

# Геометрическая алгебра

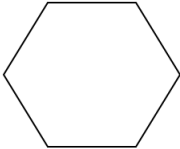
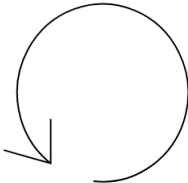
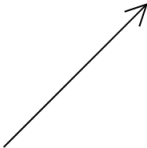
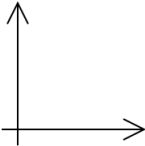
	<p>Базис группы движений:</p> <p>1 симметрия + все повороты</p>	<p>конечные группы</p>	<p>понятие группы, базиса</p>
	<p>Базис группы движений:</p> <p>1 симметрия + все повороты</p>	<p>конечные группы, группы типа <math>\mathbb{Z}</math> по сложению</p>	<p>число пи и арифметика остатков <math>\mathbb{Z}/n\mathbb{Z}</math></p>
	<p>Базис группы движений:</p> <p>1 симметрия + все сдвиги</p>	<p>группы типа <math>\mathbb{Z}, \mathbb{R}</math> по сложению</p>	<p>гомотетии и кольцо <math>(\mathbb{R}, +, \times)</math></p>
	<p>Базис группы движений:</p> <p>1 симметрия + все переносы + все повороты</p>	<p>группа типа <math>\mathbb{C}</math> по сложению, группа корней из 1</p>	<p>поворотные гомотетии и кольцо <math>(\mathbb{C}, +, \times)</math> число e</p>
<p>Евклидовы кольца</p>	<p>Норма и деление с остатком, алгоритм Евклида</p>	<p>ОТА</p>	<p>числа Гаусса и Эйзенштейна</p>

Рис. 1.1: Вехи арифметики.

## 1.1 Натуральные числа

---

### Аннотация.

Цель: на основе геометрических понятий выйти на арифметику Пеано.

---

Предположим, что мы находимся в рамках стандартной планиметрии Евклида, т.е. умеем оперировать точками, прямыми, отрезками, отличаем неравные точки и неконгруентные отрезки (т.е. такие, которые нельзя совместить движением). При этом нам не дана метрика, т.е. мы не умеем вычислять расстояния между точками.

Будем говорить, что отрезок нулевой, только в том случае, когда его конечные точки совпадают.

Кроме того, мы отличаем понятия равенства и конгруентности отрезков. У равных отрезков совпадают концы (соответствующие точки равны), а у конгруентных — не обязательно, но их всегда можно совместить движением. При этом, как само понятие «движение», так и возможность проверки конгруентности отрезков, мы считаем интуитивно понятными постольку, поскольку это представляется возможным в рамках школьной аксиоматики Евклида.

Наконец, мы считаем интуитивно понятным отношение «лежать между» для трех точек, т.е. когда одна точка является внутренней точкой отрезка, соединяющего две другие точки.

### 1.1.1 Построение модели

Одна из аксиом геометрии Евклида говорит о том, что от любой точки в любом заданном направлении можно отложить данный отрезок (аксиома о построении окружности и, как следствие, отрезка заданной длины на прямой, проходящей через центр этой окружности).

Возьмем какой-нибудь мерный ненулевой отрезок  $AB$ , какую-нибудь прямую  $l$  и произвольную точку  $O$  на ней. Кроме того, определим направление на этой прямой, задав на ней еще одну точку  $Q$ , не равную  $O$ .

Следуя упомянутой аксиоме Евклида, отложим на прямой  $l$  от точки  $O$  отрезок  $OC$ , конгруентный  $AB$ , в направлении  $QO$ , т.е. таким образом, чтобы точка  $O$  оказалась между  $Q$  и новой точкой  $C$ . Для дальнейшего удобства точку  $C$  обозначим  $O^+$ , а отрезок  $OO^+$  обозначим символом  $s$ . Очевидно, что он ненулевой, т.к. отрезок  $AB$  ненулевой.

Продолжим процедуру откладывания отрезка  $AB$  на той же прямой в том же направлении, только теперь от точки  $O^+$ . Снова получим точку  $C$  (символ  $C$  мы используем как итеративную переменную) такую, что  $O^+C$  конгруентно  $AB$ . Полученную точку  $C$  обозначим  $O^{++}$ , а отрезок  $OO^{++}$  обозначим  $ss$ . Будем продолжать эту процедуру неограниченно постольку, поскольку это

позволяют аксиомы Евклида. В результате получим бесконечно много точек и отрезков:

$$O, O^+, O^{++}, O^{+++}, \dots, \quad OO, OO^+ = s, OO^{++} = ss, OO^{+++} = sss, \dots$$

Полученные отрезки будем называть  $s$ -отрезками. Кроме того, обозначим через  $\Lambda$  нулевой отрезок  $OO$ , полностью сосредоточенный в точке  $O$ . Символ  $\Lambda$  обозначает пустой символ, его можно выбрасывать и добавлять в любой записи отрезка в начале без потери семантики. Т.е.  $\Lambda ssss = ssss$  и т.п. (сравните с записью ведущего нуля у чисел).

Заметим, что каждый следующий  $s$ -отрезок содержит в себе все предыдущие, включая нулевой отрезок  $\Lambda$ , кроме того, всякий ненулевой  $s$  отрезок имеет запись вида  $xs$ , где  $x$  есть какой-то  $s$ -отрезок. В то же время, очевидно, что  $\Lambda$  не может быть записан как  $xs$  ни при каком  $x$ .

Два  $s$ -отрезка равны тогда и только тогда, когда они конгруэнтны, поскольку они имеют общее начало (точку  $O$ ) и общее направление на прямой  $l$ .

