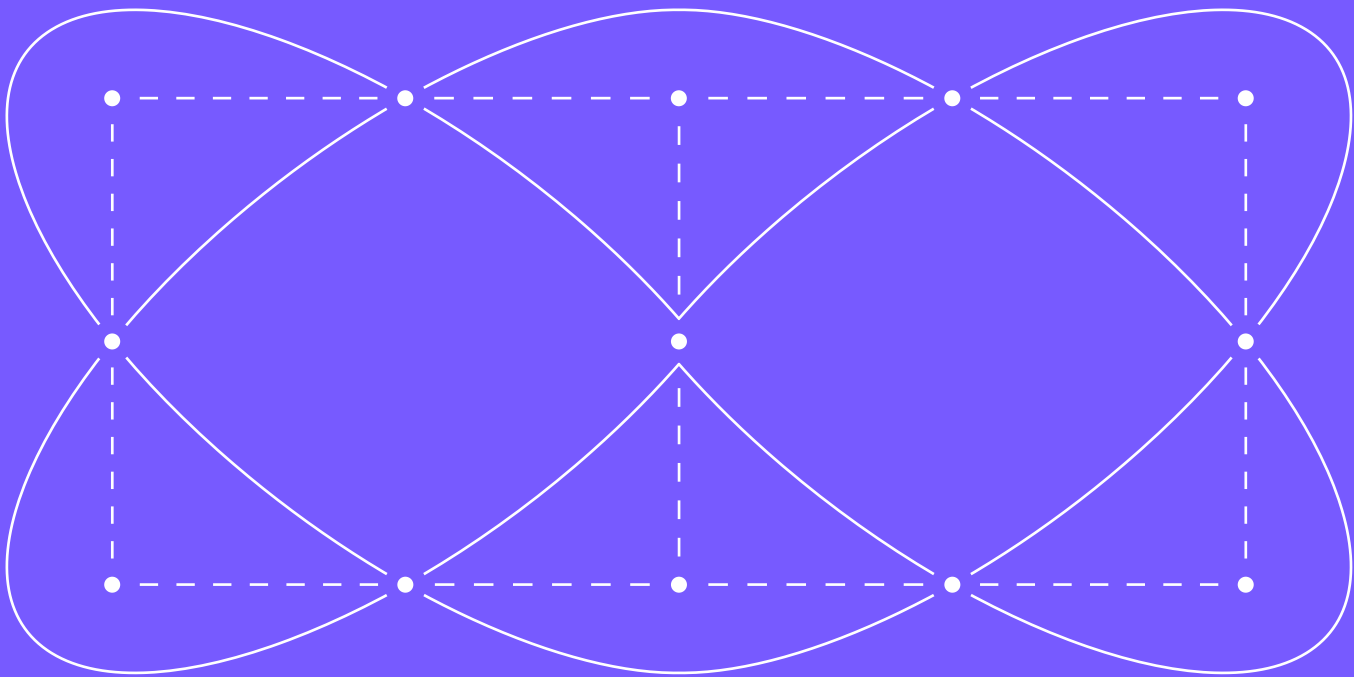
ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

Перестановки



ЛИНЕЙНАЯ АЛГЕБРА И ГЕОМЕТРИЯ

ЛОНГРИД

НЕДЕЛЯ 4

Перестановки

1. ОТОБРАЖЕНИЯ МНОЖЕСТВ

Пусть X,Y — некоторые множества, а $\varphi\colon X \to Y$ — отображение. Тогда φ называется *инъективным*, если оно «не склеивает точки», а именно: для любых $x, y \in X$ из условия $x \neq y$ следует, что $\varphi(x) \neq \varphi(y)$. Отображение φ называется *сюръективным*, если в любой элемент что-то переходит, то есть для любого $y \in Y$ существует $x \in X$ такой, что $\varphi(x) = y$. Отображение φ называется *биективным*, если оно одновременно инъективно и сюръективно[13].

Свойства отображения можно подчеркивать видом стрелки. Например, инъективное отображение обычно обозначается $\varphi\colon X \hookrightarrow Y$, сюръективное — $\varphi\colon X \twoheadrightarrow Y$, а биективное — $\varphi\colon X \xrightarrow{\sim} Y$.

