Группы. Первое знакомство.

Пример 1. Самосовмещения правильного треугольника.

Дан равносторонний треугольник ABC. Какие движения плоскости переводят его в себя? Мы уже умеем решать эту задачу. Во-первых, это Id, преобразование, которое "ничего не делает". Во-вторых, это R^+ и R^-, повороты вокруг центра треугольника на 120° по часовой стрелке и против часовой стрелки. Ну и в-третьих, осевые симметрии относительно каждой из трёх биссектрис — S_a, S_b и S_c.

Есть ли другие движения? Чтобы попытаться найти их, вспомним, что композиция движений — это новое движение. С помощью композиции из двух движений можно сконструировать третье. Так, применяя последовательно сдвиг и осевую симметрию, мы получили в своё время скользящую симметрию. Пробуем: $S_a \circ S_a = Id$, $S_a \circ S_b = R^+$, $R^+ \circ S_a = S_c$, $R^+ \circ R^+ = R^-$, ... ничего нового не выходит.

Может хоть какие-то композиции дадут новые движения? Нет, увы, можно скрупулёзно выписать в таблицу все композиции — ничего нового не получается, мы топчемся на месте.

	Id	S_a	S_b	S_c	R^+	R^-
Id	Id	S_a	S_b	S_c	R^+	R^-
S_a	S_a	Id	R^+	R^-	S_b	S_c
S_b	S_b	R^-	Id	R^+	S_a	S_b
S_c	S_c	R^+	R^-	Id	S_a	S_b
R^+	R^+	S_c	S_a	S_b	R^-	Id
R^-	R^-	S_b	S_c	S_a	Id	R^+

То есть, либо ничего больше не существует, либо есть какие-то ещё движения, которые никак не связаны с найденными. Окончательно поставить точку в этом вопросе может помочь, например, теорема Шаля: любое движение является сдвигом, поворотом или скользящей симметрией. Но есть другой путь: попробуем последить за вершинами треугольника. Пусть при движении вершины A и B перешли в A_1 и B_1 соответственно. Поскольку $A_1B_1 = AB$, то A_1 и B_1 — какие-то вершины треугольника — расстояние, равное стороне, может быть только между вершинами. Отсюда вывод: при движении вершина переходит в вершину. Далее вспоминаем теорему из курса геометрии — всякое движение определяется образами трёх точек. То есть движений никак не больше, чем возможных образов трёх вершин. Теперь самое время обратиться к следующему примеру.

Пример 2. Перестановки из трёх элементов.

Рассмотрим всевозможные перестановки из трёх элементов. Их, как известно, ровно шесть: $[1,2,3]$, $[1,3,2]$, $[3,2,1]$, $[2,1,3]$, $[2,3,1]$, $[3,1,2]$.

Перестановки, как вы уже знаете, можно умножать, выполняя последовательно, например $[2,3,1]\cdot[3,2,1] = [2,1,3]$.

Понятно, что при перемножении перестановок получается новая перестановка. Мы опять имеем шесть объектов, которые можно умножать, получая снова один из этих шести.

	[123]	[132]	[321]	[213]	[231]	[312]
[123]	[123]	[132]	[321]	[213]	[231]	[312]
[132]	[132]	[123]	[231]	[312]	[321]	[213]
[321]	[321]	[312]	[123]	[231]	[213]	[132]
[213]	[213]	[231]	[312]	[123]	[132]	[321]
[231]	[231]	[213]	[132]	[321]	[312]	[123]
[312]	[312]	[321]	[213]	[132]	[123]	[231]

Между самосовмещениями треугольника и перестановками есть много параллелей. Аналогом Id служит $[1, 2, 3]$, её композиция с любым элементом не отражается на последнем. Композиция симметрий с самими собой равна Id, среди перестановок таковы три транспозиции. И так далее. Можно отождествить между собой перестановки и движения треугольника так, чтобы таблицы совпали.

Это можно сделать естественно, так, что проверка тождественности не составит труда. Каждому движению поставим в соответствие перестановку вершин треугольника, которую оно осуществляет. Например, Id это $[A, B, C]$, S_a это $[A, C, B]$ и так далее. Понятно, что композиция преобразований соответствует композиции перестановок. А движений оказалось ровно шесть — перестановок-то больше нет.

Пример 3. Алгебраическая магия.

Забудем про треугольник и перестановки и зайдём на урок алгебры в 9 класс. Что это они там делают? А-а, дробно-линейную функцию изучают!

Рассмотрим несколько функций: $f(x) = x$, $g(x) = 1 - x$, $h(x) = \frac{1}{x}$. Попробуем получить из них новые функции методом подстановки: будем рассматривать $g \circ f$ как $g(f(x))$. Вот что у нас получается:

$f \circ g = 1 - x = g$,

$g \circ f = 1 - x = g$,

$f \circ h = \frac{1}{x} = h$,

$h \circ f = \frac{1}{x} = h$.

Пока ничего интересного. Попробуем умножать функцию саму на себя:

$g \circ g = 1 - (1 - x) = x = f$,

$h \circ h = \frac{1}{1/x} = x = f$.

Ах, да, мы ещё g и h не перемножали:

$h \circ g = \frac{1}{1-x}$,

$g \circ h = 1 - \frac{1}{x} = \frac{x-1}{x}$.