Далее определим операцию сложения  $s$ -отрезков следующим образом:

$$x + y = \begin{cases} x, & \text{если } y = \Lambda, \\ (x + z)s, & \text{если } y = zs \end{cases}$$

Поскольку это определение рекурсивное, нетрудно заметить, что сложение отрезков — это откладывание второго отрезка от первого. Например,

$$ss + sss = (ss + ss)s = ((ss + s)s)s = (((ss + \Lambda)s)s)s = (((ss)s)s)s = sssss.$$

Иначе говоря, сложению отрезков соответствует конкатенация (склейка) их записей. Отсюда, в частности, легко видеть, что  $x + s = xs$  (не путаем конкатенацию с умножением!), так что в дальнейшем приписывание суффикса  $s$  всюду будем заменять прибавлением отрезка  $s$ .

Аналогично определим умножение отрезков:

$$x \times y = \begin{cases} \Lambda, & \text{если } y = \Lambda, \\ (x \times z) + x, & \text{если } y = z + s \end{cases}$$

Например,

$$sss \times ss = (sss \times s) + sss = ((sss \times \Lambda) + sss) + sss = (\Lambda + sss) + sss = ssssss,$$

т.е. умножение отрезков соответствует репликации первой записи столько раз, сколько букв  $s$  во второй записи.

Умножение можно интерпретировать следующим образом. Над каждым  $s$ -отрезком восстановим прямоугольник высоты в один отрезок  $s$ , так что отрезку  $ss \dots s$  соответствует прямоугольник  $ss \dots s \times s$ . Такой прямоугольник

мы считаем базовым умножением, т.е. умножением на мерную единицу  $AB$ , или на отрезок  $s$ . Далее, умножение на  $ss$  означает, что над прямоугольником  $ss \dots s \times s$  мы восстанавливаем еще один такой же прямоугольник, и в итоге получаем уже новый прямоугольник  $ss \dots s \times ss$ . И так, с каждым новым увеличением множителя надстраиваем очередной прямоугольник, получая все БОЛЬШИЕ прямоугольники. Количество букв  $s$  в результирующей записи произведения при этом будет равно количеству единичных квадратов в таком прямоугольнике.

Определенные на  $s$ -отрезках сложение и умножение обладают следующими свойствами:

I  $\Lambda \neq x + s$  ни при каком  $s$ -отрезке  $x$ ;

II если  $x + s = y + s$ , то  $x = y$ ;

III  $x + \Lambda = x$ ;

IV  $x + (z + s) = (x + z) + s$ ;

V  $x \times \Lambda = \Lambda$ ;

VI  $x \times (z + s) = (x \times z) + x$ ;

VII для любого одноместного предиката  $P$ : если  $P(\Lambda) \wedge (\forall x P(x) \rightarrow P(x + s))$ , то  $\forall x P(x)$  (принцип индукции).

В самом деле, первое свойство говорит о том, что никакой отрезок, содержащий в себе единичный, не является нулевым, а это очевидно из геометрических построений. Второе свойство также очевидно из построения, поскольку отбрасывание у равных отрезков (не просто конгруэнтных, а равных!) равных же частей с одной и той же стороны, приводит к равным же отрезкам (просто в силу геометрических построений). Следующие четыре свойства есть повторение определения операций сложения и умножения.

Наконец, последнее свойство (принцип индукции) также довольно очевидно, поскольку оно приводит к цепочке силлогизмов:

$$P(\Lambda) \rightarrow P(s) \rightarrow P(ss) \rightarrow P(sss) \rightarrow P(ssss) \rightarrow \dots,$$

которая не может оборваться ни на каком  $s$ -отрезке, иначе это сразу привело бы к противоречию с условием индуктивного перехода. Существенным местом в данном рассуждении является то, что каждый ненулевой  $s$ -отрезок  $z$  есть композиция вида  $x + s$ , а значит, если  $P(z)$  неверно, то неверно и  $P(x)$ , и т.д., пока не будут исчерпаны все  $s$  и мы не дойдем до нулевого отрезка, а для него по условию  $P$  истинно.

Перечисленные выше семь свойств  $s$ -отрезков иллюстрируют выполнение в данной модели аксиом Пеано для натуральных чисел.<sup>1</sup>

## 1.1.2 Свойства сложения и умножения

Определения операций сложений и умножения отрезков, приведенные выше (как и соответствующие им аксиомы Пеано), позволяют получить стандартный набор алгебраических свойств.

**Теорема 1.1** (Свойства суммы). *Для любых  $s$ -отрезков  $x, y, z$*

*S1  $(x + y) + z = x + (y + z)$  (ассоциативность);*

*S2  $x + \Lambda = x = \Lambda + x$  (нейтральный элемент);*

*S3  $x + y = y + x$  (коммутативность);*

*S4 если  $x + z = y + z$ , то  $x = y$  (правило сокращения);*

*S5 либо  $x = \Lambda$ , либо  $x = y + s$  при некотором  $y$  (дихотомия);*

*S6 если  $x + y = \Lambda$ , то  $x = \Lambda$  и  $y = \Lambda$  (принцип мажоритарности);*

*S7 верно одно и только одно: либо  $x = y$ , либо  $x = y + z$ , либо  $x + z = y$  при некотором  $z \neq \Lambda$  (трихотомия).*

*Доказательство.* 1) Ассоциативность доказывается индукцией по  $z$ . Ясно, что при  $z = \Lambda$  это равенство верно. Предполагая, что оно верно при некотором  $z$ , покажем его при  $z + s$ :

$$(x+y)+(z+s) = ((x+y)+z)+s = (x+(y+z))+s = x+((y+z)+s) = x+(y+(z+s)).$$

2) Нейтральность  $\Lambda$  слева также доказывается индуктивно: предполагая  $\Lambda + X = X$ , имеем

$$\Lambda + (x + s) = (\Lambda + x) + s = x + s.$$

3) Коммутативность докажем двойной индукцией сначала по  $y$  и затем по  $x$  (равенство при  $y = \Lambda$  следует из предыдущего свойства). Внешний шаг индукции: предполагаем, что для любого  $x$ :  $x + y = y + x$ , и доказываем, что  $x + (y + s) = (y + s) + x$  для данного  $y$  и при любом  $x$ .