Для любого множества X отображение $\mathrm{Id}\colon X \to X$, заданное по правилу $\mathrm{Id}(x) = x$, называется *тождественным*. Пусть $\varphi\colon X \to Y$ — некоторое отображение. Тогда $\psi\colon Y \to X$ называется *левым обратным* (соответственно *правым обратным*) к φ, если $\psi\varphi = \mathrm{Id}$ ($\varphi\psi = \mathrm{Id}$)[14]. Левых и правых обратных для φ может быть много. Однако если есть оба обратных и ψ_1 — левый обратный, а ψ_2 — правый обратный, то они совпадают, так как $\psi_1 = \psi_1(\varphi\psi_2) = (\psi_1\varphi)\psi_2 = \psi_2$. Следовательно, совпадают все левые обратные со всеми правыми, и такой единственный элемент называют *обратным* и обозначают φ^{-1}, а φ называют *обратимым*. Легко проверить следующее.

УТВЕРЖДЕНИЕ

Пусть $\varphi\colon X \to Y$ — некоторое отображение. Тогда:

1. φ инъективно тогда и только тогда, когда φ обладает левым обратным;
2. φ сюръективно тогда и только тогда, когда φ обладает правым обратным;
3. φ биективно тогда и только тогда, когда φ обратимо.

2. ПЕРЕСТАНОВКИ

ОПРЕДЕЛЕНИЕ 2

Пусть $X_n = \{1, \ldots, n\}$ — конечное множество из n занумерованных элементов[a]. *Перестановкой* называется биективное отображение $\sigma\colon X_n \to X_n$. Множество всех перестановок на n элементном множестве будем обозначать через S_n.

[a] Формально говоря, это множество из n элементов и фиксированный линейный порядок на нём.

Как задавать перестановки. Как только вам встречается новый объект, первый важный вопрос: как подобные объекты вообще задавать? Для перестановок есть три способа.

[13] В теории множеств: множества — это мешки с элементами, а отображения «сравнивают» эти мешки между собой. Биекция между множествами говорит, что это, по сути, одно и то же множество, но по-разному заданное. Поэтому на биекцию между X и Y можно смотреть не как на отображение между разными множествами, а как на правило, «переименовывающее» элементы на одном и том же множестве.

[14] Легко проверить, что существование левого обратного никак не связано с существованием правого обратного и наоборот.

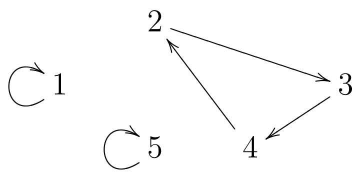
1. Задать стрелками соответствие на элементах.

$$\begin{tikzcd}
1 \arrow[d] & 2 \arrow[dr] & 3 \arrow[dr] & 4 \arrow[dll] & 5 \arrow[d] \\
1 & 2 & 3 & 4 & 5
\end{tikzcd}$$

2. С помощью таблицы значений (графика). Здесь под каждым элементом пишется его образ:

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

3. Графически в виде действия на элементах.



Все эти виды записи однозначно задают перестановку. Самым популярным методом в литературе является второй способ. В общем виде для перестановки $\sigma \in \mathrm{S}_n$ табличная запись выглядит следующим образом:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Заметим, что если записать элементы $1, \dots, n$ в другом порядке, скажем, $i_1, \dots, i_n$, то перестановка σ запишется в виде[15]

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_n) \end{pmatrix}.$$

Из однозначности табличной записи получаем следующее.

УТВЕРЖДЕНИЕ

Количество перестановок на n элементах есть $n!$, то есть $|\mathrm{S}_n| = n!$.