О, что-то новенькое. Вводим в оборот две новые функции: $p(x) = \frac{1}{1-x}$ и $q(x) = \frac{x-1}{x}$. Поэкспериментируем:

$q \circ p = \frac{\frac{1}{1-x}-1}{\frac{1}{1-x}} = x = f$,

$p \circ p = \frac{1}{1-\frac{1}{1-x}} = \frac{x-1}{x} = q$,

$q \circ q = \frac{\frac{x-1}{x}-1}{\frac{x-1}{x}} = \frac{1}{1-x} = p$.

Новых функций не получается. Попробуем ещё:

$p \circ h = \frac{1}{1-\frac{1}{x}} = \frac{x}{x-1}$.

Этого ещё не было. Шестая функция в нашей коллекции. Обозначим её $k(x) = \frac{x}{x-1}$. Сколько новых функций получится комбинированием этих шести?

А нисколько. Ничего нового не получится. Например,
$q \circ k = \frac{\frac{x}{x-1}-1}{\frac{x}{x-1}} = \frac{1}{x} = h$ и так далее. Вот полная таблица:

	f	h	g	k	p	q
f	f	h	g	k	p	q
h	h	f	p	q	g	k
g	g	q	f	p	k	h
k	k	p	q	f	h	g
p	p	k	h	g	q	f
q	q	g	k	h	f	p

Таблица очень похожа на умножение перестановок. Но какая связь между функциями и перестановками? О, более чем мистическая!

Рассмотрим набор чисел: $\left(-1\,;\,\frac{1}{2}\,;\,2\right)$. Как его изменит функция f? Правильно, никак:
$f : \left(-1\,;\,\frac{1}{2}\,;\,2\right) \longrightarrow \left(-1\,;\,\frac{1}{2}\,;\,2\right)$.

А остальные функции?

$g : \left(-1\,;\,\frac{1}{2}\,;\,2\right) \longrightarrow \left(2\,;\,\frac{1}{2}\,;\,-1\right)$,
$h : \left(-1\,;\,\frac{1}{2}\,;\,2\right) \longrightarrow \left(-1\,;\,2\,;\,\frac{1}{2}\right)$,
$k : \left(-1\,;\,\frac{1}{2}\,;\,2\right) \longrightarrow \left(\frac{1}{2}\,;\,-1\,;\,2\right)$,
$q : \left(-1\,;\,\frac{1}{2}\,;\,2\right) \longrightarrow \left(2\,;\,-1\,;\,\frac{1}{2}\right)$,
$p : \left(-1\,;\,\frac{1}{2}\,;\,2\right) \longrightarrow \left(\frac{1}{2}\,;\,2\,;\,-1\right)$.

Теперь всё становится ясно.

Группа.

Мы рассмотрели три набора из шести объектов. В каждом наборе объекты можно было "перемножать", получая новые объекты того же набора. Наверное, вы заметили, что порядок сомножителей был важен. Объекты были различны, но их перемножение было устроено схожим образом, создавая в каждом множестве одну и ту же структуру.

Оказалось, что такую структуру интересно изучать безотносительно к природе самих объектов. Если сконцентрировать внимание только на свойствах "умножения", мы отчётливо увидим свойства, которые иначе бы затерялись среди частных подробностей.

Допустим, задано множество G и операция "умножения", сопоставляющая двум его элементам третий (это записывается как $a * b = c$ или просто как $ab = c$).

1. Пусть умножение ассоциативно, то есть $a(bc) = (ab)c$.

2. Пусть также среди элементов G есть такой, умножение на который не изменяет множимое: $ea = ae = a$. Такой элемент называется ***нейтральным*** или ***единицей*** и обозначается e, как уже написано выше.

3. Пусть, наконец, для всякого $a \in G$ найдётся $b \in G$, что $ab = ba = e$. Такой b называется ***обратным*** к a и обозначается a^{-1}.

При соблюдений этих трёх условий говорят, что G — ***группа*** с заданной операцией умножения.

Это определение чуть избыточно, зато с ним удобно работать.

Нетрудно проверить, что во всех трёх примерах возникала группа, причём в некотором смысле "одна и та же".

Изоморфные группы.

Группы G и G' ***изоморфны***, если между ними можно установить биекцию так, что произведению элементов одной группы соответствует произведение их образов. Иногда просто говорят, что это одна и та же группа.

Рассмотрим для примера другую группу из шести элементов — чисел 0, 1, 2, 3, 4, 5. Умножением будем считать сложение по модулю 6. Нетрудно проверить, что это группа. Единицей здесь служит 0, пары взаимно-обратных элементов 1 — 5, 2 — 4, 3 — 3, ну и 0 — 0. Изоморфна ли она ранее рассмотренной группе перестановок? Нет, хотя бы потому, что умножение в ней коммутативно, а в перестановках это не всегда так. Группы, в которых умножение коммутативно, называют ***коммутативными***, или ***абелевыми***, в честь норвежского математика Нильса Хенрика Абеля.

А вот ещё пример: числа 1, 2, 3, 4, 5, 6. Умножением будет умножение по модулю 7. Это группа? Если группа, то, конечно, абелева, поэтому не изоморфна группе перестановок. А группе остатков по сложению изоморфна?

Оставим пока эти вопросы без ответа.