---

<sup>1</sup>ВНИМАНИЕ: это не означает, что в стандартную геометрию можно погрузить арифметику, дело в том, что уже при построении  $s$ -отрезков мы неявно пользовались рекурсией, которая никак не постулируется в аксиомах геометрии! И, по большому счету, рекурсия возможна постольку, поскольку возможна индукция, и наоборот.

Покажем это индукцией по  $x$ . Очевидно, что при  $x = \Lambda$  это верно. Внутренний шаг индукции: предполагаем, что  $x + (y + s) = (y + s) + x$  для данного  $y$  и данного  $x$ , и доказываем, что  $(x + s) + (y + s) = (y + s) + (x + s)$ .

Итак, пользуясь обоими предположениями и ассоциативностью, получаем:

$$\begin{aligned}(x + s) + (y + s) &= ((x + s) + y) + s = (x + (s + y)) + s = \\ &= (x + (y + s)) + s = ((y + s) + x) + s = (y + s) + (x + s),\end{aligned}$$

что завершает внутреннюю индукцию, и вместе с тем завершает и внешнюю.

4) Докажем правило сокращения. Ясно, что при  $z = \Lambda$  оно верно. Предполагая его справедливость для  $z$ , покажем его для  $z + s$ . Пусть  $x + (z + s) = y + (z + s)$ . Это равносильно  $(x + z) + s = (y + z) + s$ , откуда по аксиоме P2 получаем, что  $x + z = y + z$ , а отсюда уже в силу индуктивного предположения получаем  $x = y$ .

Из правила сокращения, в частности, следует, что если  $y \neq \Lambda$ , то  $x + y \neq x$ .

5) Правило дихотомии уже отмечалось выше как очевидное, но и его можно вывести индукцией по  $x$  из аксиом Пеано. Действительно, если  $x = \Lambda$ , то правило истинно. Предполагая, что оно верно для  $x$ , для  $x + s$  оно следует автоматически.

6) Из правила дихотомии сразу же следует принцип мажоритарности: если допустить, что  $x \neq \Lambda$ , то  $x = z + s$  при каком-то  $z$ , откуда  $x + y = y + z + s$ , что не может быть равно  $\Lambda$ . Аналогично — в случае предположения  $y \neq \Lambda$ .

7) Покажем правило трихотомии. Легко видеть, что никакие два случая трихотомии не могут выполняться. Действительно, если  $x = y$  и  $x = y + z$  ( $z \neq \Lambda$ ), то  $y = y + z$ , что противоречит правилу сокращения. Аналогично, если  $x = y$  и  $x + z = y$ , то  $x = x + z$ , что невозможно. Наконец, если  $x = y + z$  и  $x + z' = y$ , то  $x = x + z + z'$ , что также невозможно по принципу мажоритарности.

Покажем, что хотя бы один случай должен выполняться, индукцией по  $y$ . Нам нужно вывести истинность предиката  $P(y)$ :

$$\forall x (x = y) \vee (\exists z \neq \Lambda x = y + z) \vee (\exists z \neq \Lambda x + z = y).$$

Ясно, что при  $y = \Lambda$  это верно, т.к. либо  $x = \Lambda$ , либо  $x = \Lambda + x$  по доказанному ранее. Предположим далее, что  $P(y)$  истинно и покажем истинность  $P(y + s)$ .

Действительно, по предположению, один из случаев, указанных в предикате  $P(y)$ , верен. Если верно  $x = y$ , то  $x + s = y + s$  (реализуется случай  $x + z = y + s$ , где  $z = s$ ). Если верно  $x = y + z$ , где  $z \neq \Lambda$ , то  $z = z' + s$  (дихотомия) и  $x = (y + s) + z'$  (здесь реализуется либо случай  $x = y + s$ , если  $z' = \Lambda$ , либо случай  $x = (y + s) + z'$ , где  $z' \neq \Lambda$ ). Если же верно  $x + z = y$ , то  $x + (z + s) = y + s$  (реализуется случай  $x + z' = y + s$ , где  $z' \neq \Lambda$ ).

Таким образом,  $P(y + s)$  выполняется, индукция завершена.  $\square$

**Теорема 1.2** (Свойства произведения). Для любых  $s$ -отрезков  $x, y, z$

*P1*  $(x + y) \times z = x \times z + y \times z$  (правый дистрибутивный закон);

*P2*  $s \times x = x = x \times s$  (нейтральный элемент);

*P3*  $\Lambda \times x = \Lambda$  (мультипликативное свойство нуля);

*P4*  $x \times y = y \times x$  (коммутативность);

*P5*  $z \times (x + y) = z \times x + z \times y$  (левый дистрибутивный закон);

*P6*  $(x \times y) \times z = x \times (y \times z)$  (ассоциативность);

*P7* если  $x \times y = \Lambda$ , то  $x = \Lambda$  или  $y = \Lambda$  (отсутствие делителей нуля);

*P8* если  $x \times z = y \times z$  и  $z \neq \Lambda$ , то  $x = y$  (правило сокращения);

### 1.1.3 Отношение порядка

Введем арифметический аналог геометрического отношения «лежать между», а именно: скажем, что для  $s$ -отрезков  $x$  и  $y$  выполняется отношение  $x < y$ , если существует такой  $s$ -отрезок  $z \neq \Lambda$ , что  $y = x + z$ . Также наряду с отношением  $<$  часто используется нестрогое неравенство:  $x \leq y$ , когда  $x = y$  или  $x < y$ .