3. ОПЕРАЦИЯ НА ПЕРЕСТАНОВКАХ

Так как перестановки являются отображениями, а на отображениях есть операция композиции, то и на перестановках появляется операция. Пусть $\sigma, \tau \in \mathrm{S}_n$ — две произвольные перестановки, определим $\sigma\tau$ как композицию, а именно: $\sigma\tau(k) = \sigma(\tau(k))$. На языке диаграмм получаем следующее.

$$\begin{tikzcd}
X_n \arrow[r, "\tau"] \arrow[rr, bend right, "\sigma\tau"'] & X_n \arrow[r, "\sigma"] & X_n
\end{tikzcd}$$

Важно. Обратите внимание, что перестановки применяются к элементам справа налево. Это связано с тем, что они являются отображениями, а когда вы считаете композицию отображений, то вы сначала

[15] Заметим, что в этой записи можно произвольным образом перемешивать столбцы; это никак не изменит задаваемую перестановку.

применяете к аргументу самое правое, потом следующее за ним и так далее.

Давайте посмотрим, как выглядит произведение двух перестановок в табличной записи. Пусть даны перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \text{ и } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Тогда перестановки $\sigma\tau$ и $\tau\sigma$ имеют вид

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ и } \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Свойства умножения

- Если $\sigma, \tau, \rho \in \mathrm{S}_n$ — произвольные перестановки, то, как легко видеть по определению, $(\sigma\tau)\rho = \sigma(\tau\rho)$. Другими словами, в выражениях, составленных из перестановок и произведений, не важно, в каком порядке расставлять скобки. Поэтому скобки обычно опускаются.
- Умножение перестановок некоммутативно, то есть, вообще говоря, $\sigma\tau \neq \tau\sigma$[16].
- Тождественное отображение Id является нейтральным элементом для умножения перестановок в том смысле, что верно $\mathrm{Id}\,\sigma = \sigma\,\mathrm{Id} = \sigma$ для любой перестановки σ. В табличной записи Id имеет вид

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

- Обратное отображение к σ будем обозначать через σ^{-1}. Оно будет обратным элементом относительно операции в том смысле, что $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \mathrm{Id}$. В табличной записи обратное отображение можно записать так:

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

4. ПЕРЕИМЕНОВАНИЕ ЭЛЕМЕНТОВ

В нашем определении перестановка — это биекция на множестве X_n. Однако элементы X_n имеют конкретные имена — это числа от 1 до n. Что произойдёт, если мы сменим имена элементов? Как изменится табличная запись перестановки?

Вначале надо понять, что значит переименование элементов. Во-первых, у нас есть запас старых имён $\{1, \dots, n\}$, во-вторых, у нас должен быть список новых имён, скажем, $\{1, \dots, n\}$, и, в-третьих, у нас должно быть соответствие, которое по старым именам строит новые, то есть $\tau\colon \{1, \dots, n\} \to \{1, \dots, n\}$. Поэтому если мысленно убрать кавычки, то на переименование можно смотреть как на перестановку $\tau\colon X_n \to X_n$.

Пусть теперь у нас есть перестановка $\sigma\colon X_n \to X_n$. Её можно записать в табличном виде в старых и новых именах. Чтобы различать эти таблицы, мы будем использовать обозначения $\sigma_{\text{стар}}$ и $\sigma_{\text{нов}}$ для них

[16] Один пример мы уже видели, ещё один будет в разделе «Циклические перестановки».

соответственно. Тогда мы можем записать связь между ними с помощью следующей диаграммы.

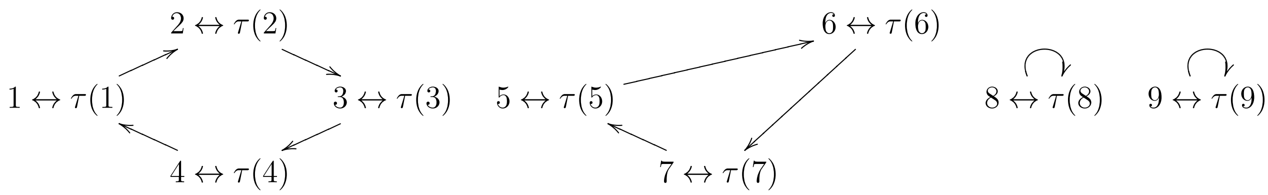
$$\begin{tikzcd} \{1,\ldots,n\} \arrow[r, "\tau"] \arrow[d, "\sigma_{\text{стар}}"'] & \{1,\ldots,n\} \arrow[d, "\sigma_{\text{нов}}"] \\ \{1,\ldots,n\} \arrow[r, "\tau"] & \{1,\ldots,n\} \end{tikzcd}$$

Если вспомнить, что $\{1,\ldots,n\} = \{\tau(1),\ldots,\tau(n)\}$, то действие $\sigma_{\text{нов}}$ в новых именах устроено так: мы берём произвольный элемент с новым именем $\tau(k)$, находим его старое имя — k, на старом имени можем подействовать $\sigma_{\text{стар}}$, которое есть $\sigma(k)$, а теперь надо найти новое имя для образа, что есть $\tau(\sigma(k))$.

