётно.
3. $l(\sigma)$ чётно.

В противном случае перестановка **нечётная**.

Множество всех чётных перестановок в S_n обозначается за A_n.

Произведение чётных - чётно, произведение двух нечётных - чётно, произведение чётной и нечётной - нечётное. Обратная к чётной - чётна, к нечётной - нечётна.

Предложение. $A_n \leq S_n$.
Предложение. $|A_n| = \begin{cases} 1, & n = 1 \\ n! \cdot 1/2 & n > 1 \end{cases}$