**Теорема 1.3** (Линейная упорядоченность). Отношение  $<$  на  $s$ -отрезках является линейным порядком, т.е. для любых  $x, y, z$ :

1. не верно  $x < x$  (антирефлексивность);
2. если  $x < y$  и  $y < z$ , то  $x < z$  (транзитивность);
3. верно одно и только одно: либо  $x < y$ , либо  $y < x$ , либо  $x = y$  (трихотомия).

Кроме того, если  $x < y$ , то  $x + s \leq y$ .

Эта теорема легко выводится из теоремы 1.1 о свойствах сложения.

**Теорема 1.4** (Монотонность). Отношение  $<$  строго монотонно относительно сложения и умножения, т.е.

*O1*  $x + z < y + z$  тогда и только тогда, когда  $x < y$ ;

*O2* если  $x < y$  и  $z \neq \Lambda$ , то  $x \times z < y \times z$ ;

*O3* если  $x \times z < y \times z$ , то  $x < y$ .

**Теорема 1.5** (Вполне упорядоченность).  *$s$ -отрезки вполне упорядочены отношением  $<$ , т.е. каков бы ни был одноместный предикат  $P(x)$ , истинный хотя бы для одного  $s$ -отрезка  $x$ , найдется наименьший  $x$ , для которого  $P$  истинно.*

*Доказательство.* Пусть задан одноместный не тождественно ложный предикат  $P(x)$ . Рассмотрим предикат  $Q(x)$  следующего вида:

$$\forall y (P(y) \rightarrow (x \leq y)).$$

Предположим, что теорема не верна, т.е. не существует наименьшего  $x$  такого, что  $P(x)$ , и докажем при этом условия истинность  $Q(x)$  индукцией по  $x$ .

Действительно,  $Q(\Lambda)$  истинно, т.к.  $\Lambda \leq y$  при любом  $y$ .

Пусть  $Q(x)$  истинно, покажем истинность  $Q(x + s)$ . Нам дано условие:  $\forall y P(y) \rightarrow x \leq y$ . Ясно, что  $P(x)$  ложно, иначе  $x$  был бы наименьшим искомым элементом. Следовательно, если  $P(y)$  истинно, то  $x < y$  (исключили равенство), и тогда  $x + s \leq y$ . Т.е. для любого  $y$  имеет место импликация  $P(y) \rightarrow x + s \leq y$ , т.е. выполняется  $Q(x + s)$ .

Таким образом,  $Q(x)$  истинно для всех  $x$ .

По условию теоремы  $P(x)$  истинно для некоторого  $x$ . В то же время  $Q(x + s)$  также истинно, откуда, полагая в формуле  $Q$   $y = x$ , получаем импликацию  $P(x) \rightarrow x + s \leq x$ . Отсюда следует, что для всех  $x$  имеем  $x + s \leq x$ . Но это противоречит трихотомии отношения  $<$ .  $\square$

Отсюда выводится более общий принцип индукции

**Теорема 1.6.** *Пусть  $P(x)$  — одноместный предикат. Если для всякого  $x$  имеет место*

$$(\forall y < x P(y)) \rightarrow P(x),$$

*то для любого  $x$  истинно  $P(x)$ .*

### 1.1.4 Универсализация

$s$ -отрезки и символьные строки, состоящие из буквы  $s$ , удобнее записывать иначе. Положим

$$0 = \Lambda, \quad 1 = s, \quad 2 = ss, \quad 3 = sss, \quad 4 = ssss, \dots,$$

т.е., добавляя очередной  $s$ , мы будем увеличивать последнюю цифру в записи в порядке 0123456789, а при достижении 9, будем сбрасывать ее в 0 и применять данное правило к предпоследней цифре, и т.д. Если цифры кончились и нам нужно увеличить 9, то мы также сбрасываем ее в 0 и впереди добавляем 1. Иначе говоря, мы будем заменять  $s$ -строку обычной десятичной



записью количества букв  $s$  в ней тогда, когда это будет проще и не вызовет коллизий в понимании текста.

Всякая система чисел  $0, 1, 2, \dots$ , для которой определены операции сложения и умножения, удовлетворяющие свойствам  $I - VII$ , а также определено отношение  $<$ , удовлетворяющее теоремам  $??-??$ , называется **системой натуральных чисел**, а ее элементы — **натуральными числами**.

Построение с помощью  $s$ -отрезков, произведенное выше, показывает возможность построения модели натуральных чисел.

Однако, при этом мы воспользовались некоторым мерным отрезком  $AB$ , некоторой прямой  $l$  и некоторым направлением  $QO$  на данной прямой. Зависит ли полученная «арифметика» натурального ряда от выбора этих параметров?