Подытожим: $\sigma_{\text{нов}} = \tau\sigma_{\text{стар}}\tau^{-1}$. В табличной записи перестановки выглядят так:

$$\sigma_{\text{стар}} = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}, \quad \sigma_{\text{нов}} = \begin{pmatrix} \tau(1) & \tau(2) & \ldots & \tau(n) \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \ldots & \tau(\sigma(n)) \end{pmatrix}.$$

Хорошо ещё иметь перед глазами следующую картинку.



Здесь в вершинах подписаны и старые, и новые имена, а перестановка одна и та же.

5. ЦИКЛЫ

Пусть $\sigma \in \mathrm{S}_n$ действует следующим образом: для некоторого множества $i_1,\ldots,i_k$ ($k \geqslant 2$) выполнено

$$\sigma(i_1) = i_2,\ldots,\sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1,$$

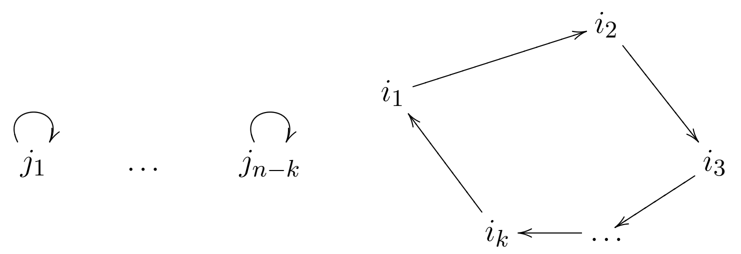
а все остальные элементы остаются на месте под действием σ. Тогда σ называется *циклом* длины k. Такая перестановка для краткости обозначается $(i_1,\ldots,i_k)$. Заметим, что такая запись не единственная: например, можно сказать, что $\sigma = (i_2,\ldots,i_k,i_1)$[17]. Стоит отметить, что если в определении выше выбрать $k = 1$, то перестановка, обозначаемая (i_1), совпадает с тождественной перестановкой. Следовательно, циклов длины 1 просто не существует. Однако в некоторых случаях сама запись (i_1) является удобным обозначением для единообразия в формулах. Поэтому такие «циклы» принято называть тривиальными (подразумевая не цикл, а обозначение), а настоящие циклы — нетривиальными.

Таблицей цикл задаётся следующим образом:

$$\begin{pmatrix} i_1 & \ldots & i_{k-1} & i_k & j_1 & \ldots & j_{n-k} \\ i_2 & \ldots & i_k & i_1 & j_1 & \ldots & j_{n-k} \end{pmatrix},$$

[17] Как легко видеть, другой неоднозначности в записи цикла нет.

где $\{1,\ldots,n\} = \{i_1,\ldots,i_k\} \sqcup \{j_1,\ldots,j_{n-k}\}$. Графически этот цикл выглядит так.



Цикл длины 2 называется *транспозицией*, то есть транспозиция (i,j) — это перестановка двух элементов i и j. Два цикла $(i_1,\ldots,i_k)$ и $(j_1,\ldots,j_m)$ называются *независимыми*, если множества $\{i_1,\ldots,i_k\}$ и $\{j_1,\ldots,j_m\}$ не пересекаются, а именно, множества действительно перемещаемых элементов не пересекаются. Заметим, что независимые циклы коммутируют друг с другом, а зависимые, вообще говоря, нет, как показывает следующий пример: $(1,2)(2,3) = (1,2,3)$, а $(2,3)(1,2) = (3,2,1)$[18,19].

УТВЕРЖДЕНИЕ 8

Пусть $\rho = (i_1,\ldots,i_k) \in \mathrm{S}_n$ — некоторый цикл длины k и $\tau \in \mathrm{S}_n$ — произвольная перестановка, тогда

$$\tau(i_1,\ldots,i_k)\tau^{-1} = (\tau(i_1),\ldots,\tau(i_k)).$$

ДОКАЗАТЕЛЬСТВО

Есть два способа понять это равенство. Первый — посмотреть на τ как на переименование элементов. Тогда справа написан цикл по элементам с новыми именами, а слева — правило переименования.

Второй способ — проверка в лоб. Надо проверить, что и левая, и правая часть одинаково действуют на всех элементах вида $\tau(i)$. Возьмем элемент $\tau(i_1)$, тогда правая часть его переводит в $\tau(i_2)$. Посмотрим, что с ним делает левая часть. Вначале мы переходим в i_1, потом в i_2, а потом в $\tau(i_2)$. Получили то же самое. Аналогично проверяется, что $\tau(i)$ остаётся на месте, если i не совпадает ни с одним из i_s.

Теперь мы готовы доказать структурный результат о перестановках.

УТВЕРЖДЕНИЕ 9

Пусть $\sigma \in \mathrm{S}_n$ — произвольная перестановка. Тогда выходит следующее.

1. Перестановку σ можно представить в виде $\sigma = \rho_1\ldots\rho_k$, где ρ_i — независимые циклы, причём это представление — единственное с точностью до перестановки сомножителей.
2. Пусть $\rho \in \mathrm{S}_n$ — произвольный цикл длины k, тогда его можно представить в виде $\rho = \tau_1\ldots\tau_{k-1}$, где τ_i — транспозиции[a].

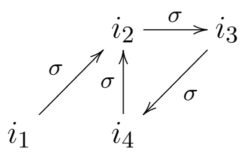
[a] Это представление уже не единственное.

ДОКАЗАТЕЛЬСТВО

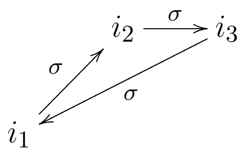
(1) Пусть $i_1 \in X_n$ — произвольный элемент. Подействуем на него σ, получим $i_2 = \sigma(i_1)$ и так далее. Так

[18] Проверьте это.
[19] Зависимые циклы могут коммутировать, например, $(1,2)$ коммутирует с $(1,2)$.

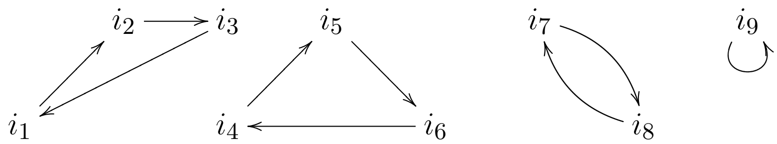
как X_n конечно, то мы в какой-то момент повторимся, например, $i_5 = i_2$, как на рисунке ниже.



На этой картинке видно, что $\sigma(i_1) = \sigma(i_4)$, но σ инъективно, поэтому $i_1 = i_4$. Тогда правильная картинка следующая.



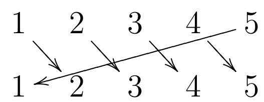
Далее возьмём элемент, который не попал на этот цикл, и повторим рассуждение для него. Так найдём другой цикл и так далее. В итоге картинка будет приблизительно такая.



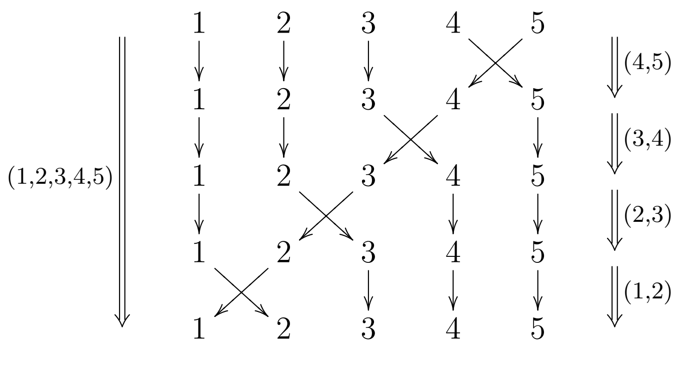
Значит, перестановка выше раскладывается в циклы $\sigma = (i_1, i_2, i_3)(i_4, i_5, i_6)(i_7, i_8)$[a].