Пусть мы взяли еще какой-то мерный отрезок  $A'B'$ , прямую  $l'$  и направление на ней  $Q'O'$ , и построили новые  $O'$ -точки:

$$O', O'^+, O'^{++}, O'^{+++}, \dots$$

Построим соответствие  $F$  между  $O$ -точками и  $O'$ -точками по правилу:

$$F(X) = \begin{cases} O', & \text{если } X = O, \\ F(Z)^+, & \text{если } X = Z^+. \end{cases}$$

**Теорема 1.7.** *Соответствие  $F$  является взаимно однозначным, сохраняет операцию сложения и порядок точек.*

*Доказательство.* Для начала заметим, что значениями  $F$  могут быть только  $O'$ -точки. Если это не так, то найдем ближайшую к  $O$  точку  $X$  такую, что  $F(X)$  не является  $O'$ -точкой.  $X \neq O$ , значит,  $X = Z^+$ , где уже  $Z$  есть  $O$ -точка. Но тогда  $F(X) = F(Z)^+$  есть  $O'$ -точка, т.к.  $F(Z)$  есть  $O'$ -точка в силу выбора  $X$ .

Покажем, что  $F$  сохраняет сложение (предполагается, что для  $O'$ -точек оно определено так же, как для  $O$ -точек), т.е.

$$F(X + Y) = F(X) + F(Y).$$

Ясно, что при  $Y = O$  это верно, т.к.  $F(X + O) = F(X) = F(X) + O' = F(X) + F(O)$ . Предположим, что равенство верно при некотором  $Y$  и покажем его для  $Y^+$ :

$$F(X + Y^+) = F((X + Y)^+) = F(X + Y)^+ = (F(X) + F(Y))^+ = F(X) + F(Y)^+ = F(X) + F(Y^+)$$

Теперь легко видеть, что если  $X \leq Y$ , то  $F(X) \leq F(Y)$ . Действительно,  $Y = X + Z$ , так что

□

## 1.2 Диэдральные группы

---

### Аннотация.

Цель: знакомство с языком алгебры.

---

### 1.2.1 План

1. Группа симметрий правильного треугольника, ее таблица Кэли.
2. Группа симметрий ромба (четверная группа Клейна), ее таблица Кэли.
3. Группа симметрий правильного многоугольника (снежинки).
4. *Почему помимо вращений можно обойтись только одной симметрией для описания всех движений?*
5. Понятие группы  $(G, \circ)$  и подгруппы, смежные классы, порядок элемента.
6. Несколько слов о базисе группы, порождающие элементы, эквивалентные базисы.
7. Базисы  $S_3$  и  $V_4$ .

### 1.2.2 Группа симметрий правильного треугольника

Представим себе, что есть дверь и в ней замок треугольной формы (треугольник правильный). Вершины треугольника пронумерованы числами 1, 2, 3. Чтобы открыть дверь, нужно вставить в замок ключ (формы треугольной призмы) в правильном положении. Углы ключа также пронумерованы цифрами 1, 2, 3, но это не означает корректного соответствия цифрам замка. Вставить ключ можно как с одной стороны двери, так и с другой. Каковы шансы открыть дверь с первого раза?

Чтобы это описать математическим языком, рассмотрим все возможные соединения ключа и замка, которые сводятся к следующим действиям:

- а) вставить ключ так, что его бородка вертикальна,
- б) вынуть и повернуть ключ до совмещения следующих углов, снова вставить, и так далее,
- с) те же действия с другой стороны двери.

Таким образом, на треугольнике вводятся следующие элементарные операции, переводящие треугольник в себя (со сменой номеров вершин):

- $\text{id}$  — тождественное преобразование (ничего не меняем),
- $R_\varphi$  — поворот на угол  $\varphi$ , где  $\varphi \in \{120^\circ, 240^\circ\}$ ,
- $S_1$  — симметрия относительно биссектрисы, проходящей через 1-ю вершину треугольника (верхнюю).

Итого имеем 4 преобразования. Вопрос: *могут ли быть еще какие-то преобразования и сколько их?*

Сразу же очевидно, что симметрию можно выполнять относительно двух оставшихся биссектрис, т.е. у нас добавляются симметрии  $S_2$  и  $S_3$ .

**Теорема 1.8.** *Преобразования правильного треугольника, при которых вершины переходят в вершины, а ребра в ребра с сохранением инцидентности (т.е. без разрушения треугольника), исчерпываются списком  $\text{id}, R_{120}, R_{240}, S_1, S_2, S_3$ .*

*Доказательство.* Заметим, что при указанных преобразованиях разные вершины всегда остаются разными и, кроме того, все вершины всегда переходят во все вершины (никакая не выпадает). Это значит, что всякое такое преобразование осуществляет перестановку вершин. Но все различные перестановки вершин таковы:

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

Нетрудно видеть, что эти перестановки в точности соответствуют преобразованиям  $\text{id}, R_{120}, R_{240}, S_1, S_2, S_3$ .  $\square$

Предполагая, что только одно положение ключа с одной стороны двери и одно — с другой стороны соответствуют открыванию замка, мы теперь можем ответить на поставленный в начале вопрос: у нас ровно 2 шанса из 6, что замок будет открыт.

Предположим теперь, что ключом пользуется сразу несколько человек (например, этот ключ весит 100 кг, поэтому приходится меняться), и каждый из них проделывает строго одно из указанных преобразований (свое любимое). Назовем этих людей «операторами». Какое преобразование получится, если два оператора подряд произведут одно из указанных преобразований?

Ясно, что ничего нового мы не получим, но мы хотим знать, сколько и каких операторов нужно, чтобы, чередуя их действия, получить все преобразования треугольника. Для этого составим таблицу Кэли (сначала выполняется преобразование в столбце, затем — в строке):

id	$R_{120}$	$R_{240}$	$S_1$	$S_2$	$S_3$
$R_{120}$	$R_{240}$	id	$S_2$	$S_3$	$S_1$
$R_{240}$	id	$R_{120}$	$S_3$	$S_1$	$S_2$
$S_1$	$S_3$	$S_2$	id	$R_{240}$	$R_{120}$
$S_2$	$S_1$	$S_3$	$R_{120}$	id	$R_{240}$
$S_3$	$S_2$	$S_1$	$R_{240}$	$R_{120}$	id

Таблица 1.1: Таблица Кэли для треугольника.