Единственность такого разложения следует из метода пристального взгляда на картинку и наше рассуждение. Если нужно формальное объяснение, то нужно делать так. Пусть $\sigma = \rho_1 \ldots \rho_k$ и пусть $\rho_1 = (i_1, \ldots, i_s)$. Подействуем σ на элемент i_1. Так как циклы справа независимы, то только ρ_1 действует на i_1, следовательно, $\sigma(i_1) = \rho_1 \ldots \rho_k(i_1) = i_2$, то есть i_2 однозначно определено. Продолжая в том же духе, мы видим, что все циклы однозначно определяются через σ.

(2) Пусть цикл σ действует по правилу, как на картинке ниже.



Чтобы получить цикл длины k, нам необходимо применить $k - 1$ транспозиций. Другими словами, в нашем примере надо применить 4 транспозиции. Сделаем это следующим образом.



Тогда в общем случае $(1,2,\ldots,k) = (1,2)(2,3)\ldots(k-2,k-1)(k-1,k)$.

[a] Цикл (i_9) здесь не используется, так как он совпадает с тождественной перестановкой Id, как и любой другой цикл длины 1.

Давайте поймём, почему представление во втором случае не единственное. Рассмотрим перестановку

$(1,2)(2,3)$. Тогда

$$(1,2)(2,3) = (1,2)(2,3)(1,2)^{-1}(1,2) = (1,3)(1,2).$$

Здесь в первом равенстве мы поделили и домножили на $(1,2)$, а во втором воспользовались утверждением 8.

6. ЗНАК ПЕРЕСТАНОВКИ

Задача этого раздела — поделить все перестановки на два типа: «чётные» и «нечётные». При этом мы хотим, чтобы выполнялись обычные для чётности и нечётности правила при «умножении», а именно

$$\begin{aligned} &\text{«чётная»} \cdot \text{«чётная»} = \text{«чётная»}, &&\text{«чётная»} \cdot \text{«нечётная»} = \text{«нечётная»}, \\ &\text{«нечётная»} \cdot \text{«чётная»} = \text{«нечётная»}, &&\text{«нечётная»} \cdot \text{«нечётная»} = \text{«чётная»}. \end{aligned}$$

Такое разделение можно сделать с помощью специальной функции, называемой знаком. Такая функция принимает на всех чётных перестановках значение 1, а на всех нечётных — -1:

$$\operatorname{sgn}\colon \mathrm{S}_n \to \{\pm 1\}.$$

Чтобы выполнялось условие на поведение чётности и нечётности при произведении перестановок, нам достаточно потребовать следующее свойство:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$

для всех возможных $\sigma, \tau \in \mathrm{S}_n$. Оказывается, что существует единственный способ разбить перестановки на чётные и нечётные с выполнением свойства на произведение. Однако мы не будем доказывать единственность. Вместо этого мы просто построим отображение sgn и научимся им пользоваться.

В этом случае такое отображение обозначается $\operatorname{sgn}\colon \mathrm{S}_n \to \{\pm 1\}$ и называется знаком. Значение $\operatorname{sgn}(\sigma)$ называется знаком перестановки $\sigma \in \mathrm{S}_n$. Перестановка называется чётной, если знак 1, и нечётной, если -1. Вначале определим вспомогательную характеристику $d(\sigma)$ следующим образом.

ОПРЕДЕЛЕНИЕ 3

Пусть $\sigma \in \mathrm{S}_n$ — некоторая перестановка и $i, j \in X_n$ — НЕупорядоченная пара различных элементов[a]. Тогда эта пара называется *инверсией*, если «σ меняет характер монотонности», то есть $i < j$ влечёт $\sigma(i) > \sigma(j)$, а $i > j$ влечёт $\sigma(i) < \sigma(j)$. При использовании записи перестановки в виде

$$\begin{tikzcd} 1 \arrow[d] & 2 \arrow[dr] & 3 \arrow[dr] & 4 \arrow[dll] & 5 \arrow[d] \\ 1 & 2 & 3 & 4 & 5 \end{tikzcd}$$

инверсия соответствует пересечению стрелок. Определим число $d_{ij}(\sigma) = 1$, если пара i, j образует инверсию, и 0, если не образует. Тогда число всех инверсий для всевозможных пар — это $d(\sigma) = \sum_{i<j} d_{ij}(\sigma)$.