Таблица Кэли является аналогом таблицы умножения, если под умножением понимать композицию отображений, т.е. последовательное применение операторов. Заметим, что, в отличие от обычного умножения, операторы не коммутируют, т.е. результат их действий зависит от того, в каком порядке они работают. Например,  $R_{120}S_1 \neq S_1R_{120}$  (таблица не симметрична относительно главной диагонали).

Раскрывая эту таблицу, мы можем получить результат последовательного применения 3-х, 4-х и т.д. операторов. При этом, мы можем заметить, что произведение трех одинаковых поворотов подряд (их третья степень) дает id, а произведение двух одинаковых симметрий подряд также дает id. Условимся последовательное применение какого-либо оператора  $k$  раз записывать как его степень.

Кроме того, можно заметить что  $R_{120}^2 = R_{240}$ , что уже говорит о том, что один оператор  $R_{240}$  можно заменить на степень  $R_{120}$ . Верно и обратное:  $R_{240}^2 = R_{120}$ . Кроме того, все симметрии можно получить как комбинации одной симметрии и поворотов:  $S_2 = S_1R_{120}$ ,  $S_3 = S_1R_{240} = S_1R_{120}^2$ .

Итак, видим, что для осуществления всех видов операций поворота и симметрии треугольника нам достаточно иметь двух операторов (одного поворота и одной симметрии) и применять их в различной последовательности. Любая пара поворот-симметрия образует базис всех преобразований треугольника в себя.

При этом, невозможно уменьшить базис, т.е. невозможно ограничиться только одной симметрией или только одним или двумя поворотами. Однако, композиция двух разных симметрий дает поворот ( $R_{240} = S_1S_2$ ), а это значит, что в качестве базисных операторов можно брать и любые две различные симметрии!

30 минут |

### 1.2.3 Группа симметрий ромба

Аналогично треугольнику рассмотрим ромб, не являющийся квадратом. Нетрудно видеть, что его симметриями будут следующие преобразования:

$$\text{id}, \quad R_{180}, \quad S_1, \quad S_2, \quad (1.1)$$

где  $S_k$  — симметрии относительно диагоналей ромба.

**Теорема 1.9.** *Списком (1.1) исчерпываются все возможные преобразования ромба (с различными диагоналями) в себя, сохраняющие фигуру (т.е. расстояния между точками).*

*Доказательство.* Пронумеруем вершины ромба цифрами 1,2,3,4 (1 и 3 противоположны). Предположим, что при некотором преобразовании 1 переходит в 1. В этом случае 3 не может перейти ни в 1, ни в 2 или 4, иначе произойдет потеря инцидентности - вершина 3 либо совпадет с 1, либо будет соседней. Стало быть, 3 также останется на месте. Но тогда остается ровно два преобразования:  $\text{id}$  и симметрия относительно оси 13 (обозначим ее  $S_1$ ).

Очевидно также, что 1 не может перейти в 2 или 4, т.к. в противном случае расстояние 1-3 перейдет в расстояние 2-4, а это невозможно для ромба с различными диагоналями. Остается вариант перехода 1 в 3, который дает два оставшихся преобразования: поворот на  $180^\circ$  и симметрию относительно диагонали 24 (обозначим ее  $S_2$ ).

Если провести аналогичный анализ для остальных вершин, то мы получим те же самые преобразования.  $\square$

Отметим, что уже в случае ромба преобразований, сохраняющих его, сильно меньше, чем количество всех перестановок вершин (4 и 24).

Таблица Кэли для ромба:

id	$R_{180}$	$S_1$	$S_2$
$R_{180}$	id	$S_2$	$S_1$
$S_1$	$S_2$	id	$R_{180}$
$S_2$	$S_1$	$R_{180}$	id

Таблица 1.2: Таблица Кэли для ромба.

Легко видеть также, что и в данном случае в качестве базисных преобразований можно выбрать либо пару вращение–симметрия, либо пару из двух симметрий.

10 минут |

### 1.2.4 Группа симметрий правильного многоугольника

Наконец, рассмотрим еще один случай преобразований фигуры в себя (по-научному: автоморфизмов). Пусть имеется правильный  $n$ -угольник. Тогда очевидными преобразованиями, сохраняющими форму и размеры фигуры, будут:

$$R_{360k/n}, S_1, \dots, S_k, \quad k = \overline{1, n}$$

В случае четного  $n$  в многоугольнике все вершины разбиваются на пары противоположных, лежащих на общей оси симметрии, поэтому имеется  $n/2$  осей симметрии, проходящих через вершины, и  $n/2$  осей, проходящих через середины сторон. В случае нечетного  $n$  на каждую вершину приходится своя ось симметрии.

Как и в предыдущих случаях, несложно показать, что этими  $2n$  преобразованиями исчерпываются все преобразования правильного многоугольника в себя, что, как видим, сильно меньше общего числа перестановок вершин, которое равно  $n!$  (совпадение получается только при  $n = 3$ ).

Однако и в этом случае в качестве базисных можно выбрать всего два преобразования:  $R_{360/n}$  и  $S_1$ , либо две симметрии, оси которых являются соседними.

Следует заметить, что в общем случае, когда мы рассматриваем движения плоскости, в базис достаточно включать вращения и всего лишь одну симметрию, т.к. они отвечают за смену ориентации фигуры, ее переворачивание на другую сторону плоскости.

5 минут |

### 1.2.5 Понятие группы

В рассмотренных примерах можно заметить некоторые общие особенности:

- Движения фигур описываются набором из нескольких преобразований плоскости, сохраняющих расстояния (размеры, инцидентность).
- Существует преобразование  $\text{id}$ , которое ничего не меняет (поворот на нулевой угол), в том числе, его композиция с любым другим преобразованием равно этому преобразованию.
- Композиция (т.е. последовательное применение нескольких) преобразований — тоже преобразование из того же набора.
- В композиции из нескольких преобразований можно по-разному составлять скобки:  $R_{120}(S_1 S_2) = (R_{120} S_1) S_2$ .

- У каждого преобразования есть обратное (например, обратным к  $R_{120}$  является  $R_{240}$ ), т.е. такое, что их композиция есть  $\text{id}$ .
- Менять преобразования местами не всегда возможно:  $R_{120}S_1 \neq S_1R_{120}$ .
- Каждое преобразование в некоторой степени (т.е. будучи выполненное подряд несколько раз) дает  $\text{id}$ .

Абстрагируясь от замков, ключей, треугольников, ромбов, плоскостей и геометрических картинок, дадим чисто алгебраическое определение, учитывающее только тот факт, что у нас есть какой-то (конечный) набор существ, которые можно выстраивать в цепочку композиций, и которые при этом обладают перечисленными свойствами.

Итак, пусть имеется множество  $G$  с бинарной операцией композиции  $\circ$ , которое удовлетворяет следующим свойствам:

G1 операция композиции *замкнута* на  $G$ :  $\forall g_1, g_2 \in G: g_1 \circ g_2 \in G$  (свойство группоида);

G2 операция композиции *ассоциативна*:  $\forall g_1, g_2, g_3 \in G: (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ ;

G3 существует *нейтральный элемент*:  $\exists e \in G: \forall g \in G: g \circ e = g = e \circ g$ ;

G4 у каждого элемента существует *обратный*:  $\forall g \in G: \exists g' \in G: g \circ g' = e = g' \circ g$ .

Тогда говорят, что множество  $G$  вместе с операцией  $\circ$  образует **группу**. Если дополнительно потребовать, чтобы операция  $\circ$  была коммутативна (т.е.  $\forall g_1, g_2 \in G: g_1 \circ g_2 = g_2 \circ g_1$ ), то такая группа называется **абелевой**.

В примерах выше мы встретили абелеву группу симметрий ромба и неабелевы группы симметрий правильных многоугольников.

Договоримся в дальнейшем, если не указанного обратное, групповую операцию  $\circ$  называть умножением, ее обозначение опускать в формулах, т.е. вместо  $g \circ g'$  записывать  $gg'$ , а саму группу называть мультипликативной.

Аксиомы группы, указанные выше, постулируют существование нейтрального и обратного элементов, но не гарантируют их однозначного определения.

**Теорема 1.10.** *В группе нейтральный элемент единственный, обратный элемент определяется однозначно.*

*Доказательство.* Предположим, что существует два нейтральных элемента  $e_1$  и  $e_2$ . Тогда, в силу того, что  $e_1$  — нейтральный, имеем равенство  $e_1e_2 = e_2$ , а в силу того, что  $e_2$  — нейтральный, имеем  $e_1e_2 = e_1$ . Итого,

$$e_1 = e_1e_2 = e_2,$$

т.е.  $e_1 = e_2$ . Таким образом, нейтральный элемент в группе всегда единственный.

Пусть  $g'$  и  $g''$  — обратные к  $g$ , т.е.

$$gg' = e = g'g, \quad gg'' = e = g''g.$$

Отсюда получаем:

$$g'' = eg'' = (g'g)g'' = g'(gg'') = g'e = g',$$

т.е.  $g' = g''$ . □

Нейтральный элемент обозначается по-разному в зависимости от контекста. В примерах с преобразованиями фигур мы его обозначали  $\text{id}$ , т.к. это было тождественное преобразование плоскости. Часто его также обозначают  $I$ ,  $E$  или  $e$ . По умолчанию мы будем предполагать, что если групповая операция названа умножением, то нейтральный элемент называется единицей и обозначается  $e$ .

В том случае, когда групповая операция названа сложением, нейтральный элемент называется нулём и обозначается  $0$  или  $O$ , а сама группа называется аддитивной.

Под записью  $g^k$  будем понимать (как и ранее) композицию элемента  $g$  с самим собой  $k$  раз, т.е.

$$g^k = \underbrace{gg \dots g}_{k \text{ раз}}, \quad k > 0.$$

Поскольку для всякого элемента  $g$  группы существует, и притом единственный, обратный, его принято обозначать  $g^{-1}$  (если группа мультипликативная) или  $-g$  (если она аддитивная).

Кроме того, обозначим  $g^0 = e$  и  $g^{-k} = (g^k)^{-1}$ . Пользуясь индукцией, несложно показать, что степени в группе подчиняются обычным правилам арифметики:

$$g^k g^m = g^{k+m}, \quad k, m \in \mathbb{Z}.$$

Ввиду существования и единственности обратного элемента в группе можно любые равенства делить на один и тот же элемент. Покажем это на примере конечных групп.