[a] То есть пару i, j и j, i мы считаем одной и той же.

ОПРЕДЕЛЕНИЕ 4

> Пусть $\sigma \in \mathrm{S}_n$ — некоторая перестановка. Определим знак перестановки σ по правилу $\operatorname{sgn}(\sigma) = (-1)^{d(\sigma)}$.

Теперь покажем, что знак перестановки согласован с произведением.

УТВЕРЖДЕНИЕ 10

Пусть $\sigma,\tau \in \mathrm{S}_n$ — произвольные перестановки, тогда

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

ДОКАЗАТЕЛЬСТВО

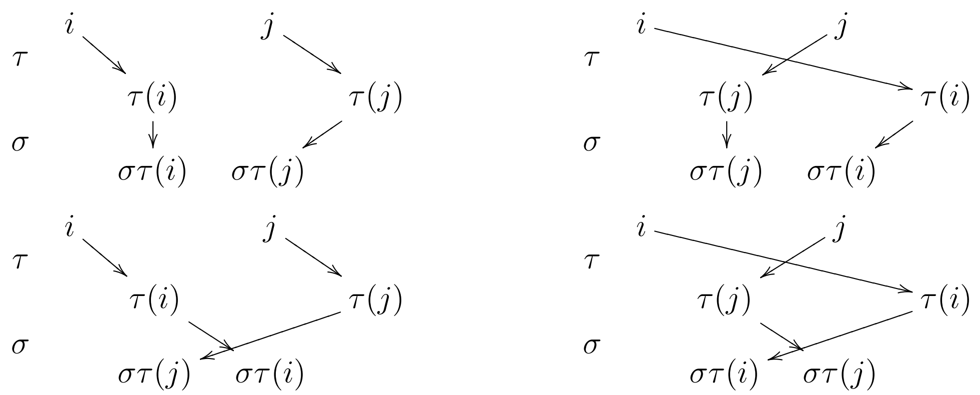
Для доказательства нам надо показать, что

$$d(\sigma) + d(\tau) = d(\sigma\tau) \pmod 2.$$

Давайте зафиксируем пару i, j и докажем следующее равенство[a]

$$d_{ij}(\tau) + d_{\tau(i)\tau(j)}(\sigma) = d_{ij}(\sigma\tau) \pmod 2.$$

Возможны следующие 4 случая.



Занесём результаты в таблицу.

$d_{ij}(\tau)$	0	1	0	1
$d_{\tau(i)\tau(j)}(\sigma)$	0	0	1	1
$d_{ij} + d_{\tau(i)\tau(j)}(\sigma)$	0	1	1	2
$d_{ij}(\sigma\tau)$	0	1	1	0

Это и доказывает равенство

$$d_{ij}(\tau) + d_{\tau(i)\tau(j)}(\sigma) = d_{ij}(\sigma\tau) \pmod 2.$$

Теперь сложим его для всех пар $i < j$. Получим

$$\sum_{i<j} d_{ij}(\tau) + \sum_{i<j} d_{\tau(i)\tau(j)}(\sigma) = \sum_{i<j} d_{ij}(\sigma\tau) \pmod 2.$$

Отсюда

$$d(\tau) + \sum_{i<j} d_{\tau(i)\tau(j)}(\sigma) = d(\sigma\tau) \pmod 2.$$

Так как $\tau \colon X_n \to X_n$ — биекция, то, если (i,j) пробегает все разные пары, $(\tau(i), \tau(j))$ пробегает все разные пары. Значит, оставшаяся сумма равна $d(\sigma)$, что завершает доказательство.

[a]Указанное равенство по модулю 2 означает, что чётность левой и правой части равенства одинаковая.

Вычисление знака. Давайте вначале вычислим знаки в специальном случае.