**Теорема 1.11.** *В конечной группе для любого элемента  $g$  существует такая натуральная степень  $k > 0$ , что  $g^k = e$ .*

*Доказательство.* Пусть в группе  $G$  всего  $n$  элементов. Рассмотрим ряд степеней произвольно выбранного элемента  $g$ :

$$g^1, g^2, g^3, \dots, g^n, g^{n+1}.$$



Ясно, что какие-то две из этих степеней совпадают (принцип Дирихле!), например,

$$g^k = g^m, \quad k < m.$$

Домножим справа это равенство на  $g^{-k}$  (т.е. разделим на  $g^k$ ):

$$e = g^k g^{-k} = g^m g^{-k} = g^{m-k},$$

т.е.  $m - k$  — искомая степень. □

Минимальное положительное  $k$ , при котором  $g^k = e$ , называется **порядком элемента**  $g$  в группе  $G$ .

Выше мы уже видели, что в группе симметрий треугольника

$$R_{120}^3 = R_{240}^3 = \text{id}, \quad S_1^2 = S_2^2 = S_3^2 = \text{id}.$$

Отметим также, что количество элементов в группе называется **порядком группы**.

Глядя на выписанные выше таблицы Кэли, можно отметить еще одну особенность: композиции поворотов всегда дают повороты. Иначе говоря, если рассмотреть только часть группы симметрий фигуры, включающую повороты и только их (вместе с  $\text{id}$ ), то мы также будем иметь дело с группой, но только меньшего порядка.

В общем случае, говорят, что  $G'$  есть **подгруппа** группы  $G$ , если  $G' \subseteq G$  и сама является группой с этой же операцией. Так, все повороты в группах симметрий правильных многоугольников и ромба образуют подгруппы. В то же время симметрии подгрупп не образуют.

Произведением (или суммой в случае аддитивной группы) **по Минковскому** называют следующие операции над элементами и множествами:

$$gH = \{gh \mid h \in H\}, \quad Hg = \{hg \mid h \in H\}, \quad HH' = \{hh' \mid h \in H \wedge h' \in H'\},$$

где  $g \in G$ ,  $H, H' \subseteq G$ .

## 1.3 Движения окружности

---

### Аннотация.

Цель: разобраться с группой  $O(2)$  и ее подгруппами.

---

**Определение:** преобразование пространства (прямой/плоскости), сохраняющее размеры (попарные расстояния), называется **движением** (изометрией).

---

### 1.3.1 План

1. Классификация движений окружности: лемма о гвоздях.
2. *Почему помимо вращений можно обойтись только одной симметрией?* Все движения есть композиция вращений и одной выделенной симметрии.
3. Эквивалентность базисов группы движений: все вращения + одна симметрия, все симметрии.
4. Конечные подгруппы, соответствующие диэдральным и циклическим группам.
5. Бесконечные подгруппы: иррациональность числа  $\pi$  и группа  $(\mathbb{Z}, +)$  (вращение на несоизмеримый с  $\pi$  угол).
6. Арифметика остатков: конечные циклические группы и факторизация  $\mathbb{Z}/n\mathbb{Z}$ .

### 1.3.2 Классификация движений окружности

## 1.4 Движения и гомотетии вещественной прямой

---

#### Аннотация.

Цель: найти кольцо  $(\mathbb{R}, +, \times)$ .

---

#### План:

1. Классификация движений прямой: аналог теоремы Шаля.
2. *Почему можно обойтись только одной симметрией?* Все движения есть композиция смещений и одной выделенной симметрии (умножение на  $-1$ ).
3. Эквивалентность базисов: все сдвиги + одна симметрия, все симметрии.
4. Все сдвиги образуют группу, изоморфную  $(\mathbb{R}, +)$ .
5. Действие группы  $\mathbb{Z}$  на прямой. Понятие орбиты.
6. **Определение:** гомотетией с заданным центром и коэффициентом называется преобразование пространства (прямой/плоскости), при котором все векторы с началом в этом центре удлиняются на заданный коэффициент. Подобие на прямой — это гомотетия + сдвиг.
7. Подобия на прямой можно описать с помощью кольца  $(\mathbb{R}, +, \times)$ .

## 1.5 Движения и подобия на плоскости

---

### Аннотация.

Цель: найти кольцо  $(\mathbb{C}, +, \times)$ .

---

### План:

1. Классификация движений плоскости: теорема Шаля.
2. *Почему можно обойтись только одной симметрией?* Все движения есть композиция параллельных переносов, поворотов и одного выделенного отражения (умножение на  $-1$  вдоль одной оси).
3. Эквивалентность базисов: все параллельные переносы  $+$  все повороты  $+$  одна симметрия, все отражения.
4. Все параллельные переносы образуют группу, изоморфную  $(\mathbb{C}, +)$ .
5. Формула Эйлера и число  $e$ . Группа корней из 1. Связь умножения комплексных чисел со сложением в группе вычетов.
6. Мультипликативная группа  $|z| = 1$ , ее действие на комплексной плоскости. Орбиты.
7. Подобия на плоскости — это поворотные гомотетии  $+$  параллельные переносы.
8. Подобия на плоскости описываются арифметикой кольца  $(\mathbb{C}, +, \times)$ .

## 1.6 Делимость в евклидовых кольцах

---

### Аннотация.

Цель: общий вывод основной теоремы арифметики и ее следствий.

---

### План:

1. Понятие кольца.
  2. Понятие нормы и обратимых элементов кольца.
  3. Алгоритм Евклида деления с остатком.
  4. Представление НОД двух чисел в виде линейной комбинации этих чисел.
-

5. Основная теорема арифметики. Факториальное кольцо.
6. Приложение к кольцам: многочленов, гауссовых чисел.
7. Примеры нефакториальных колец.
8. Несколько теорем теории делимости: МТФ, РТФ,...