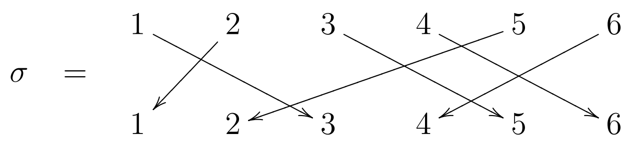
УТВЕРЖДЕНИЕ 11

Следующие свойства знака выполнены:

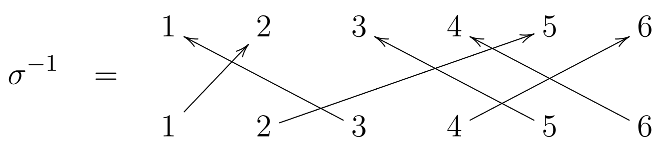
1. $\operatorname{sgn}(\mathrm{Id}) = 1$;
2. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$;
3. для любой транспозиции $\tau = (i, j)$ выполнено
$$\operatorname{sgn}(\tau) = -1;$$
4. для любого цикла $\rho = (i_1, i_2, \ldots, i_k)$ длины k верно
$$\operatorname{sgn}(\rho) = (-1)^{k-1}.$$

ДОКАЗАТЕЛЬСТВО

1. Ясно, что у тождественной перестановки нет инверсий, то есть $d(\mathrm{Id}) = 0$, а значит, $\operatorname{sgn}(\mathrm{Id}) = 1$.
2. По определению пара i, j образует инверсию в σ тогда и только тогда, когда пара $\sigma(i), \sigma(j)$ образует инверсию в σ^{-1}. Значит, $d(\sigma) = d(\sigma^{-1})$. Однако это доказательство не очень наглядное. Давайте я покажу, как это представлять себе графически. Давайте я возьму конкретный пример перестановки.



Тогда $d(\sigma)$ — количество пересечения стрелок в этом представлении. Например, в указанном примере всего 6 пересечений. Однако диаграмма для σ^{-1} получается лишь обращением стрелок.



Это значит, что у нас те же самые стрелки, которые обращены в другую сторону, следовательно, и количество пересечений будет такое же.
3. Вначале заметим, что для транспозиции $(1, 2)$

значение $d(1,2) = 1$. Отсюда получаем, что $\operatorname{sgn}(1,2) = -1$.

Теперь докажем, что для любой транспозиции (i,j) верно $\operatorname{sgn}(i,j) = -1$. Для этого выберем любую перестановку $\tau \in \mathrm{S}_n$ такую, что $\tau(1) = i$ и $\tau(2) = j$, а на остальных элементах она действует как угодно. Тогда из правила переименования имеем

$$(i,j) = \tau(1,2)\tau^{-1}.$$

Значит:

$$\operatorname{sgn}(i,j) = \operatorname{sgn}(\tau)\operatorname{sgn}(1,2)\operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\tau)(-1)\operatorname{sgn}(\tau) = (-1)\operatorname{sgn}(\tau)^2 = -1.$$

4. Если ρ — цикл длины k, то, по утверждению 9, он представляется в виде произведения $k-1$ транспозиций:
$$\rho = (i_1, i_2, \ldots, i_k) = (i_1, i_2)(i_2, i_3)\ldots(i_{k-1}, i_k).$$
Но тогда
$$\operatorname{sgn}(\rho) = \operatorname{sgn}(i_1, i_2)\operatorname{sgn}(i_2, i_3)\ldots\operatorname{sgn}(i_{k-1}, i_k) = (-1)^{k-1},$$
что и требовалось доказать.

Для перестановки $\sigma \in \mathrm{S}_n$ вычисление $d(\sigma)$ занимает $\frac{n(n-1)}{2}$ операций — это долго. Так вычислять знак стоит не всегда. Если воспользоваться утверждением 9, то можно разложить любую перестановку в произведение независимых циклов
$$\sigma = \rho_1 \cdot \ldots \cdot \rho_k,$$

после чего знак σ вычисляется как произведение знаков её циклов. Однако знак цикла легко определяется по его длине, как сказано в предыдущем утверждении. Это на практике даёт более удобный способ вычислять знак.